TP Central Odisha Distribution Limited | TP Nothern Odisha Distribution Limited | TP Southern Odisha Distribution Limited | TP Western Odisha Distribution Limited

CENTRALIZED CONTRACTS GROUP

NIT No.: TPCODL/CCG/24-25/1000002320

Corrigendum No. – I

Dt.: 24-04-2025

Tender Enquiry No- TPCODL/CCG/24-25/1000002320

Tender Subject – Purchase Order (PO) for Supply of Extended Detection and Response (XDR) License for Endpoints & Servers including 04 year Warranty and Support under TPCODL, TPNODL, TPSODL and TPWODL

Corrigendum Summary:

A] Clause 1.3: Revised Calendar of Event shall be as follows:

Existing Clause	Proposed Clause
Due Date of Posting Consolidated replies to all the pre-bid queries as received - 1**6.04.2025, 18:00 Hours**	*Revised time line 25.04.2025, 11:00 Hours*
Due date and time of receipt of Bids – **25.04.2025, 17:00 Hours**	*Revised time line 02.05.2025, 17:00 Hours*

NOTE : All Other Terms & Conditions of the tender shall remain unchanged as per NIT document, GCCs and Pre-bid reply.

Approved By,

Sd/-
(**Head – Centralized Contracts Group**)

FORMAT F.1	Format for Query / Clarification / Deviation (QCD)				
Tender No	NIT No.: TPCODL/CCG/2024-25/1000002320				
Package Name	Purchase Order (PO) for Supply of Extended Detection and Response (XDR) License for Endpoints & Servers including 04 year				
Note :	The said format to be used only for any Pre-bid Query / Clarifiaction/ Deviation on any of the Tender documents				
Sr. No.	**Detailed Reference to concerned Document . Please specify Document No / Clause No / Page No**	**Description as per Bid Document**	**Remarks**	**Query / Clarification / Deviation**	**TP Odisha Discom's Reponse**
1	Technical Requirement for "XDR for Endpoints & Servers Page 32 Clause 1	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on- premises or hybrid, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software, and licenses.	Sir ,The Specification asked prohibits vendor participation and favours a specific OEM hence request you to allow the changes as mentioned	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on-premises/ hybrid/cloud, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software, and ..	**Tender Clause remain same**
2	Page 32 Clause 7	Provide an account criticality score for both domain and service account. Account's criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Provide an incident criticality on the basis of severity. Administrators should be able to manually change the status of the incident as suspicious, false positive or true positive	**Tender Clause remain same.** This given point is supported by other OEMs too. This is called User behaviour check. The point remains the same
3	Page 32 Clause 9	The solution should assign a score on each workbench insight calculated based on a number of criteria including the overall impact scope of all related alerts	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	The solution should assign a severity (low, medium or high) of each incident and should provide a visual graph of related incidents	**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same. Workbench is not at all a keyword of specific.
4	Page 32 Clause10	The solution should display the list of alerts associated with an insight and perform actions such: - Change Findings to update the progress of alerts or investigations - Associate with Insight to associate the selected alerts with the specified insight - Remove from Insight to unlinked an alert from an insight - Execute Playbook to execute Automated Response playbooks for the specified alerts.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute Automated Response for the specified alerts.	**Tender Clause can be read as follows:** The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute
5	Page 32 Clause 12	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs and identify the severity of incident for related assets.	**Tender Clause remain same.** "scope of impact across assets" means how many assets are impacted with a specific incident. It is the generic feature of Impact assessment.

