OIL INDIA LIMITED
(A Government of India Enterprise)
P.O. Duliajan, Pin – 786602
Dist.-Dibrugarh, Assam

CORRIGENDUM No.2

GeM Tender No. GEM/2025/B/6579903

This **Corrigendum No. 2** dated 23.09.2025 to GeM Tender No. GEM/2025/B/6579903 for **"Hiring of services for supply, implementation and management of an Endpoint Detection and Response (EDR) solution to protect approximately 4000 endpoints across OIL."** is issued to amend the following:

1.0 Bid Closing / Opening dates extended as per following:

(i) Bid Closing Date & Time: Extended up to **07.10.2025 [1400 Hrs (IST)]**

(ii) Bid Opening Date & Time: Extended up to **07.10.2025 [1430 Hrs (IST)]**

2.0 Minutes of the Pre-Bid meeting held on 04th & 05th September, 2025 is enclosed herewith.

3.0 All others terms and conditions of the Bid Document (including any amendment thereof) remain unchanged. Details can be viewed at www.oil-india.com.

MANAGER – CONTRACTS (S)

ऑयल इंडिया लिमिटेड

OIL INDIA LIMITED

Minutes of Pre-Bid Conference held against GeM Tender No: GEM/2025/B/6579903 on 04th -05th September, 2025 at Hotel Hindusthan International, Kolkata.

Members Present:

OIL Officials

1.0 Shri Chandan Kumar Barman, GM (IT)
2.0 Shri Habibur Rahman Khan, CM-F&A (FC)
3.0 Shri Ankur Nath, CE (IT)
4.0 Shri Srijit Borah, CE (IT)
5.0 Shri Bikramjit Borgohain, Manager (Contracts)

Bidders Present (Physical & Video Conferencing):

1. M/s. Trend Micro India Pvt. Ltd.
2. M/s. Airtel
3. M/s. Allied Digital
4. M/s. Black Box
5. M/s. CMS
6. M/s. Dynacons
7. M/s. Embee Software Pvt. Ltd.
8. M/s. ESDS Software Solution Ltd.
9. M/s. Eventus Security Pvt Ltd
10. M/s. HPE
11. M/s. Indigi Consulting and Solutions Pvt. Ltd
12. M/s. SIFY
13. M/s. SISL Infotech Private Limited
14. M/s. Check Point Software Technologies Ltd.
15. M/s. Trellix
16. M/s. Microsoft
17. M/s. Seqrite
18. M/s. BMG Informatics Pvt Ltd

Preamble:

A GeM Tender was floated for Hiring of services for supply, implementation and management of an Endpoint Detection and Response (EDR) solution to protect approximately 4000 endpoints across OIL vide Tender No. GEM/2025/B/6579903.

As a part of the tendering process, a Pre-Bid Conference was scheduled on 04th & 5th September 2025 at Kolkata to address any queries from the prospective bidders. In the aforesaid GeM Tender, provision for submission of queries beforehand via Email was mentioned so that the queries could be addressed in the Pre-Bid Conference. Accordingly, a few queries were received via emails which were addressed during the Pre-Bid Conference. Moreover, a few queries were also raised during the Conference itself and the same were also addressed. Details of deliberations are mentioned in **ANNEXURE-Z**:

****

Queries from M/s. Bharti Airtel Services Ltd

ANNEXURE-Z

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
18		68-69	5.4 Managed Services	Dedicated Security Analysts: The Contractor will identify and deploy at least one (01) security analyst for each shift of 24/7 security monitoring of OIL's EDR solution.	The requirement for deploying 24/7 security analysts is not reflected in the BOQ (Section 6, Pages 79–81). Kindly confirm if this cost should be included under the "Managed Services" line item or if a separate BOQ line can be added for transparency and accurate costing.	Dedicated Security Analysts is part of "5.4 Managed Services". Hence corresponding costs must be included in "Charges towards Managed Service".
19		-	-	Payment term for licenses is mentioned as Quarterly	Request to amend the clause to make payment -yearly in advance	Shall deliver and issue amendment if needed.

Queries from M/s. Allied Digital **ANNEXURE-Z**

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "**Malicious file**" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "**Malicious network**" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "**Malicious driver & service**" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is **malicious and matched** with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, **CSV Formats**		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
18	2.1.3	23	The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** - It may be Email confirmation. **Providing Managed EDR services –** Request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	Trend Micro, as an OEM, offers both Managed EDR/XDR as well as Managed SOC-as-a-Service. As per our understanding, you are seeking Managed Services for the proposed EDR solutions in line with the technical specifications. However, the terminology for "Managed EDR" may vary across different Purchase Orders depending on the organization's RFP title. For example, it may appear as: •Managed XDR (MXDR) •Managed SOC with XDR (which includes Managed EDR/XDR services along with Managed SOC services, and hence covers more than Managed EDR alone) In this regard, we kindly request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	The bidder may submit documentary evidence to substantiate the experience requirement as mentioned in the clause BEC/PQC Clause No. 2.1.3. Clarified in the pre-bid conference.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
19	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** – Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	The bidder may submit documentary evidence to substantiate the experience requirement as mentioned in the clause-2.1.4. Clarified in the pre-bid conference.
20	2.1.8 - B	24	Proof of requisite Experience, viz. award and subsequent successful execution/completion of 'SIMILAR WORK' (refer Clause No. 2.1.1 above), must be substantiated by submission of the following documents along with the bid:	**Job Completion Certificate showing –** we can provide the mail for On boarding for this Manage Service and product implementation certificate for the proposed EDR solutions.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	Clarified in the pre-bid conference. Also, it may be noted that PQC/BEC Clause No. 2.1.8(b) pertains to "An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that OIL's data shall never move outside India for any purpose."
21	5.4	102	**Managed Services -** The Contractor will provide remote administration, monitoring, and management services for the deployed EDR solution, ensuring its effective operation, maintenance and ongoing optimization. This includes proactive threat hunting, incident response support, and regular reporting, as per the following table.	**OEM's Managed Services**	EDR Managed Service is one of the most crucial cybersecurity requirements for any organization. Continuous 24x7 monitoring and timely response are the key factors for the success of a Managed EDR service. It is always more effective to manage and maintain the following services and solutions directly through the OEM's Managed EDR service. The OEM team brings in-depth product knowledge and expertise, ensuring: •Faster resolution of issues •Seamless support coordination •Better alignment with evolving product capabilities In comparison, when the service is delivered through a Bidder/MSSP partner, it often remains more generic, with a lower level of product-specific expertise compared to the OEM. Therefore, for critical security operations, it is strongly recommended to rely on the OEM's own Managed EDR service to ensure comprehensive, reliable, and expert-driven protection.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
22	6 Payment Terms	116	**Subscription Charges for 4000 endpoints** - Quarterly **EDR Subscription Charges for one Endpoint for one months** - Monthly	**Subscription Charges for 4000 endpoints** - Instated of Quartely payment, please make it Upfront **EDR Subscription Charges for one Endpoint for one months** - Instated of Monthly payment, please make it Upfront	As an OEM, we do not have any provision for Quarterly or Monthly licensing. Our licenses are only available for the entire subscription period with an upfront payment. Therefore, we kindly request you to consider making at least the product payment upfront.	Shall deliver and issue amendment if needed.

Queries from M/s.Blackbox						ANNEXURE-Z
Sl. No.	**Section Details from the RFP**	**Page No.**	**Details Mentioned in the RFP**	**Clarification / Change Requested by Bidder**	**Justification for Clarifications Sought**	**OIL's Responses**
1	Clause 2.1.1 refer	24	A. 'SIMILAR WORK' mentioned above means "Experience in successfully completing the following: I. Experience in successful implementation and/or maintenance of EDR (Endpoint Detection and Response) solution. II. In case the bidder is providing OEM's Managed Security Services then – "Experience in successful implementation and/or maintenance of enterprise IT solution involving server, storage, network devices, firewalls, security solution, data centre'	Either On-Prem EDR supply & implementation with O&M (Operation and Maintenance) / Managed for 3 / 5 years will be considered. **Kindly clarify our understanding.**	We have credentials for supply, Installation and Maintenance for more than 4000 EDR license in a single PO where value is more than Rs. 2,00,54,700.00 (as asked in tender)	No change. Clarified in the pre bid conference.
2	Clause 2.1.5	24	(a) The proposed EDR solution must be operational in at least five (05) implementations in India during the last 5 years reckoned from the original bid closing date of this tender.	1. It is a OEM credentials asked for. 2. The OEM should have 5 implementation of the quoted product/solution in India in last 5 years. **Kindly clarify our understanding.**	We believe it is a credential asked from OEM.	No change. Clarified in the pre bid conference.
3	Clause 3.4	25	EMD/Bid Security: Bid Security in Original shall be furnished as a part of the Technical Bid and shall reach the office of CGM- CONTRACTS, OIL at Duliajan on or before 14.15 Hrs (IST) on the Bid Closing Date (BCD).	Request you to allow to submit the original EMD / Bid Security **within One (1) week** from the date of Bid Closing Date(BCD)	As we prepare our EMD BG at our Head office, so sending the original copy to Duliajan might take addional few days time.	No change. Clarified in the pre bid conference.
4	Components	85	**On-Premises Communication Server/Relay:** This is the bare minimum on-premises component. Its primary function is to act as a communication relay or proxy for Type-2 endpoints that cannot directly reach the cloud.On-Premises Communication Server/Relay shall be deployed by the Contractor in highly available manner in OIL's FHQ in Duliajan.	Any hardware deployed for the On-Premises setup for Type-2 endpoints need to be on **HA mode** at FHQ in Duliajan **Kindly Clarify it.**		On-Premises Communication Server/Relay shall be deployed by the Contractor in highly available manner in OIL's FHQ in Duliajan.
5	Clause 4.1 Project Timeline	98	**Present time line in the Tender-** Project Milestone / Timeline End Provisioning of required compute resources at OIL's premises at FHQ, Duliajan / D+60 days Training / D+60 days Pre-Deployment Planning / D+90 days Installation and Commissioning - Agent Deployment, On- Premises Infrastructure Deployment, Integration, Configuration, Acceptance Testing / D+120 days	Project Milestone / Timeline End Provisioning of required compute resources at OIL's premises at FHQ, Duliajan / D+90 days Training / D+90 days Pre-Deployment Planning / D+120 days Installation and Commissioning - Agent Deployment, On- Premises Infrastructure Deployment, Integration, Configuration, Acceptance Testing / D+150 days		No change. Clarified in the pre bid conference.
6	3.8.1 -1	86	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
7	3.8.1 - 3	86	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
8	3.8.1 - 6	86	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
9	3.8.1 - 8	86	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen together.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
10	3.8.1 - 11	86	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
11	Real-time endpoint monitoring, visibility, and activity logging	87	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
12	Contextual Enrichment	87	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in geographical mode		No change
13	Feedback and Tuning	89	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	Need more clarity on it.		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
14	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
15	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
16	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	Please clarify either the credentials asked (last 03 years reckoned from the original bid closing date of this tender) is from the OEM / MSS service provider of whom the bidder will quote. **Request you to please clarify our understanding.**	We understand the credential is asked from the MSS provider.	Clarified in the pre bid conference
17	Clause 5.3	100	5.3 Implementation: Workforce (To be present onsite at Duliajan during the Implementation phase)	We understand the Project Manager has to be deployed on site for the Implementation phase only not for the entire Contract period of 5 years. **Request to clarify our understanding.**		Clarified in the pre bid conference

Queries from M/s. BMG				ANNEXURE-Z
SL	**Tender Specification**	**OEM Request**	**OEM Justification for Requested Change/ Modification**	**OIL's Responses**
3.8.1	**Real-time endpoint monitoring, visibility, and activity logging**			
	Custom Rules and Detection Logic:	**OEM Request**	**OEM Justification for Requested Change/ Modification**	
2	**YARA Rule Support:** Must support YARA Rules for custom malware detection.	Partial Compliance.	Sophos have a custom Live Discover query that can leverage YARA rules.	Shall deliver and issue amendment if needed.
		"Request to accept " a custom Live Discover query that can leverage YARA rules".	With Sophos XDR, we have access to the OS Query-supported tables and the ability to write our own SQL queries that can include variables. One of the tables available is a YARA table.	
			This allows you to supply a signature file and path, and the underlying engine in OS Query will perform a search for files that match the signature.	
3.8.3	**Automated Incident Response and Remediation**			
	Automated Containment	**OEM Request**	**OEM Justification for Requested Change/ Modification**	
4	**User Account Lockdown:**	**Comply**		Shall deliver and issue amendment if needed.
			Sophos MDR does not natively integrate with Active Directory to directly disable user accounts. However, Sophos can detect account compromise indicators (e.g., unusual logins, privilege escalation) and escalate these to the customer's security team. (Auto device Lock Down).	
	Temporarily disables or locks user accounts that have been compromised. The solution shall be able to lockdown both local and Active Directory Users.	**** But OIL India team is requested to check our proposed functionality & confirm please.**		
	The solution may employ multiple methods to achieve user account lockdown for Active Directory users, like direct AD integration using APIs (Application Programming Interfaces) provided by Active Directory or using management tools (to be offered and integrated by the bidder).		Lockdown of AD accounts typically requires integration with third-party identity management tools or manual action.	
	The Contractor shall provide full details on how this functionality shall be achieved.			
	Response Orchestration and Automation :	**OEM Request**	**OEM Justification for Requested Change/ Modification**	
2	**Conditional Logic and Branching**:	Partial Compliance.	Sophos MDR's automated actions are based on severity and threat classification, but it does not offer user-configurable branching logic within playbooks.	Shall deliver and issue amendment if needed.
	Support conditional logic within playbooks, allowing for different actions to be taken based on specific conditions (e.g., severity of the threat, type of endpoint, privilege level of the user).			
		Request for Relaxation on Branching Logic.	Conditional responses are handled by the MDR team based on incident context and customer-defined response mode (Notify, Collaborate, Authorize).	
	Data Analysis and Visualization Tools	**OEM Request**	**OEM Justification for Requested Change/ Modification**	
5	**Memory Analysis**: Capabilities for capturing and analysing memory dumps to identify malicious code or artifacts in memory	Partial Compliance.	While Sophos MDR provides behavioural detection and process-level telemetry, direct memory dump capture and in-depth memory forensics are not core features of the MDR platform.	Shall deliver and issue amendment if needed.
		Request for consideration.	However, Sophos does detect memory-resident threats through behavioural indicators and integrates with tools that can support deeper memory analysis if needed. **For full memory dump analysis, third-party tools may be required.**	
		Please allow to use Third party tools		
3.9	**Security & Compliance**			
	Data Security and Privacy	**OEM Request**	**OEM Justification for Requested Change/ Modification**	Shall deliver and issue amendment if needed.
3	**Data Minimization and Control:**	Partial Compliance.	Sophos MDR collects a broad set of telemetry data to support threat detection and response.	
	The solution should allow for granular control over the types of data collected from endpoints, enabling minimization of the collection of sensitive data.		While the platform does not currently offer granular user-configurable controls to limit specific types of data collected from endpoints, Sophos does provide transparency on what data is collected and allows organizations to manage data retention policies	

