Unisys Managed Security Services (MSS)

Service Descriptions and Cost
GTA GETS Ready Contract

MSS Monitoring
MSS SDM for Firewalls
MSS SDM for IDS/IPS
MSS Vulnerability Management
MSS Stealth
Other MSS Services - TBD

Wednesday, November 22, 2017

Copyright © 2017 Unisys Corporation. All Rights Reserved.
Unisys Confidential

Table of Contents

UNISYS MANAGED SECURITY SERVICES (MSS) 3

1. UNISYS SECURITY MONITORING SERVICE 4

Log Retention and Log Management Service 4
Cyber Threat Intelligence 4
Advanced Security Analytics 5
Incident Response and Orchestration 5
MSS Monitoring Service Cost 6

2. UNISYS SECURITY DEVICE MANAGEMENT (SDM) 7

Security Device Management Services 7
Device Management Activity Summary 7
Architecture of Security Device Management service 8
SDM Services Cost - Firewall 10
SDM Services Cost – Intrusion Detection/Prevention Systems (IDS/IPS) 10

3. UNISYS MSS CLOUD BASED VULNERABILITY SCANNING & REMEDIATION SUPPORT SERVICE 11

Vulnerability Management Services 11
Remediation Support 12
Additional Steps of Remediation Process 12
Vulnerability Management Service Cost 13

4. UNISYS STEALTH® MSS 14

Stealth Service Description 14
Stealth MSS Cost 14

5. ADDITIONAL UNISYS MANAGED SECURITY SERVICES 15

Cloud Security 15
IAM 15
GRC 15

This document is designed to provide the State of Georgia Entity ("Client") detail behind the Unisys Services that are listed on the GETS Ready Contract.

Unisys Managed Security Services (MSS)

As businesses extend their IT organizations into clouds and virtual environments to drive down IT costs, many find substantial challenges in the form of advanced security threats, while at the same time maintaining compliance and assessing the overall security risk. Protection of information distributed throughout the enterprise requires a holistic, comprehensive and integrated security strategy – one that includes solutions for protecting IT assets, securing cloud applications, mobile devices and safeguarding intellectual property.

The Managed Security Services (MSS) division of Unisys will provide the Client best-in-class support from Augusta, GA. With years of experience in the field, Unisys provides direct access to subject matter experts in various word-class security technologies and well-tuned processes that help businesses. Besides providing some of the best security services, the Unisys MSS also provides traditional remote device management of security devices.

Unisys Managed Security Services deliver comprehensive real-time protection solutions – Security Information and Event Management (SIEM), Security Device Management (SDM), Vulnerability Management (VMS), Stealth Services, as well as Governance Risk & Compliance (GRC), Managed Identity and Access Management Services (IAM) and Cloud Services, helping organizations to manage overall risk, improve their security posture, prevent emerging threats and demonstrate compliance in a cost-effective manner.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

1. Unisys Security Monitoring Service

Unisys Security Information and Event Management (SIEM) Services delivers comprehensive cross enterprise protection by unifying event management and incidents management across towers on a common platform.

Unisys SIEM service incorporates Unisys Noise Cancellation Advanced Analytics Platform (UNCAAP) technology, developed over many years to identify events of interest arising from the ever-evolving threat landscape. It provides the essential feedback loop to senior management on the performance and cost effectiveness of their IT Security program. UNCAAP minimizes false alarm rates and offers advanced forensics & analytics including actionable intelligence, decision support and aids in executing our clients' security strategies.

The Security Event Management Service provides the following functionality:

Log Retention and Log Management Service

Log Retention and Log Management Service provides Log Collection and retention, information searches, reporting, alerting and real-time information displayed via dashboards, to meet specific compliance requirements. The service consists of:

1. Log Collection - Collecting security event data, log and machine data and forensic sensor data (host and network).
2. Log Storage, retention and archival policies –
   - Online raw data: 14 days active data and 351 days archive storage
   - Metadata: Logs are stored for one year.
   - Archive storage: Logs are stored for one year.
3. Log Search - Provide a dedicated Web Console to allow clients to perform forensic searches against all their log data.
4. Log Reporting - Provide out of the box or custom reports. The SIEM platform currently has over 1250 pre-defined reports plus 170 additional templates that can be used to create an unlimited number of reports automatically. The reports provide Auditing, Security and Operations summaries, details, "most frequent/most used" lists, and specific reports for compliance.