6	Clause 16	Ability to execute SQL queries using osquery to obtain system information on the specified endpoints.	The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Ability to execute queries to obtain system information on the specified endpoints.	**Tender Clause read as follows:** **Ability to execute SQL queries/adnvanced quary like (indicators "if", "and" ,"or", "join","then", "where",ifelse" etc...) and combination of advance serach option should be available to obtain system information on the specified**
7	Clause 21	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX and TAXII.	The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX or TAXII or API	**Tender Clause remain same.**
8	Clause 22	The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns and Threat Actors.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	The solution must collect, organize, and provide an up-to-date information resource for active Threat Intelligence and Threat Actors.	**Tender Clause remain same.** **The Bidder may propose additional advanced features.**
9	Clause 23	Threat Campaign must include information such as Threat Actor profile, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Threat Campaign must include information such as Threat Information, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Incident Severity.	**Tender Clause remain same.** In XDR "impact scope" refers to the assessment of how a detected threat or incident affects an organization's assets, data, systems, and operations. It helps determine the extent of the potential damage and inform incident response strategies. Generic term
10	Clause 24	Campaign Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Threat Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.	**Tender Clause remain same.** **The Bidder may propose additional advanced features.**
11	Clause 32	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the severity of the assets.	**Tender Clause remain same.** Both are same. "identify the severity of the assets" for the said infection means Scope of impact.
12	Clause 38	Must have mapping with threat actors and risk prioritization.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	Must have mapping with Mitre TTPs and provide incident severity priority (low,medium,high)	**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same. Proper MITRE mapping will give the name of threat actors.
13	Clause 39	Historical behavior analysis	considered historical behavior as threat history via threat intelligence.	Considered historical behavior as threat history via threat intelligence.	**Tender Clause remain same.** Every behaviour will not match with threat behaviour, but if you have the behaviour history then you can come to conclution by analyzing the threshold
14	Page 33 Clause 45	The solution should be tested for vulnerabilities by CERT-In empaneled auditor prior to moving into production	bidder to do auditing via CERT_IN empanelled auditor . Out of OEM scope.	Bidder to do auditing via CERT_IN empanelled auditor . Out of OEM scope.	**Tender Clause can be read as below:** **Pre production vulnerability Testing of the solution by CERT-In empaneled auditor is under Bidder scope**

15	Page 32Clause 1	1.Does TATA power has Active directory through which all agent will be pushed to endpoints.			Each DISCOM has own separate AD in place and operational. The agent deployment in all endpoints and any further financial implecations falls under Bidder scope within given timeline
16	2.0 Pre- Qualification Criteria	2. XDR management server will install at one location or at each DISCOM separately.			XDR management server will install at each DISCOM separately.
17	13.0 Post Award Contract Administration/ 13.1 Special Conditions of Contract - **B. Financial Pre-Qualification Requirements/ Sl No. 2/ Experience**	The bidder should have executed similar works / cyber security for a single order value of Rs. 5 Cr. or Rs. 10 Cr. for cumulative orders (Maximum 5 orders) during the last 3 years. Copy of work order / completion certificate to be submitted in this regard.	Kindly amend "The bidder/ **OEM** should have **supply order of 50000 nodes in the last 3 years** in any of the state/central/PSU or Govt departments. Copy of work order / completion certificate to be submitted in this regard."		**Tender Clause remains same.**
18	2.0 Pre- Qualification Criteria - Delivery Period - A. Technical Pre-Qualification Requirements/ Sl No. a/ Technical Experience / Performance	The devices/Solution should be delivered within 1 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution).	Kindly amend "The devices/Solution should be delivered within **3 to 4** weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution)."		**Tender Clause read as follows:** ***The devices/Solution should be delivered within 2 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution).***
19	2.0 Pre- Qualification Criteria - A. Technical Pre-Qualification Requirements/ Sl No. e/ Technical Experience / Performance	The offered solution against the supply order shall be latest version and should not be end of life for next 5 years, however if any product which is declared end of life product by OEM during the supply period of material, in this case the tenderer should supply replaced model or next higher model/version of the Product/solution	OEM should have **supply order of 50000 nodes in the last 3 years** in any of the state/central/PSU or Govt departments.		**Tender Clause remain same.**
20	Technical Requirement for "XDR for Endpoints & Servers" - Functional Requirements/ Sl No. 1	OEM should have presence in INDIA for last 8 years and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance.	Kindly amend "OEM should have presence in INDIA for **last 3 years** and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance."		The Tender clause can be read as ***OEM should have presence in INDIA for last 5 years and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance.***
21	Technical Requirement for "XDR for Endpoints & Servers" - Functional Requirements/ Sl No. 7	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on- premises or hybrid, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software, and licenses.	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on- premises/ hybrid/cloud, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software,	Sir, the Specification asked prohibits vendor participation and favours a specific OEM hence request you to allow the changes as mentioned	**Tender Clause remain same.**
22	Technical Requirement for "XDR for Endpoints & Servers" - Functional Requirements/ Sl No. 9	Provide an account criticality score for both domain and service account. Account's criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.	Provide an incident criticality on the basis of severity. Administrators should be able to manually change the status of the incident as suspicious, false positive or true positive.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** This given point is supported by other OEMs too. This is called User behaviour check. The point remains the same.

