Cybersecurity - SecuLore Service Guide

Version 2025.04.21

Contents

1. Introduction

This Service Guide describes the different cybersecurity services offered by SecuLore Solutions, LLC ("SecuLore") and resold by Intrado, each as detailed more fully herein (collectively, "Services").

2. Services Overview

2.1. Managed Services

2.1.1. CyberSight™

CyberSight
CyberSight includes remote management, data storage, and access to SecuLore's 24x7x365 Cyber-SOC; alerts the End-Customer's team to vulnerabilities based on custom sensitivity levels; and SecuLore's Cyber-SOC Analysts perform daily checks and provide reports to aid the End-Customers' team in improving their network. With these techniques, the End-Customers can more easily adjust their firewall to blacklist cyber-threats and prevent an attack before it occurs. End-Customers can choose the option of weekly, monthly or semi-annual reports.

Tiers available:
All tiers include the same deliverables detailed below with the only difference being the reporting and meeting frequency.

- Premier – Weekly reporting and weekly availability to End-Customer's dedicated SecuLore SOC Analyst
- Signature – Monthly reporting and monthly availability to the End-Customer's dedicated SecuLore SOC Analyst
- Core – Semi-annual reporting and semi-annual availability to the End-Customer's dedicated SecuLore SOC Analyst

Deliverables:

- **24x7x365 Cybersecurity Monitoring**
  CyberSight uses SecuLore's technology designed for Public Safety by their team of cyber experts. This technology combined with SecuLore's 24x7x365 Cyber-SOC, provides the ability to monitor the End-Customer's networks for vulnerabilities.
- **SOC Cyber Threat Analysts**
  SecuLore's Cyber-SOC engages in ongoing threat analysis utilizing a range of tools, and researches the latest cyber threats to implement them into the End-Customer's alert platform. SecuLore's analysts learn the baseline of the End-Customer's network and are their partners in identifying & resolving vulnerabilities.
- **Dedicated SOC Analyst**
  CyberSight includes a dedicated analyst who helps the End-Customer baseline their network and becomes an extension of their team. This analyst will be available for meetings to go over the End-Customer's report at the same cadence as their report delivery: weekly, monthly or semi-annually.
- **Forensic Event Logging**
  SecuLore's technology enables their Cyber-SOC to save off raw packet data to an encrypted drive in the event of a cyber-attack.

- **Reports**
  Seculore sends the End-Customer an in-depth vulnerability report with remediation recommendations weekly, monthly or semi-annually depending on the tier selected.
- **Nationwide Public Safety Cyber Threat Awareness**
  Seculore is deployed across the US in small, medium, and large ECCs. This provides the End-Customers with a unique viewpoint of the threats against Public Safety infrastructure and gives the End-Customer the opportunity to enhance their alert methodology and threat analysis on a daily basis based on active threats to the End-Customer's market.
- **Ongoing Incident Escalation and Response**
  SecuLore's Cyber-SOC actively evaluates every alert that is raised, determines if and what type of escalation is required, and responds accordingly to the End-Customers with actionable remediation guidance.
- **Prioritized Action Items**
  Prioritized actionable remediation recommendations are included in every report delivered to the End-Customers and in the event of a critical alert being raised by their technology.
- **Custom Cybersecurity Alerts**
  Seculore immediately contacts the End-Customers for urgent vulnerabilities found in their network based on their custom sensitivity levels.

2.1.2. CJIS Assist

Utilizing key elements of SecuLore's CyberSight service, CJIS Assist is focused on fulfilling important requirements within the CJIS Security Policy to keep End-Customers safe. CJIS Assist includes SecuLore's US-based 24x7x365 SOC empowered by Tenable's Vulnerability Management solution and deployed on SecuLore's proprietary device, CyberDSP. CJIS Assist will provide End-Customers with a robust understanding of the vulnerabilities present on CJIS devices by utilizing SecuLore's proven passive monitoring solution paired with Tenable's active scanning methodology, while being managed by SecuLore's SOC. This all limits the impact of the day-to-day management on the End-Customers' precious time. This service is also able to be deployed on any existing CyberSight deployment that is currently monitoring CJIS devices.

