RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

DEVELOPMENT BANK OF THE PHILIPPINES

INCEPTION REPORT

PROJECT TITLE:

One (1) Lot Supply, Delivery, Installation, Configuration and Subscription of Managed Detection and Response Plus Remediation (MDR+R) Solution

Version Number:	1.0
Created by:	Mathew Dalisay
Date of version:	November 27, 2025

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Primary Author:

Mathew Dalisay
Project Manager
Radenta Technologies, Inc.

Prepared for:

Development Bank of the Philippines

Jose Marie Bonto
Chief Technology Officer, Concurrent Head
IT Security Department

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Table of Contents

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Approval Sheet

The undersigned authorized representative/s of the Development Bank of the Philippines (DBP) hereby attest that the Inception Report, a standard requirement for the project "**One (1) Lot Supply, Delivery, Installation, Configuration and Subscription of Managed Detection and Response Plus Remediation (MDR+R) Solution**" has been completed, reviewed and approved.

Prepared by:

Mathew Dalisay
Project Manager
Strategic Project Leadership Team
Radenta Technologies, Inc.

Noted by:

Denis G. Bermudez
Director
Client Success and Delivery Excellence Team
Radenta Technologies, Inc.

Ma. Nathalie Rose Regala – Acebedo
Director
Future Edge Business Strategist
Radenta Technologies, Inc.

Reviewed and Approved by:

Jose Marie Bonto
Chief Technology Officer (CTO) | Concurrent Head
IT Security Department
Development Bank of the Philippines

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Executive Summary

Objective

The objective of this Inception Report is to define the framework, processes, and management approach for the successful implementation of the **Managed Detection and Response (MDR) Plus Remediation Solution project**.

This engagement covers the supply, delivery, installation, configuration, and subscription of the MDR Plus Remediation Solution, including maintenance and technical support services to be provided by **Radenta Technologies Inc**. The project aims to use the proposed solutions' proprietary technology to enhance cybersecurity posture of the Development Bank of the Philippines (DBP) through the implementation of the proposed solutions, monitoring, threat detection, incident response, and remediation throughout the project's contract period.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Terms of Reference

As required by the project's Terms of Reference and Technical Specifications, the project shall cover one lot supply, delivery, installation, configuration and subscription of Managed Detection and Response Plus Remediation Solution with maintenance support by a service provider, including use of its propriety technology.

You may refer to below required specifications for your reference:
You may refer to below required specifications for your reference:

A. Solutions Provider Criteria

A.1. Certification, Expertise and Reference.

1. The solutions provider must be an authorized partner of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.

2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).

3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.

4. The solutions provider/principal must provide a 24 x 7 x 365 Cyber Security Operations Center (CSOC) of the solutions being offered for the period of three (3) years with certified cybersecurity support engineers provided locally and globally. Please refer to Figure 1 (CSOC Network Diagram) and Figure 2 (CSOC Facility Layout) for additional details.

5. The solutions provider/principal must deploy the Managed Detection and Response plus Remediation MDR+R-SOC services with the following technical expertise:

    - A dedicated onsite support engineer as full-time employee (during the contract period) of the solutions provider and must provide proof of Certificate of Employment and Curriculum Vitae.
    - The assigned support engineer must have at least: two (2) years of work experiences as an IT security support engineer, certification on MDR+R solution being offered, and two (2) formal trainings on IT Security Fundamentals.

6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.

7. The solutions provider must have at least 8 years of experience in the ICT industry and must possess extensive knowledge and skills in the latest security technologies, with at least three (3) years of experience in providing cybersecurity solutions preferably on an Enterprise MDR+R-SOC services.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

8. The solutions provider must have a similar installed base enterprise cybersecurity solution in private or government entity for the past three (3) years.

9. The solutions provider/principal must deploy a local technical account manager to oversee the continuous improvement of selected technologies installed in DBP's environment. The technical account manager must not be outsourced and must be a full-time employee of the solutions provider/principal, with proof of Certificate of Employment and Curriculum Vitae.

10. The solutions provider must designate a Project Manager who must be employed with the solutions provider for at least five (5) years before the bid opening and have at least three (3) years' experience in project management.

    Must submit the following:

    - Certificate of Employment for the assigned personnel indicating the date of hire.
    - Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).
    - Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

A.2. Customization, Data Retention and Coverage

1. The solutions provider must deliver customized reports and dashboard. They must tailor the reports and dashboard to align

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

with DBP's specific organizational requirements and cybersecurity challenges.

2. The solutions provider must formulate a complete Knowledge Transfer (KT) on the application, tools, agents, sensors, data collection and data analysis of the proposed solution.

3. The solutions provider must provide continuous collection and centralized storage of all security data for behavioral analytics.

4. The solutions provider must provide data retention of at least 90 days, with options to extend based on DBP's operational and regulatory requirements. Compliance with industry standards and legal mandates for data storage and privacy.

5. The solutions provider must provide a visibility of lateral movement across the network and other parts of the infrastructure

6. The solutions provider must support detection and response for threats involving managed and unmanaged endpoints, servers, networks, managed email users/mailbox and remote users. Detection mechanisms must include signature-based, behavioral, and AI-driven techniques, with automated response workflows and alerting.

A.3. Trainings, Security Awareness and Other Requirements

1. The solutions provider must formulate a comprehensive cybersecurity training program with TESDA-accredited training center for the following modules and participants:
   - Basic Administration for at least ten (10) participants
   - Knowledge Transfer (Minimum of One (1) knowledge transfer session provided onsite with complete materials.)

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

2. The solutions provider must develop an Annual Security Posture Assessment Plan, which includes a comprehensive evaluation of DBP's security measures and recommendations for enhancements.
3. The solutions provider must conduct phishing simulation with a unified platform that allows DBP to perform unlimited phishing simulation exercises and security awareness trainings.

4. The solutions provider must include Security Awareness licenses for at least 500 users per campaign and allow tracking of campaigns.

5. The solutions provider must provide phishing simulation tool with standard templates and allow creation of custom templates. The phishing simulation tool must allow recipients to be chosen from different data sources such as but not limited to Active directory, Microsoft Entra ID and Okta.

6. The solutions provider must provide phishing simulation tool with training campaigns. The training campaigns must have training programs in video and interactive format and be targeted for a list of recipients. The training programs must include the following training categories:

    - Business Email Compromise
    - Executives
    - Malware
    - Mobile Security
    - Password Protection
    - Phishing
    - Physical Security
    - Safe Web Browsing
    - Security Beyond the Office
    - Security Essentials
    - Social Engineering

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

7. The solutions provider must provide phishing simulation tool which allows custom templates to include company images including logos and informative content to the training campaign notification email.

B. SOLUTIONS PLATFORM REQUIREMENT

Summary List of Required Licenses, Equipment and Services	
Solutions	Technical Specifications
1. Endpoint Protection (Workstations)	• 4750 endpoints
2. Endpoint Detection and Response	• 5500 sensors
3. Server Protection	• 750 servers
4. Network Detection and Response	• 2 units with 1Gbps each of traffic inspection
5. Network Threat Prevention/IPS (Intrusion Prevention System)	• 1-unit 10Gb inspection throughput; • 2 segment 100GbE with bypass option
6. Cloud Email Security	• 5000 mailboxes
7. Security Awareness (Phishing Simulation)	• 500 users
8. CSOC Layout	• 1 Lot

All facility/solution components (servers/nodes) must be equipped with dual power supplies. This ensures power redundancy and enhances system availability in the event of a power source failure.

Any facility/solution components (servers/nodes) that requires a direct connection to the core switch-based on its designated function or operation demands-must be equipped with a network interface supporting a minimum throughput of 10Gbps. This ensures compatibility with existing network infrastructure.

B.1. Threat Detection and Continuous Monitoring

Threat Hunting and Threat Intelligence

1. The proposed solution must be able to monitor for advanced threat protection security alerts, breaches, anomalies and advanced

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

persistent threats within the scope of licenses installed under this project.

2. The proposed solution must have defined hunting techniques that are implemented using the capabilities from existing Bank's Anti-APT (Advanced Persistent Threats) technologies, proposed EDR (Endpoint Detection and Response), Email Sensor and Network Forensic device.

3. The proposed solution must provide a 24x7x365 Managed Threat Hunting Service. 5. The proposed solution must conduct continuous Vulnerability Management, Phishing Simulation Exercises and (IR) Incident Response as needed.

4. The proposed solution must have proven and established protocols for threat hunting, defined threat hunting process and triggers for threat hunts and hunt success measurement.

5. The proposed solution must conduct threat hunting based on analysis of suspicious signals, custom detection rules, and internal threat intelligence research.

6. The proposed solution must contain active threats detected, by isolating endpoints and removing malicious files or processes.

7. The proposed solution must provide integration with threat intelligence feeds for the identification of loC (Indicators of Compromise).