23	Technical Requirement for "XDR for Endpoints & Servers" - Functional Requirements/ Sl No. 10	The solution should assign a score on each workbench insight calculated based on a number of criteria including the overall impact scope of all related alerts	The solution should assign a severity (low, medium or high) of each incident and should provide a visual graph of related incidents	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same.
24	Technical Requirement for "XDR for Endpoints & Servers" - Functional Requirements/ Sl No. 12	The solution should display the list of alerts associated with an insight and perform actions such: - Change Findings to update the progress of alerts or investigations - Associate with Insight to associate the selected alerts with the specified insight - Remove from Insight to unlinked an alert from an insight - Execute Playbook to execute Automated Response playbooks for the specified alerts.	The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute Automated Response for the specified alerts.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause can be read as follows:** The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute
25	Technical Requirement for "XDR for Endpoints & Servers" - Response Requirements/ Sl No. 16	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs and identify the severity of incident for related assets.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** "scope of impact across assets" means how many assets are impacted with a specific incident. It is the generic feature of Impact assessment.
26	Technical Requirement for "XDR for Endpoints & Servers" - Response Requirements/ Sl No. 21	Ability to execute SQL queries using osquery to obtain system information on the specified endpoints.	Ability to execute queries to obtain system information on the specified endpoints.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause read as follows:** **Ability to execute SQL queries/adnvanced quary like (indicators "if", "and" ,"or", "join","then", "where",ifelse" etc...) and combination of advance serach option should be available to obtain system information on the specified**
27	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 22	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX and TAXII.	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX or TAXII or API.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.**
28	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 23	The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns and Threat Actors.	The solution must collect, organize, and provide an up-to-date information resource for active Threat Intelligence and Threat Actors.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** **The Bidder may propose additional advanced features.**
29	Technical Requirement for "XDR for Endpoints & Servers"	Threat Campaign must include information such as Threat Actor profile, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope.	Threat Campaign must include information such as Threat Information, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Incident Severity.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** In XDR "impact scope" refers to the assessment of how a detected threat or incident affects an organization's assets, data, systems, and operations. It helps determine the extent of the potential damage and inform incident response strategies. Generic term
30	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 24	Campaign Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.	Threat Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** **The Bidder may propose additional advanced features.**

