TENDER NIT NO: TPSODL/OT/2022-23/063

Sr.No	Subject/Description, Page number	Original RFP Clause	Query sought / Suggestion from the bidder/OEM	TPSODL Response
1	1.7 Qualification Criteria, Page 6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors Organizations in India (PO copies to be attached)	Proposed SIEM solution must have been offered in atleast 1 Power Sector organization in India (PO /Completion Cert/ Any other document in support to be attached) Justification- Power, Oil and Gas are equally critical sectors and a PQ in any one should meet your similar Indusrty experience requirement	Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies/completion certificates to be attached)
2	1.7 Qualification Criteria, Page 6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	OEM should be in Gartner's Leader Quadrant for SIEM in any one of the last 3 reports. Justification-Most of the OEM' in leader' quadrant in lastest report of Gartner are new entrants in India and will not meet required Industry experience by you. Moreover the latest report of Gartner has done the evaluation basis cloud offerings ,Where as your requirement of SIEM and soar is on premise .	OEM should be in Gartner's Quadrant for SIEM in latest report
3	Technical Specification, Pt 27, Page 19	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.	Justification : In the RFP Network Forensic is considered as a part of the SIEM Functionality however there is no Specification related to the SOW of Data Forensics we suggest to add Data Forensic in terms of Deep Packet Inspection as log Inspection is already covered, however log information is not suffice for forensics, Most of the SOC RFP does include log and packet capture for complete visibility at all layers of the OSI stack (Layer 2-7)	no change
4		**Additional Clause**	The collectors should be able to store/retain both normalized & raw data (Logs and Packets)for forensic purposes, should support throughput upto 100 Mbps for incoming & outgoing data through Internet, Solution should store RAW packet DATA for 7 days and normalized packet data for 15 days for forensics	NA
5		**Additional Clause**	Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data should support session and application reconstruction.	NA
6		**Additional Clause**	SIEM Should have single GUI for Logs and Packet data for quick response	NA
7		**Additional Clause**	Solution should have the ability to convert traffic from raw packets to meaningful arti facts like email, FTP data files, and VoIP conversations including PHP, JavaScript.	NA
8	Qualification Criteria (Sl No.3) Page No.6	OEM should have presence in INDIA for last 8 years.	With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY, Kindly requesting to Exempt startups or by Amending this clause as "OEM should have presence in INDIA for last 3 years". In addition to the exception, Kindly requesting you to add preference for Make In India Solutions.	no change
9	Qualification Criteria (Sl No.5) Page No.6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors Gov.Organizations in India (PO copies to be attached)	Kindly requesting to Amend this clause as "Proposed SIEM solution must have been offered in atleast 2 Organisation in which one should be in Power Sector Gov.organization in India.	Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies/completion certificates to be attached)
10	Qualification Criteria (Sl No.6) Page No.6	Proposed SIEM solution should be in Gartner since last 5 years	With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY Point No.8:-**In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order.** Kindly requesting to Provide waive off for this clause for Startups who are technically fully compliant.	Proposed SIEM solution should be in Gartner last 3 years.
11	Qualification Criteria (Sl No.7) Page No.6 & Annexure-II-Technical Specification (Sl No.9) Page No.17	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30000 EPS from any Government of India organizations)	Kindly Requesting to Amend this clause as "Proposed SIEM solution must have atleast 3 deployments for more than 10,000 EPS in Govt of India organizations. (Atleast 2 sign-off copies/Purchase Order/Implementation Letter must be provided for more than 10000 EPS from any Government of India organizations)	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)
12	Qualification Criteria (Sl No.8) Page No.6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY Point No.8:-**In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order.** Kindly requesting to Provide waive off for this clause for Startups who are technically fully compliant.	OEM should be in Gartner's Quadrant for SIEM in latest report
13	1.1 EMD, Page no-4	Rs.2,00,000/- for Other State MSME Registered Bidder.	As per Govt. Guideline all MSME Vendors are eligible for 50% on EMD or Waiver, Kindly request change this Clause.	As per tender 9.4 Preferential norms for procurement from MSMEs registered in the State of Odisha "iv. Earnest Money Deposit (EMD) - EMD shall be exempted for MSME registered in the State of Odisha. However, Bidder shall be barred to participate in the tendering process for a period of 2 years in case it backs out post award of the contract." Your company is not registered as MSME in the state of Odisha so Kindly submit the EMD.
14	8. Qualification Criteria, Page no-6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	TPSODL has already asked for presence of OEM in Gartner as per point.no 6 of this section. So asking presence especially in this year's Gartner leader quadrant will limit the participation to a minimum vendors and also will take away the opportunity from many other vendors to participate in this bid, **We would request you to delete this clause.**	OEM should be in Gartner's Quadrant for SIEM in latest report
15	7.3 Payment Terms: , Page no-13	Post submission of an error-free and verified invoice (s) from EIC, payment shall be released within 45 days.	Being MSME we request you, the payment shall be released within 30 days against successful delivery and acceptance of Material.	As per Tender
16	Page no-6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors organizations in India (PO copies to be attached)	Remove this point	Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies/completion certificates to be attached)