8. The proposed solution must have defined indicators that will trigger a proactive threat hunt.

9. The proposed solution must support sharing of loCs across multivendor security stack.

10. The proposed solution must provide proactive threat reports for verified threats and/or provide emerging threat reports on emerging threats affecting multiple organizations, designed to help the organization stay ahead of high-profile cyber- attacks.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Visibility and Detection

1. The proposed solution must provide a comprehensive visibility across network, endpoint, server, and email.

2. The proposed solution must have visibility into data sources including endpoint device, email, network packet/session.

3. The proposed solution must provide monitoring and detection of behavioral anomalies on unmanaged devices.

4. The proposed solution must provide monitoring and detection of behavioral anomalies for users.

5. The proposed solution must provide analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, email and user events over time.

6. The proposed solution must have identity analytics to detect user-based threats such as lateral movement.

7. The proposed solution must provide optimized and customizable detections and BIOCS (Behavioral Indicator of Compromises).

B.2. XDR (Extended Detection and Response)

1. The proposed solution must not be of the same brand and Service Provider that DBP is currently using with Shared Cyber Defense solution. It must be complementing and not conflicting with the currently installed solutions.

2. The proposed solution must be able to collect and correlate XDR activity data for one or more vectors using the same brand, including but not limited to - endpoints, emails, servers and networks.

3. The proposed solution must include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking for the proposed sensors for endpoints, servers, email, identities and network. It must be regularly

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

updated to improve threat detection capabilities and reduce false positive alerts.

4. The proposed solution must have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.

5. The proposed solution must allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.

6. The proposed solution must be able to analyze and determine if certain indicators signal an ongoing attack, enabling IT Admins and CSOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.

7. The proposed solution must list all the events that are mapped into the MITRE ATT&CK framework, the CSOC Analyst can use these events as starting point to do further investigations.
8. The proposed solution must provide more context with mapping to the MITRE ATT&CK TTPS for faster detection and higher fidelity alerts.

9. The proposed solution must have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.

10. The proposed solution must have an AI-powered chatbot to guide with the investigations and automatically provide answers to any questions related to cybersecurity.

11. The proposed solution must generate a root cause analysis, investigate the execution profile of an attack - including associated MITRE ATT&CK TTPS - and identify the scope of impact across assets.

12. The proposed solution must provide different search methods, filters, and an easy- to-use Kibana-like query language to identify, categorize, and retrieve search results.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

13. The proposed solution must provide a unified platform that enables security teams to take immediate response and track actions across email, identity, endpoints, and networks.

14. The proposed solution must be able to take response actions directly from the platform's investigation workbench.

15. The proposed solution must be able to automate response and remediation actions by identifying compromised accounts, applying advanced analytics, streamlining response rules, and making contextualized decisions from the platform's security playbook.

16. The proposed solution must have the ability to Add or Remove supported indicators of compromise to the block list, including but not limited to File Hash, URL, IP address, Email Addresses and Domains.

17. The proposed solution must allow automatic and manual collection of files and objects from specified endpoints.

18. The proposed solution must support automatic and manual sweeping based on solutions provider curated and third-party custom intelligence to search the environment for indicators of compromise.

19. The proposed solution must be able to view information about suspicious objects obtained by analyzing the suspicious file in a sandbox, a secure virtual environment.

20. The proposed solution must allow a CSOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX (Structured Threat Information expression) and TAXII (Trusted Automated eXchange of Intelligence Information).

21. The proposed solution must have the capability to automate a variety of actions usings playbooks to help reduce workload and speed up security tasks and investigations.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

22. The proposed solution must have the capability to create playbooks from scratch or use built-in templates to suit the organization's specific needs.

23. The proposed solution must be capable of integrating with a cybersecurity platform that can manage the organization's Email, Identity, Endpoint, Network and XDR solution all in a single console.

24. The proposed solution must provide insights into the organization's security posture using an executive level dashboard. It must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.

25. The proposed solution must have the capability to provide recommended actions to harden the environment with security configuration against future potential attacks.

26. The proposed solution must have a highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Email, Identity, Endpoint, Network, SecOps and XDR.

27. The proposed solution must be able to produce manual and scheduled reports that can be customized to display company information and logo. The generated reports must at least support PDF format and can be sent to specified email recipients.

28. The proposed solution must provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.

29. The proposed solution must be able to integrate with common SIEM and SOAR solutions.

30. The proposed solution must be able to integrate with 3rd party LDP solutions for Single Sign-On (SSO) requirements.

31. The proposed solution must provide connectors ready to integrate with other supported third-party security solutions (provide a list) or via API.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

B.3. Network Threat Prevention/IPS (Intrusion Prevention System)

1. Network Intrusion Prevention System.

1.1. The proposed IPS solution must be an appliance-based on a hardened OS shipped by-default from manufacturer.

1.2. The proposed IPS solution must be able to store at least 200 million historical events.

1.3. The proposed IPS solution must allow the update and distribution of latest security updates to be manually, automatically or based on schedule to the IPS device.

1.4. The proposed IPS solution must be able to provide a customized 'At-a- glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.

1.5. The proposed IPS solution must serve as a central point for IPS security policies management including versioning, rollback, import and export(backup) tasks.

1.6. The proposed IPS solution must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report.

1.7. The proposed IPS solution must support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis.

1.8. The proposed IPS solution must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.

1.9. The proposed IPS solution must support the archiving and backup of events and export to NFS, SMB, SCP or SFTP.

1.10. The proposed IPS solution must be able to support the syslog CEF (Common Event Format) for SIEM integration.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.11. The proposed IPS solution must support Active Directory for user ID correlation.

1.12. The proposed IPS solution must support AFC (Adaptive Filter Configuration) which will alert or disable ineffective filter in case of noisy filters.

1.13. The proposed IPS solution must support 3rd party VA (Vulnerability Assessment) scanners (e.g. Qualys, Rapid7 or Tenable) to fine tune the IPS policy.

1.14. The proposed IPS solution must support 'threat insights' dashboard that show correlated data such as how many breached hosts, how many loc data, 3rd party VA scan integration data and how many pre-disclosed vulnerabilities are discovered.

1.15. The proposed IPS solution must be able to integrate with the existing Endpoint and Server Security solution to share loC (Indicator of Compromise) feed with IPS for protection.

1.16. The proposed IPS solution must be integrated with the XDR platform for single visibility of events and management.

2. Network IPS Security

2.1. The proposed IPS solution must provide intrusion prevention functionality out of the box, with approximately 20% of filters enable in blocking mode by default.

2.2. The proposed IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine.

2.3. The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic, detect and block unknown threats associated with known malware families as well as unknown malware in real-time as they enter and cross the network.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

2.4. The proposed IPS filters must be categorized into the following list for easy
management.

2.4.1. Exploits
2.4.2. Identity Theft/Phishing
2.4.3. Reconnaissance
2.4.4. Security Policy
2.4.5. Spyware
2.4.6. Virus
2.4.7. Vulnerabilities
2.4.8. Network Equipment
2.4.9. Traffic Normalization
2.4.10. Peer to Peer
2.4.11. Internet Messaging
2.4.12. Streaming Media
2.4.13. Filters not limited to Microsoft, Adobe, SCADA/ICS system.

2.5. The proposed IPS solution must provide the following security features on top of the IPS filters:

2.5.1. Domain Generation Algorithm (DGA) Defense family of filters to detect DNS requests from malware infected hosts that are attempting to contact their command and control (C&C) hosts using DGAs.

2.5.2. Ransomware protection

2.5.3. Identify malicious Internet Protocol (IP)

2.6. The proposed IPS solution must be able to support granular security policy enforcement based on the following methods:

2.6.1. Per IPS device (all segments)
2.6.2. Per physical segment uni-direction and bi-directional
2.6.3. Per 802.1Q VLAN Tag uni-direction and bi-directional
2.6.4. Per CIDR IP address range
2.6.5. Per 802.1Q VLAN Tag and CIDR as well
2.6.6. Firewall policy per security profile

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

2.7. The proposed IPS solution must have a vulnerability-based filters as part of the security policies.

2.8. The proposed IPS solution must support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods

2.9. The proposed IPS solution must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc.

2.10. The proposed IPS solution must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C.

2.11. The proposed IPS solution must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment.

2.12. The proposed IPS solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploitability type and the reputation score.

2.13. The proposed IPS solution must be able to provide zero-day filters.

2.14. The proposed IPS solution must have the ability to view attack activities base on continent and countries.

2.15. The proposed IPS solution must allow drill-down to view detailed threat source and destination data on each attack type.

3. Network IPS appliance.

3.1. The proposed IPS appliance must support a centralized management server for enterprise management of up to 25 IPS devices.

3.2. The proposed IPS appliance must have at least 64GB RAM and 800GB storage (2x800GB SSD, RAID 1), 1RU and with redundant hot-swappable power supply.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

3.3. The proposed IPS appliance must have a Dual 1GbE RJ45/Dual 25GbE SFP28 with out-of-box remote management capabilities.

3.4. The proposed IPS appliance must have a flexible and scalable licensing model capable of up to 40Gbps of inspection throughput. The inspection throughput required must be a minimum of 10Gbps.

