Scope of Work  
1. Thorough Detection of Threats:  
 Identify threats throughout our entire IT setup, covering data centers, user systems, endpoints, and network infrastructure.

2. Advanced Threat Detection:  
Utilize advanced methods, such as machine learning and security analytics, to detect both known and previously unidentified threats.

3. Data Consolidation and Analysis:  
Consolidate data from different sources, including current security technologies, to extract practical insights.

4. Proactive Threat Hunting:  
Conduct daily proactive threat hunting activities to uncover potential threats that could be missed by traditional signature-based systems.

5. Swift Cyber Response:  
Ensure preparedness to respond rapidly to cyberattacks and security incidents.

6. Log Analysis and Correlation:  
Conduct thorough analysis and correlation of logs generated by all devices and solutions within the specified scope.

7. Continuous 24x7 Security Monitoring:  
Provide uninterrupted security monitoring operations

8. Automation of Security Processes:  
Implement automation to reduce resource usage and improve the speed of threat response.

9. Expert Staffing:  
Maintain a skilled and proficient team with expertise in various areas including event monitoring, incident detection and response, threat intelligence, use case engineering, threat hunting, and security analytics.

10. Alert Prioritization:  
Utilize automated real-time alert prioritization to correlate low-priority alerts with subsequent alerts, enabling the identification of multi-stage attacks.  
  
11. Remediation Efficiency:  
Enhance the efficiency of remediation efforts by automating data collection for investigations and facilitating quick analysis through a unified interface. Additionally, offer support for assisted remediation steps to accelerate threat mitigation.

12. Central Risk Dashboard:  
Provide a centralized dashboard for evaluating the organization's risk posture and maturity levels at any given time.  
  
13. Anomaly Detection:  
Employ a combination of rule-based methods and machine learning models to identify user anomalies.  
  
14. Network-Level Threat Detection:  
Incorporate capabilities for capturing netflow data to identify threats at the network level.

**Requirements for MDRaaS Proposal**

**Comprehensive Service Components:**

The Security Service Providers (SSPs) should include a variety of essential services, such as: Security monitoring Incident response, Security analytics, Proactive threat hunting, Threat intelligence (including indicators of compromise and different threat intel categories),SIEM engineering, Endpoint detection & response, User behavioral anomaly detection, Network threat detection.

**Monitoring Platform Proposal:**

Providers are encouraged to suggest monitoring platforms that meet the criteria set out in this Request for Proposal (RFP). These platforms should be able to provide the required functionality.

**SOC Improvement Recommendations:**

The chosen Service Provider should be able to create and make suggestions for improvements to the SOC. These suggestions should keep the SOC running efficiently and securely.

**Governance Model and Reviews:**

Service providers must establish effective and efficient governance models.This model should include periodic reviews, such as biweekly, monthly, quarterly, or annually, to ensure service level agreement (SLA) compliance and continuous improvement.

**SLAs and Implementation Planning:**

Specific SLAs and implementation schedules for various activities will be determined by mutual agreement at contract signing with the selected service provider.

However, service providers are expected to provide a comprehensive implementation and deployment plan as part of this proposal.

This plan should include templates for SLAs, project plans, governance meeting formats, and other related documents.

**Data Source Compatibility Requirement:**

Security providers inherently need to provide support for a wide range of data sources, totaling 500 or more. These sources should span various categories including, but not limited to, domain controllers, VPNs, firewalls (FWs), and web application firewalls (WAF)., intrusion prevention systems (IPS), intrusion detection systems (IDS), Windows and Linux servers, databases, and various network devices. This requirement highlights the need for solutions that seamlessly integrate with and collect data from numerous data sources across network environments.

**Integration and Data Format Support Requirement:**

• Security providers must be able to support multiple integration methods and data formats.

This includes the ability to work with REST APIs, Common Event Format (CEF), Syslog, JSON, ODBC/JDBC, and integrate into text files via log sources.