		Request for consideration on granular Control Part		
	Threat Intelligence Platforms (TIPs)	**OEM**	**OEM Justification for Requested Change/ Modification**	
		Request		
	Flexible Ingestion Methods: The solution should support various ingestion methods, such as:			Shall deliver and issue amendment if needed. .
	i). STIX/TAXII : These are standardized formats for exchanging	Please remove this clause	Not supported .	
			Pease relax this Clause (**STIX/TAXII).**	
3.10	**Integration Capabilities**			
	Active Directory (AD)		**OEM Justification for Requested Change/ Modification**	
4	**Organizational Unit (OU) Information:** The solution should be able to retrieve OU information for endpoints.	Not Comply	Sophos Central's MDR/XDR interface does not currently expose OU-based policy assignment or filtering in the same granular way.	Shall deliver and issue amendment if needed.
	This allows for:	(Please relax this clause)		
	a). Applying different security policies based on organizational structure.			
	b). Filtering and grouping endpoints based on their OU.			
		OEM	**OEM Justification for Requested Change/ Modification**	
		Request		
	Automated Account Lockdown:	Partial Compliance.	Sophos MDR analysts can lock down user accounts in Microsoft 365 and Azure AD as part of incident response workflows.	
	The solution shall be able to automate the lockdown of compromised user accounts in Active Directory.			
	This is a critical capability for containing security incidents quickly.	Request for allowing	However, automated lockdown of on-premises Active Directory accounts is not natively supported through Sophos Central APIs.	Shall deliver and issue amendment if needed.
		" Sophos MDR analysts to lock down user accounts in Microsoft 365 and Azure AD as part of incident response workflows".		
			https://community.sophos.com/mdr-community-channel/mdr-integrations/b/announcements/posts/sophos-xdr-new-response-actions-for-microsoft-365	
3.12	**Backup & Recovery**			
	Data to be Backed Up	**OEM**	**OEM Justification for Requested Change/ Modification**	
		Request		
1	**Configuration Settings:**	**Requested Line**:	Sophos Central supports backup and restore of firewall configurations, including policy settings and integrations.	No change
	This includes all settings related to policies, detection rules, response playbooks, integrations, user accounts, and other configurations within the EDR management console.	"Solution Provider should keep Data Back up " This includes all settings related to policies, detection rules, response playbooks, integrations, user accounts, and other configurations "		
			However, backup of endpoint-related configuration settings (e.g., detection rules, playbooks, user accounts) is not natively supported within Sophos Central (Management Console).	

Queries from M/s. Check Point Software Technologies Ltd.						ANNEXURE-Z
Sl. No	**Pg. No.**	**nder Reference Do**	**Reference Section**	**Original Clause**	**Points of clarification/Change request**	**OIL's Responses**
1	5 of 36	SECTION-III, Scope of Work (SoW)	3.8.1 Real-time endpoint monitoring, visibility, and activity logging.	Configurable Data Retention Policy: Allow administrators to define data retention periods based on compliance and business requirements.	*Request for Modification:* Standard time basis Data Retention Policy: Allow administrators to define data retention periods based on compliance and business requirements.	No change. Clarified in the pre bid conference.
2	8 of 36	SECTION-III, Scope of Work (SoW)	3.8.3 Automated Incident Response and Remediation	Registry Remediation: Reverts malicious changes made to the Windows Registry.	*Request for Modification:* Registry Remediation: Provide either automated way or actionable way to revert changes as register keys are sensitive function	Shall deliver and issue amendment if needed.
3	11 of 36	SECTION-III, Scope of Work (SoW)	3.8.5 Threat Hunting	The solution shall provide capability that allows threat hunters to remotely connect to endpoints and perform real time investigations.	*Request for Modification:* The solution Shall provide the capability to execute scripts remotely from console to perform real-time investigations	No change. Clarified in the pre bid conference.
4	13 of 36	SECTION-III, Scope of Work (SoW)	3.10 Integration Capabilities	• STIX/TAXII: These are standardized formats for exchanging threat intelligence data.	Request for Modification: This clause is eligible to one specific vendor, hence, request to remove this for broader participation.	No change. Clarified in the pre bid conference.
5	15 of 36	SECTION-III, Scope of Work (SoW)	3.11 Operational Requirements	Automated Updates: Automated and frequent updates of threat detection content (signatures, behavioural rules, machine learning models) to ensure protection against the latest threats.	Request for Clarification: Mechanism for agent updates for latest signature and admin controlled through agent version upgrade	Clarified in the pre bid conference.
6	02 of 36	SECTION-III, Scope of Work (SoW)	3.7 Deployment Architecture	1. Endpoints with Internet access (Type-1): These are non-sensitive endpoints which can access the vendor's Cloud-based EDR solution. 2. Sensitive endpoints without Internet access (Type-2): These endpoints do not have Internet access but have Network Connectivity to Internal corporate network.	*Request for clarification:* These Type-1 and Type-2 Oil's endpoint are cumualtive of all Desktop/Laptop devices (3500 nos.) and Servers - Physical and Virtual (500 nos.).	Clarified in the pre bid conference.
7	02 of 36	SECTION-III, Scope of Work (SoW)	3.7 Deployment Architecture	Leverage the cloud for as much functionality as possible, minimizing on-premises infrastructure to only what is necessary for supporting Type-2 endpoints.	*Request for clarification:* 1. Are all the Type-2 endpoints located in a single site and are connected to the same network LAN infrastructure ? 2. Shall we consider that "Type-2 endpoints and servers" are present in all the 11nos of OIL's offices? If not, kindly specify how many OIL's offices with Nos of Type-2 endpoints. 3. Is there any specific OIL's offices where the "Type-2 endpoints" are more that 1000 in a single site/offices? 4. The required on-premises infrastructure (VM and Server) for supporting Type-2 will be provisioned by Oil india only ?	Clarified in the pre bid conference.
8	03 of 36	SECTION-III, Scope of Work (SoW)	3.7 Deployment Architecture	All compute infrastructure needed for the EDR solution which are not required to be deployed on-premises in OIL shall be "cloud-based" and shall be provisioned in the EDR OEM's cloud infrastructure.	*Request for clarification:* All compute infrastructure needed for the EDR solution (VM and Server) for supporting Type-2 will be provisioned by Oil India only ?	Clarified in the pre bid conference.

Queries from M/s. CMS						ANNEXURE-Z
Sl. No.	**Section Details from the RFP**	**Page No.**	**Details Mentioned in the RFP**	**Clarification / Change Requested by Bidder**	**Justification for Clarifications Sought**	**OIL's Responses**
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
18	**Clause 25.0**	**17**	Below modifications suggested: In the event of failure on the part of the successful Bidder to sign the contract, OIL reserves the right to terminate the LOA issued to the successful Bidder and invoke the Performance Security if submitted by the successful Bidder. The bidder will be suspended for the period of two years . This suspension of two years shall be automatic without conducting any enquiry.	Please delete The bidder will be suspended for the period of two years . This suspension of two years shall be automatic without conducting any enquiry.		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
19	**Clause 15**	49	Liability	Clause to be deleted Below modifications suggested: Defaulting Party shall be liable to the aggrieved Party for any and all losses and expenses arising out of claims due to failure of compliance with applicable laws, death or bodily injury or damage to personal property whatsoever arising directly or proximately from any willful misconduct or dishonest, grossly negligent, criminal or fraudulent act of any of the Defaulting Party's representatives and employees, gross negligence or willful misconduct under this Agreement. The Defaulting Party hereby agrees to indemnify and hold the aggrieved party harmless from any direct loss, damage, costs or expense of any kind including but not limited to reasonable attorney's fees, arising out of third party claims that the Services, proprietary materials or any information supplied by the defaulting party to the aggrieved party infringes any intellectual property rights, including patent, trademark and copyrights of such third party.		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
20	**Clause 16**	**51**	Limitation of liability	Clause to be deleted In no event shall CMS IT be liable to the Company or any third party for a monetary amount collectively and in aggregate greater than the total amounts for the immediately preceding six (6) months received by CMS IT for the Services under a particular SOW under which the liability principally arises. Neither Party shall be liable to the other Party for any loss of profit, production, anticipated savings, goodwill or business opportunities or any type of indirect, economic or consequential loss even if that loss or damage was reasonably foreseeable or that party was aware of the possibility of that loss or damage arising. The limitations set forth in this section shall apply even if any other remedies fail of their essential purpose and such limitation shall be considered cumulatively and not per incident. The existence of claims or suits will not enlarge or extend the limit.		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
21	**Clause 19**	**52**	Risk Purchase	Below modifications suggested: In the event, CONTRACTOR's failure to provide the services as per the Contractual scope, terms and conditions, COMPANY (OIL) reserves the right to hire the services from any other source at the CONTRACTOR's risk & cost and the difference in cost shall be borne by the CONTRACTOR.However the liability under this clause of the bidder shall not exceed the 5% of the differential cost for unperformed service Further, OIL shall retain the right of forfeiture of Performance Bank Guarantee and any other action as deemed fit. In certain operational situations OIL reserves the right to take over the site including the service equipment at the risk and cost of the CONTRACTOR.		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
22	**Clause 20**	**52**	Indemnity Agreement/ Indemnity Application/ Royalty Patent	To be deleted		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
23	**Clause 23.2**	**53**	Should COMPANY discover at any time during the tenure of the Contract or till the Unit/equipment/tools are demobilised from site or base camp (if applicable) that the work does not conform to the foregoing warranty, CONTRACTOR shall after receipt of notice from COMPANY, promptly perform any and all corrective work required to make the services conform to the Warranty. Such corrective Work shall be performed entirely at CONTRACTOR's own expenses. If such corrective Work is not performed within a reasonable time, the COMPANY, at its option may have such remedial Work performed by others and charge the cost thereof to CONTRACTOR subject to a maximum of the contract value payable for the defective work which needs corrective action which the CONTRACTOR must pay promptly. In case CONTRACTOR fails to perform remedial work, or pay promptly in respect thereof, the performance security shall be forfeited.	to be capped at 5% of differential costs		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
24	**Clause 26.0**	**54**	Confidentiality, Use of Contract Documents and information	Below modifications suggested: The obligations contained in this clause shall apply mutatis mutandis to Company to the extent of any Contractor's Confidential Information being disclosed to Company		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
25	**Clause 27.0, 28.0,**	**55**	Renumeration & Terms of Payment	Payment terms for license to be yearly adavcne		Shall deliver and issue amendment if needed.
26	**Clause 30.0, 32.0, 33.0**	**57**	Timely mobilisation & LD	30 LD capped at 7.5% of the TCV- ok Clause 32 to be deleted Clause 33 ok		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
27	**Clause 44.5**	**68**	Termination for unsatisfactory performance	Below modifications suggested: If the COMPANY considers that, the performance of the CONTRACTOR is ~~unsatisfactory, or~~ not as per the provision of the Contract, the COMPANY shall notify the CONTRACTOR in writing and specify in details the cause of dissatisfaction. The COMPANY shall have the option to terminate the Contract by giving 60 ~~15~~ days notice in writing to the CONTRACTOR, if CONTRACTOR fails to comply with the requisitions contained in the said written notice issued by the COMPANY. In the event CONTRACTOR rectifies its non performance to the satisfaction of the COMPANY, the option of termination may not be exercised by the COMPANY. If however CONTRACTOR repeats non-performance subsequently, COMPANY shall exercise the option to terminate contract by giving 30 ~~07~~ days notice. ~~Such CONTRACTOR shall be put on holiday as per the Banning Policy of OIL [available at www.oil-india.in].~~ Clause 44.6 to be deleted 45,46- to be capped at 5% of the differential costs		No change. It may be noted that the Clauses in the GCC are the standrad clauses of the company. The Clauses of SCC shall supplement and / or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions in the SCC shall prevail over those in the GCC.
28	**Clause 6.0**	**116**	Payment terms	for Subscribtion/license - yearly advance		Shall deliver and issue amendment if needed.
29		**121**	PAYMENT TERMS	for Subscribtion/license - yearly advance		Shall deliver and issue amendment if needed.
30	**128**	36	NDA (Duration)	Below modifications suggested: This Agreement shall come into force on the date written hereunder, and shall remain in force for a period of four (4) years starting from such date. The obligations set forth in Article 2 hereof shall survive 2 years post termination or the expiration of this Agreement for the period specified in such Article.		No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
31			Clause to be added	**Non Solicitation**: Neither party shall solicit/induce/entice away or endeavour to solicit/induce/entice away an employee of the other party who is directly involved for 2 years after such resource has ceased to be engaged for performance of services pursuant to proposal and this RFP. Notwithstanding the foregoing, either party may hire (a) personnel who independently responds to indirect solicitation (such as general newspaper advertisements, employment agency referrals, and internet postings) not targeting the personnel of the other party and (b) personnel who have separated or have been separated from the services of a party for at least a period of 1 (One) year.		No change
32			Clause to be added	In the event of delay in installation or commissioning of equipment supplied by the Service Provider, or delay in submission of documents required under the RFP / Agreement / PO, or delay in issuance of the acceptance certificates by the Client, due to reasons beyond the reasonable control of the Service Provider, including but not limited to site not being ready, or force majeure situations, government orders and notifications, government ordered lockdown, epidemics and pandemics etc., the Client shall make immediate payment and not withhold payment of fees for the Products supplied and / or services already rendered, on this account. In such cases the Service Provider shall raise the invoice to the extent of the value of goods delivered and/or quantum of work performed and the Client shall make payment thereof. Further, it shall be the obligation of the Service Provider to perform all the unperformed / partially performed work and submit all the necessary documents in terms of the RFP / Agreement / PO as soon as practicably possible upon normalization of the situation		No change

