ASTI – FM 03-17
REV 2 / 31 January 2020

PURCHASE ORDER

Supplier:	CT Link Systems, Inc.	PO No.:	20-06-076
Address:	4F Maripola Building, 109 Perea Street, Makati City	PO Date:	June 8, 2020
TIN:	201-380-940-000	Mode of Procurement:	NP: Small Value Procurement

Gentleman:

Please furnish this Office the following articles subject to the terms and conditions contained herein:

Place of Delivery:	ASTI Bldg., C.P. Garcia Ave., U.P. Technology Park Complex, U.P. Campus, Diliman, Quezon City 1101	Delivery Term:	Per End-user's Schedule
Date of Delivery:		Payment Term:	Government Terms
		Warranty Term:	

Stock / Property No.	Unit	Description	Quantity	Unit Cost	Amount
1	Lot	Lease of Intrusion Detection System	1	₱795,000.00	₱795,000.00
		(See attached Abstract of Bids and Canvass and Offers)			
				TOTAL:	₱795,000.00
(Total Amount in Words)		Seven Hundred Ninety-Five Thousand Pesos			

The contract price is inclusive of taxes and other fees or charges. In case of failure to make the full delivery within the time specified above, a penalty of one-tenth (1/10) of one percent for every day of delay shall be imposed on the undelivered item/s. Once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract, DOST-ASTI may rescind or terminate the contract, without prejudice to other courses of action and remedies available under the circumstances and in accordance with the provisions of the latest implementing rules and regulations of RA 9184.

Conforme:

(Signature over Printed Name of Supplier)

(Date)

Very Truly Yours,

Digitally signed by PETER ANTONIO B. BANZON
Date: 2020.06.12 13:34:36 +08'00'

PETER ANTONIO B. BANZON
Officer-in-Charge, DOST-ASTI

Fund Cluster:	01	ORS / BURS No.:	011011012020-06-000224
		ORS / BURS Date:	June 10, 2020
Funds Available:	Php 795,000.00	Amount:	₱795,000.00

Digitally signed by Gay Concepcion S. Bugagao
Date: 2020.06.15 13:05:28 +08'00'

GAY CONCEPCION S. BUGAGAO
Accountant III

08 June 2020

NOTICE TO PROCEED
ALTERNATIVE MODE OF PROCUREMENT

Ms. GENA NASOL
Sales Manager
CT LINK SYSTEMS, iNC.
4F Maripola Building, 109 Perea Street
Makati City

Dear Ms. Nasol,

This Notice to Proceed is hereby issued for the following contract details:

Contract Name	: Lease of Intrusion Detection System
Purchase Request No.	: GAA-20-04-9885
Purchase / Work Order No.	: 20-06-076
Total Contract Price (inclusive of taxes, import duties and all other charges or fees)	: Php 795,000.00
Total Contract Price in Words	: Seven Hundred Ninety Five Thousand Pesos

Upon issuance of this Notice, your company, CT LINK SYSTEMS, iNC. is hereby directed to commence the delivery of items and/or performance of services stipulated in the said Purchase Order which shall become due and demandable in accordance with the delivery schedule stipulated therein.

Please acknowledge receipt and acceptance of this Notice by signing in the space provided below. There are two (2) copies of this document; you may keep one copy and return the other to the Bids and Awards Committee (BAC) Secretariat of the Advanced Science and Technology Institute. Should you have any questions or clarifications, you may reach us at bac-sec@asti.dost.gov.ph.

Respectfully,

Digitally signed by PETER ANTONIO B. BANZON
Date: 2020.06.15 13:36:11 +08'00'

PETER ANTONIO B. BANZON
Officer-in-Charge, DOST-ASTI

DATE OF ISSUANCE:

RECEIVED BY:

Signature over Printed Name

Date and Time

May 26, 2020

PEDRITO MANGAHAS
Chairperson, BAC-1
Advanced Science And Technology Institute
C.P. Garcia Avenue, UP Campus
Diliman, Quezon City

RFQ NO.: 20-04-3121
PR NO.: GAA-20-04-9885

Dear Sir:

In response to your RFQ, pls find below our quotation for your Lease of Intrusion and Detection System requirements:

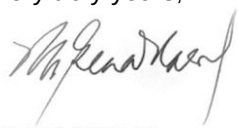
Item Number	Description	Qty	Unit Price	TOTAL Price
1	**Trend Micro Deep Discovery Inspector (DDI) 1000s** Includes 6months DDI1100 license renewal and Support License Renewal date : June 21, 2020 to December 31, 2020 (pls see attached technical specifications)	1	Php 795,000.00	Php 795,000.00

Terms and Conditions:

1. Price : VAT inclusive
2. Validity of quote : Valid until June 15, 2020.
3. Availability : Within 15 days upon receipt of Purchase Order.

We hope that our proposal meets your approval. Please do not hesitate to call us should you have any questions. We look forward to being of service to your organization.