Cyber Threat Intelligence

Security is only as effective as the security intelligence it is based on. Overcoming zero-day security challenges requires security intelligence from a number of trusted threat sources focused on a multitude of threat vectors. To meet these requirements, Unisys has combined multiple key SIEM ingredients powered by LogRhythm technologies into a Security Monitoring offering. This allows Unisys to offer a cost effective SIEM Solution, including the benefits of our Threat Intelligence and Advances Security Analytics to a broader base of customers.

Unisys provides Threat Intelligence Services in accordance with our policies and standards. Unisys delivers Threat Intelligence Services utilizing intelligence gathering sources and actionable intelligence designed to assist with highly valuable decision-making and operational analysis.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

Advanced Security Analytics

Unisys Advanced Security Analytics analyzes data and assess the threats to determine the risks and if a full investigation is necessary. In coordination with Cyber Threat Intelligence, Unisys uses Advanced Analytics to analyze Client security events from Client Devices for security threats to the Client IT Infrastructure using Unisys baseline security policy to aggregate and correlate security events for in-scope Devices into actionable events.

Incident Response and Orchestration

Unisys takes the market leading and proven LogRhythm technology and integrate our Threat Intelligence and Advanced Security Analytics and couple them with our Incident Response and Orchestration processes to offer a robust all-around solution for our clients, all in one package.

Unisys believes that Threat Intelligence Services are required to ensure that the security services provide are based on the most comprehensive, accurate, and actionable intelligence available. This includes the insight gained from integrating SIEM with the best threat intelligence feeds available.

The service consists of:

1. Security Incidents Investigation – Incidents categorized as requiring further investigation are analyzed in more depth. Unisys hunts for Indicators of Compromise (IoC), analyze the threat and determine the nature and extent of the incident.
2. Security Incident Response – Unisys will notify the Client of the incident and provide associated information relating to how to mitigate the threat and associated risk by implementing suitable countermeasures. Where possible and appropriate, those countermeasures are platform, with appropriate levels of authorization, utilizing integration with other technologies such as NAC, Firewalls, AD and Unisys Stealth® to quarantine devices, block traffic or disable user accounts.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

MSS Monitoring Service Cost

Monitoring Packages (per year) - US Based Resource						
MPS Volume	**(S) 100-250**	**(P1) 250-500**	**(P2) 501-750**	**(P3) 751-1000**	**(P4) 1001-1250**	**(P5) 1251-1500**
Total Package Price per Year	**$57,554**	**$90,681**	**$116,968**	**$146,162**	**$174,595**	**$200,544**
Packages Include						
Labor Source	100% On-Shore (US based)					
Log Archive Storage per Year	75GB	250GB	400 GB	500 GB	750 GB	1 TB
Standard Reports:	5	5	5	5	5	5
• *Customer may select from standard available LogRhythm reports*						
• *1 compliance pack*						
Monitoring Agents	Pro Agents – 1 Lite Agents – 2	Pro Agents – 2 Lite Agents – 3	Pro Agents – 3 Lite Agents – 4	Pro Agents – 5 Lite Agents – 6	Pro Agents – 5 Lite Agents – 9	Pro Agents – 6 Lite Agents – 10
Restrictions						
Datacenters	Up to 2 Client Sites					
Average Number of Incidents per Month	3	10	15	20	25	30
One-Time Price for Additional Compliance Packs (up to two max)	Not Available	$50	$100	$150	$200	$250

*MPS Volumes above 1500 will require a custom quote

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

2. Unisys Security Device Management (SDM)

The Security Device Management service provided by Unisys covers the following device types.

- Firewall devices
- IPS devices
- IDS devices
- IDS devices
- UTM devices
- VPN appliances
- Web proxy appliances
- Load balancer appliances.

