



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO ST., SAN MIGUEL, MANILA

BIDS AND AWARDS COMMITTEE

Resolution No. 2020-

WHEREAS, the Department of Budget and Management-Bids and Awards Committee (DBM-BAC) conducted a public bidding for the Project, "Subscription of Advanced Endpoint Security Solution," with an Approved Budget for the Contract of P5,030,000.00 for twelve months, authorized under the FY 2020 General Appropriations Act;

WHEREAS, under Resolution No. 2020-20 dated March 17, 2019, the BAC declared the first bidding for the Project as "failed" in accordance with Section 35.1(a) of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184;

WHEREAS, on May 12, 2020, the second Invitation to Bid was posted on the Philippine Government Electronic Procurement System website, the DBM website, and all DBM bulletin boards;

WHEREAS, three (3) prospective bidders responded to the said Invitation and participated in the online Pre-Bid Conference on May 19, 2020, namely: (i) Accent Micro Technologies Inc.; (ii) Palo Alto Networks Philippines; and (iii) Secur Links Network and Technologies Inc.;

WHEREAS, Supplemental/Bid Bulletin No. 1 was issued on May 26, 2020 to clarify, modify or amend items in the Bidding Documents;

WHEREAS, during the submission and opening of bids on June 2, 2020, only one (1) bidder, Accent Micro Technologies Inc., submitted a bid;

WHEREAS, after preliminary examination of the bid, the BAC, using non-discretionary "pass/fail" criteria, determined the submission of Accent Micro Technologies Inc. as "passed" for complying with all the eligibility and technical requirements as stated in the Bidding Documents;

WHEREAS, after evaluation of the financial proposal, the BAC declared the submission of Accent Micro Technologies Inc. as the Single Calculated Bid in the amount of P4,996,000.00;

WHEREAS, after careful evaluation, validation and verification of the eligibility, technical and financial proposals of the bid, the BAC found that the submission of Accent Micro Technologies Inc. passed all the criteria for post-qualification; thus, it was declared as the Single Calculated and Responsive Bid in the amount of P4,996,000.00.

NOW, THEREFORE, for and in consideration of the foregoing premises, the BAC **RESOLVED**, as it hereby **RESOLVED**, to recommend to the Secretary of the Department of Budget and Management that the contract for the Project, "Subscription of Advanced Endpoint Security Solution," be awarded to Accent Micro Technologies Inc., in accordance with Republic Act No. 9184 and its 2016 Revised Implementing Rules and Regulations.

ADOPTED, this 11th day of June 2020 at the Department of Budget and Management, General Solano St., San Miguel, Manila.


HENRY CARANDANG
End-user Representative

not present
VIRGILIO A. UMPACAN, JR.
B.U.D.G.E.T. Representative


JEANNE TERESITA V. IMPORTANTE
Member

not present
ROWEL D. ESCALANTE
Member


ROSEMARIE D. PAGALA
Alternate Member


ANDREA CELENE M. MAGTALAS
Vice Chairperson

not present
ACHILLES GERARD C. BRAVO
Chairperson

☒ Approved
☐ Disapproved


WENDEL E. AVISADO
Secretary

Date: _____



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

BIDS AND AWARDS COMMITTEE

NOTICE OF AWARD

MR. CHRISTOPHER B. GARCIA

Accent Micro Technologies, Inc.
8/F East Tower
Philippine Stock Exchange Center
Exchange Road, Ortigas Center
Pasig City

Dear **Mr. Garcia**:

We are pleased to inform you that the contract for the Project, "Subscription of Advanced Endpoint Security Solution," is hereby awarded to Accent Micro Technologies, Inc. in the amount of P4,996,000.00.

In this regard, you are hereby required to post a performance security in the amount and form stated in Section 39 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184 prior to the signing of the contract.

Thank you and God Bless.

Very truly yours,

WENDEL E. AVISADO
Secretary



JUL 8 2020
RAYMOND NAVARRO



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF BUDGET AND MANAGEMENT
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

NOTICE TO PROCEED

MR. CHRISTOPHER B. GARCIA

Accent Micro Technologies, Inc.
8/F East Tower
Philippine Stock Exchange Center
Exchange Road, Ortigas Center
Pasig City

Dear **Mr. Garcia:**

This is to inform your company that performance of the obligations specified in the attached Contract for the Project, "Subscription of Advanced Endpoint Security Solution," shall commence upon receipt of this Notice to Proceed in accordance with Section 37.4 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184.

Thank you and God Bless.

Very truly yours,


WENDEL E. AVISADO
Secretary



I acknowledge receipt and acceptance of this Notice on July 28, 2020.

Name of Authorized Representative: Christopher Garcia

Signature:  _____

CONTRACT No. 2020-19
SUBSCRIPTION OF ADVANCED ENDPOINT SECURITY SOLUTION

This CONTRACT made and entered into by and between the following:

DEPARTMENT OF BUDGET AND MANAGEMENT, a government agency created by virtue of the laws of the Republic of the Philippines, with principal office address at General Solano St., San Miguel, Manila, represented herein by its **SECRETARY, WENDEL E. AVISADO**, hereinafter called the "**DBM**";

- and -

ACCENT MICRO TECHNOLOGIES INC., a corporation duly organized and existing under the laws of the Republic of the Philippines, with office address at 8/F East Tower, Philippine Stock Exchange Center, Exchange Road, Ortigas Center, Pasig City, represented by **ITS AUTHORIZED REPRESENTATIVE, CHRISTOPHER B. GARCIA**, hereinafter referred to as the "**SUPPLIER**";

(COLLECTIVELY, THE "PARTIES")

WITNESSETH:

WHEREAS, the DBM conducted a public bidding for the Project, "Subscription of Advanced Endpoint Security Solution," and the bid of the Supplier is in the amount of Four Million Nine Hundred Ninety-Six Thousand Pesos (P4,996,000.00), hereinafter called the "Contract Price";

WHEREAS, pursuant to Sections 37 and 39 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, the Notice of Award was issued to the Supplier last July 8, 2020, and the Supplier posted its performance security in the form of an Irrevocable Domestic Standby Letter of Credit on July 15, 2020, in the amount of Two Hundred Forty-Nine Thousand Eight Hundred Pesos (P249,800.00);

NOW, THEREFORE, for and in consideration of the foregoing premises, the parties hereby mutually stipulate and agree as follows:

1. In this Contract, words and expressions shall have the same meanings as are respectively assigned to them in the General and Special Conditions of Contract referred to in Annex D and E, respectively.
2. The following documents shall form and be read and construed as part of this Contract:

Annex A	-	Bid Form
B	-	Schedule of Requirements
C	-	Technical Specifications
D	-	General Conditions of Contract
E	-	Special Conditions of Contract
F	-	Notice of Award
G	-	Performance Security

10

3. In consideration of the payments to be made by the DBM to the Supplier, the Supplier hereby covenants with the DBM to provide the Goods and Services, which is the Subscription of Advanced Endpoint Security Solution, and to remedy defects therein in conformity with the provisions of the Contract.
4. The DBM hereby covenants to pay the Supplier, in consideration of the provision of the Goods and Services, which is the Subscription of Advanced Endpoint Security Solution, and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the time and in the manner prescribed by the Contract.
5. The period for the performance of the obligations under this Contract shall not go beyond the validity of the appropriation for this Project.
6. Entire Agreement. All parties agree that this Contract, including the attached Annexes, contains their full agreement and supersedes all previous agreements, either written or oral, if there are any. No agreements, understandings, commitments, discussions, warranty, representations or other covenants, whether oral or written, between the parties are included in this Contract, including the attached Annexes, except as set forth herein.

IN WITNESS WHEREOF, the parties hereto have signed this Contract on this ____ day of _____, 2020 at General Solano St., San Miguel, Manila, Philippines.

DEPARTMENT OF BUDGET
AND MANAGEMENT

by:


WENDEL E. AVISADO
Secretary



ACCENT MICRO TECHNOLOGIES, INC.

by:


CHRISTOPHER B. GARCIA
Authorized and Designated
Representative

SIGNED IN THE PRESENCE OF


ANDREA CELENE M. MAGTALAS
Director IV
Information and Communications Technology
Systems Service



Soliman Chua

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY OF MANILA) S.S.

BEFORE ME, a Notary Public for and in the City of MANILA, Philippines on this JUL 28 2020 day of _____, 2020 personally appeared the following:

NAME	VALID ID	VALID UNTIL
WENDEL E. AVISADO	DBM ID No. 4601	

CHRISTOPHER B. GARCIA

known to me to be the same persons who executed the foregoing Contract and who acknowledged to me that the same is their free and voluntary act and deed and of the entities they respectively represent.

This CONTRACT for the Subscription of Advanced Endpoint Security Solution was signed by the parties, and their material witnesses on each and every page thereof.

WITNESS MY HAND AND SEAL this _____ day of _____, 2020.

Doc. No. 26;
Page No. 7;
Book No. 14
Series of 2020.

ATTY. JOEL E. PANER
NOTARY PUBLIC COMMISSION NO. 2020-013
Issued on 01/20/20 UNTIL 12/31/2021 MANILA
UNIT 237 TMR 2 TAFT AVE., MALATE, MANILA
Roll No. 44009 * IBP Lifetime No. 2022/15-12-00
PTR No. 9120231/01-02-2020 MANILA / TIN 104063310
MCLE COMPLIANCE No. VI-0013321/04-14-2022

15

Bid Form

Date: JUNE 2, 2020
Invitation to Bid No.: **DBM-2020-31**

To: DEPARTMENT OF BUDGET AND MANAGEMENT
DBM Bldg. III, General Solano St.
San Miguel, Manila

Gentlemen and/or Ladies:

Having examined the Bidding Documents including Bid Bulletin Number 1, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to the DBM, our services for the Project, **“Subscription of Advanced Endpoint Security Solution”** in conformity with the said Bidding Documents for the sum of *Four Million Nine Hundred Ninety Six Thousand pesos only (Php 4,996,000.00)*.

We undertake, if our Bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in **BDS** provision for **ITB** Clause 18.2 and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements as per **ITB** Clause 5 of the Bidding Documents.

We likewise certify/confirm that the undersigned, is granted full power and authority by the **ACCENT MICRO TECHNOLOGIES, INC.**, to participate, submit the bid, and to sign and execute the ensuing contract on the latter's behalf for **“Subscription of Advanced Endpoint Security Solution”** of the **Department of Budget and Management**.

A handwritten signature in black ink, consisting of a large, stylized 'S' or 'G' shape with a horizontal line extending to the right.

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Dated this 2nd day of June 2020.


CHRISTOPHER B. GARCIA

[Signature]

AVP – ICT SOLUTIONS

[In the capacity of]

Duly authorized to sign Bid for and on behalf of ACCENT MICRO TECHNOLOGIES, INC.



Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter the date of delivery to the project site.

Item	Description	Delivery Date
1.	Delivery, Installation, Configuration, and Operationability of Advanced Endpoint Security Solution and its components for 1,500 devices (servers, work station, and mobile devices) (see attached Annex "A," item V, 5.2).	Within sixty (60) calendar days after receipt of Notice to Proceed (NTP)
2.	Submission of copy of certificates for the following Certified Professionals for the Advanced Endpoint Security Solution installation, configuration, testing, commissioning and integration with Network Access Contro (NAC) and alignment to the DBM enterprise network (see attached Annex "A," item V, 5.2). <ul style="list-style-type: none">▪ Manufacturer-Certified Advanced Endpoint Security Professional or its equivalent; and▪ CISCO Certified Network Professional	Copy of certificates must be submitted in the submission of bid documents and subject for post qualification (see attached Annex "A," item V, 5.20)
3.	Conduct of Training	As indicated in item V, 5.4 of Annex "A"

I hereby certify to comply and deliver all the above requirements.

Accent Micro Technologies Inc.
Name of Company/Bidder


Christopher B. Garcia
Signature Over Printed Name of Representative

June 2, 2020
Date



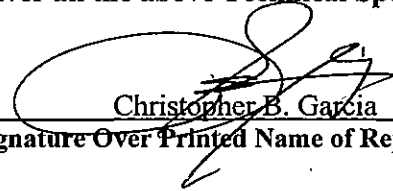
Section VII. Technical Specifications

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

Specifications	Bidders's Statement of Compliance
I. Objective (<i>see attached Annex A, item II</i>)	Comply
II. Duration of the C (<i>see attached Annex A, item III</i>)	Comply
III. Specifications (<i>see attached Annex A, item IV</i>)	Comply
IV. Scope of Work (<i>see attached Annex A, item V</i>)	Comply
V. Service Level Agreement (<i>see attached Annex A, item VI</i>)	Comply
VI. Warranties of Contractors (<i>see attached Annex A, item VII</i>)	Comply
VII. Confidentiality of Data (<i>see attached Annex A, item VIII</i>)	Comply
VIII. Terms of Payment (<i>see attached Annex A, item IX</i>)	Comply
IX. Pre-Termination of Contract (<i>see attached Annex A, item X</i>)	Comply

I hereby certify to comply and deliver all the above Technical Specifications.

Accent Micro Technologies Inc.
Name of Company/Bidder


Christopher B. Garcia
Signature Over Printed Name of Representative

June 2, 2020
Date



TECHNICAL SPECIFICATION

I. PROJECT TITLE

Subscription of Advanced Endpoint Security Solution

II. OBJECTIVE

To implement a comprehensive and advanced endpoint security platform based on next generation cybersecurity technologies, endpoint detection and response, unknown malware analysis and managed protection for the DBM users' end devices and application servers.

III. DURATION OF THE CONTRACT

The contract duration for the subscription shall be twelve (12) months from the issuance of Certificate of Acceptance.

IV. SPECIFICATIONS

4.1 Endpoint

4.1.1 The proposed solution must be able to support a wide range of Windows operating systems including Windows Servers 2016.

4.1.2 The proposed solution must be able to support MacOS and Linux including Linux Containers.

4.1.3 The proposed solution must be able to support both Workstations, Servers and Android with single license.

4.1.4 The proposed solution must be a signature-less solution.

4.1.5 The proposed solution must be a Microsoft Windows Security Center Certified or recognized.

4.1.6 The proposed solution must be able to protect proprietary applications such as in-house applications.




4.2 Management

- 4.2.1 The proposed solution must be cloud based management
- 4.2.2 The proposed solution shall have the capability to report all security incidents back to management immediately as long as the endpoint is connected to the management.
- 4.2.3 The proposed solution shall provide Web-based Graphical User Interface (GUI).
- 4.2.4 The proposed solution management shall allow user to manage policy for mobile (e.g. Android) in one single console.
- 4.2.5 The proposed solution management shall allow user to upgrade endpoint without third party software or tool.
- 4.2.6 The proposed solution management shall provide malware file report view online or download as pdf.
- 4.2.7 The proposed solution management shall provide capability for administrator to create exception directly from security event.
- 4.2.8 The proposed solution management shall provide 2FA capability without need of customer integration.
- 4.2.9 The proposed solution shall provide grouping capability as following but not following to:
 - Static – select from existing connected endpoints
 - Dynamic – by define condition based on Endpoint name, Domain, IP Addresses, VID, agent version, and the Operating System on Endpoints.

4.3 Integration

- 4.3.1 The proposed solution shall provide the capability to get intelligence feed from the existing Palo Alto Networks Firewall without any additional custom integration or configuration.
- 4.3.2 The proposed solution shall provide capability to integrate with on-premises Active Directory.
- 4.3.3 The proposed solution shall provide capability to forward logs to SIEM or Syslog server.
- 4.3.4 The proposed solution must have sandbox capability.

