



Bid Notice Abstract

Request for Quotation (RFQ)

Reference Number 8103447
Procuring Entity MARITIME INDUSTRY AUTHORITY (MARINA)
Title SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION) – 3rd Posting
Area of Delivery Metro Manila

Solicitation Number:	2021-07-309	Status	Pending
Trade Agreement:	Implementing Rules and Regulations		
Procurement Mode:	Negotiated Procurement - Small Value Procurement (Sec. 53.9)	Associated Components	1
Classification:	Goods		
Category:	Information Technology Parts & Accessories & Perip	Bid Supplements	0
Approved Budget for the Contract:	PHP 750,000.00		
Delivery Period:	30 Day/s	Document Request List	0
Client Agency:			
Contact Person:	VADM Rene V. Medina AFP (Ret) The BAC Chairperson c/o BAC Office, 10th Floor, MARINA Bldg. A. Bonifacio Drive cor. 20th Street, Port Area Manila Metro Manila Philippines 1018 63-2-85246518 2021marinabac@gmail.com	Date Published	21/10/2021
		Last Updated / Time	20/10/2021 15:44 PM
		Closing Date / Time	26/10/2021 13:00 PM
Description SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION) – 3rd Posting Please see attached file. You may visit our website at marina.gov.ph (under transparency tab)			

Created by VADM Rene V. Medina AFP (Ret)
Date Created 20/10/2021

The PhilGEPS team is not responsible for any typographical errors or misinformation presented in the system. PhilGEPS only displays information provided for by its clients, and any queries regarding the postings should be directed to the contact person/s of the concerned party.



REQUEST FOR QUOTATION

The Maritime Industry Authority (MARINA) – Bids and Awards Committee (BAC), will undertake a Small Value Procurement for the **SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION) – 3rd Posting** for FY 2021 in accordance with Section 53.9 of the 2016 Revised Implementing Rules and Regulation of Republic Act No. 9184.

Please quote your **best offer** for the item described herein, **subject to the Terms and Conditions** provided at the last page of this Request for Quotation (RFQ). Submit your quotation duly signed by you or your representative **not later than (26 October 2021, 01:00 P.M.)** at the MARINA BAC Office, located at 10th Floor MARINA Building, Bonifacio Drive cor. 20th Street, Port Area, Manila, Philippines.

Qualification of the supplier: The supplier must be **legally registered**, and has at **least 3 years' experience in supplying Intrusion and Detection System**.

A copy of your **2021 Business/Mayor's Permit¹, PhilGEPS Registration Number, Latest Income Tax Return and Omnibus Sworn Statement²** are required to be submitted along with your quotation/proposal.

Additional MARINA requirements to be submitted, a brochure/**datasheet of the proposed Intrusion Detection System** and **submit atleast two (2) Client Satisfactory Certificates in the last two (2) years**.

For any clarification, you may contact us at 2021marinabac@gmail.com



ATTY. KORINA MAE V. PIMENTEL
Head, BAC Secretariat

¹ In case of recently expired Mayor's/Business permit, it shall be accepted together with its official receipt as proof that The Supplier has applied for renewal within the period prescribed by the concerned local government unit, provided that the renewed permit shall be submitted after award of contract but before payment in accordance with item 6.2 of Government Procurement Policy Board (GPPB) Resolution No. 09-2020.

² In case of Unnotarized Omnibus Sworn Statement, it shall be accepted, provided that the notarized Omnibus Sworn Statement shall be submitted after award of contract but before payment in accordance with item 6.3 of GPPB No. 09-2020.

DATE: _____

NAME OF COMPANY:

ADDRESS:

COMPANY ADDRESS:

COMPANY TIN NUMBER:

PHILGEPS REGISTRATION NUMBER:

NAME OF REPRESENTATIVE & DESIGNATION:

INSTRUCTIONS:

- (1) Accomplish this RFQ correctly and accurately.
- (2) Do not alter the content of this form in any way.
- (3) All technical specifications are mandatory. Failure to comply with any of the mandatory requirements will disqualify your quotation.
- (4) Failure to follow these instructions will disqualify your entire quotation.

