Security as a Service (SECaaS)

Service Overview

LOGIS's Security as a Service (SECaaS) offering provides a flexible cybersecurity program designed to meet members where they are. Whether they need just the enterprise grade tooling and platform or a fully managed solution supported by LOGIS security experts. Both service types empower members to strengthen their security posture, gain deeper visibility across their environment, and respond more effectively to emerging threats.

SECaaS Core	**SECaaS Complete**
Platform Only	*Fully Managed Security Partnership*
Access to platform with full native capabilities under a license only model. Members are responsible for day-to-day operation and management of the tooling. LOGIS onboarding support is available on a limited, billable time and materials basis.	Full EDR and SIEM platforms with 24/7 Managed Detection and Response. Includes LOGIS Security Team oversight, SIEM tuning, threat hunting, incident response support, and quarterly reviews under a predictable subscription.
Best for teams who need control and visibility today, with the option to hand off operations tomorrow.	*Best for organizations seeking to augment IT capacity without adding headcount.*

Value Proposition

- **Enterprise-Grade Protection** — We've partnered with CrowdStrike to provide enterprise grade security for members of any size
- **Consortium Power** — Aggregated purchasing delivers discounted licensing and centralized contract management, reducing cost and admin burden
- **Unified Visibility** — Single pane of glass across endpoints, identities, and infrastructure, enhanced by shared threat intelligence across all SECaaS members
- **Scalable & Flexible** — From license-only to fully managed, SECaaS augments your internal IT capabilities without adding headcount

SECaaS Core Features

Security Information and Event Management Platform (SIEM)

- Event correlation and detections to identify threats and anomalies in real time, across multiple log sources
- 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) on endpoint events

- 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

Access to Advanced Security Modules

- File Integrity Monitoring — Tracks changes to critical system files, configurations, and directories to detect unauthorized modifications and support CJIS compliance requirements
- Host-Based Vulnerability Management — Continuously scans endpoints for known vulnerabilities and misconfigurations, providing prioritized exposure insights to guide remediation efforts
- Identity Protection — Monitors user accounts and credentials for suspicious behavior, compromised access, and identity-based threats to reduce the risk of unauthorized access

SECaaS Complete Features | Includes everything in SECaaS Core plus:

Security Professional Services

- Provide support for initial deployment and ongoing maintenance to maximize ingestion and gain the most value from the SIEM
- Conduct quarterly reviews to assess visibility gaps, logging coverage, detection effectiveness, and support any deployment gaps
- Set up foundational CJIS dashboards for compliance requirements

Security Operations Support

- 24/7 continuous Managed Detection and Response (MDR) on all events
- Detection, containment, and mitigation of active threats – with customizable response levels based on your preference
- 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

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	Member
	Manage partnership and subscriptions	Review and comply with contract terms

Security as a Service (SECaaS)

Management & Ongoing Operations	Procure and provision licenses to members	Process payments and maintain internal budget alignment
		Operate and manage the platform
Onboarding & Access	Provision and configure the tenant	Complete enrollment and authorization forms
	Activate licensing, entitlements, and LOGIS access	Provide accurate environment and asset information
	Assist with scoping and initial onboarding activities	Approve onboarding timelines and prerequisites
Deployment & Configuration	Deploy agents and integrate telemetry sources (firewalls, cloud apps, identity)	Deploy log sources where LOGIS lacks access
	Validate telemetry and log flows	Configure and maintain system settings for log ingestion
	Support troubleshooting and system-level issues	
Monitoring & Detection	24/7 monitoring, triage, investigation, and escalation	Respond to requests for context or escalation
	Threat hunting using emerging Indicators of compromise and intelligence	Monitor and act on notifications and advisories
	Build custom detections and tune alerts to reduce false positives	
Incident Response	Lead initial incident response and containment actions	Make business and recovery decisions post-mitigation
	Analyze and alert on SIEM and log-based events	Review and acknowledge incident reports
	Provide investigation and response support for critical incidents	Coordinate incident response handling & recovery
Maintenance & Reviews	Maintain platform health and resolve service interruptions	Maintain and support all log sources
	Perform detection engineering and rule updates	Participate in quarterly reviews and implement corrective actions
	Conduct quarterly reviews and distribute threat intelligence bulletins	Act on recommendations to enhance security posture
Offboarding	Deprovision tenant and terminate licensing	Remove integrations and revoke LOGIS and vendor access
	Remove service configuration and assist with data transfer	Plan for log retention if required by service termination date
	Assist with agent removal and integration cleanup	

Security as a Service (SECaaS)

Appendix

What is an Endpoint?

An endpoint is any device capable of running an endpoint agent, including but not limited to:

- Physical or virtual machines
- Desktops, laptops, servers, tablets
- Devices running Windows, macOS, Linux

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 CrowdStrike 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 led 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.

Core and Complete Comparison

Feature	SECaaS Core	SECaaS Complete
Platform		
EDR (Endpoint Protection)	✓ Licensing	✓ Licensing
SIEM Platform + 365d Storage	✓ Licensing	✓ Licensing
File Integrity Monitoring	- Available	- Available
Exposure Management	- Available	- Available
Identity Protection	- Available	- Available
Monitoring & Detection		
24/7 Response (MDR)	- Endpoint Only	✓ Included Endpoint + SIEM
SIEM Tuning & Rule Optimization	- Not Available	✓ Included
Custom Detections	- Not Available	✓ Included
Threat Intelligence & Hunting	- Not Available	✓ Included
Incident Response		
IR Containment & Support	$ T&M	✓ Included
IR Handling & Recovery	$ T&M	$ T&M
Post-Incident Review	$ T&M	✓ Included
Professional Services		
Onboarding Support	$ T&M	✓ Included
Quarterly Reviews	- Not Available	✓ Included
Ad Hoc Support	$ T&M	✓ Included