4.4 Exploit Prevention

- 4.4.1 The proposed solution shall provide the prevention against exploit kit that do fingerprinting through browser (e.g. Internet Explorer Edge)
 - 4.4.2 The proposed solution shall provide prevention against exploit that attack the operating system kernel through kernel privilege escalation.
 - 4.4.3 The proposed solution shall prevent attacks which change the execution order of a process by redirecting an asynchronous procedure call (APC) to point the attackers' malicious shellcode
 - 4.4.4 The proposed solution shall be able to provide real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc.
- 

- 4.4.5 The proposed solution must be able to protect the systems without knowing the CVE numbers
- 4.4.6 The proposed solution shall prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking through core exploits techniques.
- 4.4.7 The proposed solution should provide the capability to perform exploit monitoring and prevention based on core exploit techniques without connection to the Management Server and/or Cloud Service or without relying on signatures.
- 4.4.8 The proposed solution shall collect forensic data like process name, file source and path, time stamp, memory dump, operating system version, user ID, vulnerable application version while terminate the particular process under attack.
- 4.4.9 The proposed solution shall utilize core exploit technique to prevent or block. It shall not be based on signatures or reputation of the file.
- 4.4.10 The exploit technique modules shall be able to apply to known and popular applications as well as authorized unknown or in-house developed applications.
- 4.4.11 The proposed solution shall provide protection against exploit including MacOS, Windows, Linux, and processes running in Linux Containers.
- 4.4.12 The proposed solution shall provide automated forensic memory dump analysis to allow administrators to quickly understand exploit events.
- 4.4.13 The proposed solution shall also provide Behavior Analytics capability to prevent or block suspicious activities which may or may not related to exploit.

4.5 Malware Prevention

- 4.5.1 The proposed solution shall provide protection against malicious DLL files
- 4.5.2 The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file.
- 4.5.3 The proposed solution shall support protection against the execution of malicious executables.
- 4.5.4 The proposed solution shall have the capability to restrict files and applications execution on or from local folder, network folder, external media (e.g. USB Drive and Optical Media).
- 4.5.5 The proposed solution shall have the capability to restrict files and applications from loading another process that is unknown or in the backgroup (a.k.a. child processes)
- 4.5.6 The proposed solution shall use signature-less type of technology to prevent malware.
- 4.5.7 The proposed solution shall use dynamic analysis technology (e.g. Sandbox) to identify unknown malicious executables including DLL.
- 4.5.8 The proposed solution shall use Machine Learning technology to prevent malware on Windows, Mac OS, Linux Containerized processes, and Android.
- 4.5.9 The proposed solution shall have multi-layer prevention technology that includes but not limited to sandbox, machine learning and restriction.

4.6 Unknown Malware Analysis

- 4.6.1 The proposed solution shall include cloud sandbox with NO additional cost



- 4.6.2 The proposed solution shall have the capability to prevent unknown or zero-day malware when the endpoint is in offline stage (no internet or management connection).
- 4.6.3 The proposed solution shall have the capability to prevent unknown file or application through restriction policy.
- 4.6.4 The proposed solution shall have the capability to prevent executable file from executing until the file is been verify.
- 4.6.5 The proposed solution shall have the capability to prevent executable files by customer provided hashes.
- 4.6.6 The proposed solution shall have the capability to identify and prevent greyware
- 4.6.7 The proposed solution shall automatically submit unknown file to sandbox without the need of administrator intervention.
- 4.6.8 The proposed solution shall have the capability to quarantine unknown and zero malware.
- 4.6.9 The proposed solution shall be able to identify and prevent sophisticated attacks that utilize legitimate processes and actions for malicious activity based on run-time behavior.

4.7 Detection and Response

- 4.7.1 The proposed solution shall allow security administrator to hunt using Indicator of Compromise or Combine of multiple behavior of the Indicator.
- 4.7.2 The proposed solution shall have the capability to display attack timeline.
- 4.7.3 The proposed solution shall has the capability to show the suspicious file was loaded or launch by which parent processes.
- 4.7.4 The proposed solution shall not limit to only endpoint but also able to show and correlate network data from firewall.
- 4.7.5 The proposed solution shall provide the behavior recording capability like network and user behavior analysis through solution provided sensors and no through Netflow data.
- 4.7.6 EDR, network user behavior analysis and Prevention should be single endpoint agent.
- 4.7.7 The proposed solution shall have the capability to isolate the endpoint.
- 4.7.8 The proposed solution shall have the capability to blacklist suspicious file from the investigation console.
- 4.7.9 The proposed solution shall able to provide the environment for behavior detection base on but not limited to peer, time and entity.
- 4.7.10 The proposed solution shall be able to detect behavior as following but not limited to:
 - 4.7.10.1 Command and Control
 - 4.7.10.2 Reconnaissance
 - 4.7.10.3 Lateral Movement
 - 4.7.10.4 Data Exfiltration
- 4.7.11 The proposed solution Network and User behavior analysis shall not be based on NetFlow. It shall be base on AI or Machine Learning technology with combine of Endpoint, Logs and Networks.
- 4.7.12 The proposed solution shall be able to detect file-less attack and script base attack.



- 4.7.13 The proposed solution shall provide query builder for threats hunting base on the following but not limited to:
- 4.7.13.1 Process
 - 4.7.13.2 File
 - 4.7.13.3 Hash (MD5 and SHA256)
 - 4.7.13.4 Network (IP addresses, port, protocol, country)
 - 4.7.13.5 Registry
 - 4.7.13.6 Signer
- 4.7.14 The proposed solution shall be able to provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process.
- 4.7.15 The proposed solution shall be able to create behavior indicators to identify malicious intent
- 4.7.16 The proposed solution shall be able to detect threats on unmanaged device or network anomalies based on peer behavior.
- 4.7.17 The proposed solution must have the capability to chain detection from network, endpoint and cloud.
- 4.7.18 The proposed solution shall allow administrator to create custom detection rules to adapt based on environment.
- 4.7.19 The proposed solution shall have live remote and remote isolation as response.
- 4.7.20 The proposed solution shall have process termination capability.
- 4.7.21 The proposed solution shall have the capability to assign and mark the stage of investigation of specific incident.

4.8 Reporting

- 4.8.1 The proposed solution shall have a natively built-in dashboard to monitor the following:
- Unresolved Security Events in the defined timeframe with different severities.
 - The OS platform and the number of managed agents.
 - The endpoint license consumption status and its expiry date.
- 4.8.2 The proposed solution shall be able to monitor the health of the individual endpoints including but not limited to:
- Endpoint Hostname
 - User
 - Status
 - Underlying OS
 - Agent Version
 - Last Seen Time
- 4.8.3 The proposed solution shall provide a high-level summary of the security and deployment status of endpoints. The report can be scheduled to run on a recurring basis and on-demand. The report shall be able to optionally send to one or more e-mail addresses.



4.9 Forensics

- 4.9.1 The proposed solution shall support the collection of forensic data captured by the advanced endpoint solution to a centralized location.
- 4.9.2 The proposed solution shall support automatic collection of the following forensic information for further investigation purposes:
 - Memory Dump
 - Accessed Files
 - Loaded Modules
 - Accessed URI
 - Ancestor Processes
- 4.9.3 The proposed solution shall have the capability to view high level system information about the endpoint after the threats has been detected and also provide the capability to retrieve the prevention data for further analysis and investigation.

5 SCOPE OF WORK AND SERVICES

5.1 The CONTRACTOR shall conduct pre-implementation meeting with DBM representatives and current Facility Management Service provided so that all the necessary preparations, ideal set-up, contractor's familiarization of the computing environment, and other implementation matters are clearly discussed and finalized.

5.2 The CONTRACTOR shall deliver, install, configure and make operational the Advanced Endpoint Security Solution and its components for 1,500 devices (servers, workstations and mobile devices) within sixty (60) calendar days from the receipt of Notice to Proceed (NTP).

The CONTRACTOR must have the following Certified Professionals for the Advanced Endpoint Security Solution installation, configuration, testing, commissioning and integration with the Network Access Control (NAC) and alignment to the DBM enterprise network (certificates must be submitted in the submission of bid documents and subject for post qualification):

- Manufacturer-Certified Advanced Endpoint Security Professional or its equivalent
- CISCO Certified Network Professional

5.3 Technical Support

- 5.3.1 The CONTRACTOR must be able to provide 3-tier support:
 - Local reseller as the first-level of support
 - Distributor as the second-level of support
 - Principal as the third-level of support



5.3.2 The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in a form of telephone call, electronic mail, and/or on-site support.

The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.

5.4 The CONTRACTOR shall provide Technology Transfer based on the following schedule:

Training	Schedule	No. of Participants	Duration
Advanced Endpoint Security Solution installation, configuration and administration	To be scheduled by the DBM-ICTSS prior to the engagement of the contract	At least five (5) ICTSS personnel.	One (1) day
	To be scheduled by the DBM-ICTSS prior to the engagement of the contract	At least five (5) ICTSS personnel.	One (1) day
	To be scheduled by the DBM-ICTSS prior to the engagement of the contract	At least five (5) ICTSS personnel.	One (1) day

The CONTRACTOR shall issue individual training certificates and training materials for each of the participants.

5.5 The CONTRACTOR shall provide as-built documentation of the Advanced Endpoint Security Solution set-up/diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage and backup within sixty (60) calendar days from the receipt of NTP.

5.6 A Certificate of Acceptance shall be issued by the Director of Information and Communication Technology Systems Services (ICTSS).



6 SERVICE LEVEL AGREEMENT

6.1 DBM shall maintain a Service Level Agreement (SLA) with the CONTRACTOR, with provision for liquidated damages for their non-compliance.

Component	Description	Liquidated Damages
6.1.1 Delivery, Installation, Configuration and Operationability	The CONTRACTOR shall deliver, install, configure, and make operational the Advanced Endpoint Security Solution and its components for 1,500 devices (servers, workstations and mobile devices) within sixty (60) calendar days from receipt of Notice to Proceed (NTP).	One (1) % of the total contract price shall be imposed for everyday of delay.
6.1.2 Technical Support	<p>The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in a form of telephone call, electronic mail, and/or on-site support.</p> <p>The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.</p>	1/10 th of 1% of the total contract price shall be imposed for every hour of delay. Said penalty shall be deducted from the special bank guarantee.
6.1.3 Technical Training	The CONTRACTOR shall provide Technology Transfer based on the schedule that will be provided by DBM-ICTSS prior to the engagement of the contract.	1/10 th of 1% of the total contract price shall be imposed for every day of delay. Said penalty shall be deducted from the special bank guarantee.
6.1.3 Documentation	The CONTRACTOR shall provide as-built documentation of the Advanced Endpoint Security Solution set-up/diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, configuration, integration, usage and backup within sixty (60) calendar days from the receipt of NTP.	1/10 th of 1% of the total contract price shall be imposed for every day of delay. Said penalty shall be deducted from the special bank guarantee.



7 WARRANTIES OF THE CONTRACTOR

- 7.1 The CONTRACTOR warrants that it shall conform strictly to the terms and conditions of the TOR.
- 7.2 The CONTRACTOR warrants, presents and undertaker reliability of the services and that their manpower complements are hardworking, qualified/reliable and dedicated to do the service required to the satisfaction of the DBM. It shall employ well-behaved and honest employees with ID displayed conspicuously while working within the compound. It shall not employ DBM employees to work in any category or whatsoever.
- 7.3 The CONTRACTOR in the performance of its services shall secure, maintain, at its own expenses all registration, licenses or permits required by Nation or Local Laws and shall comply with the rules, regulations and directives of Regulatory Authorities and Commissions.
- 7.4 The CONTRACTOR's personnel shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standard and established safety regulations, rules and practices.
- 7.5 The CONTRACTOR shall coordinate with the authorized and/or designated DBM personnel in the performance of their jobs.
- 7.6 The CONTRACTOR shall be liable for loss, damage or injury due directly or indirectly through the fault or negligence of its personnel. It shall assume full responsibility thereof and the BDM shall be specifically released from any and all liabilities arising therefrom.
- 7.7 The CONTRACTOR shall neither assign, transfer, pledge, nor sub-contract any part of interest therein.
- 7.8 The CONTRACTOR shall identify the certified technical support personnel that will be given authority to access and operate the specified equipment. DBM shall be informed thru a formal notice on the change or replacement of technical personnel five (5) days prior the actual rendering of technical support services.
- 7.9 The CONTRACTOR shall provide a services which shall include technical support and technology transfer which shall be covered by special band guarantee equivalent to 10% of the total contract price. The said amount shall be released after the lapse of the subscription period. Provided that all conditions imposed under the contract have been fully met.

The subscription period shall commence on the day the DBM issues the Certificate of Acceptance.



8 CONFIDENTIALITY OF DATA


- 8.1 All project personnel of CONTRACTOR shall be required to sign a Non-Disclosure Agreement (NDA).
- 8.2 The CONTRACTOR agrees to hold the Proprietary Information in strict confidence. The CONTRACTOR furthermore agrees not to reproduce, translate or disclose the Proprietary Information to 3rd parties without prior written approval of the DBM.

9 TERMS OF PRAYMENT

- 9.1 The CONTRACTOR shall be paid upon provision of license and support service of this Project subject to the required Final Withholding VAT (Services) of five percent (5%) and Expanded Withholding Tax of two percent (2%).
- 9.2 Payment shall be made within a reasonable time from the submission of the documentary requirements such as, but not limited to the following, based on existing accounting and auditing rules and regulations:
- 9.2.1 Sales Invoice/Billings
 - 9.2.2 Training Certificate and Manual
 - 9.2.3 Documentation
 - 9.2.4 Certificate of Acceptance issued by ICTSS Director
 - 9.2.5 Non-Disclosure Agreement
- 9.3 No advance payment shall be made as provided for in Section 88 of PD 1445.

10 PRE-TERMINATION OF CONTRACT

- 10.1 The contract for the Renewal of Licenses for the Subscription of Advanced Endpoint Security Solution may be pre-terminated by the DBM for any violation of the terms of the contract. In case of pre-termination, the CONTRACTOR shall be informed by the DBM thirty (30) days prior to such pre-termination.
- 10.2 In case of pre-termination, the CONTRACTOR shall be liable to an additional liquidated damages equivalent to one percent (1%) of the contract price as provided by the Government Accounting Manual (GAM) and forfeiture of the Performance Security.
- 10.3 The DBM shall have the right to blacklist the CONTRACTOR in case of pre-termination.



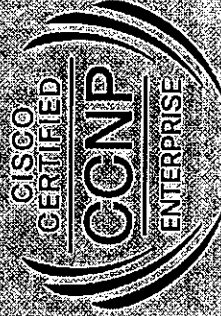


Cisco Certifications

Cherubim S Ramirez

has successfully completed the Cisco certification exam requirements and is recognized as a

Cisco Certified Network Professional Enterprise



Date Certified January 24, 2015
Valid Through May 3, 2021
Cisco ID No. CSCO12228329

Validate this certificate's authenticity at:
www.cisco.com/go/verifycertificate
Certificate Verification No. LKCBP9XPDGRE1Z37

© 2020 Cisco and/or its affiliates

Chuck Robbins
Chief Executive Officer
Cisco Systems, Inc.

CERTIFIED COPY



Certificate of Accreditation

for

Palo Alto Networks

is hereby granted to

Bradley Pucan

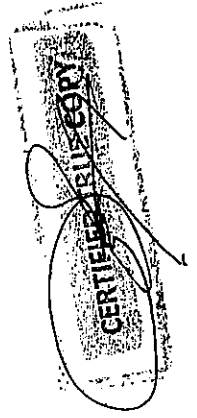
for successful completion of

**Palo Alto Networks Accredited Systems Engineer (PSE): Endpoint Associate Accreditation
Exam**

Date: 2/11/2020



Linda Moss
VP Global Enablement





Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom detection rules.
- **Reduce alerts by 50 times:** Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts.
- **Investigate eight times faster:** Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- **Stop attacks without degrading performance:** Obtain the most effective endpoint protection available with a lightweight agent.
- **Maximize ROI:** Use existing infrastructure for data collection and control to lower costs by 44%.

Cortex XDR

Cut Through the Noise and Focus on Real Threats with Extended Detection and Response

Security teams can't detect and stop active attacks quickly. Even though they've deployed countless security tools, they lack the enterprise-wide visibility and deep analytics needed to find threats. These siloed tools generate endless alerts and force analysts to pivot from console to console to verify threats, resulting in missed attacks. Faced with a shortage of security professionals, teams must simplify operations.

