TENDER FOR THE SUPPLY, DELIVERY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE SUPPORT SERVICES FOR MCMC MANAGED SECURITY SERVICES

Tender No: MCMC/SITD/MNSD(01)/MSS_2023/TC/09/2023(04)

Questions & Answers

Tender Requirements

No.	Question	Answer
1	Referring to the tender requirements, item 3.1 , is it a must with Syarikat Bumiputera to be the tender submission party? We are MOF certified but not Syarikat Bumiputera. The tenderer shall provide proof of valid **Sijil Akuan Pendaftaran Syarikat Bumiputera** issued by the Ministry of Finance registration with the following Kod Bidang, Kepala, and Sub Kepala. Desired Kod Bidang, Kepala, and Sub Kepala related to the tender are as follows: **210105** - Telecommunication / networking-supply product, infrastructure, services including maintenance (LAN / WAN / Internet/wireless/ satellite); and ·**210107** - ICT Security and firewall, encryption, PKI and antivirus	As explained during the tender briefing, the Bumiputera requirement is not a mandatory requirement, and you can participate in this tender.
2	Upon vetting through the document/requirements we noticed that this tender is only open to Bumiputera companies (as in point 3.1 of the tender document) with an ASP license (as in point 8.3.1 (iii) d). This being the case, please be informed that we will be partnering with another company for this tender bid exercise, a Bumiputera company with an ASP License	As explained during the tender briefing, the Bumiputera requirement is not a mandatory requirement, and you can participate in this tender. Kindly be informed that the requirement of ASP license is NOT a compulsory requirement for this tender and will not disqualify you to participate in this tender
3	May I know either this tender is only eligible for Bumiputera company?	As explained during the tender briefing, the Bumiputera requirement is not a mandatory requirement, and you can participate in this tender.

No.	Question	Answer
4	We would like to seek some clarification as per below: **Section 2: Clause 8.3.1 (iii)(d): Certified true copy of a valid Application Service Provider (ASP) license**. Is this a compulsory requirement and tenderer without ASP license are not qualified to participate?	Kindly be informed that the requirement of ASP license is NOT a compulsory requirement for this tender and will not disqualify you to participate in this tender

Technical Questions

No.	Question	Answer
1	SOAR 1. Can MCMC confirm if the deployment requires On-Prem or Cloud SaaS? 2. If it is Cloud SaaS, will MCMC accept SaaS instance in SEA region? Requirement "Be hosted in the country for cloud deployment model. Any hosting outside of the region will not be accepted;" states in country however hosting can be in the region.	SOAR 1. The solution can be hosted on-prem or Cloud SaaS depending on the proposal. 2. If SaaS Solution, it can be hosted anywhere.
2	FW 1. Log retention – how many years? 2. Network connection to switch– 1g/10g?	FW 1. Minimum 2 years 2. 10G
3	SOC Monitoring Firewall logs, got requirement to keep how long?	SOC Monitoring Minimum 2 years
4	What is the current percentage of internet gateway traffic?	75%.
5	Is it possible for MCMC to share with us the brand for the current IPS/AV?	Not possible.
6	Does MCMC need the Load balancer feature in NGFW?	No. MCMC does not require the load balancer feature in NGFW.
7	Does MCMC have enough resources to host SOAR/EDR in their existing server/ environment?	Yes.