31	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 32	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the severity of the assets	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** Both are same. "identify the severity of the assets" for the said infection means Scope of impact.
32	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 33	The solution should be certified with the following international compliance standards: - ISO 27001, ISO 27014, ISO 27034-1, ISO 27017, SOC 2/3	The solution should be certified with the following international compliance standards: - ISO 27001/ ISO 27014/ISO 27034-1/ISO 27017/SOC 2/3		**Tender Clause remain same.**
33	Technical Requirement for "XDR for Endpoints & Servers" - Threat Intelligence Requirements/ Sl. No. 38	Must have mapping with threat actors and risk prioritization.	Must have mapping with Mitre TTPs and provide incident severity priority (low,medium,high)	Sir, The specification asked mentions keywords of a specific OEM hence request you to generalise the specification as mentioned	**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same. Proper MITRE mapping will give the name of threat actors.
34	Technical Requirement for "XDR for Endpoints & Servers"- Threat Intelligence Requirements/ Sl. No. 39	Historical behavior analysis		considered historical behavior as threat history via threat intelligence.	**Tender Clause remain same.** Every behaviour will not match with threat behaviour, but if you have the behaviour history then you can come to conclution by analyzing the threshold
35	Technical Requirement for "XDR for Endpoints & Servers"Threat Intelligence Requirements/ Sl. No. 45	The solution should be tested for vulnerabilities by CERT-In empaneled auditor prior to moving into production		bidder to do auditing via CERT_IN empanelled auditor . Out of OEM scope.	**Tender Clause can be read as below:** **Pre production vulnerability Testing of the solution by CERT-In empaneled auditor is under Bidder scope**
36	Technical Requirement for "XDR for Endpoints & Servers"Threat Intelligence Requirements/ Sl. No. 31	The solution should have the capability to create playbooks from scratch or use built-in templates. Security playbook template types should include but not limited to the following: - XDR threat investigation actions. - Automated Response Playbook - Endpoint Response Actions - Incident Response Evidence Collection	The solution should have the following capability - - - XDR threat investigation actions. - Endpoint Response Actions - Incident Response Evidence Collection	Limited capabilities with playbook, Sophos has dedicated MDR (Managed detection & response) team work tirelessly 24X7 and consists of threat researcher/analyst/Lab team provide virtual SOC response to any incident. MDR team proactively reaches out to customer SOC/Security admin and collaborate with them to stop any active threat or any incident with outmost priority. Hence, we would request you to include MDR like response capability instead of standard play book creation	**Tender Clause remain same.**

37	Technical Requirement for "XDR for Endpoints & Servers"Threat Intelligence Requirements/ Sl. No. 33	The solution should be certified with the following international compliance standards: - ISO 27001, ISO 27014, ISO 27034-1, ISO 27017, SOC 2/3	The solution should be certified with the following international compliance standards: - ISO 27001, SOC 2/3 & PCI DSS	Sophos XDR, as a cybersecurity solution, aligns with industry standards and certifications to ensure robust security and compliance, including ISO 27001, SOC 2 Type 2, and PCI DSS 4.0, demonstrating its commitment to data protection and security practices.	**ISO 27001**: This is the standard for information security management systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system. **ISO 27014**: This standard focuses on information security governance. It provides guidance on the governance of information security, covering the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources needed to ensure effective governance. **ISO 27034-1**: Part of the ISO 27034 series, this standard addresses application security. It provides guidelines for integrating security into the development of software applications, ensuring that security is considered throughout the entire software development lifecycle. **ISO 27017**: This standard specifically deals with cloud security. It provides guidelines and controls for information security applicable to the provision and use of cloud services, helping organizations ensure the security of their data and operations in cloud environments. **This is**
38	Delivery Period	The devices/Solution should be delivered within 1 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation	1 week deliver and within 4 week installation can not possible please increased thedeliver time to 2-3 weeks and installation time to 90 days		**Tender Clause read as follows:** ***The devices/Solution should be delivered within 2 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder***
39	Scope of Work Delivery Time (Point no 7)	The devices/Solution should be delivered within 1 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to bidder for installation of Solution).	How the Installation will happended, It will be manual installation on every machine or remotely, also please mention you have any remote installation tool or not.		**Tender Clause read as follows:** ***The devices/Solution should be delivered within 2 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder***
40	Scope of Work ope of Work (point no 3, sl no e)	e) Complete configuration of the device to integrate with existing DC and DRC Servers, End User Systems, Azure AD, On prime AD, O365, Firewall, SIEM by OEM personal only.	For SIEM integration please mention the SIEM tool, we required the help from SIEM OEM also.		**Accepted.** **We will Provide the deatails prior the installation**
32	Technical Specification Point No-27	The solution should allow a SOC analyst to manually add iOSsuch as File Hashes, IP Addresses, Domains, and URL's as part of the custom intelligence.	It should be IOC. It's a typo error. Please correct it		**Tender Clause can be read as :** **The solution should allow a SOC analyst to manually add IOC such as File Hashes, IP Addresses, Domains, and URL's as part of the**

