Insight Customer Account Number	10325365
Statement of Work #	4010060856
State/Fed Contract	Texas DIR-IT Outsourcing DIR-CPO-5030-61002175

Statement of Work

("SOW")

Parties and addresses for notice:

"Insight"	"Customer"
Company name: Insight Public Sector, Inc.	Company name: Hidalgo County
Primary contact: Steven Capps	Primary contact: Rigoberto Hinojosa
Address: 13755 Sunrise Valley Drive, Suite 750 Herndon, VA 20171	Address: 100 N. Closner Boulevard Edinburg, TX 78539
Phone number: 956.266.3867	Phone number:
Email: Steven.Capps@Insight.com	Email:

Agreed and accepted:

Insight	Customer
Authorized signature:	Authorized signature:
Name:	Name:
Title:	Title:
Date:	Date:

Invoicing procedures:

Method (Customer MUST select ONE option below.)	PO Process (Customer MUST select ONE option below.)
☐ **Mail Invoice** – Hard copy of invoice will be mailed to: Company name: Address: Attention: Accounts Payable or Accounts Payable Contact: Phone:	☐ **Customer issues system-generated POs or internal reference numbers for service engagements.** Please fill in the PO number below and attach a hard copy of the PO to this signed SOW. Note: Services cannot be performed until a hard copy of the PO is received, or a billing reference is provided. PO number: PO release number (if applicable): Internal billing reference number/name:
OR ☐ **Email invoice** – Invoice copy will be sent electronically via email to:	OR ☐ Customer does NOT issue system generated POs for service engagements. Accordingly, performance of and payment for any Services under this SOW do not require, and are not contingent upon, the issuance of any PO or other similar document.

This Statement of Work ("SOW") is effective as of the date last signed above ("SOW Effective Date") and subject to the Contract for End-User IT Outsourcing, DIR Contract No. DIR-CPO-5030-61002175 dated February 28, 2022, (the "Agreement") between Insight Public Sector, Inc. and State of Texas Department of Information Resources ("DIR").

1. Purpose

The purpose of this SOW is to set forth the specific Services that Insight will provide to Customer in connection with the Agreement.

2. Definitions

a. “Deliverables” means the items created by Insight in connection with the Services and as specifically described in the Scope of Services and Delivery Schedule Section below

b. “Services” has the meaning given to it in the Scope of Services and Delivery Schedule Section

3. Scope of Services and Delivery Schedule

Insight will perform the following services (“Services”) per the terms of this SOW.

3.1. Service Description

The following is a high-level description of the Services Insight will provide:

1. Security Operations Management Services as outlined in the Exhibit(s) of this SOW.

3.1.1. Location

Performance of the Services will be remote.

3.2. Project Management

Insight will provide project management as detailed in the applicable Exhibit of this SOW.

3.3. How Services are Accepted

After Insight performs a Service or delivers a Deliverable to Customer, if the Service or Deliverable does not meet the material requirements described in the SOW, then Customer will provide Insight with a written explanation describing how the requirements were not met within 5 days following the date the Service or Deliverable was delivered to Customer. If Customer fails to provide the written explanation within this 5-day period, the Service and Deliverable will be deemed accepted by Customer.

3.4. Business Hours

Services will be performed during normal United States business hours unless otherwise mutually agreed upon in the attached Exhibit(s). Normal business hours are defined as an 8-hour day, Monday through Friday, excluding designated Insight Holidays.

3.5. Customer Responsibilities

Customer is responsible for the following:

1. Customer will provide a project contact with decision-making authority to support the scope of services described in this SOW and ensure the proper personnel are scheduled to review each completed Service or Deliverable upon notification of completion by Insight.
2. If applicable, Customer will provide site contacts for each Customer location. Each such contact will provide Insight with sufficient detail regarding his/her site, and will coordinate or perform required onsite work, as reasonably requested by Insight and Customer IT, for the duration of the project.
3. Customer will provide Insight the necessary access to its internal experts, location(s), critical systems, applications, workspace, and equipment required at each field location to complete the project. Access to Customer systems will be provided to Insight via either onsite direct access or remote/VPN access. If Customer cannot provide access or required resources under this SOW, then additional project duration, labor hours, travel expenses, and other costs may be incurred and due to Insight by Customer.
4. Customer will provide the necessary hardware, software, tools, and permits required for the successful completion of the project prior to Insight’s arrival. Further, Customer is responsible for all licensing requirements to be compliant per their own agreements.