3.5. The proposed IPS appliance must support up to 300million concurrent connections

3.6. The proposed IPS appliance must support up to 1M new connections per second.

3.7. The proposed IPS appliance must have a latency of less than forty (60) microseconds.

3.8. The proposed IPS appliance must have at least 2segment 100GbE SR4 Bypass interface.

3.9. The proposed IPS appliance must have a built-in power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedures.

3.10. The proposed IPS appliance must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors.

3.11. The proposed IPS appliance must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime.

B.4. Network Detection and Response (NDR)

1. NDR Security.

1.1. The proposed NDR solution must be able to monitor multiple network segments (including internal network east-west traffic) for lateral movements.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.2. The proposed NDR solution must be able to monitor over 100 network protocols to identify targeted attacks, advanced threats, and ransomware.

1.3. The proposed NDR solution must provide detection of known and unknown malware being transmitted through a variety of communications channels such as: HTTP, SMTP, IMAP, POP3, and FTP

1.4. The proposed NDR solution must be able to detect zero-day malware such as document exploits.

1.5. The proposed NDR solution must provide detection of known malicious communications such as Command and Control and Data Exfiltration.

1.6. The proposed NDR solution must provide detection of targeted attacks and advanced threats.

1.7. The proposed NDR solution must provide details of attackers' network activity.

1.8. The proposed NDR solution must have built-in sandboxing technology. It must be a custom sandbox that allows the DBP to upload their tailor fitted image on the box.
1.9. The proposed NDR solution must be able to integrate with the proposed email, endpoint and server solution for automatic and seamless blocking of malicious files, IPs, or URLS.

1.10. The proposed NDR solution must provide a configurable dashboard for quick access to critical information.

1.11. The proposed NDR solution must provide extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.

1.12. The proposed NDR solution must have an automated response. Once an unknown C&C connection has been detected inside the

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

network, it must be able to share to the IPS or supported firewall solution for blocking.

2. NDR Appliance.

2.1. The proposed NDR appliance must be managed by the solutions provider, control and visibility must be extended to DBP.

2.2. The proposed NDR appliance must include a regular (at least quarterly and/or as needed) preventive maintenance.

2.3. The proposed NDR appliance must include 2 units of at least 1 Gbps each. 2.4. The proposed NDR appliance must support packet level analysis.

2.4. The proposed NDR appliance must be installed in monitoring mode only 2.6. The proposed NDR appliance must report to a unified XDR platform for event correlation across proposed endpoint, server and email sensors.

3. NDR Sandboxing.

3.1. The proposed NDR solution must support custom Windows and MacOS Sandbox.

3.2. The proposed NDR solution must be able to provide threat execution and evaluation summary.

3.3. The proposed NDR solution sandbox reports must be exportable.

3.4. The proposed NDR solution must be able to track system file and registry modification.

3.5. The proposed NDR solution must be able to detect system injection behavior detection.

3.6. The proposed NDR solution must be able to detect network connections initiated.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

3.7. The proposed NDR solution must support the following content types for document exploits: PDF, XLS, DOC, SWF, RTF.

3.8. The proposed NDR solution must support the following compressed files: ZIP, RAR, PKZIP, LZH.

3.9. The proposed NDR solution must support the following Microsoft OS file formats: EXE, DLL, SYS, CHM, LNK.

B.5. Cloud based Email Threat Security

1. Threat Detection and Protection.

1.1. The proposed solution must have protection from AETS (Advanced Evasion Techniques) using malformed emails.

1.2. The proposed solution must have retroactive alerting for URLs later determined to be malicious.

1.3. The proposed solution must extract and block suspicious URLs embedded in PDF files within emails.

1.4. The proposed solution must detect and block advanced threats in emails: attachment, URL, and impersonation-based attacks.

1.5. The proposed solution must dynamically analyze attached files, including those with password-protection and TLS (Transport Layer Security) encryption.

1.6. The proposed solution must have a collaboration protection capability to detect malicious files found in SharePoint, OneDrive, Teams, Google Drive, Box, and Dropbox.

1.7. The proposed solution must have an IP reputation checking capability to block emails from known sources of spam emails (RBL-Realtime Blackhole Lists).

1.8. The proposed solution must have domain authentication capabilities (e.g. SPF, DKIM, DMARC).

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.9. The proposed solution must protect against spam, malware, phishing, BEC (Business Email Compromise), and ransomware email attacks.

1.10. The proposed solution must be able to identity and detect graymail based on their category (e.g. marketing and newsletter, social network notifications, forum notifications, bulk email message).

1.11. The proposed solution must support file sanitization (or Content Disarm and Recovery) to neutralize all unfamiliar code hiding in emails that contain active content such as macros in the email attachments.

1.12. The proposed solution must have an attachment password guessing capability which attempts to find passwords in email content to access password-protected attachments, making it possible to scan and detect any malicious payload in these files.
1.13. The proposed solution must have a predictive machine learning scanning capability to find unknown malware before cloud sandboxing and improve delivery efficiency.

1.14. The proposed solution must support cloud sandboxing of suspicious file attachments and suspicious URLs found in email.

1.15. The proposed solution must provide URL rewriting and URL time of click protection capabilities.

1.16. The proposed solution must have a web reputation technology to scan URLs in email messages and track the credibility of web domains by assigning a reputation score based on factors including website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing attacks that are designed to trick users into providing personal information.

1.17. The proposed solution must support URL extractions from QR codes to stop phishing, ransomware, and BEC attacks.

1.18. The proposed solution must support dynamic URL scanning and crawl on the web pages of untested URLs in real-time to determine

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

whether the pages contain malicious patterns to keep users from zero-day phishing attacks.

1.19. The proposed solution must leverage artificial intelligence (AI)-based computer vision to analyze branded website elements and recognize fake sites to protect users against credential phishing.

1.20. The proposed solution must have an AI-based computer vision to recognize key elements of a valid cloud service log-on page or forms to help prevent users from submitting credentials to untrusted sites and help them get rid of account compromise.

1.21. The proposed solution must detect display name spoofing and be able to analyze messages from external senders with a look-alike display name as used in the company.

1.22. The proposed solution's BEC detection must support adding and maintaining a list of HPU (High-Profile Users) and HPD (High-Profile Domains).

1.23. The proposed solution's BEC detection must check the email header for behavior analysis and the email content for intention analysis. 1.24. The proposed solution's BEC detection must support Writing Style DNA technology and provide authorship analysis to detect email attacks impersonating high-profile users.

1.25. The proposed solution must check for unusual signals or behaviors in email (e.g. the sender has not sent any email in at least the past 30 days, unfamiliar sender discussing payment related issues, etc.).

1.26. The proposed solution must provide account takeover protection and alert if an account has been compromised to steal data, deliver malware, or conduct internal and supply chain phishing.
1.27. The proposed solution must offer DLP (Data Loss Prevention) capability both for email messages and files in cloud collaboration services.

1.28. The proposed solution must offer an email encryption capability and be able to encrypt email content for confidentiality.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.29. The proposed solution must be able to retro-scan historical email messages to identify and stop previously unknown or undetected threats in messages, such as spam, phishing, and malware, and take automated remediation actions using the latest pattern files and machine learning technologies.

1.30. The proposed solution must be able to rescan historical URLs in users' email metadata and perform automated remediation (automatically taking configured actions or restoring quarantined messages) using the latest pattern files updated by the web reputation services.

1.31. The proposed solution must be able to run a manual scan and perform an on-demand scan of targets including exchange mail stores, SharePoint sites, and file stores.

1.32. The proposed solution must be able to integrate with MIP (Microsoft Information Protection) to decrypt and scan MIP-encrypted emails and files.

1.33. The proposed solution must be able to decrypt and scan MIP-encrypted email messages/attachments in Exchange Online and MIP-encrypted files in SharePoint, OneDrive, and MS Teams.

1.34. The proposed solution must include an email continuity feature and provide a standby email system for virtually uninterrupted use of email in the event of a mail server outage.

1.35. The proposed solution must be able to keep the incoming email messages for at least 10 days and be able to restore email messages to the email server once it's back online within the 10-day period, if a planned or unplanned outage occurs.

1.36. The proposed solution must have a continuity mailbox available instantly and automatically providing end users the ability to read, forward, download and reply to any email messages and have continued email access during an outage.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.37. The proposed solution must have the ability to delete the selected email message from the selected mailboxes.

1.38. The proposed solution must have the ability to move the selected email message to the quarantine folder and quarantine the message from all affected mailboxes.

1.39. The proposed solution must be able to prevent or mitigate cyberthreats and other email attacks with solutions provider or DBP's feed threat intelligence.

2. Advanced Threat Alerts and Forensics.

2.1. The proposed solution must provide detailed information on every advanced threat alert, including alert ID, date and time, sender's email address, targeted email addresses, malicious email subject, MD5 hash, malicious URL or attachment, originating email server, email status, threat classification, and severity.

2.2. The proposed solution must provide dynamic analysis of malware file types, vulnerable applications, and operating systems.

