NASPO Pricing Notes and Explanations

Smartronix is pleased to provide the State of Utah with its pricing response to Bid #: CH16012. The attached NASPO Pricing offers pricing for the following Cloud Models: Iaas, Paas, SaaS. We are offering our Cloud Assured Managed Services (CAMS) for cloud services utilized in Public/Government Community Clouds.

The prices for Public and Government Community Cloud Services can be found within the same links provided in the price attachment and receive the same discounts, 3%. The pricing and discount schedule for Managed Services can also be found in the attached pricing.

Due to the rapid innovation and growth of available services in the cloud marketplace Smartronix is offering the use of all current and future cloud services as they are available. The current generation instance configurations can be found outlined in the attached pricing document. The full suite of products available to the state under contract with Smartronix can be found here:

- AWS: https://aws.amazon.com/products
- Azure: https://azure.microsoft.com/en-us/services/
- GCP: https://cloud.google.com/products/

Note: Not all services are available in all regions.

With current list pricing for all services can be found here:

- AWS: https://aws.amazon.com/pricing/services/
- Azure: https://azure.microsoft.com/en-us/pricing/
- GCP: https://cloud.google.com/pricing/

Pricing Methodology

Smartronix’ approach to pricing and discounts based on consumption (or utility style), with Managed Service cost broken out from the cost of compute. We believe this model, of separating the cloud service and management costs provide the customer with the most flexible and transparency.

First we are offering discounts, outlined below, based on your month AWS spend. For example, utilizing CloudCheckr we run your AWS invoice at list price. We then discount that amount and invoice you. Our CAMS offering, invoiced separately, from your cloud services is priced per instance. In a variable environment where instances are stood up and shut down frequently we invoice the number of effective instances:

$$\frac{\text{Total hours consumed}}{\text{Total hours in that month}} = \text{\# of effective instances}$$

Cloud Services Price Estimating

AWS provide pricing calculators to estimate the cost of their services. These calculators are an important tool to estimate the cost of future task orders. And with all prices being publicly available there are no hidden cost. These calculators can be found here:

- AWS: http://calculator.s3.amazonaws.com/index.html
- Azure: https://azure.microsoft.com/en-us/pricing/#explore-cost
- GCP: https://cloud.google.com/products/calculator/

Discounting

We are offering the following discounts off of the list price at the time of consumption for each cloud provider:

- 3% on AWS cost
- 3% on GCP cost

Note: There are no discounts provided on products and services sold thru Amazon AWS for which Smartronix does not receive a discount. This currently includes fees associated with: Amazon DevPay, Amazon Mechanical Turk, Amazon Flexible Payment Services and any 3rd party products purchased in theAWS Marketplace.

We are also offering a volume based discount off of the States's month managed service spend:

Monthly Cost	Vol Discount %
$0 - $15,000	0%
$15,000 - $30,000	2.5%
$30,000 - $45,000	5%
$45,000 - $60,000	10%
Over $60,000	12.5%

Additional services can be purchased utilizing our rate card:

Labor Category	Hrly Rate
Sr Cloud Architect	$250
Cloud Architect	$225
Sr Cloud Engineer	$200
Cloud Engineer	$180
Security Architect	$200
Security Analyst	$175
Sr I&O Engineer	$140
I&O Engineer	$120
Cloud Program Manager	$220
Cloud Project Manager	$200

Google Workspace Development Specialist*	$237
Project Manager*	$237
Implementation Specialist*	$213
Google Certified Training Specialist*	$182
Change Management Specialist*	$182
CSP Consulting/ Professional Services	$3250/day

Rates marked * indicate staffed through Resultant

Amazon Web Services

Note 1: AWS pricing is based on per hour consumption.

Note 2: AWS Compute services vary between regional availability and OS

Note 3: When you have purchased a sufficient number of Reserved Instances in an AWS Region, you willautomatically receive discounts on your upfront fees and hourly fees for future purchases of Reserved Instances in that AWS Region. Reserved Instance discounts are determined based on the total list price (non-discounted price) of upfront fees for the active Reserved Instances you have per AWS Region to determine the applicable volume discount tier. As an example, imagine that we had the following volume discount tiers:

- $0-$500K: Upfront - 0%, Hourly - 0%
- $500K - $4M: Upfront - 5%, Hourly - 5%
- $4M - $10M: Upfront - 10%, Hourly - 10%
- $10M+: Negotiated

Microsoft Azure

Note 1: Azure pricing is based on per hour consumption.

Note 2: Azure Compute services vary between regional availability and OS

GCP

Note 1: GCP pricing is based on per hour consumption.

Note 2: Google Compute services vary between regional availability and OS

Smartronix AWS Market Place

https://aws.amazon.com/marketplace/seller-profile?id=cb17135a-f9d6-4e4a-8818-9377c415134e

Resultant

SMX is pleased to partner with Resultant, a consulting firm who partners with clients in the public and private sectors to help them overcome their most complex challenges, empowering our clients to drive meaningful change in their organizations and communities. Through Resultant, SMX can offer Google Workspace, Chrome Enterprise Licenses, and Professional services related to the implementation of the two aforementioned products.

Alation

SMX is pleased to be an Alation resale and implementation partner. Alation is a modern data platform that supports data governance, data cataloging data quality, data lineage, connectors and protected sheets.

Snowflake

SMX has deep experience working with government agencies on Snowflake implementations. SMX is a direct distributor for Snowflake. SMX's Select Tier partnership with Snowflake ensures that SMX team members are up to date on the latest Snowflake Capabilities. SMX's unique position as a systems integrator and direct distributor allows SMX to negotiate deep discounts for Snowflake capacity purchases based on volume on behalf of the state.

Informatica

SMX is pleased to be an Informatica resale and implementation partner. Informatica is an Intelligent Data solution that can support ETL, data transformation, data de-identification, data governance, data quality, data integration, master data management, AI, and data cataloging.

Tableau

SMX works closely with Tableau as both a reseller and implementation provider. Tableau is a best-in-class data visualization and analytics tools.

Cardinality

Cardinality.ai is a data technology company helping government agencies deliver better citizen services through AI enabled SaaS solutions. Cardinality's built-for-government suite of case management solutions employ configurable modules, cloud-based tech, a powerful AI assistant, an intuitive interface, and data-driven workflows on a low-code platform that enables agencies to modernize faster, and with greater confidence, than custom development projects. SMX is both a reseller and implementation partner for Cardinality.

