			Tender No : RAILTEL/TENDER/OT/CO/DNM/2019-20/Security & Infra Solution of DC & DR /489 Dtd. 06.06.2019 Infra/489			
			Name of the work : Supply, Installation, Testing &Commissioning of Security Solution and Expansion of Cloud Infrastructure for Data Center (DC & DR) of RailTel.			
	Firm Name:	**Intech Infonet Private Limited**		**vishal kaushik: vishal@intecinfonet.com**		
SN	**Page/ Clause no. / Point no.**	**Topics**	**Original Clause**	**Query /Requested Changes / Should read as,**	**Reason**	**RailTel Resonse**
1	Page 59 Point 36	Cloud Orchestration	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later, Microsoft Hyper-V, System Center 2016 or above, RedHat virtualization	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later/ Microsoft Hyper-V and System Center 2016 or above / RedHat virtualization.		Refer Corrigendum-II
2	Page 60 Point 46	Cloud Operations & Management	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi, Hyper-V, RHEV	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi/ Hyper-V/ RHEV.		Refer Corrigendum-II
3	Page 60 Point 49	Cloud Operations & Management	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware, Hyper-v, RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware / Hyper-v / RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis		Refer Corrigendum-II
4	Page 77 Point 12.1.8	Technical Capability	The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.	The bidder shall furnish documentary proof of backend support including software upgrades.	Spares availability is not applicable for Software products.	As per RFP
5	Page 73 Point 3.2	Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty.	Should be deleted for software products/ components.	Long Term Maintenance Support after completion of Warranty period for Software products ranges from 22% to 27% per annum.	As per RFP. Bidder can quote higher rates for AMC
6	Page 51 Point 13	SOR-E- i- Rack Server: 13. Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	HCI node should have minimum number of 4 x 10G physical uplinks. All the host should have same sequence of physical uplinks. Hence, this clause should be changed as "2 x 1G RJ45 and 4 x 10G SFP+ populated with Multimode Transceivers."	This is required for redundant network connectivity on compute workload.	Refer Corrigendum-II
7		Query		Please confirm if Compute Infra (Cores) required for Management cluster have been factored into the sizing or will be given separately by the customer		Clarification: Compute Infra (Cores) required for Management cluster has been factored into the sizing.
8		Query		Please confirm if the 3rd party Softwares required for management cluster like Operating Sytems and Data base will be provided by the Customer.		Clarification: The 3rd party Softwares required for management cluster like Operating Sytems and Data base will be provided by the Bidder.
9		Query		The Scope of work doesnot cover the Cloud infrastructure in detail, kindly consider the document enclosed for reference. (Letter has been enclosed for your referene)		Refer Corrigendum-II
Que						
SN	Page no.	Clause No.	Clause Description	Clarification / Change request	Justification	
1	Page No.: 22, Clause No: 13	13	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix, and Mac OS.	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix	Understanding is there is no Mac OS in the environment, request you to relax this clause without Mac OS	As per RFP.

2	Page No.: 23, Clause No: 34	34	Solution Should have 48TB of Usable Capacity with HW RAID 60	Solution Should have absolute 80TB of Usable Capacity with minmum 2 copies using 8TB or higher drives	As there is no other backup media mechanism, request to have higher capacity for higher resilience	As per RFP
3	Page No.: 24, Clause No: 36	SOR-B: Backup Solution	Appliance Should have Hot Swappable Disks, In case of failure , individual drives can be replaced without impacting any other drives	The appliance solution should provide controller level redundancy. In case one of the controller fails the backup solution should not be affected. Each virtual controller node should provide minimum SSD/NVMe cache to ensure backup process does not have any bottleneck, The controller should have its own filesystem that will manage the backup storage including data protection, replication, deduplication & compression features, the filesystem should be distributed file system and should not rely on wrting the data adjacent to the controller	For redundancy feature & to ensure backup is maintained & restored as and when required. Request to add this clause	As per RFP.
4	Page No.: 50, SOR-E- i- Rack Server:	1: General Requirement	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates, system drift detection and secure erase security features inbuilt	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates.	request to relax " System drift detection and secure erase" for wider participation	As per RFP
5	Page No.: 51, SOR-E- i- Rack Server:	1: General Requirement	Inbuild Server Management iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping with historical power counters, Temperature monitoring & graphing through dashboard	iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping , Temperature monitoring & graphing through dashboard	request to relax "historical power counters" for wider participation	Refer Corrigendum-II
6	Page No.: 51, SOR-E- i- Rack Server:	2. Market position	The OEM for the proposed server must be in Leaders quadrant in the last two Gartner's report of "Magic Quadrant for Modular Servers".	The OEM for the proposed server must be in Leaders quadrant in the last Gartner's report of "Magic Quadrant for Modular Servers".	this clause restricits only 2 vendors to qualify, for wider participation request you to dilute "Two "	Refer Corrigendum-II
7	Page No.: 52, SOR-E- i- Rack Server:	21. Configuration & management	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, storage management, monitoring of FC, HBA & CNA & system health	There is no external storage, the system is running internal storage system	Refer Corrigendum-II
8	Page No.: 52, SOR-E- i- Rack Server:	23. Server security	- Silicon-based Hardware Root of Trust	Hardware Root of Trust	Silicon root of trust is vendor specific, request to use generic term as HW root of trust	As per RFP
9	Page No.: 52, SOR-E- i- Rack Server:		- Configuration and firmware drift detection	Configuration and firmware updates	The solution should be able to manage firmware updates. request to relax "drift detection"	As per RFP
10	Page No.: 52, SOR-E- i- Rack Server:	25. Warranty	03 years On-site comprehensive warranty with 24x7x365 remote hardware support.	03 years On-site comprehensive warranty with 24x7x365 remote hardware support with with automated transmission of support files to the OEM support center	For ease of management, request you to add this clause	Refer Corrigendum-II
11	Page No.: 26, SOR-C- i- Virtual Firewall	1	The solution should be virtual appliance based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The solution should be virtual appliance based and enterprise class (complete control from GUI and CLI/Dervice Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Refer Corrigendum-II
12	Page No.: 26, SOR-C –ii - UTM:	2	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI and CLI / Device Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Refer Corrigendum-II
13	Page No.: 26, SOR-C –ii - UTM:	3	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 4 x 1GE SFP ports with fully populated from day one	Please confirm whether proposed platform should additionally support 8 x 10G SFP+ ports in future	This ensure that propose platform doesn't require forklift upgrade and hence increases ROI	As per RFP
14	Page No.: 26, SOR-C –ii - UTM:	5	Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.	Please change the clause to "Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, and IPS) from day one."	As per industry standard terminology, NGFW mean Firewall supporting Firewall, Application Visibility, and IPS) and hence requesting change. Clause already include the phrase used by other vendor and hence requesting change	Refer Corrigendum-II
15	Page No.: 27, SOR-C –ii - UTM:	40	URL database should have at least 200 million+ sites and 50 + categories.	Please confirm whether proposed platform should support "URL database should have at least 200 million+ sites and 80 or more categories."	Solution with 200 million+ sites and just 50 categories would be less flexible and might create false positive. Hence it is requested to have support for higher categories	As per RFP

16	Page No.: 27, SOR-C –ii - UTM:	50	High Availability Configurations should support Active/Active / Clustering, Active/ Passive	Please change the clause to "High Availability Configurations should support Active/Active / Clustering or Active/ Passive"	Since the solution will be deployed at perimeter, it suggested to have bigger appliance from day one rather can clustering multiple appliance and hence requesting change	Refer Corrigendum-II
17	Page No.: 28, SOR-C –ii - UTM:	58	For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and other	Please change the clause to "For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and for Anti-APT based solution should have automatic local malware detection updates "	Different OEM use different technolgy to detect and block zero-day or unknown, few oem leverages AV based solution and other leverages Anti-APT and hence requesting change	As per RFP
18	26		New Clarification	Please confirm that whether proposed solution should include all license like URL Filtering, Zero-Day Protection from day one	This is to avoid any ambiguity and ensure all bidder include the require license from day one	Clarification: All features asked in RFP (Fw, IPS , Application Control , URL filterig , Anti Malware , Zero Day Protection , Anti Bot will be required from day 1)
	FIRM-2:	CIPL	Sudipta Banerjee: sudipta@cipl.org.in			
	Page/ Clause no./ Point no.	Topics	Original Clause	Query /Requested Changes / Should read as,	Reason	
	Page 59 Point 36	Cloud Orchestration	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later, Microsoft Hyper-V, System Center 2016 or above, RedHat virtualization	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later/ Microsoft Hyper-V and System Center 2016 or above / RedHat virtualization.		Already Clarified above
	Page 60 Point 46	Cloud Operations & Management	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi, Hyper-V, RHEV	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi/ Hyper-V/ RHEV.		Already Clarified above
	Page 60 Point 49	Cloud Operations & Management	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware, Hyper-v, RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware / Hyper-v / RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis		Already Clarified above
	Page 77 Point 12.1.8	Technical Capability	The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.	The bidder shall furnish documentary proof of backend support including software upgrades.	Spares availability is not applicable for Software products.	Already Clarified above
	Page 73 Point 3.2	Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty.	Should be deleted for software products/ components.	Long Term Maintenance Support after completion of Warranty period for Software products ranges from 22% to 27% per annum.	Already Clarified above
	Page 51 Point 13	SOR-E- i- Rack Server: 13. Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	HCI node should have minimum number of 4 x 10G physical uplinks. All the host should have same sequence of physical uplinks. Hence, this clause should be changed as "2 x 1G RJ45 and 4 x 10G SFP+ populated with Multimode Transceivers."	This is required for redundant network connectivity on compute workload.	Already Clarified above
		Query		Please confirm if Compute Infra (Cores) required for Management cluster have been factored into the sizing or will be given separately by the customer		Already Clarified above
		Query		Please confirm if the 3rd party Softwares required for management cluster like Operating Sytems and Data base will be provided by the Customer.		Already Clarified above

		Query		The Scope of work does not cover the Cloud infrastructure in detail, kindly consider the document enclosed for reference.		Already Clarified above
						Already Clarified above
	FIRM-3:	CISCO	Vishal Prakash: vishapra@cisco.com			
SN	Page no.	SOR No.	Clause No.		Clarification / Change request	Justification
1	Page No. 22, Clause No. 13	SOR-B: Backup Solution	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix, and Mac OS.	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix	Understanding is there is no Mac OS in the environment, request you to relax this clause without Mac OS	Already Clarified above
2	Page No. 23, Clause No 34	SOR-B: Backup Solution	Solution Should have 48TB of Usable Capacity with HW RAID 60	Solution Should have absolute 80TB of Usable Capacity with minmum 2 copies using 8TB or higher drives	As there is no other backup media mechanism, request to have higher capacity for higher resilience	Already Clarified above
3	Page No. 24, Clause No 36	SOR-B: Backup Solution	Appliance Should have Hot Swappable Disks, In case of failure , individual drives can be replaced without impacting any other drives	The appliance solution should provide controller level redundancy. In case one of the controller fails the backup solution should not be affected. Each virtual controller node should provide minimum SSD/NVMe cache to ensure backup process does not have any bottleneck, The controller should have its own filesystem that will manage the backup storage including data protection, replication, deduplication & compression features, the filesystem should be distributed file system and should not rely on wrting the data adjacent to the controller	For redundancy feature & to ensure backup is maintained & restored as and when required. Request to add this clause	Already Clarified above
4	Page No. 50, SOR-E- i- Rack Server:	1: General Requirement	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates, system drift detection and secure erase security features inbuilt	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates.	request to relax " System drift detection and secure erase" for wider participation	Already Clarified above
5	Page No. 51, SOR-E- i- Rack Server:	1: General Requirement	Inbuild Server Management iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping with historical power counters, Temperature monitoring & graphing through dashboard	iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping , Temperature monitoring & graphing through dashboard	request to relax "historical power counters" for wider participation	Already Clarified above
6	Page No. 51, SOR-E- i- Rack Server:	2. Market position	The OEM for the proposed server must be in Leaders quadrant in the last two Gartner's report of "Magic Quadrant for Modular Servers".	The OEM for the proposed server must be in Leaders quadrant in the last Gartner's report of "Magic Quadrant for Modular Servers".	this clause restricits only 2 vendors to qualify, for wider participation request you to dilute "Two "	Already Clarified above
7	Page No. 52, SOR-E- i- Rack Server:	21. Configuration & management	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, storage management, monitoring of FC, HBA & CNA & system health	There is no external storage, the system is running internal storage system	Already Clarified above
8	Page No. 52, SOR-E- i- Rack Server:	23. Server security	- Silicon-based Hardware Root of Trust	Hardware Root of Trust	Silicon root of trust is vendor specific, request to use generic term as HW root of trust	Already Clarified above
9	Page No. 52, SOR-E- i- Rack Server:		- Configuration and firmware drift detection	Configuration and firmware updates	The solution should be able to manage firmware updates. request to relax "drift detection"	Already Clarified above
10	Page No. 52, SOR-E- i- Rack Server:	25. Warranty	03 years On-site comprehensive warranty with 24x7x365 remote hardware support.	03 years On-site comprehensive warranty with 24x7x365 remote hardware support with with automated transmission of support files to the OEM support center	For ease of management, request you to add this clause	Already Clarified above
11	Page No. 26, SOR-C- i- Firewall:	1	The solution should be virtual appliance based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The solution should be virtual appliance based and enterprise class (complete control from GUI and CLI/Dervice Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Already Clarified above
12	Page No. 26, SOR-C- ii- UTM:	2	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI and CLI / Device Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Already Clarified above

13	Page No. 26, SOR-C- ii- UTM:	3	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 4 x 1GE SFP ports with fully populated from day one	Please confirm whether proposed platform should additionally support 8 x 10G SFP+ ports in future	This ensure that propose platform doesn't require forklift upgrade and hence increases ROI	Already Clarified above
14	Page No. 26, SOR-C- ii- UTM:	5	Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.	Please change the clause to "Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, and IPS) from day one."	As per industry standard terminology, NGFW mean Firewall supporting Firewall, Application Visibility, and IPS) and hence requesting change. Clause already include the phrase used by other vendor and hence requesting change	Already Clarified above
15	Page No. 27, SOR-C- ii- UTM:	40	URL database should have at least 200 million+ sites and 50 + categories.	Please confirm whether proposed platform should support "URL database should have at least 200 million+ sites and 80 or more categories."	Solution with 200 million+ sites and just 50 categories would be less flexible and might create false positive. Hence it is requested to have support for higher categories	Already Clarified above
16	Page No. 27, SOR-C- ii- UTM:	50	High Availability Configurations should support Active/Active / Clustering, Active/ Passive	Please change the clause to "High Availability Configurations should support Active/Active / Clustering or Active/ Passive"	Since the solution will be deployed at perimeter, it suggested to have bigger appliance from day one rather can clustering multiple appliance and hence requesting change	Already Clarified above
17	Page No. 28, SOR-C- ii- UTM:	58	For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and other	Please change the clause to "For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and for Anti-APT based solution should have automatic local malware detection updates "	Different OEM use different technolgy to detect and block zero-day or unknown, few oem leverages AV based solution and other leverages Anti-APT and hence requesting change	Already Clarified above
18	26		New Clarification	Please confirm that whether proposed solution should include all license like URL Filtering, Zero-Day Protection from day one	This is to avoid any ambiguity and ensure all bidder include the require license from day one	Already Clarified above
	FIRM-04:		Vmware	Tapan Johri: tjohri@vmware.com		
	Page/ Clause no./ Point no.	Topics	Original Clause	Query /Requested Changes / Should read as,	Reason	
	Page 59 Point 36	Cloud Orchestration	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later, Microsoft Hyper-V, System Center 2016 or above, RedHat virtualization	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later/ Microsoft Hyper-V and System Center 2016 or above / RedHat virtualization.		Already Clarified above
	Page 60 Point 46	Cloud Operations & Management	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi, Hyper-V, RHEV	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi/ Hyper-V/ RHEV.		Already Clarified above
	Page 60 Point 49	Cloud Operations & Management	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware, Hyper-v, RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware / Hyper-v / RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis		Already Clarified above
	Page 77 Point 12.1.8	Technical Capability	The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.	The bidder shall furnish documentary proof of backend support including software upgrades.	Spares availability is not applicable for Software products.	Already Clarified above
	Page 73 Point 3.2	Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty.	Should be deleted for software products/ components.	Long Term Maintenance Support after completion of Warranty period for Software products ranges from 22% to 27% per annum.	Already Clarified above
	Page 51 Point 13	SOR-E- i- Rack Server: 13. Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	HCI node should have minimum number of 4 x 10G physical uplinks. All the host should have same sequence of physical uplinks. Hence, this clause should be changed as "2 x 1G RJ45 and 4 x 10G SFP+ populated with Multimode Transceivers."	This is required for redundant network connectivity on compute workload.	Already Clarified above

		Query		Please confirm if Compute Infra (Cores) required for Management cluster have been factored into the sizing or will be given separately by the customer		Already Clarified above
		Query		Please confirm if the 3rd party Softwares required for management cluster like Operating Sytems and Data base will be provided by the Customer.		Already Clarified above
	FIRM-05:	Exato Technologies Pvt. Ltd.		Varun Gupta: varun.gupta@exatotechnologies.com		
	Page/ Clause no./ Point no.	**Topics**	**Original Clause**	**Query /Requested Changes / Should read as,**	**Reason**	
	Page 59 Point 36	Cloud Orchestration	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later, Microsoft Hyper-V, System Center 2016 or above, RedHat virtualization	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later/ Microsoft Hyper-V and System Center 2016 or above / RedHat virtualization.		Refer Corrigendum-II-II
	Page 60 Point 46	Cloud Operations & Management	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi, Hyper-V, RHEV	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi/ Hyper-V/ RHEV.		Already Clarified above
	Page 60 Point 49	Cloud Operations & Management	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware, Hyper-v, RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware / Hyper-v / RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis		Already Clarified above
	Page 77 Point 12.1.8	Technical Capability	The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.	The bidder shall furnish documentary proof of backend support including software upgrades.	Spares availability is not applicable for Software products.	Already Clarified above
	Page 73 Point 3.2	Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty.	Should be deleted for software products/ components.	Long Term Maintenance Support after completion of Warranty period for Software products ranges from 22% to 27% per annum.	Already Clarified above
	Page 51 Point 13	SOR-E- i- Rack Server: 13. Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	HCI node should have minimum number of 4 x 10G physical uplinks. All the host should have same sequence of physical uplinks. Hence, this clause should be changed as "2 x 1G RJ45 and 4 x 10G SFP+ populated with Multimode Transceivers."	This is required for redundant network connectivity on compute workload.	Already Clarified above
		Query		Please confirm if Compute Infra (Cores) required for Management cluster have been factored into the sizing or will be given separately by the customer		Already Clarified above
		Query		Please confirm if the 3rd party Softwares required for management cluster like Operating Sytems and Data base will be provided by the Customer.		Already Clarified above
	15	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	Is the expectation by this requirement is that the proposed solution should have a minimum of 6000 signatures as default to detect and protect Web Applications. Kindly clarify		Refer Corrigendum-II
	19	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	we understand that it's a multimode SFPs that is required but as required the appliance has to be fully populated request you to Kindly clarify how many Interfaces is required for each type 1Gig, 10Gig and 40gig. As there could be a possibility of permutation combination on the type and interfaces proposed while fully populating the appliance SFP slots		Refer Corrigendum-II