Prevent, Detect, Investigate, and Respond to All Threats

Cortex XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies

prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. Combined with our Managed Threat Hunting service, Cortex XDR gives you round-the-clock protection and industry-leading coverage of MITRE ATT&CK® techniques.

Block the Most Endpoint Attacks with Best-in-Class Prevention

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response. The integrated Device Control module granularly manages USB access to prevent data loss and malware delivery from malicious devices. The agent shares protections across network and cloud security offerings from Palo Alto Networks to provide ironclad, consistent security across the entire enterprise.

Detect Stealthy Threats with Machine Learning and Analytics

Cortex XDR identifies evasive threats with unmatched accuracy by continuously profiling user and endpoint behavior with analytics. Machine learning models analyze data from Palo Alto Networks and third-party sources to uncover stealthy attacks targeting managed and unmanaged devices.

Investigate and Respond at Lightning Speed

Cortex XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

Get MDR Services from Our Industry-Leading Partners

Powered by Cortex XDR, our managed detection and response (MDR) partners' services relieve the day-to-day burden of security operations and provide the instant maturity of a 24/7 SOC, delivering a range of services from alert management to incident response and threat hunting. Get help with custom tuning and deployment to get up and running in weeks, not years, and immediately benefit from decades of investigations, forensics, and security operations expertise.

Key Capabilities

Safeguard Your Assets with Industry-Best Endpoint Protection

Prevent threats and collect data for detection and response with a single, cloud native agent. The Cortex XDR agent offers

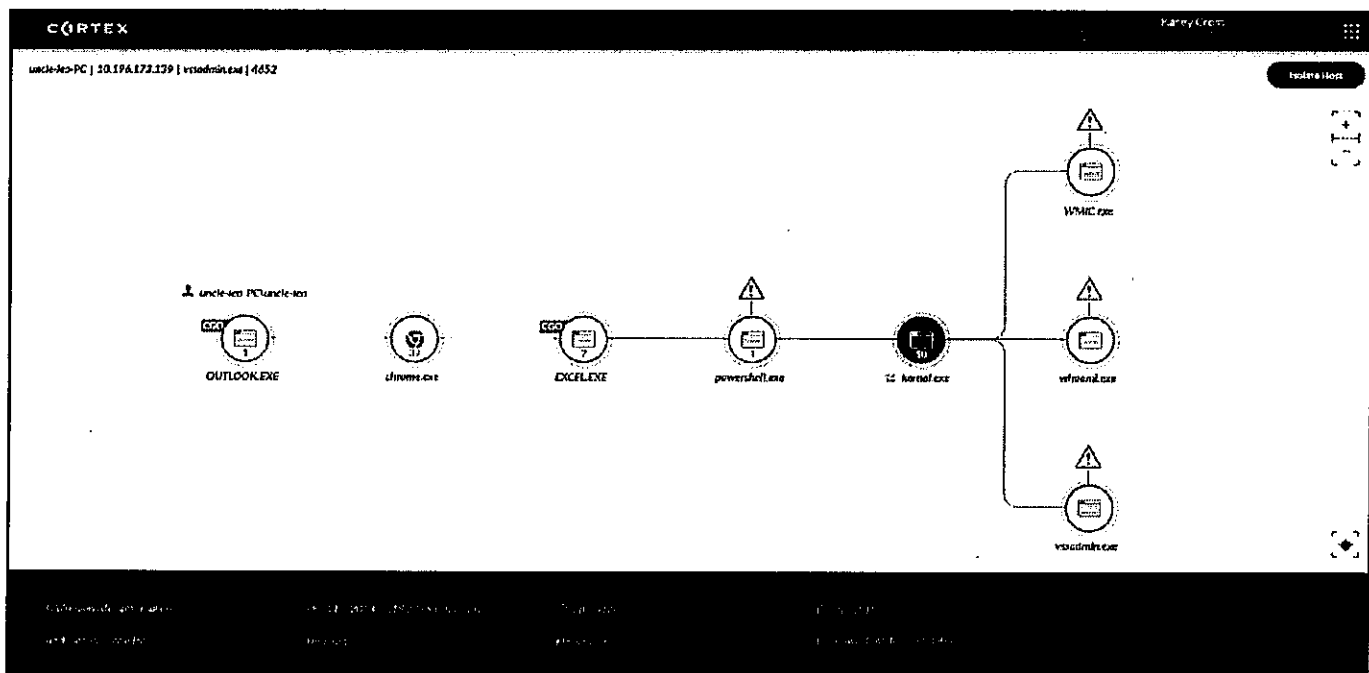


Figure 1: Cortex XDR triage and investigation view

a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptive AI-driven local analysis engine that's always learning to counter new attack techniques. A Behavioral Threat Protection engine examines the behavior of multiple, related processes to uncover attacks as they occur. Integration with the Palo Alto Networks WildFire® malware prevention service boosts security accuracy and coverage. Read more about endpoint protection.

Securely Manage USB Devices

Protect your endpoints from malware and data loss with Device Control. The Cortex XDR agent allows you to monitor and secure USB access without needing to install another agent on your hosts. You can restrict usage by vendor, type, endpoint, and Active Directory® group or user. Granular policies allow you to assign write or read-only permissions per USB device.

Protect Endpoint Data with Host Firewall and Disk Encryption

Reduce the attack surface of your endpoints. With host firewall and disk encryption capabilities, you can lower your security risks as well as address regulatory requirements. The Cortex XDR host firewall enables you to control inbound and outbound communications on your Windows® endpoints. Additionally, you can apply BitLocker® encryption or decryption on your endpoints by creating disk encryption rules and policies. Cortex XDR provides full visibility into Windows endpoints that were encrypted using BitLocker and lists

all the encrypted drives. Host firewall and disk encryption capabilities let you centrally configure your endpoint security policies from the Cortex XDR management console.

Get Full Visibility with Comprehensive Data

Break security silos by integrating all data. Cortex XDR automatically stitches together endpoint, network, and cloud data to accurately detect attacks and simplify investigations. It collects data from Palo Alto Networks products as well as third-party logs and alerts, enabling you to broaden the scope of intelligent decisions across all network segments. Third-party alerts are dynamically integrated with endpoint data to reveal root cause and save hours of analysts' time. Cortex XDR examines logs collected from third-party firewalls with behavioral analytics, enabling you to find critical threats and eliminate any visibility blind spots.

Discover Threats with Continuous ML-Based Threat Detection

Find stealthy threats with analytics and out-of-the-box rules that deliver unmatched MITRE ATT&CK coverage. Cortex XDR automatically detects active attacks, allowing your team to triage and contain threats before the damage is done. Using machine learning, Cortex XDR continuously profiles user and endpoint behavior to detect anomalous activity indicative of attacks. By applying analytics to an integrated set of data, including security alerts and rich network, endpoint, and cloud logs, Cortex XDR meets and exceeds the detection capabilities of siloed network traffic analysis (NTA), endpoint detection and response (EDR), and user behavior analytics (UBA) tools. Automated detection works all day, every day, providing you peace of mind.



Figure 2: Customizable dashboard

Investigate Eight Times Faster

Automatically reveal the root cause of every alert. With Cortex XDR, your analysts can examine alerts from any source—including third-party tools—with a single click, streamlining investigations. Cortex XDR automatically reveals the root cause, reputation, and sequence of events associated with each alert, lowering the experience level needed to verify an attack. By consolidating alerts into incidents, Cortex XDR slashes the number of individual alerts to review and alleviates alert fatigue. Each incident provides a complete picture of an attack, with key artifacts and integrated threat intelligence details, accelerating investigations.

Manually Hunt for Threats with Powerful Search Tools

Uncover hidden malware, targeted attacks, and insider threats. Your security team can search, schedule, and save queries to identify hard-to-find threats. Flexible searching capabilities let your analysts hunt threats and search for both indicators of compromise (IOCs) and behavioral indicators of compromise (BIOCs) without learning a new query language. By incorporating threat intelligence from Palo Alto Networks with a complete set of network, endpoint, and cloud data, your team can catch malware, external threats, and internal attacks whether the incidents are in progress or have occurred in the past.

Coordinate Response Across Endpoint, Network, and Cloud Enforcement Points

Stop threats with fast and accurate remediation. Cortex XDR lets your security team instantly contain endpoint, network, and cloud threats from one console. Your analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update prevention lists like bad domains through tight integration with enforcement points. The powerful Live Terminal feature lets Tier 1 analysts swiftly investigate and shut down attacks without disrupting end users by directly accessing endpoints; running Python®, PowerShell® or system commands and scripts; and managing files and processes from graphical file and task managers.

24/7 Threat Hunting Powered by Cortex XDR and Unit 42 Experts

Augment your team with the industry's first threat hunting service operating across endpoint, network, and cloud data. Cortex XDR Managed Threat Hunting offers round-the-clock monitoring from world-class threat hunters to discover attacks anywhere in your environment. Our Unit 42 experts work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware. To detect adversaries hiding in your organization, our hunters comb through comprehensive data from Palo Networks and third-party security solutions. Detailed Threat Reports reveal the tools, steps, and scope of attacks so you can root out adversaries quickly, while Impact Reports help you stay ahead of emerging threats.

Natively Integrate with Cortex XSOAR for Security Orchestration and Automation

Standardize and automate response processes across your security product stack. Cortex XDR integrates with Cortex™ XSOAR, our security orchestration, automation, and response platform, enabling your teams to feed incident data into Cortex XSOAR for automated, playbook-driven response that spans more than 370 third-party tools and promotes cross-team collaboration. Cortex XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks. You can leverage Cortex XSOAR case management to monitor and correlate Cortex XDR incidents with other alerts in your organization.

Unify Management, Reporting, Triage, and Response in One Intuitive Console

Maximize productivity with a seamless platform experience. The management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response. You can quickly assess the security status of your organization's or individual endpoints with customizable dashboards, and summarize incidents and security trends with graphical reports that can be scheduled or generated on demand. Public APIs extend management to third-party tools, enabling you to retrieve and update incidents, collect agent information, and contain endpoint threats from the management platform of your choice.

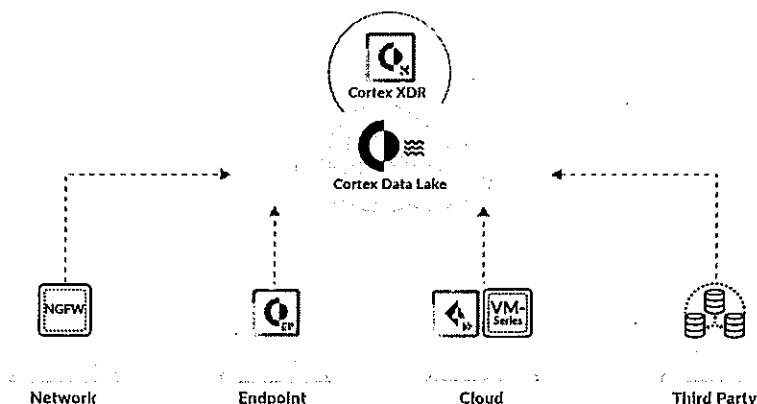


Figure 3: Analysis of data from any source for detection and response

Operational Benefits

Block known and unknown attacks with powerful endpoint protection: Leverage AI-based local analysis and Behavioral Threat Protection to stop the most malware, exploits, and fileless attacks in the industry.

Gain visibility across network, endpoint, and cloud data: Collect and correlate data from Palo Alto Networks and third-party tools to detect, triage, investigate, hunt, and respond to threats.

Automatically detect sophisticated attacks 24/7: Use always-on AI-based analytics and custom rules to detect advanced persistent threats and other covert attacks.

Avoid alert fatigue and personnel turnover: Simplify investigations with automated root cause analysis and a unified incident engine, resulting in a 98% reduction in alerts and lowering the skill required to triage alerts.

Increase SOC productivity: Consolidate endpoint security policy management and monitoring, investigation, and response across your network, endpoint, and cloud environments in one console, increasing SOC efficiency.

Eradicate threats without business disruption: Shut down attacks with surgical precision while avoiding user or system downtime.

Eliminate advanced threats: Protect your network against malicious insiders, policy violations, external threats, ransomware, fileless and memory-only attacks, and advanced zero-day malware.

Supercharge your security team: Disrupt every stage of an attack by detecting IOCs, anomalous behavior, and malicious patterns of activity.

Continually improve your security posture: Save threat hunting searches as behavioral rules to detect similar threats in the future. Flexible informational alerts improve timeline analysis by identifying suspicious behavior and making complex events easy to understand.

Extend detection, investigation, and response to third-party data sources: Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster, more effective investigations.

Ease Deployment with Cloud Delivery

Get started in minutes. The cloud native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy new on-premises network sensors or log collectors. You can use your Palo Alto Networks products or third-party firewalls to collect data, reducing the number of products you need to manage. You only need one source of data, such as

Next-Generation Firewalls or Cortex XDR agents, to detect and stop threats, but additional sources can eliminate blind spots. Easily store data in Cortex Data Lake, a scalable and efficient cloud-based data repository. By integrating data from multiple sources together, automating tasks, and simplifying management, Cortex XDR delivers a 44% cost savings compared to siloed security tools.

Table 1: Cortex XDR Features and Specifications

Detection and Investigation Features and Capabilities

Automated stitching of network, endpoint, and cloud data from Palo Alto Networks and third-party sources	Machine learning-based behavioral analytics
Third-party alert and log ingestion from any source with required network information	Custom rules to detect tactics, techniques, and procedures
Third-party log data from Check Point, Fortinet, and Cisco ASA firewalls	Root cause analysis of alerts
Cloud-based malware prevention with WildFire	Timeline analysis of alerts
Malware and fileless attack detection	Unified incident engine
Detection of targeted attacks, malicious insiders, and risky user behavior	Post-incident impact analysis
Network traffic analysis (NTA) and user behavior analytics (UBA)	Dashboards and reporting
Endpoint detection and response (EDR)	IOC and threat intelligence searches
Native integration with Cortex XSOAR for orchestration, automation, and response	Threat hunting
Cortex XDR Managed Threat Hunting service	Incident response and recovery

Table 1: Cortex XDR Features and Specifications (continued)

Endpoint Protection Capabilities	
Malware, ransomware, and fileless attack prevention	Disk encryption with BitLocker
Behavioral Threat Protection	Endpoint script execution (available with Cortex XDR Pro)
AI-based local analysis engine	Optional automatic agent upgrades
Integration with the cloud-based WildFire malware prevention service	Live Terminal for direct endpoint access
Child process protection	Network isolation, quarantine, process termination, file deletion, file blacklist
Exploit prevention by exploit technique	Public APIs for response and data collection
Device control for USB device management	Credential theft protection
Host firewall	Scheduled and on-demand malware scanning
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Reduction of MTTD and MTTR
Investigation of every alert and incident generated by Cortex XDR	Custom tuning of Cortex XDR for enhanced prevention, visibility, and detection
Guided or full threat remediation actions	Direct access to partners' analysts and forensic experts
Technical Specifications	
Delivery model	Cloud-delivered application
Data retention	30-day to unlimited data storage
Cortex XDR Prevent subscription	Endpoint protection with Cortex XDR agents
Cortex XDR Pro per endpoint subscription	<ul style="list-style-type: none"> Detection, investigation, and response across endpoint data sources Endpoint protection with Cortex XDR agents
Cortex XDR Pro per TB subscription	Detection, investigation, and response across network and cloud data sources, including third-party data
Cortex XDR Managed Threat Hunting subscription	24/7 threat hunting powered by Cortex XDR and Unit 42 experts
Cortex XDR Pathfinder endpoint analysis service	Collects process information from endpoints that do not have Cortex XDR agents; included with all Cortex XDR subscriptions

Reinvent Security Operations with Cortex

Cortex XDR is part of Cortex™, the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities. The suite is built on the tightly integrated offerings of Cortex XDR and Cortex XSOAR, which enables you to transform your SOC operations from a manual, reactive model that required endless resources to a lean, proactive, and automated team that reduces both MTTD and MTTR for every security use case.