These devices are accessed and managed remotely over a dedicated management network. Depending on the device, management is performed via a purpose-build management station (e.g., Provider-1 for Checkpoint) or via a dedicated Terminal Server, located on a client site or in a Unisys SOC, using HTTPS or SSH for secure communications. Connectivity between a client's site and the Unisys SOC is provided via a secure Site-to-Site VPN over IPsec or MPLS.

Security Device Management Services

The Unisys Service Device Management (SDM) services consist of:

- Centralized and Remotely Managed Security Device Management Services
  - Incident and Change Management Services
  - Configuration Management Services
  - Problem Management Services
  - Knowledge Management Services
  - Vendor Management Services
- Reporting Services

Security device management includes system monitoring of a device, including availability and system health.

Device Management Activity Summary

Exhibit 1 shows a Security Device Management Activity Example.

Activity	Sub-tasks
Incident Management	Device up/down status updates Interface up/down status updates
Change Management	Modify system settings Modify system policy Modify other device configuration Perform content updates Perform firmware/OS updates

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

	Perform user access management activities
Configuration Management	Define configuration item Identify and register configuration item (CI) Perform CI Audits Configuration Management Database (CMDB) change control
Problem Management	Identify problem or recurring incidents Perform root cause analysis If problem identified with Unisys managed device, work towards giving a permanent fix to the problem with vendor support
Knowledge Management	Maintain knowledge base
Vendor Management	Track and update support contracts Work with vendor to get bug fixes Escalate issues to vendors and follow up until a fix has been found

Exhibit 1. Device Management Activity Summary Example

Architecture of Security Device Management service

The following section provides the high-level architecture of security device management service. This section focuses on the various components used to provide the security device management service and summarizes their functions.

Security Device Management Component	Description
Managed Device	Any of the supported security devices that are serving client infrastructure and are under sole management of Unisys. The list of supported device types is given in the previous section.
Management Station	The Palo Alto Panorama Management server, used to manage one or more managed devices over an in band management connection.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

In band management	This is a process of managing a managed device using management station over a regular WAN connection, such as IPsec/Internet or MPLS VPN.
Unisys Security Operations Center (USOC)	This secure location houses Unisys security engineers and analysts, the management stations and portal servers used to provide the service over an in band or out of band management access connection,

The Parties' detailed responsibilities are set forth in a Joint Responsibility Matrix (JRM) document provided to the Client.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

SDM Services Cost - Firewall

Security Device Management (SDM) Firewall Packages One-Time Set-up Cost		
SDM Firewall Packages	New Firewalls	Existing Firewall Takeover
Small (1 -150 rules)	$ 5,357	$ 1,902
Medium (151-350 rules)	$ 5,556	$ 2,101
Large (>350 rules)	$ 6,264	$ 2,808

SDM Firewall Packages (US based resources) On-Going Support			
Description		Price per Month	Price per Year
Small (1 -150 rules)	2 Changes per Month	$ 1,761	$ 23,033
Medium (151-350 rules)	5 Changes per Month	$ 3,829	$ 48,045
Large (>350 rules)	8 Changes per Month	$ 6,138	$ 76,462
	Price per Additional Change per Month	$ 566	$ 6,796

SDM Services Cost – Intrusion Detection/Prevention Systems (IDS/IPS)

Security Device Management (SDM) IDS/IPS Packages One-Time Set-up Cost		
SDM IDS/IPS Packages	New IDS/IPS Set-up	Existing IDS/IPS Takeover
Small (3 Changes/Month)	$ 4,871	$ 1,415
Medium (10 Changes/Month)	$ 5,092	$ 1,636
Large (18 Changes/Month)	$ 5,191	$ 1,736

SDM IDS/IPS Packages (US based resources) On-Going Support		
Description	Price per Month	Price per Year
Small (3 Changes/Month)	$ 1,791	$ 21,489
Medium (10 Changes/Month)	$ 4,977	$ 59,729
Large (18 Changes/Month)	$ 8,785	$ 105,419
Price per Additional Change/Month	$ 441	$ 5,293

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

3. Unisys MSS Cloud Based Vulnerability Scanning & Remediation Support Service

Unisys Cloud-Based Vulnerability Management Service will permit the Client to assess their server and infrastructure scanned devices for known vulnerabilities. These scanned devices can be either in the cloud or in the Client data centers.