Function	Product Description	Product Part Number
Child Welfare	Cardinality Annual SaaS licenses	CDY.RBS.CCWIS.xx.H00500D10.NPO
Child Care	Cardinality Annual SaaS licenses	CDY.RBS.CC.xx.H00500D10.NPO
Child Support	Cardinality Annual SaaS licenses	CDY.RBS.CS.xx.H00500D10.NPO
Integrated Eligibility	Cardinality Annual SaaS licenses	CDY.RBS.IES.xx.H00500D10.NPO

Case Management	Cardinality Annual SaaS licenses	CDY.IT.CM.xx.H00100D10.NPO
Assumption: 1. Onetime Implementation Cost is additional 2. Annual SaaS license includes Hosting and 3rd Party software for ESB, Rule Engine, Reporting and Work Flow designer 3. Annual SaaS license includes the following a. Yearly 2 upgrades b. Monthly critical patch release c. Level 3 Technical Support		

Smartronix DBA Creoal Consulting, LLC a wholly owned subsidiary of SMX

Creoal Consulting, LLC (“Creoal”), a wholly owned subsidiary of SMX Group, LLC (SMX) is a member of the Oracle Partner Network and has a 19-year record of success providing Oracle Cloud applications, program management, systems integration, custom development, business intelligence, and sustainment services to public sector, higher education, Federal Government, and commercial clients. Our 280+ expert-level resources—including former executives from Oracle as well as members of the Big Four Accounting firms—bring a collective wealth of experience with ERP, HCM, and Enterprise Planning and Budgeting solutions. Our experience with public sector customers is unsurpassed by any other Oracle Partner (with well over 250 Oracle implementations completed), providing our customers with the advantage of our exceptional level of expertise in this area. Our focus is to help customers improve processes and get the highest level of value possible from their investments in technology.

An industry thought leader in Oracle implementations, Creoal has been working with Oracle Cloud Applications since their inception in 2012. We have extended our knowledge and experience as the applications have grown in functionality and have performed more than 40 Cloud implementations encompassing project management, knowledge transfer, system design and build, conversion, testing, and end-user training.

Building on our success in the Federal Government marketplace, Creoal began focusing on delivering technology solutions and services to the public sector in 2016. We help State and Local Government agencies improve efficiency and customer service while meeting issues such as shrinking budgets, intricate compliance and reporting requirements, and risk management. Many public sector organizations rely on Creoal’s technical expertise as they move to the cloud. We help them modernize systems to take advantage of the latest innovations in technology and overcome the constraints of their legacy systems. Creoal provides services and support that enable state and local government agencies to streamline operations and achieve the mission of improving service to citizens.

Creoal Areas of Expertise

Creoal provides Oracle Cloud Services, systems implementations, integrations, upgrades, and consulting services that maximize Oracle ERP, EPM, HCM, and SCM system performance for federal, public sector and commercial customers.

Enterprise Resource Planning	Creoal’s Oracle ERP services automate and simplify business-critical activities. Creoal’s support goes beyond implementation to include business process analysis, upgrades, and operations and maintenance—making us a one-stop shop for the entire range of ERP needs.

Enterprise Performance Management	Our EPM services deliver actionable business information that enables our clients to enhance efficiency and streamline business processes.
Human Resources and Payroll Management	Our HCM services maximize the value of the workforce by automating HR processes from hire to retire. Creoal also supports payroll processing, including ensuring compliance with tax reporting and regulatory rules. Learn More
Manufacturing and Supply Chain Management	Creoal's SCM services automate and integrate business processes, providing end-to-end visibility for effective procurement, manufacturing, inventory, and logistics management. Learn More

Creoal Service Offerings

Oracle Cloud Application Implementations – Creoal provides a dedicated certified team to provide best practice implementations and guidance for net new adoption, co-existence, or migration from existing systems.

Oracle Cloud Application Support – Creoal delivers an expansive array of managed services and support options for customers to help lower costs, optimize performance, and enable staff to focus on key business objectives and innovation. Our service models span the entire Oracle stack, including hardware, operating systems, database, middleware, and applications. We deliver end-to-end managed services and 24x7x365 support from our United States and India-based offices, along with onsite, onshore, and offshore resources to meet every level of demand.

Program Management – Creoal provides strategic oversight function responsible for the consistent delivery of large-scale initiatives.

Systems Integrations – Offering cloud-based services that enable businesses to connect their applications and data sources, automate end-to-end processes, and centralize management CEMLI stands for Configuration, Extension, Modification, Localization, and Integration. Using CEMLIs, Creoal can provide software extension framework.

Business Intelligence – With more than 15 years of experience working with Oracle Cloud, Hyperion, OBIEE, Exalytics, Endeca, BI Foundation Suite, Informatica, ODI, E-Business Suite Applications, and custom data warehousing solutions, Creoal has the expertise to support and expand our clients' BI capabilities.

Enterprise Architecture – Current and future state architecture definitions, future state roadmap development, and overall information technology (IT) and IT strategy assessment services.

Digital Roadmap and Approach – Prepare the organization for the modernization journey; define business process and capabilities as well as desired results; define target digital transformation roadmap and approach.

Define Digital Solutions – Creoal conducts due diligence for solution selection based on capabilities, fit/gap analysis, and desired target end state; and finalized plan.

Agile Development – Complex software engineering can be wide in scope, often yielding incomplete results while exceeding budgets and timelines. Embracing Agile methodologies for software engineering helps clients realize value and achieve success regardless of a program's size and complexity. Creoal's focus on User Experience Design ensures that agencies can effectively deliver information, resources, and services both internally and externally. Creoal helps customers deliver and share information for more rapid decision-making, improving how users receive services.

Sustainment – Creoal makes continuous improvements while managing, monitoring, and supporting steady-state operations.

Assessments and Implementation Assurance – Creoal Implementation Experts review in-process implementation to identify issues before they become major problems. Review planned and completed system configurations; Validate key decisions: Chart of Accounts, Inventory orgs, Intercompany; Determine whether internal controls are properly defined & configured; Evaluate project team fitness to execute tasks at hand; Validate operational, regulatory and financial reporting requirements.

Creoal Pricing Structure: Products and Services

Creoal's offerings for Oracle SaaS, PaaS, and IaaS Products include a 30% discount on Oracle then current Manufacturer's Suggested Retail Price, subject to the terms and conditions of our partner agreement including but not limited to any flow up and/or end user requirements. More product specific information can be found at http://www.oracle.com/corporate/pricing/naspo-cloud-solutions.html

Creoal Consulting Services Pricing Structure for Oracle Applications – Commercial/ SLED

Resource	Discounted Rate
Oracle ACE COMMERCIAL/ SLED	$313.50
Partner COMMERCIAL/ SLED	$275.50
Architect COMMERCIAL/ SLED	$251.75
Project Manager COMMERCIAL/ SLED	$228.00
Program Manager COMMERCIAL/ SLED	$232.75
Project Administrator COMMERCIAL/ SLED	$133.00
Senior Business Analyst COMMERCIAL/ SLED	$204.25
Business Analyst COMMERCIAL/ SLED	$166.25
Senior Technical Analyst COMMERCIAL/ SLED	$194.75
Technical Analyst COMMERCIAL/ SLED	$161.50
Associate COMMERCIAL/ SLED	$118.75
Remote Senior Business Analyst COMMERCIAL/ SLED	$90.25
Remote Senior Technical Analyst COMMERCIAL/ SLED	$76.00
Remote Business Analyst COMMERCIAL/ SLED	$74.10
Remote Technical Analyst COMMERCIAL/ SLED	$61.75

Elevate Manage - Service Catalog

1. ELEVATE – MANAGED SERVICES

1.1 INTRODUCTION

SMX Elevate Managed Services allows your organization to take advantage of the scalability and efficiency of cloud computing, while minimizing the cost and complexity of in-house infrastructure and application management and monitoring. Our team of experts, utilizing the SMX Intelligent Automation Platform, offers comprehensive management of cloud services from provisioning to solution life cycle. Our Elevate Managed Services support private, public, multi-cloud, and hybrid cloud offerings, freeing up your organization to concentrate on important business and technology initiatives while entrusting IT operations to our experienced team.