Supplier's must state here either "Comply" or any equivalent term in the column "Supplier's Statement of Compliance" against each of the individual parameters of each specification.

After having carefully read and accepted the Terms and Conditions in the Request for Quotation, hereunder is our quotation for the item/s as follows:

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION) – 3rd Posting		
Code	Specifications	Supplier's Statement of Compliance
TECHNICAL SPECIFICATION		
	a) GENERAL SPECIFICATION The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, suspicious mail attachments and internal infections. The proposed solution should support the native CEF, LEEF format for SIEM log integration. Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network. Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection and have the following additional features/capabilities: 1. Should be able to store Packet Captures (PCAP) of all malicious communications detected by sandbox. 2. Should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip-based function. 3. Should have the ability to interrupt malicious communication 4. Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only 5. The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment. 6. Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack. 7. Should cause limited interruption to the current network environment. 8. Should allow the customer to gain visibility to the internal networks and flag detected threats immediately. 9. Should have the ability to support out-of-band detection 10. Should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/server machines 11. Should not have any port-based limitation and should support all ports. 12. Should support at least 100+ protocols for inspection. 13. Should have event detection capabilities that should include malware type, severity, source and destination of attack. 14. Should provide risk-based alerts or logs to help prioritize remediation effort. 15. Should be deployed on premise along with on-premise sandboxing capability. 16. Should be able to store real payload of the detected threats. 17. Should be able to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance. 18. Should be able to support up to 5 network segments on a single appliance. 19. Should be able to detect any suspicious communication within and outside of customer's network. 20. Should be able to detect communications to known command and control centers. 21. Should be able to detect reputation of URLs being accessed. 22. Should provide risk-based alerts or logs to help prioritize remediation effort. 23. Should be deployed on premise along with on-premise sandboxing capability. 24. Should be able to store real payload of the detected threats.	

	25. Should be able to store Packet Captures (PCAP) of all malicious communications detected by sandbox 26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack. 27. Should have built-in capabilities to add exceptions for detections. 28. Should have capabilities to configure files, IP, URLs and Domains to black list or white list 29. Should support multiple protocols for inspection. • Example: HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols • Internal direction: SMB, Database protocol (MySQL, MSSQL, Oracle) on a single device 30. Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 31. Should have a correlation engine to automatically correlate across multiple protocols, multiple sessions and volume traffic analysis. 32. Must provide a web service interface/API for customer to customize their own system integration. 33. Must have capabilities to correlate the detections on the device itself. 34. Should support remote packet capturing to pass Kerberos traffic from remote locations for analysis 35. The proposed solution should monitor Inter-VM traffic on a Port Mirror Session. 36. The proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal. 37. The proposed solution should be able to run at least 4 parallel sandboxes for analysis of payload 38. The proposed solution should have an option to allow sandbox instances to use a proxy for internet access. 39. The proposed solution should have support for analysis of embedded URLs in PDFs 40. The proposed solution should support IPv6 environments, and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results.	
	b) MALWARE ANALYSIS 1. Should have multiple built-in virtual execution environments within a single appliance to simulate file activities and find malicious behaviors for advanced threat detection. The solution should be able to provide detection details including the CVE-ID, HTTP referrer and targeted attack campaign name 2. Should be able to provide customizable sandbox to fulfill customer's environments and needs. 3. The sandbox must support multiple operating systems and for both 32-bits and 64-bits OS 4. Must have the capability to analyze large files. Must be able to support more than 40MB file size 5. Sandbox must have the ability to simulate the entire threat behavior .i.e. honeynet and honeypot framework 6. Should support windows XP, Windows 7, Windows 8, Windows 10, Microsoft 2003 and Microsoft 2008 operating environments for sandboxing. This requirement should be based on virtual execution and should not be a hardware or chip-based function. 7. Should have grayware detection capabilities. 8. Should be able to detect any malicious communication within and outside of customer's network. 9. Must provide a web service interface/API for customer to customize their own system integration. 10. Should be able to detect network attacks and exploits. 11. Should have the capability to scale out the detection when the bandwidth increases in the future. 12. Must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp 13. Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 14. Must provide the capability to export network packet files and encrypted suspicious files for further investigation. 15. Should have the capability to perform tracking and analysis of virus downloads and suspicious files. 16. Should support exporting of analysis results such as C&C server IP and malicious domain listing 17. Should have capabilities to scan inside password protected archives 18. Should have capabilities to detect malwares and spywares on Windows and non-Windows platforms 19. Should have an option to configure unrestricted Internet for sandboxes 20. Should have capabilities to configure files, IP, URLs and Domains to blacklist or whitelist 21. Must have capabilities to detect Mac, Linux and mobile malwares 22. Should have capability to include user-defined and context-derived passwords for protected archives 23. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, blacklist and license events etc. 24. The proposed solution should be able to detect known malwares before sending suspicious files to sandbox for analysis 25. The proposed solution should be able to correlate local APT attacks with Global historical APT attacks. 26. The proposed solution should support at least 1 Gbps of throughput 27. The proposed solution should have two (2) x 1TB Hard disks 28. The proposed solution should support at least 5x10/100/1000 Ethernet Interfaces. 29. The proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc.) 30. The proposed solution should be able to detect malicious and suspicious behaviors during non- office hours 31. The proposed solution should have onbox correlation of threats 32. The proposed solution should support open Web Services API for 3rd party or scripting integration 33. The proposed solution should support manual submission for analysis 34. The proposed solution should be able to identify suspicious embedded objects in document files like OLE & Macro extraction, Shellcode & exploit matching	