Deliverables:

- **24x7x365 Cybersecurity Monitoring**
  Similarly to CyberSight, CJIS Assist uses SecuLore's technology designed for Public Safety by their team of cyber experts. This technology combined with SecuLore's 24x7x365 Cyber-SOC, provides the ability to monitor the End-Customers' networks for vulnerabilities.
- **SOC Cyber Threat Analysts**
  SecuLore's Cyber-SOC engages in ongoing threat analysis utilizing a range of tools, and researches the latest cyber threats to implement them into their alert platform. SecuLore's analysts learn the baseline of the End-Customers' networks and are their partners in identifying & resolving vulnerabilities.
- **Forensic Event Logging**
  SecuLore's technology enables their Cyber-SOC to save off raw packet data to an encrypted drive in the event of a cyber-attack.
- **Nationwide Public Safety Cyber Threat Awareness**
  Seculore is deployed across the US in small, medium, and large ECCs. This provides the End-Customers a unique viewpoint of the threats against Public Safety infrastructure and gives the End-Customers the opportunity to enhance their alert methodology and threat analysis on a daily basis based on active threats to End-Customer's market.

- **Monthly Active Scans**
  Active scans will be run on a monthly basis at a designated time to be determined in the Configuration and Contact sheet or during the Kickoff Call. SecuLore's SOC will review these scan outputs upon completion of the scan and escalate an alert to the End-Customer following their typical alert escalation practices in the event of a critical finding.
- **Monthly Scan Reports**
  Reports of the active scans will be delivered monthly to the End-Customers via the same methods used for CyberSight. These monthly reports break down vulnerabilities by asset and include remediation recommendations.
- **Scans when new vulnerabilities are identified and reported**
  In the event of a critical alert being raised within SecuLore's SOC or a critical risk CVE is released, additional scans may be run to give SecuLore's SOC an additional level of detail to assist the End-Customer in risk assessment.
- **Ability to readily update vulnerabilities to be scanned**
  As with CyberSight, SecuLore and Tenable both stay on top of the latest vulnerabilities the End-Customers face daily. All updates to CyberDSP and Tenable's Nessus scanner are included and managed by SecuLore's SOC.
- **Ongoing Incident Escalation and Response**
  SecuLore's Cyber-SOC actively evaluates every alert that is raised, determines if and what type of escalation is required, and responds accordingly to the End-Customers with actionable remediation guidance.

2.2. Professional Services

2.2.1. Cyber Benchmark

This cybersecurity assessment and remediation plan is based upon FCC, DHS and NIST best practices to protect the End-Customers' network. Seculore shall conduct a risk evaluation and guide an End-Customer's team towards an in-depth cyber defense strategy that provides constant monitoring and protection.

The deliverables of a typical CyberBenchmark are set forth below:

Deliverables:

- **Cyber Benchmark Report**
  A complete review of the project's findings.
- **Vulnerability Reports**
  Actionable vulnerability remediation recommendations for each segment captured.
- **NIST-Based Risk Analysis Checklist**
  A prioritized list of all vulnerabilities discovered based on risk per segment.
- **Key Cybersecurity Policies**
  Customized cybersecurity policies specific to the End-Customer's environment.
- **Cyber Incident Response Plan Template**
  A recommended action plan to guide the End-Customer's team when a cyber incident occurs.
- **Master IP List**
  Detailed breakout of each vulnerability with all supporting data discovered by SecuLore's team.

2.2.2. Incident Response

Seculore's Incident Response service provides immediate access to an expert Cyber Strike Force that utilizes behavioral based methodologies to track down and quarantine any cyber activity that threatens the safety and security of the impacted End-Customer. The Cyber Strike Force uses Seculore's technology to capture preceding and ongoing incident data, visualizing traffic flow within the network architecture. Captured data is investigated to provide a thorough forensic analysis. The Cyber Strike Force analysis identifies malware within the network and provides remediation consultation and guidance for cyber incidents such as ransomware. This remediation also identifies accidental misconfigurations in the End-Customer's firewall and architecture, discovering the methods used by the cyber threat affecting the agency to prevent future incursion.

