Managed Network Anomaly Security Service

Detection and investigation of emerging cyber-threats that evade traditional security tools

Synoptek's Network Anomaly Security Service is built to help organizations detect and investigate emerging cybersecurity threats that evade traditional security tools. The service is powered by an Enterprise Immune System technology, which uses machine learning and mathematics to monitor behaviors and detect anomalies in your organization's network. This approach does not require signatures or rules and can detect emerging attacks that have not been seen before.

Service Overview

Synoptek's Security team provides ongoing management of the Enterprise Immune System platform – an "in a box" solution, including installation, configuration, and interpreting the Threat Visualizer. Our consultative approach allows for our clients to take advantage of Synoptek's experience working with complex environments that require People, Process, and Technology to achieve higher levels of IT security. This managed service is designed to help clients detect and respond faster to new threats as well as develop strategies to strengthen their overall security posture. As part of the service, Synoptek delivers weekly threat intelligence reports, where Synoptek cybersecurity experts provide your team with guidance covering ongoing threats, misconfigurations, IT operational deficiencies, policy violations, and more.

Weekly threat intelligence reports are delivered with three key elements:

- Executive summary of the events that unfolded from the prior week as well as detailing the severity level associated with each event
- Incident/breach details for both Network and System Engineers; and
- Detailed remediation planning from Synoptek's Security Analysts

Managed Network Anomaly Security Service

Key Benefits

- 24x7 Security team that can detect and respond to threats in real-time
- Visibility into your entire network – all devices and users
- Detection of insider threats, including suspicious operations and harmful behaviors
- Weekly consultative meetings with a Virtual Chief Information Security Officer
- Skilled Security resources for on-going remediation

Types Of Anomalies Synoptek Can Detect

- Remote access attacks linked to malware
- Malicious web drive-by
- Use of “Tor” browser for accessing the Dark Web
- Bitcoin mining application
- Harmful end user behavior
- Suspicious Java downloads
- Infection with ransomware
- Peer to peer connects with the Far East
- Unauthorized use of administrator credentials
- Illegitimate access to database server
- Use of virtual Cyrillic keyboard
- Harmful file downloads
- Risks from BYOD policies
- Port-scanning for internal company resources
- Hijacked servers

About Synoptek

Synoptek is a Global Systems Integrator and Managed IT Services Provider offering Comprehensive IT Management and Consultancy Services to organizations worldwide. Our focus is to provide maximum “business value” to our clients enabling them to grow their businesses, manage their risk/compliance, and increase their competitive position by delivering improved business results.