5. Customer is responsible for all product and material, including distribution and transport of Customer-owned product and material, unless otherwise specified in writing. Product and material are defined as any items purchased, owned and/or provided by Customer (or others) that Insight is required to use for fulfillment of any Services described herein.
6. Customer is responsible for providing adequate and secure onsite storage for all Customer-owned product and material unless otherwise specified in writing.
7. Customer will be responsible for managing and maintaining, if applicable: (a) back-up and/or data migration of existing data and Customer's information unless otherwise agreed to by Insight; (b) computer system and network designs; (c) component selection as it relates to the performance of the computer system and/or the network; (d) reasonable firewalls and if appropriate encryption; (e) least-privileged-based access controls (including provisioning, de-provisioning, authentication, authorization, and accountability controls); and (f) physical, electronic, and procedural controls to ensure the confidentiality, integrity, and availability of Customer's information on all applicable Customer computing systems used to store or transmit Customer's information, in accordance with current applicable industry standards and best practices.
8. Customer and its employees, contractors, and agents will: (a) cooperate with any reasonable request of Insight, (b) provide input throughout the project and will review progress at review meetings requested by Insight; and (c) provide Insight with access to all of Customer's information, documentation, and technology, necessary for Insight to perform the Services, including a list of all Customer and third-party contacts necessary for Insight to do so.

3.6. Assumptions

1. If applicable, any onsite skills transfer that takes place during this project will not replace the manufacturer's formal system implementation and administration classes.
2. Outside the scope of this SOW, Insight has no obligation to mount, affix, or otherwise fasten any cable, hardware, or other product to any building or structure (inside or outside), and Insight has no obligation to run cable above, under, behind, or through any ceiling, floor, or wall of any building or structure. If such services are requested by Customer, such services may be performed by Insight only to the extent permitted by applicable law and will be subject to a Change Request for additional services.
3. Each party agrees that personnel will not be asked to perform, nor volunteer to perform, engineering and/or consulting tasks that lie outside the skill sets and experience of personnel. Personnel have the right to decline a service request if the request falls outside their scope of experience and expertise.

3.7. Change Request Procedure

If either party identifies any alterations to the scope of work, specifications, or requirements in this SOW, it shall be brought to the attention of the other party's management for pre-authorization by completing and submitting a written Change Request in a manner described in this section and signed by both parties ("Change Request Form").

Without limitation, Change Request Forms are appropriate in the following examples, as well as other situations that alter the scope of work, specifications, or requirements in this SOW:

- Changes to environment, scope, management, performance of projects (regular and special), milestones, tasks, systems, service levels
- Additional resources, scope, projects, new services, tasks
- Changes to management and control of hardware and software
- Adjustments to baselines, assets, volumes, or other areas where changeover time results in the need to adjust pricing
- Additions, deletions, and/or changes to sites where services are provided, or the nature of services provided at a site

If any such change causes an increase or decrease in the cost or time required for the performance of the Services, the price and/or delivery schedule shall be equitably adjusted and identified within the Change Request Form.

If Insight believes an operational change is required and Customer does not agree to the change (or the applicable Change Request), Insight will be relieved of any related service level obligations. Any additional resources or costs expended or incurred to address the failure to make the change will be treated as an additional service.

3.8. Project Kickoff

A project kickoff meeting will be held to review project expectations, discuss IT infrastructure design, discover any possible problems/risks, and formulate an appropriate plan (including a firm engagement schedule and downtimes).

3.9. Start Date

The project start date will be mutually determined upon receipt of this signed SOW and, if applicable, a valid Purchase Order (PO). A minimum lead time of at least 20 business days from receipt of both documents may be required for scheduling purposes.