**Cloud Infrastructure and Multicloud Support Requirements:**

• Security providers must provide comprehensive support for cloud infrastructure.

Must be able to seamlessly integrate and provide security protections with a variety of cloud environments, including but not limited to Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. This requirement highlights the need for a well-equipped solution to protect data and assets across a variety of cloud environments and ensure the security of multicloud deployments.

**Cloud Asset Support Requirements:**

• Security service providers must have built-in support for a predefined list of standard cloud assets.

Additionally, for all other cloud assets not included in the standard list, the solution must be flexible and able to support custom configurations.

This requirement highlights the need for a solution that can easily handle standard cloud assets while adapting to custom cloud asset configurations as needed.

**Integration Options Requirements:**

• The security provider should offer multiple integration options with various databases such as MySQL, PostgreSQL, MS SQL, and Oracle.

Additionally, the solution should support seamless integration with web applications.

This requirement highlights the need for solutions that provide versatile and robust integration options across a variety of database platforms, web applications, and network components.

Traffic Logs, Active Directory, IAM, Application Gateways, WAF, Network Security Groups, Security Groups, Console Logs.

**Cloud SaaS Application Integration Requirements:**

• Security service providers must be able to seamlessly integrate with various cloud software, there is As-a-Service (SaaS) applications, including but not limited to Office 365 (O365), Salesforce, and more.

This requirement highlights the need to efficiently integrate cloud-based SaaS applications and solutions to ensure comprehensive coverage across multiple platforms.

**Web Interface Requirements for a Single View of Assets:**

• Security service providers need a web-based interface that provides a single view of all integrated assets across various environments, including data centers, cloud infrastructure, and cloud SaaS applications.

This requirement highlights the need for an easy-to-use web interface that enables integrated monitoring and management of assets across various IT environments.

**Security Monitoring Requirements Security Log Monitoring and Alerting Requirements:**

• Security service providers are expected to continuously monitor security logs to identify malicious or anomalous events.Additionally, providers must immediately generate alerts for suspicious events that could lead to security breaches.This requirement emphasizes the important role of providers in proactive security monitoring, alert generation, and threat detection to prevent security breaches.

**SIEM module use case requirements:**

• The SIEM module must provide a library of over 500 ready-to-use use cases.

This requirement highlights the need for a SIEM module that provides comprehensive predefined use cases for effective monitoring and analysis of security events.

**Requirement** **to** **provide** **protocol** **baselines:**

Security providers are expected to provide protocol baselines for all platforms within a defined scope that require monitoring.This requirement emphasizes the obligation of providers to create and provide baseline protocols for monitored platforms to ensure a standardized reference for analyzing security events.

**Comprehensive attack detection requirements:**

Security providers must be able to detect and respond to both internal and external security attacks.This includes monitoring security events across IT infrastructure, not just events related to databases and servers.This requirement emphasizes the need for providers to provide comprehensive security monitoring to cover a wide range of assets within the IT environment and to detect and mitigate both internal and external attacks.

**Database Security Event Monitoring Requirements:**

Security providers must monitor, detect, and manage incidents related to minimal database security events.

The list provided is illustrative and not exhaustive.

Vendors are expected to provide a list of events as part of their bid response.

Minimum events include, but are not limited to:

1. Monitor access to sensitive data
2. Record database access details such as login, client IP address, server IP address, and source program information.
3. Track and monitor administrative commands executed within the database.

This requirement specifies the need to proactively monitor and manage security incidents related to core database activity while providing flexibility for providers to suggest additional events based on their expertise and capabilities.

**Multi-vector** **attack** **detection** **requirements:**

Security service providers must perform log correlation between logs generated from multiple sources to effectively identify and detect multi-vector attacks.

This requirement emphasizes the role of vendors in correlating logs from different sources to detect complex multi-vector attacks and improve threat detection capabilities.

