Telesystem
IT's About Trust

#HackersSuck

Managed Security Operations Center (SOC)

24/7/365 Monitoring

ISO-27001 Certified

Real-Time Alerting

Rapid Remediation

SIEM + EDR Platform

What is Managed SOC?

Managed Security Operations Center (SOC) is a complete, managed security platform to prevent, detect, respond and even predict future attacks across your entire business. Our cybersecurity experts work as an extension of your in-house team to understand your environment and proactively respond to threats as they occur, eliminating the need to staff, train and maintain your own SOC.

Predict
Deep Learning Analysis stops attacks pre-execution

Prevent
Automatic remediation of threats at the endpoint

Detect
Comprehensive monitoring and alert escalation

Respond
Customized incident response plans and support

Managed SOC Capabilities

Security Operations Center - Your infrastructure is monitored and protected 24/7 by a fully staffed team of cybersecurity experts.

SIEM - Security Information and Event Management provides intelligence, greater visibility and aggregation of events across your network.

Endpoint Protection - Managed endpoint protection platform powered by deep learning for zero-time prevention.

Threat Detection and Response - Managed threat detection and response (MDR) to defend your entire IT environment.

Intrusion Detection - Monitor malicious activity within your network and endpoints.

Network Traffic Analysis (NTA) - Monitor network traffic for early threat detection and a swift response.

Vulnerability Assessment - Avoid attacks by identifying your network's vulnerable systems.

Threat Hunting - Proactively guard your critical business infrastructure with a team that understands adversary tactics and techniques.

Threat Detection and Response

Our managed platform approach to cybersecurity simplifies operations and reduces security gaps left by traditional IT security tools. Compromised login credentials are found in over 80% of all network intrusions where traditional tools provide limited visibility and protection. We leverage machine learning to trigger detailed and actionable alerts in real time when abnormal behavior occurs that could signal a data breach, including compromised credentials, lateral movement, and insider threats.

Integrated Endpoint Detection and Response
Endpoint detection and response (EDR) provides a response beyond legacy anti-virus for an endpoint security solution that is integrated, powerful, and includes remediation capabilities.

Secure Microsoft 365
In cooperation with Microsoft, we restore visibility to user, application, and data behavior through audit/logging, PowerShell activity tracking, and a 24/7 SOC to detect and escalate incidents, alerting you to security problems and recommending mitigation steps before downtime occurs.

Protect Remote Work Employees
Security gaps increase with remote access to corporate servers, to VPNs (virtual public networks), or personal networks. Remote Workforce Threat Detection from Netsurion protects sensitive data that's outside your company network to fill cybersecurity gaps.

Achieve Actionable Threat Intelligence
Our Threat Center portal easily incorporates threat intelligence from the MITRE ATT&CK framework, commercial and open source threat feeds, and security analysts. Intuitive reports and recommendations ensure that cyber threat intelligence (CTI) is actionable and tailored to your organization and customers.

Security Information and Event Management (SIEM)

SIEM begins with the collection, standardization, and storage of security event data, and then uses an array of analytical methods to examine, report, and act upon security alerts pulled from that data in real time. SIEM and log management capabilities provide the core of our threat protection platform, and empower threat detection with support for thousands of devices and applications and over 2,000 out-of-the-box reports.

Our SIEM platform is tasked with monitoring an ever-increasing attack surface that encompasses physical servers, workstations, endpoints, and cloud infrastructure to ensure your environment is safe. Rule-based alerts are set and backed by dashboards, alert scores, contextualization, and automated response capabilities to ensure your organization quickly responds to any alarming anomalies or threats.

Real-time Alerting and Incident Response - Utilize rule-based alerts with dashboard updates and remediation recommendations.

Security Reporting - Over 1,500 pre-defined security and compliance reports. Comprehensive support is included for PCI-DSS, HIPAA, ISO 27001, NIST 800-171, DOD, RMF, GDPR, and more.

Threat Intelligence - Our platform integrates with valuable threat data feeds from ecosystem partners and open source providers to enable quick and accurate detection of threats to your network.

Search and Forensic Analysis - Logs are indexed to Elastic Search using an extensible Common Indexing Model.

Behavior Analysis and Correlation - Quickly detect and address changes in system and user behaviors. Real-time processing and correlation gives a complete picture of what's new and different.