32	Technical Specification Point No-30	The solution must support Windows, Linux, and macOS endpoints and servers, and be compatible with integration into existing **TPSODL** Endpoint EDR, Azure AD, on-premises AD, 0365, as well as network and security solutions.	It should be TPSODL, TPCODL, TPNODL, TPWODL		Accepted . The modified Tender Clause will be as follows: ***The solution must support Windows, Linux, and macOS endpoints and servers, and be compatible with integration into existing TPCODL,TPNODL,TPWODL & TPSODL Endpoint EDR, Azure AD, on-premises AD, 0365, as well as***
33	Technical Specification Point No-45	The solution should be tested for vulnerabilities by CERT-In empaneled auditor prior to moving into production.	Who will test and Certified? "Please remove the point because no one will give any access of the system." our proposed solutions is already SOC-2 / 3 compliant		**Tender Clause can be read as below:** **Pre production vulnerability Testing of the solution by CERT-In empaneled auditor is under Bidder scope**
33	Technical Specification Point No-46	Solution Provider must share SLA for Incident response and vulnerability closure timeline Solution provider to share Security patching frequency	Please need to discuss.		**Tender Clause remain same.**
33	Technical Specification Point No-47	The proposed solution **should not be developed**, hosted, or operated by entities based out of country of prior reference.	Please remove the red marked portion		**Tender Clause remain same.** The modified Tender Clause will be as follows: ***The proposed solution should not be developed, hosted, or operated by entities based out of country of prior reference.Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance.***
34	SOW	Complete configuration of the device to integrate with existing DC and DRC Servers, End User Systems, Azure AD, On prime AD, O365, Firewall, SIEM by OEM personal only.	Physical onsite installation for all the endpoints is not possible. Installation can be done from TPCODL, TPSODL, TPWODL and TPNODL's Head Office only, it will be done online by remote installation tools, and it needs your cooperation.		**Tender Clause can be read as follows:** The entire activity falls under Bidder Scope. Complete configuration of the device to integrate with existing DC and DRC Servers, End User Systems, Azure AD, On prime AD, O365, Firewall, SIEM by OEM/Bidder personal only. Physical presence of OEM/Bidder personal should be mandatory for the solution implementation & production integration.
34	Delivery Timeline	The devices/Solution should be delivered within 1 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to bidder for installation of Solution).	Request you to amend this clause as "**The solution should be delivered within 2 weeks from order issuance date."** and Timeline of the installation also depends on the availability of the Endpoint systems, where we need your help		**Tender Clause read as follows:** ***The devices/Solution should be delivered within 2 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution).***
32	Technical Requirement for "XDR for Endpoints & Servers" - Point 17	Submit selected file or object for automated analysis in a sandbox, a secure virtual environment.	Clarification required on the specific requirements, intended use cases, and expectations related to the sandbox functionality		**Will be discussed prior installation.**
32	Technical Requirement for "XDR for Endpoints & Servers" - Point 1	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on-premises or hybrid, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software, and licenses	Please suggest if the proposed solution could be completely SAAS based with logging and management from MeitY compliant DC in India		**Tender Clause remain same**