2.3. The proposed solution must provide forensic evidence including malicious files and network activity packet captures.

2.4. The proposed solution must provide malware communications report detailing URL analysis and raw requests.

2.5. The proposed solution must provide native report on operating system changes, services, registry keys, and system configuration changes.

2.6. The proposed solution must provide threat intelligence report with detailed information on detected threats, including risk level, affected software, vulnerability information, and remediation patches.

3. Deployment Modes.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

3.1. The proposed solution must support for inline deployment mode via MX redirection (active analysis and blocking/quarantine of threats).

3.2. The proposed solution must support API for internal email inspection.

3.3. The proposed solution must be Cloud-based with no hardware or software to install.

3.4. The proposed solution must provide real-time, dynamic threat protection.

3.5. The proposed solution must be ISO27001 compliant, adhering to the Information Security Management System (ISMS) standard.

3.6. The proposed solution must be 99.9% availability guaranteed.

4. Access Control.

4.1. The proposed solution must limit domains and domain groups access for users (Full or Read Only access).

4.2. The proposed solution must not allow users to modify policies outside their assigned domains and groups.

5. Customization and User Interface.

5.1. The proposed solution must provide customizable email digest templates in the Web UI.

5.2. The proposed solution must provide end-user portal for quarantine management and review of malicious emails.

6. Integration and Compatibility.

6.1. The proposed solution must provide integration with an XDR platform for alert correlation.

7. Dashboard and Reporting.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

7.1. The proposed solution must provide native dashboard statistics with threat map displaying threat locations.

7.2. The proposed solution must provide daily digests of quarantined emails for specific users/recipients.

7.3. The proposed solution must provide executive summary report of email traffic, content analysis, and threat categories.

8. Email Handling Rules.

8.1. The proposed solution must provide creation of allow and deny rules based on criteria such as reverse DNS validation, sender country internet domain suffix, recipient email address, sender IP address, sender email address, and sender email domain.

8.2. The proposed solution must have the ability to drop, quarantine, deliver, route, BCC (Blind Carbon Copy), insert custom headers, and modify the subject of emails based on specific criteria.

8.3. The proposed solution must have the ability to bypass antivirus and antispam scanning based on specific criteria.

9. File Type Analysis.

9.1. The proposed solution must provide dynamic analysis of attached file types and/or extensions such as EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives.

B.6. Server Security and Protection.

1. General Server Security.

1.1. The proposed solution must have an option for on-premise management for server protection over physical and virtual servers.

1.2. The proposed solution must allow the on-premise management server to connection to a cloud-based unified XDR platform.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.3. The proposed solution must provide layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.

1.4. The proposed solution must protect a wide range of platforms including but not limited to: AIX, AlmaLinux, Amazon Linux, CentOS, CloudLinux, Debian, Oracle Linux, RHEL, Micracle Linux, Red Hat OpenShift, Rocky Linux, Solaris, SUSE Linux, Ubuntu Linux and Windows including legacy OS.

1.5. The proposed solution must have multiple security modules listed below, providing a line of defense at the server in a single agent:

1.5.1. Anti-Malware

1.5.1.1. The proposed anti-malware solution must provide agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, trojans, and spyware.

1.5.1.2. The proposed anti-malware solution must allow manual and schedule scans to be configured.

1.5.1.3. The proposed anti-malware solution must be able to provide Web Reputation filtering to protect against malicious web sites

1.5.1.4. The proposed anti-malware solution must have an option to configure its detection and prevention level from cautious, moderate to aggressive and extra aggressive for its protection capabilities.

1.5.1.5. The proposed anti-malware solution must have Predictive Machine Learning to protect against unknown malware.

1.5.1.6. The proposed anti-malware solution must have behavioral monitoring to protect against suspicious activity and unauthorized changes including ransomware.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.5.1.7. The proposed anti-malware solution must provide ransomware protection, that can backup & restore encrypted documents.

1.5.1.8. The proposed anti-malware solution must scan process memory for malware.

1.5.2. Device Control

1.5.2.1. The proposed device control solution must support USB mass storage, autorun function and mobile - MTP (Media Transfer Protocol)/PTP (Picture Transfer Protocol).

1.5.2.2. The proposed device control solution must have option to choose from full access, read only and block.

1.5.3. Intrusion Detection and Prevention System

1.5.3.1. The proposed solution must be able to provide HIPS (Host Intrusion Prevention System) /HIDS (Host-Based Intrusion Detection System) features.

1.5.3.2. The proposed solution must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.

1.5.3.3. The proposed solution must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.

1.5.3.4. The proposed solution must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.

1.5.3.5. The proposed solution must be able to provide protection against known and zero-day attacks

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.5.3.6. The proposed solution must provide protection that can be pushed out to thousands of servers in minutes without a system reboot.

1.5.3.7. The proposed solution must include out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services.

1.5.3.8. The proposed solution must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code

1.5.3.9. The proposed solution must include exploit rules to stop known attacks and malwares.

1.5.3.10. The proposed solution must assist in compliance of PCI DSS (Payment Card Industry Data Security Standard) to protect web applications and the data being process.

1.5.4. Firewall

1.5.4.1. The proposed solution must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.

1.5.4.2. The proposed solution must have fine-grained filtering (IP and MAC addresses, ports).

1.5.4.3. The proposed solution must have coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)

1.5.4.4. The proposed solution must have prevention of denial of service (DoS) attack

1.5.4.5. The proposed solution must allow policies per network interface

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.5.4.6. The proposed solution must have detection of reconnaissance scans.

1.5.5. Integrity Monitoring

1.5.5.1. The proposed solution must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.

1.5.6. Virtual Patching

1.5.6.1. The proposed solution must provide virtual patching which shields vulnerable systems that are awaiting a security patch. It must automatically shield vulnerable systems within hours and push out protection to thousands of workloads within
minutes.

1.5.6.2. The proposed solution must have the intelligence to provide recommended virtual patching rules to protect against OS & Application vulnerabilities.

1.5.6.3. The proposed solution must be able to create scheduled tasks to run recommendation scan to discover new rules to apply.

1.5.6.4. The proposed solution must be able to automatically assign new virtual patching rules through scheduled tasks.
1.5.6.5. The proposed solution must be able to automatically unassign virtual patching rules after physical patch has been installed.

1.5.6.6. The proposed solution must support more than 350 distinct applications for virtual patching but not limited to web applications, databases, etc.

1.5.7. Log Inspection

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.5.7.1. The proposed solution must be able to provide the capability to inspect logs & events generated by operating systems & applications

1.5.7.2. The proposed solution must be able to automatically recommend and assign relevant log inspection rules to the server based on the operating system & applications installed

1.5.7.3. The proposed solution must be able to automatically recommend and unassign log inspection rules that are not required

1.5.7.4. The proposed solution must have predefined template for operating system and enterprise application to avoid manual creation of the rules

1.5.7.5. The proposed solution must allow creation of customized rules to support custom application

1.5.8. Application Control

1.5.8.1. The proposed solution must be able to monitor changes made to the server compared to baseline software

1.5.8.2. The proposed solution must be able to allow or block the software and optionally lock down the server from unauthorize change

1.5.8.3. The proposed solution must allow maintenance mode to allow installation of software and changes OS

1.5.8.4. The proposed solution must have an alert when unauthorized scripts and application are executed.

1.5.8.5. The proposed Application Control solution must support the following software:

1.5.8.5.1. Windows applications (.exe, .com, .dll, .sys)

1.5.8.5.2. Linux libraries (so) and other compiled binaries and

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Libraries

1.5.8.5.3. Java jar and .class files, and other compiled byte code
1.5.8.5.4. PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly

1.5.8.5.5. Windows PowerShell scripts, batch files and other Windows-specific scripts (.wsf, .vbs, js)

B.7. Endpoint Protection, Detection and Response with Remediation

1. General Endpoint Protection and EDR.

1.1 The proposed solution must be able to integrate with the proposed Network Detection and Response Solution.

1.2 The proposed solution must be able to automatically receive IOCS regarding alert detections from existing Network Advance Threat Platform.

1.3 The proposed solution must be a SaaS based endpoint security and EDR solution.

1.4 The proposed solution must have an option to deploy a hardened service gateway to act as a forward proxy service that connects on- premise solutions to the cloud-based platform.

1.5 The proposed solution must be managed through the unified XDR platform.

1.6 The proposed solution must be able to analyze and validate network alerts by finding evidence of matching threat activity on endpoints quickly.
1.7 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence.

1.8 The proposed solution must allow for detection, validation and containment through the native interface.

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.9 The proposed solution must able to isolate at-risk endpoints to run an investigation and resolve security issues and restore the connection promptly when all issues have been resolved.

1.10 The proposed solution must allow creation of custom indicators of compromise, and support those shared by others using OpenIOC format.

1.11 The proposed solution must display inactive hosts i.e. the number of monitored hosts that have not checked in for 30 days or more.

1.12 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence including known malware, malware variants/key functions, methodology and behavioral IOCS.