Queries from M/s.Dynancons						ANNEXURE-Z
Sl Nos.	**RFP**	**Clause Description**	**Request**			**OIL's Response**
1	Bid Evaluation Criteria 2.1 TECHNICAL REQUIREMENTS:	2.1.3 The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	We request to revise this clause as 2.1.3 The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the **any OEM EDR solution** to whom they are currently providing/ provided the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.			No change
2	Bid Evaluation Criteria 2.1 TECHNICAL REQUIREMENTS:	2.1.7 The MSS centre proposed by the bidder against the tender must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 1/Type 2 or SOC 3 certified. The bidders shall have to furnish the relevant certificate to substantiate the same .	We request to revise this payment term as 2.1.7 The MSS centre proposed by the bidder against the tender must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 1/Type 2 or SOC 3 certified OR CMMI Level 5 Certified. The bidders shall have to furnish the relevant certificate to substantiate the same .			No change
3	6 Payment Terms	EDR Subscription Charges for 4000 endpoints - Quarterly	Considering the OEM payment term & better cashflow, we request you to revise this payment term as "EDR Subscription Charges for 4000 endpoints - 100% against the delivery & installation of the licenses			No change
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	No change
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen together.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
18	2.1.3	23	The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** - It may be Email confirmation. **Providing Managed EDR services –** Request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	Trend Micro, as an OEM, offers both Managed EDR/XDR as well as Managed SOC-as-a-Service. As per our understanding, you are seeking Managed Services for the proposed EDR solutions in line with the technical specifications. However, the terminology for "Managed EDR" may vary across different Purchase Orders depending on the organization's RFP title. For example, it may appear as: •Managed XDR (MXDR) •Managed SOC with XDR (which includes Managed EDR/XDR services along with Managed SOC services, and hence covers more than Managed EDR alone) In this regard, we kindly request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the clause-2.1.3. Clarified in the pre-bid conference.
19	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** – Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the clause-2.1.4. Clarified in the pre-bid conference.
20	2.1.8 - B	24	Proof of requisite Experience, viz. award and subsequent successful execution/completion of 'SIMILAR WORK' (refer Clause No. 2.1.1 above), must be substantiated by submission of the following documents along with the bid:	**Job Completion Certificate showing** – we can provide the mail for On boarding for this Manage Service and product implementation certificate for the proposed EDR solutions.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	2.1.8(b) pertains to "An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that OIL's data shall never move outside India for any purpose." Clarified in the pre-bid conference.

21	5.4	102	**Managed Services -** The Contractor will provide remote administration, monitoring, and management services for the deployed EDR solution, ensuring its effective operation, maintenance and ongoing optimization. This includes proactive threat hunting, incident response support, and regular reporting, as per the following table.	**OEM's Managed Services**	EDR Managed Service is one of the most crucial cybersecurity requirements for any organization. Continuous 24x7 monitoring and timely response are the key factors for the success of a Managed EDR service. It is always more effective to manage and maintain the following services and solutions directly through the OEM's Managed EDR service. The OEM team brings in-depth product knowledge and expertise, ensuring: •Faster resolution of issues •Seamless support coordination •Better alignment with evolving product capabilities In comparison, when the service is delivered through a Bidder/MSSP partner, it often remains more generic, with a lower level of product-specific expertise compared to the OEM. Therefore, for critical security operations, it is strongly recommended to rely on the OEM's own Managed EDR service to ensure comprehensive, reliable, and expert-driven protection.	No change
22	6 Payment Terms	116	**Subscription Charges for 4000 endpoints** - Quarterly **EDR Subscription Charges for one Endpoint for one months** - Monthly	**Subscription Charges for 4000 endpoints** - Instated of Quartely payment, please make it Upfront **EDR Subscription Charges for one Endpoint for one months** - Instated of Monthly payment, please make it Upfront	As our OEM, do not have any provision for Quarterly or Monthly licensing. the desired licenses are only available for the entire subscription period with an upfront payment. Therefore, we kindly request you to consider making at least the product payment upfront.	Shall deliver and issue amendment if needed.

Queries from M/s. Embee				ANNEXURE-Z
Bid Page No	**Bid Clause No.**	**Original Clause**	**Query sought/ Suggestions of the Bidder**	**OIL's Responses**
BEC/ PQC Pg 1 of 13	**2.1.1**	Bidder must have experience of successfully completing at least one '**SIMILAR WORK'** of minimum value of **₹ 2,00,54,700.00 (Rupees Two Crore Fifty-Four Thousand Seven Hundred)** ..... Public Limited Company of India.	Please clarify is this value has to be the annual value OR total contract value of the entire period of contract	The minimum value corresponds to total value of the contract. Please be guided by the Notes to Clause 2.1.1 in the tender.
BEC/ PQC Pg 2 of 13	**2.1.2**	The bidder must be an IT Solution Provider having a functional MSS (Managed Security Service) center.	Please help us understand what the criteria of evaluation by OIL are OR How can the bidder establish they have a functional MSS.	Please refer to the clause PQC /BEC Clause No. 2.1.4. of the tender
Annexure 1. Page 1 of 2	Annexure Point 7	Commitment to MSS Service We undertake to offer MSS service to OIL through our partner [Name of the Bidder] against OIL Tender No._____ for the entire duration of the contract as per the given scope of work.	Pl incorporate the words 'but by our own technical human resources' in the statement. i.e, We undertake to offer MSS service to OIL through our partner [Name of the Bidder] *but by our own technical human resources* against OIL Tender No._____	No change. Clarified in the pre bid conference.
BEC/ PQC Pg 2 of 13	**2.1.3**	The EDR OEM or the Solution Provider must have experience of providing managed EDR services .....Public Limited Company **using the proposed EDR solution** to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	Request OIL to remove the phrase 'using the proposed EDR solution' from this criterion.	No change. Clarified in the pre bid conference.
PROFORMA-XVII, Price Bid Format	**1.3.1**	The Bidder must be incorporated / constituted in India and must maintain more than or equal to 20% local content for the offered services. With regard to calculation of local content and submission of documents during bidding & execution of contracts	Bidders being all Indian companies and all bids being 100% services (OPEX/ Subscription), we believe bidder can qualify as Class 1 LC even if bidder quotes a product which does not have qualify for Class II LC in its product natively. Kindly elaborate on this and clarify.	No change. Clarified in the pre bid conference.

Queries from M/s. ESDS **ANNEXURE-Z**

Sr.No.	Document Name & Number	Page No.	Clause	Details	Clarification Required	OIL's Responses
1	Scope of work: 1755515608	1	INTRODUCTION 1 (iii) Technical Bid Opening Date & Time	As mentioned in GeM Portal. Bidders must refrain from seeking an extension of the due date for bid submission. Moreover, any such requests will not be entertained by OIL.	As per current timelines Bid Submission is due on 09 Sep 2025 the pre-bid meeting has been concluded on 05 Sep 2025, many bidders have sought clarifications which needs to be replied by OIL, hence we request that the bid submission date may kindly be extended atleast 14 days post issue of Pre-Bid response.	The tender has been extended.
2	Scope of work: 1755515608	1	BID EVALUATION CRITERIA (BEC)/ PRE QUALIFICATION CRITERIA (PQC) 2.0 TECHNICAL EVALUATION CRITERIA 2.1 TECHNICAL REQUIREMENTS	2.1.1 Bidder must have experience of successfully completing at least one 'SIMILAR WORK' of minimum value of ₹ 2,00,54,700.00 (Rupees Two Crore Fifty-Four Thousand Seven Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with Central Government / State Government Organization / PSUs / Nationalised Banks/ Public Limited Company of India.	In case the Bidder is MSSP and having experience of providing EDR service, however the value of EDR services is as per bid requirement, then can the experience of proposed OEM for EDR with bid requirement value be considered. Kindly clarify.	Clarified in the pre bid conference.
3	Scope of work: 1755515608	10	BID EVALUATION CRITERIA (BEC)/ PRE QUALIFICATION CRITERIA (PQC) 10.0 CERTIFICATION OF DOCUMENTS BY INDEPENDENT THIRD-PARTY INSPECTION AGENCIES (TPIA)	Oil India Limited (OIL) has engaged the following 17 (Seventeen) Independent Inspection Agencies for a period of 04 (Four) years up to 06.06.2028 to verify and certify various documents submitted by the bidders required against BEC/BRC of the tender	We request that the requirement of verification of documents of Bidder by TPIA during bid submission may kindly be relaxed, instead the verification of documents to be done only for the successful bidders before opening of financial bid.	No change
4			**Generic Queries**	**A. Project Timeline & Implementation**		
5				1. Will OIL provide a detailed environment inventory (endpoint OS versions, applications, AD structure, existing SIEM/SOAR integrations) before Pre-Deployment Planning?		Clarified in the pre bid conference
6				2. What is the expected approval timeline for solution design by OIL, since delays here may affect installation & commissioning milestones?		Clarified in the pre bid conference
7				3. Can provisioning timelines (D+60 days for compute) be extended if OIL's physical infra (rack/power/cooling) is not ready?		Clarified in the pre bid conference
8				4. Is there a parallel testing environment available for pilot deployment, or should the pilot be conducted in production?		Clarified in the pre bid conference
9				5. For vertical auto-scaling and infra provisioning – will OIL allow hypervisor-level access for performance tuning?		Clarified in the pre bid conference
10				**B. Supply & Licensing**		
11				6. For the Hybrid (SaaS + On-Premises) model, what percentage of services are expected to run on OIL infra vs. cloud?		Clarified in the pre bid conference
12				7. For cloud storage – can the vendor choose any cloud provider, or must it be OIL-approved (AWS, Azure, GCP, NIC Cloud, etc.)?		Clarified in the pre bid conference
13				8. Can endpoint/user license counts be flexible across categories (e.g., 4000 endpoint licenses reused across VMs and physical devices)?		Clarified in the pre bid conference
14				9. For additional 1000 endpoints licensing – will the unit rate escalation clause be applicable in later years (e.g., after renewal or OEM price hikes)?		Clarified in the pre bid conference
15				10. During installation & commissioning, will OIL provide temporary licenses or must the vendor provision full subscriptions from day one?		Clarified in the pre bid conference
16				**C. Infrastructure & Deployment**		
17				11. For on-premises infra supply, does OIL mandate specific OEM brands (servers, storage) or is vendor free to propose equivalent?		Clarified in the pre bid conference
18				12. Will OIL provide the networking components (firewall, load balancer, switches), or should the vendor provision them?		Clarified in the pre bid conference
19				13. What is the storage performance (IOPS) requirement for centralized EDR data repository?		Clarified in the pre bid conference
20				14. Should data be encrypted at rest and in transit for cloud storage? If yes, is there a preferred KMS (Key Management Service)?		Clarified in the pre bid conference
21				15. For automated agent deployment – will OIL provide GPO/SCCM/Intune/Other tools access, or must vendor propose a custom deployment tool?		Clarified in the pre bid conference
22				**D. Integration & Testing**		
23				16. Will OIL share API documentation for integration with their SIEM, SOAR, TIP, and AD during planning?		Clarified in the pre bid conference
24				17. Should integration include bi-directional workflows (e.g., alerts from EDR trigger playbooks in SOAR and vice versa)?		Clarified in the pre bid conference
25				18. What are the log retention and forwarding requirements from EDR to OIL's SIEM?		Clarified in the pre bid conference
26				19. For acceptance testing – will OIL provide real malware/simulation tools (like Red Team test cases, Atomic Red Team, etc.)?		Clarified in the pre bid conference
27				20. What baseline KPIs (threat detection rate, false positive ratio, response time) must be met during UAT & performance testing?		Clarified in the pre bid conference
28				**E. Managed Services & Operations**		

29				21. Can the 24/7 monitoring team be partly offshore/remote SOC, or must analysts be physically deployed in India?		Clarified in the pre bid conference
30				22. Will OIL's IT/Security team require co-managed access (shared console) or full independence in policy management?		Clarified in the pre bid conference
31				23. What is the expected MTTR (Mean Time to Respond) for incidents outside SLA metrics?		Clarified in the pre bid conference
32				24. Will OIL provide incident playbooks or should the vendor design them?		Clarified in the pre bid conference
33				25. For knowledge transfer – is OIL expecting monthly training workshops or hands-on shadowing sessions?		Clarified in the pre bid conference
34				**F. SLA & Compliance**		
35				26. For SLA measurements (99% availability, alert triage timelines), will OIL provide an independent monitoring tool, or should the vendor propose one?		Clarified in the pre bid conference
36				27. Are SLA penalties negotiable (7% quarterly cap) if non-performance is due to external dependencies (OIL infra failures, power, connectivity issues)?		Clarified in the pre bid conference
37				28. Will DR/BCP compliance be required for EDR infrastructure hosted at OIL's site?		Clarified in the pre bid conference
38				29. Does OIL mandate compliance with any specific frameworks (ISO 27001, CERT-In guidelines, IT Act, DPDP Act)?		Clarified in the pre bid conference
39				30. In case of a critical incident (e.g., ransomware), who leads incident ownership – OIL or the vendor?		Clarified in the pre bid conference

