Security as a Service (SECaaS)

Service Overview

LOGIS' Security as a Service (SECaaS) offering delivers a unified, subscription-based cybersecurity solution that blends advanced threat-detection technology with the hands-on expertise of the LOGIS Security Team. This service enables members to strengthen their security posture, gain deeper visibility across their environment, and respond more effectively to security threats without the cost, complexity, or staffing demands of building and managing these capabilities in-house.

Value Proposition

This integrated security platform reduces operational complexity, enhances efficiency, and strengthens organizational resilience. By augmenting internal IT capabilities without requiring additional staff, providing predictable subscription-based pricing, and leveraging proven technologies with expert oversight, SECaaS lowers risk while enabling faster detection and response to emerging cyber threats.

Security Information and Event Management Platform (SIEM)

- 24/7 continuous Managed Detection and Response (MDR).
- Event correlation and detections to identify threats and anomalies in real time, across multiple log sources.
- Detection, containment, and mitigation of active threats – with customizable response levels based on your preference.
- 365 days of searchable log storage for investigations, audits, and compliance.
- Customizable dashboards with visual analytics, and compliance reporting.

Endpoint Detection and Response (EDR)

- 24/7 continuous Managed Detection and Response (MDR).
- Continuously monitor end-user devices to detect suspicious activity and threats. Ongoing rule optimization to improve detection fidelity and reduce false positives.
- Detailed reports and recommendations following security incidents or investigations.

Security Professional Services

- Support efforts to maximize ingestion and gain the most value from the SIEM.
- Provide support for initial deployment.
- Conduct quarterly reviews to assess visibility gaps, logging coverage, detection effectiveness, and support any deployment gaps.
- Perform threat intelligence and threat hunting activities, with distribution of intelligence bulletins.
- Provide hands-on support during confirmed critical security incidents.
- Lead investigations with expert guidance and provide containment recommendations.
- Conduct post-incident reviews and capture lessons learned.

Security as a Service (SECaaS)

Service Responsibilities

To ensure seamless service delivery and mutual accountability, LOGIS has outlined the following responsibilities and expectations for each party, helping foster transparency, efficiency, and successful collaboration.

	LOGIS	Strategic Partner	Member
Product Management	• Manage strategic partner relationships • Procure and manage licensing, subscriptions, and contracts	Provide, manage and maintain the tooling and platform	*N/A*
Onboarding & Access	• Assist with scoping member environment • Manage initial onboarding activities • Configure tenant for LOGIS access and management	• Provision and configure the tenant • Activate and manage licensing and entitlements	• Complete enrollment and authorization forms • Provide accurate environment and asset information • Provision required access credentials • Approve onboarding timelines and prerequisites
Deployment & Configuration	• Assist with deployment of agents on endpoints • Integrate telemetry sources (e.g., firewalls, cloud apps, identity) • Validate telemetry and log flows • Assist with system level issues affecting members telemetry	• Monitor initial sensor health and support troubleshooting efforts • Support activation and operation of endpoint sensors	• Deploy log sources where LOGIS lacks access • Configure and maintain system settings for log ingestion
Monitoring & Detection	• Review trending alert data for tuning opportunities and optimization • Build out custom detections based on local incidents and indicators of compromise • Threat intel and hunting using local intelligence	• 24/7 monitoring, triage, investigation, escalation • Threat intel and hunting using global intelligence	• Maintain visibility by ensuring agents/log sources remain operational • Respond to requests for system context or escalation • Monitor and act on notifications and advisories
Incident Response	• Provide investigation and Incident Response support for confirmed critical non-endpoint incidents • Coordinate incident	• Lead Incident Response for endpoint incidents • Analyze and alert on SIEM/log-based events • Execute endpoint	• Perform recovery actions after incident is mitigated • Responsible for business and operational decisions during incidents

	communications with the member	containment actions per policy	• Review and acknowledge incident reports
Maintenance & Reviews	• Configure/administer the SIEM platform • Provide ongoing reporting (dashboards, metrics, summaries) • Support efforts to maximize ingestion and gain the most value from the SIEM • Conduct quarterly reviews to assess visibility, detection effectiveness, review configurations, best practices etc. • Perform threat intelligence and threat hunting activities, with distribution of intelligence bulletins	• Deliver updates improving detection efficacy • Perform detection engineering and rule updates • Resolve platform level issues or service interruptions	• Maintain and support all log sources • Participate in quarterly reviews and implement corrective actions • Act on recommendations to enhance security posture
Offboarding	• Assist service termination between all parties • Assist member with removal of agents and integration configurations	• Deprovision/disable tenant • Terminate licensing entitlements • Remove service side configuration • Assist with transfer of log data when requested	• Remove agents and undo integration configurations • Revoke LOGIS and vendor access • Plan for preservation of logs if required by service termination date

Pricing

* Please contact security@logismn.gov for pricing information.

Security as a Service (SECaaS)

Appendix

What is an Incident?

An “Incident” is defined as a confirmed or reasonably suspected compromise of systems, endpoints, accounts, or data resulting from malicious activity and requiring immediate containment, eradication, or recovery actions. Suspicious activity, user-reported concerns, automated security alerts, or events that are determined through triage to be benign, unsuccessful, or fully mitigated (including but not limited to phishing emails without payload execution or compromise) do not, by themselves, constitute an Incident. All reported security concerns will be initially evaluated through a triage and validation process, and Incident Response services will be initiated only upon confirmation or high confidence determination that an Incident has occurred.

Regulatory and Compliance Considerations

The security services provided under this offering, including MDR, EDR, and SIEM, are intended to support the Member’s overall security posture and are not specifically designed or certified to meet Bureau of Criminal Apprehension (BCA) compliance requirements, CJIS Security Policy requirements, or other regulatory or statutory compliance obligations. The Member retains responsibility for understanding and meeting all applicable compliance requirements, including those related to the State of Minnesota BCA and CJIS.

Deployment and Incident Response Support

During onboarding, LOGIS will work collaboratively with the Member to deploy agents and configure integrations wherever the appropriate access is available. LOGIS will revisit and support this process on a quarterly basis at a minimum. However, the Member remains responsible for ensuring that all required log sources are properly maintained to achieve full coverage and visibility. Any gaps in ingestion or visibility that lead to missed security events fall outside the scope of LOGIS responsibility.

Members who request assistance with deployment, configuration, or incident response acknowledge that such support may require LOGIS to be granted appropriate administrative or delegated privileges within the Member’s environment. The Member retains full ownership and control of their environment and is responsible for approving, provisioning, and reviewing all access granted. LOGIS will use any provided access solely for the purpose of delivering the agreed-upon services and in accordance with established security and access management practices.

LOGIS will perform Incident Response activities to the best of our professional ability and in accordance with the information and access provided. However, we do not make any guarantees regarding outcomes, containment effectiveness, threat eradication, or the prevention of future incidents. The Member acknowledges that cybersecurity incidents carry inherent risk, and we bear no responsibility for any damages, losses, or impacts resulting from a cybersecurity event. Additionally, LOGIS assumes no liability for any unintended or unforeseen consequences arising from Incident Response actions performed on the Member’s behalf.