1.13 The proposed solution must allow creation of custom indicators of compromise coming from past/ongoing investigations or external entities.

1.14 The proposed solution must have anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. It must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.

1.15 The proposed solution must support the ability to exclude applications or files from exploit detection.

1.16 The proposed solution must support the recording of recent activity on each endpoint in an indexed and searchable lookback cache, minimally file writes, registry operations, network connections, DNS resolutions, URL collection, process loaded in memory.

1.17 The proposed solution must be able to remotely acquire files and other triage information for investigation purposes.

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.18 The proposed solution must be able to remotely connect to an endpoint and dump process memory.

1.19 The proposed solution must have the ability to remotely connect and execute custom PowerShell or Bash scripts.

1.20 The proposed solution must have the ability to execute custom YARA rules on the specified endpoints.

1.21 The proposed solution must have the ability to view and terminate active processes on a specific endpoint or multiple endpoints.

1.22 The proposed solution must offer a built-in graphical triage viewer to ease security operations and require no more than an entry level CSOC analysts and/or IR responder skillset to operate

1.23 The proposed solution must support concurrent searches across all endpoints.

1.24 The proposed solution must have the ability to pull locally stored data from specified endpoints in near real-time to support high priority hunt and forensic operations

1.25 The proposed solution must provide full visibility into commands issued via the native operating system shell (i.e., Windows command prompt or Bash). It must also provide full visibility into commands issued via augmented shells, such as Windows PowerShell.

1.26 The proposed solution must be able to read and display locally stored data from specified endpoints

1.27 The proposed solution must support containment of suspected hosts while maintaining access to the endpoint forensics solution for investigation as well as other whitelisted resources used for investigation or remediation.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.28 The proposed solution must be able to automatically terminate exploited applications or automatically prevent any payload from exploited application to run.

1.29 The proposed solution must be able to notify end-user automatically when isolating at-risk endpoints ensuring seamless user experience. 1.30 The proposed solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must be able to identify and label high-value hosts.

1.31 The proposed solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.

1.32 The proposed solution must at the minimum support the following prevention capabilities:

i. Antimalware with signature/Pattern based detection
ii. Ransomware protection
iii. Machine learning-pre-execution and runtime
iv. Browser exploit protection
V. Behavior monitoring
vi. Injection protection
vii. Script protection
viii. Anti-exploit
ix. C&C communication prevention
X. Application control
xi. File less malware prevention
xii. File/web reputation

1.33 The proposed solution must support proxy, fully configurable in the Web UI and in the CLI.

1.34 The proposed solution must support tamper protection, such as requiring password to uninstall the agent from an endpoint.

1.35 The proposed solution must be able to regulate the number of indicators and exploit alerts processed by the service provider solution.

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.36 The proposed solution must also include Anti-virus protection and machine learning protection.

1.37 The proposed solution's machine learning must have pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.

1.38 The proposed solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and must have feature with documents to be protected from unauthorized encryption or modification.

1.39 The proposed solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.

1.40 The proposed solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/ Port/Protocol/Application to provide stateful inspection and high performance network virus scanning.

1.41 The proposed solution must have an integrated Application Control to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities.

1.42 The proposed Application Control solution must provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.
1.43 The proposed Device Control solution must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The devices able to be restricted must include but not limited to the following:

i. USB Storage Drives (Also able to disable autorun)
ii. CD-ROM
iii. Floppy Disk
iv. Network Drives

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.44 The proposed Device Control solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT, Imaging Devices, Wireless Nic, Infrared devices

1.45 The proposed solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.

1.46 The proposed solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (trojans, registry entries, and viral files).

1.47 The proposed solution must be able to schedule and provide on-access malware scan support. e.g. Requests for full scans, quick scans, and memory scans (which scan running processes).

1.48 The proposed solution must support malware remediation. e.g. removing artifacts created by the malware and revert changes the malware made to other files or registry entries.

1.49 The proposed solution must provide global and exception policies to control malware protection.

1.50 The proposed solution must be able to support malware definitions downloadable either from the Internet or service provider solution

1.51 The proposed solution must be able to download false positive malware information.

1.52 The proposed solution must support malware alert throttling. Alerts generated when malware is detected on endpoints are throttled to limit the maximum number of alerts produced for a single infection in a given time interval.

1.53 The proposed solution must classify attack detections using the taxonomy defined in the MITRE ATT&CK framework.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

1.54 The proposed solution must provide automated analysis and visualization of an attack; including entity relations graphing, production of an event timeline and initial assessment of severity/impact/confidence level.

1.55 The proposed solution must provide vulnerability protection solution integrated on a single security agent.

1.56 The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.

1.57 The proposed solution must support at least Windows 7 Operating System.

B.8. Firewall Monitoring

1. The solution provider must provide continuous firewall log monitoring 24x7.

2. The solution provider must provide detection of security anomalies such as:

2.1. Unauthorized access attempts
2.2. Policy violations
2.3. Port Scans, DoS attempts, or unusual traffic patterns
2.4. Denial of Service (DoS) or DDoS attempts
2.5. Intrusion attempts (via IPS)
2.6. Command and Control (C2) communications
2.7. Access to malicious or phishing websites
2.8. Unusual traffic patterns or spikes
2.9. Use of unauthorized or risky applications

3. The solution provider must provide escalation of critical alerts according to severity and predefined SLAs.

4. The solution provider must generate monthly monitoring reports including:

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

4.1. Alert Summary
4.2. Top Talkers
4.3. Policy usage
4.4. Threat trends

B.9. CSOC Facility Layout

Technical Specifications	Quantity
1. Videowall 2 x 3 Display, Diagonal Size 55", Resolution 1920x1080 (min), with wall-mounting brackets.	6 units
2. Videowall Controller (Minimum Core i9 12th Gen) and Videowall Management Software	1 unit
3. Triple Monitor Workstation with table console, chair and peripherals.	3 sets
4. Uninterruptible Power Supply (UPS) covering the power load requirements of the CSOC equipment.	1 lot
5. Air Cooling Unit (ACU) covering the CSOC area	1 lot
6. Networks (42u Modular Rack, 24port POE Switch, cablings, roughing in materials and accessories).	1 lot

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

7. Other Miscellaneous Components (video capture card, graphic card, HDMI extender/splitter, USB extender, wall plate, etc.)	1 lot
8. Installation, Configuration and Knowledge Transfer.	1 lot

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Scope of work

The Onsite SOC Security Engineer will provide monitoring, analysis, and support for the Managed Detection and Response plus Remediation (MDR+R) solution and the Check Point firewall environment. This role ensures proactive detection of security incidents, effective response to threats, and proper documentation of actions, while working within defined operational boundaries.

The scope, limitations, and assumptions outlined below define the responsibilities and expectations for this engagement.

Onsite SOC Security Engineer	**MDR+R Scope** • Monitor Vision One alerts, detections, and anomalies. • Perform alert triage and classification. • Execute containment actions, such as endpoint isolation and blocking, upon approval of the DBP • Correlate Vision One events with firewall and network logs for comprehensive analysis. • Document all Vision One-related incidents, investigations, and actions taken. • Provide input for incident reports and participate in post-incident reviews as needed. **Firewall** *(Checkpoint)* **Monitoring** • Monitor Check Point Firewall logs and security events • Review and identify unusual or suspicious traffic patterns • Validate and review firewall rule changes and policy updates, as required • Support firewall-related incident response (IP/domain blocks, policy tuning) • Analyze network traffic correlated with Vision One alerts • Monitor VPN, NAT, and access rules for irregularities • Report firewall health, performance, and security posture • Recommend firewall-related security improvements, as required *Note:* ***The Onsite SOC Security Engineer will perform all responsibilities during regular office hours (8x5 business hours). Any urgent incidents or alerts outside these hours will be escalated according to the agreed escalation protocol with the customer.***
24 by 7 Remote Monitoring	**MDR+R**

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

	• 24 by 7 monitoring of alerts, detections, and behavioral anomalies • Real-time triage and severity classification • Correlation of endpoint, network, identity, email, and cloud security events • Remote containment actions (isolation, blocking, quarantine) • IOC searches and retro-analysis across Vision One telemetry • Support incident investigation through log and artifact collection • Identify patterns and recurring threats impacting overall risk • Notify client and onsite SOC of high-severity alerts • Provide incident summaries including indicators, timeline, and recommended actions **Firewall** *(Checkpoint)* **Monitoring** • 24/7 monitoring of firewall logs, events, and traffic flows • Identification of suspicious inbound or outbound activities • Verification of firewall rule behavior and IPS events • Remote support for blocking malicious IPs/domains based on approval • Correlating firewall traffic with Vision One detections • Monitoring VPN, NAT, and access rule activities • Reporting on firewall health and potential security gaps
Limitations	• Direct firewall configuration and management • Management of access provisions (accounts, IAM) • Execution of security recommendations; these require approval/action by client or authorized personnel • Administration of third-party security tools outside MDR+R and firewall systems
Assumptions	• Timely access to systems, logs, and tools will be provided • Vision One and Check Point systems are properly deployed and operational • Required firewall and network logs are accessible • Actions outside scope will be requested and approved separately • Client will provide necessary network, policy, and security documentation • SOC engineer relies on accuracy and completeness of alert and log data • Recommendations will be implemented by client or authorized personnel

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Project Deliverables

The following section outlines the key deliverables essential to the successful execution of the project. These deliverables are derived from and aligned with the Terms of Reference (TOR) provided, ensuring that all requirements and expectations are clearly addressed. Each item represents a critical output that will be provisioned, reviewed, and delivered within the agreed timelines, serving as a foundation for tracking progress and evaluating project success.