Quries from M/s. Eventus						ANNEXURE-Z
Sl. No.	**Section Details from the RFP**	**Page No.**	**Details Mentioned in the RFP**	**Clarification / Change Requested by Bidder**	**Justification for Clarifications Sought**	**OIL's Response**
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "**Malicious file**" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "**Malicious network**" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "**Malicious driver & service**" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is **malicious and matched** with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, **CSV Formats**		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
3+12:	2.1.3	23	The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** - It may be Email confirmation. **Providing Managed EDR services –** Request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	Trend Micro, as an OEM, offers both Managed EDR/XDR as well as Managed SOC-as-a-Service. As per our understanding, you are seeking Managed Services for the proposed EDR solutions in line with the technical specifications. However, the terminology for "Managed EDR" may vary across different Purchase Orders depending on the organization's RFP title. For example, it may appear as: •Managed XDR (MXDR) •Managed SOC with XDR (which includes Managed EDR/XDR services along with Managed SOC services, and hence covers more than Managed EDR alone) In this regard, we kindly request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the BEC/PQC clause-2.1.3 of the tender. Clarified in the pre-bid conference.
19	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** – Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the PQC/BEC clause-2.1.4 of the tender. Clarified in the pre-bid conference.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
20	2.1.8 - B	24	Proof of requisite Experience, viz. award and subsequent successful execution/completion of 'SIMILAR WORK' (refer Clause No. 2.1.1 above), must be substantiated by submission of the following documents along with the bid:	**Job Completion Certificate showing –** we can provide the mail for On boarding for this Manage Service and product implementation certificate for the proposed EDR solutions.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service. We trust this clarification addresses your concern. Please let us know if any additional documentation is required.	Clarified in the pre-bid conference. Also, it may be noted that PQC/BEC Clause No. 2.1.8(b) pertains to "An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that OIL's data shall never move outside India for any purpose."
21	5.4	102	**Managed Services -** The Contractor will provide remote administration, monitoring, and management services for the deployed EDR solution, ensuring its effective operation, maintenance and ongoing optimization. This includes proactive threat hunting, incident response support, and regular reporting, as per the following table.	**OEM's Managed Services**	EDR Managed Service is one of the most crucial cybersecurity requirements for any organization. Continuous 24x7 monitoring and timely response are the key factors for the success of a Managed EDR service. It is always more effective to manage and maintain the following services and solutions directly through the OEM's Managed EDR service. The OEM team brings in-depth product knowledge and expertise, ensuring: •Faster resolution of issues •Seamless support coordination •Better alignment with evolving product capabilities In comparison, when the service is delivered through a Bidder/MSSP partner, it often remains more generic, with a lower level of product-specific expertise compared to the OEM. Therefore, for critical security operations, it is strongly recommended to rely on the OEM's own Managed EDR service to ensure comprehensive, reliable, and expert-driven protection.	No change
22	6 Payment Terms	116	**Subscription Charges for 4000 endpoints** - Quarterly **EDR Subscription Charges for one Endpoint for one months** - Monthly	**Subscription Charges for 4000 endpoints** - Instated of Quartely payment, please make it Upfront **EDR Subscription Charges for one Endpoint for one months** - Instated of Monthly payment, please make it Upfront	As an OEM, we do not have any provision for Quarterly or Monthly licensing. Our licenses are only available for the entire subscription period with an upfront payment. Therefore, we kindly request you to consider making at least the product payment upfront.	Shall deliver and issue amendment if needed.

Queries from M/s. HPE						ANNEXURE-Z
Sl No	**RFP Section**	**Page No. / Point No.**	**RFP Specificiation**	**Query / Change Request**	**Justification**	**OIL's Responses**
1	2	3	BACKING OUT BY L1 BIDDER AFTER ISSUE OF LOA	To remove the reference of an additional policy.	Forfeiting the bid security alone should suffice as a deterring factor to the Bidder. Adding an additional ground of a policy not imbedded in this document would be quite punitive and we would kindly request for this reference to be removed.	No change
2	9.8	9	Grounds of forfeiture of Bid Security	We would kindly request that the forfeiture be restricted to point e, i.e. fraudulent actions.	We would kindly request that the forfeiture be restricted to point e, i.e. fraudulent actions as forfeiture for the other grounds would be quite harsh.	No change
3	25.3	17	The bidder will be suspended for the period of two years. This suspension of two years shall be automatic without conducting any enquiry.	To remove this suspension.	we would kindly request that blacklisting be restricted to fraudulent actions.	No change
4	15	49	Liability	To remove this portion.	We would kindly request that this entire portion be removed as the LOL clause (clause 16) covers the main portions, and this appears to complicate the clause. Additionally, the clause also includes references to indemnification when there is a subsequent clause on the same. We would kindly request that all indemnities fall under the one clause only.	No change
5	16 (a)	51	Notwithstanding any other provisions herein to the contrary, except only in cases of Wilful misconduct and/or criminal acts and/or criminal negligence, neither the CONTRACTOR nor the COMPANY (OIL) shall be liable to the other, whether in Contract, tort, or otherwise, for any consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided however that this exclusion shall not apply to any obligation of the CONTRACTOR to pay Liquidated Damages to the COMPANY and/or COMPANY's right to forfeit the Performance Bank Guarantee(s) in terms of the contract.	Notwithstanding any other provisions herein to the contrary, ~~except only in cases of Wilful misconduct and/or criminal acts and/or criminal negligence,~~ neither the CONTRACTOR nor the COMPANY (OIL) shall be liable to the other, whether in Contract, tort, or otherwise, for any consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, ~~provided however that this exclusion shall not apply to any obligation of the CONTRACTOR to pay Liquidated Damages to the COMPANY and/or COMPANY's right to forfeit the Performance Bank Guarantee(s) in terms of the contract~~.	We would kindly request that there be no exceptions to indirect damages as these are too remote to account for and is standard practice to exclude all indirect damages.	No change
6	16 (b)	51	Notwithstanding any other provisions incorporated elsewhere in the contract, the aggregate liability of the CONTRACTOR in respect of this contract, whether under Contract, in tort or otherwise, shall not exceed 100% of the Contract Price (if not specified otherwise in SCC), provided however that this limitation shall not apply to the cost of repairing or replacing defective equipment by the CONTRACTOR, or to any obligation of the CONTRACTOR to indemnify the COMPANY with respect to Intellectual Property Rights.	Notwithstanding any other provisions incorporated elsewhere in the contract, the aggregate liability of the CONTRACTOR in respect of this contract, whether under Contract, in tort or otherwise, shall not exceed 100% of the Contract Price (if not specified otherwise in SCC), provided however that this limitation shall not apply ~~to the cost of repairing or replacing defective equipment by the CONTRACTOR, or~~ to any obligation of the CONTRACTOR to indemnify the COMPANY with respect to Intellectual Property Rights.	We would request that all liabilities except for IPR be capped to the TCV as these are general aspects covered under the contract. Additionally, the customer has multiple grounds already, such as PBG, SLAs, penalties, etc.	No change
7	16 (c)	51	COMPANY shall indemnify and keep indemnified CONTRACTOR harmless from and against any and all claims, costs, losses and liabilities in excess of the aggregate liability amount in terms of clause (b) above.	Removal of clause	We would kindly request that this portion be deleted because otherwise it defeats the very purpose of having a limitation of liability clause or a cap. This would then essentially imply that the whole contract and the claims that arise from it are uncapped and can be claimed under indemnities. The customer again already has multiple recourses such as the PBG, penalties, liabilities, etc.	No change

8	20.1	52	Except as provided hereof CONTRACTOR agrees to protect, defend, indemnify and hold COMPANY harmless from and against all claims, suits, demands and causes of action, liabilities, expenses, cost, liens and judgments of every kind and character, without limit, which may arise in favour of CONTRACTOR's employees, agents, CONTRACTORs and sub-CONTRACTORs or their employees or in favour of any third party(is) on account of bodily injury or death, or damage to personnel/property as a result of the operations contemplated hereby, regardless of whether or not said claims, demands or causes of action arise out of the negligence or otherwise, in whole or in part or other faults.	Except as provided hereof CONTRACTOR agrees to ~~protect, defend,~~ indemnify **the**~~and hold~~ COMPANY ~~harmless~~ from and against all **direct third party** claims, suits, demands and causes of action, liabilities, expenses, cost, liens and judgments of every kind and character, without limit, which may arise in favour of CONTRACTOR's employees, agents, CONTRACTORs and sub-CONTRACTORs or their employees or in favour of any third party(is) on account of bodily injury or death, or damage to personnel/property as a result of the operations contemplated hereby, regardless of whether or not said claims, demands or causes of action arise out of the negligence or otherwise, in whole or in part or other faults.	We would kindly request that this be restricted to third party direct claims.	No change
9	23.1	53	CONTRACTOR warrants that they shall perform the work in a first class, workmanlike, and professional manner and in accordance with their highest degree of quality, efficiency and current state of the art technology/industry practices and in conformity with all specifications, standards and drawings set forth or referred to in the Terms of Reference and with instructions and guidance, which COMPANY may, from time to time, furnish to the CONTRACTOR.	CONTRACTOR warrants that they shall perform the work in a ~~first class, workmanlike,~~ ~~and~~ professional manner and in accordance with **the reasonable market standards for** ~~their~~ ~~highest~~ degree of quality, efficiency and current state of the art technology/industry practices and in conformity with all specifications, standards and drawings set forth or referred to in the Terms of Reference and with instructions and guidance, which COMPANY may, from time to time, furnish to the CONTRACTOR.	We would request that these amendments be made to the clause to paint a more standardized approach that is acceptable to both parties.	No change
10	29 (i), (ii)	57	i) Copy of PF-ECR duly stamped by the designated Bank, alongwith a print of the digitally signed PDF data sheet of the ECR, as proof of payment, each month, details of this PDF data sheet shall be verified by the appropriate authority (i.e. Payment Making Authority) in the COMPANY from the official website of EPFO (http://www.epfindia.gov.in). (ii) (a) Copy of the online challan endorsed/stamped by the designated bank as proof of receipt of payment towards monthly contribution of ESI contribution. (b) Copy of Return of contribution in respect of ESI for each contribution period of the six months i.e. for the contribution period ended 30th Sept and the contribution period ended 31st March.	Removal of clause	We would kindly request that this clause be removed as it would be a lot of sensitive information that we would have to share. However, we are willing to submit the declaration and in case any employee of ours attempts to make a claim with you, we shall immediately step in and address those and take on full liability for the same.	No change
11	31	58	FORCE MAJEURE	Amendments to the clause	We would kindly request that a force majeure event be mutually decided, and not soleyl by the company as this is an event that affects at a wide scale. Additionally, we would also request that such an event not exclude the obligation of the company to make due the payments that are owed to the contractor.	No change
12	44.5	68	Termination for Unsatisfactory Performance	Minor amendment requested	We would kindly request that the termination be for material breaches.	No change
13	44.9	69	Notwithstanding any provisions herein to the contrary, the Contract may be terminated at any time by the COMPANY on giving 30 (thirty) days written notice to the CONTRACTOR due to any other reason not covered under the above Article from 44.1 to 44.8 and in the event of such termination the COMPANY shall not be liable to pay any cost or damage to the CONTRACTOR except for payment of services as per the Contract upto the date of termination.	Notwithstanding any provisions herein to the contrary, the Contract may be terminated at any time by the COMPANY on giving **90 (ninety)** ~~30 (thirty)~~ days written notice to the CONTRACTOR due to any other reason not covered under the above Article from 44.1 to 44.8 and in the event of such termination the COMPANY shall not be liable to pay any cost or damage to the CONTRACTOR except for payment of services as per the Contract upto the date of termination.	would request that for termination for convenience the notice period be extended to 90 days.	No change
14	8	128	The obligations set forth in Article 2 hereof shall survive the expiration of this Agreement for the period specified in such Article.	Clarity sought	We would kindly request that the obligations also be valid for a term of 2 years post contract termination or any such term as applicable by laaw. Article 2 does not call any such duration, and thereby it is unclear from this clause.	No change
15	Annexure I	135	OEM undertaking	Amendments throughout the undertaking.	We would kindly request that the entire undertaking restrict the scope and obligations of the OEM only to what they are providing, since there may be multiple OEMs and it would be difficult for them to commit to other aspects.	No change

16	Proforma XIII	198	FORMAT OF PERFORMANCE BANK GUARANTEE	Amendments throughout the format.	We would kindly request that the PBG only be invoked for **material** breaches not cured within 30 days of the notice of such breach to the Bidder/ Contractor.	No change
17	Proforma XV	201	FORM OF BID SECURITY (BANK GUARANTEE FORMAT)	Amendments throughout the format.	We would kindly request that the EMD be forfeited only for fraudulent activities, i.e. point 5. Alternatively, for the other points, we would request that the forfeiture be after a notice of 30 days of failure to comply has been provided to the Bidder.	No change
18	9	207	This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the respective contract, and for all other Bidders 6 months after the contract has been awarded.	This Pact begins when both parties have legally signed it. It expires for the Contractor ~~12 months~~ after the last payment under the respective contract, and for all other Bidders 6 months after the contract has been awarded.	We would kindly request that the Integrity Pact's validity align with the term of the contract.	No change
19	Payment Terms	Missing	Missing	Bidder request Payment within 30 days from date of invoice		No change
20	Payment Terms	79/6.1	Quarterly payment for EDR Subscription Charges for 4000 endpoints	1. Bidder request for Payment of Lumsum on delivery of EDR licenses. 2. The ATS for EDR licenses to be paid yearly in advance.		Shall deliver and issue amendment if needed.
21	Payment Terms	79/6.1	Quarterly payment for Charges towards Managed Service	Bidder Request for Monthly Invoice		Shall deliver and issue amendment if needed.
22	Performance Security	16/24	03% of Contract Value.	Bidder Request Allow yearly rolling BG of same of amount which will be renewed every year till the completion of period 5 year 90 days		No change
23	Rate Card	80	EDR Subscription Charges for one Endpoint for one month	Bidder Clarifies The rate for additional EDR licenses will be quoted with 1 Year ATS, any additional ATS needed will be renegotiated. 2. The rate will be valid for first 1 year of contract.		No change

Queries from M/s. Indigi						ANNEXURE-Z
Sl. No.	**Section Details from the RFP**	**Page No.**	**Details Mentioned in the RFP**	**Clarification / Change Requested by Bidder**	**Justification for Clarifications Sought**	**OIL's Response**
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns)	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
18	2.1.3	23	The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** - It may be Email confirmation. **Providing Managed EDR services –** Request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	Trend Micro, as an OEM, offers both Managed EDR/XDR as well as Managed SOC-as-a-Service. As per our understanding, you are seeking Managed Services for the proposed EDR solutions in line with the technical specifications. However, the terminology for "Managed EDR" may vary across different Purchase Orders depending on the organization's RFP title. For example, it may appear as: •Managed XDR (MXDR) •Managed SOC with XDR (which includes Managed EDR/XDR services along with Managed SOC services, and hence covers more	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the clause-PQC/BEC Clause No. 2.1.3 of the tender. Clarified in the pre-bid conference.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
19	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** – Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in BEC/PQC Clause No. 2.1.4 of the tender. Clarified in the pre-bid conference.
	2.1.8 - B	24	Proof of requisite Experience, viz. award and subsequent successful execution/completion of 'SIMILAR WORK' (refer Clause No. 2.1.1 above), must be substantiated by submission of the following documents along with the bid:	**Job Completion Certificate showing –** we can provide the mail for On boarding for this Manage Service and product implementation certificate for the proposed EDR solutions.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For	Clarified in the pre-bid conference. Also, it may be noted that BEC/PQC Clause No. 2.1.8(b) pertains to "An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that OIL's data shall never move outside India for any purpose.