Operating System Support

The Cortex XDR agent supports multiple endpoints across Windows®, macOS®, Linux, Chrome® OS, and Android® operating systems. For a complete list of system requirements and supported operating systems, please visit the Palo Alto Networks Compatibility Matrix. Cortex XDR Pathfinder minimum requirements: 2 CPU cores, 8 GB RAM, 128 GB thin-provisioned storage, VMware ESXi™ V5.1 or higher, or Microsoft Hyper-V® 6.3.96 or higher hypervisor.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. cortex-xdr-051520

XDR: Enterprise-Scale Detection and Response

Everything you need to know about the market category that
is unifying data silos and reshaping security operations



Table of Contents

1	Introduction	23	Use Cases for XDR
2	About This Guide	24	Detection
2	The Challenge	27	Alert Triage and Validation
4	The Elusive Balance	29	Automated and Simplified Investigations and Response
7	Technologies for Detection and Response	31	Threat Hunting
7	EDR	33	Conclusion
8	SIEM	34	XDR RFP Checklist
9	NTA and UEBA		
11	The Bottom Line		
11	Addressing the Security Skills Gap		
13	Defining XDR		
14	Requirement 1: Find Stealthy Threats Faster with Analytics Across Network, Endpoint, and Cloud		
17	Requirement 2: Simplify Investigation and Response to Known and Unknown threats		
19	Requirement 3: Improve the ROI of Current and Future Security Investments		

Introduction

Year after year, the challenge of securing critical data intensifies. Evolving technology trends, including the recent growth in cloud and IoT adoption, continue to expand the enterprise cyberattack surface and make companies' sensitive data more vulnerable to sophisticated attackers. At the same time, adversaries use those exact tools to increase their own power and scale, allowing them to efficiently wage repeated attacks—and they only need to succeed once. Future technologies threaten to exacerbate both of these problems.

Security teams have deployed tools, processes, and staffing models to respond to new threat vectors as they have emerged, but they are outnumbered and outgunned. The consequence of continually bolting new capabilities onto existing systems over time is an eventual mess of poorly integrated tools that require a lot of time, energy, and experience to utilize. Junior analysts are charged with the impossible task of triaging a never-ending stream of security alerts despite limited training and equally limited toolkits. The combination of too many alerts and too little context causes security teams to lose visibility and become less agile than their adversaries. Ultimately, the company becomes even more vulnerable as a result.

"XDR" emerged as a market category in response to this complexity, the basic premise being a simple one: XDR is a category of threat detection, investigation, and response solutions that work across all threat vectors in a company's infrastructure (i.e., network, endpoint, and cloud), rather than just one piece thereof. By increasing integration, XDR tools also increase visibility and insight for both for the machine learning models powering them and the security analysts using them.

"Cybercrime is the greatest threat to every company in the world."

Source: Ginni Rometty, CEO, IBM



About This Guide

Need to get up to speed on the XDR category and what it means for your company? You've come to the right place. We will define XDR, describing its key capabilities, applicable use cases, and impact on key security operations functions. By the end of this guide, you will have a clear understanding of what XDR is and what it is not; the advantages it has over legacy detection and response tools; which capabilities to look for when evaluating XDR solutions; and how XDR can help to simplify and improve your security operations.

The Challenge

Reports of data breaches and attacks from sophisticated adversaries have become so frequent that society has become numb to them. In the business world, it's become an accepted reality and running joke that "you have adversaries in your environment, whether you know it or not." The fact that adversaries are commonplace does not, however, make them less dangerous. The truth is that every minute an active adversary operates within your environment, untold damage occurs. As a security operations professional, you already know this and doubtless work hard to detect attacks and respond as quickly and effectively as possible—before data loss can occur.

This is an uphill battle in the face of increasingly advanced attacks and tactics used by adversaries. Attackers can now compromise devices without using file-based malware at all. Sophisticated attackers use different approaches, such as compromising authorized system files, inserting attacks into a device's registry, or using utilities like PowerShell maliciously. This has driven the need for new methods of detection.

**Almost 4 million
digital records are
stolen from
breaches every day.**

Source: Cybersecurity Ventures



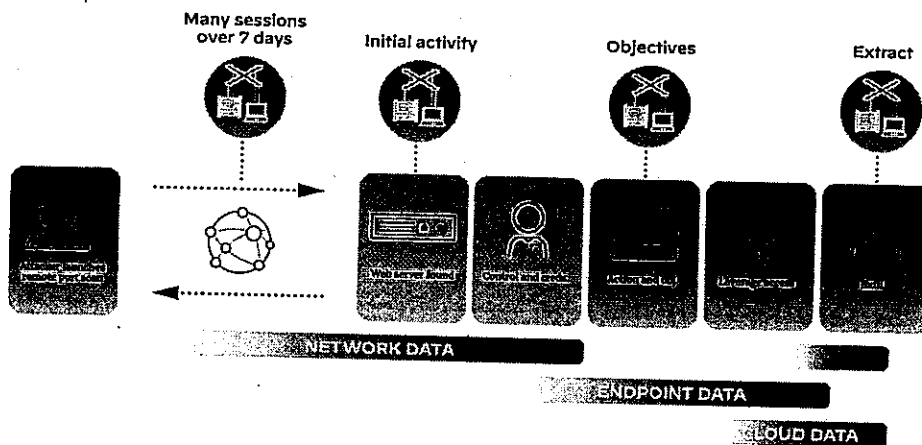


Figure 1: Example of a multi-stage attack

Further complicating matters is the continued investment in new technologies like the cloud and internet of things (IoT) to move faster, increase agility, and use data in new ways. Each of these new technologies gives attackers additional ways to enter and exploit your infrastructure. Your security team must employ the best prevention possible, optimize the ability to locate adversaries, decrease the time those adversaries dwell in your environment, and accelerate the response to the incident.



Signature

The Elusive Balance

An organization's ability to achieve these objectives relies on two things: effective tools and a team of capable security analysts. Unfortunately, having the proper balance of technology and human capital tends to be the exception rather than the rule.

Detection and prevention technologies generate hundreds or thousands of alerts per day—far exceeding the amount security teams are staffed to handle. These alerts come from many disconnected sources, leaving analysts to piece the puzzle together. Analysis of a potential threat generally requires a number of steps:

- 1) Review available log data to start piecing together what may have occurred.
- 2) Manually compare against threat intelligence sources to determine if indicators are known to be malicious.
- 3) Find information gaps and search for available data that may indicate additional steps in the attack.
- 4) Check if new information links to alerts being handled by other team members to coordinate efforts.
- 5) Evaluate whether the alert needs to be escalated, discarded, or quickly remediated and closed out.

**69% of organizations
don't trust their anti-
virus software to
block threats to their
environments.**

Source: Ponemon Institute



All of these steps traditionally take a lot of time and multiple tools to complete—and that's just triage. The net result is that analysts only have time to address the highest priority alerts they come across each day; meanwhile, a disconcerting number of lower priority alerts aren't addressed at all.

Further, security analysts who are responsible for alert triage are often left with insufficient context to determine the real risk an attack presents to the organization. Thus, the alert is escalated to a more sophisticated group for further validation, requiring even more time, labor, and resources—creating inefficiencies at all levels of the system.

Many organizations attempt to use APIs to integrate their detection and response data. This generally involves using an expensive SIEM as the centerpiece of their security operations, which aggregates log data by parsing and normalizing it, thus stripping away much of the valuable context. Security teams get to see the log data in one place, but it isn't pieced together meaningfully, and the frontline analysts charged with making sense of it often can't use the tools that contain the richer source data.

Other companies choose to outsource their detection and response functions, entirely or in part, to either managed security service providers (MSSP) or even more threat-focused managed detection and response (MDR) vendors. There's nothing wrong with outsourcing this function, particularly for organizations with smaller security budgets or that don't have the desire or resources to manage their own security; however, organizations that want comprehensive visibility and control shouldn't be stuck outsourcing their security simply because their tools are inadequate. It's also worth noting that the technology stack is just as important for an outsourced security team; vendors using legacy tools will wrestle with the same inefficiencies that plague in-house security teams.



What's really needed is a set of technologies to reduce the total number of alerts while at the same time allowing less sophisticated analysts to efficiently and confidently assess threats on their own, ensuring that only fully validated alerts are escalated to more senior analysts.

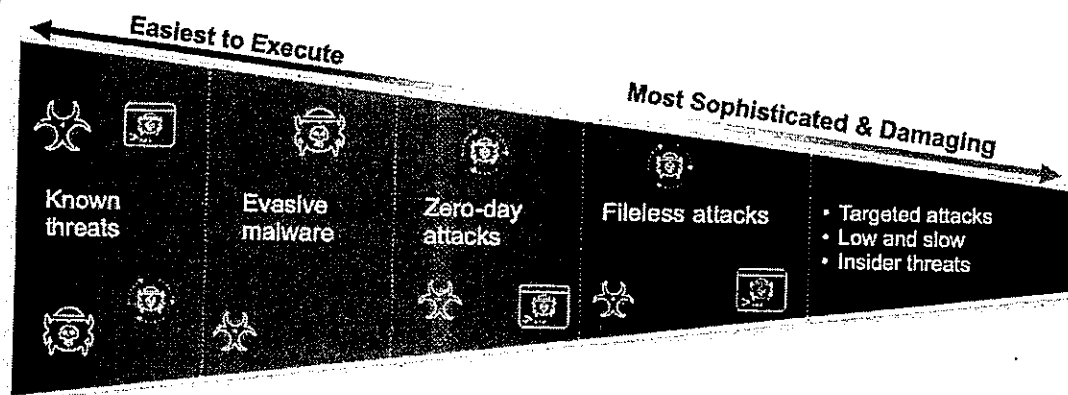


Figure 2: Detection and response tools are designed to stop sophisticated attacks



Technologies for Detection and Response

While the ultimate goal remains preventing successful attacks, organizations must plan for the reality that some percentage of crafty attackers will find their way into their infrastructure and accomplish their objectives. An array of logging, detection, and response tools has come to market to help security teams find threats that have managed to circumvent prevention. Each of these tools has strengths and weaknesses, and can be useful against simple attacks, such as known file-based malware scenarios or attacks that threaten just one part of the infrastructure. Most of them, however, are tuned for a single purpose, and none is particularly well-suited to handle complex campaigns on its own. For those reasons, security teams primarily rely on the detection and response tools described in the sections that follow.

EDR

Gartner definition: The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems. EDR solutions must provide the following four primary capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

IDC predicts a compound annual growth rate of 9.9% in security spending through 2022.

Source: Worldwide Security Spending Guide, IDC



Endpoint detection and response (EDR) first emerged in 2013 to help forensic investigations requiring very detailed endpoint telemetry to reverse engineer malware and understand exactly what the attacker did on a compromised device.

EDR alone cannot provide enterprise threat detection due to its sole focus on the endpoint. It doesn't offer visibility into network traffic of devices without installing agents on devices (IoT, BYOD, ICS, as well as switches, routers, servers, etc.) and cloud resources (e.g., workloads, cloud networks, PaaS). Further, companies use many unmanaged endpoint devices that cannot support EDR agents, providing potential attackers with unmonitored entry points.

SIEM

Gartner definition: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

Many organizations allocate large portions of their security budgets to SIEM tools to gather logs from security devices (IDS/FW) and server environments (event logs). SIEMs were initially designed primarily as log collectors for compliance reporting purposes. Over time, their usage expanded to threat detection, and SIEMs are now the central alert repository for many security operations centers.

Gartner data indicates that security is a top driver of IT spending, and detection and response is the top category of security spending.

Source: Gartner



SIEM centralizes alerts from many security and network devices and alerts on common attacks. Looking to the SIEM for advanced detection is challenging because the SIEM can only look for specific attacks using rules enumerated in the system. If a sophisticated attacker uses a new pattern, a SIEM will likely miss the attack. Moreover, the logs driving SIEM-based analysis don't provide the context required to validate alerts, as much of the contextual data is lost in normalization. Therefore, other systems are required to determine if a device is really compromised or data is being exfiltrated.

NTA and UEBA

Gartner definitions:

Network traffic analysis (NTA) uses a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks. NTA tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NTA tools detect abnormal traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NTA solutions can also monitor east/west communications by analyzing network traffic or flow records that it receives from strategically placed network sensors.

User and entity behavior analytics (UEBA) offers profiling and anomaly detection based on a range of analytics approaches, usually using a combination of basic analytics methods (e.g., rules that leverage signatures, pattern matching and simple statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic and data repositories) to discover potential incidents.



Finally, a newer class of security analytics tools, including NTA and UEBA, emerged to address the challenges SIEM has in detecting unknown attacks. These tools use machine learning to develop a baseline of activity from the gathered telemetry and then look for atypical actions that may indicate malicious behavior. These technologies allow organizations to identify previously unknown attacks by recognizing unusual traffic patterns.

These tools also have their limitations. Network-based products are limited to the network and cannot monitor or track local events, such as process information gathered on the endpoints. NTA also has very limited depth; if EDR is deep and narrow, NTA is wide and shallow. UEBA tools are heavily reliant on third-party logs to monitor and detect network and endpoint-based security threats. The UEBA then analyzes these threats to assign risk scores to users. However, if the third-party tools fail in their detections, or aren't logging a certain piece of infrastructure, then the UEBA is rendered ineffective.

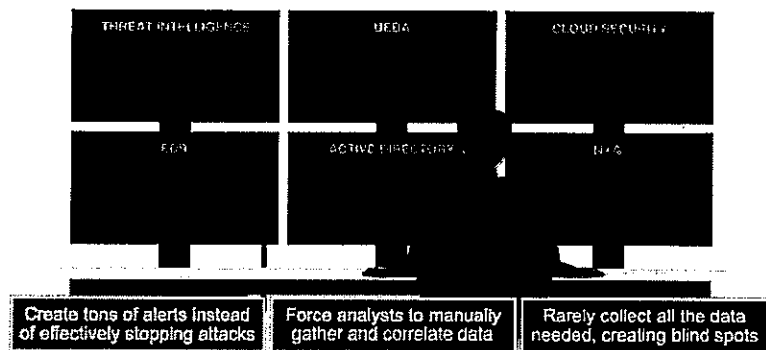


Figure 3: Siloed tools slow down investigation and response



[Handwritten signature]

The Bottom Line

The complexity of modern attacks requires analysis of multiple data sources to identify and confirm malicious activity. Layering on one-dimensional tools adds significant expense for security teams, creates potential blind spots, and requires a lot of manual effort on the part of security analysts to switch between software applications and make sense of an attack. 451 Research has found that 76% of security teams initiate at least a quarter of their attacks through manual threat hunting, indicating that the detection technologies and processes they have in place to surface attacks are not delivering against the objective. Unless you have full visibility and analysis of all the components in your environment, you could be missing threats.

Addressing the Security Skills Gap

Even with better and more comprehensive tools for threat detection, dealing with alerts—and possible incidents—requires further validation and triage from skilled responders. Unfortunately, there are not enough of these security practitioners, and this significant skills gap impacts the ability of organizations to keep pace with attackers.

Adversaries now utilize highly automated attacks to find vulnerabilities and gain initial presence in your environment. This further exacerbates the skills gap as attackers are able to scale their automated toolkits faster and more affordably than organizations can add skilled security personnel. Thus, you need to look for tools that make your less experienced personnel more effective and efficient, automating repetitive tasks, simplifying investigations, and helping analysts to improve their skills.

ESG Research found that 66% of organizations feel their threat detection and response effectiveness is limited because it is based on multiple independent point tools.

Source: ESG



Conclusion: Most enterprises receive thousands of alerts from a multitude of monitoring solutions, but more noise is counterproductive. Advanced detection is not about more alerts; it's about better alerts—more actionable alerts. Achieving this requires integration of not only all of the detection technologies in use but also sophisticated analytics that analyze endpoint, network, and cloud data to find and validate adversary activity in your environment.