	35. The proposed solution should be able to detect malicious or malformed files, zero-day detection and embedded scripting. 36. The proposed solution should be able to detect and alert if file has suspicious attributes like True-file type, File extension & Naming trick. The proposed solution should support Microsoft Office 2016 application for Office file analysis in sandbox images.	
	c) REPORTING - Should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions. - Should have the flexibility to provide customizable dashboard. - Should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, blacklist and license events etc. - Should have the option to provide an investigative dashboard that can display correlated graphical data based on link-graph, geo-map, chart, tree-map/pivot table. - Should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information. - Must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable - Review detection details based on predefined smart filters - Should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time) - Should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration - Should have the ability to programmatically output sandbox detections in OpenIOC format - Should have an intuitive dashboard that offers real time threat visibility - Should provide reports with (but not limited to) HTML/CSV/PDF formats - Should provide an intuitive dashboard that offers real time threat visibility and attack characteristics. - Should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules - Should be able to provide details of prevalence, maturity of a given file	
	d) AUTHENTICATION ADMINISTRATION AND CONFIGURATION REQUIREMENT - Shall support local password authentication schemes - Shall support remote administration using SSH/HTTPS - Shall support CLI, GUI/Web based Administration Console.	
SUPPORT		
	- The Supplier shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance - The Supplier must have access to high-level of support via the principal for critical level concerns - The Supplier must provide professional implementation services - The Supplier must provide a monthly health check during the subscription period to ensure that the product is properly working - The Supplier must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.	
WARRANTY		
The warranty shall be for a period of One (1) year.		
OTHERS		
	- The bidder is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc. - The bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance. - At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.	
TERMS OF SUBSCRIPTION		
The subscription shall be for a period of One (1) year.		
UNIT COST	TOTAL COST	

**The above quoted prices are inclusive of all costs and applicable taxes.*

The delivery schedule expressed as week/months stipulates hereafter a delivery date which is the date to the project site.