**Alert and Mitigation Notification Requests:**

• Security service provider operations teams are expected to send alerts to appropriate personnel and provide comprehensive details of mitigations.

This communication must also include all identified Unibank service providers.This requirement emphasizes the provider's obligation to promptly notify certain individuals, and where applicable, he Unibank's service provider, of useful warnings and mitigation instructions in the event of a security incident.

**Automating Incident Response Activities Requirement:**

Security service providers must employ workflows and solutions that can automate key parts of incident response activities.

• This automation should include tasks such as managing false positives, handling whitelists, implementing escalation workflows, and managing service level agreements (SLAs), among other related activities.This requirement emphasizes the need for bidders to provide automation capabilities that streamline the incident response process and improve efficiency and effectiveness in managing various tasks.

**Alerts and Extension Requests:**

Alerts should only be sent to Unibank after a thorough triage process.

Alerts generated by the SIEM must be enriched with relevant contextual data, environmental data, vulnerability information, historical data, threat information, and other relevant details before being forwarded to Unibank.This requirement emphasizes the importance of a well-defined alert triage process and the need to provide Unibank with enriched alert information by incorporating various contextual elements to support informed decision-making.

**Including Historical Parameters in Alerts Requirements:**

• Alerts must include historical parameters including, but not limited to, attack volume, attacker volume, and target volume for each alert.This requirement emphasizes the need for alerts to provide historical context by incorporating specific parameters such as attack volume, attacker data, and target information to better understand security incidents.

**Requirements** **for** **long-term** **threat** **protection** **solutions:**

• Security service providers are expected to present durable solutions that proactively and long-term mitigate and prevent future threats.

This requirement emphasizes the need for bidders to propose sustainable and future-oriented solutions aimed at preventing future security threats.

**Use Case Definition and Implementation Requirements:**

• Selected entities must define, develop, and execute use cases according to established methodologies such as Cyber ​​Kill Chain.

This requirement emphasizes the need for organizations to build and implement use cases using recognized methodologies, specifically the cyber kill chain, to improve their threat detection and response capabilities.

**Protocol Integration from Non-Standard Sources Requirements:**

• Service providers must be able to seamlessly integrate protocols from non-standard applications and devices.

Additionally, the service provider's platform must be able to process these logs to effectively generate alerts and reports.

This requirement emphasizes the obligation of service providers to process logs from a variety of nonstandard sources and ensure that they can be used to generate alerts and reports.

**Incident Analysis Centralized Security Incident Management Support Request:**

• Security service providers must be able to enable centralized incident management that allows security incidents to be prioritized and effectively managed.This requirement highlights the need for a solution that provides the ability to centralize and efficiently manage security incidents to ensure that incidents are appropriately prioritized and handled.

**Alarm triage support for multiple security products Requirement:**

• Security service providers must be able to triage alarms originating from a variety of security products, including but not limited to SIEM, DLP (data loss prevention), IPS (Intrusion Prevention System), WAF (Web Application Firewall), Anti-APT (Advanced Persistent Threat), and ETDR (Endpoint Threat Detection and Response).

**Machine Triage and Alert Prioritization Requirements:**

• Security service providers can use machine-driven triage algorithms that take into account contextual parameters, past behavior, and external threat information to generate real-time triage scores.You need to be able to power it up and set alerts.These triage scores should serve as the basis for prioritizing alerts and determining further actions.

• Environmental parameters such as, but not limited to, asset criticality, user criticality, and vulnerability status of each alert should be considered.

• Historical parameters should also be considered, including but not limited to attack volume, attacker volume, target volume, alert severity, and other relevant factors.

• Additionally, a centralized threat intelligence feed should be deployed to identify threats related to known malicious actors.

This requirement calls for a solution that employs sophisticated algorithms to effectively triage alerts, taking into account a wide range of parameters to prioritize incidents and guide subsequent actions for efficient incident response.

**Custom Triage Rules Engine Support Request:**

• Security service providers require a rules engine that allows users to define custom triage rules.