Tactical detection and response solutions have not solved the problem of finding advanced attackers. Organizations still get hacked and data is lost, so whatever skills an enterprise can field need to work more effectively and efficiently.

**There are over
300,000 available
cybersecurity job
openings in the
US today—a number
expected to grow
substantially in the
coming years.**

Source: Cyberseek



Defining XDR

XDR is a new category that has emerged to meet the need for more comprehensive and sophisticated detection and response. The "X" stands for any data source, recognizing that it's not efficient or effective to look at individual components of the infrastructure in isolation. XDR uses machine learning and dynamic analysis techniques to combine capabilities and outcomes associated with SIEM, UEBA, NTA, and EDR.

The "X" stands for any data source.

If XDR is the future of detection and response, it must meet the key challenges that we face on a daily basis. With that in mind, let's define the requirements for XDR based on the challenges identified above.

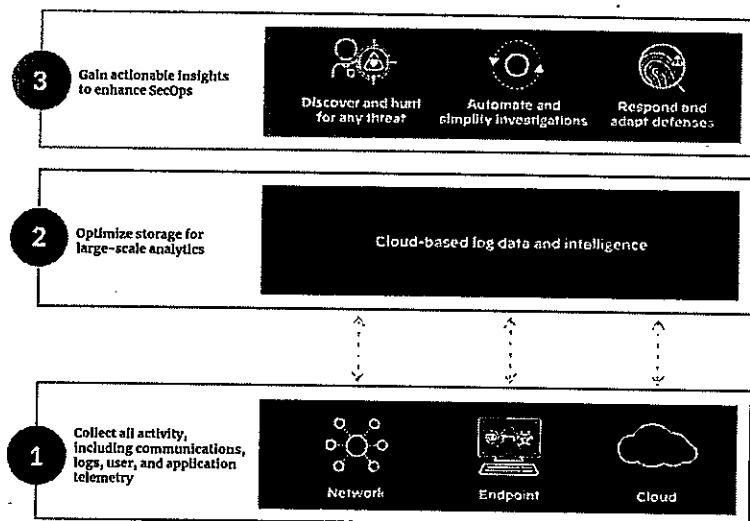


Figure 4: XDR breaks the traditional silos of detection and response



Requirement 1: Find Stealthy Threats Faster with Analytics Across Network, Endpoint, and Cloud

The first step in detection in response is, logically, detection. If you can't see a threat, you can't investigate it; and you certainly can't stop it. Attackers leverage the power of cloud and machine learning to wage multifaceted campaigns that allow them to gain persistence and exfiltrate critical data and intellectual property. This means XDR must have all of the capabilities that follow.

Broad Visibility and Contextual Understanding

Siloed point products lead to siloed data—and that's no longer acceptable. You can't possibly hope to fight attackers effectively if you aren't at least as nimble in your own environment as they are. XDR must have visibility and detection capabilities across your entire environment, integrating telemetry from your endpoints, networks, and cloud environments. Moreover, it must be able to correlate these data sources to understand how various events are linked and when a certain behavior is, or isn't, suspicious based on context.

Data Retention

Attackers can be patient. They know they are harder to detect if they move slowly, waiting out the log retention periods of the detection technologies they are up against. XDR should not make this easy for them. Your detection systems need to collect, correlate, and analyze data from the network, endpoint, and cloud within a single repository, offering 30 days or more of historical retention.

88% of hackers believe they can infiltrate a target in less than 12 hours.

Source: Nuix (via NBC)



Analysis of Both Internal and External Traffic

Traditional detection techniques focus primarily on external attackers, providing an incomplete view of potential adversaries. Detection cannot solely look for attacks coming from beyond the perimeter. It must also profile and analyze internal constituencies to look for anomalous and potentially malicious behavior to identify credential misuse.

Integrated Threat Intelligence

You must be equipped to deal with unknown attacks. One method of balancing the scales is leveraging known attacks that other organizations see first. Detection needs to rely on threat intelligence gathered across a global network of enterprises. When an organization within the extended network identifies an attack, you can use the knowledge gained from the initial attack to identify subsequent attacks within your organization.

Customizable Detection

Protecting every organization presents unique challenges concerning specific systems, user constituencies, and adversaries. Detection systems must also be highly customizable based on the specific needs of your environment. This involves supporting both custom and predefined detections.

Machine Learning-Based Detection

With attacks that don't look like traditional malware, such as those that compromise authorized system files, utilize scripting environments, and attack the registry, detection technology needs to use advanced analytical techniques to analyze all of the collected telemetry. These approaches include supervised and semi-supervised machine learning.

Only 38% of organizations feel that they are prepared to handle a sophisticated cyber-attack.

Source: Cybint



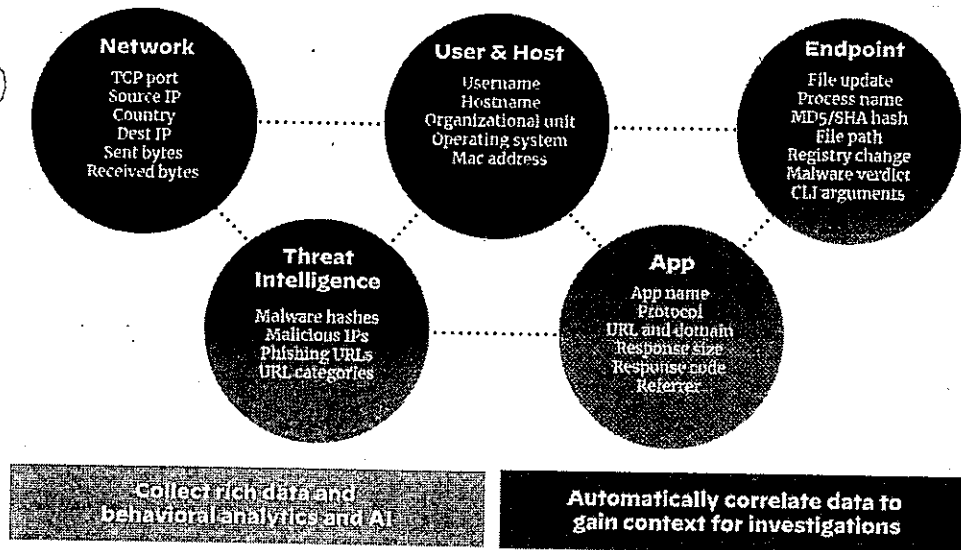


Figure 5: XDR correlates and stitches together rich data



Signature

Requirement 2: Simplify Investigation and Response to Known and Unknown Threats

Once you are alert to the potential threats in your environment, you must be able to quickly triage and investigate those threats. Doing this quickly and effectively—especially during an attack that touches multiple parts of your infrastructure—is where traditional detection and response systems fail. XDR solutions can dramatically improve the investigation process. These next sections explain how.

Correlation and Grouping of Related Alerts and Telemetry Data

By the time you receive an alert, the attacker is already hard at work to carry out the mission and achieve an objective. Thus, time is of the essence. You need to be able to quickly understand the attack and its full causality chain. This first means your XDR tool must reduce noise by automatically grouping related alerts and effectively prioritizing the events that most urgently require your attention. Then, your XDR tool must be able to build a timeline of the attack, stitching together activity logs from the network, endpoint, and cloud. By visualizing the activity and sequencing of events, the root cause of the attack can be determined, and the potential damage and proliferation assessed.

Consolidated User Interfaces with the Ability to Pivot

Once they start digging into alerts, the analysts need a streamlined work environment that enables them to pivot within the data from any source with a single click. Analysts should not have to waste time switching between two tools, let alone a multitude of different tools.



Manual and Automated Threat Hunting

An increasing number of organizations proactively hunt for active adversaries, allowing their analysts to develop attack hypotheses and look for relevant activity within the environment. Supporting threat hunting requires powerful search capabilities to look for evidence to prove the hypotheses as well as integrated threat intelligence to search for activity seen within the extended network. This threat intelligence should be integrated and automated in a way that makes it clear whether a threat has been seen before without requiring tons of manual analyst work, for example, opening 30 different browser windows to search numerous threat intelligence feeds for a "bad" IP address.

Orchestration Capabilities

Once attacker activity has been detected and investigated, the next step is efficient and effective enforcement. Your system must be able to orchestrate a coordinated response to active threats and prevent future attacks across network, endpoint, and cloud. This includes communication between prevention technologies (e.g., an attack blocked on the network automatically updates the policies on the endpoints), either natively or built through APIs. It also includes the ability for an analyst to take response actions directly through the XDR interface.



Requirement 3: Improve the ROI of Current and Future Security Investments

XDR should radically advance the return on your security investments. This means improving the efficiency of your team to help avoid and overcome staffing shortages, improving the integration between your existing tools, and strengthening your prevention efficacy over time with scalable infrastructure and artificial intelligence. To meet these criteria, XDR must have these next capabilities.

Security Orchestration

The same attributes that make orchestration important to simplifying investigations also allow it to maximize the ROI of your security stack. Every organization has an installed base of security controls that can be brought to bear in responding to active threats. A key aspect of any detection and response system is to leverage the investments in these existing controls, ensuring any response can be undertaken consistently across the enterprise.

Third-Party Data Ingestion

All enterprises have heterogeneous security toolkits. The more an XDR solution is able to have visibility into data from each of those different tools, the more comprehensive the security it will be able to provide. The best XDR solutions will have the flexibility to ingest data from the other tools in your environment to maximize both value and effectiveness.



Scalable Storage and Compute

Given the unpredictability of today's adversaries, you don't want to discard telemetry that can provide clues as to attacker activity in slower persistent attacks. This requires sufficient capacity to store forensic evidence for months or even years, as well as analytics horsepower to be able to utilize all of the telemetry effectively. Cloud-based platforms provide this unrestricted accessibility and scale.

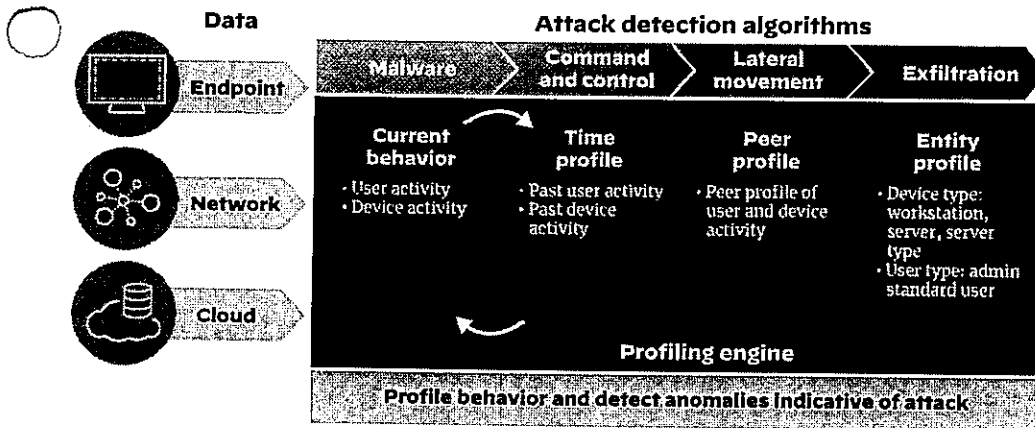
Improvement over Time

Detecting increasingly sophisticated attacks requires embedded artificial intelligence or machine learning as well as automation to reduce manual efforts in order to make scarce security analysts more effective and efficient. XDR solutions should learn from experience, reducing future risk and continually strengthening prevention by applying knowledge gained through detection, investigation, or response.

Reporting and Dashboards

Security teams need to be able to understand and communicate their security posture and operational metrics. Not only must XDR solutions be capable of providing better security outcomes, they must also be able to summarize the state of security through reports and dashboards.





XDR is a new way to think about detection and response, providing a broader view of your environment across networks, endpoints, and the cloud. Using advanced analytics and integrated threat intelligence ensures that both responders and hunters have the information they need at their fingertips to effectively and efficiently pinpoint and address attacker activity.

Figure 6: Pinpoint threats unique to your environment with AI



[Handwritten signature]

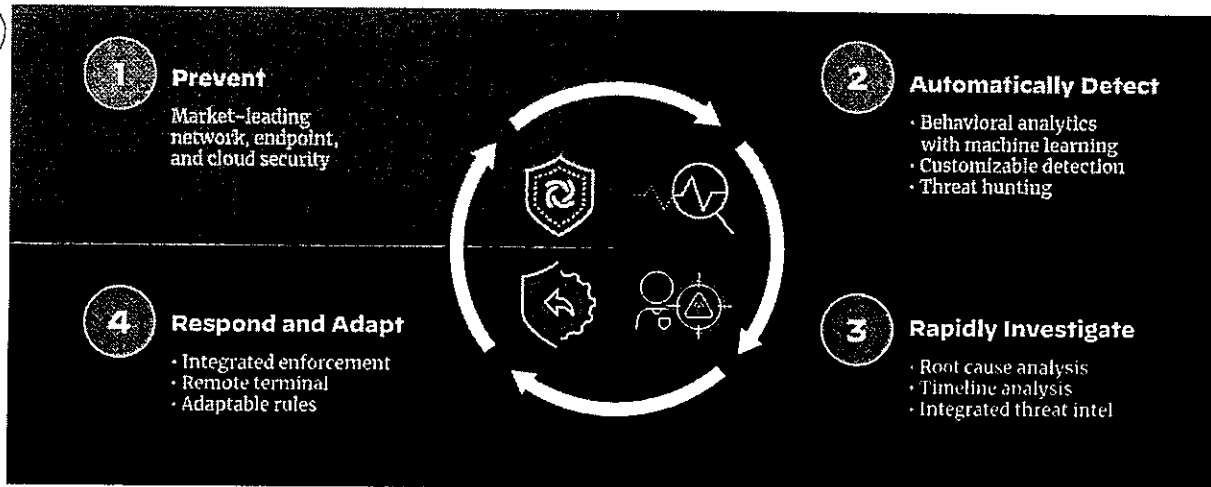


Figure 7: XDR adapts over time to continually improve defenses



[Handwritten signature]

Use Cases for XDR

Security operations teams big and small share some key functions. A traditional model for many SecOps teams divides these functions into a tiered analyst structure, based on level of experience. Here are the primary responsibilities of those tiers.

Tier 1: Triage

This is where the majority of security analyst hours are typically spent. Tier 1 analysts are generally the least experienced analysts, and their primary function is to monitor event logs for suspicious activity. When they feel that something needs further investigation, they gather as much information as they can and escalate the incident to Tier 2.

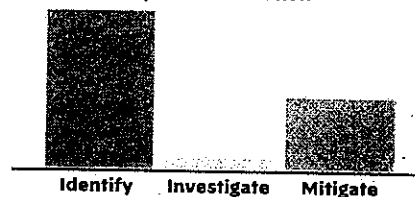
Tier 2: Investigation

Tier 2 analysts dig deeper into the suspicious activity to determine the nature of the threat and the extent to which it has penetrated the infrastructure. These analysts then coordinate a response to remediate the issue. This is a higher impact activity that often requires more analyst experience.

Tier 3: Threat Hunting

These are the most experienced analysts, who support complex incident response and spend any remaining time looking through forensic and telemetry data for threats that may not have been identified as suspicious by detection software. The average company spends the least time on threat hunting activities, as the activities of Tier 1 and Tier 2 consume so many analyst resources.

Traditional analyst time allocation



Ideal analyst time allocation

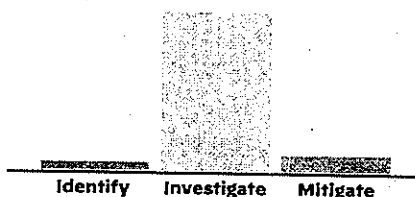


Figure 8: The traditional SOC model does not optimally use analyst time and talent



While this model may be the most common, it is not necessarily ideal. For one thing, most people are not well-suited to monitoring logs all day long. Alert fatigue is real, and threats slip through among all the noise generated by the myriad sensors in a SOC. It can be hard to retain analysts to perform this task; they'd much rather be contributing meaningfully to investigations (and may have new and innovative approaches that are never revealed because they don't have the technical skills required for legacy investigation processes). Secondly, far too little time is spent on threat hunting and process improvement, as the majority of resource hours are spent uncovering and mitigating threats.