1.2 CASE MANAGEMENT PORTAL

The Case Management Portal is the primary interface for our customers, providing a range of functions, including access to information, request submissions and tracking, and access to our knowledge base. The portal's integrated features streamline the support experience, with real-time collaboration adding further value. We use a customized GCC High ServiceNow instance for our back-office ITSM functionality, which ensures that customer data is strictly separated by organization. This helps us meet regulatory and compliance requirements, including those that require special background investigations, public clearances, or industry-specific clearance activities. The Case Management Portal was designed with Managed Services customers in mind, offering a centralized location for creating, tracking, managing, and reporting on all service requests. This capability gives customers greater control over their services, enabling us to meet their needs more efficiently and effectively.

1.3 MANAGED SERVICES AND SERVICE MANAGEMENT

The Managed Core Services are developed and integrated to provide customers with fully instrumented Cloud experience. Our optional services are designed to enhance the customer experience and capabilities by providing discrete capabilities within the SMX Cloud Management Platform. This includes the necessary processes, procedures, tooling, and licensing to deliver predictable results. Our service catalog includes Core, Optional, and Optional Security Services, defined in Table 1 and 2 below. We understand that some customers may have specific business requirements, existing tools, or interoperability needs, and we can accommodate these with custom service integrations. Pricing for custom integrations is separate and tailored to the unique licensing costs and labor required for a tailored solution.

1.4 CLOUD RESALE AND CONSOLIDATED BILLING

The Cloud Resale and Consolidated Billing service provides value-added Cloud Service Expense Management Services, allowing customers to consume Cloud Services through resale from SMX. Customers who use our resale service receive a single consolidated invoice that shows all services used across all managed accounts. The billing detail can be tailored to support the customer's business and financial management needs, including organizational and divisional separation for show-back/chargeback purposes. Additionally, the Cloud Service Expense Management Advisory service (Optional Services) is included in the CRCB as a value-added service to help optimize cloud expense efficiency.

2 SERVICE DESCRIPTIONS

The following sections describe the Core, Optional, Managed Security Services, and Pods and Squads offerings, these are offered in bundled pricing models in section 0.

Core Account Services (Required)	
2.1.1 CSP Account Management Services	2.1.5 Boundary and Network Management Infrastructure Provisioning
2.1.2 Infrastructure Service Incident Management	
2.1.3 SLA Management	2.1.7 Serverless Compliance, Logging, and Real-Time Monitoring
2.1.4 Log Aggregation Service	2.1.8 Container Service Monitoring (ECSM)
Core Services for Managed Instances	
2.2.1 Monitoring and Notification Service	2.2.3 Anti-malware Management Service
2.2.2 Operating System Patch Management	2.2.4 Backup Service

Table 1. Elevate Core Managed Services

Optional Managed Services	Optional Managed Security Services
2.3.1 Cloud Service Expense Management Advisory	2.7.1 Security Incident Response
2.3.2 Infrastructure Advisory	2.7.2 Enhanced Log Aggregation and Analysis
2.3.3 Workspaces Management	2.7.3 Host Intrusion Detection/Prevention
2.3.4 Database Monitoring	2.7.4 Host File Integrity Monitoring
2.4 SITE Reliability Engineering (SRE)	2.7.5 Application Control
2.5 Pods and Squads SUPPORT	2.7.6 Systems Vulnerability Scanning
2.6 AWS Managed Services from SMX	2.7.7 Continuous Monitoring Security and Regulatory Compliance Support Services

Table 2. Elevate Optional Services

2.1 CORE ACCOUNT SERVICES (REQUIRED)

2.1.1 CSP Account Management Services

The CSP Account Management Service is optimized to enforce and report CIS Benchmark Compliance and provide event trail aggregation that may be leveraged for analysis and operational break/fix incident/event triage. Security Benchmarks are defined and monitored in accordance with CIS best-practices, which are made up of industry-standard checks. Environments are audited to identify potential security compliance shortfalls, against relevant standards.

Scope:

- CSP Account Event Trails: AWS CloudTrail, Azure Monitor Logs
- AWS S3, Azure Storage Accounts,
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level

Standard Audited CSP Events (CIS Benchmarks 3.01- 3.14):

- Privileged (root) Login
- Non-MFA Login

- Identity and Access Management changes to Policies, Groups, Users and Roles
- Notification of new Security Groups and changes to existing Security Groups
- Object Storage Policies/ACL changes
- Public access grant notifications for Object Storage
- Service Quota Limits

Automated Compliance Reporting:

- Reports on best practices and customer compliance with Center for Internet Security (CIS) benchmarks compared against the CSP IaaS environment and assets.

2.1.2 Infrastructure Service Incident Management

The Infrastructure and Incident Management Services enable the identification, classification, and filtering of events, while offering structured responses to address and resolve infrastructure service incidents in customer environments. Event management, utilizing the Monitoring Solution automation framework, oversees detection and notification through designated service topics. Critical events trigger infrastructure incident response processes and procedures, as the SMX team employs structured methodologies to identify, classify, escalate, and resolve incidents concerning managed cloud infrastructure and supported operating systems.

2.1.3 SLA Management

Customer service requirements are monitored and tracked against documented Service Level Agreements (SLAs). The SLA Management Service reports service performance against standard Service Level targets identified below in Section 3 Service Level Agreements. The reports are provided monthly and are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement.

2.1.4 Log Aggregation Service

The Log Aggregation Service captures cloud service provider logs, network and load balancer & object access logs for retention and archive.

Please note that log correlation, advanced search, analysis and support for other log types are not part of this service – see 2.7.2 Enhanced Log Aggregation and Analysis. Technologies used in support of log aggregation include:

- CSP API Logs
- Virtual Network Flow Logs
- Load Balancer Logs
- Object Storage Access Logs

2.1.5 Boundary and Network Management

The Boundary and Network Management Service offers monitoring and configuration management for various cloud service provider (CSP) native components. Our team of experts provides secure and highly available management and monitoring of CSP native boundary services, load balancers, and virtual networks. We identify and mitigate network-level changes in response to events or customer requests, such as VPN tunnel configuration, firewall policy changes, IP route configurations, public IP allocation for service advertising, load balancing capabilities deployment and monitoring, and deployment of new cloud IP subnets.

Our service also includes implementation of changes to cloud-native layer 3 network configuration items upon request, diagnostic support for connectivity troubleshooting, native Cloud networking logging and retention management, log interrogation and analysis upon request, coordination with remote network operators for real-time diagnostic feedback on interconnectivity support, and external application HTTP status code validation using Pingdom, with monitoring and alerting.

