MANAGED SECURITY SERVICES
Protect. Detect. Respond.
Cybersecurity is Mission Critical

In this new era of increasing hacking and digital espionage, cyberattacks pose a serious risk to the viability of all organizations. Cyberattacks frequently compromise personal and business data resulting in loss of reputation and revenue, as well as potential violation of data privacy laws. Governments are reacting by drafting and passing new data privacy laws and regulations, mandating organizational requirements for information security, breach notifications and penalties for failing to protect personal data.

In order to adapt, all organizations need a strategic, integrated set of information security solutions. These solutions consist of a comprehensive set of policies, procedures and processes with certified and experienced people, not just a set of technologies. The goal is simple – to minimize cyberattacks while allowing organizations to respond quickly and effectively when information security breaches occur.

At CANCOM, we deliver a comprehensive model of support to our clients through the following set of managed service offerings:

- Security Operations Center
- Endpoint Detection & Response
- Intrusion Detection & Prevention Systems
- Security Information & Event Management
**Managed SOC Service**

All CANCOM Managed Security Services alarm to our Security Operations Center (SOC). The SOC was built using best practices from the NIST-800-61r2 Computer Security Incident Handling Guide and Crafting the InfoSec Playbook to ensure our top-tier service meets and exceeds existing business, legal, and strategic requirements – while having the capacity to adapt to future needs.

Our SOC operates 24-hours a day, 7-days a week with certified and experienced personnel (e.g. HIPAA, FISMA, 10CFR73.54, INPO (Nuclear), SOX, NIST 171, & NIST 800-53) who perform tasks according to our standardized Security Incident Response Process. Based on the security incident type, our SOC team quickly performs an analysis and implements the corrective actions, depending on the level of delegation of remediation responsibility established by the customer.

Standard or custom reports are provided based on our customers’ needs. Reports are used to gauge performance and to make recommendations for improvement.

**Managed EDR Service**

Endpoint Detection and Response (EDR) provides the single largest security benefit to any organization. EDR helps block malware at the point of entry, gain visibility into file and executable-level activity and removes malware from PCs, Macs, UNIX/Linux, and mobile devices.

The challenge in deploying an EDR solution is responding to Indication of Compromise (IOC) alerts and resolving them in a timely manner. Forensic analysis of EDR alerts takes significant time and a unique skillset. Most organizations believe vulnerabilities happen on the network; however, end users are the most vulnerable because they are targeted through phishing, social engineering and mainline advertising on legitimate websites. Nefarious individuals target employees, exposing your organization to potentially devastating malware and ransomware attacks. CANCOM has the solutions and security playbook for this.

CANCOM’s Managed EDR Service comes bundled with our Managed SOC Service and the Cisco AMP solution via a subscription model. If you have an existing Cisco Sourcefire solution, we can incorporate it into our offering.

**Managed IDPS Service**

Intrusion Detection and Prevention Systems (IDPS) continuously monitor your network for malicious activity or security policy violations. They are powerful, sophisticated and are typically mandated network monitoring technologies by law.

CANCOM’s Managed IDPS Service comes bundled with our Managed SOC Service and Cisco Sourcefire via a subscription model. If you have an existing Cisco Sourcefire solution, we can incorporate it into our offering.

**Managed SIEM Service**

A Security Information and Event Management (SIEM) solution captures, indexes and correlates real-time security information log data from multiple systems and network devices (e.g. Cisco AMP & SourceFire, Microsoft Active Directory, Microsoft SCCM, Microsoft Windows System Logs and UNIX/Linux System Logs). A SIEM is a searchable repository that can generate graphs, reports, alerts, dashboards and visualizations to support metric tracking, problem diagnoses and provides actionable intelligence for business operations.

A SIEM is required for organizations subject to SOX, HIPAA, GDPR, CCPA or other security audit data retention policies.

CANCOM’s Managed SIEM Service comes bundled with our Managed SOC Service and the Splunk SIEM solution via a subscription model. If you have an existing Splunk solution, we can incorporate it into our managed service offering.
Why CANCOM?

- We have years of experience implementing policies, procedures, processes, people and information security monitoring technologies.
- We can adapt and enhance your existing environment and security playbook to ensure seamless coverage.
- We are comprised of certified and experienced personnel providing security governance so your in-house support personnel can focus on core activities.
- Our solution grows with your business; it is scalable from small to large complex networks.
- We provide relevant and actionable reporting for remediation, compliance, and trend analysis.
- We are continuously monitoring your network via Cisco Sourcefire — a top tier IDPS solution. We maintain a close partnership with Cisco for third-level escalation analysis and remediation.
- We are continuously monitoring for alerts from the Splunk SIEM solution — a top tier SIEM solution. We maintain a close partnership with Splunk for third-level escalation analysis and remediation.
- We provide the expertise to implement, monitor and optimize your Splunk SIEM solution, significantly reducing its time-to-value.
- The Splunk SIEM solution receives log streams from your systems and network devices to protect against tampering or data deletion.