Now that we've defined XDR, let's take it a level deeper, delving into how it impacts security operations across these tiers and how it can improve this model. We'll break this down by key functions, including detection, alert triage, investigation and response, and threat hunting.

Detection

The ability to prevent data loss rests with the capability of detecting adversaries attempting malicious activity in your environment. XDR uses machine learning to absorb the unique characteristics of your organization, allowing it to differentiate between attacks and harmless activity beyond what is possible with manual analysis or static correlation rules. This machine learning fuels advanced analytics, profiling, and behavioral threat detection. Through this comprehensive detection, an XDR solution improves the ability to detect nefarious activity, including targeted attacks, malicious insiders, and more.



Targeted Attacks

Attackers attempt to blend in with legitimate users as they perform reconnaissance and exploit targeted networks. With XDR's ability to perform sophisticated analysis on security data encompassing the network, endpoint, and cloud, you can detect anomalous behavior as attackers compromise devices and move laterally on the network, looking for and exfiltrating customer data and intellectual property.

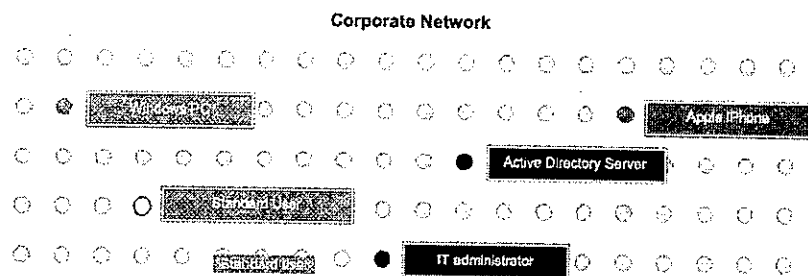


Figure 9: Behavioral analytics discover anomalies at the user, application, and device level

Malicious Insiders

Malicious insiders use their trusted credentials and access to steal significant amounts of corporate data without being detected. XDR addresses this challenge by looking for changes in user behavior and the resulting infrastructure activity, which provides the ability to pinpoint internal reconnaissance and lateral movement.

Inadvertent Risk

Well-meaning employees can inadvertently expose organizations to undue risk through their careless activities. An XDR solution allows organizations to follow security best practices by monitoring user activity and identifying risky behavior to detect when an employee is violating security policies—inadvertently or not.



Compromised Endpoints

Attackers often use malware to infiltrate targeted networks by compromising an endpoint and moving laterally through the network. XDR brings security data together across networks and endpoints to look for anomalous traffic generated by malware and other malicious activity. This security data also provides the means to investigate across infrastructure to determine the proliferation of the attack campaign.

Given the challenges presented by the security skills gap mentioned previously, XDR improves the ability of a less experienced analyst to detect and validate a potential attack by grouping alerts into incidents, and within those incidents, summarizing activities or actions into tags that add context. This flexibility ensures knowledge is captured and leveraged for the entire team.

For example, if an adversary adds a new value to the Autorun registry key, an XDR solution could automatically generate a tag creating an action for the analyst called "Executable File Set to Start after Boot;" the type of attack, labeled "Persistence;" and a detailed description like "Process added a new key to the Autorun folder in the Windows Registry; this will ensure an executable or script is run at startup. Review which file and why."

By integrating attack detection algorithms with data collected across network and endpoint as well as cloud, applying a structured detection framework, and continuously learning from both internal responses and external threat intelligence, an XDR solution identifies active attacks with unparalleled precision.

SUMMARY

The benefits of XDR for detection

XDR gives security teams an increased ability to:

- Detect malicious activity from both internal and external resources by finding patterns among activity happening on the network, at endpoints, and within the cloud.
- Utilize cutting-edge analytical techniques on significant amounts of security data to identify abnormal activity without increasing the level of false positives.
- Leverage internal response and external threat intelligence to learn from past attacks and make that experience accessible to less sophisticated analysts, improving the performance of the entire security team.



Alert Triage and Validation

As described previously, security analysts are challenged to triage more security issues both earlier in the process (i.e., reduce dwell time) and by less sophisticated staffers (address the skills gap). The more work that can be done by Tier 1 staff, the more alerts can be handled, and the more attacks detected. Better yet, the more automation that can be built into the triage process, the more effective Tier 1 analysts will be at reviewing and prioritizing security threats that need to be escalated.

Because XDR stitches together network, endpoint, and cloud data, it can automatically determine the root cause of attacks, making them much faster to validate and investigate. For example, not only does XDR determine which endpoint executable was responsible for a network attack, it can figure out which application launched the executable. XDR produces a timeline of the events leading to the attack and provides integrated threat intelligence. All of this allows analysts to understand the root cause of an attack, the exact nature of the threat, and what action to take.

Here's how alert triage and validation works with XDR:

(1) **Assessment:** The process starts with the XDR solution evaluating both external alerts (from SIEM and other controls) and internally generated alerts (based on rules and other indicators) to determine potentially suspicious behavior.

(2) **Prioritization:** The XDR tool then automatically groups those alerts into incidents, assigning a priority level to each incident in order to direct analysts to the incidents that pose the greatest threat. Analysts can click into each incident and see the full list of alerts, devices, associated threat intelligence, and other context to help understand the full extent of the attack.

Palo Alto Networks' product usage data shows an average of 50 alerts generated per each security incident. By identifying these related events and grouping them into incidents, XDR can reduce the number of alerts an analyst sees by 98%.



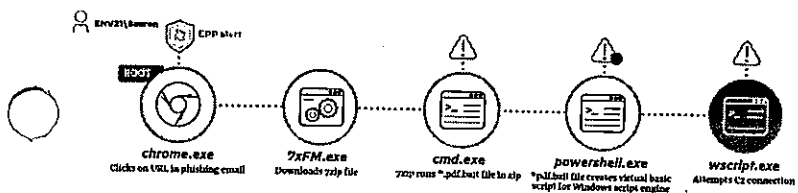


Figure 10: Visualized attack chain using XDR

(3) **Analysis:** Within each incident, analysts can click further into alerts to access a visual attack chain, leveraging the various sources of telemetry to collect anything and everything that's relevant to the alert to ensure faster and better analysis.

(4) **Enrichment:** The attack chain is then enriched with additional contextual information, including a play-by-play view of how the alert was generated; its root cause; other involved endpoint, network, and cloud devices; and the reputation of all forensic artifacts.

(5) **Validation:** The enrichment, analysis, assessment, and prioritization processes all happen automatically before the responder receives the alert for a more formal investigation. XDR uses the history of all previous alerts investigated to add context to the timeline of current alerts, improving prioritization and the speed at which the alert can be validated.

With thousands—sometimes millions—of alerts coming through each day, automating the triage process and providing analysts with enriched contextual information is the only way to manage the volume. With XDR, security teams can focus their time and energy where it will have the greatest impact: on remediating attacks with the potential to cause the most damage.

The benefits of XDR for alert triage and validation

Analysts have an increased ability to:

- Get to more events per day, not just the ones prioritized by security alerting tools or SIEMs.
- Dramatically reduce the chance of a missed alert.
- Analyze false positive alerts to improve detection as well as ensure downstream productivity and defenses are not adversely impacted.
- Apply new behavioral triggers to improve triage times and tighten defenses continually.



Automated and Simplified Investigations and Response

Once an alert has been triaged and prioritized, a more in-depth investigation is warranted. Analysts need context to better understand attacks and how to mitigate them. They need to understand the user, the endpoint information (the process, etc.) the threat intelligence details (e.g., whether a process is known malware), and network details. They should be able to understand the root cause and the timeline of the attack. If they need to manually piece together this information, it will take a while, increasing dwell times and risk. The automation of XDR accelerates the investigation process of any alert or hunting campaign, eliminating time-consuming manual tasks by providing a clear picture of the threat, performing root-cause analysis, verifying reputation, and resolving attack attribution.

XDR tools begin by aggregating all endpoint, network, and cloud telemetry within a security data repository, such as a data lake. To reduce investigation time, the XDR solution can correlate and group alerts from across detection tools into a small number of accurate, actionable incidents, including information about the user, application, and device. XDR can also eliminate lengthy forensics investigations by interrogating endpoints to determine which process or executable initiated an attack.

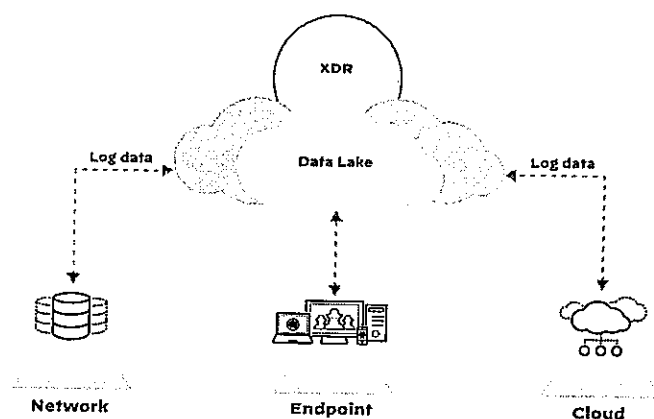


Figure 11: XDR tools stitch together data from different sensors in a cloud-based data lake



To dig deeper into the incident, an XDR solution then ascertains whether the endpoint process is malicious. It does this by integrating with threat intelligence sources and services to analyze the process. An XDR solution makes it easy for security analysts to verify attacks by presenting all the information they need in a single interface.

XDR tools can also adapt defenses, applying knowledge from previous incidents and hunting campaigns to automatically prevent the recurrence of any threat found previously. This "assisted learning" allows early detection of attacks based on what has already been seen.

Incident responders can then choose from dozens of remote response and remediation techniques to surgically clean infected systems without business disruption. The security team will become highly efficient, require less training, reduce the burden on more experienced incident responders, and minimize incident resolution times.

SII

The benefits of XDR for investigations

Incident responders have an increased ability to:

- Find stealthy threats faster by leveraging threat intelligence and behavioral analytics.
- Simplify and speed up investigation and response by providing deep and extensive searching of telemetry gathered from networks, endpoints, and the cloud.

 21

Threat Hunting

XDR solutions provide a significant boost to threat hunting capabilities through both automated and ad hoc identification of malicious activity across the infrastructure. Threat hunters can perform advanced queries, gaining instant results with superior precision. Examples of how XDR provides the necessary capabilities to support the different methods of threat hunting follow.

Intel-Based Threat Hunting

This is the most common type of threat hunting exercise, where the hunter has been given a clue about a potential threat before looking for it. Whether a lead from threat intelligence, newfound indicator of compromise (IOC), tip from someone within the organization, or mere suspicion, the complexity of tip-based threat hunting will depend on the level of detail the tip provides. Drawing from an integrated data source that is linked to multiple threat intelligence providers, an XDR solution can manually import artifacts or IOCs from different standards to provide fast and robust search results.

Leadless Threat Hunting

A close second in terms of common approaches to threat hunting, leadless is where the hunter uses their own or sought-after knowledge of how a computer, application, user, data, or network is meant to be used and aims to identify anomalous or abnormal use. This type is typically referred to as advanced threat hunting as it is commonly left to the most experienced of team members who use techniques such as data carving and analytics to achieve results. An XDR solution simplifies this process by building these advanced techniques into its UI, allowing hunters of any experience level to leverage these techniques without scripts, additional tools, or the need to learn a new query language.



Outcome-Based Threat Hunting

In this approach, the hunter looks into past quarantined alerts, completed investigations, or any other resolved threats and uses these to identify variants of the threat, potential new threats, or open attack vectors. A quality XDR solution can incorporate outcome-based threat hunting directly into the workflow of security alerts and incident handling automatically and continuously. Lessons learned from every investigation are applied to ensure you don't get hit by repeat attacks.

Compliance-Based Threat Hunting

This hunting approach is focused on ensuring compliance with internal, industry, and government policies by performing routine searches that indicate non-compliance, such as sensitive data stored in unauthorized systems or escalation of privileges by admin users. An XDR solution can be configured to alert security analysts of this type of activity and provide a means to investigate the situation quickly.

Machine Learning-Based Hunting

Machine learning systems baseline the typical behaviors of an organization to understand what is normal and what is not. Using large-scale analytics, XDR solutions use machine learning to monitor behaviors and identify anomalies that deviate from these baselines. These behavioral indicators of compromise (BIOCs) pick up on many stealthy threats that an analyst may not be able to identify manually and are continually optimized over time to improve the machine learning model. This form of threat hunting represents the ultimate time savings for analysts and is critical for optimizing security outcomes.

SUMMARY

The benefits of XDR for threat hunting

Threat hunters have an increased ability to:

- Take advantage of network, endpoint, and cloud data for searches and analysis.
- Leverage automation to hunt across all network, endpoint, and cloud activity.
- Use both highly configurable search and wizards to find both internal and external threats identified by traditional IOCs and BIOCs stored within your threat library.
- Remediate attacks via integration with security controls.



Conclusion

Enterprises are in need of foundational changes to their detection and response technologies and processes. Legacy technologies are too rigid and limited, failing to provide either the flexibility or scale to keep pace with today's adversaries. Companies need to work more effectively and efficiently to address the scarcity of qualified security analysts. XDR offers a new way forward, with broader visibility across endpoints, networks, and the cloud, along with more effective machine learning analytics and integrated remediation to fundamentally change threat hunting, detection, investigation, and response.



XDR RFP Checklist

XDR must deliver a wide range of common EDR capabilities to provide efficient and effective security against modern attacks, while also integrating with other key prevention, detection, and response tools across the infrastructure. The following RFP checklist includes requirements within nine key categories to help you evaluate the quality of the platforms you're considering.

Use this checklist as a starting point, and tailor it to your company's needs to ensure you're able to identify vendors that can best support your organization.

Download the spreadsheet version to start your RFP today at
go.paloaltonetworks.com/xdrrfp.