17	Page no-6	Proposed SIEM solution should be in Gartner since last 5 years	Proposed SIEM solution should be in Gartner last 3 years.	Proposed SIEM solution should be in Gartner last 3 years.
18	Page no-6	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30000 EPS from any Government of India organizations)	Remove this point	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)
19	Page no-6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	Remove this point	OEM should be in Gartner's Quadrant for SIEM in latest report
20	1.7 Qualification Criteria, Page 6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors Gorganizations in India (PO copies to be attached)	Proposed SIEM solution must have been offered in atleast 1 Power Sector organization in India (PO /Completion Cert/ Any other document in support to be attached) Justification- Power, Oil and Gas are equally critical sectors and a PQ in any one should meet your similar Indusrty experience requirement	**Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies to be attached)**
21	1.7 Qualification Criteria, Page 6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	OEM should be in Gartner's Leader Quadrant for SIEM in any one of the last 3 reports. Justification-Most of the OEM' in leader' quadrant in lastest report of Gartner are new entrants in India and will not meet required Industry experience by you. Moreover the latest report of Gartner has done the evaluation basis cloud offerings ,Where as your requirement of SIEM and soar is on premise .	**OEM should be in Gartner's Quadrant for SIEM in latest report**
22	Technical Specification, Pt 27, Page 19	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.	Justification : In the RFP Network Forensic is considered as a part of the SIEM Functionality however there is no Specification related to the SOW of Data Forensics we suggest to add Data Forensic in terms of Deep Packet Inspection as log Inspection is already covered, however log information is not suffice for forensics, Most of the SOC RFP does include log and packet capture for complete visibility at all layers of the OSI stack (Layer 2-7)	**no change**
23		**Additional Clause**	The collectors should be able to store/retain both normalized & raw data (Logs and Packets)for forensic purposes, should support throughput upto 100 Mbps for incoming & outgoing data through Internet, Solution should store RAW packet DATA for 7 days and normalized packet data for 15 days for forensics	**na**
24		**Additional Clause**	Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data should support session and application reconstruction.	**na**
25		**Additional Clause**	SIEM Should have single GUI for Logs and Packet data for quick response	**na**
26		**Additional Clause**	Solution should have the ability to convert traffic from raw packets to meaningful arti facts like email, FTP data files, and VoIP conversations including PHP, JavaScript.	**na**
27	ANNEXURE-II Technical Specification Page no.17	The SIEM Solution should support security data lake concept for future scalability and expansion perspective	The majority of SIEM solutions have their own databases and do not use a single database for SIEM. Please relax this point	**no change**
28	ANNEXURE-II Technical Specification Page no.17	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30000 EPS from any Government of India organizations)	Kindly Clarify if Govenment PSU reference work for this point.	**Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)**
29		Date of submission extended	Please extend the date of submission to 3 weeks	As per Tender