If Customer causes any delays to the delivery start date, which was agreed upon by both parties in writing (email is acceptable), Customer may incur additional fees based upon such delay, including but not limited to, travel expenses already incurred, if any, and/or other equitable relief as a remedy for such delay. The delays and charges will be defined and communicated through the Change Request process described in this SOW.

Services will be performed over a consecutive timeframe unless otherwise provided herein. If Customer requests or causes a change in the schedule that prohibits Services from being delivered in a consecutive timeline, an additional lead time of 20 business days (from written confirmation to resume Services) may be required, new resources may be assigned, and there may be additional fees.

3.10. Estimated Duration

The Services' duration will be approximately 52 weeks.

3.11. Fixed Fee

Customer shall pay Insight the fixed fee of **$167,868.00**. The total amount paid to Insight will not exceed the total fixed fee without the prior written approval of Customer. Customer will not reimburse Insight for travel expenses, if any are required.

The fixed fee is based on the following:

Description	Monthly Fee	Term	Total Fee for Term
ProVision SIEM-as-a-Service Monitoring and Management (251-300 Employees) • Monitoring and Management (MA4) - Palo Alto PA-850 NGFW (w/WF, TP, URL Filt, GP, DNS Sec) • 1 Monitoring and Management (MA4) - Cisco ASA 5514-X • 1 Monitoring and Management (MA4) - Palo Alto PA-220 NGFW • 1 Monitoring and Alerting Aruba ClearPass (Central Management Appliance w/ 10 APs) • 15 Monitoring and Alerting as applicable for route/switch (Aruba, Cisco, HP) **Consulting-as-a-Service (MA2 and MA4)** Time and material Consulting Services based on the services listed in the Service Scope. Year 1 – 50 Hours	$5,489.00	12 months	$65,568.00
Subtotal Year 1:			**$65,868.00**

SIEM-as-a-Service (MA2 and MA4) (251-300 Employees) • Monitoring and Management (MA4) - Palo Alto PA-850 NGFW (w/WF, TP, URL Filt, GP, DNS Sec) • 1 Monitoring and Management (MA4) - Cisco ASA 5514-X • 1 Monitoring and Management (MA4) - Palo Alto PA-220 NGFW • 1 Monitoring and Alerting Aruba ClearPass (Central Management Appliance w/ 10 APs) • 15 Monitoring and Alerting as applicable for route/switch (Aruba, Cisco, HP) **Consulting-as-a-Service (MA2 and MA4)** Time and material Consulting Services based on the services listed in the Service Scope. Year 2 – 20 Hours	$4,250.00	12 months	$51,000.00
Subtotal Year 2:			**$51,000.00**
SIEM-as-a-Service (MA2 and MA4) (251-300 Employees) • Monitoring and Management (MA4) - Palo Alto PA-850 NGFW (w/WF, TP, URL Filt, GP, DNS Sec) • 1 Monitoring and Management (MA4) - Cisco ASA 5514-X • 1 Monitoring and Management (MA4) - Palo Alto PA-220 NGFW • 1 Monitoring and Alerting Aruba ClearPass (Central Management Appliance w/ 10 APs) • 15 Monitoring and Alerting as applicable for route/switch (Aruba, Cisco, HP) **Consulting-as-a-Service (MA2 and MA4)** Time and material Consulting Services based on the services listed in the Service Scope. Year 3 – 20 Hours	$4,250.00	12 months	$51,000.00
Subtotal Year 3:			**$51,000.00**

3.11.1. Invoicing

Insight will invoice Customer monthly for Services performed based upon a percentage complete, plus any taxes incurred (if applicable).

Customer will be required to pay each invoice within 30 days from the date that Customer receives the invoice, per Texas Government Code, chapter 2251.

3.12. Pricing Notes

1. Pricing offer is valid for 30 days from the date a copy of this SOW is first presented to Customer. This SOW must be executed and returned to Insight by Customer within such 30-day period or pricing will expire.

