



MANAGED SOC

Security Operations Center

Next Generation Advanced Security Solution For Today's Cyber Threats. Overcome the top IT and cybersecurity challenges impacting your organization by focusing on real-time threat detection, investigating and incident response strategies.

Why It Matters:

A security operations center (SOC) is a centralized hub or command center that augments your overall IT & data security defense posture by harnessing the collective power of technology, processes, and people to aggregate, analyze, support, and manage the multiple security measures in place to protect your organization.



24/7 Threat Monitoring and Analysis

Effective Defense Strategy

Today's cyber threats require equally advanced security strategies that continuously adapt to overcome new and evolving security risks and vulnerabilities. To protect your business-critical operations and its valuable information assets, adopting a comprehensive, layered-security defense is essential. Implementing and effectively managing the security operations for your business can be challenging without the proper resources.



Real-Time Investigation and Threat Hunting

Our Managed Security Operations Center or SOC-as-a-Service solution can solve this problem for your business. We combine the power of people, processes, and technology to provide essential security capabilities like real-time threat and intrusion detection, rapid incident response and investigations, and continuous 24/7 monitoring and vulnerability management.



Threat Isolation and Remediation

Overcome Security Challenges

Take advantage of our team of seasoned cybersecurity professionals and expert analysts to empower your business to overcome today's top cybersecurity challenges and implement a more proactive and preventative approach to protecting your business.



Incident Response and Notifications

Contact us to find out how our SOC service can reduce the time to detect, contain, and respond to threat incidents or security breaches and enable your business to avoid costly disruptions and damaging data loss from cyberattacks.

LET US HELP YOU CONQUER YOUR CYBERSECURITY CHALLENGES. CONTACT US TO LEARN MORE.

866-634-9633

jkconsulting.com

24x7 Detection & Response

Across 3 Main Attack Pillars

Endpoints

Windows & MAC OS

IT Network Infrastructure

Edge Devices, Systems and Firewalls

Cloud Applications

Microsoft 365 & AzureAD



Enhanced Visibility into Email Threats

We monitor your O365 accounts for business email compromises (BEC), unauthorized rule forwarding, and excess privileges risking data leakage. We monitor the Dark Web 24x7 for any exposed credentials linked to your domain or IP details.

Real-time Threat Hunting and Investigations

Empower a more proactive and preventative approach to your security posture by creating a robust look at your overall risks and defensive measures and leveraging the intel and insights to adjust or change your future tactics or strategies.

Monitor & Track Firewall Logs

We monitor firewall logs acting as a syslog collector. Activities and alert messages are then aggregated, parsed, and investigated to identify potential threat indicators.

Detect Suspicious Tools & Programs

We can detect suspicious tools that should not be present on your network, such as hacking utilities, password crackers, etc. used for malicious intent.

DNS Filter Monitoring

Monitor DNS Filter log activity for new threats or known vulnerabilities or malicious network and IP connections.

Maintain Regulatory Compliance

The need for 24/7 continuous cyber monitoring is fundamental no matter the industry or business size.

Crypto Mining Detection

Detects network connections to various nation states that have been known to engage in cyberterist activities.

Cyber Terrorist Network Connections

Detects network connections to various nation states that have been known to engage in cyberterist activities.

Securing your business is not a one-time investment. Even the best antivirus or firewall is no match for today's well-funded and highly skilled cyber-criminal. You need around-the-clock protection to ward off cyberattacks.

Why use a Security Operations Center?

- Supplement limited internal security
- Improved threat detection and response
- Immediately improve security posture
- Cost-effective solution

Benefits

- Proactive & Preventative Security Management
- 24x7 x 365 SOC Cover/Support
- Overcome IT Skills & Resource Gaps
- Increased Threat Awareness & Risk Mitigation
- Critical Documentation & Record keeping
- CUSTOMIZABLE!

LET US HELP YOU CONQUER YOUR CYBERSECURITY CHALLENGES. CONTACT US TO LEARN MORE.

866-634-9633

jkconsulting.com