30	1.7 Qualification Criteria, Page 6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors organizations in India (PO copies to be attached)	Kindly Amend this term as OEM like IBM don't share Purchase Order due to NDA as applicable.Request Tenderer to ask for equivalent coponent to share experience in Power Sectors	**Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies/Completion certification to be attached)**
31	1.7 Qualification Criteria, Page 6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors Gorganizations in India (PO copies to be attached)	Proposed SIEM solution must have been offered in atleast 1 Power Sector organization in India (PO /Completion Cert/ Any other document in support to be attached) Justification- Power, Oil and Gas are equally critical sectors and a PQ in any one should meet your similar Indusrty experience requirement	Proposed SIEM/OEM solution must have been offered in atleast 2 Power/gas/oil/ Sectors Gorganizations in India (PO copies/completion certificates to be attached)
32	1.7 Qualification Criteria, Page 6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	OEM should be in Gartner's Leader Quadrant for SIEM in any one of the last 3 reports. Justification-Most of the OEM' in leader' quadrant in lastest report of Gartner are new entrants in India and will not meet required Industry experience by you. Moreover the latest report of Gartner has done the evaluation basis cloud offerings ,Where as your requirement of SIEM and soar is on premise .	OEM should be in Gartner's Quadrant for SIEM in latest report
33	Technical Specification, Pt 27, Page 19	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.	Justification : In the RFP Network Forensic is considered as a part of the SIEM Functionality however there is no Specification related to the SOW of Data Forensics we suggest to add Data Forensic in terms of Deep Packet Inspection as log Inspection is already covered, however log information is not suffice for forensics, Most of the SOC RFP does include log and packet capture for complete visibility at all layers of the OSI stack (Layer 2-7)	no change
34		**Additional Clause**	The collectors should be able to store/retain both normalized & raw data (Logs and Packets)for forensic purposes, should support throughput upto 100 Mbps for incoming & outgoing data through Internet, Solution should store RAW packet DATA for 7 days and normalized packet data for 15 days for forensics	NA
35		**Additional Clause**	Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data should support session and application reconstruction.	NA
36		**Additional Clause**	SIEM Should have single GUI for Logs and Packet data for quick response	NA
37		**Additional Clause**	Solution should have the ability to convert traffic from raw packets to meaningful arti facts like email, FTP data files, and VoIP conversations including PHP, JavaScript.	NA
38	Page no-6	Proposed SIEM solution must have been offered in atleast 2 Power Sectors Gorganizations in India (PO copies to be attached)	Remove this point	Proposed SIEM/OEM solution must have been offered in atleast 1 Power/gas/oil/ Sectors Gorganizations in India (PO copies to be attached)
39	Page no-6	Proposed SIEM solution should be in Gartner since last 5 years	Proposed SIEM solution should be in Gartner last 3 years.	Proposed SIEM solution should be in Gartner last 3 years.
40	Page no-6	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30000 EPS from any Government of India organizations)	Remove this point	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)