This rules engine should provide flexibility by supporting a variety of data fields such as asset data fields, event data fields, user data fields, triage scores, and triage parameters.This requirement highlights the need for a solution that provides an easy-to-use rules engine that enables the creation of custom priority rules, leveraging various data fields for rule definition and customization to meet specific security requirements.

**Requirements** **for** **enabling** **alert** **investigation:**

• Security providers must provide users with the ability to investigate both classified alerts and custom alerts identified as critical.This requirement highlights the need for solutions that provide the tools and functionality necessary to enable users to effectively investigate alerts, especially those identified as critical, thereby The response process will be improved.

**Investigation module integration and data analysis requirements:**

• The investigation module seamlessly integrates with log sources such as SIEM, ETDR, EPP, and Data Lake to enable retrieval of data related to the alerts being investigated.

Additionally, the module should include the ability to generate charts and graphs to facilitate data analysis.This requirement emphasizes the need for the investigation engine to be properly connected to relevant log sources so that users can retrieve data for further analysis.

**Impact Analysis Feature Requirement:**

* The Security Service Provider should be equipped with features for conducting a comprehensive analysis of the impact of an attack on the targeted asset. This analysis should encompass aspects such as configurations, Indicators of Compromise (IOCs), external network connections, and additional relevant factors.This requirement underscores the need for the solution to provide tools and capabilities for thoroughly assessing the consequences of an attack on the affected asset, considering a range of critical factors.

**Attacker Attribute Identification Feature Requirement:**

* The Security Service Provider should offer features that enable the identification of attacker attributes, consolidating essential information such as the threat intelligence score of the attacker, WHOIS lookup details, and geo-mapping, all accessible through a single, unified console.

This requirement underscores the need for the solution to provide a comprehensive set of tools and functionalities for promptly identifying various attributes of attackers, facilitating efficient incident response and threat assessment.

**Attack Chain Modeling Support Requirement:**

* The Security Service Provider should offer capabilities for constructing models that depict the entire attack chain, covering the attack's initiation, progression within the network, and its spread.This requirement underscores the need for the solution to provide tools and features that enable the creation of comprehensive attack chain models, facilitating a holistic understanding of the attack's development and propagation within the network.

**Investigation Run Books for Attack Inception and Progress Requirement:**

* The Security Service Provider should include run books that outline investigation steps tailored to different types of attacks. These run books should aid in the identification of attack inception, the analysis of attack progression, and the determination of crucial factors, including Patient Zero, Attack origin, and Blast Radius.This requirement emphasizes the need for the solution to offer comprehensive run books that guide users through the investigation process, helping them understand when and how an attack began, its evolution, and the associated impact on the network.

**Attack Inception and Progress Models Requirement:**

* The Security Service Provider should provide support for models that assist in deriving the attack's initiation and its development over time. Furthermore, the solution should furnish a comprehensive list of the investigation models employed within the system.This requirement underscores the need for the solution to offer models that aid in understanding the attack's starting point and how it evolves, as well as providing transparency by listing the investigation models in use, promoting effective incident response and threat assessment.

**Case Management and Artifact Storage Requirement:**

* The Security Service Provider should encompass case management features that enable the storage of raw and analyzed data associated with a particular alert or a collection of alerts. Additionally, the requirement seeks information regarding the specific artifacts that can be preserved in connection with an investigation.This requirement emphasizes the need for the solution to offer robust case management capabilities, allowing for the retention of pertinent data in various forms related to specific alerts or investigations, contributing to comprehensive incident documentation and analysis.

**Quick Search and Supported Search Features Requirement:**

* The Security Service Provider should include functionality for rapid searches across stored datasets. Additionally, the requirement seeks information on the specific search features that are supported by the solution.This requirement underscores the need for the solution to facilitate quick and efficient searches across the stored datasets, while also specifying the types of search features available, contributing to effective data retrieval and analysis.

