

SOURCETEKIT MANAGED SOC SERVICE



**FOR MORE INFORMATION
CONTACT US**



MANAGED SOC SERVICE

SOURCETEKIT MANAGED SOC SERVICE

- Provides a hybrid resourcing model of on-site and off-site professionals, combining 24x7 coverage with a SOC model that is customized around your core business needs.
- Provides your business with greater threat detection capabilities through the use of advanced monitoring technologies.
- Offer integrated threat intelligence, security monitoring, incident response, behavioral analytics and security analytics competencies.
- Ability to detect Advanced Persistent Threat (APT) style behavior on your network, including endpoint threat detection and data exfiltration.
- Helps manage and monitor compliance, increase application availability, and save IT resources.

Threats continue to evolve, your SOC must too. SourcetekIT Managed SOC is designed to wrap experienced people and efficient processes around leading technologies to provide a business-focused SOC that will evolve with your organization's needs and the changing threat landscape.

MODULES INCLUDED

1. SIEM and Log Management

Correlate, analyze and securely store security event data from across your environments.

- Event Correlation
- Log Management
- Incident Response
- Integrated Threat Intelligence
- Security Team and the Open Threat Exchange (OTX)



MANAGED SOC SERVICE

MODULES INCLUDED

2. Asset Discovery

Monitors all the details of all devices connected on the network.

- API-Powered Asset Discovery
- Network Asset Discovery
- Software and Services Discovery

3. Intrusion Detection

Detects and responds to threats faster with built-in host, network and cloud intrusion detection technologies.

- Network Intrusion Detection (NIDS)
- Cloud Intrusion Detection

4. Vulnerability Assessment

Identify vulnerabilities on your assets to avoid exploitation and compromise.

- Network Vulnerability Scanning
- Endpoint Vulnerability Scanning
- Cloud Vulnerability Scanning
- Cloud Infrastructure Assessment
- Operating Systems Security Assessment (OSSA)
- Database Assessment



MANAGED SOC SERVICE

MODULES INCLUDED

5. Endpoint Detection and Response

Detection and investigation of security Incidents using 24x7x365 real-time monitoring providing immediate notification of breach and continuous vulnerability scanning.

- Host-based Intrusion Detection (HIDS)
- File Integrity Monitoring
- Continuous Endpoint Monitoring & Proactive Querying

6. Behavioural Monitoring

Identifies suspicious behavior, user activities and potentially compromised systems.

- Asset Access Logs
- Cloud Access and Activity Logs
- AWS VPC Flow Monitoring
- VMware ESXi Access Logs

KEY DIFFERENTIATORS

1. Robust SOC Offering

Adaptive awareness of the threat landscape. Rapid local and global threat detection for quick response. Reduced complexity in managing the onslaught of alerts and alarms. A comprehensive and more holistic approach to managing risk. Reporting and analytics that enable IT, a line of business managers, C-level, and board members to better understand how the organization's risk profiles are being managed.

2. CyberSecure Canada Certification

The program outlines baseline cyber security controls that will give SMEs the greatest amount of protection from cyber threats.

3. 7x24x365 Monitoring

Our Security Operations Center Specialists are continuously monitoring.

4. Insurance for Business Interruption

Only SOC in Canada that offers business interruption insurance up to \$500,000 annually, applicable to companies with revenues up to \$50 million.