No.	Question	Answer
8	Does MCMC have an existing Threat Intel Platform (TIP)? If no, do we require to quote it in - as per Section 43.2.1, (b)2?	Yes, but we would like to consolidate the features into the NGFW.
9	Does MCMC have any requirement for customized automation use cases or the out-of-the-box use cases (phishing / alert and event triage) is sufficient for now?	Tenderer to propose the solutions.
10	Section 43.2.1, (b)1 what are the customer's existing solutions for integration? please specify: a) AD (Microsoft) b) DLP & web security (Forcepoint) c) MFA (Cisco DUO) d) Email security (Proofpoint) e) DDOS (NSFOCUS) f) DNS security (Cisco Umbrella) g) Load balancers (layer 4 or layer 7?) h) IPS (to be replaced with new firewalls). Any others? i) Any ransomware monitoring? j) Anything other points of integration?	a) Partially. b) Yes. c) Yes. d) Yes. e) Yes. f) Yes. g) Layer 7. h) Tenderer to propose solutions. i) To include ransomware monitoring features in NGFW. j) Tenderer to propose solutions.
11	Section 42.6.4. Will the SOC on on-site at MCMC or it can be remote within Malaysia?	Tenderer to propose solutions.
12	If SOC needs to be on-site, can it use the same resource for Section 42.6.2 Resident Engineer?	Resident Engineer should be placed at MCMC as 1st level support, please refer 43.6.4. b of the Tender Document.
13	Section 42.6.4. Is there any expectations of how many staff required per 8 hour shift?	Tenderer to propose the solutions.
14	(Network) DCs and Branch Offices which are involved in this change:	Changes of hardware at DC (MCMC HQ).
15	(Network) How many subnets and vlans are involved in the change?	Approximately 900 vlan.
16	(Network) How is the client going to share the existing Firewall rules and WAF config, is a third-party tool going to be used?	Tenderer to propose on the migration plan.
17	(Network) If a third-party tool has to be used then do we need to bear the cost of the license, or will it be provided by the client?	Tenderer to propose on the migration plan.
18	(Network) How are the branch offices currently connected to the main office?	Through SD-WAN.
19	(Network) Are there currently any vdoms in use?	No.
20	(Network) Are there any NACs in use in existing infrastructure?	Yes.

No.	Question	Answer
21	(Network) Is any AD/ldap configuration required to be configured in the firewalls?	Tenderer to propose.
22	(Network) Which device is currently being used as VPN gateway for remote access VPN users?	Cisco Anyconnect.
23	(Network) 43.1.1.c (11) mentions firewalls with Vxlan capabilities. Is Vxlan alredy configured in existing infra or is there a requirement to cofigure Vxlan?	No.
24	(EDR) No of endpoints in total? No. of users? Can the solution handle this increase by approx. % from 2500 devices and 1200 users?	1200U, 2500D, increment 10% yearly.
25	(EDR) What is the current AV Solution and asset list where it is installed?	Traditional Antivirus.
26	(EDR) What is the SOAR solution in place?	As per the tender document/briefing slide, we required the tenderer to migrate and replace the current antivirus solution with EDR solution for MCMC. Tenderer to propose the migration plan.
27	(EDR) Describe EDR's key features and capabilities.	
28	(EDR) How does your solution detect and respond to endpoint threats?	
29	(EDR) Provide technical specifications of EDR solution.	
30	(EDR) Explain your approach to real-time threat intelligence and updates.	
31	(EDR) How does your EDR solution identify and prioritize threats?	
32	(EDR) Can it detect both known and unknown threats? If so, how?	
33	(EDR) Describe any machine learning or AI technologies used for threat detection.	
34	(EDR) Outline your incident response process and timeline.	
35	(EDR) What types of alerts and reports does your EDR system generate?	
36	(EDR) Can your solution automate response actions, such as isolating compromised endpoints?	
37	(EDR) List the operating systems and platforms your EDR solution supports.	
38	(EDR) Does it integrate with other security tools and systems?	
39	(EDR) Describe the ease of deployment and scalability of your solution.	
40	(EDR) Provide examples of the reports and dashboards available with your EDR solution.	
41	(EDR) How does your solution help organizations analyze and improve their security posture?	
42	(EDR) Explain how your EDR solution assists with compliance (Ex. GDPR,HIPAA).	
43	(EDR) Have you undergone any third -party audits or certifications related to security?	
44	(EDR) Share case studies or references from clients who have used your EDR	