Target Group Metrics for Load Balancer Monitoring

- Healthy Host Count
- Request Count Per Target
- Request Count
- Target Response Time
- HTTP 4XX Count
- HTTP 2XX Count
- Unhealthy Host Count
- Target Connection Error Count

2.1.6 Infrastructure Provisioning

Infrastructure Provisioning services guarantee consistent and repeatable deployment of native cloud infrastructure into a predefined environment. Customers submit provisioning requests via the customer management portal for any services requiring management. SMX reviews the requests, confirms the requirements, provisions the resources, and configures them to ensure proper integration with Account and Core Services. This includes tagging provisioned resources for Managed Services, potentially through a client-updated CI/CD pipeline script. Provisioning resources not managed under SMX Account and Core services or defining new landing zones or associated network and account definitions, must be supported by an SMX professional services team under a separate statement of work.

2.1.7 Serverless Compliance, Logging, and Real-Time Monitoring

SCLRM is optimized for monitoring CSP Serverless implementations, enforcing, and reporting CIS Benchmark Compliance. Security Benchmarks follow CIS best practices, composed of industry-standard checks. All serverless environments undergo audits to ensure security compliance with relevant standards.

Scope:

- Serverless Monitoring and Notification: AWS Lambda, GCP Cloud Functions, Azure Function Apps
- AWS/Azure/GCP CIS Benchmark Compliance Implementation/Auditing/Reporting at the Account/Subscription/Project level

Serverless Event Monitoring and Notification:

- Captures all (CSP) events, logs, audit information, and monitoring information provided by in-scope services.
- Alerts are defined for key events within the environment to trigger further analysis or incident response.
- Monitored Metrics include:
  - Number of invocations

- Failed executions (permissions, timeouts, exceptions)
- Concurrent executions
- Execution throttling

2.1.8 Container Service Monitoring (ECSM)

ECSM is a monitoring capability designed specifically for AWS Elastic Container Services.

The Monitoring Service (CMS) has been extended to support monitoring of tagged ECS clusters. The following metrics are automatically enabled across the cluster and services:

ECS Supported Metrics (Dimension)

- Cluster
  - CPU Utilization
  - Memory Utilization
  - CPU Reservation
  - Memory Reservation
  - GPUReservation
- Service
  - CPU Utilization
  - Memory Utilization

2.2 CORE SERVICES FOR MANAGED INSTANCES

Core services for managed virtual machine instances integrate with the Infrastructure Service Incident Management and ITSM Portal for Service Request Management.

2.2.1 Monitoring and Notification Service

The Monitoring and Notification Service leverages the Intelligent Automation Platform's Monitoring Solution automation framework. The monitoring platform leverages micro services to detect all assets that are tagged for management and enables a defined set of standardized alarms/alerts. Each alarm can be customized to a tagged instance definition, allowing customer environments to have different defined alarm triggers for specific workloads. The CMS framework leverages web hooks to pull in the alarms/alerts and to automate creation of ITSM tickets.

Example Triggers include:

High CPU Utilization*	**Instance failed health check**
Disk space utilization*	Excessive network utilization*
Excessive disk IOPs*	High memory usage*
Excessive disk write queue length*	

*Triggers can be customized to customer workloads. Custom event types not identified above can be created/deployed and actioned directly to the customer as a professional services effort.

2.2.2 Operating System Patch Management

The Operating System Patch Management Service actively monitors and applies operating system patches and updates. The Elevate team performs monthly patching of guest operating systems based on vendor release schedules, coordinating maintenance and patching windows with customers to minimize disruption. The solution automatically downloads and applies identified patches to the guest OS through a scripted process, while the Intelligent Automation Platform logs applied patches to track system configuration. Critical or security-related patches are quickly escalated to customers for approval during an out-of-cycle maintenance window.

SMX advises organizations requiring updated source images for container deployments to update their container cluster instance fleet with the latest patches. This process is triggered either through a Set Schedule (time-based Patch Window) or when a new patched cluster host image is verified and published. The process automatically deploys the new cluster image, drains, and removes the old cluster host from service. Notifications are sent upon successful patching, and in case of failure, a rollback to the previous launch configuration occurs. Customers can configure hosts to accept patching and updates via instance tags. Suspending or delaying patch windows may increase vulnerabilities in scan results and impact customer security posture.

Supported Operating Systems include:

- Amazon Linux
- Amazon Linux 2
- Amazon Linux 2023
- CentOS
- Debian Server
- Oracle Linux
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)
- Ubuntu Server
- Windows Server

2.2.3 Anti-malware Management Service

The Anti-malware Management Service safeguards managed OS instances from malware by ensuring the -provided anti-malware remains active and current with the latest signatures. Upon malware detection, the host is quarantined, and an incident ticket is generated for remediation. Compliance audits verify server adherence to customer anti-malware policies. The service operates within a unified management framework, supporting multiplatform CSP and on-premises environments using the TrendMicro Deep Security Suite. Protection against file-based threats, such as viruses, trojans, worms, rootkits, spyware, grayware, packers, and keyloggers, is included. Alerts and threats generate service tickets, investigated by SMX experts. Remediation activities follow the shared responsibility model, with same-day SLA for services. Malware definition and virus scan engine updates are provided within 24 hours and 30 days, respectively.

SMX will update each managed instance to the current malware definitions under management within 24 hours of their publication by the Original Equipment Manufacturer (OEM) and virus scan engine updates within 30 days of their release unless delayed to comply with a specific client approved maintenance window.

2.2.4 Backup Service

The Backup Service includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The backup retention duration will impact cloud storage costs. Through the ITSM process, the SMX team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful.

2.3 OPTIONAL SERVICES

2.3.1 Cloud Service Expense Management Advisory

The Cloud Service Expense Management Advisory Service promotes cost optimization by analyzing aggregated usage data and correlations. Recommendations stem from actual data analysis, advanced toolsets modeling future spend based on utilization, "what-if" scenarios, knowledge of customer workloads and environments, and experience across various cloud environments. This Advisory Service is an integrated component of the Cloud Resale and Consolidated Billing Service.

Examples of cost optimization opportunities include:

- Resource utilization (Throttling under-utilized instances; Parking off-period resources)
- Right-sizing instance type
- Selection of workload-appropriate pricing models
- Resource tagging
- Reclamation of orphaned resources
- Optimization of BYOL (Bring-your-own-license)
- Storage life-cycle management
- Cost Monitoring and Alerting

This service requires deployment of the Cloud Service Expense Management Advisory tool which requires read only access to the CSP billing data and optional read only access to performance data (for service utilization optimization.)

For maximum utilization of the Cloud Service Expense Management Advisory tool additional configuration is required including all linked accounts will need credentialed for asset meta data ingestion, CloudWatch or collection agent of the client's choice is required to gather memory and disk metrics to generate accurate Right Sizing reports.