	19	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	Gartner report of 2019 is not yet published so the Gartner report of 2017/2018 will suffice kindly confirm		Already Clarified above
	20	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution should support Unified Anti-Bot Detection and Protection & Cloning Application Traffic	Does this clause means that a proposed WAF solution should have capability to detect and mitigate BOT attacks using multiple level of security checks Via Bot Signature, Application Figure printing, Java Challenge, Browser capability check and Captcha. Kindly confirm		As per RFP
	20	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	Kindly elaborate		Refer Corrigendum-II
	72	CHAPTER 4 - - - COMMERCIAL TERMS & CONDITIONS. - - - 3. Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added to the equipment cost towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five years differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 5 years after the warranty	3.5% AMC for security solution like WAF or any similar security solution is not a realistic %. We request Railtel to kindly make this clause to at least 15% per annum instead of 3.5% per annum		Already Clarified above
		CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The proposed WAF solution should also have capability for BOT Detection that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	To be added New	As per RFP
	19	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	In case of RMA Process, Define the no of days to deliver the solution.	Kindly elaborate as RMA is NBD, do you mean to ask how many days will it take to deliver the hardware onsite in case of RMA?		As per RFP
	50	SOR-E- i- Rack Server:	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates, system drift detection and secure erase security features inbuilt	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates.	request to relax " System drift detection and secure erase" for wider participation	Already Clarified above
	51	SOR-E- i- Rack Server:	Inbuild Server Management iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping with historical power counters, Temperature monitoring & graphing through dashboard	iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping , Temperature monitoring & graphing through dashboard	request to relax "historical power counters" for wider participation	Already Clarified above
	51	SOR-E- i- Rack Server:	The OEM for the proposed server must be in Leaders quadrant in the last two Gartner's report of "Magic Quadrant for Modular Servers".	The OEM for the proposed server must be in Leaders quadrant in the last Gartner's report of "Magic Quadrant for Modular Servers".	this clause restricits only 2 vendors to qualify, for wider participation request you to dilute "Two "	Already Clarified above
	52	SOR-E- i- Rack Server:	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, storage management, monitoring of FC, HBA & CNA & system health	There is no external storage, the system is running internal storage system	Already Clarified above
	52	SOR-E- i- Rack Server:	- Silicon-based Hardware Root of Trust	Hardware Root of Trust	Silicon root of trust is vendor specific, request to use generic term as HW root of trust	Already Clarified above

	52	SOR-E- i- Rack Server:	- Configuration and firmware drift detection	Configuration and firmware updates	The solution should be able to manage firmware updates. request to relax "drift detection"	Already Clarified above
	52	SOR-E- i- Rack Server:	03 years On-site comprehensive warranty with 24x7x365 remote hardware support.	03 years On-site comprehensive warranty with 24x7x365 remote hardware support with with automated transmission of support files to the OEM support center	For ease of management, request you to add this clause	Already Clarified above
	26	SOR-C –i -Virtual Firewall:	The solution should be virtual appliance based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The solution should be virtual appliance based and enterprise class (complete control from GUI and CLI/Dervice Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Already Clarified above
	26	SOR-C –ii - UTM:	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)	Please change the clause to "The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI and CLI / Device Manager)"	firewall appliance physical or virtual can be managed either using Centralized Management platform or inbuilt device manager. CLI mode is not required hence requesting change	Already Clarified above
	26	SOR-C –ii - UTM:	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 4 x 1GE SFP ports with fully populated from day one	Please confirm whether proposed platform should additionally support 8 x 10G SFP+ ports in future	This ensure that propose platform doesn't require forklift upgrade and hence increases ROI	Already Clarified above
	26	SOR-C –ii - UTM:	Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.	Please change the clause to "Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, and IPS) from day one."	As per industry standard terminology, NGFW mean Firewall supporting Firewall, Application Visibility, and IPS) and hence requesting change. Clause already include the phrase used by other vendor and hence requesting change	Already Clarified above
	27	SOR-C –ii - UTM:	URL database should have at least 200 million+ sites and 50 + categories.	Please confirm whether proposed platform should support "URL database should have at least 200 million+ sites and 80 or more categories."	Solution with 200 million+ sites and just 50 categories would be less flexible and might create false positive. Hence it is requested to have support for higher categories	Already Clarified above
	27	SOR-C –ii - UTM:	High Availability Configurations should support Active/Active / Clustering, Active/ Passive	Please change the clause to "High Availability Configurations should support Active/Active / Clustering or Active/ Passive"	Since the solution will be deployed at perimeter, it suggested to have bigger appliance from day one rather can clustering multiple appliance and hence requesting change	Already Clarified above
	28	SOR-C –ii - UTM:	For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and other	Please change the clause to "For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and for Anti-APT based solution should have automatic local malware detection updates "	Different OEM use different technology to detect and block zero-day or unknown, few oem leverages AV based solution and other leverages Anti-APT and hence requesting change	Already Clarified above
	26		New Clarification	Please confirm that whether proposed solution should include all license like URL Filtering, Zero-Day Protection from day one	This is to avoid any ambiguity and ensure all bidder include the require license from day one	Already Clarified above
Firm 2:		Millennium Automation Private Ltd.		Amar Pratap: amarp@milleniumsystem.com		
	FOR SOR-A					
SL#	Page no. & Clause No.	RFP Volume Section and sub-section	Content in the RFP	Clarification sought/ Change Request		
1	Page No.: 15, Clause No.: 22	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	Is the expectation by this requirement is that the proposed solution should have a minimum of 6000 signatures as default to detect and protect Web Applications. Kindly clarify		Already Clarified above

2	Page No.: 19, Clause No.: 104	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	we understand that it s a multimode SFPs that is required but as required the appliance has to be fully populated request you to Kindly clarify how many Interfaces is required for each type 1Gig, 10Gig and 40gig. As there could be a possiblity of permutation combination on the type and interfaces proposed while fully populating the appliance SFP slots		Already Clarified above
3	Page No.: 19, Clause No.: 103	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	Gartner report of 2019 is not yet published so the Gartner report of 2017/2018 will suffice kindly confirm		Already Clarified above
4	Page No.: 20, Clause No.: 128	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution should support Unified Anti-Bot Detection and Protection & Cloning Application Traffic	Does this clause means that a proposed WAF solution should have capability to detect and mitigate BOT attacks using multiple level of security checks Via Bot Signature, Application Fingure printing, Java Challenge, Browser capability check and Captcha. Kindly confirm		Already Clarified above
5	Page No.: 20, Clause No.: 127	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	Kindly elaborate		Already Clarified above
6	Page No.: 72, Clause No.: 3.2	CHAPTER 4 - - - COMMERCIAL TERMS & CONDITIONS. - - - 3. Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added to the equipment cost towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five years differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 5 years after the warranty	3.5% AMC for security solution like WAF or any similar security solution is not a realistic %. We request Railtel to kindly make this clause to at least 15% per annum instead of 3.5% per annum		Already Clarified above
7	Page No.: 19, Clause No.: 99	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	In case of RMA Process, Define the no of days to deliver the solution.	Kinldy elaborate as RMA is NBD, do you mean to ask how many days will it take to dleiver the harwdare onsite in case of RMA ?		Already Clarified above

Additional Points suggested to be Added for a better & Competent WAF Solution						
8	NA	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The proposed WAF solution should also have capability for BOT Detection that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.		As per RFP
	FOR SOR-B					
SN	Page No./clouse No.	Particulars	Bidder's Comments (BC)			
			Tender Specification	Suggested specification	Justification	
1	23/22		Solution must be able to perform Source (Client) & Target (Backup Server) base block-level deduplication without requiring expensive and proprietary disk appliances.	Solution must be able to perform Source (Client) & Target (Backup Server) base block-level deduplication with proposed backup solution.	As requirement here is for Purpose Built Backup Appliance, this point is coming as contradictory to the ask of an appliance.	Refer Corrigendum-II
2	24/32		Solution should support rapid/instant VM recovery with LiveBoot for Vmware and Microsoft Hyper-V	Solution should support rapid/instant VM recovery for Vmware and Microsoft Hyper-V	Live Boot is propritory to one specific OEM hence request you to remove this point.	Refer Corrigendum-II
3	24/34		Solution Should have 48TB of Usable Capacity with HW RAID 60	Solution Should have 48TB of Usable Capacity with HW RAID 6 with hotspares with every 15 disks.	RAID 60 is not supported on purpose built backup appliance as it will increase the cost storage per bit hence request you to accept the suggested change.	Already Clarified above
	FOR SOR-C					
SN	Page no	Clouse no	Existing	Changes Required		
			SOR-C-ii -UTM			
1	26	6	UTM/NGFW appliance should have at least 32 GB RAM or higher	UTM/NGFW appliance should have at least 16 GB RAM or higher		As per RFP
2	26	10	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one		Refer Corrigendum-II
3	27	35	The IPS system should have at least 25,000 signatures with support for custom IPS signatures	The IPS system should have at least 10,000 signatures with support for custom IPS signatures		Refer Corrigendum-II
			SOR-C –iii - Firewall Manager			
4	28	3	The management appliance should have 2 x 1G port and integrated redundant power supply from day one	The management appliance should have 2 x 1G port.		As per RFP
5	29	14	The centralized management platform must not have any limit in terms of handling logs per day	The centralized management platform must have minimum 100 GB limit in terms of handling logs per day		Refer Corrigendum-II
	FOR SOR-D					

	Page no	Clouse no	Existing	Changes Required		
			SOR-D-iii - Vulnerability Assessment:			
	46	1	the scanning solution must be software / appliance based, that is deployable in windows and linux platforms	Linux flavours is more secure than windows. Therefore , as a request , please arrange to remove the Ms platform		Refer Corrigendum-II
	47	13	The Signature database must be exportable to CSV, PDF etc	Every OEM has different way of exporting the plugins database, we do in CSV format		Refer Corrigendum-II
	48	24	vi) Inventory of Hardware manufacturer for Host OS like workstations, Servers and laptops	Request to remove		As per RFP
	48	24	vii) Inventory of drives & file shares	Request to remove		As per RFP
	48	31	The solution Must provide a graphical, interactive and search friendly topology of the discovered assets	Request to remove		Refer Corrigendum-II
	48	46	The solution Must allow various output formats like CSV, DOC, HTML, PDF, XML etc	multiple reporting format like PDF, CSV, Richtext and cyberscope. Please remove native support for DoC, HTML and XML, etc for removing restriction of vendor specific. And provide common ground.		As per RFP
	49	61	iii) Identify vulnerabilities with zero day	First inform the zero day vulnerability to the respective OEM and don't declare it publicly as its likely to be exploited if OEM is not ready with the solution/Patch.		As per RFP
	49	61	iv) Identify Zero Day vulnerabilities	first inform the zero day vulnerability to the respective OEM and don't declare it publicly as its likely to be exploited if OEM is not ready with the solution/Patch.		As per RFP
	50	71	The solution must offers integrated password management integration with PowerBroker Password Safe as well as it includes a built-in third party password management connector.	CyberArk is global leader in Privilege Identity Management space and is more widely used in India than Beyond Trust. Request you here to include add cyberArk as well with Beyond Trust.		Refer Corrigendum-II
	N/A	N/A	Additional Suggestion			
			OEM should be the leader as per Gartner peer Insights			
			How many number of applications/URLs they intend to scan?			
	Page no	Clouse no	Existing	Changes Required		
	SOR-D-i - SECURITY DETECTION AND					
		RFP Volume Section and sub-section	Clause/ Content in the RFP	Clarification sought/ Change Request		
	30	SOR-D-i – SOC:, ADMINISTRATION AND CONFIGURATION	4. The solution must support auto discovery of assets that are being protected or monitored and automatically start accepting events without any administrator intervention through an agent less solution	The 'auto discovery of assets' is additional feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		As per RFP
	30	SOR-D-i – SOC:, ADMINISTRATION AND CONFIGURATION	5 The solution should support automated classification of assets that are being protected.	Please elaborate on 'classification of assets that are being protected', this seems value add feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		As per RFP
	31	SOR-D-i – SOC:, OPERATIONAL REQUIREMENT	6. The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	Building high availability at different components is design aspect, it is not necessary the product must have it as embedded fashion. This again an OEM specific product feature, request you to modify this as "the proposed SIEM solution must provide high availability at all layers including collection, normalization, correlation and management with the need for additional 3rd party software"		Refer Corrigendum-II
	31	SOR-D-i – SOC:, OPERATIONAL REQUIREMENT	6. The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	The "support high availability" is just a capability to be present in the solution, but Railtrail want the bidder to provide SIEM solution with high availability or stand-alone solution so that HA capability may be leveraged in future ?		Already Clarified above

	31	SOR-D-i – SOC:, OPERATIONAL REQUIREMENT	13. The solution must maintain an externally accessible store or database of all assets discovered on the network. This asset data should include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database.	Scanning IT infra, discovering assets and maintaining inventory are features of "Asset Management Software" tools and may be value add feature of specific SIEM OEM but not a general SIEM functionality. Hence this clause must be removed from the RFP		As per RFP
	32	Security and Data Integrity of SIEM	2 The system must provide Real-time remote indexing of data to minimize the opportunity for alteration of audit trails on compromised hosts 4 The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data 5 The solution must provide event hashing at index time to determine at search time if events have been tampered with 6 The solution must monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more.	Every SIEM Product have its way to manage the data integrity for the logs collected in real-time and near-real time. This clause is specific feature of OEM Product, hence please remove this or change this to "the system must perform indexing for real-time data and maintain data integrity check for both index and processed in a remote location for future audit and compliance purposes"		Refer Corrigendum-II
	32	Security and Data Integrity of SIEM	4 The solution must support industry log collection methods (syslog-UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195),DNS,DHCP, WMI, JDBC, XML,CSV,JSON,SNMP, Checkpoint LEA,FTP,S/FTP,ODBC,SDEE,Window event logs-agent based and agent less etc.,mail server, web server),directly pointing to log files over the network or on the indexer,Custom inputs which includes scripted and modular inputs, vendor supplied universal agents.	While the support of log collection methods is standard ask, but for exporting of offline log data or custom data may be supported differently by each SIEM OEM. Please modify this clause to what RailTel wanted to achieve instead referring to specific product feature of a OEM SIEM.		As per RFP
	33	LOG NORMALIZATION AND CATEGORIZATION	7 The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. E.g.: The categorization may by be HIGH, MEDIUM, LOW or color coding.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify this to as per end objective that RailTel wanted to achieve.		As per RFP
	34	REPORTING	10 The solution must support the ability to centrally deliver vulnerability reports. 11 The solution may support the ability to centrally deliver asset reports. 27 Dashboard should display asset list and capture details including name, location, owner, value, IP address, platform details	Delivering vulnerability/Asset reports and dashboards is feature provided by Vulnerability/Asset Management solution, this requirement is a feature of specific to a SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP or modify as per end objective that RailTel wanted to achieve.		Already Clarified above
	36	Open Platform	2 The solution must offers multiple SDKs written on top of the API for: 2.1. Python 2.2. Java 2.3. JavaScript 2.4. PHP 2.5. Ruby 2.6. C# 3 The solution should offers hundreds of free, public Apps for point products or use cases to create more value and accelerate time-to-value	These features apart from 'support of API for external integration' are specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify this to as per end objective that RailTel wanted to achieve.		Refer Corrigendum-II
	37	CORRELATION AND ALERTING	15 The solution may provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify to "the proposed SIEM must collect business context such as asset classification data and leverage in better incident prioritization and reduction of false positives" or as per end objective that RailTel wanted to achieve.		Already Clarified above

	39	SEARCH	7 The solution must have the ability to directly search raw data (using existing search capabilities) stored externally in Hadoop HDFS file systems and the results made available for advanced visualizations	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		As per RFP
	41	INDEXING	6 The solution must have ability to import raw data from Hadoop for indexing	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		As per RFP
	33	SOR-D-i – SOC, LOG MANAGEMENT REQUIREMENT	8 The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.	Please provide the retention duration for long term and also would it be offline or online retention ?		Refer Corrigendum-II
	34	SOR-D-i – SOC, REPORTING	10 The solution must support the ability to centrally deliver vulnerability reports.	This is an additional feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		As per RFP
	35	SOR-D-i – SOC, REPORTING	Dashboard should display asset list and capture details including name, location,owner, value, IP address, platform details	Scanning IT infra, discovering assets and maintaining inventory are features of "Asset Management Software" tools is value add feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		As per RFP
	42	SOR-D-i – SOC, Packet Capture:	1 Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident 6 Solution should be sized for traffic rate of 1Gbps or higher.	Please provide how no of network points at each location and their link bandwidth to be covered by full packet capture solution		Already Clarified above
	42	SOR-D-i – SOC, Packet Capture:	12 Should provide Regeneration and Playback functionality: Ability to create shadow networks. Regeneration and Playback: Point and click to instantly regenerate traffic (at configurable speeds) to a chosen NIC on a shadow network for further analysis in 3rd party systems. Without interruption of regular services.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		As per RFP
	43	SOR-D-i – SOC, Packet Capture:	19 Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years	The purpose of EDR solution is to detect malicious software/activities on the endpoint which can't be detected by AV solution deployed on the same. When these two products are from same OEM, it wont be of benefit (depth in defense).		As per RFP
	42	SOR-D-i – SOC, Packet Capture:	26 Solution must perform flow generation and analysis and must perform aggregation of all traffic pertaining to single session with a single flow records.	This is feature is specific to a SIEM OEM not general functionality of SIEM, there is not a much value of flow data when there Deep Packet Inspecting in place with Packet Capture. Hence remove this clause from RFP		As per RFP
	43	SOR-D-i – SOC, Packet Capture:	34 The solution provided for SSL decryption must support 78+ Ciphers and TLS 1.3. The packet capyure tool and SSLVA must be from same OEM.	Please explain why is that SSL decryption must from the same OEM that supplies Packet Capture? Not every DPI/Packet Capture OEM is not into SSL decryption products, and this may be true for specific OEM. Therefore request you allow the bidder to support Packet Capture and SSL decryption from different OEMs.		Refer Corrigendum-II
	SOR-E					
	Page no	Clouse no	Existing	Changes Required	Clarification	
			SOR-E- i- Rack Server:			
	50	1	General Requirement: Server should be a vSAN certified ready node	Server should be a vSAN certified ready node or a Factory pre-configured integrated and tested VSAN Appliance with pre-installed softwares of VSAN, vcenter.	Since the requirement is for VSAN, it is always preferred to have a factory pre-configured appliance which comes pre-installed with all the hardwares and software components with single file upgrade for entire solution.	As per RFP
	50	1	SAP Certification: Server should be SAP HANA certified.	SAP Certification: Server should be preferred to have SAP HANA certified.	For wider participation, would request to make it optional.	As per RFP