No.	Question	Answer
	solution.	
45	(EDR) Can potential clients contact existing clients for feedback?	
46	(EDR) Detail your pricing structure and any licensing models.	
47	(EDR) Are there additional costs for support or updates?	
48	(EDR) Is there a trial or demo period available?	As per the tender document/briefing slide, we required the tenderer to migrate and replace the current antivirus solution with EDR solution for MCMC. Tenderer to propose the migration plan.
49	(EDR) Describe the support options and response times for technical issues.	
50	(EDR) Do you offer training and resources for using your EDR solution effectively?	
51	(EDR) Explain how you secure client data and prevent unauthorized access.	
52	(EDR) What data retention policies do you have in place?	
53	(EDR) Share your product roadmap and plans for future EDR features	
54	(EDR) What sets your EDR solution apart from competitors in functionality or technology?	
55	(EDR) How do you plan to adapt to emerging cybersecurity threats?	
56	(EDR) Detail your data privacy policy and compliance with data protection laws.	
57	(EDR) Provide examples of successful EDR implementations in similar industries or Organizations.	
58	(EDR) Provide information on the system's performance under heavy workloads.	
59	(EDR) Can it automatically update threat indicators and IOC's	
60	(EDR) Does your solution covers both on-premises and cloud-based endpoints?	
61	(EDR) Do we have any cloud-integration EDRs?	
62	(SIEM) No of devices to be onboarded?	We have onboarded approximatively 21 devices.
63	(SIEM) Types of logs that needs to be ingested by SIEM	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
64	(SIEM) Break up of devices: Linux, Windows, networking etc.	Networking and security devices.
65	(SIEM) Retention period of logs for Auditing/Compliance	Minimum 2 years.
66	(SIEM) EPS/Average Data size per day/week/month	Will be disclosed during project assessment.
67	(SIEM) Use case development ease.	Will be disclosed during project assessment.
68	(SIEM) Please provide an overview of your company, including its history, size, and areas of expertise.	Kindly refer to paragraph 40.1 of the Tender Document.
69	(SIEM) How long have you been offering SIEM solutions?	In use for more than 5 years.
70	(SIEM) Can you share any customer references or case studies related to SIEM implementations?	Will be disclosed during project assessment.
71	(SIEM) Describe your SIEM solution's architecture and deployment options.	Will be disclosed during project assessment.

No.	Question	Answer
72	(SIEM) What sets your SIEM solution apart from others in terms of features and capabilities?	Will be disclosed during project assessment.
73	(SIEM) Does your SIEM solution support both on-premises and cloud environments?	Currently on-premises.
74	(SIEM) Can your SIEM solution integrate with a wide range of third-party security tools and devices?	Yes.
75	(SIEM) How does your SIEM handle log and event data from various sources?	Will be disclosed during project assessment.
76	(SIEM) Explain your SIEM's alerting and notification capabilities.	Will be disclosed during project assessment.
77	(SIEM) What reporting features that your SIEM offer, and can it generate custom reports?	Will be disclosed during project assessment.
78	(SIEM) Describe the methodologies and technologies used in your SIEM for threat detection.	Will be disclosed during project assessment.
79	(SIEM) How does your SIEM facilitate incident response and forensics?	Will be disclosed during project assessment.
80	(SIEM) Can your SIEM solution scale to accommodate our organization's growth?	Yes.
81	(SIEM) What is the maximum event processing capacity of your SIEM ?	Will be disclosed during project assessment.
82	(SIEM) Does your SIEM solution assist in meeting regulatory compliance requirements?	Yes.
83	(SIEM) Can it provide predefined compliance templates or reports?	Yes.
84	(SIEM) What training and onboarding resources do you provide to help our team effectively use the SIEM?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
85	(SIEM) Describe your support and maintenance offerings?	Will be disclosed during project assessment.
86	(SIEM) How do you ensure the security and privacy of our data within your SIEM?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
87	(SIEM) What encryption and access control measures are in place?	Will be disclosed during project assessment.
88	(SIEM) Provide details on your pricing model, including licensing, subscription, and any hidden costs.	We cannot disclose any pricing.
89	(SIEM) Are there additional fees for support, updates, or consulting services?	We cannot disclose any pricing.
90	(SIEM) What key performance indicators (KPI's)can your SIEM monitor and report on?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
91	(SIEM) How can we measure the effectiveness of your SIEM in our environment?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
92	(SIEM) Please provide case studies or success stories of previous SIEM implementations.	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
93	(SIEM) Can you share references from other clients who have used your SIEM?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.