2.3.2 Infrastructure Advisory

The Infrastructure Advisory Services offer prescriptive guidance on cloud services optimization, encompassing capacity management reviews, architectural evaluations, best practices reviews, auto-scaling tuning, and migration paths for on-premises workloads. These reviews utilize our Well Architected guidelines and ITSM processes.

The Well Architected Review is an in-depth analysis of your infrastructure, comprehensive review of security practices, application integration architectures, and resource sizing. This review empowers the SMX team to guarantee that customers utilize cloud services according to CSP best practices, ensuring cost-effective and secure service delivery.

2.3.3 Workspaces Management

The Workspaces Managed Services (WMS) provides comprehensive management and assurance for virtual desktop users, including operating system patch and update management, software packaging, and software lifecycle management. Backups are also included with the option to choose a Recovery Point Objective (RPO) that suits your organization's needs, ensuring protection of virtual workstation data. The service also includes antivirus and antimalware protection. Integration with your existing directory service allows for seamless application of organizational configurations, policies, and controls to your Workspaces, managed by SMX WMS just like your servers. This service includes core management of workspaces with optional security services available to meet customer specific regulatory compliance requirements.

2.3.4 Database Monitoring

Database Monitoring Service enables automated monitoring of cloud native Relational Database Services. This includes performance and availability monitoring, backup and restore, and patching. The DBMS currently supports Oracle, MySQL, Microsoft SQL, and PostgreSQL.

Tasks:

- Monitoring
    - Resource consumption monitoring:

CPU Utilization	Disk Queue Depth
Read Latency	Freeable Memory
Write Latency	Free Storage Space
Database Connections	

- Backup/Restore
    - Perform scheduled Database backups and restorations of backups (per customer request)

2.4 SITE RELIABILITY ENGINEERING (SRE)

The Site Reliability Engineering (SRE) services cater to customers seeking team members with specialized DevSecOps skillsets to be embedded within their platform or application teams, typically for extended engagements. The SRE model's value proposition lies in customers receiving an advanced level of build and support functions through the intrinsic knowledge of the SRE team members who have helped develop the systems. The SRE team focuses on building highly reliable and resilient systems, automating deployment processes, and continuously improving the systems they manage. SRE resources are expected to allocate time to operational support tasks while balancing developmental tasks that enhance the system. SREs identify suitable fixes, including runbooks and automation, develop monitoring and observability capabilities, and integrate with service catalogs and ITSM systems. The SRE model's essence is "you build it, you run it, you own it" concerning the systems they manage.

2.5 PODS AND SQUADS SUPPORT

Pods and Squads have increasingly become popular staffing models and are closely aligned with Site Reliability Engineering (SRE). The Pod and Squad teams have distinct objectives and are not connected or necessarily dependent on each other. The Pod team is a cross-functional group consisting of a mix of resources, typically organized to support specific, shorter-term engagements. These resources are usually packaged and billed at a fixed monthly rate, rather than traditional Time & Materials invoicing. The Pod team composition is adaptable and may include Project Management, Architectural, Development, Engineering, Operations, Database Operations Administration Security, and FinOps resources. In the example below, the collection of resources would be suitable for supporting a customer's rapid onboarding into our managed services environment and initial professional services engagements.

Example Pod Team:

Role
Project Manager
FinOps Analyst
Sr SA
SA
Operations Engineer
Security Engineer

Squads are groups of similar resources brought together to address customer requirements in a specific area of focus. Squads can be considered a surge capability to help customers augment their teams or scale when a particular skillset is required for a defined initiative. Scenarios requiring a specialized Squad are often long-term in nature, lasting from 90-180 days or longer. Examples of Squads include Site Reliability Engineers, Migration Teams, Application Development, Serverless/Container Development, Security Resources, and ATO Support Teams.

Example of SRE Squad

Role
Project Manager
Sr DevOps Architect
Developer
SRE x 3

2.6 AWS MANAGED SERVICES FROM SMX

AWS Managed Services (AMS) helps you operate your AWS infrastructure more efficiently and securely. Leveraging AWS services and a growing library of automations, configurations, and run books, AMS can augment and optimize your operational capabilities in both new and existing AWS environments. AMS provides a consistent operating model for your entire AWS fleet leveraging detective guardrails, monitoring, security, and incident management best practices for both traditional and modernized workloads.

Advanced

AWS Managed Services Advanced operations plan with preventative controls via a change management system within an AWS managed landing zone, which provides a full operational solution and trades some flexibility for increased operational rigor to protect Client critical business applications. Additional details available at https://aws.amazon.com/managed-services/features/advanced-operations-plan/

Accelerate

AWS Managed Services Accelerate operations plan augments Client capabilities for operating AWS workloads. Clients then have the flexibility to choose the level of operational support that meets support needs and long-term goals. Additional details available at https://aws.amazon.com/managed-services/features/accelerate-operations-plan/

2.7 MANAGED SECURITY SERVICES

2.7.1 Security Incident Response

The Security Incident Response Service aligns with the NIST 800-61 Computer Incident Handling Guide, defining scope, roles, and responsibilities during the contracting process. The process covers seven major areas: Preparation, Detection and Analysis, Incident Analysis, Incident Response, Containment, Eradication, and Recovery, Post-Incident Activity, and Coordination and Information Sharing.

- Preparation: Emphasizes continuous preparation by ensuring secure systems, networks, and applications, and establishing practices to manage incidents within set SLAs.
- Detection and Analysis: SMX works with clients to identify attack vectors and provide definitive incident classification, using various sources to identify precursors and indicators.
- Incident Analysis: SMX analyzes client-prioritized incidents, utilizing multiple data sources to assess indicators of compromise, document, prioritize, and invoke notification processes.
- Incident Response: The SMX team supports incident response processes through escalation, break/fix remediation, disaster recovery, system restore, and event information reporting.
- Containment, Eradication, and Recovery: SMX collaborates with clients to develop containment strategies for each major incident type and determine appropriate risk thresholds. Proprietary CyberHunter® tools assist with isolation, containment, and eradication.
- Post-Incident Activity: SMX documents incidents and shares findings in a formal Incident Review and Lessons Learned report, updating incident handling guidance and checklists accordingly.
- Coordination and Information Sharing: SMX coordinates with external parties as needed, discussing information sharing with clients before incidents occur to establish policies and procedures. Clients are responsible for notifying law enforcement and handling external media communications.

2.7.2 Enhanced Log Aggregation and Analysis

The Enhanced Log Aggregation and Analysis Service (compliant with SOC 2, ISO 9001, ISO 20000, ISO 27001, and FedRAMP Moderate) ingests and monitors logs such as event logs, audit information, and monitoring data from operating systems, platforms, networks, and infrastructure 24/7. Security alerts for key events and activity patterns are defined to trigger further analysis or incident response. ELAA team members continuously refine and tune alerts to eliminate false positives. ELAA Security Monitoring is separate from the Security Incident Response service described in section 2.4.1.