2. Travel expenses, if applicable, are not reimbursable.
3. Pricing and estimated time to complete this engagement are based upon Customer providing necessary access to internal experts, location(s), all critical systems, applications, and hardware required to complete the project. Any additional requirements, including without limitation, additional screening, background check, vaccination or covid-related requests and other out-of-scope or previously undisclosed resource-related requests may result in Service commencement or completion delays and additional fees.
4. Customer acknowledges that cancellation of this engagement may cause Insight to incur non-refundable pre-approved travel expenses and other costs. Accordingly, if Customer cancels this engagement, Customer shall pay Insight the fees set forth below. Such cancellation shall be in writing and shall be effective when received by Insight.

Cancellation Period	Cancellation Fee
Less than 3 business days prior to start of engagement	100% of total cost of engagement OR $12,500.00, whichever is less
Between 3 and 10 business days prior to start of engagement	10% of total cost of engagement OR $2,500.00, whichever is less
More than 10 business days prior to start of engagement	None

5. Insight is not responsible for delays or repeated tasks caused by factors outside of Insight's control. These factors include, but are not limited to, availability of Customer personnel, equipment, and facilities.

3.13. Customer Work Product

All results of the Services described in and delivered pursuant to this SOW, including Deliverables and Customer's proprietary information contained therein, authored or created by Insight specifically for Customer as a Work Made for Hire, excluding any Insight IP incorporated therein ("Work Product"), will be and remain the property of Customer. Insight retains all right, title, and interest in, without limitation, any intellectual property rights in works of authorship, know-how, or any invention, device, process, method, development, design, specifications, technique, apparatus, reports, schematic, or technical information (whether patentable or not), documentation, software or enhancements, improvements, alterations, interfaces, workflows, and best practices developed, invented, created, or reduced to practice by Insight and used for the Services, including any derivatives or modifications ("Insight IP"). To the extent Work Product includes any works of authorship that are Insight IP, Insight grants Customer a nonexclusive and non-transferable license to use each such portion of the Work Product for its internal business purposes, provided that no Insight IP may be unbundled or separated from the Work Product or used on a stand-alone basis.

4. Exhibit – Project Management

Insight will provide the following project management and technical direction:

Project Manager

- Serve as the primary point of contact on all project issues, needs, and concerns
- Provide team leadership and guidance
- Facilitate kickoff meeting to review scope and project expectations, discuss IT infrastructure design, assess Customer readiness (hardware, software, infrastructure pre-requisites, etc.), discover any possible problems/risks, formulate an appropriate work breakdown structure for primary project tasks, and create project timeline/schedule (including potential downtimes and maintenance windows)
- In conjunction with Customer, measure and communicate weekly progress against mutually agreed-upon milestones
- Maintain a project log proactively to identify and communicate key decisions made, action items to be completed, risks/issues that may impact scope, schedule, and lessons learned; and mitigate and/or escalate any critical risks or issues under Insight's control, as needed
- Manage Customer expectations and satisfaction throughout the life of the project
- Schedule and coordinate the necessary resources to support the project
- Schedule and conduct project team update/status meetings
- Prepare written status reports for Customer at mutually agreed-upon intervals
- Monitor, manage, and communicate changes to the project's scope, budget, schedule, and resources; complete Change Request (CR) documentation as required; and obtain signed CRs for mutually agreed upon changes
- Facilitate closeout meeting, as needed

4.1. Project Contacts

Contact Name	Contact Email
Customer Sponsor - Rigoberto Hinojosa	
Customer Executive - Steven Capps	Steven.Capps@Insight.com
Services Manager – Jennifer Pless	Jennifer.Pless@Insight.com

5. Exhibit – Network Operations Support Services

5.1. Service Description

The following is a high-level description of the Services Insight will provide:

ProVision SIEM-as-a-Service

The ProVision SIEM-as-a-Service has 2 levels supporting Co-Managed and Fully Managed, as outlined in the table below:

Managed Service	MA2 Monitored	MA4 Co-Managed
Security Information Event Monitoring	✓	✓
ProVision Security Suite Portal	✓	✓
Log Storage and Analysis	✓	✓
Reporting	✓	✓
Alerting	✓	✓
Notification and Escalation	✓	✓
24x7x365 Analysis and Alerting	✓	✓
Full r/w access to infrastructure	✓	
Incident Remediation		✓
Change Requests		✓
System Upgrades*		✓
System Configuration Backup**		Option

*System Upgrades are included for minor upgrades that can be performed remotely. If onsite work is recommended and required, this will be covered by an additional SOW.