1. AV Requirements

- ☐ ML-based threat prevention
- ☐ Behavior-based threat prevention
- ☐ Exploit technique prevention
- ☐ Signature-based threat prevention
- ☐ Realtime verdict updates provided by the vendor
- ☐ Integration with cloud-based malware analysis service
- ☐ Transparent threat detection engine updates
- ☐ Security profiles and exceptions



- ☐ Ad-hoc and scheduled scanning of endpoints
- ☐ Protection against malware, ransomware, and fileless attacks
- ☐ Single, lightweight agent for endpoint protection and for detection and response

2. Data Visibility and Logging Requirements

User information

- ☐ Domain and distinguished name
- ☐ Email address
- ☐ Organizational unit
- ☐ Phone number

Device information

- ☐ MAC address
- ☐ Hostname of device
- ☐ Domain name
- ☐ Distinguished name of host
- ☐ Organizational unit
- ☐ Operating system
- ☐ Operating system version
- ☐ Name of firewall, if applicable
- ☐ Other names used by firewall configuration, if applicable



Process information

- ☐ Process timestamp
- ☐ Path and name
- ☐ Process ID
- ☐ Loaded modules
- ☐ Hash values such as MD5 and SHA256
- ☐ Command line arguments
- ☐ Signature state

File information for file create, write, access, open, rename, or delete

- ☐ Timestamp
- ☐ Path and name
- ☐ Previous file name and path for file rename events
- ☐ Hash values, such as MD5 and SHA-256
- ☐ Username

Network activity including outgoing connections, failed connections, and incoming connections

- ☐ Timestamp
- ☐ Source IP address, destination IP address, source port, and destination port
- ☐ Bytes sent and received
- ☐ Protocol



- ☐ Remote country
- ☐ Proxy information
- ☐ User
- ☐ Integration with next-generation firewalls for complete Layer 7 visibility, including application name
- ☐ Connection duration
- ☐ Transaction-level data and enhanced information about key protocols, such as DNS, HTTP, DHCP, RPC, ARP, and ICMP

Registry activities such as create key, modify key, delete key, and rename key

- ☐ Timestamp
- ☐ Key name
- ☐ Value and type
- ☐ Previous key name for rename events

System events

- ☐ User status change event, such as login and logout
- ☐ Host status change event
- ☐ Agent status change event



Security alerts

- ☐ URL filtering logs
- ☐ Firewall threat logs
- ☐ Endpoint threat logs

Contextual user data

- ☐ Logged-in user
- ☐ Typical user of a machine
- ☐ User creating the process that initiated communication
- ☐ User group and organizational unit from directory services

3. Data Retention and Coverage Requirements

- ☐ Visibility into lateral movement across the network and other parts of the infrastructure
- ☐ Detection and response for threats involving both managed and unmanaged endpoints
- ☐ Detection and response for threats involving remote users
- ☐ Detection and response for threats involving cloud servers
- ☐ Minimum of 30 days of data retention
- ☐ One year of retention for audit logs of administrative and investigative activity



4. Investigation Requirements

- ☐ Automated root cause analysis of any alert, including network alerts, if endpoint data is available
- ☐ Ability to view chains of execution leading up to an alert
- ☐ Timeline analysis view to see all actions and alerts on a timeline
- ☐ Query capability for indicators of compromise (IOCs) and for endpoint behaviors
- ☐ Query capability for online and offline hosts
- ☐ Ability for an analyst to easily pivot between views
- ☐ Granular filtering and sorting of query results
- ☐ Identification if an event was blocked by an endpoint agent, a firewall or another prevention technology
- ☐ Automated stitching of security alerts, such as firewall alerts, to endpoint data
- ☐ Noise cancellation, removal of non-significant binaries and DLLs from chain
- ☐ SOC analyst context of TTPs to utilize knowledge gained in future investigations

5. Incident Management Requirements

- ☐ Automated reduction of related alerts from various sources into a single incident
- ☐ Ability to extract notable artifacts from the alerts and match them with threat intelligence services
- ☐ Ability to extract the entities involved in the incidents for ease of view
- ☐ Ability to assign incidents to team members



- ☐ Ability to get notifications on incident assignment
- ☐ Ability to add comments
- ☐ Ability to manage the incident lifecycle (new, investigation, closed, handled, etc.)
- ☐ Ability to merge and split incidents
- ☐ Ability to send incident data to third-party case management

6. Threat Intelligence Requirements

- ☐ Ability to alert on known malicious objects on endpoints with IOC rules
- ☐ Automatically scan historic data for IOCs as they are added to the system and raise alerts
- ☐ Integrate with one or more threat intelligence services for threat intelligence tags and additional context on key artifacts
- ☐ Ability to remotely run arbitrary scripts

7. Response Requirements

- ☐ Remote terminal capability
- ☐ UI-based remote terminal, not only CLI
- ☐ Ability to run CMD, PowerShell and Python commands
- ☐ Ability to run custom scripts
- ☐ Remote isolation of the endpoint
- ☐ Remote file deletion
- ☐ Automatic and manual collection or retrieval of quarantined files and objects



- ☐ Remotely suspend or terminate processes
- ☐ Ability to view running processes
- ☐ File manager with ability to view, download, rename, or move files
- ☐ UI task manager

8. Detection, Integration, and Automation Requirements

- ☐ Behavioral analytics to profile user and endpoint behavior and detect anomalies indicative of attack
- ☐ Supervised and unsupervised machine learning capabilities
- ☐ Predefined and customizable behavior-based detection rules
- ☐ Custom rules for retroactive threat detection
- ☐ Integration with security information and event management (SIEM) solutions
- ☐ Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services
- ☐ Integration with a security orchestration, automation, and response (SOAR) solution for incident analysis
- ☐ Ability to detect reconnaissance and lateral movement attempts

9. System Support and Resource Requirements

- ☐ Modular and scalable product
- ☐ Cloud-based deployment
- ☐ Full auditing for all actions in the system



- ☐ Minimum number of agents required
- ☐ Average CPU usage of less than 3% with all services enabled
- ☐ Agent installation size of less than 50 MB
- ☐ Ability to push agent updates from the management console
- ☐ Ability to run on and protect all macOS and Mac OS X versions released in the last five years
- ☐ Support for Android
- ☐ Support for all major Linux distributions
- ☐ Support for all recent Windows versions, including Windows Server
- ☐ Multi-factor authentication for management
- ☐ Support for non-persistent VDI
- ☐ Support for temporary sessions for machines that repeatedly revert to a snapshot (or image) on which the agent is not installed

10. Managed Service Requirements (Optional)

If your security operations team uses a hybrid or fully outsourced model, consider these additional checklist items to evaluate managed security services:

- ☐ 24/7 year-round monitoring and availability
- ☐ Ability to ingest, prioritize, and triage alerts from all vendors
- ☐ Identification and validation of critical threats in one hour or less



- ☐ Visibility into data sources that include endpoint device, network packet/session, and cloud packet/session/config
- ☐ Monitoring and detection of behavioral anomalies on unmanaged devices
- ☐ Monitoring and detection of behavioral anomalies for users
- ☐ Continuous threat hunting across managed and unmanaged devices
- ☐ Tuning of tools to individual customer environments, including custom rules and exceptions
- ☐ Access to specialists via email, phone, or messaging system (e.g., Slack)
- ☐ Visibility, communication, and response portal or mobile application
- ☐ Customer access to tools

3000 Tannery Way

Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. cortex-xdr-ebook-013020





Sophisticated cyberattackers can sneak past even the best threat prevention systems to compromise critical data—often in public, damaging ways. Most enterprises have tools to deal with attacks that skirt their initial defenses, but each of these only sees a tiny slice of the IT infrastructure. The tools aren't intelligent or integrated enough to correlate different events over the course of an attack, so they send out alerts for anything remotely suspicious, often hundreds or thousands per day. Security analysts waste time sifting through these alerts for the ones that matter. When real threats slip through the cracks, they frequently go uncovered for months.

That system doesn't work.

Introducing a better category of detection and response tools: XDR. XDR stitches together data from the endpoint, network, and cloud in a robust data lake. Applying advanced machine learning and analytics, it identifies threats and benign events with superior accuracy and gives analysts contextualized information, simplifying and accelerating investigations. Read this e-book to learn more, including:

- Challenges with the current state of detection and response
- Tactical use cases for improving security operations with XDR
- The definition and key requirements of XDR



July 13, 2020

DEPARTMENT OF BUDGET AND MANAGEMENT (DBM)
General Solano Street, San Miguel, Manila

Gentlemen:

We hereby issue this Irrevocable Domestic Standby Letter of Credit No. **ISB-130020000952** in your favor (hereinafter referred to as "**BENEFICIARY**") for the account of **ACCENT MICRO TECHNOLOGIES, INC.** (hereinafter referred to as "**APPLICANT**") with office address at 8th Floor East Tower, Philippine Stock Exchange Center, Exchange Road, Ortigas Center, Pasig City, available by your drafts at sight in duplicate up to the aggregate amount of **Philippine Pesos: Two Hundred Forty Nine Thousand Eight hundred Only (Php249,800.00)**.

This Standby LC guarantees the performance obligation of the **APPLICANT** for Subscription of Advanced Endpoint Security Solution (Project ID No. DBM-2020-31) covered under Notice of Award.

Drawings under this Credit shall be made against presentation of the following:

1. The original of this Credit and amendment/s, if any.
2. Your sight drafts in duplicate drawn on Security Bank Corporation and marked "Drawn under Security Bank Corporation's Irrevocable Domestic Standby Letter of Credit No. **ISB-130020000952** dated July 13, 2020".
3. Certification duly signed by your authorized signatory(ies) stating that the Applicant has been declared in default of its obligation.

This Credit shall expire on **July 8, 2021** at the counters of Security Bank Corporation, International Banking Services Division 3rd Floor, 6776 Ayala Avenue, Makati City.

We hereby engage with you that drafts drawn under and in compliance with the terms and conditions of this Credit, together with the specified documents stated herein, shall be duly honored upon presentation to us on or before **July 8, 2021**. This Credit shall cease to have any force or effect upon its expiration, whether or not the original credit is returned by the Beneficiary (any policy, rule, regulation of the Beneficiary to the contrary notwithstanding).

Furthermore, it is expressly agreed and understood that the Applicant shall, upon demand, have the sole and absolute liability to reimburse us for any drawings made under this Standby Letter of Credit.

Unless otherwise stated herein, this Credit is subject to the Uniform Customs and Practice for Documentary Credits (2007 revision) International Chamber of Commerce Publication No. 600.

Very Truly Yours,

SECURITY BANK CORPORATION
International Banking Services Division
By:



GHIA E. CLEOFE
Asst. Manager



NELLY L. BOGNADON
Senior Manager

For inquiries and comments, please call our 24-Hour Customer Service hotline at (632) 888-791-88 or email us at customercare@securitybank.com.ph. Security Bank Corporation is supervised by Bangko Sentral ng Pilipinas with telephone number (632) 8708-7087 and email address consumeraffairs@bsp.gov.ph

Section IV. General Conditions of Contract

TABLE OF CONTENTS

1.	DEFINITIONS.....	47
2.	CORRUPT, FRAUDULENT, COLLUSIVE, AND COERCIVE PRACTICES	48
3.	INSPECTION AND AUDIT BY THE FUNDING SOURCE.....	49
4.	GOVERNING LAW AND LANGUAGE.....	49
5.	NOTICES	49
6.	SCOPE OF CONTRACT	50
7.	SUBCONTRACTING	50
8.	PROCURING ENTITY’S RESPONSIBILITIES	50
9.	PRICES.....	50
10.	PAYMENT.....	51
11.	ADVANCE PAYMENT AND TERMS OF PAYMENT.....	51
12.	TAXES AND DUTIES.....	52
13.	PERFORMANCE SECURITY	52
14.	USE OF CONTRACT DOCUMENTS AND INFORMATION.....	53
15.	STANDARDS	53
16.	INSPECTION AND TESTS.....	53
17.	WARRANTY	54
18.	DELAYS IN THE SUPPLIER’S PERFORMANCE	55
19.	LIQUIDATED DAMAGES	55
20.	SETTLEMENT OF DISPUTES.....	55
21.	LIABILITY OF THE SUPPLIER	56
22.	FORCE MAJEURE.....	56
23.	TERMINATION FOR DEFAULT	57
24.	TERMINATION FOR INSOLVENCY.....	57
25.	TERMINATION FOR CONVENIENCE.....	57
26.	TERMINATION FOR UNLAWFUL ACTS	58
27.	PROCEDURES FOR TERMINATION OF CONTRACTS	58
28.	ASSIGNMENT OF RIGHTS	60

29. CONTRACT AMENDMENT60

30. APPLICATION.....60

1. Definitions

1.1. In this Contract, the following terms shall be interpreted as indicated:

- (a) “The Contract” means the agreement entered into between the Procuring Entity and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
- (b) “The Contract Price” means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.
- (c) “The Goods” means all of the supplies, equipment, machinery, spare parts, other materials and/or general support services which the Supplier is required to provide to the Procuring Entity under the Contract.
- (d) “The Services” means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Supplier covered under the Contract.
- (e) “GCC” means the General Conditions of Contract contained in this Section.
- (f) “SCC” means the Special Conditions of Contract.
- (g) “The Procuring Entity” means the organization purchasing the Goods, as named in the SCC.
- (h) “The Procuring Entity’s country” is the Philippines.
- (i) “The Supplier” means the individual contractor, manufacturer distributor, or firm supplying/manufacturing the Goods and Services under this Contract and named in the SCC.
- (j) The “Funding Source” means the organization named in the SCC.
- (k) “The Project Site,” where applicable, means the place or places named in the SCC.
- (l) “Day” means calendar day.
- (m) The “Effective Date” of the contract will be the date of signing the contract, however the Supplier shall commence performance of its obligations only upon receipt of the Notice to Proceed and copy of the approved contract.

- (n) “Verified Report” refers to the report submitted by the Implementing Unit to the HoPE setting forth its findings as to the existence of grounds or causes for termination and explicitly stating its recommendation for the issuance of a Notice to Terminate.

2. Corrupt, Fraudulent, Collusive, and Coercive Practices

2.1. Unless otherwise provided in the **SCC**, the Procuring Entity as well as the bidders, contractors, or suppliers shall observe the highest standard of ethics during the procurement and execution of this Contract. In pursuance of this policy, the Procuring Entity:

- (a) defines, for the purposes of this provision, the terms set forth below as follows:
 - (i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the Government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in Republic Act 3019.
 - (ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.
 - (iii) “collusive practices” means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.
 - (iv) “coercive practices” means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;
 - (v) “obstructive practice” is
 - (aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an

administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

2.2. Further the Funding Source, Borrower or Procuring Entity, as appropriate, will seek to impose the maximum civil, administrative and/or criminal penalties available under the applicable law on individuals and organizations deemed to be involved with any of the practices mentioned in GCC Clause 2.1(a).

3. Inspection and Audit by the Funding Source

The Supplier shall permit the Funding Source to inspect the Supplier's accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Funding Source, if so required by the Funding Source.

4. Governing Law and Language

4.1. This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

4.2. This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

5. Notices

5.1. Any notice, request, or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request, or consent shall be deemed to have been given or made when received by the concerned party, either in person or through an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the SCC, which shall be effective when delivered and duly received or on the notice's effective date, whichever is later.

- 5.2. A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to the provisions listed in the **SCC** for **GCC** Clause 5.1.

6. Scope of Contract

- 6.1. The Goods and Related Services to be provided shall be as specified in Section VI. Schedule of Requirements.
- 6.2. This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. Any additional requirements for the completion of this Contract shall be provided in the **SCC**.

7. Subcontracting

- 7.1. Subcontracting of any portion of the Goods, if allowed in the **BDS**, does not relieve the Supplier of any liability or obligation under this Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants or workmen.
- 7.2. If subcontracting is allowed, the Supplier may identify its subcontractor during contract implementation. Subcontractors disclosed and identified during the bidding may be changed during the implementation of this Contract. In either case, subcontractors must submit the documentary requirements under **ITB** Clause 12 and comply with the eligibility criteria specified in the **BDS**. In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

8. Procuring Entity's Responsibilities

- 8.1. Whenever the performance of the obligations in this Contract requires that the Supplier obtain permits, approvals, import, and other licenses from local public authorities, the Procuring Entity shall, if so needed by the Supplier, make its best effort to assist the Supplier in complying with such requirements in a timely and expeditious manner.
- 8.2. The Procuring Entity shall pay all costs involved in the performance of its responsibilities in accordance with **GCC** Clause 6.

9. Prices

- 9.1. For the given scope of work in this Contract as awarded, all bid prices are considered fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances and upon prior approval of the GPPB in accordance with Section 61 of R.A. 9184 and its IRR or except as provided in this Clause.

- 9.2. Prices charged by the Supplier for Goods delivered and/or services performed under this Contract shall not vary from the prices quoted by the Supplier in its bid, with the exception of any change in price resulting from a Change Order issued in accordance with **GCC** Clause 29.

10. Payment

- 10.1. Payments shall be made only upon a certification by the HoPE to the effect that the Goods have been rendered or delivered in accordance with the terms of this Contract and have been duly inspected and accepted. Except with the prior approval of the President no payment shall be made for services not yet rendered or for supplies and materials not yet delivered under this Contract. Ten percent (10%) of the amount of each payment shall be retained by the Procuring Entity to cover the Supplier's warranty obligations under this Contract as described in **GCC** Clause 17.
- 10.2. The Supplier's request(s) for payment shall be made to the Procuring Entity in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and/or Services performed, and by documents submitted pursuant to the **SCC** provision for **GCC** Clause 6.2, and upon fulfillment of other obligations stipulated in this Contract.
- 10.3. Pursuant to **GCC** Clause 10.2, payments shall be made promptly by the Procuring Entity, but in no case later than sixty (60) days after submission of an invoice or claim by the Supplier. Payments shall be in accordance with the schedule stated in the **SCC**.
- 10.4. Unless otherwise provided in the **SCC**, the currency in which payment is made to the Supplier under this Contract shall be in Philippine Pesos.
- 10.5. Unless otherwise provided in the **SCC**, payments using Letter of Credit (LC), in accordance with the Guidelines issued by the GPPB, is allowed. For this purpose, the amount of provisional sum is indicated in the **SCC**. All charges for the opening of the LC and/or incidental expenses thereto shall be for the account of the Supplier.