Section	Clause	Complied/Not Complied/ Query	Reference Document	Remarks	OIL'S Response
3.7	**Deployment Architecture**				
Core Principle	Leverage the cloud for as much functionality as possible, minimizing on-premises infrastructure to only what is necessary for supporting Type-2 endpoints.	Yes			
	Hybrid Architecture Support: The EDR solution must support a hybrid deployment model with a cloud-based management console and an on-premises communication server/relay.	Yes			
	Centralized Management: A single, cloud-based management console must provide complete visibility and control over all deployed EDR agents, regardless of connectivity method.	Yes			
Components	All compute infrastructure needed for the EDR solution which are not required to be deployed on-premises in OIL shall be "cloud-based" and shall be provisioned in the EDR OEM's cloud infrastructure.	Yes			
	On-Premises Communication Server/Relay: This is the bare minimum on-premises component. Its primary function is to act as a communication relay or proxy for Type-2 endpoints that cannot directly reach the cloud.	Yes			
	On-Premises Communication Server/Relay shall be deployed by the vendor in highly available manner in OIL's FHQ in Duliajan.	Yes		Deployment to be done by partner	
	All other components like Management Console, Data storage and analytics, Threat Intelligence feeds are hosted on EDR OEM's cloud infrastructure.	Yes			
Network Flow	Endpoints with Internet access communicate directly to EDR OEM's cloud infrastructure through secure, encrypted communication channels (e.g., HTTPS or proprietary secure protocols).	Yes			
	Sensitive endpoints without Internet access communicate with the on-premises communication server or relay through secure, encrypted communication channels, which subsequently transmits traffic to and from the EDR OEM's cloud infrastructure.	Yes			
	The On-Premises Communication Server/Relay communicates with the EDR OEM's cloud infrastructure over secure, encrypted communication channel.	Yes			
3.8	**Core Features**				
3.8.1	**Real-time endpoint monitoring, visibility, and activity logging**				
Continuous Data Collection	The solution must continuously collect data on all endpoint activity, including:				
	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	Need clarity since this is File Integrity Monitoring feature. Can get logs from Endpoint DLP solution.			Shall deliver and issue amendment if needed.
	2.Process Activity: Process creation, termination, parent-child relationships (process lineage/ancestry), command-line arguments, loaded modules/DLLs.	Yes			
	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	Defender for Endpoint has network protection capabilities			
	4. Registry Activity: Registry key creation, modification, deletion, value changes.	Yes			
	5. User Activity: Logons, logoffs, account changes, privilege escalations.	Can be achieved with Defender for Identity			
	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	Yes	Review events and errors using Event Viewer - Microsoft Defender for Endpoint | Microsoft Learn		
	7. Memory Activity: Memory access, modifications, memory dumps (for advanced analysis).	Yes			Shall deliver and issue amendment if needed.
	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Yes			
	9. WMI Activity: Monitoring Windows Management Instrumentation queries and executions.	We can configure behavior monitoring using WMI			
	10. Scheduled Tasks: Monitoring creation, modification, and execution of scheduled tasks.	Yes			
	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	Yes	Live response command examples - Microsoft Defender for Endpoint | Microsoft Learn		
	Configurable Data Collection: The solution must allow administrators to fine-tune data collection granularity based on performance and security needs (e.g., selectively exclude certain file paths or processes)	Yes			
	Data Integrity: The solution must ensure collected data is tamper-proof and securely stored.	Yes			
Real-time Visibility and Alerting	Centralized Console/Dashboard: The solution must provide a single pane of glass providing a consolidated view of endpoint activity across the environment.	Yes			
	Customizable Dashboards and Visualizations: The solution must allow security analysts to create custom dashboards and visualizations to focus on specific metrics and trends.	Yes		Using PowerBI	
	Real-time Alerting: The solution must generate immediate alerts upon detection of suspicious or malicious activity.	Yes			
	Alert Prioritization and Correlation: The solution shall be able to prioritize alerts based on severity and correlate related events to provide a more complete picture of an incident.	Yes			
	Detailed Alert Information: Alerts must include the following information:				
	1. Timestamp	Yes			
	2. Affected endpoint(s)	Yes			
	3. User(s) involved.	Yes			
	4. Process (es) involved.	Yes			
	5. File(s) involved.	Yes			
	6. Network connections.	Yes			
	7. MITRE ATT&CK technique(s) mapped.	Yes			
	8. Severity level	Yes			
	Alert Notification Methods: Must support the following notification methods – Email, SIEM integration.	Yes			
	Visualizations: The solution shall offer graphical representations of data, such as process trees, network maps, and timelines, to aid in understanding complex events.	Yes			Shall deliver and issue amendment if needed.
Data Retention and Search	Configurable Data Retention Policy: Allow administrators to define data retention periods based on compliance and business requirements.	Default Data retention is 180 days. SIEM can be used for longer retention.			
	Powerful Search Capabilities: Enable security analysts to search through collected data using various criteria (e.g., keywords, timestamps, file hashes, IP addresses).	Yes			
	Advanced Search Operators and Filters: Support advanced search operators (e.g., Boolean operators, wildcards, regular expressions) and filters to refine search results.	Yes			
	Historical Analysis: Allow for retrospective analysis of past events to identify trends and patterns.	Yes			
	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Yes			
Contextual Enrichment	Threat Intelligence Integration: Enrich collected data with threat intelligence feeds to identify known malicious indicators.	Yes			
	Geographic Location: Provide geographic location information for IP addresses and network connections.	Yes			
	User and Asset Context: Correlate endpoint activity with user and asset information (e.g., user roles, department, and asset criticality).	We can integrate with Defender for Identity and Entra ID			Shall deliver and issue amendment if needed.
3.8.2	**Advanced threat detection with integrated threat intelligence**	Yes			
Detection Engines	Signature-Based Detection: Support detection method that relies on pre-defined patterns, or "signatures," to identify known malicious code. The vendor must provide regular and frequent up-to-date signature databases.	Yes			
	Behavioral Analysis: Support detection method that relies on observing the actions and activities of processes and applications on an endpoint, rather than relying on static signatures. It establishes a baseline of "normal" behavior and identifies deviations that may indicate malicious activity. The solution must be able to detect following suspicious actions using behavioral analysis:	Yes			
	• Unusual process execution.	Yes			
	• Unauthorized access to sensitive files or registry keys.	Unauthorized access to sensitive files can be detected by MIP.			
	• Network connections to known malicious IP addresses or domains.	Yes			
	• Command-and-control (C2) communication.	Yes			
	• Data exfiltration attempts	Need clarity on use cases			Use case: - detecting transfer of large volume of data over unusual external connection
	• Persistence mechanisms (e.g., creating scheduled tasks or registry run keys).	MDE maps detected behaviors to known persistence techniques, helping security teams understand how attackers are maintaining access.			
	Anomaly Detection: Support establishment of a baseline of normal endpoint behavior and identifies deviations from that baseline, to detect insider threats and other unusual activity that may not be explicitly malicious.	Yes			
	Machine Learning (ML): The solution must use statistical models trained on large datasets of both benign and malicious activity to identify anomalies and potential threats.	Yes			
Advanced Detection Capabilities	Zero-Day and Unknown Threat Detection: Zero-day threats refer to vulnerabilities or exploits that are unknown to the software vendor or the security community. Similarly, "unknown threats" encompass malware or attack techniques that have not been previously observed or catalogued. The solution must be able to detect zero-day and unknown threats, using techniques that focus on behavior, anomalies, and contextual analysis.	Yes			
	Dynamic Analysis in Sandboxes: The solution must have sandboxing capability to execute and analyse suspicious files or processes can be executed in a controlled environment (sandbox). The solution must have cloud-based sandbox, without the need for any on-premises compute resources.	Yes	Run Microsoft Defender Antivirus in a sandbox environment - Microsoft Defender for Endpoint | Microsoft Learn		
	Memory Scanning: The solution must be able to scan endpoint memory for malicious code and artifacts.	Yes	Automating investigation and response for memory-based attacks | Microsoft Community Hub		
	Rootkit Detection: The solution must be able to detect rootkits that attempt to hide their presence from the operating system.	Yes	Rootkits - Microsoft Defender for Endpoint | Microsoft Learn		
	Exploit Detection: The solution must be able to detect attempts to exploit software vulnerabilities.	Yes	Turn on exploit protection to help mitigate against attacks - Microsoft Defender for Endpoint | Microsoft Learn		
	Fileless Malware Detection: The solution must be able to detect malware that operates entirely in memory without writing files to disk.	Yes	Automating investigation and response for memory-based attacks | Microsoft Community Hub		
	Living-off-the-Land (LotL) Detection: The solution must be able to detect malicious use of legitimate system tools and processes.	Yes	Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV | Microsoft Security Blog		
Correlation and Contextualization	Event Correlation: Correlates related events from diverse sources (endpoints and servers in the scope of the solution) to provide a more complete picture of an incident.	Yes	Alert correlation and incident merging in the Microsoft Defender portal - Microsoft Defender XDR | Microsoft Learn		
	MITRE ATT&CK Framework Mapping: Maps detected activity to the MITRE ATT&CK framework to provide a standardized understanding of attacker tactics and techniques.	Yes	View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn		
Custom Rules and Detection Logic	Customizable Detection Rules: Allow security analysts to create custom detection rules based on specific organizational needs and threat profiles.	Yes	https://learn.microsoft.com/en-us/defender-xdr/custom-detection-rules		
	YARA Rule Support: Must support YARA rules for custom malware detection.	Please clarify why YARA rules are required. MDE uses Kusto Query language for customer detection.			Shall deliver and issue amendment if needed.