	51	8	Front drive bays: Up to 24 x 2.5" SAS/SATA/SSD	Should be scalable upto 16 x 2.5" SAS/SATA/SSD	24 will be specific to a single OEM	As per RFP
	51	8	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 4Gb cache	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2Gb cache	4Gb Cache is specific to a single OEM	As per RFP
	51	5	Configured CPU Should be populated with 2nos. of Intel Xeon Skylake CPU architecture, each CPU should be 16 core 2.3Ghz or more.	Configured CPU Should be populated with 2nos. of Intel Xeon Skylake CPU architecture, each CPU should be 16 core 2.1Ghz or more.	Would request you to accept this change as 16 Core CPU only comes with 2.1 GHz processor ie. Intel Skylake 6130 procesoor.	Refer Corrigendum-II
	51	7	Memory configured Configured with 128GB using 32 GB DIMM's scalable to 1.5TB	Memory to be configured with 128GB per processor using 32 GB DIMM's scalable to 1.5TB	128 GB memory with 32 GB DIMMS is only capable to support wit one processor.	As per RFP
	51	9	RAID Controller 12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 4Gb cache	RAID Controller 12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 4Gb cache is preferred but not mandatory.	Since solution based on VSAN always supports Raid - 10, 5 and 6 along with caching drives so would request to put this caluse as an optional.	As per RFP
	51	10	Disks configured 2 nos. of 240GB BOSS card or SATA/SAS SSD in mirrored configuration for OS & 3 nos. of 960 GB SSD SAS and 6x2.4 TB 10k rpm SAS drives.	Disks configured 2 nos. of 240GB BOSS card or SATA/SAS SSD in mirrored configuration for OS & 3 nos. of 800 GB SSD Drives as caching drives and 6x2.4 TB 10k rpm SAS drives as capacity drives.	Would request you to accept this change as it will clearly defined the sizing guidelines.	Refer Corrigendum-II
	51	11	DVD writer DVD RW	Request to remove	For wider participation, would request to make it optional.	Refer Corrigendum-II
	51	12	I/O slots Up to 6x PCIe Gen3 Slots	I/O slots Up to 4x PCIe Gen3 Slots	Would request you to accept this change as 4 PCI slots per server are enough for scalability. Also, it will qulify us for the participation	As per RFP
	51	13	Ethernet ports 2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	Ethernet ports 1 x 1G RJ45 for Management Ports and 4 x 10G SFP+ populated with Multimode Transceivers.	For wider participation, would request to accept this change.	Already Clarified above
	52	24	Intrusion alert in case chassis cover being opened	Request to removed	Specific to single OEM	As per RFP
	Page no	Clouse no	Existing	Changes Required	Clarification	
			SOR-E- ii- switch			
	53	12	Switch should have a minimum 40MB buffer of more.	We request to modify the minimum buffer to 32MB for better participation	request to please change the clause to "Switch should have a minimum 32MB buffer of more"	Refer Corrigendum-II
	FIRM-3:	DXC Technology		Preeta.Roy@dxc.com		
SN	Section	Pg No	Clause	Remarks	Suggested Changes	
1	SOR-D-i – SOC	41	4.7 PCAP Files	This would be available on the PCAP solution in raw format	Kindly remove the clause	As per RFP
2	SOR-D-i – SOC	41	Packet Capture	The Packet capture soltuion should be a separate solution and should come as a separate requirement (SOR). In its current state this favors OEMs who have both SIEM and Packet capture offerings. Kindly also refer Pg 6, Clause VII where it is mentioned that the bidder can quote only one OEM against one SOR.	Kindly add a separate SOR for Packet Capture solution	Refer Corrigendum-II
3	SOR-D – iv - Vulnerability Assessment:	46	Vulnerability Assessment	The Vulnerability Assessment soltuion should be a separate solution and should come as a separate requirement (SOR). In its current state this favors OEMs who have both SIEM and Vulnerability Assessment offerings. Kindly also refer Pg 6, Clause VII where it is mentioned that the bidder can quote only one OEM against one SOR.	Kindly add a separate SOR for Vulnerability Assessment solution	Refer Corrigendum-II
4	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	43	The solution must be in Leader's quadrant of the latest Gartner Magic Quadrant report on End Point Protection	There are other analyst reports where we have been recognized as leaders, IDC being one among them.	The solution must be in Leader's quadrant of the latest Gartner Magic Quadrant report on End Point Protection or IDC Marketscape for worldwide endpoint specialized threat analysis and protection	As per RFP

5	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	46	Solution should have Deception component from same or different OEM which helps identify the unknown attacks that conduct file traversals, network discovery, terminate processes, try to conduct credential theft, and more	Deception technologies are used to lure attackers using different mechanisms which may include a separate agent. Typical deception architecture would include a separate setup altogether that will have endpoint lures; network traps; OS traps all integrated with an intelligence platform and an operations console. This is in itself a requirement with multiple components and should be a separate requirement altogether.	Kindly remove this requirement.	As per RFP
6	SOR-C-ii -UTM	26	UTM/NGFW appliance should have at least 32 GB RAM or higher		UTM/NGFW appliance should have at least 16 GB RAM or higher	Already Clarified above
7	SOR-C-ii -UTM	26	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module		The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one	Already Clarified above
8	SOR-C-ii -UTM	27	The IPS system should have at least 25,000 signatures with support for custom IPS signatures		The IPS system should have at least 10,000 signatures with support for custom IPS signatures	Already Clarified above
9	SOR-C –iii - Firewall Manager	28	The management appliance should have 2 x 1G port and integrated redundant power supply from day one		The management appliance should have 2 x 1G port.	Already Clarified above
10	SOR-C –iii - Firewall Manager	29	The centralized management platform must not have any limit in terms of handling logs per day		The centralized management platform must have minimum 100 GB limit in terms of handling logs per day	Already Clarified above
	FIRM-4:	Inspira Enterprise India Pvt. Ltd.		Naveen Datta: naveen.datta@inspira.co.in		
SN	Tender clause No.	Tender Pg No.	Tender clause description	Modification/Clarification	Justification	
1	Page No.: 73, Clause No.: 3.3	73	Separate agreement for AMC (Long term Maintenance Support) before expiry of warranty period shall be entered with OEM/the authorized partner of OEM by RailTel. A fresh Bank Guarantee @10% of issued LOA/PO value valid for 64 months (4 months beyond the AMC period of 5 years)from the date of issue of LOA shall be required to be submitted by OEM/ Tenderer for due fulfillment of long term maintenance support obligation.	Pls confirm if Bank Gaurantee of 10% of AMC PO value to be submitted.	Clarity for the same in better cost estimation	No Change. PO for AMC will be isuued after expiry of Warranty. On submission of PBG against AMC PO, BG submitted against main PO will be released.
2	Page No.: 5, Clause No.:SOR	5	SOR G	Pls confirm if we have to enter incremental percentage or incremental value in price bid for SOR G	clarity for the same is required for quoting perfectly	Bidder has to quote incremental percentage.
				Pls confirm if the SOR G shall be awarded in a single PO along with other SOR.	Clarity for the same in better cost estimation	No PO for SOR G (AMC) will be issued on expiry of warranty.
3	Page No.: 11, Clause No.:12 F	11	Selection of vendors for RA shall be as under: If the number of tenderers qualified are 3 to 6, only 3 tenderers shall be eligible for participating in RA.	Pls clarify what will be the qualifying criteria for selection of 3 tenderers for participating in RA	Criteria for selection is not mentioned	
4	Page No.: 11, Clause No.:12 F	11	If the number of tenderers qualified are more than 6, only 50% of tenderers shall be eligible for RA (rounded off to next higher integer).	Pls clarify what will be the qualifying criteria for selection of 50% of tenderers for participating in RA	Criteria for selection is not mentioned	
5	Page No.: 13, Chapter 3 A - 2	13	Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.	Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with **30 days** of OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.	Quantiying the OEM professional services shall be beneficial for Railtel as it would ensure the duration of assured Services.	Refer Corrigendum-II
6	Page No.: 13, Chapter 3 A - Note 2	13	Bidder should submit the vetted BOM from their respective OEMs.	Bidder should submit the signed BOM from their respective OEMs on OEM letter head.	Signed BOM on OEM letter head ensures propoer vetting.	As per RFP
7	Page No.: 6,Note: V (A)	6	Integration with existing Network as required.	Pls share details of Existing Network	No Justification	As per RFP.

8	Page No.: 64, Clause No.: 1.2	64	Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.	Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and **brief** inspection at site as per mutually agreed testing procedure like physical verification shall be carried out. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.	After Test reports genreration the equipment is shipped from manufacturing facility to warehouse. It is not feasible to carry out detailed testing at warehouse. Request to please consider physical verification in inspection	As per RFP
9	Page No.: 72, Clause No.: 2.4.3	72	During the free warranty maintenance period contractor should stabilize the working of the system. Purchaser has the right to extend the period of supervision of the maintenance free of cost till the system stabilizes and works satisfactorily for a reasonable period of time. If during the time any equipment etc. is to be added or deficiencies are to be rectified to make the system work trouble free the same also will have to be done by the contractor at no cost to RailTel as to make good all the deficiencies.	Request to please define maximum duration of extension period of supervision.	We have to consider cost for same in bid. Open ended timeline shall result in incorrect cost estimation.	As per RFP
				Also if the scope is changed by Railtel and deficiencies arise due to same then the additional requirement shall be taken care by Railtel.	No Justification	As per RFP
10	Page No.: 73, Clause No.: 5.2	73	last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC)	Can the BG equivalent to 5% and valid for one year after PAC be acceptable for claiming the balance 5% amount.	No Justification	Standered Clause, As per RFP.
11	Page No.: 74, Clause No.: 5.7.1	74	final 5% on issue of Final Acceptance Certificate	Can the BG equivalent to 5% and valid for one year after PAC be acceptable for claiming the balance 5% amount.	No Justification	Standered Clause, As per RFP.
12	Page No.: 77, Clause No.: 12.1.2	77	The Tenderer/bidder should have supplied and provision of similar offered security solution with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.	The Tenderer/bidder should have supplied and provision of similar offered security solution **like NG Firewall or UTM and SIEM+SOC** with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company/ **Public Sector Banks** during the last three years from the date of opening of tender.	It is suitable to mention the requisite experience so that appropriate bidder with required experience to qualify.	As per RFP
13	Page No.: 84, Clause No.: 33.5.9	84	Documentary proof of equipment being proven and working for more than 6 months in India or outside India along with user certificate and Contact Details of user/firm.	Shall OEM certification w.r.t documentary prrof be acceptable	No Justification	As per RFP
14	Page No.: 89, Clause No.: 12.2.1	89	The tenderer should present at least one (1) project worth at least INR 7.52Crore showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.	The tenderer should present at least one (1) project worth at least INR 7.52 Crore showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions **and one project of next generation SIEM+SOC** commercially in India in the last 3 years.	It is suitable to mention the requisite experience so that appropriate bidder with required experience to qualify.	As per RFP
15	Additional clause suggestions			It is suggested to ask from bidder for certified resources 1 no. each as follows and to furnish the certificates: 1) CISSP 2) PMP/Prince 2 3) HCI OEM certified professional level. 10 resource of ISO 27001 Lead auditor	These certificates shall ensure that the bidder with right skill set of resources qualify.	As per RFP
16	Additional clause suggestions			It is suggested to ask from bidder for furnishing 2 nos. Purchase order from Government/PSUs/Telecom Service Providers/Public Listed Company/ Banks for implementation of SOC for minimum 30000 EPS in India in last 3 years.	As SOC is the major part of this RFP so experience pertainig to the EPS deployment shall ensure the requisite bidder capabilities can be ascertained from the furnished Purchase Orders.	As per RFP
17	Page No.: 26, SOR-C –ii - UTM: > S.No. 6	26	UTM/NGFW appliance should have at least 32 GB RAM or higher	We request you to kindly modify this clause as "UTM/NGFW appliance should have at least 16 GB RAM or higher"	No Justification	Already Clarified above

18	Page No.: 26, SOR-C –ii - UTM: > S.No. 10	26	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module	We request you to kindly modify this clause as "The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one "	No Justification	Already Clarified above
19	Page No.: 27, SOR-C –ii - UTM:> S. No. 35	27	The IPS system should have at least 25,000 signatures with support for custom IPS signatures	We request you to kindly modify this clause as "The IPS system should have at least 10,000 signatures with support for custom IPS signatures"	No Justification	Already Clarified above
20	Page No.: 28, SOR-C –iii – Firewall Manager: > S. No. 3	28	The management appliance should have 2 x 1G port and integrated redundant power supply from day one	We request you to kindly modify this clause as "The management appliance should have 2 x 1G port."	No Justification	Already Clarified above
21	Page No.: 29, SOR-C –iii – Firewall Manager: > S. No. 14	29	The centralized management platform must not have any limit in terms of handling logs per day	We request you to kindly modify this clause as "The centralized management platform must have minimum 100 GB limit in terms of handling logs per day"	No Justification	Already Clarified above
22	Page No.: 22, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	22	5. Solution Must support Host-Level Virtual Environments Including VMware vSphere, Microsoft Hyper-V	Please modify Clause as "Solution Must support Host-Level Hypervisor integration for Virtual Environments Including VMware vSphere, Microsoft Hyper-V, RedHat KVM, Nutanix AHV, OpenStack and Containers"	This is recommended for considering current and future requirment for cloud Infrastructure of the Railtel Department.	Refer Corrigendum-II
23	Page No.: 22, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	22	6. Solution must support back agents Including Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux and macOS	Please modify Clause as "Solution must support back agents Including Microsoft Windows, Linux, Unix and macOS. Also include Agent/Modules for online backup of applications and databases such as MS Exchange, MS SQL, Oracle, DB2, Sybase, MySQL, MongoDB, PostGre SQL and distributed databases/filesystems like NoSQL, Bigdata and hadoop. "	This is recommended for considering current and future requirment for cloud Infrastructure of the Railtel Department.	As per RFP
24	Page No.: 23, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	23	9. Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Please modify as "Solution must support Advanced sharing of different media across the environment (disk and tape)."	Optical device like CD,DVD cannot be shared and usually never used as backup storage, so request to remove Optical word.	Refer Corrigendum-II
25	Page No.: 23, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	23	11. Solution should offer rate limiting for data sent offsite to limit the impact of replication on critical Internet resources.	Please modify clause as "Solution should offer inbuild WAN Optimizer for data sent offsite to limit the impact of replication on critical Internet resources."	This clause is specific to some vendor, request to modify it as requested so that most of Enterprise backup vendors will participate in the bid. WAN optimization is the proper term and feature in most of backup solutions for optimizing backup data replication to offsite location.	As per RFP
26	Page No.: 23, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	23	15. Solution should offer message level backups for MS Exchange and allow for restore of individual messages or entire folders.	Please modify clause as " Solution should offer full backup of MS Exchange databases and allow for restore of full and individual messages."	This clause looks favouring a specific vendor and not a geniric feature. Please note most of the enterprise backup solution vendors provide MS Exchange backup at database level, however the restore can be done on granular single mail/message level. please modify so that most of enterprise backup solution vendors can participate in the bid.	Refer Corrigendum-II
27	Page No.: 23, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	23	18. Solution must support GUI with centralized management / Single interface for management of all backup and archival activities.	Please modify clause as "Solution must support GUI with centralized management / Single interface for management of all backup activities.	request to remove archival word as this requirment is related to a backup solution and not the archival software, both of them cater to a different requirment.	Refer Corrigendum-II
28	Page No.: 23, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	23	19. Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Remove this repeated clause no 9	Repeated clause, request to delete clause or remove optical word.	Refer Corrigendum-II
29	Page No.: 24, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	24	32. Solution should support rapid/instant VM recovery with LiveBoot for Vmware and Microsoft Hyper-V	Please modify clause as "Solution should support rapid/instant VM recovery with LiveBoot for proposed virtualization hypervisor platform"	This is recommended for considering current and future requirment for cloud Infrastructure of the Railtel Department.	Already Clarified above
30	Page No.: 24, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	24	34. Solution Should have 48TB of Usable Capacity with HW RAID 60	Please modify clause as "Backup Appliance Should have minimum 50TB of Usable Capacity and scalable to more than 300TB Usable with HW RAID 60"	No Justification	Already Clarified above

31	Page No.: 24, CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	24	35 . Appliance Should have 2 x 10Gb RJ45 or 2-port SFP+ Network Interface	Please modify clause as "Appliance Should have minimum 4 x 1Gbps Ethernet, 4 x 10Gbps Ethernet(SFP and Copper) and 2 Fibre Channel ports of minimum 8Gbps speed"	Considering current and furture requirments of railtel cloud infrastructure, it is necessary for department to request for all the necessary network interfaces in requested backup appliance. Please note almost all the backup appliance vendors provide all 1Gbps, 10Gbps and FC ports with their devices and if not rerequested, department may get the appliance missing these common required interfaces.	As per RFP
32	Page No.: 53, SOR-E-ii-10G Switch > SN - 5	53	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking	Hence, we request you to kindly modify this clause as " The switching OEM should be in Gartner Leader Quadrant for Data Center Networking"	As in gartner quadrant published document switching OEM is mentoned and not switch	Refer Corrigendum-II
33	SOR-E-ii-10G Switch >SN-12	53	Switch should have a minimum 40MB buffer of more.	This clause is specific to a single OEM. Hence, we request you to kindly modify this clause as "Switch support 32Mb buffer"	No Justification	Already Clarified above
34	SOR-E-ii-10G Switch > SN-13	53	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	-	This looks OEM specific customer should add this or similar technologies to achive the functionality	As per RFP
35	SOR-E-ii-10G Switch > SN-56	55	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	This clause is specific to a single OEM. Hence, we request you to kindly modify this clause as "Switch should support ARP Inspection"	Same functionality can be achived via Static ARP Inspection.	As per RFP
36	SOR-E-ii-10G Switch > SN-62	55	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	This clause is specific to a single OEM. Hence, we request you to kindly modify this clause as "Switch should support Port Mirroring"	No Justification	As per RFP
37	SOR-E-ii-10G Switch> SN-67	56	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management	The statement looks grammatically incorrect customer requirment needs to be rephrased	No Justification	As per RFP
38	SOR-E-ii-10G Switch >SN-75	56	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events	This clause is specific to a single OEM and feature is with only single OEM. Hence, we request you to kindly modify this clause as "Switch should support NTP Support over IPv4"	This feature is not available in our proposed OEM and is limiting our participation	As per RFP
39	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall > So. No 22	15	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	Is the expectation by this requirement that the proposed solution should have a minimum of 6000 signatures as default to detect and protect Web Applications. Kindly clarify	No Justification	Already Clarified above
40	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall > So. No 104	19	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	we understand that it s a multimode SFPs that is required but as required the appliance has to be fully populated request you to Kindly clarify how many Interfaces is required for each type 1Gig, 10Gig and 40gig. As there could be a possiblity of permutation combination on the type and interfaces proposed while fully populating the appliance SFP slots	No Justification	Already Clarified above
41	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall> So. No 103	19	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	Pls clarify that the gartner report of any year mentioned in the clause shall fulfill the clause requirement.	No Justification	Already Clarified above
42	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall> So. No 128	20	The solution should support Unified Anti-Bot Detection and Protection & Cloning Application Traffic	Does this clause means that a proposed WAF solution should have capability to detect and mitigate BOT attacks using multiple level of security checks Via Bot Signature, Application Fingure printing, Java Challenge, Browser capability check and Captcha. Kindly confirm	No Justification	Already Clarified above
43	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall > So. No 127	20	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	This requirement is not clear so request to please elaborate.	No Justification	Already Clarified above