No.	Question	Answer
94	(SIEM) What enhancements or developments can we expect from your SIEM solution in the coming years?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
95	(SIEM) Share examples of real-world security incidents that your SIEM has successfully detected and mitigated?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
96	(SIEM) Outline the SLAs for response times, system availability, and issue resolution in your service contracts.	Tenderer to propose.
97	(SIEM) What is the process for migrating away from your SIEM solution if needed?	Tenderer to propose on the migration plan.
98	(SIEM) List any industry certifications or compliance standards that your SIEM solution adheres to.	Will be disclosed during project assessment.
99	(SIEM) Will you provide training to our security team to maximize the use of your SIEM?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
100	(SIEM) How does your SIEM handle security monitoring in hybrid environments (combining on-premises and cloud resources)?	Our current SIEM is on-premises.
101	(SIEM) Provide detailed information about USE CASES?	Referring to paragraph 43.2.1, we will be replacing SIEM to SOAR solution.
102	(SIEM) How will you correlate events to find real incidents?	Will be disclosed during project assessment.
103	(SIEM) Data Ingestion Process/Method	Will be disclosed during project assessment.
104	(SIEM) Data Ingestion Capacity: Per day	Will be disclosed during project assessment.
105	(SIEM) Roles and Responsibilities of a Admin & Developer.	Tenderer to propose.
106	(SIEM) Incidents response information & Updates	Will be disclosed during project assessment.
107	(SOAR) Which security tools will be integrated to SOAR, EDR, AV, SIEM, VAPT, Patching tools?	Tenderer to propose.
108	(SOAR) Can it integrate with any API? Dependency on developers?	Tenderer to propose.
109	(SOAR) Dashboard creation for KPI?	Tenderer to propose.
110	(SOAR) Scaling ability of the SOAR?	Tenderer to propose.
111	(SOAR) Please provide an overview of your organization, including its size, industry, and any unique security challenges.	Kindly refer to paragraph 40.1 of the Tender Document.
112	(SOAR) What are the organization's primary security goals and objectives?	Kindly refer to paragraph 41.1 & 41.2 of the Tender Document.
113	(SOAR) List the key security tools and systems currently in use within your organization (Ex. SIEM, IPS/IDS, Firewall, Antivirus)	Kindly refer to the Diagram 1 in the Tender Document.
114	(SOAR) Are there any security tools or systems you plan to implement in the near future?	Tenderer to propose.
115	(SOAR) What types of threats and security incidents are most relevant to your	All types of threats and security incident.

No.	Question	Answer
	organisation?	
116	(SOAR) Are there any repetitive security tasks processes you'd like to automate?	Tenderer to propose.
117	(SOAR) Which security tools and systems do you need the SOAR platform to integrate with?	To the propose and current systems.
118	(SOAR) Are there any custom applications or scripts that require integration?	Tenderer to propose.
119	(SOAR) Describe your alert handling and triage process. What criteria are used to assess the severity of alerts?	Tenderer to propose.
120	(SOAR) How quickly do you aim to respond to critical security alerts?	Tenderer to propose.
121	(SOAR) Do you have existing incident response playbooks, or do you need assistance in creating them?	Tenderer to propose.
122	(SOAR) What specific incident response workflows do you want to automate?	Tenderer to propose.
123	(SOAR) Do you require automated data enrichment of security alerts with threat intelligence feeds?	Tenderer to propose.
124	(SOAR) Are there specific threat intelligence sources you want to integrate?	Tenderer to propose.
125	(SOAR) How important is the ability to customize automation workflows and playbooks to your organisation?	Tenderer to propose.
126	(SOAR) What level of customization do you anticipate needing without extensive coding?	Tenderer to propose.
127	(SOAR) What are your scalability requirements, considering potential future growth?	Tenderer to propose.
128	(SOAR) What is the expected volume of alerts and incidents that the SOAR platform should handle?	Tenderer to propose.
129	(SOAR) Do you have any concerns regarding user adoption and usability?	Depends on the proposed solution.
130	(SOAR) What security and compliance standards or regulations does your organization need to adhere to?	MCMC ITSEC Policy.
131	(SOAR) Are there any specific compliance reporting requirements?	Depends on the proposed solution.
132	(SOAR) Do you have a budget range allocated for implementing a SOAR solution?	The budget cannot be disclosed.
133	(SOAR) Are you open to considering both on-premises and cloud-based solutions?	Yes.
134	(SOAR) What key performance indicators (KPI's) do you plan to monitor to evaluate the effectiveness of the SOAR platform?	Tenderer to propose.
135	(SOAR) Are there any specific vendor-related requirements, such as support, maintenance, or geographic location?	Kindly refer to the paragraph 43.6.4 on the Tender Document.