**Backups of the Device/Asset are the responsibility of the Customer. At Customer request, Vendor will perform a manual configuration backup prior to implementing any Change Requests, subject to the technology allowing it.

Consulting-as-a-Service (Bucket of Hours)

The Customer may draw upon the block of hours stated in the Pricing Section in order to complete projects from the Service Scope below on an as time allows or time and materials basis. Should the block of hours be consumed, the Customer may execute a change order to purchase more hours. The available Consulting-as-a-Service options are described in more detail in section 6.2.2 below.

5.2. Scope and Approach

Insight will perform the following Services:

5.2.1. SIEM-as-a-Service (MA4)

Monitoring

- Monitoring Service delivers real time cybersecurity monitoring providing visibility of cyber threats with actionable intelligence through analysis of the log stream from the Device/Asset under Service. The log source will vary dependent on technology but is typically syslog. Monitoring will be conducted 24/7/365. Customer shall make available log feeds for monitored devices, which will be sent to the on premise collector, VisionLink

Management

- Provide remote management services for the Device/Asset that include policy updates, rule-base changes and any configuration changes as required for the operation of the service

  - Co-Managed (MA4) means that the Customer and Insight will have the same full access to the Device/Asset to perform any changes as appropriate. If the Customer does make any changes to the Device/Asset, it should be logged within the Pro-Vision Portal using a Change Request Ticket to keep track of all updates. Customer can use a combination of Customer implemented and Insight implemented changes throughout the lifetime of the Service

- All activities will be implemented remotely. In the event of issues that require physical or local access to the Device/Asset, a Customer resource may be required for assistance to trouble shoot (e.g. system rebuild, power-cycle, reboot or console access)

Alerting and Escalation

- Log streams collected by VisionLink are parsed, normalized, and sent to the Pro-Vision threat engine for additional analysis. The business rules in the threat engine raise any suspicious logs or patterns of behavior to an Event. Event conditions that have been determined as a threat will be brought to the attention of the Customer's designated POC(s) by the creation of a Ticket within Pro-Vision
- Events are classified in to 4 severities;
  - ***Emergency*** – Existence of conditions which indicate a potential security incident has occurred
  - ***Critical*** – Existence of conditions which indicate the presence of a potential security threat requiring attention
  - ***Warning*** – Potential Incidents that may have been averted but warrant investigation and confirmation
  - ***Informational*** – System and vendor information to bring additional context to higher priority Events
- Track incident progress within the Pro-Vision Ticket. The SOC will also call the Customer for P1 incidents. Other priority incidents may be called depending on the severity and criticality of asset involved. Communication preferences are confirmed during Onboarding and can be adapted throughout the lifetime of the Service

Ticketing

- Ticket types include but are not limited to the following; Security Incident, Support Ticket and Change Request. The assignee of a Ticket will always be an SOC representative and if the status of the Ticket is set to "Waiting for Customer', then the progress of the Ticket is the responsibility of the Customer's designated POC(s)
- Tickets have 4 severity levels as below:
  - ***P1 Emergency*** – System down or potential security Incident that warrants urgent attention
  - ***P2 Critical*** – Significant impact that could lead into a security Incident or system outage if not addressed
  - ***P3 Warning*** – Moderate loss of functionality or security that should be addressed
  - ***P4 Informational*** – Supporting information and notification of behavior
- The SOC Analyst will work closely with the Customer's designated POC(s) to progress and resolve the Ticket where appropriate
  - If the Customer doesn't respond to the Ticket in a timely manner, reserves the right to close the Ticket and tune out the logs to stop it reoccurring
- Tickets can be updated/progressed within the Pro-Vision Portal or via email by responding to the Ticket update email that will get sent to all those set as a 'Follower' within the Ticket. 'Followers' can be automatically assigned for all Customer Tickets or individually depending on the actual Ticket. 'Followers' are confirmed during Onboarding and can be adapted throughout the lifetime of the Service