**Investigation Run Books Requirement:**

* The Security Service Provider should offer run books that outline investigation steps tailored to different types of attacks.This requirement highlights the need for the solution to provide comprehensive run books that guide users through the investigation process, assisting in responding to and mitigating various types of attacks effectively.

**Incident Response**

**Rapid Counter Response Integration Requirement:**

* The Security Service Provider should have the capability to swiftly initiate counter responses by integrating with devices like firewalls, WAF, and Active Directory. These counter responses should encompass actions such as traffic blocking and system quarantine.This requirement underscores the need for the solution to enable rapid and effective counter responses through seamless integration with relevant devices, enhancing the organization's ability to mitigate threats promptly and enhance overall security posture.

**Integration with EDR for Endpoint Containment Requirement:**

* The Security Service Provider should possess the capability to seamlessly integrate with EDR solutions, enabling the execution of containment actions on endpoints. These actions may include terminating malicious processes and isolating the affected endpoint.This requirement highlights the need for the solution to facilitate integration with EDR solutions, allowing for swift and effective containment actions on endpoints in response to security incidents, bolstering the organization's ability to mitigate threats and protect its assets.

**Edge-Based Incident Containment Module Requirement:**

* The incident containment module should be designed with an edge architecture, ensuring that response actions are executed by a local response engine. This architecture should prevent open access to the Unibank environment via a cloud-based system.This requirement underscores the need for the incident containment module to have an edge-based architecture, enhancing security by ensuring that response actions are conducted locally and not through a cloud-based system with open access to the Unibank environment.

**Incident Workflow Support Requirement:**

* The Security Service Provider should provide comprehensive support for the complete incident workflow, encompassing incident classification, incident coordination, task assignment to diverse teams, tracking for closure, task escalation, and the handling of exception approvals.This requirement emphasizes the need for the solution to offer robust capabilities for managing the entire workflow associated with incident handling, including task delegation, tracking, escalation, and approvals, facilitating effective incident response and resolution.

**Activity Assignment and Closure Tracking Requirement:**

* The Security Service Provider should include features that enable the assignment of activities to various teams and the subsequent tracking of these activities until they are successfully closed.This requirement highlights the need for the solution to provide capabilities for efficiently assigning tasks and activities to different teams within the organization and maintaining oversight through the tracking of these activities until they are satisfactorily completed.

**Auto Mitigation Approval Workflow Requirement:**

* The Security Service Provider should have the capacity to accommodate the workflow essential for approving auto mitigation actions. Additionally, it should provide the flexibility to exempt particular auto mitigation actions from the approval process.This requirement underscores the need for the solution to facilitate a structured workflow for approving auto mitigation actions while also allowing for exceptions where certain auto mitigations may be exempted from the approval process when deemed appropriate.

**Escalation Workflow Support Requirement:**

* The Security Service Provider should offer features for managing escalation workflows, complete with an escalation matrix that defines different levels of escalation. The escalation mediums, such as IM, telephone calls and email, should be clearly specified within the solution.This requirement highlights the need for the solution to provide tools for implementing and managing escalation workflows, with a defined matrix that outlines various escalation levels and the communication mediums, like IM, telephone calls and email, used for the escalation process.

**Security Exception Approval Tracking Requirement:**

* The Security Service Provider should include capabilities for monitoring and recording security exception approvals. This should apply to situations where remediation is not achievable or where compensating controls have been implemented.This requirement emphasizes the need for the solution to facilitate the monitoring and documentation of security exception approvals, particularly in cases where traditional remediation is not possible, and alternative compensating controls have been deployed to address security threats and incidents.

**Integration with External Service Desks Requirement:**

* The Security Service Provider should have the capability to seamlessly integrate with external service desks, including platforms such as Jira (etc.). This integration is essential for harnessing the functionality of existing service desk platforms.This requirement emphasizes the need for the solution to support integration with external service desks like Jira (etc.), allowing organizations to leverage their existing service desk platforms for enhanced incident and ticket management.