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION)) – 3rd Posting		
Code	Specifications	Delivery Date**
TECHNICAL SPECIFICATION		The winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed.
	a) GENERAL SPECIFICATION The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, suspicious mail attachments and internal infections. The proposed solution should support the native CEF, LEEF format for SIEM logintegration. Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internalnetwork. Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection and have the following additional features/capabilities: 1. Should be able to store Packet Captures (PCAP) of all malicious communications detected by sandbox. 2. Should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip-based function. 3. Should have the ability to interrupt malicious communication 4. Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only 5. The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment. 6. Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack. 7. Should cause limited interruption to the current network environment. 8. Should allow the customer to gain visibility to the internal networks and flag detected threats immediately. 9. Should have the ability to support out-of-band detection 10. Should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/server machines 11. Should not have any port-based limitation and should support all ports. 12. Should support at least 100+ protocols for inspection. 13. Should have event detection capabilities that should include malware type, severity, source and destination of attack. 14. Should provide risk-based alerts or logs to help prioritize remediation effort. 15. Should be deployed on premise along with on-premise sandboxing capability. 16. Should be able to store real payload of the detected threats. 17. Should be able to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance. 18. Should be able to support up to 5 network segments on a single appliance. 19. Should be able to detect any suspicious communication within and outside of customer's network. 20. Should be able to detect communications to known command and control centers. 21. Should be able to detect reputation of URLs being accessed. 22. Should provide risk-based alerts or logs to help prioritize remediation effort. 23. Should be deployed on premise along with on-premise sandboxing capability. 24. Should be able to store real payload of the detected threats. 25. Should be able to store Packet Captures (PCAP) of all malicious communications detected by sandbox 26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack. 27. Should have built-in capabilities to add exceptions for detections. 28. Should have capabilities to configure files, IP, URLs and Domains to black list or white list 29. Should support multiple protocols for inspection. • Example:HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols • Internal direction: SMB, Database protocol (MySQL, MSSQL, Oracle) on a single device 30. Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. 31. Should have a correlation engine to automatically correlate across multiple protocols, multiple sessions and volume traffic analysis. 32. Must provide a web service interface/API for customer to customize their own system integration. 33. Must have capabilities to correlate the detections on the device itself. 34. Should support remote packet capturing to pass Kerberos traffic from remote locations for analysis 35. The proposed solution should monitor Inter-VM traffic on a Port Mirror Session. 36. The proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal. 37. The proposed solution should be able to run at least 4 parallel sandboxes for analysis of payload 38. The proposed solution should have an option to allow sandbox instances to use a proxy for internet access. 39. The proposed solution should have support for analysis of embedded URLs in PDFs 40. The proposed solution should support IPv6 environments, and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results.	
	b) MALWARE ANALYSIS 1. Should have multiple built-in virtual execution environments within a single appliance to simulate file activities	