Log Retention

- Pro-Vision security stream data consisting of processed log information (Alerts) for a minimum period of 1 year unless otherwise specified in the Service Initiation Document (SID). 90 days of Alerts are available and searchable online in the Pro-Vision Portal with the additional 9 months being stored on offline storage. Additional storage requirements are available on request

Additional Checks

- Apply additional checks to a Device/Asset depending on requirement. These checks include ICMP (Ping), HTTP, HTTPS, and SSH. Any additional checks are confirmed during Onboarding and can be adapted throughout the lifetime of the Service

5.2.2. Pro-Vision Portal

Customer will have access to the Pro-Vision Portal for access to the Service. The Portal is the interaction between the SOC Analysts and the Customer. Through the Pro-Vision Portal, Customer can:

- View Dashboards for summary of Service
- Manage Devices/Assets and system inventory
- View and search Alert logs and Events
- View and update profile information
- View and update Customer information
- Access Reports
- Search, update and manage all types of Tickets
- Access appropriate Knowledge Base articles

The Pro-Vision Portal has a multitude of preconfigured reports. Reporting is very flexible, including custom and quick date ranges, Device/Asset or Account information, tabular or graphical view in a variety of different formats including bar graphs, line graphs, heat maps and more.

Reporting includes but is not limited:

- Monthly Management Report (Overview of Service for the monthly period)
- Estate (Users, Managed Assets/Devices)
- Tickets (Management Report, Support Tickets, Security Tickets, Change Requests)
- Authentication (Management Report, Summary Report, By User, By Device, By Disabled Accounts)
- Accounts (Created, Disabled, Deleted, Enabled, Locked, Password Activity)
- Security Analysis (Management Report, Events, Log Messages, Anti-Virus, Policy Changes)
- Traffic (Management Report, Dropped Traffic, By Source, By Destination, By Destination Port)

Additional Reports can be requested during Onboarding and can be adapted throughout the life-time of the Service (subject to availability of data). With the aim of continuous improvement, reports in the Pro-Vision Portal may be added, removed or changed as needed.

5.2.3. VisionLink

All Pro-Vision managed services require VisionLink, which works as the log collector. VisionLink is typically located on the Customer site and receives the log stream of the Device/Assets associated with the Service. VisionLink is provided as a VM installation.

VisionLink VM

The VisionLink VM will either be an image provided to the Customer for installation or Customer will provide the resources in a VM for Insight to install the VisionLink Agent. Specifications for the VM will depend on the number of Devices/Assets in the Service and will be worked out during Onboarding but is typically Quad-core, 1TB HDD and 4GB Memory. The VisionLink agent is installed on Ubuntu 16.04 LTS (or later approved system). It is the Customers responsibility to ensure that the VM is available for the Service.

5.2.4. On-Boarding

- Work with the Customer to bring all Devices/Assets in to live Service during the On-boarding process. This is typically 30-60 days but will depend on the size of the estate and commitment of resources. The Onboarding consists of 2 parallel streams:

- ***Technical*** – to set up the infrastructure required for the service. This includes; Installation of VisionLink, collection of logs, creation of Events and Tickets, Portal training.
- ***Information Gathering*** – to provide as much context as possible to enrich the analysis. This involves either completing a document or online tool to gather all the required information to set up the Service. Areas covered are contact details, facilities, network design, topology, platforms, apps and users.

Once the Onboarding is complete, the Service is considered live. All this is handled and communicated through the Onboarding Process.