44	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall, 99	19	The proposed WAF solution should also have capability for BOT Detection that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	No Justification	Already Clarified above
	Additional Points suggested to be Added for a better & Competent WAF Solution				No Justification	
45	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	NA	The proposed WAF solution should also have capability for BOT Detection that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	No Justification	Already Clarified above
46	SOR-D-ii&iii > S. No. 31	44	Solution must provide to create classify applications which are attempting network access, and block unauthorized connections and data transfers by malicious programs.	We request department to remove this clause.	No Justification	Refer Corrigendum-II
47	SOR-D-ii&iii > S. No. 36	45	After development of signatures for logs submitted for a suspicious system, analysis report must be submitted to RailTel. The Analysis report should contain IP address of the system, List of files found suspicious in the submitted log	We request department to remove this clause.	No Justification	Refer Corrigendum-II
48	SOR-D-ii&iii > S. No. 46	45	Solution must provide a Utility program for all supported Windows, Linux and MAC operating systems for collecting logs of infected endpoints for analyzing and developing signatures.	We request department to remove this clause.	No Justification	Refer Corrigendum-II
49	SOR-D-ii&iii >	43	Anti Virus + EDR (Client & Server)	Does RailTel only looking for a Antivirus EDR solution for Server. As for server security, an enhanced security solution is also required along with AV.	No Justification	As per RFP
50	SOR-D-i-SOC > S. No. 19	42	Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console	We request department to elaborate more on the EDR requirement in the RFP.	No Justification	Already Clarified above
51	SCHEDULE OF REQUIREMENT	5	Commercial SOC includes software components SIEM, Incident forensic and packet capture.	Since Quantity is mentioned as 1, Please clarify 1) if SIEM needs to be deployed in HA in DC ? 2) If DR is to be considered for SIEM instance?	No Justification	As per RFP
52	SOR-D-i – SOC:> Detailed Technical Specifications	29	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000.	Please suggest if proposed hardware should support 80000 EPS scalability without further hardware expansion. Also, kindly confirm the flow/sec scalability. We suggest to have following clause - The proposed solution should be able to handle 10,000 EPS& 5000 Flows/sec from day one and should be scalable to handle 40,000 EPS & 10,000 FPS on the same hardware and solution should be horizontally scalable to 80,000 EPS by adding additional hardware.	No Justification	Already Clarified above
53	Detailed Technical Specifications	29	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000.	Kindly confirm the log sources locations so as to size collectors for the same.	No Justification	Already Clarified above
54	Detailed Technical Specifications	30	The Bidder will give the hardware sizing for the EPS count required if solution is software based.	We understand bidder doesn't need to provision hardware for software based solution. Pls confirm.	No Justification	Refer Corrigendum-II
55	Detailed Technical Specifications	30	The Bidder will give the hardware sizing for the EPS count required if solution is software based.	Kindly confirm the log & flow retention policy(online & offline) so as to suggest on storage requirements.	No Justification	Already Clarified above
56	Detailed Technical Specifications	31	The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	Kindly confirm if solution needs to be deployed in high availability at all the layers ?	No Justification	Already Clarified above

57	Detailed Technical Specifications	32	The solution must easily expand to support additional demand.	Kindly clarify additional demand if this is w.r.t additional EPS/log sources integration.	No Justification	Refer Corrigendum-II
58	Detailed Technical Specifications	32	The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data	We suggest to modify this clause to read as " The solution should be able to support integrity of the indexed data" since most of the SIEM players doesn't support digitial signatures.	No Justification	As per RFP
59	Detailed Technical Specifications	32	The solution must monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more.	We suggest to modify this clause to read as "The solution must monitor its own configurations and usage to maintain a complete, audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more." since most of the SIEM players doesn't suport digital signature	No Justification	As per RFP
60	Detailed Technical Specifications	32	The solution must support Disaster Recovery.It should have the provision to run in active / passive mode in a DC-DR environment and should be able to failover to automatically DR in case of a primary failure.	Kindly confirm if solution needs to be deployed in DR as well. Also, will this DR be in Active/Passive Mode. Incase of passive DR, kindly confirm the RTO/RPO to adhere.	No Justification	As per RFP
61	Detailed Technical Specifications	41	Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident	Please confirm the number of locations & interfaces to be captured for packet capture.	No Justification	As per RFP.
62	Detailed Technical Specifications	42	Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints via single agent EDR and Anti-virus solution.The AV and EDR must be from same OEM. Provided AV must be in leaders Gartner Quadrant.	We suggest to read this clause as "Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints "	No Justification	As per RFP
63	Detailed Technical Specifications	42	Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.	We recommend to have appliance based solution for packet analysis. We suggest to have software based solution for storing pcap and session reconstruction.	No Justification	Already Clarified above
64	Detailed Technical Specifications	42	Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.	Kindly confirm following for sizing the packet solution - 1) No of locations/interfaces including DC & DR for packet data collection 2) Link & current bandwidth utilization details for each interface/location to be cpatured 3) Retention policy to be considered for raw & meta data retention.	No Justification	As per RFP
65	Detailed Technical Specifications	42	Should capture signature/heuristics and behavioral based alerts and block the malicious activity	We suggest to remove this clause since Packet capture solutions are not supposed to block the activity	No Justification	Refer Corrigendum-II
66	Detailed Technical Specifications	42	Solution must support provision to implement custom environment.	Kindly provide with the expectations.	No Justification	Refer Corrigendum-II
67	Detailed Technical Specifications	42	The solution should be able to provide suggested mitigation actions for events	Clause mentioned are applicable to SOAR platform hence we suggest to remove this clause from packet capture.	No Justification	As per RFP
68	Detailed Technical Specifications	42	Proposed solution should Integrate with On Premise Malware Sandbox Analytics solution. Security analytics should be able submit files for detonation and analysis.The ATP solution must be able to submit files for sandbox.	We suggest to remove "The ATP solution must be able to submit files for sandbox." from the mentioned clause since packet capture & ATP solution are different.	No Justification	Refer Corrigendum-II
69	Detailed Technical Specifications	42	Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years	We suggest to remove this clause since this clause is not applicable to Packet Capture solution.	No Justification	As per RFP

70	Detailed Technical Specifications	35	"The solution should include following native visualizations: Tables Time charts Line charts Bar charts Area charts Pie charts Scatterplot charts Radial, filler, and marker gauges Geo-IP maps"	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
71	Detailed Technical Specifications	35	The solution should have the ability to convert dashboards into PDF files and schedule them to be emailed to others.	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
72	Detailed Technical Specifications	35	The solution should have the ability to integrate with external visualization frameworks and options (D3, Tableau, etc) for additional visualizations	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
73	Detailed Technical Specifications	36	Dashboard should support export of data to multiple formats including CSV, Excel, PDF	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
74	Detailed Technical Specifications	36	The solution must offers multiple SDKs written on top of the API for: Python Java JavaScript PHP Ruby C#	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
75	Detailed Technical Specifications	36	The solution must assist in following use cases due to indexed data leading to a high ROI and cross-department collaboration. Compliance Fraud IT Operations Application Management Web/Digital Intelligence Business Analytics Industrial Data and Internet of Things	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP

76	Detailed Technical Specifications	38	The solution must be able to do full-text search on any field in the indexed data based on: Keywords Time ranges Specific or relative time windows down to the month/day/minute/second Boolean logic (and, or, not, etc) Regular expressions Wild card syntax Statistical analysis including: Count of occurrences, distinct count of occurrences, sum Most common values or least common values of a field Minimum, maximum Average, mean, mode, median Standard deviation, variance The identification of anomalous values in results that may be irregular, or uncommon The statistical correlation between fields Clustering of events together based on their similarity to each other as a single event Truncate outlying numerical values in selected fields to assist in statistical correlation First and last seen value Percentile Predicted values (search that looks at historical data to mathematically predict future values) Perform a union, diff, or intersection of individual or multiple	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
77	Detailed Technical Specifications	38	The solution must be able to do baselining and then apply the above search logic to find outlier/anomalies from the baseline that may be advanced, non-signature based threats	This seems to be specific OEM clause hence we request to remove this clause	No Justification	As per RFP
78	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 20	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log	Pager is an obsolete technology and most of vendors has stop supporting as a medium for sending notification so we request you to kindly modify this clause as "Shall offer customizable & standard notifications via - SMTP, SNMP, NT Event Log"	No Justification	Refer Corrigendum-II
79	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 21	The solution should provide quarantine management in order to prevent spreading. A management interface must be provided to allow the administrator to review, sort and analyze quarantined items.	This is specific to one OEM and restricting us from participation so we request you to kindly modify this clause as " The solution should provide quarantine management in order to prevent spreading. A management must be provided to allow the administrator to restore quarantined items in case file found to be legitimate"	No Justification	As per RFP
80	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 28	Solution must provide virtualized environment	Please help in elaborating the use case of this requirement	No Justification	Refer Corrigendum-II
81	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	45, Point no. 56	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers or provide attack prevention using the least privilege containment approach	This is specific to one OEM and restricting us from participation so we request you to kindly modify this clause as "The solution should use HIPS (host) based signature to proactively protect against intrusion targeted at the servers"	No Justification	Refer Corrigendum-II
82	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	46, Point no. 70	Solution should have an emulator to cause threats to reveal themselves. This should not be a part of sandboxing and should run individually in each agent	This is specific to one OEM and restricting us from participation So we request you to kindly modify this clause as" Solution should have a mechanism to Identifies packed malware in memory as it unpacks prior to execution using machine learning functionality"	No Justification	Refer Corrigendum-II

83	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	45, Point no. 71	Solution should have Deception component from same or different OEM which helps identify the unknown attacks that conduct file traversals, network discovery, terminate processes, try to conduct credential theft, and more	This is specific to one OEM and restricting us from participation Clause Should Read as : Solution should have functionality which helps identify the unknown attacks	No Justification	As per RFP
84	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	46, Point no. 73	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest OS patches have been applied to the operating system.	This is specific to one OEM and restricting us from participation So we request you to kindly modify this clause as" The Solution should check for the existence of open known vulnerabilities and shield them using virtual patching technology"	No Justification	As per RFP
85	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	46, Point no. 74	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, downloading and executing/inserting a software, running scripts , by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.	This is specific to one OEM and restricting us from participation. Hence we request you to kindly remove this clause to allow alteast more than one OEM participation	No Justification	As per RFP
86	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	46, Point no. 75	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.	This is specific to one OEM and restricting us from participation. Hence we request you to kindly remove this clause to allow alteast more than one OEM participation	No Justification	As per RFP
87	SOR-D-i – SOC:Packet Capture	41	Specifications from Serial no. 1 to 38	Specificaitons are specific to one particular OEM and restricting us from participation. Hence we request you to kindly remove this clause to allow alteast more than one OEM participation	No Justification	As per RFP
88	2	28	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	Rrequest to please change the clause to "The management platform must be a dedicated OEM appliance orr VM running on server"	A virtual appliance is more flexible and scalable. Rresticting the solution to a HW based appliance will rrestric competition.	As per RFP
89	8	28	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	Request to please delete this item	This is a SIEM capability and since SIEM has been requested as a separate item in SOR thereforre this functionaality is not required on the FW manager	As per RFP
90	SOR-E-ii-10G Switch	27	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.		Our proposed OEM is partially complied as they support this for VM ware	As per RFP
91	SOR-E-ii-10G Switch	53	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4		Our proposed OEM is Partiall Complaint, they don't support this by default but can be added via Scripting	As per RFP
92	SOR-E-ii-10G Switch	53	Switch Support Max 64VRF	Switch Support Max 16VRF	No implementation requires such high VRF Scale most of time 8 to 16 VRF Suffice	As per RFP
93	SOR-E- i- Rack Server > S. No 1	50	Server should be a vSAN certified ready node	We request to remove this clause as this is Vendor Specific.		As per RFP
94	SOR-E- i- Rack Server > S. No 2	51	The OEM for the proposed server must be in Leaders quadrant in the last two Gartner's report of "Magic Quadrant for Modular Servers"	MQ retired and not even valid since last 2 years. We request to remove this clause.		Already Clarified above
96	Software defined Storage For DR > S. No. 1	57	The solution should provide unified and centralized software defined platform that intergates market leading compute, storage, networking and security virtualization into a common platform to deliver enterprise-ready cloud infrastructure for the private and public cloud.	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		As per RFP
99	Software defined Storage For DR > S. No. 4	57	The solution should provide broad ecosystem to flexibly deploy on premises on certified hardware from major OEM vendors or run it as a service from AWS or from a selected number of Cloud Providers.	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		Refer Corrigendum-II

102	Server Virtualization > S. No. 8	57	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus, HIPS integration, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as linux VMs, VM level encryption, secure boot, vMotion within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		Refer Corrigendum-II
109	Storage Virtualization > S. No. 10	57	Should include storage virtualization /HCI software supporting all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any server manufacturer & should support mixing of different compatible Server brands in same Cluster. It should work on mutually certified hardware of any vendor like dell, HP, Cisco, Lenovo, Hitachi etc. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		As per RFP
115	Network Virtualization> S. No. 18	58	The network virtualization should provide distributed in-kernel routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN services, distributed L2-L4 stateful in kernel firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, vCenter objects and tags, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration)..	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		Refer Corrigendum-II
121	Network Virtualization> S. No. 19	58	The solution should be capable to provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		As per RFP
126	Network Virtualization> S. No. 20	58	Solution provide traffic visibility (IPFIX), end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		Refer Corrigendum-II
129	Network Virtualization> S. No. 21	58	The solution should have the ability to deliver end to end security for all applications by delivering network-level micro-segmentation, distributed firewalls, load balancers, virtual routers, virtual switches and VPN,	Vendor Specific and if you search for it on internet using the red highlighted font, you will reach the vendor in question site/documentation		As per RFP
	Firm-5:	Vehere		Mannu Kalra: mannu.kalra@vehere.com		
SN	Page No	Clause No.	Clause in the RFP	Query		
1	41	Packet Capture: SN#1	Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident.	Please clarify if incident investigation shall be on a per-incident basis or, can be multiple incidents being explored at the same time. If there's a possibility of multiple incidents being explored at the same time, related explorations and retrievals should be supported as such.		Already Clarified above
2	41	Packet Capture: SN#2	Support importing archived PCAP files for analysis, Support importing other structured and unstructured content for analysis	Request please clarify the nature of structure and unstructured content that is likely to be ingested for analysis. Kindly clarify of the Packet Capture tool is to include an ETL facility to support importing of supplemental data such as IPDR.		Clarification: Refer RFP specs

3	42	Packet Capture: SN#4	Highlight potentially malicious or suspicious content,Allow for assigning security analysts to specific security incident investigations	Kindly clarify if incident assignment is to be driven by the central pane-of-glass (SIEM) or, Packet-Capture? Packet-Capture tool based event discoveries should be forwarded to SIEM which should take care of workflow and task assignments. Anyway, the point #5 solicits SIEM integration.		Clarification: Refer RFP specs
4	42	Packet Capture: SN#5	Solution should generate a whitelist policy based on real-time application behavior and keep the policies up-t-date as applications evolves and more applications are added and modified. It should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.	Security is getting paranoid to a point of being zero-trust. It is our opinion that this requirement of whitelisting applications not only creates integration challenges and security posture gaps, it opens the environment to more risk by use of any form of whitelisting. Therefore, we request this requirement to be dropped. Let the system monitor 100% of network traffic and flows without any bias.		As per RFP
5	42	Packet Capture: SN#10	Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints via single agent EDR and Anti-virus solution.The AV and EDR must be from same OEM. Provided AV must be in leaders Gartner Quadrant.	This requirement prohibits worthy vendors of competing and reduces on Railtel's leverage to negotiate for a better technology to be delivered as it favors only one vendor. Aside to that it presents a security risk - One vendor, one solution, one threat-intelligence feed. What one misses, the other misses too. Adding external threat intelligence sources for detection implies additional cost over and above the cost of solution. It's a sure win-win for the vendor but not for the buyer. A better strategy is to as for a standards (STIX) based integration with a competent EDR technology. Two products - not all eggs in one basket. Allows for the buyer to best negotiate for technology on merit and has open integration interfaces for better utility over a long period.		Already Clarified above
6	42	Packet Capture: SN#14	The solution should support - classification from more than 3000 protocols/applications(natively without writing any custom parsers) and thousands of descriptive, metadata attributes, including content types, file names, and more - for easy analysis and recall without writing any custom parsers.	May we request Railtel to stregthen this clause by ensuring that the OEM is the owner of this technology piece too. After-all, the Deep Packet & Payload Inspection lends the Packet Capture technology one of its most important capability to quickly determine activities of interest that an analyst may want to investigate. Ownership with the OEM ensures better control over what you want detected and decoded and not what the DPI vendor provides.		As per RFP
7	42	Packet Capture: SN#17	Root Cause Explorer Features - Automates tracing of HTTP referrer chains that can significantly reduce time to search for related preceding sessions.	Realistically, how much clear-text traffic do we see? It's better to have a solution that allows exploration of root-cause using much contemporary technologies such as graph analysis - It is application agnostic and provides compelling insights upfront.		As per RFP
8	42	Packet Capture: SN#19	Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years	Again a repeat of point #10. This ensures that only a single vendor wins this requirement. The clause prohibits offering of equal opportunity to competent technology providers and must be taken off along with point #10.		As per RFP
9	42	Packet Capture: SN#22	The solution should support network anomaly detection that performs statistical analysis on captured data and alerts on anomalous behavior. It should support pivot from the alert to an investigation view, where details around anomaly are available for analysts review.	Statistical anomaly is history. Modern analytics use unsupervised ML algorithms to model network behavior and discover anomalies on multiple vectors not just statistical counters. Request that this clause may be eliminated as SIEM can meet these requirements.		As per RFP
10	42	Packet Capture: SN#25	Should Identify the source of an attack	Are you looking at attribution to the last known endpoint or, simply detection of Source IP Address? Request please clarify.		As per RFP