No.	Question	Answer
136	(SOAR) What is your desired timeline for implementing a SOAR solution?	Kindly refer to the paragraph 42.5.1 on the Tender Document.
137	(SOAR) Are there any critical milestones or deadlines to consider?	Kindly refer to the paragraph 42.5.1 on the Tender Document.
138	(SOAR) How will you measure the success of the SOAR implementation in your organization?	By monitoring the propose KPI for the features.
139	(SOAR) Do you have a process in place for gathering feedback and making improvements to your security operations?	Yes.
Internal Firewall – Port Checking Questions and Request		
140	Port configuration details: - Port type (Speed, capacity) - SFP details	Will be disclosed during project assessment.
141	Connectivity details: - How are these ports interconnected within the network? - Are there specific network diagrams illustrating the connectivity?	- Through core switch. - Kindly refer to paragraph 40.1.10 on the Tender Document.
142	Security policy information: - Are there firewall policies and security configurations associated with Fortigate ports? - Information about intrusion prevention settings (IPS)	- Yes. - Not consolidated.
143	Access to Monitoring Data - Can we access real-time or historical monitoring data for these Fortigate ports, such as bandwidth usage and threat detection?	Yes.
144	Additional question/request - Are there any other specific details or configurations related to Fortigate ports that we should be aware of?	Will be disclosed during project assessment.
145	Device location: - Current: (Inter rack/Intra rack) - Planned:	- Inter-rack - Inter-rack
146	Cables: - Verify if current cabling is enough for tech refresh (Please mention either UTP or Fiber) - Cable type (need upgrade or not?) i) Patch cord ii) Fiber optic e.g.: (SC-SC) (LC-LC) (Singlemode/Multimode)	Kindly refer to paragraph 43.3 on the Tender Document.

No.	Question	Answer
147	Device usage: - CPU - Memory - Bandwidth	Will be disclosed during project assessment.
External Firewall – Port Checking Questions and Request		
148	Port configuration details: - Port type and configurations - Port speed & any logical configurations	Will be disclosed during project assessment.
149	Connectivity details: - How are these Checkpoint ports connected within the network architecture? - Network diagrams that illustrate the connectivity	- Through Core Switch. - Kindly refer to paragraph 40.1.10 on the Tender Document.
150	Security policy information: - What security policies, firewall rules, or access control lists (ACLs) are applied to Checkpoint ports? - Can we gather details about these security configurations	Will be disclosed during project assessment.
151	Access to Monitoring Data Is there access to real-time or historical monitoring data for Checkpoint ports, including traffic patterns and threat detection?	Yes.
152	Device location: - Current: (Inter rack/Intra rack) - Planned:	- Inter-rack - Inter-rack
153	Cables: - Verify if current cabling is enough for tech refresh (Please mention either UTP or Fiber) - Cable conditions - Cable type (need upgrade or not?) i) Patch cord ii) Fiber optic e.g.: (SC-SC) (LC-LC) (Singlemode/Multimode)	Kindly refer to paragraph 43.3 on the Tender Document.
155	Device usage: - CPU - Memory	Will be disclosed during project assessment.

No.	Question	Answer
	- Bandwidth	
Network load Balancer – Port Checking Questions and Request		
156	Port configuration details: - Port type and configurations - Port speed & Load Balancing settings	Will be disclosed during project assessment.
157	Connectivity details: - How are the ports connected within the application delivery infrastructure? - Network diagrams depicting the connectivity?	- Through Core Switch. - Kindly refer to paragraph 40.1.10 on the Tender Document.
158	Load Balancing and Traffic Management: - What load balancing and traffic management configurations are applied to F5 ports? - Details about how traffic is distributed across these ports?	Will be disclosed during project assessment.
159	Access to Monitoring Data Is there access to real-time or historical monitoring data for F5 ports, such as traffic patterns and performance metrics?	Yes.
160	Device location: - Current: (Inter rack/Intra rack) - Planned:	- Inter-rack - Inter-rack
161	Cables: - Verify if current cabling is enough for tech refresh (Please mention either UTP or Fiber) - Cable conditions - Cable type (need upgrade or not?) i) Patch cord ii) Fiber optic e.g.: (SC-SC) (LC-LC) (Singlemode/Multimode)	Kindly refer to paragraph 43.3 of the Tender Document.
162	Device usage: - CPU - Memory - Bandwidth	Will be disclosed during project assessment.

No.	Question	Answer
163	Is MCMC utilizing an existing SIEM solution, if so; what SIEM is MCMC using. If not, does MCMC require a SIEM solution deployment included in this project?	MCMC is utilizing an existing SIEM, however we cannot disclose the brand.
164	Does MCMC have any log retention requirements?	2 years minimum.
165	Based on clause 43.4, can we get a breakdown of the 2500 devices?	Servers, laptop, desktops, network security devices.
166	Does MCMC have an existing AV / EDR Solution?	Yes, traditional AV.
167	For the SOAR solution, how many administrative / operational users will be utilizing the SOAR solution?	Tenderer to propose.