Feedback and Tuning	False Positive Management: Provides mechanisms for managing and reducing false positives.	Yes	Address false positives/negatives in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint	Microsoft Learn	
	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	Yes			
Threat Intelligence Integration	Integration with Threat Intelligence Feeds: The solution must be able to incorporate threat intelligence from various sources (e.g., commercial feeds, open-source intelligence, internal threat intelligence).	Yes	Microsoft Defender for Endpoint - Microsoft Defender for Endpoint	Microsoft Learn	
	Indicator of Compromise (IOC) Matching: Must be able match collected endpoint data against known IOCs (e.g., file hashes, IP addresses, domains) to identify known threats.	Yes			
	Contextual Enrichment: Must be able to provide context to detected threats by correlating them with threat intelligence data.	Yes			
	Threat Intelligence Subscription provided by the OEM: The solution must be integrated with active subscription to Threat Intelligence Subscription/feed provided by the OEM of the EDR solution.	Yes			
Next-Generation Antivirus (NGAV)	The EDR solution shall include Next-Generation Antivirus (NGAV) capabilities, providing comprehensive protection against known and unknown malware. The NGAV component shall utilize signature-based scanning, behavioural analysis, and machine learning-based detection to prevent, detect, and block malicious activity. The NGAV component shall also include exploit prevention capabilities to block common exploit techniques.	Yes	Overview of next-generation protection in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint	Microsoft Learn	
3.8.3	**Automated Incident Response and Remediation**				
Automated Containment	Endpoint Isolation: Immediately disconnect an infected endpoint from the network to prevent lateral movement and further spread of malware.	Yes	Take response actions on a device in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint	Microsoft Learn	
	Process Termination: Automatically terminate malicious processes to prevent them from executing further actions.	Yes	https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alert		
	File Quarantine: Moves suspicious or malicious files to a secure quarantine location, preventing them from being executed or accessed.	Yes			
	User Account Lockdown: Temporarily disables or locks user accounts that have been compromised. The solution shall be able to lockdown both local and Active Directory Users. The solution may employ multiple methods to achieve user account lockdown for Active Directory users, like direct AD integration using APIs (Application Programming Interfaces) provided by Active Directory or using management tools (to be offered and integrated by the bidder). The bidder shall provide full details on how this functionality shall be achieved.	Yes	Take response actions on a device in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint | Microsoft Learn		Shall deliver and issue amendment if needed.
Automated remediation	Malware Removal: Automatically removes malware and other malicious artifacts from infected endpoints.	Yes			
	Registry Remediation: Reverts malicious changes made to the Windows Registry.	Remove registry			Shall deliver and issue amendment if needed.
Response Orchestration and Automation	Automated Response Playbooks: Allow security teams to create predefined response playbooks that automate a series of actions based on specific triggers or events. These playbooks can be customized to handle several types of incidents.	Yes			
	Conditional Logic and Branching: Support conditional logic within playbooks, allowing for different actions to be taken based on specific conditions (e.g., severity of the threat, type of endpoint, privilege level of the user).	Yes	Partial with MDE, XDR/Sentinel for full branching		Shall deliver and issue amendment if needed.
	IoC and IoA Blocklists: Automatically block known Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) based on threat intelligence.	Yes	Overview of indicators in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint | Microsoft Learn		
	API and Scripting Support: Provide APIs and scripting capabilities to enable custom integrations and automation.	Yes			
	Exclusion Lists: Allow administrators to create exclusion lists to prevent automated actions from being taken on specific endpoints or applications.	Yes			
	Detailed Logging of Automated Actions: Log all automated actions taken by the EDR solution, providing an audit trail for incident investigations.	Yes			
	Notifications and Alerts: Provide notifications and alerts to security teams when automated responses are triggered.	Yes			
	Post-Incident Analysis: Automatically generate reports summarizing detected threats, responses, and remediation actions.	Yes			
3.8.4	**Incident Investigation and Forensics**				
Comprehensive Data Collection and Storage	Detailed Event Logging: The solution must collect and store detailed logs of endpoint activity. For details of data to be collected, refer to Real-time endpoint monitoring, visibility, and activity logging.	Yes			
	Centralized Data Repository: Collected data must be stored in a cloud hosted centralized repository for efficient analysis and correlation. The vendor must allocate sufficient storage for the Centralized Data Repository, to meet the following data retention requirements: 1. For Critical Endpoints – 90 days, for a maximum of 500 such endpoints. 2. For Non-critical Endpoints – 90 days, for a maximum of 3500 such endpoints Note: When OIL enhances the EDR coverage to additional endpoints, storage shall also be enhanced by the vendor on pro-rata basis.	Since it's a SaaS solution, there is no challenge on storage allocation of logs for upto 180 days.			
	Data Integrity and Tamper-Proofing: Ensure the integrity of collected data to prevent tampering and maintain its admissibility as evidence.	Yes			
Log Management Philosophy	OIL will follow a hybrid model w.r.t endpoint log management. EDR solution shall be used for real-time detection, investigation, and response: The EDR solution retains logs for a shorter period (30-90 days depending on the type of endpoint as mentioned above) to facilitate rapid analysis and incident response.	Yes	Microsoft Defender for Endpoint data storage and privacy - Microsoft Defender for Endpoint | Microsoft Learn		
	Critical logs are forwarded to a SOC/SIEM for long-term retention and correlation: This will enable SOC/SIEM to provide centralized visibility, compliance reporting, and the ability to detect threats that may span multiple security domains.	Yes			
Search and Filtering	Advanced Search Operators: Support for Boolean operators (AND, OR, NOT), wildcards, regular expressions, and other advanced search operators to refine search queries.	Yes			
	Timeline Analysis: Ability to visualize events on a timeline to understand the sequence of events during an incident.	Yes			
	Filtering and Sorting: Ability to filter and sort data based on various criteria, such as timestamps, user accounts, file names, IP addresses, and process names.	Yes			
Data Analysis and Visualization Tools	Process Tree Visualization: Graphical representation of process relationships to understand the origin and propagation of malicious activity.	Yes	Overview of endpoint detection and response capabilities - Microsoft Defender for Endpoint | Microsoft Learn		
	Network Connection Mapping: Visualizing network connections to identify communication with malicious IP addresses or domains.	Yes			
	File Analysis: Tools for analysing files, including viewing file metadata, examining file contents (where possible), and calculating file hashes.	Yes			
	Registry Analysis: Tools for examining registry keys and values to identify malicious modifications.	Yes			
	Memory Analysis: Capabilities for capturing and analysing memory dumps to identify malicious code or artifacts in memory.	Yes	Partial only, need to be integrated with forensic tool		Shall deliver and issue amendment if needed.
Reporting and Documentation	Evidence Export: Ability to export data and reports in various formats for sharing with other teams or for legal proceedings.	Yes			
3.8.5	**Threat Hunting**				
Behavioral Indicators of Attack (BIOA) and Tactics, Techniques, and Procedures (TTP) Mapping	The solution shall provide pre-built detections and rules that map to known attacker TTPs as defined in frameworks like MITRE ATT&CK to allow threat hunters to proactively search for specific attack techniques, such as lateral movement, privilege escalation, and data exfiltration.	Yes	MITRE ATT&CK Techniques now available in the device timeline | Microsoft Community Hub		
Interactive Shell and Live Response	The solution shall provide capability that allows threat hunters to remotely connect to endpoints and perform real-time investigations. This includes the ability to: • Execute commands on the endpoint. • Collect files and memory samples.	Yes	Investigate entities on devices using live response in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint | Microsoft Learn		
3.9	**Security & Compliance**				
Data Security and Privacy	Data Encryption (in transit and at rest): All data transmitted between the EDR agent, on-premises components, and the cloud platform must be encrypted using strong encryption protocols (TLS 1.2 or higher). Data stored at rest, both on endpoints and in centralized storage, must also be encrypted.	Microsoft stores this data securely in Microsoft Azure and maintains it in accordance with Microsoft privacy practices and Microsoft Trust Center policies			
	Data Minimization and Control: The solution should allow for granular control over the types of data collected from endpoints, enabling minimization of the collection of sensitive data.	Information collected by Defender for Endpoint includes file data (file names, sizes, and hashes), process data (running processes, hashes), registry data, network connection data (host IPs and ports), and device details (device identifiers, names, and the operating system version).			Shall deliver and issue amendment if needed.
	Data Residency: All data collected, processed, transmitted, and stored by the EDR solution, including but not limited to logs, telemetry, alerts, forensic artifacts, metadata, and any backups or replicas thereof, relating to endpoints located within India, shall remain exclusively within the geographical boundaries of India. No data shall be transferred, accessed, or processed outside of India, even for support, maintenance, troubleshooting, or disaster recovery purposes.	Defender for Endpoint operates in the Microsoft Azure data centers in the European Union, the United Kingdom, the United States, Australia, Switzerland, or **India**. Customer data collected by the service might be stored in: (a) **the geo-location of the tenant as identified during provisioning** or, (b) the geo-location as defined by the data storage rules of an online service if this online service is used by Defender for Endpoint to process such data.			
	Access Control and Authentication: The solution must have access control and authentication mechanisms - multi-factor authentication and RBAC (role-based access control) for access to the EDR solution.	Yes			
	Audit Logging and Trail: Comprehensive audit logging shall track all actions performed within the EDR solution, providing a clear audit trail for compliance audits and investigations.	Yes			
3.10	**Integration Capabilities**				
Security Information and Event Management (SIEM)	Real-time Event Streaming: The solution shall be able to stream real-time event data (alerts, logs, telemetry) to the SIEM. This allows SIEM to do correlation of endpoint activity with other security events from network devices, firewalls, intrusion detection systems, and other sources.	Defender for Endpoint supports SIEM integration through out of the box connectors, and APIs.			
	Enriched Data: The solution must enrich the data sent to the SIEM with context, such as MITRE ATT&CK mappings, threat intelligence information, and endpoint details.	Defender for Endpoint supports SIEM integration through out of the box connectors, and APIs.			
	EDR-SIEM Integration Method: The solution must support the following two integration methods:				
	1. Using syslog protocol: Send security events and logs to a SIEM solution using the syslog protocol.	Defender for Endpoint supports SIEM integration through out of the box connectors, and APIs.			
	2. Using Common Event Format (CEF): Send richer data to the SIEM, including event types, severity levels, and other relevant information.	Defender for Endpoint supports SIEM integration through out of the box connectors, and APIs.			
	Action Execution (Command and Control): The EDR solution shall provide APIs for SOAR solution to execute actions on endpoints. These actions can include:				
	Endpoint isolation/containment.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			

Security Orchestration, Automation, and Response (SOAR)	Process termination.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
	File quarantine/deletion.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
	Retrieving files or memory samples.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
	Running custom scripts.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
	Alerting and Event Notification: The EDR solution shall provide API-Driven Integration that allows the SOAR platform to subscribe to real-time alerts and events. When the EDR detects something suspicious, it sends a notification to the SOAR platform via the API.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
	Secure Communication: All communication between the SOAR platform and the EDR should be encrypted and authenticated to ensure security.	Orchestration solutions can help build playbooks and integrate the rich data model and actions that Defender for Endpoint APIs exposes to orchestrate responses, such as query for device data, trigger device isolation, block/allow, resolve alert and others.			
Threat Intelligence Platforms (TIPs)	Automated IOC Ingestion: The solution should be able to automatically ingest IOCs (Indicators of Compromise) from TIPs to enhance detection capabilities.	Yes			
	Diverse IOC Types: The solution should be able to ingest a wide range of IOCs from the TIP, including:	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	· File hashes (SHA-1, SHA-256)	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	· IP addresses	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	· Domains and URLs	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	· YARA rules	Please clarify why YARA rules are required. MDE uses Kusto Query language for customer detection.			Shall deliver and issue amendment if needed.
	Flexible Ingestion Methods: The solution should support various ingestion methods, such as:	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	STIX/TAXII: These are standardized formats for exchanging threat intelligence data.	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	APIs: The EDR can use APIs to directly retrieve IOCs from the TIP.	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
	File Imports: The EDR can import IOCs from files (e.g., CSV, JSON)	Defender for Endpoint allows you to integrate with threat-intelligence providers and aggregators to maintain and use indicators of compromise (IOCs)			
Active Directory (AD)	User and Group Context Enrichment:				
	1. The solution should be able to identify the logged-in user for each endpoint event, providing valuable context for investigations.	Can be achieved with Defender for Identity			
	2. Group Membership: The solution should be able to retrieve user group memberships from AD. This allows for:	Can be achieved with Defender for Identity			
	a.Applying different security policies based on user roles and privileges.	Can be achieved with Defender for Identity			
	Identifying potential privilege escalation attacks.	Can be achieved with Defender for Identity			
	Understanding the impact of a compromised account.	Can be achieved with Defender for Identity			
	3. Organizational Unit (OU) Information: The solution should be able to retrieve OU information for endpoints. This allows for:	Can be achieved with Defender for Identity			
	A.Applying different security policies based on organizational structure.	Can be achieved with Defender for Identity			
	b.Filtering and grouping endpoints based on their OU.	Can be achieved with Defender for Identity			
	Automated Account Lockdown: The solution shall be able to automate the lockdown of compromised user accounts in Active Directory. This is a critical capability for containing security incidents quickly.	Can be achieved with Defender for Identity			Shall deliver and issue amendment if needed.
Cloud Workloads	The EDR agent must be deployable on endpoints running within Public Cloud environment. Such endpoints must be able to integrate with the EDR solution.	Need Clarity. Are these endpoints on VDI or these are servers hosted on cloud			These are servers hosted on cloud.
Endpoint Operating System (OS)	The EDR solution shall be supported on endpoints running the following OS:				
	1. Microsoft Windows (Currently supported PC and Server versions)	Yes			
	2. Linux (RHEL 8 and higher)	Yes			
	3. Apple mac OS (Sonoma (14) and higher)	Yes. three most recent major releases of macOS are supported (Currently support on Sequoia, Sonoma, Ventura)			
3.11	**Operational Requirements**				
Agent Deployment	Automated Deployment and Uninstallation Methods: Shall support the following automated deployment and uninstallation methods to minimize manual effort:				
	Group Policy Object (GPO) deployment (for Windows environments).	Yes			
	Software distribution tools (Microsoft Intune, Ansible/Chef/Puppet).	Yes			
	Script-based deployment.	Yes			
	Silent Installation: Must be able to deploy agents silently without requiring user interaction.	Yes			
	Deployment Monitoring and Reporting: Provide mechanisms for monitoring the deployment process and generating reports on deployment status.	Yes			
	Staged Rollouts: Support for staged rollouts to minimize disruption to business operations.	Yes			
Agent Updates	Automated Updates: Automatic agent updates to ensure endpoints are always running the latest version with the latest features and bug fixes.	Yes			
	Scheduled Updates: Ability to schedule updates to minimize disruption to business operations.	Need clarity. Is it Agent update or Signature update			Signature updates.
	Bandwidth Control: Mechanisms to control bandwidth usage during updates to avoid network congestion.	Need clarity. Is it Agent update or Signature update			Signature updates.
	Update Validation: Mechanisms to validate updates before deployment to prevent issues.	Need clarity. Is it Agent update or Signature update			Signature updates.
Threat Updates (Detection Content)	Automated Updates: Automated and frequent updates of threat detection content (signatures, behavioral rules, machine learning models) to ensure protection against the latest threats.	Yes			
	Frequency of Updates: Minimum once in 24 hours.	Yes			
	Update Validation: Mechanisms to validate updates before deployment.				
Handling Network Disconnections	Offline Functionality: The EDR agent shall continue to function and collect data even when disconnected from the network or management console.	Defender for Endpoint works in disconnected environment through proxy server.	https://learn.microsoft.com/en-us/defender-endpoint/configure-environment?view=o365-worldwide		
	Local Data Storage: The EDR agent shall store collected data locally during disconnections and transmit it to the management console when connectivity is restored.	Defender for Endpoint works in disconnected environment through proxy server.	https://learn.microsoft.com/en-us/defender-endpoint/configure-environment?view=o365-worldwide		
	Local Detection Capabilities: The EDR agent must maintain some level of local detection capabilities (e.g., using cached signatures or behavioral rules) during disconnections.	Defender for Endpoint works in disconnected environment through proxy server.	https://learn.microsoft.com/en-us/defender-endpoint/configure-environment?view=o365-worldwide		
	Alert Queuing: The EDR agent shall queue alerts generated during disconnections and transmit them to the management console when connectivity is restored.	Defender for Endpoint works in disconnected environment through proxy server.	https://learn.microsoft.com/en-us/defender-endpoint/configure-environment?view=o365-worldwide		
Case/Ticket Management	The EDR solution will have in-built capability for case/ticket management to track the status and progress of alerts/incidents/service requests. OR The EDR solution must be integrated using APIs with OIL's existing ITSM tool.	Can be integrated using APIs			
3.12	**Backup & Recovery**				
Data to be Backed Up	Configuration Settings: This includes all settings related to policies, detection rules, response playbooks, integrations, user accounts, and other configurations within the EDR management console.	SaaS solution, so should not be required			
	Detection Content: This includes signature databases, behavioral rules, machine learning models, and other detection logic used by the EDR.	SaaS solution, so should not be required			
	Operational Data (Metadata): This includes data related to agent deployments, system logs, audit trails, and other operational information about the EDR infrastructure.	Can be done with SIEM			
	Database (If Applicable): If the EDR uses a dedicated database for storing configuration or operational data, this database must be backed up.	SaaS solution, so should not be required			
	Endpoint event logs and alerts	Can be done with SIEM			
Disaster Recovery Planning	The vendor must submit the disaster recovery plan for the EDR solution as part of the project deliverable.	SaaS solution, so should not be required			