41	Page no-6	OEM should be in Gartner's Leader Quadrant for SIEM in latest report	Remove this point	OEM should be in Gartner's Quadrant for SIEM in latest report

TENDER NIT NO: TPSODL/OT/2022-23/063

Sl No.	RFP Clause	Change Request	TPSODL Response
1	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities accessible within single User Interface.	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and capability to take wider range of action. The SIEM should have capability to adhoc execute FortiSOAR Playbooks and Connectors from the INCIDENTS page for individual incidents.	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities accessible .
2	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.		
3	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources	**The SIEM Solution should be EPS based at both log management and Correlation layer.**	**no change**
4	The SIEM solution support high availability feature and should be proposed in HA mode for all layers at DC	The SIEM solution support high availability feature and should be proposed in HA mode.	no change
5	The SIEM Solution should support security data lake concept for future scalability and expansion perspective.	The SIEM solution should support future scalability and expansion.	agreed
6	The SIEM solution shouild be based on open architecture so that it can be used to feed data to 3rd party analytic solutions		
7	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to be available across all tier to filter out logs as wherever required.	**Remove this point**	**no change**
8	SIEM solution should be based on open architecture so that it can be used to feed data to 3rd party analytic solutions i.e. Solution should support standard CEF or equivalent technology which is accepted globally not the proprietary one.		
9	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Remove this point	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)
10	Proposed solution's OEM must have its presence in India including development center and support centre. Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage	Proposed solution's OEM must have its presence in India including support centre. Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage	agreed
11	Solution must be agentless and should not require any agents to integrate with end devices		
12	SIEM solution must support OOB of the box integration with well known technologies e.g. firewall, AD, Switches, routers, TI etc. for creating response to an incidence		
13	Should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec,Netflow . Collectors must support integration with N Flow, Jflow	Should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, **ODBC/JDBC**, FTP, Windows Event Logging Protocol, Opsec,Netflow . Collectors must support integration with N Flow, Jflow	Agreed(Its should support oracle DB and SQL DB)
14	The solution should have connectors to support the listed devices / applications. In case device is not supported out of box it must have GUI Based SDK kit to create Parsers.		
15	Solution should consist Un-obfuscated parsers natively available with log connector to modify existing parser as when required by security operations team.		
16	All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission. No performance deggration should happen		
17	The solution should have the capability to compress the logs by at least 80 % for storage optimization.	The solution should have the capability to compress the logs for storage optimization.	no change
18	The proposed solution should have capability to provide centrally or remotely log collector installation to integrate event sources. This is to ensure to reduce time of implementation as well as any changes to be made later through single click push from central site.		
19	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system. License count should be performed post filtering of logs.	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system.	
20	Caching & Batching: The proposed solution must support local caching and batching and batching at collection level in case of connectivity failures	The proposed solution must support local buffer at collector level in case of connectivity failures.	
21	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		
22	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events		
23	The solution should be able to store both normalized and RAW logs		
24	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users		
25	Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	Solution should have the ability to perform searches for events, incidents, rules and other parameters.	
26	Proposed solution should support searching of Data/artifacts associated with historical incidents.		
27	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.		
28	The solution should have the capability to identify / remember frequently used queries		
29	The solution should include compliance reports for standard - ISO 27001/02. The solution should also generate reports for these standards		