Project Components

As the selected provider for this project, Radenta Technologies shall deliver all required project deliverables. Please note that the CSOC, DDI, and TippingPoint components may be subject to adjustments based on the final specifications identified during the onsite inspection and agreement. Furthermore, all hardware and software components included in this project shall carry the standard warranty provided by the manufacturer or vendor, ensuring support and replacement coverage in accordance with their official warranty terms.

Project Requirements	Proposed Solution
▪ **Cloud-Based Email Security** for 5,000 mailboxes	▪ Trend Vision One Email and Collaboration Security Pro (1 year subscription upon activation)
▪ **Endpoint Detection and Response (EDR)** for 5,500 sensors	▪ Service One Complete Endpoint & Workloads Includes Messaging (1 year subscription upon activation)
▪ **Endpoint Protection for Workstations** for 4,750 endpoints	▪ Trend Vision One – Endpoint Security Essentials (1year subscription upon activation)
▪ **On-Premise EDR Solution** for 750 servers	▪ Deep Security – Enterprise Perpetual Server (VM) (1 year subscription upon activation)

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

▪ **Network Forensics / Packet Capture Solution** – 2 units	▪ Deep Discovery Inspector 1000 Appliance (Including 1yr HW Warranty) (1 year subscription upon activation) ▪ Deep Discovery Inspector 1000 Software with 1Gbps (1 year subscription upon activation)
▪ **Network Intrusion Prevention System (IPS)** – 1 unit, inclusive of three (3) years of maintenance support	▪ TippingPoint 8600TXE HW + Support 1 year ▪ TippingPoint 10Gbps TPS Inspection License + Threat DV + TLS inspection + Support + DV 1Yr AMEA ▪ TippingPoint SMS H5 (Dell) + Support 1 Yr ▪ TippingPoint TXE IO Module 2- Segment 100GbE SR4 Bypass ▪ TippingPoint 100GbE SR4 QSFP28 XCVR
▪ **Security Awareness Training Licenses** for 500 users	▪ Trend Vision One – Cyber Risk Exposure Management Essentials
▪ **Cyber Security Operations Center (CSOC) Facility Layout** – 1 lot	▪ LG 55VL5PJ 2X3 (3 years warranty) ▪ Hardware Controllers with cabling, peripherals, and hardware console tablet (3 years warranty except for hdmi cables and POE switch for the controller modules) ▪ ASUS High End Workstation i9 12th Gen minimum; Triple monitor setup with peripherals, UPS and bracket. (3 years warranty) ▪ ASUS Mid End Workstation i5 or equivalent; Triple monitor setup, with peripherals, UPS and brackets. (3 years warranty) ▪ Standard Office Table ▪ Standard Office Chair ▪ UPS RACKMOUNT 3KVA Kebos PowerGarde 3000VA (w/ 3 yrs warranty on electronics and 3 year on battery with SNMP Card for monitoring)

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

	▪ Aircon Condura Brand (warranty to be defined) ▪ TUFFRACK 42U DATA CABINET (1 year warranty) ▪ TPLINK SG6428XHP - Omada 24-PortGigabit Stackable (3 years warranty) ▪ Electrical Cabling (3 years workmanship warranty) ▪ Structured Cabling (3 years workmanship warranty)

Implementation Deliverables

A. **Inception Report** – Work Plan including Scope, Breakdown of Regular Activities for MDR+R, and Deliverables

B. **Technology Deployment** – weekly status report with the following details:
- Number of successful and unsuccessful endpoints installation.
- Failures or errors encountered during the installation/uninstallation
- Status per endpoint (e.g. success, failed, pending) including timestamp per hostname and IP Address.

C. Conduct of MDR+R

D. **Status Reporting** – weekly, monthly, and quarterly status report of all activities

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

- Weekly reports must be submitted every Tuesday of the following week.
- Monthly reports must be submitted every first (1st) week of the succeeding month.
- Quarterly reports must be submitted every first (1st) week of the succeeding quarter.

E. **Reports** – must be available in the MDR+R Service Portal
   - Regular management reporting of detected emerging threats, trends and actionable mitigation.
   - Personalized intelligence reports that offer insight into organization's risk profile, key findings, attacker profiles and motivations, and industry-specific intelligence.
   - Investigation and analysis reports
   - Remediation activities and solutions applied

F. **Documentation and Training** – all documentation must be in hard and soft copies in **Microsoft Word (.doc, .docx)** and **PDF** format.
   - User Manuals / Technical / Reference Manuals
   - System / Operation Manuals / Troubleshooting and Installation Guides
   - System Design and Architecture
   - As Built Documents

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Main Deliverables & Proposed High-Level Project Timeline

The project will commence on **November 13, 2025**, with the release of the Notice to Proceed. The first deliverable, a detailed work plan, will be completed within two weeks. Following plan approval, the delivery, installation, and configuration of the Managed Detection and Response (MDR) system, including vulnerability and compromise assessments and required data connections, will take four weeks.

Subsequently, use cases will be identified and created over a four-week period. The final phase involves documenting the MDR processes, which is scheduled for completion within four weeks after the use cases are approved, culminating the project on **February 19, 2026**.

Deliverables	No. of Weeks	Completion Time	Start Date	End Date
Detailed work plan	2	2 weeks after the release of the Notice to Proceed (NTP)	November 13, 2025	November 27, 2025
Delivery, Installation and configuration of Managed Detection and Response Plus Remediation with Vulnerability and Compromise	4	Within 4 weeks after approval of the detailed work plan	November 27, 2025	December 25, 2025

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Assessments and other tools Required for the setup including connection of all data sources				
Identification and Creation of Use Cases	4	Within 4 weeks after implementation of Managed Detection and response plus remediation with Vulnerability and compromise assessment and other tools.	December 25, 2025	January 22, 2026
Managed Detection and Response Plus Remediation with Vulnerability and Compromise Assessments Process Documentation	4	Within 4 weeks after approval of identification and creation of Use Cases	January 22, 2026	February 19, 2026

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

High – Level Project Timeline (Gantt Chart)

The project timeline is divided into several milestones. The first milestone starts on 13 November 2025 with the submission of the Work Plan or Inception Report, which defines the project scope, activities, schedule, and reporting requirements outlined in the Terms of Reference.

The second milestone covers the delivery, installation, and configuration of the MDR+R solution. This is targeted for completion by the fourth week of December 2025, ensuring that all required components are in place and functioning.

The third milestone involves the identification and development of use cases, scheduled from late December 2025 up to the third week of January 2026.

The fourth milestone follows with the preparation of the MDR+R process documentation, including the procedures for conducting Vulnerability and Compromise Assessments.

These milestones provide a clear timeline for completing the major phases of the project. Further updates will be provided as the project progresses.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

One (1) Lot Supply, Delivery, Installation, Configuration and Subscription of Managed Detection and Response Plus Remediation (MDR+R) Solution				NOV 2025				DEC 2025				JAN 2026				FEB 2026			
Phase	Deliverable	Required Weeks	WEEK>> >	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Detailed Work Plan	2																	
2	Delivery, installation and configuration of Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments and other tools required for the setup including connection of all data sources	4																	
3	Identification and Creation of Use Cases	4																	
4	Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments Process Documentation	4																	

Legend	
Completed	
Ongoing	
Not Started	

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Proposed Implementation Plan

The proposed Implementation Plan provides a comprehensive roadmap for the completion of all project phases, culminating on February 16, 2026. The timeline ensures that all key activities, dependencies, ownership, and deliverables are clearly defined for efficient execution.

The main deliverables include the detailed work plan, delivery, installation, and configuration of Managed Detection and Response Plus Remediation with Vulnerability and Compromise Assessments along with all required tools and data source integrations, identification and creation of use cases, and the process documentation for the Managed Detection and Response Plus Remediation with Vulnerability and Compromise Assessments.

This structured timeline enables stakeholders to monitor progress effectively and ensures timely delivery of all project objectives.