5.2.5. Service Level Agreement

There are 3 targets measured for the SLA as follows:

- ***Availability of the Pro-Vision Portal***
- ***Events*** - Time to respond and target to address
- ***Tickets*** - Time to respond and target to address (Support and Security Incident Tickets)
  - 'Time to Respond' is measured from when the Event or Ticket is created to when it is first touched by a SOC Engineer
  - 'Target to Address' is the target time for the analysis of an Event
  - 'Target to Resolve' is the target time to implement a workaround or fix for the Ticket

Availability of the Pro-Vision Portal

The Pro-Vision Portal is guaranteed available 99% of the time over a one-year period and measured annually.

Events

Priority	Time to Respond	Target to Address
P1 Emergency	15 mins	1 hour
P2 Critical	30 mins	2 hours
P3 Warning	2 hours	8 hours
P4 Informational	n/a	n/a

Tickets

Priority	Time to Respond	Target to Resolve
P1 Critical Impact	1 hour	TTR + 4 hours
P2 Significant Impact	4 hours	TTR + 8 Hours
P3 Normal/Minor	24 hours	72 hours
P4 Low/Information	48 hours	7 days

SLA Exceptions: The following exclusions are not included in the SLA calculation:

- Scheduled maintenance work as required
- Change management requirements affecting managed devices
- Circumstances beyond Insight or our Partner's reasonable control
- Changes to a managed device not performed by Insight or our Partner
- Loss of connectivity due to Customer connectivity issues or Customer managed issues

SLA Failure Rebate: At Customer's request, Insight will pay a rebate each year (following each 12 months of service) in the format of a service credit which can be used to purchase additional services or extend the service period if the SLA has not been met. Customer must log the request for a rebate as a Ticket in the Pro-Vision Portal within 30 days of the proposed missed SLA. Total service credit Rebates cannot exceed 10% the total annual service charge.

Measure	Credit
Availability of the Pro-Vision Portal	Half a day service credit for every whole hour the SLA is missed
Events (Response)	1 hour service credit for every P1 or P2 Event that misses the Response SLA
Tickets (Response)	1 hour service credit for every P1 or P2 Ticket that misses the Response SLA

Maintenance Window: With the unique Pro-Vision infrastructure, it is very rare that Maintenance Windows are required that incur an interruption to the Portal or Service. Should there be a requirement for a period to conduct any maintenance, Insight's Partner reserves the right to communicate that Maintenance Window in advance through the notification system in the Portal.

Hours of Operation: The Pro-Vision SIEM-as-a-Service is delivered through Insight's Partner's Global Security Operations Centers (SOCs) which operate 24 hours per day, 7 days per week, and 365 days per year.

Language Support: All Services, Portal and communications are provided in English language only.

Service Scope – Consulting-as-a-Service (Bucket of Hours)

The Customer may draw upon the block of hours stated in the Pricing Section in order to complete projects from the Service Scope below on an as time allows or time and materials basis. Should the block of hours be consumed, the Customer may execute a change order to purchase more hours.

5.2.6. Executive Advisory

Virtual CISO (vCISO / vCSO /vCCO / vDPO)

Team of experienced practicing CISOs with decades of security leadership and strategy development experience. This service utilizes the consultants experience to coach, mentor, or assist our customers in aligning their security program to meet the business needs. Services can be selected from the following:

- Metrics development
- Strategy development
- Board, management team, and security team coaching
- Vendor product and service evaluation and selection
- Maturity modeling operations and engineering team processes, capabilities, and skills
- Board and management team briefings and updates
- Operating and capital budget planning and review Vendor

Security Advisory

The Security Advisory Service Program services can be selected from the following;

- On Demand Security Experts to provide IT Security, Compliance and Privacy consulting
- Gap Analysis for specific compliance and/or security best practice
- Gap Remediation Assistance
- 3rd Party Vendor and Product Evaluations
- Policy and Procedure Development
- PRE-IR Services
- Vulnerability Management Program Development
- Patch Management Program Development

Compliance Advisory

The Compliance Advisory Service Program services can be selected from the following:

- **PCI Gap Assessment**: A review of Customer's current PCI compliance stance through interviews, documentation review, and minimal controls validation