Very truly yours,



GENA NASOL
Sales Manager
Tel # 893-9515
Fax #893-5856
email : gena_nasol@ctlink.com.ph
mobile : 0917-568-3159

TECHNICAL SPECIFICATIONS

Lease of Intrusion Detection System

I. General Specs

1. 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.
2. The proposed solution should support the native CEF, LEEF format for SIEM log integration.
3. Proposed anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network.
4. Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection.
5. Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.
6. Solution should provide risk-based alerts or logs to help prioritize remediation effort.
7. Solution should be deployed on premise along with on-premise sandboxing capability.
8. The proposed solution should be able to store real payload of the detected threats.
9. The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox.
10. The proposed solution should use OS sandboxes for detecting zero-day malwares. This should not be a CPU or chip- based function.
11. Solution should have the ability to interrupt malicious communication
12. Solution should have no limitation in terms of supported users and limitation should be accounted in terms of bandwidth only
13. 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.
14. Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack.
15. Solution deployment should cause limited interruption to the current network environment.
16. The proposed solution should allow the customer to gain visibility to the internal networks and flag detected threats immediately.
17. The proposed solution should have the ability to support out-of-band detection
18. The proposed solution should be able to detect lateral movements of the attacker without the need of installing agents on endpoint/ server machines
19. The proposed solution should not have any port-based limitation and should support all ports.
20. The proposed solution should support at least 100+ protocols for inspection.
21. The proposed solution 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.
22. The proposed solution should be able to support up to 5 network segments on a single appliance.

23. The proposed solution should be able to detect any suspicious communication within and outside of customer's network.
24. The proposed solution should be able to detect communications to known command and control centers.
25. The proposed solution should be able to detect reputation of URLs being accessed.
26. The proposed solution should be able to identify and help the customer to understand the severity and stage of each attack.
27. The proposed solution should have built-in capabilities to add exceptions for detections.
28. The proposed solution should have capabilities to configure files, IP, URLs and Domains to black list or white list 29. The proposed solution 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. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
31. The proposed solution should have a correlation engine to automatically correlate across multiple protocols, multiple sessions and volume traffic analysis.
32. The proposed solution must provide a web service interface/ API for customer to customize their own system integration.
33. The proposed solution must have capabilities to correlate the detections on the device itself.
34. The proposed solution 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.

II. Malware Analysis
1. The proposed solution 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. The proposed solution 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. Solution 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. The proposed solution 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. The proposed solution should have grayware detection capabilities.

8. The proposed solution should be able to detect any malicious communication within and outside of customer's network.

9. The proposed solution must provide a web service interface/ API for customer to customize their own system integration.

10. The proposed solution should be able to detect network attacks and exploits.

11. The proposed solution should have the capability to scale out the detection when the bandwidth increases in the future.

12. Solution 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. The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.

14. The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation.

15. The proposed solution has the capability to performs tracking and analysis of virus downloads and suspicious files.

16. The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing.

17. The proposed solution should have capabilities to scan inside password protected archives

18. The proposed solution should have capabilities to detect malwares and spywares on Windows and non- Windows platforms

19. The proposed solution should have an option to configure unrestricted Internet for sandboxes

20. The proposed solution should have capabilities to configure files, IP, URLs and Domains to blacklist or white list

21. The proposed solution must have capabilities to detect Mac, Linux and mobile malwares

22. The proposed solution 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.

III. Reporting
1. The proposed solution should have an intuitive dashboard that offers real time threat visibility
2. The proposed solution should provide reports with (but not limited to) HTML/ CSV/ PDF formats
3. The proposed solution should provide an intuitive dashboard that offers real time threat visibility and attack characteristics.
4. Review detection details based on predefined smart filters
5. The proposed solution 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).
6. The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attack's sessions.
7. The proposed solution should have the flexibility to provide customizable dashboard.

8. The proposed solution 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.
9. The proposed solution 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.
10. The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.
11. 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.
12. The proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, lateral movement, asset and data discovery and data exfiltration.
13. The proposed solution should have the ability to programmatically output sandbox detections in OpenIOC format.
14. The proposed solution should be able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules
15. The proposed solution should be able to provide details of prevalence, maturity of a given file

IV. Authentication Administration and Configuration Requirement
1. The proposed solution shall support local password authentication schemes
2. The proposed solution shall support remote administration using SSH/ HTTPS
3. The proposed solution shall support CLI, GUI/ Web based Administration Console.

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

VI. OTHERS
1. The license renewal should start upon expiration of the existing license on June 20, 2020.
2. The lease period is from June 21, 2020 to December 31, 2020.
3. The winning bidder is required to conduct a requirements analysis for the configuration of the

whole setup within 30 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.

4. The winning bidder is required to deliver the solution to an ASTI-designated data center within 45 calendar days after issuance of Notice to Proceed. The bidder is also required to deploy and configure the device within 65 calendar days after Notice to Proceed.

5. The winning bidder may be required to conduct knowledge transfer for the solution delivered for at most 3 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. ASTI 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 ninety (90) calendar days from implementation acceptance.

6. 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.

5. Payment will be made every quarter after acceptance.