30	The solution must provide near-real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis	The solution must provide near-real-time analysis of events.	
31	The proposed solution must have search criteria to be saved as dashboard or reports.		
32	Solution must support searching and reporting of logs at logging layer with machine learning capabilities.		
33	Proposed solution should support predictive analyis (data science enabled) by creating custom data models in log reporting.	Proposed solution should support creation of custom data models in log reporting.	
34	Proposed solution should have data science engine that enables users to perform predictive analysis by allowing adding additional variables and columns to report for further scrutiny.		
35	Solution should have 6 month's online and 1 year offline storage.		
36	It must have auto archive feature to archive logs on secondary storage from offline storage perspective. (I.e NAS/DAS/NLSAS)		
37	All logs must get auto archived on centralized storage directly from Log management layer and archived logs must be readable from archival/ central storage directly		
Licensing			
	Proposed SIEM & SOAR solution should be perpetual software based solution. To deploy the proposed Software based SIEM & SOAR, the HW, OS and Storage related configuration details should be submitted over OEM letterhead and same would be provisioned by TataPower.		
	SIEM Solution should be proposed for 7500 Sustained EPS and 15000 Peak EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of suddden rise in EPS during any unwanted situation (eg. Cyber-attack). Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	SIEM Solution should be proposed for 7500 Sustained EPS and 15000 Peak EPS from Day 1. Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	no change
	No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.	Remove this point	no change
	SOAR solution can be from same or different OEM, however there should be out of the box integration avialble between both SIEM & SOAR. The SOAR solution shall be licensed for atleast 15 analysts		
	Solution shall be able to ingest Threat Intel feeds from both SIEM OEM (in-built feeds) & also third party (open source feeds) SIEM - Correlation & Advance Use Cases, Threat Intelligence Feeds		
	The system/solution should have the ability to correlate all the fields in a log		
	The proposed system should have the real-time correlation capability. The system should be updated with customizable correlation rules based on new identified attack patterns and threats. It must be possible to create Customized co relation rules.		
	The system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.		
	The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.		
	The event should reach the SOC monitoring team in near real-time of the log being captured		
	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports.		
	All the dashboards for SIEM monitoring should be completely customizable and shall have the feature for restricted access depending on user / group based. Dashboard should be hosted at DC premises.		
	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Behavioral based, Risk based etc.	no change
	Solution should have capability to detect identity breaches and threats even when the account is not active		
	Solution should provide a heatmap dashboard against all use cases which are active in the system which should help to strategies the security posture.		
	SIEM solution must provide threat intelligence to enrich/correlate events collected. This TI feed must be from OEM but solution should support integration with Opensource/3rd party TI feeds as well.		
	Solution should provide Threat Intel platform from same OEM and provides but not limited to 1. Threats view with monetary impact 2. Threats by business vertical 3. Threat bulletins 4. Guides and reports 5. Content specific to threat Intel Feed 6. Threats by Geography etc.		
	Solution should have ability to gather information on real time threats and zero day attacks issued by anti-virus or NGFW vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds		
	SIEM platform must support MITRE For threat intelligence.		
	Solution must support integration with 3rd party VA solutions that provides the Vulnerability database information such as Nessus, Rapid7 etc.		
	SIEM solution must support API integration with 3rd party solutions.		
	SIEM solution must provide built in ticketing system to track incident from creation to closure, provide reports on pending incidents and permit upload of related evidences such as screenshots etc at the Incident management tool manually. Also it should be able to integrate with 3rd party ticketing tools.		
	The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.		
	The solution should be capable monitoring user suspicious activites and providing but not limited to following use cases 1. User activity monitoring 2. Suspicious activity monitoring 3. Privileged use monitoring etc.		
	Solution must support detection of zero day attacks and must leverage MITRE Attack framework to provide full visibility/detection of various attacks.		

	Solution must leverage MITRE Att&ck framework to provide full visibilty/detection of various attacks.		
	SIEM solution must provide machine learning capability to detect anomalies.		
	SOAR - Security Orchestration and Automated Response		
	SOAR must be integrated platform with SIEM on same user interface	SOAR must be able to integrated with SIEM on same user interface	agreed
	SOAR solution must provide MTTR and MTTD reports/dashboards.		
	Solution should have security orchestration and automated response engine bi-directionally integrated to reduce security incident MTTR (Mean Time To Respond) and automate L1/L2 security activities.		
	SOAR solution must support automation and response by OOB readily available playbooks (auto and semi), but at the same time there should be scope to customize and create new playbooks		
	SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources as well.		
	SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner.		
	Proposed SOAR technology should have Threat intel platform inbuilt with OEM threat intel		
	The solution should provide option to manually invoke selected playbook based on any selected or set of selected events.		
	Services		
	OEM should be part of SIEM & SOAR deployment (atleast 20% efforts should be from OEM including architecture design, governance, training etc)		