Core Log Aggregation vs ELAA:

Core Log Aggregation service captures and stores core CSP log events for ad hoc search using CSP native capabilities. No security alerting is provided by Log Aggregation. ELAA extends Core Log Aggregation by integrating search capabilities, custom security alerting, threat hunting, trend analysis, proactive log review analysis, and monthly security monitoring reporting. ELAA's security analysis capability enables correlation of events across multiple log sources, improving incident identification for customer security stakeholders.

AI and ML in ELAA:

Our monitoring process uses AI and ML to identify patterns, anomalies, and issues requiring security analyst attention. Detection patterns are optimized based on intel and emerging threats. ELAA security analysts continuously refine and tune AI and ML-based alerts to eliminate false positives.

ELAA and Regulatory Requirements:

ELAA adopts a risk-based, governance approach to determine required log ingestion to meet compliance requirements, considering relevant audit and security policies and NIST guidance. ELAA handles both regulated and non-regulated customers.

ELAA Triage:

ELAA Triage follows defined processes according to severity levels. Security analysts review alert data, perform secondary log searches and data gathering, and develop recommendations if appropriate before notifying appropriate stakeholders for awareness and follow on actions.

ELAA Alert Notification Workflow:

Below is the ELAA alert notification process that is followed when an alert is triggered.

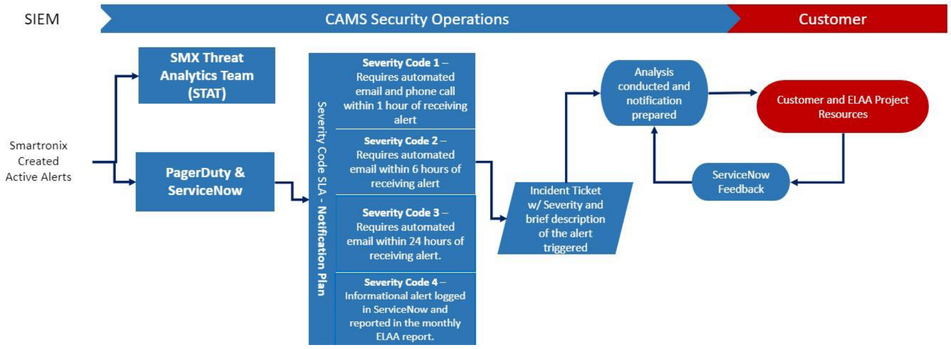
SIEM
CAMS Security Operations
Customer
Smartronix Created Active Alerts
SMX Threat Analytics Team (STAT)
PagerDuty & ServiceNow
Severity Code SLA - Notification Plan
Severity Code 1 – Requires automated email and phone call within 1 hour of receiving alert
Severity Code 2 – Requires automated email within 6 hours of receiving alert
Severity Code 3 – Requires automated email within 24 hours of receiving alert.
Severity Code 4 – Informational alert logged in ServiceNow and reported in the monthly ELAA report.
Incident Ticket w/ Severity and brief description of the alert triggered
Analysis conducted and notification prepared
Customer and ELAA Project Resources
ServiceNow Feedback

Figure 1

ELAA includes the customer in the process to ensure we meet their requirements and our own.

ELAA Monthly Reporting and Meeting:

The ELAA service offers a monthly report, detailing trends and analyses based on data from triggered alerts and non-alert generating events. This report serves as the foundation for a monthly meeting between the client and their primary analyst to review findings and discuss any relevant issues, such as customer concerns or new threat use cases.

ELAA Threat Hunting:

ELAA Analysts are US based and perform threat hunting in the environments as a part of their normal activities, these activities are done by looking at the data with a critical eye and running custom hunting queries devised by the team.

Notes:

- All the ELAA services are administered remotely.
- ELAA recommends, when starting out, providing as much logging as possible, if any of the logs are not needed the customer will be advised to stop sending those logs.
- ELAA also provides ad-hoc queries upon request from the customer.
- ELAA prefers to have independent logging with logs forwarded to the Elevate framework, however, client Security Information and Event Management tools can be integrated into the Elevate framework for an additional cost. Summary monthly reporting is provided.
- The shared responsibility model governs remediation actions. Elevate services that clients have subscribed to will be remediated by the SMX team. Elevate Services not subscribed to will be the client's responsibility. SMX will still provide recommendations for identified patterns, anomalies, and issues.

2.7.3 Host Intrusion Detection/Prevention

The Host Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) service offers 24/7 security event alerting, investigation, and response to potential security incidents detected by our endpoint HIDS/HIPS solutions. SMX's Host Intrusion Detection/Prevention service utilizes industry and partner-maintained signature sets, which are updated regularly. Our security team ensures that the most appropriate signature sets are applied to customer endpoints.

We operate the system in detect mode for a minimum of one month and switch to prevent mode only upon mutual agreement with our clients. When significant changes to the service occur, clients must submit ServiceNow tickets to initiate system transitions between detect and prevent modes. IPS events are sent to our Multi-tenant Security Information and Event Management systems, followed by ticket logging in the ServiceNow Portal, where notifications and escalations are activated based on severity.

Remediation actions follow the shared responsibility model. Elevate services that clients subscribe to will be handled by SMX, while the client is responsible for services not covered under Elevate. Nevertheless, SMX will continue to offer recommendations for intrusion incidents to aid clients in remediation. Our systems and security managed services engineers provide 24x7x365 support, extending the IT security capabilities of your team.

2.7.4 Host File Integrity Monitoring

The Host File Integrity Monitoring Service alerts you to changes in critical operating system and application files, as well as vital processes and ports. This integrity monitoring detects unauthorized changes that pose operational and security risks by identifying system incompatibilities and potential indicators of compromise.

Our FIM capability enables the service to deliver 24/7 alerts and responses to identified events. The identification of protected files can be tailored to address customer security concerns. Host File Integrity Monitoring Service necessitates the use of Elevate reporting services.

This service requires installation on a dedicated Trend Micro Deep Security tenant within Elevate. In environments lacking maturity or high stability, advisory professional services may be needed to collaborate with client workload and application owners to manage and approve changes, which may incur additional costs.

2.7.5 Application Control

The Application Control Monitoring Service alerts you to changes in key software on your protected servers. Based on your policy configuration, the service either prevents unauthorized software from running until explicitly allowed or permits unauthorized software until explicitly blocked.

This system operates in Maintenance or Enforcement modes. Maintenance mode enables the development and updating of the application inventory, while Enforcement mode actively blocks access and prevents unauthorized changes. Effective application control requires close collaboration with client workload and application owners to manage and approve changes smoothly.

In environments lacking maturity or high stability, advisory professional services may be needed to assist with mode changes from Maintenance to Enforcement at an additional cost. For complex environments and use cases, clients may need to incorporate mode changes as part of their CI/CD pipeline.

Autoscaling environments and workloads must be identified and declared, so additional instances that are scaled up utilize a shared and approved software inventory.

Our Application Control capability allows the service to provide 24/7 alerts and responses to identified events. The identification of protected files can be tailored to address customer security concerns.

2.7.6 Systems Vulnerability Scanning

The Systems Vulnerability Scanning Service facilitates assessments of networks and connected IT systems against regulatory compliance standards, identifying any known vulnerabilities. This solution offers automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery.