11. Advance Payment and Terms of Payment

- 11.1. Advance payment shall be made only after prior approval of the President, and shall not exceed fifteen percent (15%) of the Contract amount, unless otherwise directed by the President or in cases allowed under Annex "D" of RA 9184.
- 11.2. All progress payments shall first be charged against the advance payment until the latter has been fully exhausted.
- 11.3. For Goods supplied from abroad, unless otherwise indicated in the **SCC**, the terms of payment shall be as follows:
- (a) On Contract Signature: Fifteen Percent (15%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent

amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms.

- (b) On Delivery: Sixty-five percent (65%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents.
- (c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by the Procuring Entity's authorized representative. In the event that no inspection or acceptance certificate is issued by the Procuring Entity's authorized representative within forty five (45) days of the date shown on the delivery receipt, the Supplier shall have the right to claim payment of the remaining twenty percent (20%) subject to the Procuring Entity's own verification of the reason(s) for the failure to issue documents (vii) and (viii) as described in the SCC provision on Delivery and Documents.

12. Taxes and Duties

The Supplier, whether local or foreign, shall be entirely responsible for all the necessary taxes, stamp duties, license fees, and other such levies imposed for the completion of this Contract.

13. Performance Security

- 13.1. Within ten (10) calendar days from receipt of the Notice of Award from the Procuring Entity but in no case later than the signing of the contract by both parties, the successful Bidder shall furnish the performance security in any the forms prescribed in the **ITB** Clause 33.2.
- 13.2. The performance security posted in favor of the Procuring Entity shall be forfeited in the event it is established that the winning bidder is in default in any of its obligations under the contract.
- 13.3. The performance security shall remain valid until issuance by the Procuring Entity of the Certificate of Final Acceptance.
- 13.4. The performance security may be released by the Procuring Entity and returned to the Supplier after the issuance of the Certificate of Final Acceptance subject to the following conditions:
 - (a) There are no pending claims against the Supplier or the surety company filed by the Procuring Entity;
 - (b) The Supplier has no pending claims for labor and materials filed against it; and
 - (c) Other terms specified in the SCC.

- 13.5. In case of a reduction of the contract value, the Procuring Entity shall allow a proportional reduction in the original performance security, provided that any such reduction is more than ten percent (10%) and that the aggregate of such reductions is not more than fifty percent (50%) of the original performance security.

14. Use of Contract Documents and Information

- 14.1. The Supplier shall not, except for purposes of performing the obligations in this Contract, without the Procuring Entity's prior written consent, disclose this Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring Entity. Any such disclosure shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
- 14.2. Any document, other than this Contract itself, enumerated in GCC Clause 14.1 shall remain the property of the Procuring Entity and shall be returned (all copies) to the Procuring Entity on completion of the Supplier's performance under this Contract if so required by the Procuring Entity.

15. Standards

The Goods provided under this Contract shall conform to the standards mentioned in Section VII. Technical Specifications; and, when no applicable standard is mentioned, to the authoritative standards appropriate to the Goods' country of origin. Such standards shall be the latest issued by the institution concerned.

16. Inspection and Tests

- 16.1. The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Contract specifications at no extra cost to the Procuring Entity. The SCC Section VII. Technical Specifications shall specify what inspections and/or tests the Procuring Entity requires and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.
- 16.2. If applicable, the inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the goods' final destination. If conducted on the premises of the Supplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Entity. The Supplier shall provide the Procuring Entity with results of such inspections and tests.
- 16.3. The Procuring Entity or its designated representative shall be entitled to attend the tests and/or inspections referred to in this Clause provided that the Procuring Entity shall bear all of its own costs and expenses incurred in connection with such attendance including, but not limited to, all traveling and board and lodging expenses.

- 16.4. The Procuring Entity may reject any Goods or any part thereof that fail to pass any test and/or inspection or do not conform to the specifications. The Supplier shall either rectify or replace such rejected Goods or parts thereof or make alterations necessary to meet the specifications at no cost to the Procuring Entity, and shall repeat the test and/or inspection, at no cost to the Procuring Entity, upon giving a notice pursuant to **GCC** Clause 5.
- 16.5. The Supplier agrees that neither the execution of a test and/or inspection of the Goods or any part thereof, nor the attendance by the Procuring Entity or its representative, shall release the Supplier from any warranties or other obligations under this Contract.

17. Warranty

- 17.1. The Supplier warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the Procuring Entity provides otherwise.
- 17.2. The Supplier further warrants that all Goods supplied under this Contract shall have no defect, arising from design, materials, or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.
- 17.3. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier for a minimum period specified in the **SCC**. The obligation for the warranty shall be covered by, at the Supplier's option, either retention money in an amount equivalent to at least one percent (1%) of every progress payment, or a special bank guarantee equivalent to at least one percent (1%) of the total Contract Price or other such amount if so specified in the **SCC**. The said amounts shall only be released after the lapse of the warranty period specified in the **SCC**; provided, however, that the Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.
- 17.4. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, within the period specified in the **SCC** and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the Procuring Entity.
- 17.5. If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in **GCC** Clause 17.4, the Procuring Entity may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Entity may have against the Supplier under the Contract and under the applicable law.

18. Delays in the Supplier's Performance

- 18.1. Delivery of the Goods and/or performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Procuring Entity in Section VI. Schedule of Requirements.
- 18.2. If at any time during the performance of this Contract, the Supplier or its Subcontractor(s) should encounter conditions impeding timely delivery of the Goods and/or performance of Services, the Supplier shall promptly notify the Procuring Entity in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, and upon causes provided for under GCC Clause 22, the Procuring Entity shall evaluate the situation and may extend the Supplier's time for performance, in which case the extension shall be ratified by the parties by amendment of Contract.
- 18.3. Except as provided under GCC Clause 22, a delay by the Supplier in the performance of its obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to GCC Clause 19, unless an extension of time is agreed upon pursuant to GCC Clause 29 without the application of liquidated damages.

19. Liquidated Damages

Subject to GCC Clauses 18 and 22, if the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. The maximum deduction shall be ten percent (10%) of the amount of contract. Once the maximum is reached, the Procuring Entity may rescind or terminate the Contract pursuant to GCC Clause 23, without prejudice to other courses of action and remedies open to it.

20. Settlement of Disputes

- 20.1. If any dispute or difference of any kind whatsoever shall arise between the Procuring Entity and the Supplier in connection with or arising out of this Contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.
- 20.2. If after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Procuring Entity or the Supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.
- 20.3. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause shall be

settled by arbitration. Arbitration may be commenced prior to or after delivery of the Goods under this Contract.

- 20.4. In the case of a dispute between the Procuring Entity and the Supplier, the dispute shall be resolved in accordance with Republic Act 9285 (“R.A. 9285”), otherwise known as the “Alternative Dispute Resolution Act of 2004.”
- 20.5. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the Supplier any monies due the Supplier.

21. Liability of the Supplier

- 21.1. The Supplier’s liability under this Contract shall be as provided by the laws of the Republic of the Philippines, subject to additional provisions, if any, set forth in the SCC.
- 21.2. Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent rights, if applicable, the aggregate liability of the Supplier to the Procuring Entity shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

22. Force Majeure

- 22.1. The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that the Supplier’s delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure*.
- 22.2. For purposes of this Contract the terms “*force majeure*” and “fortuitous event” may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the Supplier could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the Supplier. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.
- 22.3. If a *force majeure* situation arises, the Supplier shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the *force majeure*.

23. Termination for Default

23.1. The Procuring Entity shall terminate this Contract for default when any of the following conditions attends its implementation:

- (a) Outside of *force majeure*, the Supplier fails to deliver or perform any or all of the Goods within the period(s) specified in the contract, or within any extension thereof granted by the Procuring Entity pursuant to a request made by the Supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contract price;
- (b) As a result of *force majeure*, the Supplier is unable to deliver or perform any or all of the Goods, amounting to at least ten percent (10%) of the contract price, for a period of not less than sixty (60) calendar days after receipt of the notice from the Procuring Entity stating that the circumstance of force majeure is deemed to have ceased; or
- (c) The Supplier fails to perform any other obligation under the Contract.

23.2. In the event the Procuring Entity terminates this Contract in whole or in part, for any of the reasons provided under GCC Clauses 23 to 26, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Entity for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of this Contract to the extent not terminated.

23.3. In case the delay in the delivery of the Goods and/or performance of the Services exceeds a time duration equivalent to ten percent (10%) of the specified contract time plus any time extension duly granted to the Supplier, the Procuring Entity may terminate this Contract, forfeit the Supplier's performance security and award the same to a qualified Supplier.

24. Termination for Insolvency

The Procuring Entity shall terminate this Contract if the Supplier is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity and/or the Supplier.

25. Termination for Convenience

25.1. The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience. The HoPE may terminate a contract for the convenience of the Government if he has determined the existence of conditions that make Project Implementation economically, financially or technically impractical and/or unnecessary, such as, but not limited to, fortuitous event(s) or changes in law and national government policies.

- 25.2. The Goods that have been delivered and/or performed or are ready for delivery or performance within thirty (30) calendar days after the Supplier's receipt of Notice to Terminate shall be accepted by the Procuring Entity at the contract terms and prices. For Goods not yet performed and/or ready for delivery, the Procuring Entity may elect:
- (a) to have any portion delivered and/or performed and paid at the contract terms and prices; and/or
 - (b) to cancel the remainder and pay to the Supplier an agreed amount for partially completed and/or performed goods and for materials and parts previously procured by the Supplier.
- 25.3. If the Supplier suffers loss in its initial performance of the terminated contract, such as purchase of raw materials for goods specially manufactured for the Procuring Entity which cannot be sold in open market, it shall be allowed to recover partially from this Contract, on a *quantum meruit* basis. Before recovery may be made, the fact of loss must be established under oath by the Supplier to the satisfaction of the Procuring Entity before recovery may be made.

26. Termination for Unlawful Acts

- 26.1. The Procuring Entity may terminate this Contract in case it is determined *prima facie* that the Supplier has engaged, before or during the implementation of this Contract, in unlawful deeds and behaviors relative to contract acquisition and implementation. Unlawful acts include, but are not limited to, the following:
- (a) Corrupt, fraudulent, and coercive practices as defined in **ITB** Clause 3.1(a);
 - (b) Drawing up or using forged documents;
 - (c) Using adulterated materials, means or methods, or engaging in production contrary to rules of science or the trade; and
 - (d) Any other act analogous to the foregoing.

27. Procedures for Termination of Contracts

- 27.1. The following provisions shall govern the procedures for termination of this Contract:
- (a) Upon receipt of a written report of acts or causes which may constitute ground(s) for termination as aforementioned, or upon its own initiative, the Implementing Unit shall, within a period of seven (7) calendar days, verify the existence of such ground(s) and cause the execution of a Verified Report, with all relevant evidence attached;

- (b) Upon recommendation by the Implementing Unit, the HoPE shall terminate this Contract only by a written notice to the Supplier conveying the termination of this Contract. The notice shall state:
 - (i) that this Contract is being terminated for any of the ground(s) afore-mentioned, and a statement of the acts that constitute the ground(s) constituting the same;
 - (ii) the extent of termination, whether in whole or in part;
 - (iii) an instruction to the Supplier to show cause as to why this Contract should not be terminated; and
 - (iv) special instructions of the Procuring Entity, if any.
- (c) The Notice to Terminate shall be accompanied by a copy of the Verified Report;
- (d) Within a period of seven (7) calendar days from receipt of the Notice of Termination, the Supplier shall submit to the HoPE a verified position paper stating why this Contract should not be terminated. If the Supplier fails to show cause after the lapse of the seven (7) day period, either by inaction or by default, the HoPE shall issue an order terminating this Contract;
- (e) The Procuring Entity may, at any time before receipt of the Supplier's verified position paper described in item (d) above withdraw the Notice to Terminate if it is determined that certain items or works subject of the notice had been completed, delivered, or performed before the Supplier's receipt of the notice;
- (f) Within a non-extendible period of ten (10) calendar days from receipt of the verified position paper, the HoPE shall decide whether or not to terminate this Contract. It shall serve a written notice to the Supplier of its decision and, unless otherwise provided, this Contract is deemed terminated from receipt of the Supplier of the notice of decision. The termination shall only be based on the ground(s) stated in the Notice to Terminate;
- (g) The HoPE may create a Contract Termination Review Committee (CTRC) to assist him in the discharge of this function. All decisions recommended by the CTRC shall be subject to the approval of the HoPE; and
- (h) The Supplier must serve a written notice to the Procuring Entity of its intention to terminate the contract at least thirty (30) calendar days before its intended termination. The Contract is deemed terminated if it is not resumed in thirty (30) calendar days after the receipt of such notice by the Procuring Entity.

28. Assignment of Rights

The Supplier shall not assign his rights or obligations under this Contract, in whole or in part, except with the Procuring Entity's prior written consent.

29. Contract Amendment

Subject to applicable laws, no variation in or modification of the terms of this Contract shall be made except by written amendment signed by the parties.

30. Application

These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of this Contract.

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1.1(g)	The Procuring Entity is the Department of Budget and Management (DBM) .
1.1(i)	The Supplier is
1.1(j)	<p>The Funding Source is:</p> <p>The Government of the Philippines (GOP) through the authorized appropriations under the FY 2020 General Appropriations Act in the amount of Five Million Thirty Thousand Pesos (P5,030,000.00).</p>
1.1(k)	<p>The Project Site is:</p> <p>Department of Budget and Management General Solano St. San Miguel, Manila.</p>
2.1	No further instructions.
5.1	<p>The Procuring Entity's address for Notices is:</p> <p style="text-align: center;">Department of Budget and Management Information and Communications Technology Systems Service (ICTSS) 3rd Floor, DBM Building II General Solano St., San Miguel, Manila Tel No. (02)657-3300 loc. 2356</p> <p style="text-align: center;">Contact Person: Andrea Celene M. Magtalas Director IV, ICTSS</p> <p>The Supplier's address for Notices is:</p>
6.2	The delivery schedule as indicated in Section VI. Schedule of Requirements may be modified at the option of the Procuring Entity, with prior due notice, written or verbal, to the Supplier.
10.3	Terms of Payment shall be in accordance with the provision under item IX of the Annex "A."
10.4	Not applicable.
10.5	Payment using LC is not allowed.
11.3	Maintain the GCC Clause.
13.4(c)	No further instructions.
15	No further instructions.
16.1	The quantity of the Goods delivered to DBM shall be inspected by the Procuring Entity. However, inspection and approval as to the acceptability of the Goods vis-à-vis its compliance with the technical specifications and its order and condition, will be done with prior

	notice, written or verbal, to the authorized representative of the Supplier. The inspection will push through as scheduled even in the absence of the Supplier's representative, if the latter was duly notified. In which case, the result of the inspection conducted by the Procuring Entity shall be final and binding upon the Supplier.
17.3	In order to assure that manufacturing defects shall be corrected by the supplier, a warranty security shall be required from the contract awarded for a minimum period of one (1) year from the date of acceptance by the DBM-ICTSS.
17.4	As indicated under item V. Scope of Work and Services of Annex "A"
19.0	<p>The imposition of liquidated damages in all instances shall be in accordance with item VI. Service Level Agreement of Annex "A"</p> <p>The imposition of liquidated damages in all instances shall be automatic, except upon prior request for extension and approval thereof by the Procuring Entity before the scheduled delivery date.</p> <p>Any request for extension not acted upon before delivery date shall be considered denied.</p>
21.1	The Supplier shall be responsible and liable for the cost of repair due to damages caused by its own staff while implementing the project.