11	42	Packet Capture: SN#26	Solution must perform flow generation and analysis and must perform aggregation of all traffic pertaining to single session with a single flow records.	Request please clarify if the buyer wants to procure a flow-based capability besides the ability to capture full packets. If yes, kindly state the performance expectations for flow ingestion.		As per RFP
12	43	Packet Capture: SN#34	The solution provided for SSL decryption must support 78+ Ciphers and TLS 1.3. The packet capyure tool and SSLVA must be from same OEM.	This requirement along with requirement #10 and, 19 hands over at-least three technologies to one vendor alone and eliminates competition. We request that the requirements from #27 till #34 be dropped as SSL isn't just one encryption technology being used. Modern perpetrators are stealthy and use data masking, code-caving, custom ciphers, using SSH, IPSec (inbuilt into IPv6) for malicious activities to which this solution offers no visibility at-all.		Already Clarified above
13	43	Packet Capture: SN#38	The Solution should include 3 yrs. Of Subscription	Kindly clarify if this is support term expectation or, subscription to something else?		Clarity: Both Subscription and Support for 3 yrs.
	FIRM-6:	RAH Infotech Pvt Ltd				
S.N.	RFP Document Reference Section No., Page No.)	Content of the RFP require clarification	Clarifications	Suggested Clauses		
	SOR-A	Web Application Firewall				
1	SOR-A:Web Application Firewall, Page No. 13 1	The solution's monitoring appliance must be able to support ALL of the following deployment modes to monitor web application traffic over the network: - Via a SPAN/TAP port sniffing mode - Layer-2 transparent inline mode - Reverse Proxy mode - Transparent Layer-2 Reverse Proxy mode	The WAF should be deployed in Reverse Proxy mode in order to provide maximum level of security. However there should be mechanism to have the WAF placed on OOP or SPAN port to enhance the traffic baseline initially before deploying in actual production.	The solution's monitoring appliance must be able to support ALL of the following deployment modes to monitor web application traffic over the network: - Via a SPAN/TAP port sniffing mode - Reverse Proxy mode - Out Of Path Mode		Refer Corrigendum-II
2	SOR-A:Web Application Firewall Page No. 15 18	The solution must provide the ability to comply to A+ Certification at the click of a button	This clause talks about strengthning the SSL security, We would recommend to simplify this clause and ask for the support of ECC and Latest TLS version i.e. TLS 1.3 support. One can achieve A+ with numeric score of greater than 80, with TLS1.3 you can go beyond that.	The solution must TLS1.3 version and ECC Ciphersuite.		Already Clarified above
3	SOR-A:Web Application Firewall Page No. 15 22	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	We recommend to go for behavioral based technology that does not rely on the number of signatures, as the spectrum for Application attacks cannot be mitigated with 6000 signatures. Hence we would recommend the combination of Positive and Negative security model.	The solution must have positive and negative security models designed to detect known and Unknown attacks on web applications.		Already Clarified above

4	SOR-A:Web Application Firewall Page No. 19 101	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities. Like:- - Acunetix - Beyond Security - Cenzic - Denim Group - HP Fortify WebInspect - IBM AppScan - NT OBJECTives - Qualys - Rapid7 - Trend Micro - Veracode - WhiteHat	The solution should not be dependent on 3rd party web application vulnerability assessment tools for virtual patching. The process should be Inbuilt and without any manual intervention the device should be able to patch the vulnerabilities with auto policy generation, hence we request to ammend this clause.	The solution must support Autamated Patching of Vulnerabilities without any manual intervention OR integration with web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities. Like:- - Acunetix - Beyond Security - Cenzic - Denim Group - HP Fortify WebInspect - IBM AppScan - NT OBJECTives - Qualys - Rapid7 - Trend Micro - Veracode - WhiteHat		Refer Corrigendum-II
5	SOR-A:Web Application Firewall Page No. 19 103	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	Please relax this clause to allow maximum participation	The solution must present in the latest Gartner Magic Quadrant of Web Application Firewalls		Refer Corrigendum-II
6	SOR-A:Web Application Firewall Page No. 20 109	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	The traffic ports requirement is not Inline with throughput asked for WAF i.e. 2 Gbps only. As per specifications 2X40G ports have been asked which comes to 80G of combined capaciy. Seems to be a typo error. Requesting to ammend the same	System must have minimum(fully populated) 6 x10G SFP+ Ports from day 1 scalable to 12 x 10G ports. Populated Optics should be Multimode.		Already Clarified above
7	SOR-A:Web Application Firewall Page No. 20 109	the proposed appliance should have capability of Hardware based DDOS protection up to 50M Sync Cookies per second	The DDoS attacks can be of any type like ack flood,ICMP flood,IGMP flood etc. Hence the solution should have advanced DOS protection to protect from every type of attack.	the proposed appliance should have Advanced Denial of Service mechanism to mitigate the DDoS attacks.		As per RFP
8	SOR-A:Web Application Firewall Page No. 20 110	The proposed hardware should include a LCD panel which should support Configuration for Initial Management IP address and display all the error and information corresponding to hardware & software without logging into the appliance.	It is not recommended and not a industry standard hence should be removed. The device should support very granular reporting mechanism that will help to identify the root cause of the issues. With LCD display its not possible.	Remove this clause		Refer Corrigendum-II

9	SOR-A:Web Application Firewall Page No. 20 123	Should support client certificate constrained delegation (C3D) which will enable the Load balancing solution to generate certificates on behalf of clients and pass it to the end servers if SSL based client authentication has been enabled on the backend servers .	Please generalise this clause.	The solution should support Front end and Backend SSL Tunnel to provide end to end Secure SSL tunnel.		Already Clarified above
10	SOR-A:Web Application Firewall Page No. 20 123	The proposed appliance should support up to 35K SSL TPS with Dedicated SSL Offloading Chip. TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.	We recommend to include ECC TPS as a capacity parameter as with TLS 1.3 RSA has been discontinued.	The proposed appliance should support up to 30K SSL CPS and 20K SSL CPS on ECC with dedicated hardware SSL card.		As per RFP
11	New Clause Request	New Clause Request	The solution should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, and acceleration resources to provide complete separate environment from applications and management perspective. This gives the IT/Operations team the flexibility to test any application functionality through server load balancer before actual deployment without an Impact on production environment. All the virtual instance on the appliance can run different OS which means you can easily boot any instance without impacting other instances, hence ensuring maximum uptime for the critical applications.	Suggested Clause: Should be appliance based solution with purpose built hardware for high performance with Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) OS The proposed device should support 30 virtual instances.		As per RFP
	SOR-B		Backup			
1	Backup Software Page 22		Solution must support Guest-Level Virtual Environments including Citrix XenServer, Kernel- based Virtual Machine (KVM), Oracle VM and Red Hat Virtualization	Solution should be able to capture APPS and DB's running on top of Guest VM's. & should capture full VM and recover on Vmware and also on Cloud Platform.		As per RFP
2	Backup Software Page 22		Solution must support back agents Including Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux and macOS	Solution must support back agents Including Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux.		Already Clarified above
4	Backup Software Page 23		Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix, and Mac OS.	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix.		Already Clarified above
5	Backup Software Page 23		Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Requesting the committee to exempt this clause as the appliance will have embedded deduplication and compression and can store data for years.		Already Clarified above
6	Backup Software Page 23		Solution must support multiple level of backups including full, incremental and differential backups including the Virtual backups	Requesting the committee members to look into VDP technology as it has Initial full with forever incremental backup technology and will create PIT synthetic full, which can capable of restoring data from any point in time. Hence does not need differnictal backup.		As per RFP

7	Backup Software Page 23		Solution must be able to perform Source (Client) & Target (Backup Server) base block-level de- duplication without requiring expensive and proprietary disk appliances.	As the solution already has incremental backups , it would be suitable not to have client level deduplication as it might cause performance issues on client.		Already Clarified above
8	Backup Software Page 24		Solution should offer automatic software updates and access to new features included with annual subscription.	Solution should let the admin to plan and upgrade to avoid any backup failure and all upgrades withour any additional cost and will get alerted when there is a new version available.		As per RFP
	SOR-D-iv	VAPT				
1	VAPT Page 49	Reporting and Schedules must be able to auto start, auto pause, auto resume and auto cancel to suit a maintenance window if required	Need more clarity on maintenance window			As per RFP
2	VAPT Page 49	Solution should allow users to customize the dashboard	Need more clarity on what all customizations are required.			Refer Corrigendum-II
3	VAPT Page 49	The Solution must provide inbuilt ticketing for vulnerability status monitoring	Need more clarity. Can the ticketing tool be integrated with the VM tool to address the requirement.			As per RFP
4	VAPT Page 50	The solution must automates policy definition and policy life cycle management	Please provide more clarity on policy life cycle management.			Refer Corrigendum-II
	SOR-D-i	SIEM				
1	SIEM Page 29	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018		Requesting the technical committee to please exempt this clause under Make in India.		Already Clarified above
2	SIEM Page 30	The Bidder will give the hardware sizing for the EPS count required since the solution is software based.		Requesting the committee members to change this cluase from Technical Specification part to Bidder Responsibilities.		Refer Corrigendum-II
3	SIEM Page 30	The solution must support the detachment of selected dashboards from the UI for use in SOC or NOC deployments.	Requesting the committee to provide more clarity on the same			As per RFP
4	SIEM Page 30	The solution should support the ability to modify communications ports between components from a central location.	Requesting the committee to provide more clarity on the same			As per RFP
5	SIEM Page 32	The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data	Please elaborate			Already Clarified above

6	SIEM Page 36	The solution must offers multiple SDKs written on top of the API for: Python Java JavaScript PHP Ruby C#		Requesting the technical committee to exempt this clause as every SIEM tool will have their own backend API's to work on or rephrase the same to Python/Java/Javascript/PHP/Ruby/C#		Already Clarified above
7	SIEM Page 36	IT Operations	Requesting the committee to provide more clarity on the same.			As per RFP
8	SIEM Page 36	Application Management	Requesting the committee to provide more clarity on the same.			As per RFP
9	SIEM Page 36	Web/Digital Intelligence	Requesting the committee to provide more clarity on the same.			As per RFP
10	SIEM Page 36	The solution must support a single solution to support all the data needs of different users, roles, and departments across the organization	Requesting the committee to provide more clarity on the same.			Clarification: Details given in the RFP specs.
11	SIEM Page 40	The solution may support information collected from proprietary applications.		SIEM Solution should be able to take logs from custom/proprietary applications and parse the raw log by developing parsers for the same		As per RFP
12	SIEM Page 41	Packet Capture		Requesting the Technical Committee to change this from SIEM perspective to PCAP tool as PCAP tools and SIEM tools are different and getting this into one consolidated solution makes it OEM Specific.		Already Clarified above
	SOR-C-ii	UTM				
1	UTM Page 26	The Firewall solution should support NAT64, DNS64 & DHCPv6	Requesting the Committee to change the same to The Firewall solution should support NAT64, DHCPv6	Requesting the committee to exempt DNS64 as this will be OEM specific		Refer Corrigendum-II
2	UTM Page 28	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	The management platform must be accessible via a web-based interface and/or with additional client software	Requesting the committee to exempt this as this is OEM specific		Refer Corrigendum-II
	SOR-C-iii	Firwall Manager				
1	Firewall Manager Page 28	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	The management platform must be accessible via a web-based interface and/or with additional client software	Requesting the committee to exempt this as this is OEM specific		Already Clarified above
2	Firewall Manager Page 28	The management platform must be able to store record of 15000 user or more	The management platform must have 1 x 2TB hot swap HDD and 32 GB RAM from day 1.	Requesting the committee to provide the storage requirement.		As per RFP
	FIRM-9:	Check Point Software Technologies, Ltd.		Anuj Madan: anujm@checkpoint.com		
	SOR-C –ii - UTM:					
SN			Minimum Requirement Description	Check Point's comment & revised specification	Remarks	
1			The solution must be present as Leaders in latest Gartner's Magic Quadrant for Enterprise Firewall			As per RFP

2			The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)			Already Clarified above
3			UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 4 x 1GE SFP ports with fully populated from day one			Already Clarified above
4			UTM appliance must have separate SYNC and management ports other than the above mentioned ports.			
5			Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.			Already Clarified above
6			UTM/NGFW appliance should have at least 32 GB RAM or higher			Already Clarified above
7			UTM appliance should have a on device storage of min 200GB to be able to hold multiple OS images, logs, backups etc			
8			Firewall should support 20,000 new sessions per second or more			
9			Firewall should support 2 Million concurrent sessions			
10			The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module			Already Clarified above
11			The Firewall solution should support NAT64, DNS64 & DHCPv6	The Firewall solution should support NAT64 & DHCPv6	Pls remove DNS64	Already Clarified above
12			Firewall should operate in Route mode and transparent mode			
13			The appliance should support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability			
14			The proposed system should have integrated Traffic Shaping / Rate-Limit functionality.			
15			Support multiple firewall domains/instants/context /zone or more			
16			Certified by ICSA 4.1x OR EAL4 OR NDPP			
17			Internationally accepted marked/Certified like RoHS, UL/CUL, FCC,CE,..etc.			
18			The system should inherit all the standard RFC's.			
19			Firewall should be either IPv6 Ready Logo certified / FIPS/ USGv6 or equivalent			
20			Should facilitate to apply policy like IPS, Content filtering, Traffic shaping/Rate-Limit & policy based routing decision			
21			User authentication facilitated by services like LDAP and RADIUS/AD.			
22			Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.			
23			Management access control using Profile/Role based for granular control.			
24			Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.			
25			Support configurable option for E-mail or SMS alerts (Via SMS gateway) incase of any event trigger.			
26			Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.			
27			All SNMP versions support (v1, v2c and v3).			
28			Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 1024 VLANs			

29			Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, BGP with IPv6), Static Route, Policy Based Routing, Multicast Routing			
30			Support DHCP relay, DNS client and NTP client; Firewall as security appliance should not use DHCP and should have static ip address			
31			Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice versa).			
			Intrusion Prevention System			
32			The IPS capability should have NSS, ICSA or other equivalent Certification			
33			The IPS detection methodologies should consist of:			
			a) Signature based detection using real time updated database			
			b) Anomaly based detection that is based on thresholds			
34			The IPS should be able to inspect SSL sessions by decrypting the traffic			
35			The IPS system should have at least 25,000 signatures with support for custom IPS signatures			Already Clarified above
36			IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available			
37			IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident			
38			Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)			
39			Solution should be able to detect & Prevent the Bot communication with C&C			
			Web Content Filtering & Application Control Features:			
40			URL database should have at least 200 million+ sites and 50 + categories.			Already Clarified above
41			Support for geographical based filtering like country level TLD etc.			
42			The appliance should have 3000 or more application signatures database			
43			Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.			
			User Authentication			
45			The proposed solution shall be able to support various form of user Authentication methods simultaneously , including:			
			a) LDAP server entries			
			b) Native Windows AD (Single sign on capability)			
46			Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.			
			High Availability			
47			System should have built-in high availability (HA) features without extra cost/license or hardware component from day one			
48			Should support state full session maintenance in the event of a fail-over to a standby unit.			
49			High Availability feature must be supported for either NAT/Route or Transparent mode			

50			High Availability Configurations should support Active/Active / Clustering, Active/ Passive			Already Clarified above
			Management, Logging and Reporting			
51			The system would be managed centrally using a web-based console that allows system monitoring, software updates, client configuration.			
52			The management solution must offer console capability for managing the logs, policy, reporting and various features of the UTM.			
53			Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)			
54			Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logsto syslog server and sending schedule reports and send via email.			
			Anti-virus, Anti-bot & Advance Persistence Threat Solution			
55			Should provide protection against zero-days, Trojan, worms or any other malicious content in traffic like SMTP, SMTPs, POP3, POP3s, IMAP, IMAPs, HTTP, HTTPs, FTP, FTPs etc. and must be configurable/applicable on specific firewall Policy			
56			Remove buffering, it will introduce latency and impact user experience. All gateway level solution are flow			
57			Should have option to respond to malicious detection like delete/quarantine the file or block the connection and send notification via e-mail/SMS.			
58			For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and other			Already Clarified above
59			Should be able to block or allow oversize file based on configurable thresholds			
60			Firewall must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also.			
			Support and Warranty			
61			Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.			
62			Online upgrade the version of firmware/software/patches as and when required.			
63			Telephonic support with call logging mechanism should be provided on 24x7x365 basis.			
64			Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.			
65			All the technical specifications mentioned above must be available from day one			
			Other Requirements			
66			For all requirements listed above, the necessary cables, connectors, external software media, manuals or any other hardware and software must be provided along			
			SOR-C –iii – Firewall Manager:			
			Minimum Specification requirement			
1			The management platform must be accessible via a web-based interface and ideally with no need for additional client software	The management platform must be accessible via a web-based interface and/or with additional client software	This is specific to one OEM. Pls change.	Already Clarified above
2			The management platform must be a dedicated OEM appliance and VM running on server will not be accepted			Already Clarified above
3			The management appliance should have 2 x 1G port and integrated redundant power supply from day one			Already Clarified above
4			The management platform must be able to store record of 15000 user or more	The management platform must have 1 x 2TB hot swap HDD and 32 GB RAM from day 1.	Pls mention the storage requirement.	Already Clarified above

5			The management platform must provide a highly customizable dashboard.			As per RFP
6			The management platform must domain multi-domain management			Refer Corrigendum-II
7			The management platform must provide centralized logging and reporting functionality			As per RFP
8			The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows			Already Clarified above
	SOR-C –iii – Firewall Manager:					
			Minimum Specification requirement	Check Point's comment & revised specification	Remarks	
1			The management platform must be accessible via a web-based interface and ideally with no need for additional client software	The management platform must be accessible via a web-based interface and/or with additional client software	This is specific to one OEM. Pls change.	Already Clarified above
2			The management platform must be a dedicated OEM appliance and VM running on server will not be accepted			Already Clarified above
3			The management appliance should have 2 x 1G port and integrated redundant power supply from day one			Already Clarified above
4			The management platform must be able to store record of 15000 user or more	The management platform must have 1 x 2TB hot swap HDD and 32 GB RAM from day 1.	Pls mention the storage requirement.	Already Clarified above
5			The management platform must provide a highly customizable dashboard.			Already Clarified above
6			The management platform must domain multi-domain management			Already Clarified above
7			The management platform must provide centralized logging and reporting functionality			Already Clarified above
8			The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows			Already Clarified above
9			The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.			
10			Should support troubleshooting techniques like Packet tracer and capture			
11			Should support REST API for monitoring and config programmability			
12			The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.			
13			The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e- mail, SYSLOG).			
14			The centralized management platform must not have any limit in terms of handling logs per day			Already Clarified above
15			Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one			
16			The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.			
17			The management platform support running on-demand and scheduled reports			
18			The management platform must risk reports like advanced malware, attacks and network			
19			The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.			
20			Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.			