32	Technical Requirement for "XDR for Endpoints & Servers" - Point 29	The solution must support multi-session VDI solutions without changing or limiting the functionality of your virtual desktop operating systems	Clarification required on the specific requirements, scope, and expected use cases for the VDI environment		Information will be shared prior installation
33	Technical Requirement for "XDR for Endpoints & Servers" - Point 34	The solution must be able to integrate with common SIEM and SOAR products and should be able to produce manual and scheduled reports that can be customized to display company information and logo and send it to specified email recipients.	Clarification required on below points: - What's the existing SIEM being used today ? - Is the SOC is managed inhouse or third party? - Do you have any SOAR tool for workflow automation? If yes please share the details		Quarries will be discussed and informed prior installation.
33	Technical Requirement for "XDR for Endpoints & Servers" - Point 45	The solution should be tested for vulnerabilities by CERT-In empaneled auditor prior to moving into production	Please suggest - would SOC2 report helps as it attests to the various security controls including vulnerability management program employed for the respective solution.		**Tender Clause can be read as below:** **Pre production vulnerability Testing of the solution by CERT-In empaneled auditor is under Bidder scope.**
			Kindly help us with the product versioning and licensing details of the currently deployed Endpoint Security solution		Will be shared prior installation
			Please suggest Would there be any exclusive component, connector, version upgrade required from existing end point vendor for it to integrate with other XDR solutions than its own		Will be shared prior installation
			Kindly help understand apart from end point what other security telemetry sources or security vectors expected to be integrated with the XDR platform		Will be shared prior installation
			Duration of Log retention expected 90 Days/180 Days/360 Days		Duration of Log retention should be 180 Days as per CERT-IN guidline
2.0 Pre-Qualification Criteria	B. Financial Pre-Qualification Requirements/ Sl No. 2/ Experience	The bidder should have executed similar works / cyber security for a single order value of Rs. 5 Cr. or Rs. 10 Cr. for cumulative orders (Maximum 5 orders) during the last 3 years. Copy of work order / completion certificate to be submitted in this regard.	Kindly amend "The bidder/ **OEM** should have **supply order of 50000 nodes in the last 3 years** in any of the state/central/PSU or Govt departments. Copy of work order / completion certificate to be submitted in this regard."		**Tender Clause remains same.**
13.0 Post Award Contract Administration/ 13.1 Special Conditions of Contract	Delivery Period	The devices/Solution should be delivered within 1 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution).	Kindly amend "The devices/Solution should be delivered within **3 to 4** weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution)."		**Tender Clause read as follows:** ***The devices/Solution should be delivered within 2 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (The client will intimate date to bidder for installation of Solution).***
2.0 Pre-Qualification Criteria	A. Technical Pre-Qualification Requirements/ Sl No. a/ Technical Experience / Performance	The offered solution against the supply order shall be latest version and should not be end of life for next 5 years, however if any product which is declared end of life product by OEM during the supply period of material, in this case the tenderer should supply replaced model or next higher model/version of the Product/solution	OEM should have **supply order of 50000 nodes in the last 3 years** in any of the state/central/PSU or Govt departments.		**Tender Clause remain same.**

2.0 Pre-Qualification Criteria	A. Technical Pre-Qualification Requirements/ Sl No. e/ Technical Experience / Performance	OEM should have presence in INDIA for last 8 years and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance.	Kindly amend "OEM should have presence in INDIA for **last 3 years** and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center compliance."		**Accepted .** The Modified Tender Clause will be ***OEM should have presence in INDIA for last 5 years and OEM should have TAC Support center and Data Storage Center based out of India only. It should comply to MeitY Cloud Data Center***
Technical Requirement for "XDR for Endpoints & Servers"	Functional Requirements/ Sl No. 1	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on- premises or hybrid, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software, and licenses.	The solution should offer a holistic approach to security with purpose-built XDR. The deployment should be on- premises/ hybrid/cloud, but the proposed solution's data center should be located in India, as per MeitY guidelines. The bidder can propose the solution inclusive of the required hardware, associated OS, software,		**Tender Clause remain same.**
Technical Requirement for "XDR for Endpoints & Servers"	Functional Requirements/ Sl No. 7	Provide an account criticality score for both domain and service account. Account's criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.	Provide an incident criticality on the basis of severity. Administrators should be able to manually change the status of the incident as suspicious, false positive or true positive.		**Tender Clause remain same.** This given point is supported by other OEMs too. This is called User behaviour check. The point remains the same.
Technical Requirement for "XDR for Endpoints & Servers"	Functional Requirements/ Sl No. 9	The solution should assign a score on each workbench insight calculated based on a number of criteria including the overall impact scope of all related alerts	The solution should assign a severity (low, medium or high) of each incident and should provide a visual graph of related incidents		**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same.
Technical Requirement for "XDR for Endpoints & Servers"	Functional Requirements/ Sl No. 10	The solution should display the list of alerts associated with an insight and perform actions such: - Change Findings to update the progress of alerts or investigations - Associate with Insight to associate the selected alerts with the specified insight - Remove from Insight to unlinked an alert from an insight - Execute Playbook to execute Automated Response playbooks for the specified alerts.	The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute Automated Response for the specified alerts.		**Tender Clause can be read as follows:** The solution should display the list of alerts associated with an incident and perform actions such as: - Change Findings to update the progress of alerts or investigations. - Categorise alerts on the basis of severity so that they can be prioritized. - Execute Playbook/workflows to execute Automated Response for the specified alerts.
Technical Requirement for "XDR for Endpoints & Servers"	Functional Requirements/ Sl No. 12	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs and identify the severity of incident for related assets.		**Tender Clause remain same.** "scope of impact across assets" means how many assets are impacted with a specific incident. It is the generic feature of Impact assessment.
Technical Requirement for "XDR for Endpoints & Servers"	Response Requirements/ Sl No. 16	Ability to execute SQL queries using osquery to obtain system information on the specified endpoints.	Ability to execute queries to obtain system information on the specified endpoints.		**Tender Clause read as follows:** **Ability to execute SQL queries/adnvanced quary like (indicators "if", "and" ,"or", "join","then", "where",ifelse" etc...) and combination of advance serach option should be available to obtain system information on the specified**