Deployment Architecture						OIL's Responses
Sl No	**Page No**	**Feature**	**Description**	**Compliance**	**Request to Change**	
Real-time endpoint monitoring, visibility, and activity logging						
1	86	Continuous Data Collection	The solution must continuously collect data on all endpoint activity, including: 1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes). 2. Process Activity: Process creation, termination, parent-child relationships (process lineage/ancestry), command-line arguments, loaded modules/DLLs. 3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns). 4. Registry Activity: Registry key creation, modification, deletion, value changes. 5. User Activity: Logons, logoffs, account changes, privilege escalations. 6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration. 7. Memory Activity: Memory access, modifications, memory dumps (for advanced analysis). 8. Hardware and Software Inventory: Tracking installed software, hardware configurations. 9. WMI Activity: Monitoring Windows Management Instrumentation queries and executions. 10. Scheduled Tasks: Monitoring creation, modification, and execution of scheduled tasks. 11. PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	Request to change:	Request to change: The solution must continuously collect data on all endpoint activity, including: 1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes). 2. Process Activity: Process creation, termination, parent-child relationships (process lineage/ancestry), command-line arguments, loaded modules/DLLs. 3. Network Activity: Network connections (inbound and outbound), protocols, ports, IP addresses, domains, URLs, HTTP/HTTPS traffic (where possible, without decryption concerns). 4. Registry Activity: Registry key creation, modification, deletion, value changes. 5. User Activity: Logons, logoffs, account changes, privilege escalations. 6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration. 7. Memory Activity: Memory access, modifications. 8. Hardware and Software Inventory: Tracking installed software, hardware configurations. 9. WMI Activity: Monitoring Windows Management Instrumentation queries and executions. 10. Scheduled Tasks: Monitoring creation, modification, and execution of scheduled tasks. 11. PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	Clarified in the pre bid conference. Shall deliver and issue amendment if needed.
2	86	Real-time Visibility and Alerting	Visualizations: The solution shall offer graphical representations of data, such as process trees, network maps, and timelines, to aid in understanding complex events.	Request to change:	Request to change: Visualizations: The solution shall offer graphical representations of data, such as process trees, and timelines, to aid in understanding complex events.	Shall deliver and issue amendment if needed.
3	87	Data Retention and Search	Advanced Search Operators and Filters: Support advanced search operators (e.g., Boolean operators, wildcards, regular expressions) and filters to refine search results.	Request to change:	Request to change: The solution should support advanced search and filtering capabilities to refine results.	No change
4	87	Data Retention and Search	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Request to change:	Request to change: Data Export: Provide options for exporting data in various formats (e.g., CSV, PDF) for further analysis and reporting.	Shall deliver and issue amendment if needed.
5	87	Contextual Enrichment	Geographic Location: Provide geographic location information for IP addresses and network connections.	Request to change:	Request to change: The solution should provide enriched threat intelligence for IP addresses and network connections, including parameters such as IP reputation, threat category, domain risk score, malware association	No change
6	87	Contextual Enrichment	User and Asset Context: Correlate endpoint activity with user and asset information (e.g., user roles, department, asset criticality).	Request to change:	Request to change: User and Asset Context: Correlate endpoint activity with users.	Shall deliver and issue amendment if needed.
Advanced threat detection with integrated threat intelligence						
7	88	Advanced Detection Capabilities	Dynamic Analysis in Sandboxes: The solution must have sandboxing capability to execute and analyse suspicious files or processes that can be executed in a controlled environment (sandbox). The solution must have cloud-based sandbox, without the need for any on-premises compute resources.	Request to change:	Request to change: Dynamic/ Manual Analysis in Sandboxes: The solution must have sandboxing capability to execute and analyse suspicious files or processes that can be executed in a controlled environment (sandbox). The solution must have cloud-based sandbox, without the need for any on-premises compute resources.	No change
8	89	Custom Rules and Detection Logic	YARA Rule Support: Must support YARA rules for custom malware detection.	Request to change:	Request to change: Must support YARA/manual rules for custom malware detection.	Shall deliver and issue amendment if needed.
9	89	Threat Intelligence Integration	Integration with Threat Intelligence Feeds: The solution must be able to incorporate threat intelligence from various sources (e.g., commercial feeds, open-source intelligence, internal threat intelligence).	Request to change:	Request to change: The solution should also support and utilize its own OEM threat intelligence platform for enriched detection and response.	No change
3.8.3 Automated Incident Response and Remediation						
10	90	Automated Containment	User Account Lockdown: Temporarily disables or locks user accounts that have been compromised. The solution shall be able to lockdown both local and Active Directory Users. The solution may employ multiple methods to achieve user account lockdown for Active Directory users, like direct AD integration using APIs (Application Programming Interfaces) provided by Active Directory or using management tools (to be offered and integrated by the bidder). The Contractor shall provide full details on how this functionality shall be achieved.	Request to change:	Request to change: The solution should support monitoring of user accounts, including both local and Active Directory users.	Shall deliver and issue amendment if needed.
11	90	Automated remediation	Registry Remediation: Reverts malicious changes made to the Windows Registry.	Request to change:	Request to change: The solution should support remediation of malicious changes made to the Windows Registry through behavioral detection and rule-based response actions.	Shall deliver and issue amendment if needed.

12	90	Response Orchestration and Automation	Conditional Logic and Branching: Support conditional logic within playbooks, allowing for different actions to be taken based on specific conditions (e.g., severity of the threat, type of endpoint, privilege level of the user).	Request to change:	Request to change: Conditional Logic and Branching: Support conditional logic within playbooks, allowing for different actions to be taken based on specific conditions (e.g., severity of the threat, type of endpoint).	Shall deliver and issue amendment if needed.
13	90	Response Orchestration and Automation	IoC and IoA Blocklists: Automatically block known Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) based on threat intelligence.	Request to change:	Request to change: Automatically block known Indicators of Compromise (IoCs) based on threat intelligence.	No change
14	90	Response Orchestration and Automation	API and Scripting Support: Provide APIs and scripting capabilities to enable custom integration and automation.	Request to change:	Request to change: The solution should support integration pre-configured connectors.	No change
3.8.4 Incident Investigation and Forensics						
15	91	Log Management Philosophy	OIL will follow a hybrid model w.r.t endpoint log management. EDR solutions shall be used for real-time detection, investigation, and response: The EDR solution retains logs for a shorter period (30- 90 days depending on the type of endpoint as mentioned above) to facilitate rapid analysis and incident response. Critical logs are forwarded to a SOC/SIEM for long-term retention and correlation: This will enable SOC/SIEM to provide centralized visibility, compliance reporting, and the ability to detect threats that may span multiple security domains.	Request to change:	Request to change: OIL will follow a hybrid/cloud model w.r.t endpoint log management. EDR solutions shall be used for real-time detection, investigation, and response: The EDR solution retains logs for a shorter period (30- 90 days depending on the type of endpoint as mentioned above) to facilitate rapid analysis and incident response. Critical logs are forwarded to a SOC/SIEM for long-term retention and correlation: This will enable SOC/SIEM to provide centralized visibility, compliance reporting, and the ability to detect threats that may span multiple security domains.	No change
16	91	Search and Filtering	Advanced Search Operators: Support for Boolean operators (AND, OR, NOT), wildcards, regular expressions, and other advanced search operators to refine search queries.	Request to change:	Request to change: The solution should support search and filtering capabilities to refine results.	No change
17	92	Data Analysis and Visualization Tools	Memory Analysis: Capabilities for capturing and analysing memory dumps to identify malicious code or artifacts in memory.	Request to change:	Request to change: The solution should support detection of in-memory threats.	Shall deliver and issue amendment if needed.
Threat Hunting						
18	93	Interactive Shell and Live Response	This includes the ability to: • Execute commands on the endpoint. • Collect files and memory samples.	Request to change:	Request to change: This includes the ability to: • Execute commands on the endpoint.	No change
3.9 Security & Compliance						
19	94	Security Orchestration, Automation, and Response (SOAR)	Action Execution (Command and Control): The EDR solution shall provide APIs for SOAR solution to execute actions on endpoints. These actions can include: • Endpoint isolation/containment. • Process termination. • File quarantine/deletion. • Retrieving files or memory samples. • Running custom scripts.	Request to change:	Request to change: Action Execution (Command and Control): The EDR solution shall provide APIs for SOAR solution to execute actions on endpoints. These actions can include: • Endpoint isolation/containment. • Process termination. • File quarantine/deletion.	No change
20	94	Security Orchestration, Automation, and Response (SOAR)	Alerting and Event Notification: The EDR solution shall provide API- Driven Integration that allows the SOAR platform to subscribe to real- time alerts and events. When the EDR detects something suspicious, it sends a notification to the SOAR platform via the API.	Request to change:	Request to change: The proposed EDR solution should provide real-time alerting and event notification through its native console.	No change
21	94	Security Orchestration, Automation, and Response (SOAR)	Secure Communication: All communication between the SOAR platform and the EDR should be encrypted and authenticated to ensure security.	Request to change:	Request to change: The solution must have an inbuilt/external SOAR module that securely handles alerting, event correlation, and automated response workflows.	No change
22	95	Threat Intelligence Platforms (TIPs)	Diverse IOC Types: The solution should be able to ingest a wide range of IOCs from the TIP, including: • File hashes (SHA-1, SHA-256) • IP addresses • Domains and URLs • YARA rules	Request to change:	Request to change: Diverse IOC Types: The solution should be able to ingest a wide range of IOCs from the TIP, including: • File hashes (SHA-1, SHA-256) • IP addresses • Domains and URLs	No change
23	95	Threat Intelligence Platforms (TIPs)	Flexible Ingestion Methods: The solution should support various ingestion methods, such as: • STIX/TAXII: These are standardized formats for exchanging threat intelligence data. • APIs: The EDR can use APIs to directly retrieve IOCs from the TIP. • File Imports: The EDR can import IOCs from files (e.g., CSV, JSON)	Request to change:	Request to change: Flexible Ingestion Methods: The solution should support various ingestion methods, such as: • APIs: The EDR can use APIs/MISP to directly retrieve IOCs from the TIP. • File Imports: The EDR can import IOCs from files (e.g., CSV)	Shall deliver and issue amendment if needed.
Integration Capabilities						
24	95	Active Directory (AD)	User and Group Context Enrichment: 1. The solution should be able to identify the logged-in user for each endpoint event, providing valuable context for investigations. 2. Group Membership: The solution should be able to retrieve user group memberships from AD. This allows for: a. Applying different security policies based on user roles and privileges. b. Identifying potential privilege escalation attacks. c. Understanding the impact of a compromised account. 3. Organizational Unit (OU) Information: The solution should be able to retrieve OU information for endpoints. This allows for: a. Applying different security policies based on organizational structure. b. Filtering and grouping endpoints based on their OU.	Request to change:	Request to change: User and Group Context Enrichment: 1. The solution should be able to identify the logged-in user for each endpoint event, providing valuable context for investigations.	No change

25	95	Active Directory (AD)	Automated Account Lockdown: The solution shall be able to automate the lockdown of compromised user accounts in Active Directory. This is a critical capability for containing security incidents quickly.	Request to change:	Request to change: The proposed solution should support incident response workflows that assist in identifying compromised user accounts.	Shall deliver and issue amendment if needed.
3.12 Backup & Recovery:						
26	97	Data to be Backed Up	Configuration Settings: This includes all settings related to policies, detection rules, response playbooks, integrations, user accounts, and other configurations within the EDR management console.	No	Requesto to remove this clause	No change
27	97	Data to be Backed Up	Detection Content: This includes signature databases, behavioural rules, machine learning models, and other detection logic used by the EDR.	No	Requesto to remove this clause	No change
28	97	Data to be Backed Up	Operational Data (Metadata): This includes data related to agent deployments, system logs, audit trails and other operational information about the EDR infrastructure.	No	Requesto to remove this clause	No change
29	97	Data to be Backed Up	Database (If Applicable): If the EDR uses a dedicated database for storing configuration or operational data, this database must be backed up.	No	Requesto to remove this clause	No change

Queries from M/s. SIFY

ANNEXURE-Z

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
1	3.8 Core Features 3.8.1	86	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	Creation, modification, deletion and renaming is not possible but if it is malicious then creation is possible. We are assuming that we are discussing about the "Malicious file" system activity here. Please confirm our understanding.	Since this is not FIM solution. So, it should monitor the suspected or malicious file activity only.	Shall deliver and issue amendment if needed.
2	3.8 Core Features 3.8.1	86	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	Only if 'malicious' then domain, IP and URL Hash is possible. Assuming we are discussing about the "Malicious network" system activity here. Please confirm our understanding.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
3	3.8 Core Features 3.8.1	86	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	Applicable only for malicious activity. Assuming we are discussing about the "Malicious driver & service" system activity here. Would request OIL to confirm our understanding.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
4	3.8 Core Features 3.8.1	86	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Please note that hardware inventory is not possible because it requires very high compute infra. Would request OIL to amend the specification / requirement accordingly.	Individual hardware inventory can be seen but all hardware inventory can not be seen together.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
5	3.8 Core Features 3.8.1	86	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	The specification / requirement is applicable only if it is malicious and matched with MITRE or if the Powershell & Linux shell command & Scripts are malicious then then only it will be detected. Please confirm our understanding.	The purpose of the solution is to identify the malicious powershell & Linux shell commands.	No change
6	3.8 Core Features 3.8.1	87	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	For wider participation we would request OIL to amend the specification / requirement as suggested here: Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV formats.	For promoting wider participation.	Shall deliver and issue amendment if needed.
7	3.8 Core Features 3.8.1	87	Geographic Location: Provide geographic location information for IP addresses and network connections.	Please note that the IP location will be provided but not in graphical mode.	For clarification of the product feature.	No change
8	3.8 Core Features 3.8.2	89	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	Please elaborate the requirement is greater detail so as to help us understand the requirement and context correctly.	Further clarification is required for better understanding of the requirement.	In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.
10	Additional Clause			We would request OIL to add the below suggested specification / requirement for procuring the best in class solution: The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.	Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the organization's cyber health.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
11	Additional Clause			We would request OIL to add the below suggested specification / requirement for procuring the best in class solution: The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score	Without prioritization it would be very tough to bring down the risk score.	No change
12	Deployment Architecture, Components	51	On-Premises Communication Server/Relay: This is the bare minimum on-premises component. Its primary function is to act as a communication relay or proxy for Type-2 endpoints that cannot directly reach the cloud. On Premises Communication Server/Relay shall be deployed by the Contractor in highly available manner in OIL's FHQ in Duliajan.	We understand that the solution involves deployment of an On-Premises Service Gateway at Duliajan FHQ. In this context, we seek clarification on the following bandwidth requirements: A minimum of 10 Mbps dedicated MPLS bandwidth at Duliajan FHQ for the On-Premises Service Gateway. A minimum of 20 Mbps dedicated Internet bandwidth at Duliajan FHQ for the Service Gateway to establish connectivity with the cloud. A minimum of 2 Mbps dedicated MPLS bandwidth from each remote location (where Type-2 endpoints are deployed) to the centrally placed Service Gateway at Duliajan FHQ. Please confirm if the above understanding of bandwidth requirements is correct, or provide the exact specifications as per the solution scope.	To deploy the solution in the Hybrid manner as suggested in RFP to support all 4000 Endpoints.	Clarified in the pre bid conference