Monthly systems vulnerability scanning is conducted, with scan outputs analyzed by Security Compliance specialists to identify and remove false positive findings. Any identified vulnerabilities trigger the opening of a ticket in the ServiceNow Portal to initiate ITSM practices and are immediately reported to system and application owners for remediation. Findings are reported separately for impacted teams at the OS and application levels.

Clients can subscribe to, or request on a one-off basis, more frequent scans for all or select workloads at an additional cost, which is a multiple of the standard monthly per-instance fees.

Note: The standard template supported by the vulnerability scanning service is based on the Center for Internet Security (CIS) benchmarks. Additional standards and templates may be supported according to customer regulatory requirements.

2.7.7 Continuous Monitoring Security and Regulatory Compliance Support Services

Security and Regulatory Compliance Advisory Service utilizes SMX's security compliance experts to guide clients in meeting regulatory requirements and recommend mitigations for threats that could impact client-specific environments as they emerge and evolve. This professional service assists in documenting and updating control documentation to maintain customer regulatory compliance.

Examples of compliance activities include:

- Creating System Security Plans
- Supporting internal compliance audits
- Tracking Plans of Action and Milestones (POAMs)
- Conducting risk assessments and planning
- Monitoring and responding to industry regulatory changes
- Analyzing vulnerability scanning results

Elevate supports numerous compliance frameworks, such as NIST, FedRAMP, StateRAMP, HIPAA, HiTrust, PCI, MARS-E, GDPR, DOD RMF, SSAE-16, SAS-70, SOC2 Type x, and others.

3 SERVICE LEVEL AGREEMENTS

3.1 SLA 1: SYSTEM AVAILABILITY

SLA 1: "System" Availability	
Description	This SLA applies to "system availability" of a service. A system is considered a series of components that make up the infrastructure service that hosts and provides the compute and storage capabilities consumed by the customer applications and services. System availability applies to the following products and services: Virtual Compute Instances (AWS EC2 and Azure Virtual Machines deployed in the same availability set) Block Storage (AWS EBS, Azure System/Data Disks) SMX SLA incorporates the AWS and Azure SLA terms defined below which are subject to change in accordance with the AWS and Azure Agreements. AWS Compute SLA: https://aws.amazon.com/ec2/sla/ Microsoft Azure Compute SLA: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_6/
Measurement	SMX will measure system infrastructure availability by using tools that will access the cloud infrastructure compute availability at 5-minute intervals to analyze cloud IaaS regional compute availability.
Calculation	NUMERATOR Uptime (Seconds) ÷

SLA 1: “System” Availability	
	DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	SMX will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside SMX control and approved as such by customer. Examples of these type of exception events include: Force majeure events: and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

3.2 SLA 2: BACKUP AND RESTORATION

SLA 2: Backup and Restoration	
Description	This SLA measures the percentage of times that the platform is restored to the last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure. Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restorations within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	SMX will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA’s may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

3.3 SLA 3: OPERATIONAL EVENT RESPONSE

SLA 3: Operational Event Response Time	
Description	This SLA measures SMX’ response time, per the Exceptions/Conditions in this SLA, following issue identification.

SLA 3: Operational Event Response Time	
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incidents receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	SMX is successful if 95% of incidents receive a response within response time for given severity level, as measured monthly.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of the incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of the incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of an incident occurring during business hours. (8am-8pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No minimal user impact. Within one business day of an incident occurring during business hours. (8am-8pm EST M-F). Exception: Impending events; notification will happen; incident response will be initiated before follow-up notification as clients will be previously notified (SLA 5) of the likelihood of the event.

3.4 SLA 4: OPERATING SYSTEM PATCHING AND UPDATING

SLA 4: Operating System Patching	
Description	This SLA measures SMX' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied according to the client-planned schedule defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷ DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.
Success Criteria	SMX is considered successful when 95% of critical patches are applied to the initial environment within ten calendar days of release from vendor and

SLA 4: Operating System Patching	
	subsequent patches are applied per the customer patch schedule. Patches must be approved by the customer. This will be measured monthly.
Exceptions / Conditions	Description

3.5 SLA 5: IMPENDING EVENT NOTIFICATION

SLA 5: Impending Event Notifications	
Description	SMX will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying SMX of service degradation, service unavailability, or service termination.
Measurement	SMX will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of SMX control are not included.

3.6 SLA 6: IMPENDING SECURITY THREAT NOTIFICATION

SLA 6: Impending Security Threat Notifications	
Description	SMX will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new threats in the environment that may impact OS, Applications, or services used by Client.
Measurement	SMX will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of SMX control are not included.

3.7 SLA 7: SECURITY MONITORING NOTIFICATION

SLA 7: Security Monitoring Notification			
Description	SMX will notify the Client of the possibility of potential security incidents which may impact system security and/or operations. Examples include detections of successful security breaches, misuse, or suspicious activities associated with security monitoring use cases implemented by SMX.		
Measurement	SMX will measure security notification from the initial time that the incident was alarmed upon.		
	Severity	**Severity Categorization Description**	**Response Expectation**
	Severity 1: Critical	A production environment or system has been compromised or is at immediate risk of being compromised or disrupted. 1. or – Production systems have experienced a substantial degradation or loss of service 2. or – A substantial portion of confidential data within any environment has been compromised or is at significant risk of being compromised or – Mission operations have been severely disrupted	Issues an email notification to designees of the CSP and CSSP Teams within 1 hour of alert and calls the designees of the CSP and CSSP Teams to join and contribute to any incident response effort.
	Severity 2: High	A non-production environment or system has been compromised or is at immediate risk of being compromised or 1. Disrupted or – An environment or system is at significant risk of being compromised, disrupted, or degraded or – Business operations may be severely disrupted or	Issues an email notification and calls designees of the CSP and CSSP Teams within 6 hours of an alert.

SLA 7: Security Monitoring Notification			
	Severity 3: Medium	There is no immediate threat, indication of compromise, or sustained attack. However, there may be a smaller issue that could become a bigger issue in the future.	These cover a 24-hour window and only go off once a day at a set time, during regular business hours. Issues an email notification to the designees of the CSP and CSSP Teams within 24 hours of an alert.
	Severity 4: Low	There is no immediate threat, indication of compromise, or sustained attack. However, there may be a potential issue that should be noted for trends.	These are sent straight to the ticketing system. The contractor reviews alerts as part of the monthly report.
	Severity five	There are made up of items that would go straight to the customer or some other unique use case.	No response time required as they go straight to the customer.
Calculation	Best Effort. Time from the initial detection of the incident, until initial notification based upon severity.		
Success Criteria	Successfully achieving timelines based on severity by incident.		
Exceptions / Conditions	Events outside of SMX control are not included. Severity levels are established by mutual agreement between SMX and customer.		

*SLA usage can vary dependent on services purchased.