Technical Requirement for "XDR for Endpoints & Servers"	Response Requirements/ Sl No. 21	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX and TAXII.	The solution should allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX or TAXII or API.		**Tender Clause remain same.**
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 22	The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns and Threat Actors.	The solution must collect, organize, and provide an up-to-date information resource for active Threat Intelligence and Threat Actors.		**Tender Clause remain same.** **The Bidder may propose additional advanced features.**
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 23	Threat Campaign must include information such as Threat Actor profile, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope.	Threat Campaign must include information such as Threat Information, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Incident Severity.		**Tender Clause remain same.** In XDR "impact scope" refers to the assessment of how a detected threat or incident affects an organization's assets, data, systems, and operations. It helps determine the extent of the potential damage and inform incident response
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 24	Campaign Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.	Threat Intelligence Data must include - Intelligence Reports, TTPs, Tools, Malicious Software Used, Associated CVEs, and Indicators.		**Tender Clause remain same.** **The Bidder may propose additional advanced features.**
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 32	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the severity of the assets.		**Tender Clause remain same**. Both are same. "identify the severity of the assets" for the said infection means Scope of impact.
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 33	The solution should be certified with the following international compliance standards: - ISO 27001, ISO 27014, ISO 27034-1, ISO 27017, SOC 2/3	The solution should be certified with the following international compliance standards: -ISO 27001, SOC 2/3 & PCI DSS		**Tender Clause remain same.**
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 38	Must have mapping with threat actors and risk prioritization.	Must have mapping with Mitre TTPs and provide incident severity priority (low,medium,high)		**Tender Clause remain same.** An asset can be a user, a laptop, a IP anything. Here Risk prioritization should be calculated which user is using the asset/laptop & the asset i.e. laptop has any exploitable vulnerability or not. Both should be reflected. Only laptop OS vulnerability will not work here. So the point remains the same. Proper MITRE mapping will give the name of threat actors.
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 39	Historical behavior analysis			**Tender Clause remain same.** Every behaviour will not match with threat behaviour, but if you have the behaviour history then you can come to conclution by analyzing the threshold
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 45	The solution should be tested for vulnerabilities by CERT-In empaneled auditor prior to moving into production			**Tender Clause can be read as below:** **Pre production vulnerability Testing of the solution by CERT-In empaneled auditor is under Bidder scope**

Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 31	The solution should have the capability to create playbooks from scratch or use built-in templates. Security playbook template types should include but not limited to the following: - XDR threat investigation actions. - Automated Response Playbook - Endpoint Response Actions - Incident Response Evidence Collection	The solution should have the following capability - - - XDR threat investigation actions. - Endpoint Response Actions - Incident Response Evidence Collection		**Tender Clause remain same.**
Technical Requirement for "XDR for Endpoints & Servers"	Threat Intelligence Requirements/ Sl. No. 33	The solution should be certified with the following international compliance standards: - ISO 27001, ISO 27014, ISO 27034-1, ISO 27017, SOC 2/3	The solution should be certified with the following international compliance standards: - ISO 27001, SOC 2/3 & PCI DSS		**Tender Clause remain same.**