PHASE 1 – PRE-IMPLEMENTATION & PLANNING Duration: November 13 – December 05, 2025					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
1.1	Unified Kickoff & Scope Confirmation	None	• Approved Scope, Roles, Communication Plan	13-Nov	13-Nov
1.2	Stakeholder Identification	1.1	• Stakeholder List	14-Nov	14-Nov
1.3	Final Communication Plan & Escalation Matrix	1.2	• Communication Plan	15-Nov	18-Nov
1.4	Technical & Site Assessment (DDI, TippingPoint, CSOC combined)	1.3	• Site Readiness Checklist, • Network Diagram, • Rack/Power Assessment	19-Nov	29-Nov
1.5	Final Implementation Plan / Inception Report	1.4	• Consolidated Implementation Plan	2-Dec	5-Dec

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

PHASE 2 – LOGISTICS & SITE PREPARATION Duration: December 6, 2025 to December 10, 2025					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
2.1	Equipment Deliveries (DDI, TippingPoint, CSOC)	1.5	• Delivery Receipts & Verification	6-Dec	10-Jan
2.2	Site Readiness (Power, Cooling, Cabling, Rack Prep)	1.5	• Ready site for installation	6-Dec	10-Jan
2.3	Hardware Commissioning (if required)	2.2	• Hardware readiness verification	8-Jan	10-Jan
PHASE 3 – DEPLOYMENT & INSTALLATION Duration: January 11, 2026 – January 24, 2026					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
3.1	Physical Installation of All Appliances (DDI, TippingPoint, CSOC)	2.1, 2.2	• Mounted and powered appliances	11-Jan	14-Jan
3.2	Network Connectivity Setup (Management, Monitoring, SPAN/TAP)	3.1	• Connectivity Validation Report	15-Jan	17-Jan
3.3	Base System Configuration (IP, DNS, NTP, Firmware, Licensing)	3.2	• Configured Systems	18-Jan	22-Jan
3.4	Setup of Workstations, Video Wall, UPS, Switches (CSOC)	3.1	• Installed and configured CSOC environment	18-Jan	24-Jan
PHASE 4 – SYSTEM CONFIGURATION & INTEGRATIONS Duration: January 25, 2026 – February 5, 2026					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
4.1	DDI Policy Import & Rule Setup	3.3	• DDI Policy Set	25-Jan	28-Jan
4.2	TippingPoint Policy, IPS, Filters, ATP Setup	3.3	• Optimized TP Configuration	25-Jan	31-Jan
4.3	Integration Setup (Vision One, LDAP/AD, SMTP, XDR)	4.1, 4.2	• Integration Confirmation	29-Jan	3-Feb
4.4	Monitoring/VLAN/L2-L3 config across platforms	3.3	• Visibility Validation Report	29-Jan	5-Feb

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

PHASE 5 – CUTOVER, MIGRATION & TESTING Duration: February 6, 2026 – February 12, 2026					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
5.1	Backup of Old Systems (DDI + TP)	4.x	• Backup Integrity Log	6-Feb	7-Feb
5.2	Cutover: Disconnect Old → Connect New (DDI + TP)	5.1	• Cutover Report	10-Feb	11-Feb
5.3	System Validation (Traffic, Alerts, Logging, Video Wall, Network)	5.2	• Validation Report	12-Feb	12-Feb
PHASE 6 – OPTIMIZATION, KT & PROJECT CLOSURE Duration: February 13, 2026 – February 19, 2026					
Task ID	**Task**	**Dependencies**	**Deliverables**	**Start**	**End**
6.1	Policy Tuning, False Positives, Threshold Optimization		• Optimized Detection Profiles	13-Feb	14-Feb
6.2	Knowledge Transfer (DDI + TP + CSOC)		• KT Completion Report	14-Feb	14-Feb
6.3	Documentation Handover		• As-Built Documents	15-Feb	15-Feb
6.4	Final Acceptance & Sign-Off		• Project Completion Certificate	16-Feb	18-Feb

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Methodology

Radenta Project Team will apply the guidelines based on project management as defined in the Project Management Body of Knowledge (PMBOK), to deliver the project from initiation to completion.

The PMBOK Guide is process-based, meaning it describes work as being accomplished by processes. This approach is consistent with other management standards such as ISO 9000 and the Software Engineering Institute's CMMI. Processes overlap and interact throughout a project or its various phases.

- Inputs (documents, plans, designs, etc.)
- Tools and Techniques (mechanisms applied to inputs)
- Outputs (documents, plans, designs, etc.)

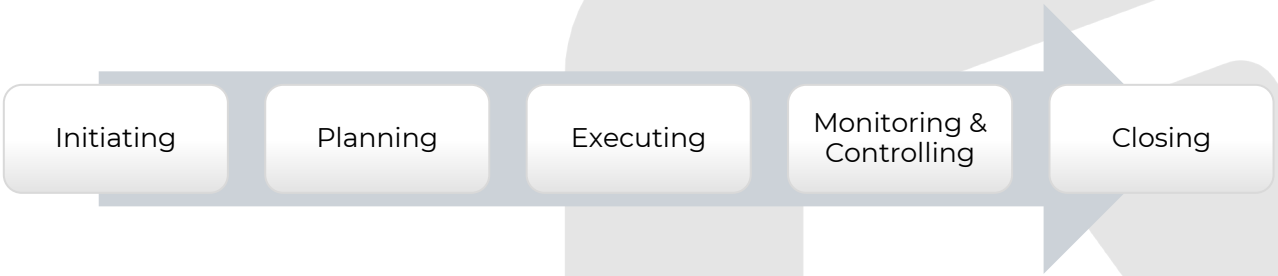

Figure 1 - **Project Phases**

In PMBOK, a project is divided into 5 phases. These phases are:

1. **Initiating** - processes performed to define a new project or a new phase of an existing project by obtaining authorization to start the project or phase.

2. **Planning** - processes required to establish the scope of the project, refine the objectives, and define the course of action required to attain the objectives that the project was undertaken to achieve.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

3. **Executing** - processes performed to complete the work defined in the project management plan to satisfy the project specifications.

4. **Monitoring and Controlling** - processes required to track, review, and regulate the progress and performance of the project; identify any areas in which changes to the plan are required; and initiate the corresponding changes.

5. **Closing** - processes performed to finalize all activities across all phases to formally close the project or phase.

Project-Specific Risk & Mitigation Plan

The Project-Specific Risk & Mitigation Plan identifies potential risks across all project phases, including hardware delivery, CSOC facility setup, DDI and TippingPoint implementation, and overall project execution.

Each risk is assessed for its impact and likelihood, with corresponding mitigation strategies to minimize disruptions, ensure security, maintain timelines, and control costs.

Ownership is clearly assigned to relevant stakeholders, enabling proactive management and effective response to challenges throughout the project lifecycle. g

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

/ Phase	Risk Description	Impact	Likelihood	Mitigation Strategy	Owner
Hardware Components Delivery	Delay in procurement or shipping of critical hardware (servers, networking, storage etc).	High	Medium	• Confirm procurement timelines; • Track shipping closely.	Project Manager / Business Strategist
	Hardware incompatibility with existing systems or other components.	High	Medium	• Conduct compatibility checks in lab/test environment; • Maintain hardware specifications document; • Involve IT architecture team early.	Solutions Integration Team Engineers / Security Analysts
	Damage during transit or faulty units received.	Medium	Medium	• Inspect all deliveries on arrival; • Maintain vendor warranty agreements; • Keep spare components for critical hardware.	Solutions Integration Team Engineers / Security Analysts
CSOC Facility Setup	Delay in facility readiness (power, cooling, network, physical security).	High	Medium	• Pre-assess facility requirements; coordinate with facility team; • Schedule early setup; • Keep contingency plan for temporary facility access.	Project Manager / Solutions Integration Team Engineers
	Security breach during setup or unauthorized access.	High	Low	• Enforce access control; • Monitor facility; • Involve IT security during setup; restrict access to authorized personnel only.	Security Analysts
	Insufficient staff trained to operate CSOC.	Medium	Medium	• Schedule training sessions early; • Create operation manuals; • Assign backup operators.	Solutions Integration Team Engineers / Project Manager
	Network downtime during	High	Medium	• Implement phased deployment;	Security Analysts

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

DDI (DNS, DHCP, IPAM) Implementation	implementation affecting users.			• Schedule maintenance windows; • Notify users in advance; maintain rollback plan.	
	Misconfiguration causing service outages.	High	Medium	• Perform thorough testing in lab environment; use configuration checklists; • Peer-review all changes.	Security Analysts
	Integration issues with existing network/security systems.	High	Medium	• Conduct integration testing; • Involve all relevant system owners; • Document dependencies clearly.	Security Analysts
TippingPoint Deployment	Security solution failing to detect threats or false positives causing disruptions.	High	Medium	• Configure according to best practices; • Test in lab environment; • Monitor logs closely post-deployment; • Provide tuning and fine-tuning schedule.	Security Analysts
	Delays due to software licensing or vendor support issues.	Medium	Medium	• Confirm license availability and vendor support early; • Maintain backup security policies until solution is fully operational.	Security Analysts
	End-user or SOC staff not trained properly on TippingPoint alerts.	Medium	Medium	• Schedule training and simulation exercises; • Create SOPs for incident handling; • Assign dedicated trainers.	Security Analysts
Overall Project	Scope creep or additional requirements affecting timelines.	High	High	• Use PMBOK methodology • Obtain sign-offs at each milestone; • Maintain clear requirement documentation.	Project Manager

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

	Budget overrun due to unplanned costs (hardware, software, licensing, services).	High	Medium	• Track expenses • Ensure deliverables are within scope	Project Manager / Business Strategist
	Resource availability conflicts (team leaves, vendor delays).	Medium	Medium	• Maintain resource schedule; • Assign backups; p • Prioritize critical tasks; consider overtime if necessary.	Project Manager
	Regulatory/compliance issues for CSOC or network systems.	High	Low	• Ensure compliance review before deployment; • Involve compliance officer; • Schedule audits for high-risk areas.	Project Manager / Security Analysts / Solutions Integration Team

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Project Team Members

Radenta Technologies, Inc. Team Members

The Radenta Technologies project team is organized to ensure strategic oversight, operational execution, and effective governance. Key roles include the Steering Committee, Project Manager, Security Analysts, and Solutions Integration Engineers, collectively responsible for planning, implementation, monitoring, and successful delivery of all project objectives.