21			Online upgrade the version of firmware/software/patches as and when required.			
22			Telephonic support with call logging mechanism should be provided on 24x7x365 basis.			
23			Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.			
24			All the technical specifications mentioned above must be available from day one			
25			Solution should be able to manage vFirewall and UTM mentioned in SOR			
	FIRM-10:	CCS Computers Pvt. Ltd.		Rana Kumar: rana.kumar@ccscomputers.co.in		
	SOC					
SN	Page No.	Heading	Point Description	Query	Recommendation/Suggestion	
1	13	Chapter 3A, Pt 2	Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.	Does this mean that OEM PS would be doing the implementation	OEM authorized partner shall do the implementation	Refer Corrigendum-II
2	29	SOR-D-i-SOC, Pt 1	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018	this should allow atleast last 3 or 5 years gartner report or it should allow both leader & challenger quadrant solution	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management atleast once in last 5 years	Refer Corrigendum-II
3	29	SOR-D-i-SOC, Pt 3	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000 EPS.	As in ArcSight SIEM, flows are also considered under EPS licensing only. So whether solution needs to be proposed including flows for 10000 EPS license or 15000 EPS license.	The proposed solution should be able to handle 10,000 sustained EPS.	Refer Corrigendum-II
4	31	SOR-D-i-SOC, Pt 4 (Operational Requirement)	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated.	Do we mean software patches updates as well by this point. Here as per industry best practices, it is never recommended to put your SIEM solution to a direct internet acess.	Either this point should be deleted or should be updated as " The solution must support the automatic update of configuration information via a centralized management console with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated."	Refer Corrigendum-II
5	31	SOR-D-i-SOC, Pt 4 (Architectural Requirement)	The solution must provide browser-based UI access for end users (does not require thick client)	As ArcSight correlation solution works with thick client based UI for advanced level analysis and content creation. Also ArcSight command centre is used for management and monitoring through browser based web UI.	This point should be modified as "The solution must provide browser-based/thick client UI access for end users"	Refer Corrigendum-II
6	33	SOR-D-i-SOC, Pt 8 (Log Management Requirement)	The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.	Please specifiy the X I.e. exact no of months for both online and offline log retention	3 months online and 1 year offline	Already Clarified above
7	33	SOR-D-i-SOC, Pt 9 (Log Management Requirement)	The solution should capture flow information from multiple network points. Solution should support Network traffic collected via TAP, SPAN, and/or Mirror.	This point is part of packet capture solution so should not be part of SIEM solution.	This point should be deleted.	Refer Corrigendum-II
8	37	SOR-D-i-SOC, Pt 9 (Correlation & Alerting)	The solution proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. a) Flow based threat Detection b) User Behavior analysis c) DNS data analysis.	Are the following systems existing in Railtel or it is mentioned from future roadmap perspective.		Already Clarified above

9	46	SOR-D-iv- Vulnerability Assessment	Vulnerability Assessment - Only Network Based	The ask in RFP is only for VA of Network/host while VA/PT of applications/web servers is missing from the ask. We highly recommend that it should also be part of RFP ask.		Already Clarified above
	FIRM-12:		Hitachi Systems	Jay ShankarSingh: jayshankar.singh.bn@hitachi-systems.com		
SN	RFP Page No.	Point/Section No.	RFP Clause	Bidder's Remarks		
1	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	the scanning solution must be software / appliance based, that is deployable in windows and linux platforms	Tenable can be deployed in Linux flavours only. Therefore , as a request , please arrange to remove the Ms platform or change the clause as- "the scanning solution must be software / appliance based, that is deployable in windows/linux platforms"		Refer Corrigendum-II
2	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The Signature database must be exportable to CSV, PDF etc	Every OEM has different way of exporting the plugins database, We request you to change the clause as- "The Signature database must be exportable to CSV/PDF etc"		Already Clarified above
3	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The solution Must allow various output formats like CSV, DOC, HTML, PDF, XML etc	Tenable has multiple reporting format like PDF, CSV, Richtext and cyberscope. We requesy client to change the clause as- "The solution Must allow various output formats like CSV/ DOC/ HTML/PDF/XML etc"		Already Clarified above
4	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The Solution must identify the critical vulnerabilities to prioritize remediation iii) Identify vulnerabilities with zero day	Tenable as a OEM has the maximum number of Vulnerability coverage and as a policy Tenable (R &D)first inform the zero day vulnerability to the respective OEM and don't declare it publicly as its likely to be exploited if OEM is not ready with the solution/Patch. So we request customer to remove the clause pls.		As per RFP
5	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The Solution must identify the critical vulnerabilities to prioritize remediation iv) Identify Zero Day vulnerabilities	Tenable as a OEM has the maximum number of Vulnerability coverage and as a policy Tenable (R &D)first inform the zero day vulnerability to the respective OEM and don't declare it publicly as its likely to be exploited if OEM is not ready with the solution/Patch. So we request customer to remove the clause pls.		As per RFP
6	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The solution must offers integrated password management integration with PowerBroker Password Safe as well as it includes a built-in third party password management connector.	CyberArk is global leader in Privilege Identity Management space and is more widely used in India than Beyond Trust. Request you here to include add cyberArk as well with Beyond Trust.		Already Clarified above
7	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	Addition of Clause	OEM should be the leader as per Gartner peer Insights		As per RFP
8	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	24.The Solution must perform automated Asset inventory and must be able to collect and allow searching via inventory details like vi) Inventory of Hardware manufacturer for Host OS like workstations, Servers and laptops vii) Inventory of drives & file shares	Since this point is refering to dedicated asset & patch management solution, we request you to remove the point vi & vii in clause 24.		As per RFP
9	47	SOR-D-iv- VULNERABILITY ASSESSMENT:	The solution Must provide a graphical, interactive and search friendly topology of the discovered assets	Since this point is refering to dedicated asset & patch management solution, we request you to remove the point.		Already Clarified above
10	15	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	Is the expectation by this requirement is that the proposed solution should have a minimum of 6000 signatures as default to detect and protect Web Applications. Kindly clarify		Already Clarified above

11	19	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	we understand that it s a multimode SFPs that is required but as required the appliance has to be fully populated request you to Kindly clarify how many Interfaces is required for each type 1Gig, 10Gig and 40gig. As there could be a possiblity of permutation combination on the type and interfaces proposed while fully populating the appliance SFP slots		Already Clarified above
12	19	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	Gartner report of 2019 is not yet published so the Gartner report of 2017/2018 will suffice kindly confirm		Already Clarified above
13	20	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The solution should support Unified Anti-Bot Detection and Protection & Cloning Application Traffic	Does this clause means that a proposed WAF solution should have capability to detect and mitigate BOT attacks using multiple level of security checks Via Bot Signature, Application Fingure printing, Java Challenge, Browser capability check and Captcha. Kindly confirm		Already Clarified above
14	20	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	Kindly elaborate		Already Clarified above
15	72	CHAPTER 4 - - - COMMERCIAL TERMS & CONDITIONS. - - - 3. Long Term Maintenance Support	Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added to the equipment cost towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five years differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 5 years after the warranty	3.5% AMC for security solution like WAF or any similar security solution is not a realistic %. We request Railtel to kindly make this clause to at least 15% per annum instead of 3.5% per annum		Already Clarified above
16	NA	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	Additional Clause	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.		
17	NA	SIEM	Query	Is it required to create entire setup replica in DR for SIEM		Already Clarified above
18	NA	LOG MANAGEMENT REQUIREMENT	Query	Pls suggest the time for which log has to be sotred online and offline so that the storage/loggers can be sized accordingly		Already Clarified above
19	NA	Collectors	Query	For the purpose of log collection, please specify if the logs to be collected are from different locations or only from the log sources at DC ? Pls suggest the count of collectors to be factored		Clarification: Log sources can be anywhere in DC & DR.

20	69	CHAPTER-3-C 1. TRAINING	The training course to be conducted at the manufacturing facilities shall be designed to train the trainees in all aspects of System engineering, equipment operation, installation and functional details, theory of operation of equipment, trouble shooting and familiarization with the equipment at card and component level. All equipment used for training shall be identical to those quoted and supplied for site installation in hardware and software versions.	We request that the traning can even be done on the product and in live encironment so that the actual real scenario can be showcased.		No Change, As per RFP
21	89	CHAPTER-5 Clause 4	Delivery Period Delivery and supervision of installation and commissioning within 120 days of issue of LOA/PO.	We request you to pls change the following clause to- Delivery and supervision of installation and commissioning within 200 days of issue of LOA/PO.		No Change, As per RFP
22	Query	SOR-D-iv Vulnerability Assessment	Query	Pls sugest the count of IPs for Vulnerability Assessment solution as the solution's BOQ needs to be sized accordingly		Refer RFP Specs, it is mentioned clearly.
23	29	SOR-D-i – SOC: Detailed Technical Specifications	1.The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018	We request you to change the clause as- 1.The solution must be a Leader/CHallenger in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018 Or The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management atleast once in last 5 years		Already Clarified above
24	NA	CHAPTER-3-A Technical Requirement - - SOR A: Web Application Firewall	The proposed WAF solution should also have capability for BOT Detection that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.	The proposed WAF solution should also have BOT Detection feature that have capability to identify Bot Signature + DNS checks, Java script challenge + Browser Fingerprinting, Browser Capabilities, Optional CAPTCHA, Human Detection & Anomalies.		Already Clarified above
1	13	Chapter 3A, Pt 2	Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.	Does this mean that OEM PS would be doing the implementation Recommendation/Suggestion- OEM authorized partner shall do the implementation		Already Clarified above
2	29	SOR-D-i-SOC, Pt 1	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018	this should allow atleast last 3 or 5 years gartner report or it should allow both leader & challenger quadrant solution		Already Clarified above
3	29	SOR-D-i-SOC, Pt 3	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000 EPS.	As in ArcSight SIEM, flows are also considered under EPS licensing only. So whether solution needs to be proposed including flows for 10000 EPS license or 15000 EPS license. Recommendation/Suggestion- The proposed solution should be able to handle 10,000 sustained EPS.		Already Clarified above
4	31	SOR-D-i-SOC, Pt 4 (Operational Requirement)	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated.	Do we mean software patches updates as well by this point. Here as per industry best practices, it is never recommended to put your SIEM solution to a direct internet acess. Either this point should be deleted or should be updated as " The solution must support the automatic update of configuration information via a centralized management console with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated."		Already Clarified above

5	31	SOR-D-i-SOC, Pt 4 (Architectural Requirement)	The solution must provide browser-based UI access for end users (does not require thick client)	As ArcSight correlation solution works with thick client based UI for advanced level analysis and content creation. Also ArcSight command centre is used for management and monitoring through browser based web UI. Request you to modify the point as "The solution must provide browser-based/thick client UI access for end users"		Already Clarified above
6	33	SOR-D-i-SOC, Pt 8 (Log Management Requirement)	The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.	Please specifiy the X I.e. exact no of months for both online and offline log retention Recommendation/Suggestion is 3 months online and 1 year offline		Already Clarified above
7	33	SOR-D-i-SOC, Pt 9 (Log Management Requirement)	The solution should capture flow information from multiple network points. Solution should support Network traffic collected via TAP, SPAN, and/or Mirror.	This point is part of packet capture solution so should not be part of SIEM solution. Request you to delete this point		Already Clarified above
8	37	SOR-D-i-SOC, Pt 9 (Correlation & Alerting)	The solution proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. a) Flow based threat Detection b) User Behavior analysis c) DNS data analysis.	Are the following systems existing in Railtel or it is mentioned from future roadmap perspective.		Already Clarified above
9	46	SOR-D-iv- Vulnerability Assessment	Vulnerability Assessment - Only Network Based	The ask in RFP is only for VA of Network/host while VA/PT of applications/web servers is missing from the ask. We highly recommend that it should also be part of RFP ask.		Already Clarified above
	FIRM-13:	M/s. Barracuda Networks		Vikas Pandey: vpandey@barracuda.com		
	SOR-B: Backup Solution:					
SN	WAF - Minimum Requirement Description	Query	Description of requested change	Justification		
1	CHAPTER- 2. Backup Solution as per Technical Nos. Specification given in Chapter-3A	The Quantity asked in the RFP is 1, we understand that the solution must go for DC and DR , we understand that there are two boxes with same configuration . Kindly confirm	Please Increase the Backup solutiion Quantity as 2 Units in the SCHEDULE OF REQUIREMENT at Page 5	We understand that the solution must go for DC and DR , we understand that there are two boxes with same configuration for Data Replication		Clarification: Quantity as per RFP. It may be deploy either DC or DR.
	SOR-A:Web Application Firewall:					
SN	WAF - Minimum Requirement Description	Query	Description of requested change	Justification		
1	The solution's monitoring appliance must be able to support ALL of the following deployment modes to monitor web application traffic over the network: - Via a SPAN/TAP port sniffing mode - Layer-2 transparent inline mode - Reverse Proxy mode - Transparent Layer-2 Reverse Proxy mode	**Span port WAFs:** (Challenges) Limited Blocking, Requires Reconfiguring Peer devices Spanning fails under load, No visibility of attacks, Lack ability to modify content (cookie security, CSRF protection, etc.) So Span port deployment is good for POC's only. Request you to please remove SPAN port / TAP mode from RFP.	The solution's monitoring appliance must be able to Various deployment modes to monitor web application traffic over the network such as :- - Via a SPAN/TAP port sniffing mode/Bridge Mode - Layer-2 transparent inline mode - Reverse Proxy mode - Transparent Layer-2 Reverse Proxy mode	For Monitoring appliance can be deployed in Bridge, We do support bridge mode . Request you to consinder the request so we can particiapte		Already Clarified above

2	The solution must support the following authentication mechanism for accessing the solution management UI: - In-built authentication in the solution - Kerberos authentication - LDAPS authentication and authorization with the following Windows platforms: 2003, 2003 R2, 2008, 2008 R2, 2012, and 2012 R2. - RADIUS authentication	Please add 2FA (RSA) for management as well	The solution must support the following authentication mechanism for accessing the solution management UI: - In-built authentication in the solution - Kerberos authentication - LDAPS authentication and authorization with the following Windows platforms: 2003, 2003 R2, 2008, 2008 R2, 2012, and 2012 R2. - RADIUS authentication and 2FA (RSA) for management as well	Addting 2FA (RSA) for management gives more security		As per RFP
14	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode.	Requesting you to Please remove the term "sniffing mode"	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in the event of active enforcement deployment mode.	This Sniffing mode feature is good for POC /Demo only , Not recommended for Actual Deployment because of Limitation		As per RFP
15	The solution must be able to protect both HTTP Web applications and SSL (HTTPS) web applications.	Yes				As per RFP
16	The solution must be able to decrypt SSL web traffic between clients and web servers.	Yes				As per RFP
17	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode.	Vendor Specific	The solution must be able to decrypt SSL web traffic if appliance deployed in transparent layer-2 mode.	Requesting you to Please remove the term "Diffie-Hellman " as this is Vendor Specific , So we can Partiicipate		As per RFP
18	The solution must provide the ability to comply to A+ Certification at the click of a button	" A+ Certification Button" is Vendor Specific , Request you to modify this Point and remove the Term "at the click of a Button "	The solution must provide the ability to comply to A+ Certification	The Term " Click of a button" is Vendor Specific. In A+ Certfications can be acieved by enabiling , Which others can also delivers Achieving an A+ grade is a non-trivial task; however, it can be done in an afternoon (even in less than an hour) when starting from the right point. Currently, to achieve an A+ rating with SSL labs, a user must follow these recommendations; otherwise the site would receive the following grade in brackets. • Disable SSLv3 [B] & RC4 [B/C] • Replace any SHA1 Certs [A] and sub-2k Certs [C] • Enable TLS_FALLBACK_SCSV [A] • Enable HTTP Strict Transport [A] • Enable and Prefer Perfect Forward Secrecy Compatible Ciphers [A-] Do not use DHE ciphers (only ECDHE). DHE ciphers will cap the grade at [B] on BIG-IP. • Enable TLS1.2 [C] • Enable Secure Renegotiation [A-] The DEFAULT cipher string included in BIG-IP version 12.0 will yield a B grade but offers full hardware acceleration. To get that coveted A+ grade, an administrator would need to have a fairly restrictive cipher list. For example “!SSLv3:!DHE:ECDHE:RSA+HIGH” will get an		Refer Corrigendum-II

22	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	The Langaue the Vendor Specific , Please Modify this Clause	The solution must have a database of minimally 6000+ signatures or Super Patterns that are designed to detect known problems and attacks on web applications.	Some Solution follows a different architecture for signatures.. we use what is called as "super patterns".. so 1 pattern would translate into multiple patterns.. and we use a digest technique called DFA to process these patterns against an incoming request. Product efficiency should be measured by the effectiveness of the blocking, not by number of patterns		Already Clarified above
55	The solution must support user tracking using both form-based and certificate-based user authentication.	This is Vendor Specific	The solution must support user tracking using form-based /certificate-based user authentication.	Others can Achieve this via client Authentication using SSL		As per RFP
	d. Other (please specify).			Our Web application Firewall supports Many predefined reports such as PCI , DSS , attack summary		
101	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities. Like:- - Acunetix - Beyond Security - Cenzic - Denim Group	Request you to Modify this Point	The solution must support the web application vulnerability assessment tools to virtually patch web application vulnerabilities. Cenzic Hailstorm v6.6 HPE Security WebInspect HPE Security Fortify On Demand IBM AppScan v7.9 IBM AppScan v9.0 ImmuniWeb ThreadFix Rapid7 Qualys	Currently our Web Application Firewall supports the following Industry Standered scanner Barracuda Vulnerability Manager Cenzic Hailstorm v6.6 HPE Security WebInspect HPE Security Fortify On Demand IBM AppScan v7.9 IBM AppScan v9.0 ImmuniWeb ThreadFix Rapid 7 Qualys		Already Clarified above
	- HP Fortify WebInspect					
	- IBM AppScan					
	- NT OBJECTives					
	- Qualys					
	- Rapid7					
	- Trend Micro					
	- Veracode					
	- WhiteHat					
102	The solution must be able to support 2 Gbps of WAF (HTTPS) throughput	Request you to Modify this Point	The solution must be able to support 4 Gbps of WAF (HTTPS) throughput	4 GBPS will have better performance		As per RFP
104	System must have minimum(fully populated) 6 x10G SFP/SFP+ Ports and 2 x 40G ports, (Should Option to Select Single Mode or Multimode Fiber Port)	Please Modifiy this Point	System must have minimum (Fully Populated) 1 no's of Management port 10/100/1000 + 8 x GbE w/bypass SPF (MM) & 2 x 10 GbE w/bypass SPF+ (MM)	The requirement is for 2 GBPS WAF throughput , Barracuda 960 Model Can deliver 5 GBPS of thoughput with 2 * 10 Gig Ports		As per RFP
105	The proposed appliance should support Hardware based HTTP Compression, that is 20GBps of Hardware compression from day one	This is Vendor Specific .. This is Load Balancer Point	Please remove this point	WAF throughtput Mesuirng creteria should be based on tps, cps, throughput and concurrent connections . Barracuda Model 960 can process 50000 Transaction per second		As per RFP
106	The proposed appliance should support 20GBps of Bulk Encryption from day one	This is Vendor Specific .. This is Load Balancer Point	Please remove this point	WAF throughtput Mesuirng creteria should be based on tps, cps, throughput and concurrent connections . Barracuda Model 960 can process 50000 Transaction per second		As per RFP
108	The proposed solution should have 64bit OS architecture	This is Vendor Specific as Every vendor have different OS Architecture	Please remove this point	Please remove this point from RFP to make it generic		As per RFP