TENDER NIT NO: TPSODL/OT/2022-23/063

Technical Specification

Sl No.	RFP Clause	Change Request	TPSODL Response
	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities accessible within single User Interface.	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and capability to take wider range of action. The SIEM should have capability to adhoc execute FortiSOAR Playbooks and Connectors from the INCIDENTS page for individual incidents.	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities accessible .
	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.		
	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources	**The SIEM Solution should be EPS based at both log management and Correlation layer.**	no change
	The SIEM solution support high availability feature and should be proposed in HA mode for all layers at DC	The SIEM solution support high availability feature and should be proposed in HA mode.	no change
	The SIEM Solution should support security data lake concept for future scalability and expansion perspective.	The SIEM solution should support future scalability and expansion.	agreed
	The SIEM solution shouild be based on open architecture so that it can be used to feed data to 3rd party analytic solutions		
	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to	**Remove this point**	no change
	SIEM solution should be based on open architecture so that it can be used to feed data to 3rd party analytic solutions i.e. Solution should support standard CEF or equivalent technology which is accepted globally not the proprietary one.		
	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Remove this point	Proposed SIEM solution must have atleast 3 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 15 k EPS from any Government of India organizations)
	Proposed solution's OEM must have its presence in India including development center and support centre. Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage	Proposed solution's OEM must have its presence in India including support centre. Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage	agreed
	Solution must be agentless and should not require any agents to integrate with end devices		
	SIEM solution must support OOB of the box integration with well known technologies e.g. firewall, AD, Switches, routers, TI etc. for creating response to an incidence		
	Should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec,Netflow . Collectors must support integration with N Flow, Jflow	Should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, **ODBC/JDBC**, FTP, Windows Event Logging Protocol, Opsec,Netflow . Collectors must support integration with N Flow, Jflow	Agreed(Its should support oracle DB and SQL DB)
	The solution should have connectors to support the listed devices / applications. In case device is not supported out of box it must have GUI Based SDK kit to create Parsers.		
	Solution should consist Un-obfuscated parsers natively available with log connector to modify existing parser as when required by security operations team.		
	All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission. No performance deggration should happen		
	The solution should have the capability to compress the logs by at least 80 % for storage optimization.	The solution should have the capability to compress the logs for storage optimization.	no change
	The proposed solution should have capability to provide centrally or remotely log collector installation to integrate event sources. This is to ensure to reduce time of implementation as well as any changes to be made later through single click push from central site.		
	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system. License count should be performed post filtering of logs.	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system.	no change
	Caching & Batching: The proposed solution must support local caching and batching and batching at collection level in case of connectivity failures	The proposed solution must support local buffer at collector level in case of connectivity failures.	no change
	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		

	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events		
	The solution should be able to store both normalized and RAW logs		
	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users		

	Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	Solution should have the ability to perform searches for events, incidents, rules and other parameters.	no change
	Proposed solution should support searching of Data/artifacts associated with historical incidents.		
	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.		
	The solution should have the capability to identify / remember frequently used queries		
	The solution should include compliance reports for standard - ISO 27001/02. The solution should also generate reports for these standards		
	The solution must provide near-real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis	The solution must provide near-real-time analysis of events.	no change
	The proposed solution must have search criteria to be saved as dashboard or reports.		
	Solution must support searching and reporting of logs at logging layer with machine learning capabilities.		
	Proposed solution should support predictive analyis (data science enabled) by creating custom data models in log reporting.	Proposed solution should support creation of custom data models in log reporting.	no change
	Proposed solution should have data science engine that enables users to perform predictive analysis by allowing adding additional variables and columns to report for further scrutiny.		
	Solution should have 6 month's online and 1 year offline storage.		
	It must have auto archive feature to archive logs on secondary storage from offline storage perspective. (I.e NAS/DAS/NLSAS)		
	All logs must get auto archived on centralized storage directly from Log management layer and archived logs must be readable from archival/ central storage directly		
Licensing			
	Proposed SIEM & SOAR solution should be perpetual software based solution. To deploy the proposed Software based SIEM & SOAR, the HW, OS and Storage related configuration details should be submitted over OEM letterhead and same would be provisioned by TataPower.		
	SIEM Solution should be proposed for 7500 Sustained EPS and 15000 Peak EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of suddden rise in EPS during any unwanted situation (eg. Cyber-attack). Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	SIEM Solution should be proposed for 7500 Sustained EPS and 15000 Peak EPS from Day 1. Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	no change
	No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and	Remove this point	no change
	SOAR solution can be from same or different OEM, however there should be out of the box integration avialble between both SIEM & SOAR. The SOAR solution shall be licensed for atleast 15 analysts		