	and find malicious behaviors for advanced threat detection. The solution should be able to provide detection details including the CVE-ID, HTTP referrer and targeted attack campaign name - Should be able to provide customizable sandbox to fulfill customer's environments and needs. - The sandbox must support multiple operating systems and for both 32-bits and 64-bits OS - Must have the capability to analyze large files. Must be able to support more than 40MB file size - Sandbox must have the ability to simulate the entire threat behavior .i.e. honeynet and honeypot framework - Should support windows XP, Windows 7, Windows 8, Windows 10, Microsoft 2003 and Microsoft 2008 operating environments for sandboxing. This requirement should be based on virtual execution and should not be a hardware or chip-basedfunction. - Should have grayware detection capabilities. - Should be able to detect any malicious communication within and outside of customer's network. - Must provide a web service interface/API for customer to customize their own system integration. - Should be able to detect network attacks and exploits. - Should have the capability to scale out the detection when the bandwidth increases in the future. - Must be capable of performing multiplefile format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .comand .hwp - Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency. - Must provide the capability to export network packet files and encrypted suspicious files for further investigation. - Should have the capability to perform tracking and analysis of virus downloads and suspicious files. - Should support exporting of analysis results such as C&C server IP and malicious domain listing - Should have capabilities to scan inside password protected archives - Should have capabilities to detect malwares and spywares on Windows and non-Windows platforms - Should have an option to configure unrestricted Internet for sandboxes - Should have capabilities to configure files, IP, URLs and Domains to blacklist or whitelist - Must have capabilities to detect Mac, Linux and mobilemalwares - Should have capability to include user-defined and context-derived passwords for protected archives - The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, blacklist and license events etc. - The proposed solution should be able to detect known malwares before sending suspicious files to sandbox for analysis - The proposed solution should be able to correlate local APT attacks with Global historical APT attacks. - The proposed solution should support at least 1 Gbps of throughput - The proposed solution should have two (2) x 1TB Hard disks - The proposed solution should support at least 5x10/100/1000 Ethernet Interfaces. - The proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers,etc.) - The proposed solution should be able to detect malicious and suspicious behaviors during non- office hours - The proposed solution should have onbox correlation of threats - The proposed solution should support open Web Services API for 3rd party or scripting integration - The proposed solution should support manual submission for analysis - The proposed solution should be able to identify suspicious embedded objects in document files like OLE & Macro extraction, Shellcode & exploit matching - The proposed solution should be able to detect malicious or malformed files, zero-day detection and embedded scripting. - The proposed solution should be able to detect and alert if file has suspicious attributes like True-file type, File extension & Naming trick. The proposed solution should support Microsoft Office 2016 application for Office file analysis in sandboximages.	
	c) REPORTING - Should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions. - Should have the flexibility to provide customizable dashboard. - Should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, blacklist and license events etc. - Should have the option to provide an investigative dashboard that can display correlated graphical data based on link-graph, geo-map, chart, tree-map/pivot table. - Should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information. - Must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable - Review detection details based on predefined smart filters - Should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time) - Should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration - Should have the ability to programmatically output sandbox detections in OpenIOC format - Should have an intuitive dashboard that offers real time threat visibility - Should provide reports with (but not limited to) HTML/CSV/PDF formats - Should provide an intuitive dashboard that offers real time threat visibility and attack characteristics. - Should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules - Should be able to provide details of prevalence, maturity of a given file	The winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed.

	d) AUTHENTICATION ADMINISTRATION AND CONFIGURATION REQUIREMENT 1. Shall support local password authentication schemes 2. Shall support remote administration using SSH/HTTPS 3. Shall support CLI, GUI/Web based Administration Console.	The winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed.
	SUPPORT	
	1. The Supplier shall provide daily 8 by 5 phone, email, and remote support with critical level on site assistance 2. The Supplier must have access to high-level of support via the principal for critical level concerns 3. The Supplier must provide professional implementation services 4. The Supplier must provide a monthly health check during the subscription period to ensure that the product is properly working 5. The Supplier must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.	
	WARRANTY	
	The warranty shall be for a period of One (1) year.	
	OTHERS	
	1. The bidder is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc. 2. The bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance. 3. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.	
	TERMS OF SUBSCRIPTION	
	The subscription shall be for a period of One (1) year.	

FINANCIAL OFFER:

Please quote your **best for** the item below. Please do not leave any blank items. Indicate "0" if item being offered is for free.

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION) - 3rd Posting	
Approved Budget for the Contract (ABC)	Total Offered Quotation
Seven Hundred Fifty Thousand Pesos (Php750,000.00)	In words: _____ _____ _____ _____ In figures: _____ _____ _____ _____

PAYMENT DETAILS:

<i>Banking Institution:</i> _____
<i>Account Number:</i> _____
<i>Account Name:</i> _____
<i>Branch:</i> _____

Signature over Printed Name_____
Position/Designation_____
Office Telephone No._____
Fax/Mobile No._____
Email Address/es

TERMS AND CONDITIONS:

1. Bidders shall provide correct and accurate information required in this form.
2. Price quotation/s must be valid for a period of *thirty (30) calendar days* from the date of submission.
3. Price quotation/s, to be denominated in Philippine peso shall include all taxes, duties and/or levies payable.
4. Quotations exceeding the Approved Budget for the Contract shall be rejected.
5. Award of contract shall be made to lowest calculated and responsive quotation (for goods and infrastructure) or, the highest rated offer (for consulting services) which complies with the minimum technical specifications and other terms and conditions stated herein.
6. Any interlineations, erasures or overwriting shall be valid only if they are signed or initialed by you or any of your duly authorized representative/s.
7. The item/s shall be delivered according to the requirements specified in the Technical Specifications.
8. The MARINA shall have the right to inspect and/or to test the goods to confirm their conformity to the technical specifications.
9. In case two or more bidders are determined to have submitted the Lowest Calculated Quotation/Lowest Calculated and Responsive Quotation, the MARINA-BAC shall adopt and employ "draw lots" as the tie-breaking method to finally determine the single winning provider in accordance with GPPB Circular 06-2005.
10. **Payment shall be processed after delivery and upon the submission of the required supporting documents, in accordance with existing accounting rules and regulations. Please note that the corresponding bank transfer fee, if any, shall be chargeable to the contractor's account.**
11. Liquidated damages equivalent to one tenth of one percent (0.1%) of value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay. The MARINA shall rescind the contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract. Without prejudice to other courses of action and remedies open to it.

Signature over Printed Name

Position/Designation

TERMS OF REFERENCE

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION)

I. Approved Budget Contract

The supplier shall bid for all items described in this Terms of reference, which shall not exceed the Approved Budget Contract (ABC) in the amount of Seven Hundred Fifty Thousand Pesos (750,000.00), inclusive of all applicable government charges.

II. Technical Specification

a. General Specification

The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, suspicious mail attachments and internal infections.

The proposed solution should support the native CEF, LEEF format for SIEM log integration.

Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network.

Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection and have the following additional features/capabilities:

1. ✓ Should be able to store packet captures (PCAP) of all malicious communications detected by sandbox.
2. ✓ Should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip-based function.
3. ✓ Should have the ability to interrupt malicious communication
4. ✓ Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only
5. ✓ The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.
6. ✓ Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack.
7. ✓ Should cause limited interruption to the current network environment.
8. ✓ Should allow the customer to gain visibility to the internal networks and flag detected threats immediately.
9. ✓ Should have the ability to support out-of-band detection
10. ✓ Should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/server machines

11. Should not have any port-based limitation and should support all ports.
12. Should support at least 100+ protocols for inspection.
13. Should have event detection capabilities that should include malware type, severity, source and destination of attack.
14. Should provide risk-based alerts or logs to help prioritize remediation effort.
15. Should be deployed on premise along with on-premise sandboxing capability.
16. Should be able to store real payload of the detected threats.
17. Should be able to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
18. Should be able to support up to 5 network segments on a single appliance.
19. Should be able to detect any suspicious communication within and outside of customer's network.
20. Should be able to detect communications to known command and control centers.
21. Should be able to detect reputation of URLs being accessed.
22. Should provide risk-based alerts or logs to help prioritize remediation effort.
23. Should be deployed on premise along with on-premise sandboxing capability.
24. Should be able to store real payload of the detected threats.
25. Should be able to store packet captures (PCAP) of all malicious communications detected by sandbox
26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack.
27. Should have built-in capabilities to add exceptions for detections.
28. Should have capabilities to configure files, IP, URLs and Domains to black list or white list
29. Should support multiple protocols for inspection.
 - a. Example: HTTP, FTP, SMTP, SNMP, IM, IRC, DNS and P2P protocols
 - b. Internal direction: SMB, Database protocol (MySQL, MSSQL, Oracle) on a single device
30. Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
31. Should have a correlation engine to automatically correlate across multiple protocols, multiple sessions and volume traffic analysis.
32. Must provide a web service interface/API for customer to customize their own system integration.
33. Must have capabilities to correlate the detections on the device itself.
34. Should support remote packet capturing to pass Kerberos traffic from remote locations for analysis
35. The proposed solution should monitor Inter-VM traffic on a Port Mirror Session.