109	the proposed appliance should have capability of Hardware based DDOs protection up to 50M Sync Cookies per second	This is Vendor Specific , Please remove this Point from WAF RFP	This is Vendor Specific , Please remove this Point from WAF RFP	This is not supported by many WAF vendor, request to please remove this from WAF RFP so Barracuda Networks can also comply , DDoS solution can be managed or can be installed seperatly. This should not be part of WAF RFP. Please remove this point from WAF RFP. Syn flood attack protection is supported on barracuda WAF & application DDoS as well.		Already Clarified above
110	The proposed hardware should include a LCD panel which should support Configuration for Initial Management IP address and display all the error and information corresponding to hardware & software without logging into the appliance.	This is Vendor Specific , Please modify this point	The proposed hardware should include a LCD panel or option to connect monitor and key board to configure Initial Management IP address and display all the error and information corresponding to hardware & software.	This is Vendor specific , Please make it Generic so Barracuda Networks can also comply		As per RFP
111	The proposed appliance should be of 1U formfactor	This is Vendor Specific , Please modify this point	The proposed appliance should be of 1U or 2U formfactor	Please change it to 2U as some have different form factor		As per RFP
113	the proposed appliance should have minimum of 450GB of SSD Hard Drive for better performmance from day one	This is Vendor Specific , Please modify this point	the proposed appliance should have minimum of 240GB of SSD Hard Drive for better performmance from day one	For historical logs SIEM / Syslog server is recommended. Please Modify this Point		As per RFP
115	The proposed appliance should support up to 35K SSL TPS with Dedicated SSL Offloading Chip. TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.	Please Modifiy this Point to 45K SSL PTB Minimum for better performance	The proposed appliance should support up to 45K SSL TPS with Dedicated SSL Offloading Chip. TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.	Better Performance		Already Clarified above
123	Should support client certificate constrained delegation (C3D) which will enable the Load balancing solution to generate certificates on behalf of clients and pass it to the end servers if SSL based client authentication has been enabled on the backend servers .	This is Vendor Specific , Please modify this point	Web Application Firewall supports Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs) to determine the current status of client digital certificates.	This is vendor specific. Request you to please Modify this point so others can qualify		Refer Corrigendum-II
124	Should Support Active/Standby, Active/Active & N+1	Term "N+1" This is Vendor Specific and is good for virtual WAF deployment	Should Support Active/Standby, Active/Active or N+1	Term "N+1" This is Vendor Specific and is good for virtual WAF deployment , Please modify this point so others comply		As per RFP
126	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL Connection mirroring for SSL connections that are terminated/offloaded on the Server Load Balancer . Hence old connection should not fail or forced for SSL renegotiation esp for applications for which the server load balancer is doing SSL offloading.	This is Vendor Specific , Please modify this point	Should have active-active and active-backup high availability with TCP/IP connection mirroring or SSL Connection mirroring for SSL connections or session state failover that are terminated/offloaded on the Web Application Firewall. Hence old connection should not fail or forced for SSL renegotiation esp for applications for which the WAF is doing SSL offloading.			As per RFP
127	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	This is Vendor Specific , Please modify this point	Should support interactive Layer 7 health checks for the application availability	Please Modifiy this point so others can comply		Already Clarified above

134	The proposed WAF should support ICAP, the security protocol for sending and receiving uploaded files for antivirus scanning from day one	Please Modify this Point	The proposed WAF should support ICAP, the security protocol for sending and receiving uploaded files for antivirus scanning from day one or Solution should have In-built anti-virus for file uplaods"	Please Modfy this point so others can Comply		As per RFP
135	The proposed solution shall support both positive and negative security model and work in HA mode with TCP, *SSL mirroring of the traffic that is offloaded on the appliance and persistence mirroring,* so that user session shall not be disconnected after failure of primary device. It shall improve the users experience.	This is Vendor Specific , Please remove this point as this allready covered Point Number 126 in the RFP	Please Remove this Point			As per RFP
136	System must support TCP optimization, TCP Buffering, TCP Connection Multiplexing to enhance protocol performance	The Term " TCP Buffering" This is Vendor Specific , Please modify this Point	System must support TCP optimization, TCP Connection Multiplexing to enhance protocol performance	The Term " TCP Buffering" This is Vendor Specific , Please modify this Point so Others can comply		As per RFP
137	WAF should support for future requirement to Anti-Bot Mobile SDK to Whitelist establish trust based on an embedded software package within the customer's application code, and corresponding cookie verification from day one	Please remove this point for the RFP	Please remove this point for the RFP	Not supported, planned… this is in Barracuda Road Map. Please remove this feature from the RFP or allow us to submit the dates when this is going to introduce within the solution.		As per RFP
138	Supported 3rd Party Repudiation Database which include Blacklisted IP Address, TOR, System Vulnerabilities, Country, Bad Proxy , Spam Source, Mobile Threats etc.	3rd Party Repudiation is specific to vendor who don't have their own research , Please Modify this point	Solution Should have buit-in or Support 3rd Party Repudiation Database which include Blacklisted IP Address, TOR, System Vulnerabilities, Country, Bad Proxy , Spam Source, Mobile Threats etc.	Supported, including our own threat research. Some Vednor does not have their own research, which is why they are asking specifically for 3rd party. Also TOR is available free without 3rd party DB's.		As per RFP
141	The Platform must be able to allow the enterprise to measure infrastructure performance as it relates to application delivery, and to factor that application performance data into business intelligence tools such as troubleshooting, ROI calculations, and capacity planning.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP

142	The Proposed Management and reporting Platform must be able to provide tools for monitoring applications across the entire Application delivery network. E.g dashboard displays system statistics in selectable graphs, gauges, and tables. In addition to the pre-defined views, you can create custom combinations of the dashboard windows, and save them in groups. You can combine windows from different software modules in a single view, or use just the windows you want for a single module. Windows are available only for those modules that you have licensed and provisioned.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
143	The Proposed Management and reporting Platform must be able to support historical statistics collection on CPU and memory usage, connections, and throughput in an easy-to-read graphical view and displays real-time historical stats by the hour, day, week, or month from the web dashboard GUI. In addition to real-time stats, historical trending reports must be viewed by hour, day, week, or month. E.g. view "real-time" profile and CPU usage statistics for individual virtual servers and "real-time" CPU and memory usage statistics for individual modules.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module ,This is achived via any 3rd party reporting module.	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
144	The Platform must be able to support Network Map of the virtual server IP addresses and server pools.	This is Vendor Specific	Please Remove this Point	This is Vendor Specific		As per RFP
145	The Platform must be able to provide aggregated application visibility and reporting tools at the application level. This include viewing of detailed statistics about application traffic running through the system.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
146	The Platform must be able to provide real-time application performance statistics, and diagnostic and troubleshooting information such as application response time, network latency, and connection statistics for the entire application, virtual servers, pools, and nodes.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP

147	The Platform must be able to provide user-created custom statistics that can be built on-the-fly by preconfiguration or predefined for more granular data and control through scripting or command shell. This is a mechanism for tracking information like metrics such as connections, data rates, etc.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
148	The Management Platform should be able to perform device discovery and monitoring: Discover, track, and monitor up to 5 devices from day one—whether physical or virtual, both on-prem and in the cloud.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
153	The Management Platform should have utility license usage reporting: Enable utility licensing of its managed devices by generating and delivering reports of device use over time.	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM	Please Remove this Point	This is Vedor Specific , Please remove this point as this is a WAF RFP and not a reporting Module , SIEM is Part of this RFP and it is achieved via SIEM		As per RFP
	FIRM-14:	Micro Focus		ARPIT GOEL: arpit.goel@microfocus.com		
SN	Page No.	Heading	Point Description	Query	Recommendation/Suggestion	
1	13	Chapter 3A, Pt 2	Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.	Does this mean that OEM PS would be doing the implementation	OEM authorized partner shall do the implementation	Already Clarified above
2	29	SOR-D-i-SOC, Pt 1	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018	this should allow atleast last 3 or 5 years gartner report or it should allow both leader & challenger quadrant solution	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management atleast once in last 5 years	Already Clarified above
3	29	SOR-D-i-SOC, Pt 3	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000 EPS.	As in ArcSight SIEM, flows are also considered under EPS licensing only. So whether solution needs to be proposed including flows for 10000 EPS license or 15000 EPS license.	The proposed solution should be able to handle 10,000 sustained EPS.	Already Clarified above
4	31	SOR-D-i-SOC, Pt 4 (Operational Requirement)	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated.	Do we mean software patches updates as well by this point. Here as per industry best practices, it is never recommended to put your SIEM solution to a direct internet acess.	Either this point should be deleted or should be updated as " The solution must support the automatic update of configuration information via a centralized management console with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated."	Already Clarified above
5	31	SOR-D-i-SOC, Pt 4 (Architectural Requirement)	The solution must provide browser-based UI access for end users (does not require thick client)	As ArcSight correlation solution works with thick client based UI for advanced level analysis and content creation. Also ArcSight command centre is used for management and monitoring through browser based web UI.	This point should be modified as "The solution must provide browser-based/thick client UI access for end users"	Already Clarified above

6	33	SOR-D-i-SOC, Pt 8 (Log Management Requirement)	The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.	Please specifiy the X I.e. exact no of months for both online and offline log retention	3 months online and 1 year offline	Already Clarified above
7	33	SOR-D-i-SOC, Pt 9 (Log Management Requirement)	The solution should capture flow information from multiple network points. Solution should support Network traffic collected via TAP, SPAN, and/or Mirror.	This point is part of packet capture solution so should not be part of SIEM solution.	This point should be deleted.	Already Clarified above
8	37	SOR-D-i-SOC, Pt 9 (Correlation & Alerting)	The solution proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. a) Flow based threat Detection b) User Behavior analysis c) DNS data analysis.	Are the following systems existing in Railtel or it is mentioned from future roadmap perspective.		Clarification
9	46	SOR-D-iv- Vulnerability Assessment	Vulnerability Assessment - Only Network Based	The ask in RFP is only for VA of Network/host while VA/PT of applications/web servers is missing from the ask. We highly recommend that it should also be part of RFP ask.		Refer Corrigendum-II
	FIRM-15:		Veritas	Nasir Mir: Nasir.Mir@veritas.com		
SN	Page no.	RFP Volume Section and sub-section	Clause/ Content in the RFP	Clarification sought/ Change Request	Remarks/Justification	
1	22	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	5. Solution Must support Host-Level Virtual Environments Including VMware vSphere, Microsoft Hyper-V	Please modify Clause as "Solution Must support Host-Level Hypervisor integration for Virtual Environments Including VMware vSphere, Microsoft Hyper-V, RedHat KVM, Nutanix AHV, OpenStack and Containers"	request to include support for lastest hypervisors also like Openstack, containers, AHV and others as requested as most of enterprise backup software vendors support all latest hypervisors. This is required considering current and future requirment for cloud Infrastructure of the Railtel Department.	Already Clarified above
2	22	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	6. Solution must support back agents Including Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux and macOS	Please modify Clause as "Solution must support back agents Including Microsoft Windows, Linux, Unix and macOS. Also include Agent/Modules for online backup of applications and databases such as MS Exchange, MS SQL, Oracle, DB2, Sybase, MySQL, MongoDB, PostGre SQL and distributed databases/filesystems like NoSQL, Bigdata and hadoop. "	Request department to include support for all major databases including Haddop Bigdata as this may be required by department consideting cloud infrastructure and haterogenous applications used by railtel. Most of the enterprise backup software vendors provide support for all these common applications and databases.	Already Clarified above
3	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	9. Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Please modify as "Solution must support Advanced sharing of different media across the environment (disk and tape)."	Optical device like CD,DVD cannot be shared and usually never used as backup storage, so request to remove Optical word.	Already Clarified above
4	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	11. Solution should offer rate limiting for data sent offsite to limit the impact of replication on critical Internet resources.	Please modify clause as "Solution should offer inbuild WAN Optimizer for data sent offsite to limit the impact of replication on critical Internet resources."	This clause looks some vendor specific, request to modify it as requested so that most of Enterprise backup vendors will participate in the bid. WAN optimization is the proper term and feature in most of backup solutions for optimizing backup data replication to offsite location.	Already Clarified above
5	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	15. Solution should offer message level backups for MS Exchange and allow for restore of individual messages or entire folders.	Please modify clause as " Solution should offer full backup of MS Exchange databases and allow for restore of full and individual messages."	This clause looks favouring a specific vendor and not a geniric feature. Please note most of the enterprise backup solution vendors provide MS Exchange backup at database level, however the restore can be done on granular single mail/message level. please modify so that most of enterprise backup solution vendors can participate in the bid.	Already Clarified above

6	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	18. Solution must support GUI with centralized management / Single interface for management of all backup and archival activities.	Please modify clause as "Solution must support GUI with centralized management / Single interface for management of all backup activities.	request to remove archival word as this requirment is related to a backup solution and not the archival software, both of them cater to a different requirment.	Already Clarified above
7	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	19. Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Remove this repeated clause no 9	Repeated clause, request to delete clause or remove optical word.	Already Clarified above
8	23	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	21. Solution must support following application and database backup without CLI and without the requirement of temporary disk space for Oracle, 64-bit Active Directory, MS SQL, MS Exchange, Share-Point, MySQL etc.	Please modify clause as "Solution must support following application and database backup without CLI and without the requirement of temporary disk space for Oracle, 64-bit Active Directory, MS SQL, MS Exchange, Share-Point, MySQL etc, also provide online backup for open and distributed databases like MongoDB, NoSQL, Nutanix, Bigdata and hadoop."	Request department to include support for all major databases including Haddop Bigdata as this may be required by department consideting cloud infrastructure and haterogenous applications used by railtel. Most of the enterprise backup software vendors provide support for all these common applications and databases.	Refer Corrigendum-II
9	24	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	32. Solution should support rapid/instant VM recovery with LiveBoot for Vmware and Microsoft Hyper-V	Please modify clause as "Solution should support rapid/instant VM recovery with LiveBoot for proposed virtualization hypervisor platform"	This clause looks some vendor specific, request to modify it as requested so that most of Enterprise backup vendors will participate in the bid.	Already Clarified above
10	24	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	34. Solution Should have 48TB of Usable Capacity with HW RAID 60	Please modify clause as "Backup Appliance Should have minimum 50TB of Usable Capacity and scalable to more than 300TB Usable with HW RAID 60"	Considering the future growth of Railtel cloud Infrastructure, it is necessary for department to define the scalability in backup appnliance. This will help department to get the lastest scalable backup appliance with storage expansion feature. Most of the Backup appliance vendors provide scalability more than 300TB usable in their backup appliance devices, so there will be no issues for most of vendors to participate in the bid.	Already Clarified above
11	24	CHAPTER-3-A Technical Requirement SOR-B: Backup Solution	35 . Appliance Should have 2 x 10Gb RJ45 or 2-port SFP+ Network Interface	Please modify clause as "Appliance Should have minimum 4 x 1Gbps Ethernet, 4 x 10Gbps Ethernet(SFP and Copper) and 2 Fibre Channel ports of minimum 8Gbps speed"	Considering current and furture requirments of railtel cloud infrastructure, it is necessary for department to request for all the necessary network interfaces in requested backup appliance. Please note almost all the backup appliance vendors provide all 1Gbps, 10Gbps and FC ports with their devices and if not rerequested, department may get the appliance missing these common required interfaces.	Already Clarified above
	FIRM-16:		TREND MICRO	Govind Singh: govind_si@trendmicro.com		
SN	RFP Volume Section and sub-section	Page no.	Clause/ Content in the RFP	Clarification sought/ Change Request		
1	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 20	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log	Pager is an obsolete technology and most of vendors has stop supporting as a medium for sending notification **Clause Should Read as :** Shall offer customizable & standard notifications via - SMTP, SNMP, NT Event Log		Already Clarified above

2	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 21	The solution should provide quarantine management in order to prevent spreading. A management interface must be provided to allow the administrator to review, sort and analyze quarantined items.	This is specific to one OEM and restricting us from participation **Clause Should Read as :** The solution should provide quarantine management in order to prevent spreading. A management must be provided to allow the administrator to restore quarantined items in case file found to be legitimate		Already Clarified above
3	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	43, Point no. 28	Solution must provide virtualized environment	Please help in elaborating the use case of this requirement		Already Clarified above
4	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	45, Point no. 56	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers or provide attack prevention using the least privilege containment approach	This is specific to one OEM and restricting us from participation **Clause Should Read as :** The solution should use HIPS (host) based signature to proactively protect against intrusion targeted at the servers		Already Clarified above
5	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	46, Point no. 70	Solution should have an emulator to cause threats to reveal themselves. This should not be a part of sandboxing and should run individually in each agent	This is specific to one OEM and restricting us from participation **Clause Should Read as :** Solution should have a mechanism to Identifies packed malware in memory as it unpacks prior to execution using machine learning functionality		Already Clarified above
6	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	45, Point no. 71	Solution should have Deception component from same or different OEM which helps identify the unknown attacks that conduct file traversals, network discovery, terminate processes, try to conduct credential theft, and more	This is specific to one OEM and restricting us from participation **Clause Should Read as :** Solution should have functionality which helps identify the unknown attacks		Already Clarified above
7	SOR-D-ii & iii - Anti Virus + EDR (Client & Server):	46, Point no. 73	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest OS patches have been applied to the operating system.	This is specific to one OEM and restricting us from participation **Clause Should Read as :** The Solution should check for the existence of open known vulnerabilities and shield them using virtual patching technology		Already Clarified above
8	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	46, Point no. 74	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, downloading and executing/inserting a software, running scripts , by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.	This is specific to one OEM and restricting us from participation. Hence please help in removing this clause to allow our participation		Already Clarified above
9	SOR-D-ii & iii - Anti Virus + EDR (Client & Server)	46, Point no. 75	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.	This is specific to one OEM and restricting us from participation. Hence please help in removing this clause to allow our participation		Already Clarified above
10	SOR-D-i – SOC:Packet Capture	41	Specifications from Serial no. 1 to 38	Specificaitons are specific to one particular OEM and restricting us from participation. Please help in diluting the specification to allow our participation		Already Clarified above
	FIRM-21:		Fortinet	Saroj Kumar Das: saroj@fortinet.com		
			Existing	Changes Required		
			SOR-C-ii -UTM			
		6	UTM/NGFW appliance should have at least 32 GB RAM or higher			Already Clarified above
		10	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one		Already Clarified above