	Solution shall be able to ingest Threat Intel feeds from both SIEM OEM (in-built feeds) & also third party (open source feeds) SIEM - Correlation & Advance Use Cases, Threat Intelligence Feeds		
	The system/solution should have the ability to correlate all the fields in a log		
	The proposed system should have the real-time correlation capability. The system should be updated with customizable correlation rules based on new identified attack patterns and threats. It must be possible to create Customized co relation rules.		
	The system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.		
	The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.		
	The event should reach the SOC monitoring team in near real-time of the log being Captured		
	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports.		
	All the dashboards for SIEM monitoring should be completely customizable and shall have the feature for restricted access depending on user / group based. Dashboard should be hosted at DC premises.		
	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Behavioral based, Risk based etc.	no change
	Solution should have capability to detect identity breaches and threats even when the account is not active		
	Solution should provide a heatmap dashboard against all use cases which are active in the system which should help to strategies the security posture.		
	SIEM solution must provide threat intelligence to enrich/correlate events collected. This		

	TI feed must be from OEM but solution should support integration with Opensource/3rd party TI feeds as well.		
	Solution should provide Threat Intel platform from same OEM and provides but not limited to 1. Threats view with monetary impact 2. Threats by business vertical 3. Threat bulletins 4. Guides and reports 5. Content specific to threat Intel Feed 6. Threats by Geography etc.		
	Solution should have ability to gather information on real time threats and zero day attacks issued by anti-virus or NGFW vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds		
	SIEM platform must support MITRE For threat intelligence.		
	Solution must support integration with 3rd party VA solutions that provides the Vulnerability database information such as Nessus, Rapid7 etc.		
	SIEM solution must support API integration with 3rd party solutions.		

	SIEM solution must provide built in ticketing system to track incident from creation to closure, provide reports on pending incidents and permit upload of related evidences such as screenshots etc at the Incident management tool manually. Also it should be able to integrate with 3rd party ticketing tools.		
	The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.		
	The solution should be capable monitoring user suspicious activites and providing but not limited to following use cases 1. User activity monitoring 2. Suspicious activity monitoring 3. Privileged use monitoring etc.		
	Solution must support detection of zero day attacks and must leverage MITRE Attack framework to provide full visibility/detection of various attacks.		
	Solution must leverage MITRE Att&ck framework to provide full visibilty/detection of various attacks.		
	SIEM solution must provide machine learning capability to detect anomalies.		
	SOAR - Security Orchestration and Automated Response		
	SOAR must be integrated platform with SIEM on same user interface	SOAR must be able to integrated with SIEM on same user interface	agreed
	SOAR solution must provide MTTR and MTTD reports/dashboards.		
	Solution should have security orchestration and automated response engine bi-directionally integrated to reduce security incident MTTR (Mean Time To Respond) and automate L1/L2 security activities.		
	SOAR solution must support automation and response by OOB readily available playbooks (auto and semi), but at the same time there should be scope to customize and create new playbooks		
	SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources as well.		
	SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner.		
	Proposed SOAR technology should have Threat intel platform inbuilt with OEM threat intel feeds and support for both commercial and open source threat intel feeds.		
	The solution should provide option to manually invoke selected playbook based on any selected or set of selected events.		
	Services		
	OEM should be part of SIEM & SOAR deployment (atleast 20% efforts should be from OEM including architecture design, governance, training etc)		