**Alert and Investigation Outcome Integration Requirement:**

* The Security Service Provider should offer the capability to link alert details and investigation outcomes, making them accessible and visible within the context of relevant remediation tickets.

**Comprehensive Incident Report Requirement:**

* The incident report should be comprehensive and include essential elements such as incident classification, a detailed chronology of events, Root Cause Analysis (RCA), and the identification of Indicators of Compromise (IOC).

This requirement emphasizes the need for the incident report to provide a thorough account of the incident, covering incident classification, a timeline of events, a root cause analysis, and the identification of potential indicators of compromise (IOC), ensuring a detailed record of the incident for analysis and remediation.

* Track impacted assets related to an incident
* Tools for Response based on data and analytics
* Usage of Ticketing and case management workflow
* Classification of incidents
* Maintain track of first response and subsequent measures taken for the incident
* Maintain IOC and artifacts related to incident
* Incident response should include investigation of end points if required to conclude the investigation
* Centralized incident management to prioritize and manage security incidents
* The Security Service Provider should bring a platform which facilitates collaboration between SOC and Unibank with features comments on incidents, maintaining a history of conversation with time line, ability to add artifacts
* The Security Service Provider should provide unlimited remote support for incident response for activities such as malware reverse engineering, log forensics, remediation support, end point forensics etc.

**Threat Hunting Requirements**

* Use algorithms and tools to actively hunt of attacks in large volume of data and create alerts that are passed on to analysts. Supports use of Big data platform for collection and analysis
* Define, develop, implement, update and maintain Hunting Framework which contains:

a. Create Strategic Hunt Missions which are objective based to identify malicious activity that has not triggered an alert

b. Search for Indicators of Compromise received from Threat Intelligence and Analytics

* Create knowledge base of IOCs
* The Security Service Provider should provide security analytics as a service to able to detect unknown attacks
* The analytics service should have models that are able to detect attacks in various stages of a cyber kill chain

The analytics service should able to detect threats from various attacks vectors such as malware, web application attacks, network attacks, watering hole attacks, DNS attacks, insider threat, and data exfiltration. List the detection use cases which can detect above attacks using pre-built machine learning techniques and analytical models.

Analytics using machine learning techniques should use multiple sources to identify malicious activity. A minimum the following sources should be used:

• Netflow

• IPS/IDS

• Proxy

• WAF

• Windows logs

• DNS

• O365

• Cloud infra such as FWs, workloads etc

* The Security Service Provider should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors).
* The Security Service Provider should have analytical models to detect different stages of Cyber Kill chain.
* Network Threat Hunting should leverage existing network sources for better detection of advanced attacks. Network sources should include Netflow, Proxy, DNS, IPS, VPN, Firewall, AD/Windows, Email logs
* Network threat hunting should use AI on network sources and enable hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks
* The service must be capable of identifying suspicious or hitherto undiscovered communication patterns. The service must support detection of newly discovered pattern in future
* The service should identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).
* Monitor malicious activity within the system that could indicate the lateral movement of threats within the environment
* The Security Service Provider should proactively monitor assets for evolving threats. These evolving threats could be using known threat vectors or new threat vectors that are still unknown and undocumented. The Security Service Provider must continuously analyze and discover any of the following or a combination of these and provide reports on an ongoing basis:
* Zero-day threats
* Known Threats
* Social Engineering Attempts

A combination of the above.

