NEUVYS TECHNOLOGIES

SOC-as-a-Service

Security Operations Center as a Service

It's critical to quickly identify threats, remediate when possible, and recover when necessary to survive and thrive, even in the midst of an attack.

In today's information age, data is your most valuable asset—and attackers know it. Every organization is at risk. Adversaries can infiltrate systems without detection, lying in wait for weeks or even months before launching an attack.

According to the 2023 IBM Cost of a Data Breach Report, it takes an average of 204 days to identify a breach, and it typically takes another 73 days to contain it.

Reduce Your Risk

In today's threat landscape, organizations must assume adversaries are already present in their networks. The best defense is a strong offense: a proactive approach to digital resilience that strengthens your security posture, allowing you to respond to both current and future threats.

Our security experts focus on mitigating risks, not just reporting alerts. We use a purple-team approach, combining red team (simulated attacks) and blue team (network defense) services. This provides a comprehensive, 360-degree view of your environment with continuous monitoring and testing.

Gain the Time Advantage

Our advanced threat detection capabilities and defense-in-depth approach give you the time advantage, ensuring your security controls are effective and potential threat actors are identified before they gain a foothold. Our team of security experts ensure you maintain digital resilience, so you can focus on your core competency.

KEY BENEFITS

- 24x7 Security Operations
- Strengthen your security program in 30 days (rapid deployment, ease of integration, and support)
- Improve threat detection and response (centralized and aggregated log information + machine learning)
- Experienced analysts provide prioritized, actionable recommendations
- Reduce attacker dwell time from months to minutes
- On-premises, cloud, & SaaS monitoring
- Replace complex and costly tools with full transparency, including SIEM access, monthly vulnerability assessments, and security controls validation
- Focus on your core business without the need to build a specialized security team

SOC-as-a-Service

SIEM & Log Management	
Log aggregation	✓
Event Correlation	✓
Forensics data collection	✓
Open Threat Exchange (OTX)	✓
Daily Updates	✓
Asset Discovery & Inventory	
Active asset scanning (NMAP)	✓
Passive asset identification (NTA)	✓
Rogue system identification	✓
Behavioral Monitoring	
User Behavior Analysis (UBA)	✓
Entity Behavior Analysis (UEBA)	✓
Threat Analysis (NTA)	✓
Intrusion Detection	
File Integrity Monitoring (FIM)	✓
Host Intrusion Detection (HIDS)	✓
Network Intrusion Detection (NIDS)	✓
Network Threat Analysis (NTA)	✓
World's largest threat feed	✓
Vulnerability Assessment	
Continuous vulnerability scanning	✓
Risk and severity classification (CVSS)	✓
Common vulnerabilities and exposures	✓
Database (CVE)	✓
Daily updates	✓
Simulated Attack (Red Team)	
Monthly internal penetration tests	✓
Security Controls Validation (SCV)	✓
MITRE ATT&CK® Matrix	✓
Leverage TTPs used by adversaries	✓
24x7x365 Security Operations Center (Blue Team)	
Seasoned security analysts, Security Academy graduates, U.S.-based staff	✓
Machine Learning (ML) augmentation	✓
Advanced correlation augmentation	✓

Optional Services

- Penetration Testing
- Advanced Phishing Security
- DNS Security
- Endpoint Security
- Network Security
- Incident Response

Contact us today for a complimentary Security Health Check.

WD/DS/SOCaaS/102224