4 PRICING

COMMERCIAL ACCOUNT SERVICES

Service Title	Monthly Price	Notes
CSP Account Management Service	$2000/Account	This fee is per organization containing up to five managed accounts. Additional organizations or groupings of five managed accounts within a single organization each incur a fee.
Infrastructure Service Incident Management		
SLA Management		
Boundary Management		
Log Aggregation (Basic)		
Infrastructure Provisioning Service		
Serverless - Compliance, Logging, and Real-Time Monitoring		
Container Service Monitoring		

Table 3. Commercial Account Services

COMMERCIAL CORE MANAGED SERVICES

Service Title	Monthly Price	Notes
Monitoring and Notification	$300/instance	An instance is a system running in AWS that has an operating system capable of being patched or having an agent deployed. This can be an EC2 instance, or instances generated by another service, such as EMR, Docker host or Elastic Beanstalk. The monthly instance cost is calculated as the total instance hours in an account covered by the Account Services divided by 730 hrs. (the average number of hours in a month). To streamline service delivery, all AMI's will need to be configured with pre-defined management tools and tagging.
Operating System Patch Management		
Anti-malware Management		
Backup Service		

Table 4. Commercial Core Managed Services

*ELEVATE has a monthly minimal commitment of $10,000 across account, core, and cluster managed services.

COMMERCIAL OPTIONAL SERVICES

Service Title	Monthly Price	Notes

Cloud Service Expense Management Advisory Service	1.5% of Invoice monthly	A percentage of your entire cloud spend as shown on your CSP invoice, inclusive of all transaction types.
Infrastructure Advisory Services	Priced based on scope	
Database Monitoring	$100 per Database	
Workspaces Management Services	Per Workspace Instance $25 less than 150 Instances $22 for 151 through 300 $18 for 301 through 700 $14 Greater than 700	Provisioned Workspace as defined by AWS
Site Reliability Engineer (SRE)	Priced based on scope	
PODS and Squads Support	Priced based on scope	
AWS Managed Services Advanced	Current AWS List Pricing	
AWS Managed Services Accelerate	Current AWS List Pricing	

Table 5. Commercial Optional Services

COMMERCIAL OPTIONAL SECURITY SERVICES

Service Title	Monthly Price	Notes
Security Incident Response	Price based on anticipated LOE and frequency for the given customer environment, security maturity, and expected threats.	
Enhanced Log Aggregation and Analysis**	Log Monitoring and Analysis - $320/per GB of indexed data, based on average daily consumption in a calendar month.	Inclusive of the SIEM software required to deliver the ELAA service. Monthly minimums apply.
Enhanced Log Aggregation and Analysis – Customer provided platform	Log Monitoring and Analysis - $160/per GB of indexed data, based on average daily consumption in a calendar month.	The customer will provide the licenses and appropriate delegated access to the SIEM software (Splunk or SUMO) to be used by SMX resources to deliver this service.
Host Intrusion Detection/Prevention & Host File Integrity Monitoring	$40 per instance	An instance is a system running in AWS that has an operating system capable of being patched or having an agent deployed. This can be an EC2 instance, or instances generated by another service, such as EMR, Docker host or Elastic Beanstalk. The monthly instance cost is calculated as the total instance hours in an account covered by the Account Services divided by 730 hrs. (the average number of hours in a month). To streamline service delivery, all AMIs will need to be configured with pre-defined management tools and tagging.
Application Control	$20 per instance	An instance is a system running in AWS that has an operating system capable of being patched or having an agent deployed. This can be an EC2 instance, or

Service Title	Monthly Price	Notes
		instances generated by another service, such as EMR, Docker host or Elastic Beanstalk. The monthly instance cost is calculated as the total instance hours in an account covered by the Account Services divided by 730 hrs. (the average number of hours in a month). To streamline service delivery, all AMIs will need to be configured with pre-defined management tools and tagging.
Security Systems Vulnerability Scanning	$30 per instance / per scan $3,000 monthly minimum	An instance is a system running in AWS that has an operating system capable of being patched or having an agent deployed. This can be an EC2 instance, or instances generated by another service, such as EMR, Docker host or Elastic Beanstalk.
Continuous Monitoring Security and Regulatory Compliance Support Services	Priced based on scope	Professional Services

Table 6. Commercial Optional Security Services

**ELAA has a monthly minimal commitment of $8,000 per month or the total of cost based on average GB indexed per day in a one-month measurement period (based on calendar), whichever is higher.

Department of Defense IL 4 Managed Services **Service Title**	**Monthly Price**
Monitoring and Notification	$600/instance per month
SLA Management	
Incident Response	
Operating System Patch Management	
Host Based Antivirus (AV) Management Government Furnished Equipment (GFE) HBSS Software)	
Boundary Management	
Enhanced Log Aggregation and Analysis	
Backup Services	
Enhanced Data Encryption Services	
Assured Compliance Assessment Solution (ACAS) (GFE vulnerability scanning Software)	

Department of Defense IL 4 Managed Services **Service Title**	**Monthly Price**
Infrastructure Provisioning Service	$50/Provisioning Request

Table 7. Department of Defense IL4 Managed Services

PRICING NOTES:

1. Customized service/pricing for customer environments that have reduced requirements, e.g., Development, Test, Quality Assurance, or Labs is available.
2. SMX will reserve one AWS resource tag for use in the management of the resources.
3. An instance is a system running in the Cloud that has an operating system capable of being patched or having an agent deployed. This can be a standard compute instance (e.g., AWS EC2), or instances generated by other services (e.g., EMR, Docker host, or Elastic Beanstalk). The monthly instance cost is calculated as the total instance hours in an account covered by the Account Services divided by 730 hrs. (the average number of hours in a month). To streamline service delivery, all machine images will need to be configured with pre-defined management tools and tagging.
4. ELEVATE is deployed to customer CSP accounts via Terraform infrastructure as code templates. This enables SMX to expedite customer onboarding and to ensure quality through a templatized, tested, and automated workflow.
5. For AWS environments, clients are required to enable AWS Guard Duty, Security Hub, Config, CloudTrail, CloudWatch, network flow logs, and allow SMX to install AWS CloudWatch agent, AWS SSM agent, and AWS Inspector Agent on managed instances in regions that run services supported by SMX.
6. For Azure environments, clients are required to enable AWS Security Center, Log Analytics, Monitor, Application Insights, Azure Automation, Logic Apps, and Functions, Recovery Services Vault, Lighthouse, and Qualys in regions that run services supported by SMX
7. SMX ELEVATE will leverage a centralized IdP with MFA enabled login to gain access to the customer CSP account. All actions performed in the customer CSP account will be logged and retained in the customer account for audit purposes.
8. Micro services (AWS lambda) will execute service automation tasks within the account to enable instance monitoring, snapshots/backups, and creation of alarms to create event notifications.
9. Clients are responsible for notifying SMX immediately when they have received a Security notification from a Cloud Service provider or a creditable threat has emerged outside the MSP, MSSP monitoring services.
10. Clients are responsible for encryption of all data transmitted to SMX or in client defined storage environments.
11. Clients are responsible for maintaining Root Access and providing SMX Access to act as their agent with named accounts.