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
13	Disaster Recovery Planning	64	The Contractor must submit the disaster recovery plan for the EDR solution as part of the project deliverable.	We request clarification on whether the requirement is applicable to the On-Premises Service Gateway component deployed at Duliajan FHQ for supporting Type-2 Endpoints. If yes, kindly confirm the Disaster Recovery (DR) location that should be considered for this component as part of the deployment architecture.	To deploy the solution as per the suggested RFP point.	Clarified in the pre bid conference
14	3 Information about OIL's ICT Infrastructure	84	3.6 Summary of endpoints and network connections: The following table summarizes the approximate user and device count along with network bandwidth in each of the OIL's offices:	Please provide the details of dedicated Bandwidth assigned for Endpoint Agents.	Details required for designing the solution architecture accordingly.	Clarified in the pre bid conference
15	3.7 Deployment Architecture	84	2. Sensitive endpoints without Internet access (Type-2): These endpoints do not have Internet access but have Network Connectivity to Internal corporate network.	Please provide the location wise count of type 2 devices that needs to be covered under this project.	Required for designing the solution architecture accordingly.	Clarified in the pre bid conference
16	3.11 Operational Requirements	96	Agent Deployment Agent Updates	We would request OIL to kindly confirm if all the end-points that needs to be covered in this EDR project are under Active Directory or not. If not, then please provide the location wise count of end-points which are not under Active Directory.	Scope clarity required for planning the deployment & monitoring approach.	Clarified in the pre bid conference

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
17	4 Detailed Scope of Work	98	Provisioning of required compute resources at OIL's premises at FHQ, Duliajan	We understand that the successful bidder has to provide only the required compute resources and all other IT and / or non-IT requirements necessary for the successful deployment of the solution at OIL's premise such as storage, switches, cables, uninterrupted power etc. would be provided by OIL . Please confirm our understanding.	Scope clarity.	Clarified in the pre bid conference
18	4.1 Project Timeline	98	Provisioning of required compute resources at OIL's premises at FHQ, Duliajan - D+60 days Training - D+60 days Pre-Deployment Planning - D+90 days Installation and Commissioning - Agent Deployment, On- Premises Infrastructure Deployment, Integration, Configuration, Acceptance Testing - D + 120 days	In view of the size and complexity of the project we would request OIL to kindly extend the delivery timelines as suggested below: Provisioning of required compute resources at OIL's premises at FHQ, Duliajan - D + **90** days Training - D + **120** days Pre-Deployment Planning - D + **120** days Installation and Commissioning - Agent Deployment, On- Premises Infrastructure Deployment, Integration, Configuration, Acceptance Testing - D + **150** days	For addressing the complexity and geographical spread of the project.	No change
19	30.0 TIMELY MOBILIZATION AND LIQUIDATED DAMAGES:	58	. . . shall recover from the CONTRACTOR, as an ascertained and agreed Liquidated Damages, a sum equivalent to @ 0.5% of contract value including mobilization cost, per week or part thereof of delay subject to maximum of 7.5% of the Contract Price.	We would request OIL to kindly revise the maximum capping of the LD charges to a maximum of **5%** of the Contract Price of the undelivered portion of the project. Please confirm the acceptance of the request.	To align with the industry standard practice for similar projects.	No change

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Response
20	5.4 Managed Services	102	Mode of Delivery: The Contractor shall deliver administration, monitoring, and management services for the EDR solution to OIL through a secure remote mechanism.	We understand that OIL would provide the necessary secure remote mechanism / connectivity at all locations required for delivering services. Please confirm our understanding.	Scope clarity for providing remote services.	Clarified in the pre bid conference
21	5.4.2 Non-performance deductions for SLA violations:	106	1. Maximum penalty for non-performance deduction in a quarter shall not exceed 07% of the total Quarterly Service Fee.	We would request OIL to kindly amend the maximum capping of the penalty charges as suggested below: Maximum penalty for non-performance deduction in a quarter shall not exceed **5%** of the total Quarterly Service Fee.	To align with the industry standard for similar projects.	No change
22	6 Payment Term	116 & 117	EDR Subscription Charges for 4000 endpoints - Quarterly EDR Subscription Charges for one Endpoint for one month -	We would request OIL to kindly amend the payment terms for the subscription charges and make it "Annual in Advance".	To align with the payment terms of the OEMs.	Shall deliver and issue amendment if needed.

Queries from M/s. SISL							ANNEXURE-Z
Sl. No	**Page No**	**Clause No**	**Clause header**	**Clause details as in RFP**	**Query/Clarification Required**	**Justification/Reason for changes required (If any)**	**OIL's Responses**
NA	121 of 209	1	Payment terms	As per Bill of Quantities - Sl. No. 1 to 6. The payment terms is - One-time charges towards Exit Management (item#3) shall not be less than 5% of the total fixed charges component of the solution (F). In case, quoted rate is less than 5%, the differential amount will be kept on hold from the 1st invoice onwards and the same will be paid at the end of the contract, after successful completion of the exit management activities.	The current payment structure outlines fixed quarterly disbursements. We kindly request that the terms be amended to allow for 100% payment release for all BoQ line items upon delivery and acceptance.	As a bidder, our payment terms with the OEM involve 100% payment upon deployment. This means the bidder must bear the financing cost, as payment to the OEM is made upfront, while project payments are received over a 5-year period. This financing gap imposes a significant cost burden on the bidder, ultimately inflating the overall bid price. As a result, this increased cost would reflect in the project expenditure, thereby impacting **public funds**. Therefore, we request that the payment terms be amended to allow for upfront payments to the bidder, with the PBG (which may be set at a higher percentage) serving as a security deposit.	Shall deliver and issue amendment if needed.

Queries from M/s. Trelix						ANNEXURE-Z
S.NO	**Page No**	**Section /clause No**	**Content of the RFP Requiring clarification**	**Clarification sought**	**Justification**	**OIL's Responses**
1	52	3.8.1/8	Hardware and Software Inventory: Tracking installed software, hardware configurations	**Request to remove this clause**	As this is part of inventory management solution and not scope of EDR Solution to track hardware and software changes	No change. Clarified in the pre bid conference.
2	52	3.8.1/Real-time visibility and Alerting	Centralized Console/Dashboard: The solution must provide a single pane of glass providing a consolidated view of endpoint activity across the environment	**Change clause to below** The solution must provide a single/dual pane of glass providing a consolidated view of endpoint activity across the environment	As lot of functionlaity has been asked in the endpoint security scope hence it is requested consider dual console for broader participation	No change. Clarified in the pre bid conference.
3	53	3.8.1/Contextual enrichment	User and Asset Context: Correlate endpoint activity with user and asset information (e.g., user roles, department, asset criticality).	**Request to remove this clause**	As this is more specific to SIEM Solution and NOT EDR and most of industry EDR will not be able to fulfill this hence removing this will allow broader Participation	Shall deliver and issue amendment if needed.
4	56	3.8.3/Response Orchestration and Automation	Automated Response Playbooks: Allow security teams to create predefined response playbooks that automate a series of actions based on specific triggers or events. These playbooks can be customized to handle several types of incidents.	**Request to remove this clause**	As playbook creation is part of SOAR Solution and it is a separate solution not part of EDR hence it is requested to put it under SOAR section for broader participation	No change. Clarified in the pre bid conference.
5	57	3.8.3/Response Orchestration and Automation	Conditional Logic and Branching: Support conditional logic within playbooks, allowing for different actions to be taken based on specific conditions (e.g., severity of the threat, type of endpoint, privilege level of the user).	**Request to remove this clause**	As playbook creation is part of SOAR Solution and it is a separate solution not part of EDR hence it is requested to put it under SOAR section for broader participation	Shall deliver and issue amendment if needed.
6	62	3.10/Integration capabilities	Automated Account Lockdown: The solution shall be able to automate the lockdown of compromised user accounts in Active Directory. This is a critical capability for containing security incidents quickly.	**Request to remove this clause**	Account lockout is a domain admin priviledge activity and it cannot be triggered using EDR it nneds to be done using Domain controller	Shall deliver and issue amendment if needed.

Queries from M/s. Trend Micro						ANNEXURE-Z
Sl. No.	**Section Details from the RFP**	**Page No.**	**Details Mentioned in the RFP**	**Clarification / Change Requested by Bidder**	**Justification for Clarifications Sought**	**OIL's Responses**
1	3.8.1 -1	52	1. File System Activity: File creation, modification, deletion, renaming, execution, access (reads, writes).	creation,modification, deletion and renaming can not possible but if it malicious then creation is possible/ Assuming we are talking about the "Malicious file" system activity here.	First of all this is not FIM solution. So it should monitor the suspected or malicious file activity only.	No change
3	3.8.1 - 3	52	3. Network Activity: Network connections (inbound and outbound), protocols (TCP, UDP, ICMP, etc.), ports, IP addresses, domains, URLs, DNS queries, HTTP/HTTPS traffic (where possible, without decryption concerns).	only malicious then domain, IP and URL, Hash is possible/ Assuming we are talking about the "Malicious network" system activity here.	This solution is not full fledged NDR which will look after the entire details of network activity. The proposed solution should look after the malicious network activity conducted/performed by a specific endpoint.	No change
6	3.8.1 - 6	52	6. Driver and Service Activity: Driver loading, unloading, service start, stop, changes in service configuration.	only malicious activity/ Assuming we are talking about the "Malicious driver & service" system activity here.	The proposed solution should be smart enough to look after the suspected DLLs or malicious DLLs.	No change
8	3.8.1 - 8	52	8. Hardware and Software Inventory: Tracking installed software, hardware configurations.	Hardware inventory is not possible because it required high compute.	Individual Hardware inventory can be seen but all hardware inventory can not be seen togather.	No change
11	3.8.1 - 11	52	PowerShell and Linux command terminal Activity: Logging PowerShell commands, Linux shell commands and scripts executed.	If it is malicious and matched with MITRE/ If the Powershell & Linux shell command & Scripts are malicious then then only it will be detected.	The purpose of the solution is to identify the malicious powershell & linux shell commands.	No change
13	Real-time endpoint monitoring, visibility, and activity logging	53	Data Export: Provide options for exporting data in various formats (e.g., CSV, JSON) for further analysis and reporting.	Data can be exported in CSV from multiple areas & Report can be generated in PPT, PDF, CSV Formats		Shall deliver and issue amendment if needed.
14	Contextual Enrichment	53	Geographic Location: Provide geographic location information for IP addresses and network connections.	The IP location will be given but not in graphical mode		No change
15	Feedback and Tuning	55	Feedback Loops: Incorporates feedback from security analysts to improve detection accuracy.	need more clarity		In an EDR solution, feedback loops mean that input from security analysts (e.g., marking alerts as true or false positives) is fed back into the system. This helps the EDR refine its detection logic, reduce false positives, and improve accuracy over time by learning from real-world analyst decisions. Clarified in the pre-bid conference.

Sl. No.	Section Details from the RFP	Page No.	Details Mentioned in the RFP	Clarification / Change Requested by Bidder	Justification for Clarifications Sought	OIL's Responses
16	Recommendation		The proposed solution should show aggregated dynamic risk score as a timeline view along with individual dynamic risk score of endpoint assets.		Individual RISK score is required to track an individual asset over the time period. Same as aggregated RISK score is also required to identify the ogranization's cyber health.	No change
17	Recommendation		The proposed solution should provide prioritization based on RISK to achieve lower organizational RISK score		This is super important point. Without prioritization it would be very tough to bring down the risk score.	No change
18	2.1.3	23	The EDR OEM or the Solution Provider must have experience of providing managed EDR services in any PSU / Central Government / State Government/ Government Department or Organization / Nationalized Banks/Public Limited Company using the proposed EDR solution to whom they are currently providing the service for at least one year in the previous five (05) years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** - It may be Email confirmation. **Providing Managed EDR services –** Request you to consider the PO name as Managed EDR, Managed XDR, or Managed SOC with XDR/EDR, as they all refer to the same scope of services being offered or more than that.	Trend Micro, as an OEM, offers both Managed EDR/XDR as well as Managed SOC-as-a-Service. As per our understanding, you are seeking Managed Services for the proposed EDR solutions in line with the technical specifications. However, the terminology for "Managed EDR" may vary across different Purchase Orders depending on the organization's RFP title. For example, it may appear as: •Managed XDR (MXDR) •Managed SOC with XDR (which includes Managed EDR/XDR services along with Managed SOC services, and	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the clause-2.1.3. Clarified in the pre-bid conference.
19	2.1.4	23	The OEM or Solution Provider must be providing MSS in India continuously during the last 03 years reckoned from the original bid closing date of this tender.	**Completion certificate(s) issued by the client(s)** – Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the renewal Purchase Order(s) as evidence to substantiate the continuity and delivery of the Managed Service.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an ongoing basis, we can provide the	The bidder shall submit documentary evidence to substantiate the experience requirement as mentioned in the clause-2.1.4. Clarified in the pre-bid conference.
	2.1.8 - B	24	Proof of requisite Experience, viz. award and subsequent successful execution/completion of 'SIMILAR WORK' (refer Clause No. 2.1.1 above), must be substantiated by submission of the following documents along with the bid:	**Job Completion Certificate showing –** we can provide the mail for On boarding for this Manage Service and product implementation certificate for the proposed EDR solutions.	As this engagement relates to a Managed Service and not a one-time product installation, it is a continuous process and activity rather than a project with a defined end date. Accordingly, a Completion Certificate can only be issued for the product implementation. For Managed Services, since most of our customers continue to renew and extend the service on an	Clarified in the pre-bid conference. Also, ita may be noted that BEC/PQC Clause No. 2.1.8(b) pertains to "An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that OIL's data shall never move outside India for any purpose."