Features:

- Supports Risk Management process
- Ensures compliance
- Custom fit/tailor made solution
- Agnostic in terms of vulnerability scanning tool
- Infrastructure – market leading tools such as Qualys, McAfee, Nessus and/or any other.
- Remote service components may be connected to client infrastructure in a Stealth®-enabled link
- Utilize combination of remote scanning and cloud based agents to meet specific requirements.
- Service options allow "one-off testing" or an annual subscription.

Scanning Activities:

- Define scanning requirements.
- Define technical requirements
- Execution of scans
- Reporting

Remediation support and coordination activities:

- Preparation of scan environment (Pre-Scan)
- Completion of preparation of Scan environment (Post Scan)
- Review of report by Unisys Security Officer
- Raise Incidents and Changes based on recommendations
- Incidents and Change closure tracking
- On-Demand Scanning and SAML Integration.

Vulnerability Management Services

Unisys will provide remote monitoring and management services for three (3) Qualys virtual scanner appliances. During each scan Unisys will follow a vulnerability management lifecycle which consists of the following phases:

1. Define scanning requirements. A discovery will be carried out to provide a list of devices to be scanned. The following will be identified during this scan-scoping activity:
   - Asset identification
   - Asset prioritization
   - Asset changes
   - Vulnerability assessment
   - Vulnerability prioritization

2. Define technical requirements
   - Vulnerability scanning requirements
   - Unisys personnel that require access IDs

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

3. Network connectivity or limitations – to be reviewed with the Client
   - Execution of scans

4. Execute scans using the Qualys tool
   - Reporting

Unisys Security Officer will review the automated scan reports generated by the Qualys tool, prioritize the vulnerabilities, and provide vulnerability scan reports to the Client as set forth in Section 8 (Reports).

Remediation Support

1. Preparation of scan environment: before running a scan, the Unisys Project Manager will open a "Preparation of Scan Environment" Change Request in the Client IMS system to handle to flowing activities.
   - Open firewall ports
   - Prepare network changes for required scan environment readiness
   - Provide network data to the Client for VPN to their three (3) data centers
   - Provide the network access to Unisys

2. The Change Request will be kept open until the scan is completed.
3. Completion of preparation of scan environment: Unisys will coordinate with resolver groups to close "Preparation of Scan Environment" Change Request upon completion of scan.
4. Review of report by Unisys Security Officer: the scan reports will be reviewed by Unisys Security Officer. Severities will be identified and a recommendation report will be shared with the Client.
5. Raise Incidents and Changes based on recommendations from Unisys Security Officer: the Client will push the critical/high/medium vulnerabilities remediation via the Client Incident and Change management process.
6. Incidents and Change closure tracking: Unisys Project Manager will maintain a tracking log of open Incidents in the Qualys tool and provide a summary report for the Client review.

The above activities are repeated for a re-scan to identify and report against the remediation achieved in the Client environment. Remediation of any affected systems remains the responsibility of the Client.

Additional Steps of Remediation Process

1. Open a Remediation Ticket in the Client IMS system and notify the Client by assigning the
2. Ticket to the Client resolver group per the timeline identified by severity type.
3. Perform two follow-ups within the time frame set forth in Section 7 (Service Level Objectives).
4. Maintain Remediation ticket in a pending status for the Client action after second (2nd) follow-up and then close per the agreed timeline with the Client. The Remediation ticket detail will remain in the incident tracking log maintained by the Unisys Project Manager.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

The duration for which the Remediation ticket will remain open after the two (2) follow- up activities will be mutually agreed upon. It is important to note that any vulnerability for which a Ticket was raised but not remediated will reappear in subsequent scans.