Role	Name	Scope
Steering Committee	• Denis Bermudez • Ma. Nathalie Rose Regala-Acebedo	- Provide Strategic Direction - Approve Major Decisions - Manage Risks and Escalations - Support Project Governance
Business Strategist	• Charlyn Dalusong-Elano	- Responsible for the commercial aspects of the project
Project Manager	• Mathew Dalisay	- Overall responsible for the project. - Coordinates with the project team - Handles the project documentation - Ensures the project meets the standards of the client.
Project Secretariat	• Jenikka Cathryn Siajuat	- Responsible for the project documentations.
Security Analysts	• Sergio Louie Paez • Jasper Amemita • Luis Miguel Makalinaw • Ivin James Medul • Allan Paul Aquino • Christian Clet Carlos Soria	- Continuous security monitoring & Firewall Monitoring - Threat detection and correlation - Security incident classification - Incident escalation - Proactive security monitoring - Reporting and documentation
Solutions Integration Team Engineers	• Francis Manuel Estrella • Jose Allen Framil • Michelle Espiritu • Niah Christle Villare	- Coordinate end-to-end implementation activities including planning, execution, and monitoring of CSOC facilities.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Development Bank of the Philippines (DBP) Team Members

The Development Bank of the Philippines project team is composed of dedicated representatives who play key roles in guiding the project toward successful completion.

DBP Representatives	
Jose Mari Bonto	Chief Technology Officer, Concurrent Head IT Security Department
Leandro Cabanilla	IT Security Department
Marie Ann Guillermo	Information Security Risk Management Department
Nica Madula	IT Security Department
Shanicka Minor	IT Security Department
Adriel Mayrina	IT Security Department
Alvin Regio	IT Security Department
Allan Brian Salvacion	IT Security Department
Patricia Roque	IT Operations Group
Robert Calimlim	Network Infrastructure Services Department
Mark Tan	Technology Innovations Group

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Responsibility Assignment Matrix (RAM)

The **RAM Matrix** defines the roles and responsibilities of both the client (DBP) and the contractor (Radenta) across all project activities. It delineates accountabilities for pre-implementation planning, logistics, site preparation, solution deployment, validation, knowledge transfer, security monitoring, and firewall management.

This serves as a guide to ensure clarity in ownership, promotes efficient collaboration, and facilitates smooth execution of project tasks while maintaining accountability for each key activity.

Activity / Tasks	**DBP** (Client)	**Radenta** (Contractor)
▪ Pre-Implementation and Planning	I	R, A
▪ Logistics (Hardware Delivery)	I	R, A
▪ Site Preparation	R, A, I	C, I
▪ Deployment and Configuration of Solutions	I	R, A
▪ Validation and Acceptance	R, I	R, A
▪ Knowledge Transfer and Project Closure	I	R, A
▪ Security Monitoring & Alerting	I	R, A
▪ Provide Security Recommendations	I	R, A
▪ Execution of Recommendation	R, A	C, I
▪ Firewall Access Provisioning/Authorization	R, A	I
▪ Firewall Policy Management/Changes	R, A	I

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Severity Level Classification

The Severity Level Classification defines the priority and response expectations for incidents based on their impact on services and security, in compliance with the Severity levels prescribed by the Development Bank of the Philippines (DBP). Incidents are categorized from **Critical (Level 1)** to **Low (Level 4)**, with corresponding acknowledgment and initial response times to ensure timely and appropriate handling. This framework enables the project team to effectively prioritize incidents, mitigate risks, and maintain operational continuity.

Severity Level		Description
1	**Critical**	Incident cause a complete loss of service or a major security breach that significantly impacts operations or data ▪ **Acknowledge within 15 mins.,** ▪ **Initial response within 30 mins.**
2	**High**	Incident results in significant service degradation or a major security threat with potential impact but does not halt operations ▪ **Acknowledge within 15 mins.,** ▪ **Initial response within 2 local business hours.**
3	**Medium**	Incident causes moderate impact, with limited-service disruption or a non-critical security vulnerability ▪ **Acknowledge within 15 mins.,** ▪ **Initial response within 4 local business hours.**
4	**Low**	Incident causes minimal impact, with a minor service disruption or a low-risk security concern ▪ **Acknowledge within 15 mins.,** ▪ **Initial response within 1 local business day.**

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Project Management Tools

To ensure effective coordination, clear communication, proper dissemination, and systematic management of project documentation, as well as continuous monitoring of project activities, the following tools will be used throughout the duration of the project:

- **Email (Office 365)** – Used for official correspondence, notifications, and updates between project stakeholders to ensure timely and documented communication.

- **Document Repository (OneDrive)** – Serves as a centralized repository for storing and sharing project documents, deliverables, and reference materials, providing secure and organized access for all authorized team members.

- **Project Management Tool (Asana)** – A dedicated platform for tracking tasks, milestones, timelines, and resource allocation. This tool facilitates monitoring of progress, identification of risks or issues, and reporting, enabling the team to maintain control over project execution and ensure alignment with the project objectives and Terms of Reference.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Communication Matrix & Guidelines

Documents	Stakeholder	Method	Frequency	Sender
Kick-off Material	All stakeholders	Kickoff meeting	Once	Project Manager (Radenta)
Status / Progress report	Project Team	Online meeting (Proposed)	Weekly	Project Manager (Radenta)
Minutes of the Meeting	Project Team	Email	48 Hours After each meeting	Project Manager (Radenta)
Implementation Technical Documentations	Project Team	Printed copy, Email	As needed	Project Manager (Radenta)

The Communication Matrix establishes a clear framework for information sharing among project stakeholders, defining the type of information, intended recipients, communication methods, frequency, and responsible sender.

Key communication / Project Documents may include: kick-off materials, weekly status and progress reports, meeting minutes, and implementation technical documentation. This ensures that all stakeholders remain informed, aligned, and able to respond promptly throughout the project lifecycle.

By providing these, we aim to provide transparency, accountability, and effective collaboration across the project team.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Activities	Guidelines
Meetings, presentations	• All meetings mut be arranged in advanced with the Project Secretariat • Meeting agenda and material must be distributed three days ahead of the meeting schedule. • Minutes of the meeting will be transmitted via e-mail within three working days after the meeting. • DBP and Radenta team must provide feedback within three working days upon receipt of meeting minutes; if no feedback is received, the minutes shall be deemed final.
Item Delivery	• Delivery receipts will be submitted to DBP together with a signed transmittal sheet.
Approvals	• All approvals must be in hardcopy, signed by respective approvers. • DBP and Radenta project teams will keep a copy of signed approval documents
Change request	• All change requests will be documented in a Change Request (CR) form. • Endorsement of CR form to Steering Committee will be through a transmittal sheet to be accepted by DBP Project Manager • A Project Steering Committee meeting will be set within three (3) working days from submission of CR Form to present, discuss and get decision about the Change Request. • Approved CR Form should be printed and signed by Steering Committee member/s for major activities • DBP and Radenta project teams will keep a copy of change request documents
Project decisions	• All project decisions will be recorded during the project duration; DBP and Radenta project teams will keep a decision log.

RADENTA TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Meetings & Reporting (SLA)

The project requires the submission of key documents that serve as the foundation for monitoring progress, validating deliverables, and ensuring alignment with the agreed scope of work.

Deliverable	Schedule
Weekly Reporting	Every Tuesday of the following week
Monthly Reporting	First (1st) week of the succeeding month
Quarterly Reporting	First (1st) week of the succeeding quarter

RADENTA
TECHNOLOGIES, INC.

U-2BC CBC Corporate Center
724 Shaw Blvd. Wack Wack
Mandaluyong City

(02)-85357801
info@radenta.com
www.radenta.com

Acceptance Criteria

The project shall be deemed successfully completed upon the satisfactory delivery and acceptance of the following key components. These deliverables collectively ensure that the project is carried out with structured planning, effective execution, and provision of knowledge transfer, in compliance with the Terms of Reference released for this project.

1. Work plan
2. Technology Deployment
3. Conduct of Managed Detection and Response plus Remediation Service
4. Status Reporting
5. Reports
6. Documentation and Training