This Service Includes:

- Analysis of captured malicious code.
- Forensics on attack methodology.
- Recommendations on configuration changes.
- Prevention guidance for future/subsequent attacks.
- Explanation of underlying attack method.
- Inoculation training to prevent reoccurrence.

2.3. Training Services

SecuLore's Cybersecurity Training services focus on providing critical cybersecurity defense skills to the Public Safety Community and other markets. Anyone who uses a computer or other device that connects to a 9-1-1 network can practice cyber defense and improve security. Training is critical to a center's digital health. The training enables an End-Customer's team to protect themselves, their center, and the public they serve.

2.3.1. Cyber Incident Response Tabletop Training:

8 Hour Onsite Course Includes:

- Cyber Incident Response for Management and Technical Staff
- Define Essential Roles
- Incident Response Overview
- Step-by-Step Drill Exercises for Three Common Attack Scenarios

2.3.2. Cyber Awareness Training:

4 Hour Onsite Course Includes:

- Cyber Attack Awareness
- Acceptable Use
- Responsible Social Media Use
- Infiltration Techniques
- Protection Techniques

3. Implementation Cooperation

Appendix A attached to this Service Guide describes a standard implementation timeframe for the Services, including End-Customer and Intrado responsibilities and key milestones (as herein attached, or as otherwise agreed by the parties, the "Implementation Schedule"). Each party will timely fulfill its obligations per the Implementation Schedule, and will make available all resources necessary to meet the Implementation Schedule, including, as applicable: personnel, facilities, circuits, APIs, network information, third party coordination, and timely approvals (each, an "Implementation Dependency"). Unless otherwise agreed, Implementation Dependencies will be completed within five business days after request.

Either party may notify the other if it has not timely completed an Implementation Dependency, and the party at fault will remedy the deficiency within ten business days. If End-Customer does not so remedy an outstanding Implementation Dependency following notice, then Intrado may commence charging for any minimum recurring fees due under the Order for the Services.

For third party dependencies outside of End-Customer's control, End-Customer will promptly communicate any expected delay, and any remedies stated above will not apply.

Any modified or expanded Implementation Schedule agreed on by the parties will replace the attached Appendix A, and the above terms will continue to apply.

4. Service Support

SecuLore provides telephone and email support for Managed Services during Business Hours (9:00 A.M. to 5:00 P.M. Eastern Time) Monday-Friday excluding Federal holidays. Calls or emails received outside of these times will be responded to at the start of the next business day.

- End-Customers may contact SecuLore's support team at:

  Customer Support: 410-305-0234 or toll free at 844-732-8567, Email: Support@seculore.com

- Cyber Incident Emergency 24x7x365:

  Phone: 855-440-7257, Email: Support@seculore.com

Appendix A

Implementation Schedule

Milestone	Duration	Deliverable	Owner
Initiation Phase	**34 days**		
Order placed & received.	10 days	Source security hardware.	Intrado
Site information provided. (Can be provided concurrently)	3 days	Gather site specific information about location and network addressing; Customer provides contact information.	End-Customer, if it is Third Party CPE. Intrado, if it is Viper.
Pre-configure and test device.	10 days	Build and test security equipment.	Intrado
Hardware shipping/arrival.	10 days	Intrado ships the device; Service Start Date begins 15 days post shipment; End-Customer receives device.	Intrado/End-Customer
Rack equipment.	0.25 day	Connect power and network cabling.	Intrado/End-Customer
Network configuration.	0.25 day	Configure network switch for internet connectivity; Configure port mirroring on a separate switch.	Intrado/End-Customer
Production Phase	**32 days**		
Validation and Complete Installation.	2 days	Ensure data is being collected; Monitoring begins; Network Connectivity confirmed. Service begins.	Intrado
Baseline Reporting Period	30 days	30-day Baseline reporting period begins. Limited reporting period. Only medium and critical alerts reported. Concurrent with Validation.	Intrado

- This schedule reflects a standard deployment of 36 days following Order Effective Date. Additional steps or requirements may be needed for non-standard deployments or unique circumstances.
- All references to “days” are to business days.