Vulnerability Management Service Cost

VMS Packages (US based resources)			
Package Scope	**One-Time**	**On-Going Price per Month**	**On-Going Price per Year**
Scanning up to 256 IP's	**$2,864**	**$1,329**	**$15,948**
Scanning > 256 up to 512 IP's	**$3,044**	**$1,796**	**$21,548**
Scanning > 512 up to 1024 IP's	**$3,044**	**$2,475**	**$29,700**
Additional Qualys Scanner			**$995**

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

4. Unisys Stealth® MSS

Stealth Service Description

Unisys Stealth® provides a unique yet extremely effective mechanism, software defined micro-segmentation, to manage and continually adapt security for mission-critical enterprises. Realizing that merely defining static security policies is not effective – and is increasingly susceptible to advanced threats for our clients – Unisys takes a different approach to implementing and managing a micro segmented environment.

Stealth(aware) **control and visibility** to reduce the time and effort required to implement micro-segmentation. It provides real-time visibility across physical and virtual infrastructure – enabling quick and easy identification of what needs to be secured. Through an intuitive visualization of network traffic flows, Stealth(aware) enables fine-grained micro segmentation security policies to be defined and applied automatically and on the fly in real-time to permit, restrict or completely block communication between sensitive assets and their end users, to address specific business requirements as they evolve.

- Basic Stealth™ Managed Service:
  Includes Stealth™ Management, Monitoring and Reporting.
- Advanced Stealth™ Managed Service:
  Includes a Combination of Stealth™ Management, Monitoring, Reporting and SIEM Integration, for advanced event correlation, and analytics.
- Premium Stealth™ Managed Service:
  Includes the Advanced Stealth™ plus a fully customizable Managed Security Services portal to provide a Single pane of Window into Stealth™ and other Unisys security services.

Stealth MSS Cost

Unisys Stealth License & Support				
Description	**Total Server License Quantities**	**License Term**	**Price (per server / per month)**	**Price (per client / per month)**
Stealth Server License and Support - Tier 1	1-499	12 months	$29.06	$4.80
Stealth Server License and Support - Tier 2	500-999	12 months	$23.16	$4.02
Stealth Server License and Support - Tier 3	1000-4999	12 months	$18.18	$3.16

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

5. Additional Unisys Managed Security Services

The following Unisys Services are expected to be added to the GTA GETS Ready contract at a later date.

Cloud Security

Cloud Security is modular, self-adapting, highly customizable service, based on advanced analytics techniques such as machine learning, supervised/un-supervised learning, active simulations, data mining and knowledge engineering. Cloud Security is also integrated with industry specific threat intelligence feeds that provides additional contextual data to supplement detection, qualification and investigation activities, to combat against advanced attacks. Our service is rapidly scalable and vendor agnostic.

Key features:

1. Highly Scalable & Rapid Deployment.
2. Pre-built template for major Industry segments.
3. Contextual Intelligence driven.

IAM

Identity Management (IdM) describes the management of individual ***identities***, their ***authentication, authorization***, roles and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.

"Identity management" and "access and identity management" (or IAM) are terms that are used interchangeably under the title of identity management while identity management itself falls under the umbrella of ***IT security***.

Identity management systems, products, applications, and platforms are commercial Identity management solutions implemented for enterprises and organizations.

Identity and Access Management Services requires a secure single sign-on solution integrated with Active Directory services or other identified directory services for accessing systems and applications on hosted, private cloud, and public cloud systems and services. This is critical as identity and access management is the front door protecting the interconnected towers and their services.

GRC

Unisys IT Governance, Risk, and Compliance (GRC) services are powered by a Unisys provided ServiceNow instance, configured to comply with our clients' security policies, and provide the required confidentiality, integrity and availability of the service. Standard ITIL processes, integrated with service management processes are used to manage the GRC tool. The required GRC tool data is integrated by API into the service management system.

The ServiceNow GRC service provides process controls aligned to our clients' risks and policies. This alignment enables GRC to automate the audit process by managing audit controls, assigning

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential

control-testing tasks, managing evidence collection, and assigning remediation activities. GRC support tasks are scheduled using the tool, including re-occurring tasks, interface execution and maintenance tasks. GRC provides a central repository for key controls and audit definitions, including a history of audit results with the corresponding findings.

Copyright © 2017 Unisys Corporation. All Rights Reserved.

Unisys Confidential