		35	The IPS system should have at least 25,000 signatures with support for custom IPS signatures	The IPS system should have at least 10,000 signatures with support for custom IPS signatures		Already Clarified above
			SOR-C –iii - Firewall Manager			
		3	The management appliance should have 2 x 1G port and integrated redundant power supply from day one	The management appliance should have 2 x 1G port.		Already Clarified above
		14	The centralized management platform must not have any limit in terms of handling logs per day	The centralized management platform must have minimum 100 GB limit in terms of handling logs per day		Already Clarified above
	FIRM-18:		Network Bulls Pvt. Ltd.	Debulina Biswas: debulina.b@networkbulls.org		
		Clouse no	Existing	Changes Required	Remarks	
			SOR-C-ii -UTM			
		6	UTM/NGFW appliance should have at least 32 GB RAM or higher	UTM/NGFW appliance should have at least 16 GB RAM or higher	Every OEM has their own architecture to achive desire throughput. Proprietary/Costomised based solution is used to radically boost the performance and scalability to enable the fastest network security appliance available. Hence request you to reduce the RAM to 16 GB.	Already Clarified above
		10	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one		Already Clarified above
		35	The IPS system should have at least 25,000 signatures with support for custom IPS signatures	The IPS system should have at least 10,000 signatures with support for custom IPS signatures	This is specific to single OEM.	Already Clarified above
			SOR-C –iii - Firewall Manager			
		3	The management appliance should have 2 x 1G port and integrated redundant power supply from day one	The management appliance should have 2 x 1G port.	Management appliance is passive device, redundent power supply will increasing the overall budget of the project.	Already Clarified above
		14	The centralized management platform must not have any limit in terms of handling logs per day	The centralized management platform must have minimum 100 GB limit in terms of handling logs per day	There should be some number for handing log per day this will help in term of sizing the suitable appliance. Requesting you kindly revise it to " The centralized management platform must not have 100 GB limit in terms of handling logs per day"	Already Clarified above
	FIRM-19:		Symantec Software India Pvt. Ltd.	Himanshu Tyagi: Himanshu_Tyagi@symantec.com		
SN	Section No.	Point No.	Content of RFP requiring clarifications		Points of clarification required	
1	Chapter 2	SOR -D (i)	Commercial SOC includes software components SIEM Inncident forensic and packet capture.		Please confirm whether department is looking for different OEM solution for SIEM and Incident forensic & packet capture. We request department to bifurcate the quantity for the same in BoQ format.	Refer Corrigendum-II
2	SOR-D-ii&iii	31	Solution must provide to create classify applications which are attempting network access, and block unauthorized connections and data transfers by malicious programs.		We request department to remove this clause.	Already Clarified above
3	SOR-D-ii&iii	36	After development of signatures for logs submitted for a suspicious system, analysis report must be submitted to RailTel. The Analysis report should contain IP address of the system, List of files found suspicious in the submitted log		We request department to remove this clause.	Already Clarified above
4	SOR-D-ii&iii	40	Solution must provide to send endpoint logs based on IP and MAC address automatically up to CMAS.		We request department to remove this clause.	Refer Corrigendum-II
5	SOR-D-ii&iii	46	Solution must provide a Utility program for all supported Windows, Linux and MAC operating systems for collecting logs of infected endpoints for analyzing and developing signatures.		We request department to remove this clause.	Already Clarified above
6	SOR-D-ii&iii	47	OEM/bidder must provide RCA (Root Cause Analysis) report of technical problem/ incidence / issues reported and resolved.		Is department looking for Premium Support of OEM. As OEM provide RCA only in premium support not traditional 24X7 support.	Refer Corrigendum-II

7	SOR-D-ii&iii	56	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers or provide attack prevention using the least privilege containment approach		We request department to remove NIPS	Already Clarified above
8	SOR-D-i-SOC	21	Proposed solution should Integrate with On Premise Malware Sandbox Analytics solution. Security analytics should be able submit files for detonation and analysis.The ATP solution must be able to submit files for sandbox.		We request department to confirm which sandbox solution do they have and it should integrate with other OEM's solution.	Already Clarified above
9	SOR-D-i-SOC	27	The Solution must maintain the integrity while sending SSL traffic		We request department to please remove the clause, as this will require a separate SSL Solution.	As per RFP
10	SOR-D-i-SOC	28	Solution must support provision to implement custom environment.		We request department to please remove the clause, as this will require a separate SSL Solution.	Already Clarified above
11	SOR-D-i-SOC	32	Security Analytics should be proposed with required SSL visibility solution to enable meticulous network forensics and monitoring across all network traffic, thousands of applications, dozens of file transports, all flows, and all packets—including encrypted traffic. Should provide total visibility into network traffic with actionable intelligence so that department can quickly shut down exposure and mitigate ongoing risk. Should provide: • Detailed insights from all forensic captures • Establish policies to selectively decrypt SSL traffic • Share encrypted traffic insight with your security applications		We request department to please remove the clause, as this will require a separate SSL Solution.	As per RFP
12	SOR-D-i-SOC	33	Solution must support automatic visibility and interpretation of SSL decrypted traffic regardless of port or protocol. SSL decryption should be provided through the dedicated purpose built appliance based. There has to be integration with SSL decryption and security analytics solution.		We request department to please remove the clause, as this will require a separate SSL Solution.	As per RFP
13	SOR-D-i-SOC	34	The solution provided for SSL decryption must support 78+ Ciphers and TLS 1.3. The packet capyure tool and SSLVA must be from same OEM.		We request department to please remove the clause, as this will require a separate SSL Solution.	Refer Corrigendum-II

14	SOR-D-ii&iii		Anti Virus + EDR (Client & Server)		We believe that EDR requirement is not coming clearly in the specifications. Hence request you to please consider the following EDR requirements to be added in specifications. 1) The proposed solution platform must be able to integrate with the proposed endpoint protection solution deployed within the current environment and should be from same OEM to provide remediation and removal of malware on infected devices. It should happen without additional agent. 2) Solution should automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware. 3) Solution should use a stateful attack analysis to detect the entire infection lifecycle. It should trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols, leading to data exfiltration. 4) Proposed solution should have the ability to Hunt for threats by searching for indicators of compromise across all endpoints in real-time. 5) Proposed solution should ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint	Already Clarified above
15	SOR-D-i&iii		Anti Virus + EDR (Client & Server)		We understand that department is looking for some server security solution like HIPS as there are mention of the same in specifications. However those specifications are not making the requirment of HIPS very clear. Hence we request department to consider below points in specifications if requirement is for HIPS. 1) The solution should provide for the prevention of access to application data files. 2) The solution restrict data being written to an external device. 3) The solution should implement memory controls by default between processes. 4) Server Security solution should have application and device control to lock down configuration settings, file systems, and use of removable media. 5) Server Security solution should provide predefined automated responses to events.Actions should include alerting the administrator, disabling the user account, logging the event and executing commands/scripts/programs. Solution should have Alerting via file output. 6) HIPS should perform log analysis, integrity checking, root kit detection, time-based alerting and active response. It should help to	Already Clarified above
	FIRM-20:		IBM India Pvt. Ltd.	Mayank Devlal: madevlal@in.ibm.com		
SN	Section	Page No	Clause	Clarification Required	Remarks	
1	SCHEDULE OF REQUIREMENT	5	Commercial SOC includes software components SIEM, Incident forensic and packet capture.	Since Quantity is mentioned as 1, Please clarify 1) if SIEM needs to be deployed in HA in DC ? 2) If DR is to be considered for SIEM instance?		Already Clarified above

2	SCHEDULE OF REQUIREMENT	29	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000.	Please suggest if proposed hardware should support 80000 EPS scalability without further hardware expansion. Also, kindly confirm the flow/sec scalability. We suggest to have following clause - The proposed solution should be able to handle 10,000 EPS& 5000 Flows/sec from day one and should be scalable to handle 40,000 EPS & 10,000 FPS on the same hardware and solution should be horizontally scalable to 80,000 EPS by adding additional hardware.		Already Clarified above
3	SCHEDULE OF REQUIREMENT	29	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000.	Kindly confirm the log sources locations so as to size collectors for the same.		Already Clarified above
4	Detailed Technical Specifications	30	The Bidder will give the hardware sizing for the EPS count required if solution is software based.	We understand bidder doesn't need to provision hardware for software based solution. Pls confirm.		Already Clarified above
5	Detailed Technical Specifications	30	The Bidder will give the hardware sizing for the EPS count required if solution is software based.	Kindly confirm the log & flow retention policy(online & offline) so as to suggest on storage requirements.		Already Clarified above
6	Detailed Technical Specifications	31	The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	Kindly confirm if solution needs to be deployed in high availability at all the layers ?		Already Clarified above
7	Detailed Technical Specifications	32	The solution must easily expand to support additional demand.	Kindly clarify additional demand if this is w.r.t additional EPS/log sources integration.		Already Clarified above
8	Detailed Technical Specifications	32	The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data	We suggest to modify this clause to read as " The solution should be able to support integrity of the indexed data" since most of the SIEM players doesn't support digitial signatures.		Already Clarified above
9	Detailed Technical Specifications	32	The solution must monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more.	We suggest to modify this clause to read as "The solution must monitors its own configurations and usage to maintain a complete, audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more." since most of the SIEM players doesn't suport digital signautr		As per RFP
10	Detailed Technical Specifications	32	The solution must support Disaster Recovery.It should have the provision to run in active / passive mode in a DC-DR environment and should be able to failover to automatically DR in case of a primary failure.	Kindly confirm if solution needs to be deployed in DR as well. Also, will this DR be in Active/Passive Mode. Incase of passive DR, kindly confirm the RTO/RPO to adhere.		Already Clarified above
11	Detailed Technical Specifications	41	Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident	Please confirm the number of locations & interfaces to be captured for packet capture.		Already Clarified above
12	Detailed Technical Specifications	42	Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints via single agent EDR and Anti-virus solution.The AV and EDR must be from same OEM. Provided AV must be in leaders Gartner Quadrant.	We suggest to read this clause as "Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints "		Already Clarified above
13	Detailed Technical Specifications	42	Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.	We recommend to have appliance based solution for packet analysis. We suggest to have software based solution for storing pcap and session reconstruction.		Already Clarified above

14	Detailed Technical Specifications	42	Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.	Kindly confirm following for sizing the packet solution - 1) No of locations/interfaces including DC & DR for packet data collection 2) Link & current bandwidth utilization details for each interface/location to be cpatured 3) Retention policy to be considered for raw & meta data retention.		Already Clarified above
15	Detailed Technical Specifications	42	Should capture signature/heuristics and behavioral based alerts and block the malicious activity	We suggest to remove this clause since Packet capture solutions are not supposed to block the activity		Already Clarified above
16	Detailed Technical Specifications	42	Solution must support provision to implement custom environment.	Kindly provide with the expectations.		Already Clarified above
17	Detailed Technical Specifications	42	The solution should be able to provide suggested mitigation actions for events	Clause mentioned are applicable to SOAR platform hence we suggest to remove this clause from packet capture.		Already Clarified above
18	Detailed Technical Specifications	42	Proposed solution should Integrate with On Premise Malware Sandbox Analytics solution. Security analytics should be able submit files for detonation and analysis.The ATP solution must be able to submit files for sandbox.	We suggest to remove "The ATP solution must be able to submit files for sandbox." from the mentioned clause since packet capture & ATP solution are different.		Already Clarified above
19	Detailed Technical Specifications	42	Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years	We suggest to remove this clause since this clause is not applicable to Packet Capture solution.		Already Clarified above
20	Detailed Technical Specifications	35	"The solution should include following native visualizations: Tables Time charts Line charts Bar charts Area charts Pie charts Scatterplot charts Radial, filler, and marker gauges Geo-IP maps"	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
21	Detailed Technical Specifications	35	The solution should have the ability to convert dashboards into PDF files and schedule them to be emailed to others.	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
22	Detailed Technical Specifications	35	The solution should have the ability to integrate with external visualization frameworks and options (D3, Tableau, etc) for additional visualizations	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
23	Detailed Technical Specifications	36	Dashboard should support export of data to multiple formats including CSV, Excel, PDF	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
24	Detailed Technical Specifications	36	The solution must offers multiple SDKs written on top of the API for: Python Java JavaScript PHP Ruby C#	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above

25	Detailed Technical Specifications	36	The solution must assist in following use cases due to indexed data leading to a high ROI and cross-department collaboration. Compliance Fraud IT Operations Application Management Web/Digital Intelligence Business Analytics Industrial Data and Internet of Things	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
26	Detailed Technical Specifications	38	The solution must be able to do full-text search on any field in the indexed data based on: Keywords Time ranges Specific or relative time windows down to the month/day/minute/second Boolean logic (and, or, not, etc) Regular expressions Wild card syntax Statistical analysis including: Count of occurrences, distinct count of occurrences, sum Most common values or least common values of a field Minimum, maximum Average, mean, mode, median Standard deviation, variance The identification of anomalous values in results that may be irregular, or uncommon The statistical correlation between fields Clustering of events together based on their similarity to each other as a single event Truncate outlying numerical values in selected fields to assist in statistical correlation First and last seen value Percentile Predicted values (search that looks at historical data to mathematically predict future values) Perform a union, diff, or intersection of individual or multiple	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
27	Detailed Technical Specifications	38	The solution must be able to do baselining and then apply the above search logic to find outlier/anomalies from the baseline that may be advanced, non-signature based threats	This seems to be specific OEM clause hence we request to remove this clause		Already Clarified above
Fir				Shishir Jain: <Shishir.Jain@rsa.com		
		Page no.	Clause/ Content in the RFP	Clarification sought/ Change Request		
		30	4. The solution must support auto discovery of assets that are being protected or monitored and automatically start accepting events without any administrator intervention through an agent less solution	The 'auto discovery of assets' is additional feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		Already Clarified above
		30	5 The solution should support automated classification of assets that are being protected.	Please elaborate on 'classification of assets that are being protected', this seems value add feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		Already Clarified above
		31	6. The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	Building high availability at different components is design aspect, it is not necessary the product must have it as embedded fashion. This again an OEM specific product feature, request you to modify this as "the proposed SIEM solution must provide high availability at all layers including collection, normalization, correlation and management with the need for additional 3rd party software"		Already Clarified above

		31	6. The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.	The "support high availability" is just a capability to be present in the solution, but Railtail want the bidder to provide SIEM solution with high availability or stand-alone solution so that HA capability may be leveraged in future ?		Already Clarified above
		31	13. The solution must maintain an externally accessible store or database of all assets discovered on the network. This asset data should include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database.	Scanning IT infra, discovering assets and maintaining inventory are features of "Asset Management Software" tools and may be value add feature of specific SIEM OEM but not a general SIEM functionality. Hence this clause must be removed from the RFP		As per RFP
		32	2 The system must provide Real-time remote indexing of data to minimize the opportunity for alteration of audit trails on compromised hosts	Every SIEM Product have its way to manage the data integrity for the logs collected in real-time and near-real time. This clause is specific feature of OEM Product, hence please remove this or change this to "the system must perform indexing for real-time data and maintain data integrity check for both index and processed in a remote location for future audit and compliance purposes"		As per RFP
			4 The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data			
			5 The solution must provide event hashing at index time to determine at search time if events have been tampered with			
			6 The solution must monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more.			
		32	4 The solution must support industry log collection methods (syslog-UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195),DNS,DHCP, WMI, JDBC, XML,CSV,JSON,SNMP, Checkpoint LEA,FTP,S/FTP, ODBC, SDEE, Window event logs-agent based and agent less etc., mail server, web server),directly pointing to log files over the network or on the indexer,Custom inputs which includes scripted and modular inputs, vendor supplied universal agents.	While the support of log collection methods is standard ask, but for exporting of offline log data or custom data may be supported differently by each SIEM OEM. Please modify this clause to what RailTel wanted to achieve instead referring to specific product feature of a OEM SIEM.		As per RFP
		33	7 The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. E.g.: The categorization may by be HIGH, MEDIUM, LOW or color coding.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify this to as per end objective that RailTel wanted to achieve.		Already Clarified above
		34	10 The solution must support the ability to centrally deliver vulnerability reports.	Delivering vulnerability/Asset reports and dashboards is feature provided by Vulnerability/Asset Management solution, this requirement is a feature of specific to a SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP or modify as per end objective that RailTel wanted to achieve.		Already Clarified above
			11 The solution may support the ability to centrally deliver asset reports.			Already Clarified above
			27 Dashboard should display asset list and capture details including name, location, owner, value, IP address, platform details			

		36	2 The solution must offers multiple SDKs written on top of the API for:	These features apart from 'support of API for external integration' are specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify this to as per end objective that RailTel wanted to achieve.		As per RFP
			2.1. Python			
			2.2. Java			
			2.3. JavaScript			
			2.4. PHP			
			2.5. Ruby			
			2.6. C#			
			3 The solution should offers hundreds of free, public Apps for point products or use cases to create more value and accelerate time-to-value			
		37	15 The solution may provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP or modify to "the proposed SIEM must collect business context such as asset classification data and leverage in better incident prioritization and reduction of false positives" or as per end objective that RailTel wanted to achieve.		Already Clarified above
		39	7 The solution must have the ability to directly search raw data (using existing search capabilities) stored externally in Hadoop HDFS file systems and the results made available for advanced visualizations	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		Already Clarified above
		41	6 The solution must have ability to import raw data from Hadoop for indexing	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		Already Clarified above
		33	8 The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.	Please provide the retention duration for long term and also would it be offline or online retention ?		Already Clarified above
		34	10 The solution must support the ability to centrally deliver vulnerability reports.	This is an additional feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		Already Clarified above
		35	Dashboard should display asset list and capture details including name, location,owner, value, IP address, platform details	Scanning IT infra, discovering assets and maintaining inventory are features of "Asset Management Software" tools is value add feature of specific SIEM OEM but not a general SIEM functionality, hence this clause must be removed from the RFP		Already Clarified above
		42	1 Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident	Please provide how no of network points at each location and their link bandwidth to be covered by full packet capture solution		Clarification: No. of interface is mentioned in the RFP
			6 Solution should be sized for traffic rate of 1Gbps or higher.			
		42	12 Should provide Regeneration and Playback functionality: Ability to create shadow networks. Regeneration and Playback: Point and click to instantly regenerate traffic (at configurable speeds) to a chosen NIC on a shadow network for further analysis in 3rd party systems. Without interruption of regular services.	This is feature is specific to a SIEM OEM not general functionality of SIEM, hence remove this clause from RFP		Already Clarified above
		43	19 Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years	The purpose of EDR solution is to detect malicious software/activities on the endpoint which can't be detected by AV solution deployed on the same. When these two products are from same OEM, it wont be of benefit (depth in defense).		As per RFP
		42	26 Solution must perform flow generation and analysis and must perform aggregation of all traffic pertaining to single session with a single flow records.	This is feature is specific to a SIEM OEM not general functionality of SIEM, there is not a much value of flow data when there Deep Packet Inspecting in place with Packet Capture. Hence remove this clause from RFP		Already Clarified above

		43	34 The solution provided for SSL decryption must support 78+ Ciphers and TLS 1.3. The packet capyure tool and SSLVA must be from same OEM.	Please explain why is that SSL decryption must from the same OEM that supplies Packet Capture? Not every DPI/Packet Capture OEM is not into SSL decryption products, and this may be true for specific OEM. Therefore request you allow the bidder to support Packet Capture and SSL decryption from different OEMs.		Already Clarified above
	Additional Points Changed					
			Existing Clause			
			The solution should have capability to integrate with SIEM to have unified visibility.			Refer Corrigendum-II