- **PCI Audit**: A complete PCI audit utilizing the latest released DSS version (currently 3.2) for auditing organizations PCI environment(s) for compliance against documented requirements
- **HIPAA Gap Assessment**: A review of current controls and gaps as compared to HIPAA requirements
- **HIPAA Audit**: A complete HIPAA audit
- **ISO Gap Assessment**: A review of current security gaps as compared to ISO 27001
- **GDPR Gap Assessment and Validation**: General Data Protection Regulation scope identification, readiness assessment and validation (AOC) services
- **NIST Gap Assessment**: A gap review of an organizations security posture as it relates to NIST CSF, 800-53 R4 and other NIST documentations
- **CIS Top 20 CSC Gap Assessment**: A gap review of an organization's current security controls against the Center for Internet Security Top 20 list of security best practices
- **Firewall Configuration Review**: A best practices review of current firewall configurations
- **Policy Audit**: A review of documented polices compared against a variety of standards and compliance bodies

Incident Response Development

- **Incident Response Program Development**: Assist in developing an internal incident response program that utilizes current capabilities, development of increased internal skills and knowledge, solutions gap and remediation plans, and roadmap for program maturation
- **Incident Response Gap Assessment**: Analyze the current people, processes, and technology of an organization as it pertains to each phase of the incident response life-cycle
- **Incident Response Plan/Playbook Development**: Assist in developing organizational Incident Response documentation based off of interviews of pertinent personnel, review of controls in-place, and our experience in delivering Incident Response services

Network Security Testing

- **Network Vulnerability Scanning**: Testing specifically targeting authenticated or unauthenticated scanning activity
- **Network Vulnerability Assessment**: Framework execution of discovery of active devices within owned/utilized IP range(s), automated vulnerability scanning from an unauthenticated perspective, manual identification of vulnerabilities, and manual validation of identified vulnerabilities
- **Network Penetration Testing**: Includes all steps performed during network vulnerability assessment testing, but includes exploitation attempts to gain access to device operating systems and/or to sensitive data within the network environment

Security Application Testing

- **Web Application Security Testing**: OWASP framework testing of web-based applications from either an authenticated or unauthenticated perspective. Tests are performed with intent to identify vulnerabilities that may be exploited to affect users of the application or to gain access to the backend server or data
- **API Security Testing**: OWASP framework testing of web-based applications from either an authenticated or unauthenticated perspective. Tests are performed with intent to identify vulnerabilities that may be exploited to affect users of the application or to gain access to the backend server or data
- **Mobile Application Security Testing**: OWASP framework testing of web-based applications from either an authenticated or unauthenticated perspective. Tests are performed with intent to identify vulnerabilities that may be exploited to affect users of the application or to gain access to the backend server or data
- **Wireless Security Assessment**: Testing of in-place wireless networks with attempts to gain access to secured/unsecured networks and devices and data that reside within the affected networks

Personnel Security Testing

- **Email Phishing**: Email campaign(s) utilized to identify weaknesses in employee security awareness in regard to email reception and actions executed as requested in the campaign email

- **Phone Social Engineering**: Phone campaign(s) to identify weaknesses in employee security awareness in regard to actions performed and information provided during the campaign phone call
- **Physical Security**: Attempts are performed to gain physical access to facilities, devices, and data that are owned by the Customer. This may be performed from a review or assessment perspective

Adversarial Simulation Services

- **Red Team Services**: Simulated adversarial attack against an organization with no knowledge approach and limited communications during the engagement, with attempts to circumvent the organizations technical and physical controls
- **Insider Threat/Assumed Compromise Testing**: Delivery personnel will simulate employee access within the organization (or that of a set of compromised credentials/user device) to identify what a malicious internal attack would look like. Attempts to be made to not be identified by internal security personnel or security solutions

5.2.7. Out of Scope

1. The following are considered out-of-scope and are not part of the Services:
    a. Electrical or cabling services
    b. Formal user training
2. Services and Deliverable items not expressly described in the Scope and Approach section is considered to be out of scope. Any out-of-scope items must be pre-authorized and verified by Insight in writing through the Change Request process.

5.3. Deliverables

Project Manager

- Communications/escalation contact list
- Weekly status reports on the progress of the project