**User Behavior Analysis**

* The Security Service Provider should provide UBA dashboard based on various UBA models outcome.
* UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behavior anomalies of the user
* Organization should be able to define risk thresholds based on their risk appetite
* Detect malicious/illegal activities performed by users
* The Security Service Provider to have capabilities to collect user data from variety of sources like Directory Services , IAM, VPN, Proxy,O365, etc.
* Service should be able to track user‘s activities locally and remote network sites and should be able to report usage behavior across the entire network
* The service should incorporate multiple baseline behavioral models which cover behavioral risk categories like Data Exfiltration, Malicious Users, Illicit Behavior, compromised credentials, etc.
* MSSP should be able to search proactively and iteratively through a network or logs data to detect and isolate advanced threats that evade Signature based systems (SIEM, IDS, DLP etc.)
* Service provider should submit a daily threat hunting based on the threat hunting models deployed at the organization

**Threat Intelligence**

* Service should anticipate likely threats to the Organization based on global threat events and data and provide proactive measures to prevent such happenings in the Organization
* Service should support integration of machine readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds
* Service should provide strategic threat intelligence about incidents and breaches happening across the global and provide actionable intelligence such as Can Unibank be susceptible to such an attack? Is yes, which assets in the organization are susceptible?
* Provide IoC’s where relevant Provide mitigation steps for each advisory
* Service should apply the threat intelligence to Organization assets, network traffic, security event and users to provide actionable report on likely impact on each entity and recommend pre emptive measures
* Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk reduction
* Service should have machine algorithms to auto-evaluate an asset and assign a business value to the asset
* MSSP should support STIX/TAXII for automated integration of actionable intelligence with security technologies.
* Service should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in SIEM and other sources of security information

**General Requirements**

Service provider team should have the following skills:

• Security analysts

• Incident investigator

• Threat hunter

• Data scientists

• Threat intelligence analytics

• Incident responders

• Specialized security team for IOC collection, deeper analysis, forensic investigation

The MSSP should have machine learning capabilities and other advanced analytics of structured as well as unstructured security & network data

The MSSP should have a unified console to view outcomes of all the above-mentioned solutions – Threat intelligence, threat hunting, SIEM alerts, incident analysis, incident response EDR, UBA, security orchestration etc.

The MSSP should have an executive dashboard to review the overall security posture of the organization and an operational dashboard for reviewing daily operational metrics.

**Service Levels**

**Platform Availability and Notification SLA**

The Security Service Provider to provide access to their platform and associated notification systems. SLA for Platform availability will be measured by the below formula

(Number of minutes in the month system is available) \*100 / (Total number of minutes in the month)

* + SLA Target metric – 99.9%

**SLA – Tim to Notify a Security Alert**

Upon The Security Service Provider detecting & prioritizing an alert, the SOC will evaluate and notify us, if it is judged as relevant and critical threat

The SLA timeframe for reporting such events is 15/30 minutes from alert detection in platform. Critical/High events in 15/30 minutes from alert detection on platform.

SLA for Alert Notification will be measured by the below formula :

(Number of Critical/High alerts notified after 15/30 minutes in a month) \* 100/(Total number of critical alerts notified in a month)

* + SLA Target metric – 98%

**SLA – Time to Investigate and provide Incident details**

Upon SOC determining a threat or likely to cause an incident, or Unibank reporting a likely incident, SOC will investigate and provide Incident details with actions to remediate.

The SLA timeframe for Incident details is 60 minutes from alert detection in the platform or from the time Unibank report an incident

SLA for Investigation & Incident details will be measured by the below formula :

(Number of times Incident investigated & reported after 60 minutes in a month) \*/ (Total number of Incidents investigated & reported in a month)

* + SLA Target metric – 98%

**Executive Summary Report**

Executive report will be delivered monthly and having all high-level summary information for the corresponding period

* + SLA Target metric – 100%

**Certification of company employees in this area with the certifications described below is welcomed and may not be limited.**

CCNA, CRTO, BTL1, OSCP, CRTO, eCTHP, RHCSA, ECC-CTIA, eCDFP, eCIR, eWTP

**Key parameters will be taken into account when evaluating proposals. These include links to similar projects, certification of both employees and the company (if any) in the field of information security, the number of qualified employees allocated to each SOC level (L1, L-2, L-3), price offer. The information provided on these aspects will play a key role in the selection of the winning candidate.**