36. ✓ The proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.
37. ✓ The proposed solution should be able to run at least 4 parallel sandboxes for analysis of payload
38. ✓ The proposed solution should have an option to allow sandbox instances to use a proxy for internet access.
39. ✓ The proposed solution should have support for analysis of embedded URLs in PDFs
40. ✓ The proposed solution should support IPv6 environments, and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results.

b. Malware Analysis

1. ✓ Should have multiple built-in virtual execution environments within a single appliance to simulate file activities and find malicious behaviors for advanced threat detection. The solution should be able to provide detection details including the CVE-ID, HTTP referrer and targeted attack campaign name
2. ✓ Should be able to provide customizable sandbox to fulfill customer's environments and needs.
3. ✓ The sandbox must support multiple operating systems and for both 32-bits and 64-bits OS
4. ✓ Must have the capability to analyze large files. Must be able to support more than 40MB file size
5. ✓ Sandbox must have the ability to simulate the entire threat behavior. i.e. honeynet and honeypot framework
6. ✓ Should support windows XP, Windows 7, Windows 8, Windows 10, Microsoft 2003 and Microsoft 2008 operating environments for sandboxing. This requirement should be based on virtual execution and should not be a hardware or chip-based function.
7. ✓ Should have grayware detection capabilities.
8. ✓ Should be able to detect any malicious communication within and outside of customer's network.
9. ✓ Must provide a web service interface/API for customer to customize their own system integration.
10. ✓ Should be able to detect network attacks and exploits.
11. ✓ Should have the capability to scale out the detection when the bandwidth increases in the future.
12. ✓ Must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp

13. Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
14. Must provide the capability to export network packet files and encrypted suspicious files for further investigation.
15. Should have the capability to perform tracking and analysis of virus downloads and suspicious files.
16. Should support exporting of analysis results such as C&C server IP and malicious domain listing
17. Should have capabilities to scan inside password protected archives
18. Should have capabilities to detect malwares and spywares on Windows and non-Windows platforms
19. Should have an option to configure unrestricted Internet for sandboxes
20. Should have capabilities to configure files, IP, URLs and Domains to blacklist or white list
21. Must have capabilities to detect Mac, Linux and mobile malwares
22. Should have capability to include user-defined and context-derived passwords for protected archives
23. The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, blacklist and license events etc.
24. The proposed solution should be able to detect known malwares before sending suspicious files to sandbox for analysis
25. The proposed solution should be able to correlate local APT attacks with Global historical APT attacks.
26. The proposed solution should support at least 1 Gbps of throughput
27. The proposed solution should have two (2) x 1TB Hard disks
28. The proposed solution should support at least 5x10/100/1000 Ethernet Interfaces.
29. The proposed solution should have capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc.)
30. The proposed solution should be able to detect malicious and suspicious behaviors during non- office hours
31. The proposed solution should have on box correlation of threats
32. The proposed solution should support open Web Services API for 3rd party or scripting integration
33. The proposed solution should support manual submission for analysis
34. The proposed solution should be able to identify suspicious embedded objects in document files like OLE & Macro extraction, Shellcode & exploit matching
35. The proposed solution should be able to detect malicious or malformed files, zero-day detection and embedded scripting.

36. The proposed solution should be able to detect and alert if file has suspicious attributes like True-file type, File extension & Naming trick. The proposed solution should support Microsoft Office 2016 application for Office file analysis in sandbox images.

c. Reporting

1. Should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions.
2. Should have the flexibility to provide customizable dashboard.
3. Should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, blacklist and license events etc.
4. Should have the option to provide an investigative dashboard that can display correlated graphical data based on link-graph, geo-map, chart, tree-map/pivot table.
5. Should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
6. Must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable
7. Review detection details based on predefined smart filters
8. Should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)
9. Should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration
10. Should have the ability to programmatically output sandbox detections in OpenIOC format
11. Should have an intuitive dashboard that offers real time threat visibility
12. Should provide reports with (but not limited to) HTML/CSV/PDF formats
13. Should provide an intuitive dashboard that offers real time threat visibility and attack characteristics.
14. Should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules
15. Should be able to provide details of prevalence, maturity of a given file

d. Authentication Administration and Configuration Requirement

1. Shall support local password authentication schemes
2. Shall support remote administration using SSH/HTTPS
3. Shall support CLI, GUI/Web based Administration Console.

