SANS Review: SOC-as-a-Service

All the benefits of a Security Operations Center without the high costs of a DIY solution

SANS Service Review

SANS reviewed Arctic Wolf's services from a customer's point of view and found that its AWN CyberSOC (SOC-as-a-service) offering provided visibility into events they launched in their mock midsize enterprise, caught and helped them repair vulnerabilities purposely left in the environment for review, and provided accurate reporting throughout the review.

Most important, SANS was also afforded access, as needed, to a live engineer to send reports and help troubleshoot investigations. All of this worked seamlessly—without the high costs of implementation, configuration and tuning.

Use Cases Tested

Identify Source of Attacks Against a Web Server

This test simulated real-world attacks against a customer's website on the Internet, for example, an e-commerce website that used to conduct online credit card transactions. AWN CyberSOC was found to provide the information needed to understand attacks in a clear and easily understood format in the AWN Customer Portal so that the right assessments could be made quickly. No user training was needed on the customer portal interface where this information was presented.

Investigate Unusual Surfing Habits in the Workplace

Unusual surfing by end users was viewable with just a few clicks in the AWN Customer Portal. The Customer Portal data view showed the IP address of the offending device, the sites it was surfing and the amount of data that was being sent and received.

Mean Time to Detect Threats: Ransomware, Anomalous Traffic, Compromised Systems (IDS)

SANS simulated real world attacks and possible indicators of compromise and system compromise. Ransomware was detected within five minutes, which included analysis to ensure it was not a false positive. Anomalous traffic was defined using a customized rule. The rule was set up completely by the Concierge Security Engineer, and the customer only had to communicate requirements. The AWN Sensor detected a compromised system with its build-in IDS capability. Having the IDS, packet and log collector all in one appliance gives Arctic Wolf the capability to correlate events quickly without dependency on any external tools.

> Download the full **SANS Service Review**

ARCTIC WOLF Layer 7 Data Solutions

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com