III. Support

1. The Bidder shall provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance
2. The Bidder must have access to high-level of support via the principal for critical level concerns
3. The Bidder must provide professional implementation services
4. The Bidder must provide a monthly health check during the subscription period to ensure that the product is properly working
5. The Bidder must provide pro-active Threat Management - giving MARINA alerts should there be any malware threat detected in other parts of the world that may pose a problem for the MARINA.

IV. Warranty

The warranty shall be for a period of One (1) year.

V. Others

1. The bidder is required to conduct a requirements analysis for the configuration of the whole setup within 15 calendar days after issuance of Notice to Proceed. The bidder must submit complete documentation of the entire work plan, resource (hw/sw) requirements, manpower requirements, network design, course syllabus (for knowledge transfer) etc.
2. The bidder is required to conduct knowledge transfer for the solution delivered for at most 5 people. The total number of training days should not exceed 3. All costs related to the training will be shouldered by the winning bidder. These include but not limited to, lease of venue, meals, transportation of participants to and from the training venue, trainer fees, etc. MARINA may, at its discretion, prefer to conduct the training in its office premises. In that case, the lease of venue may be waived. The training must be conducted within 15 calendar days from implementation acceptance.
3. At the end of the implementation phase, the winning bidder must submit a comprehensive documentation on the final setup. The documentation should include a network / logical diagram, configuration settings, and all manuals.

VI. Delivery

The winning bidder is required to deliver and deploy the solution within 30 calendar days after issuance of Notice to Proceed.

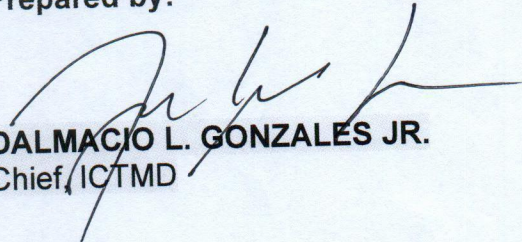
VII. Terms of Subscription

The subscription shall be for a period of One (1) year.

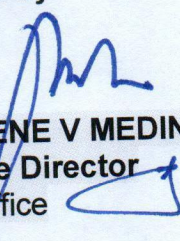
VIII. Payment

The payment can be made one-time fee annually upon issuance of the Billing Statement on a Bank-to-bank basis. Automatic Debit Arrangement (ADA) through Land Bank of the Philippines (LBP) facilities, for other Commercial Bank, applicable bank charges shall be for the account of supplier. The supplier shall submit bank details together with billing statement/ invoice for ready reference.

Prepared by:


DALMACIO L. GONZALES JR.
Chief, ICTMD

Approved by:


VADM RENE V MEDINA AFP (Ret)
Executive Director
STCW Office



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION

MARITIME INDUSTRY AUTHORITY



PURCHASE REQUEST

Office: STCW OFFICE

Division/Section: ICTMD

Date Request: July 14, 2021

PR No. :

2021-07-309

SAI No. :

30 July 2021

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
		SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF INTRUSION DETECTION SYSTEM (SUBSCRIPTION)			750,000.00
*****	*****	*****	*****	*****	*****

Requisitioning Officer

Signature:

Printed Name:

VADM RENE V MEDINA AFP (Ret)

Designation

Executive Director
STCW Office

Purpose:

To be used for monitoring malicious activity or policy violations

CERTIFICATION



FUNDS AVAILABLE



NO FUNDS AVAILABLE

RALPH A. NARVAEZ

Chief, Budget Division

☐ Approved

☐ Disapproved

PR Approver

Signature:

Printed Name:

VADM ROBERT A EMPEDRAD AFP (Ret)

Designation

Administrator

Note:

Omnibus Sworn Statement (Revised)

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

[If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

[If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

[If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

[If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

[If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the

BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and
8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
 - a. Carefully examining all of the Bidding Documents;
 - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
 - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
 - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.
10. **In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.**

IN WITNESS WHEREOF, I have hereunto set my hand this ___ day of ___, 20__ at _____, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]

[Insert signatory's legal capacity]

Affiant

[Jurat]

[Format shall be based on the latest Rules on Notarial Practice]