CASE STUDY

Hornblower goes from zero to SOC in 60 minutes

BUSINESS

Premier luxury cruise experiences for special events, private charters and tourism excursions

CHALLENGE

- Create and implement a security strategy and tools with limited IT resources
- Phishing attacks in spite of content and spam filters
- No visibility into security posture despite a number of network security tools
- Overwhelmed staff who have to manage both security and IT operations

RESULTS

- A SOC + virtual security operations team for less than the cost of a full-time security engineer
- A virtual CISO and a trusted partner that provides expert security advice and guidance
- Robust detection of previously undetectable threats
- Visibility into security posture with a scorecard and actionable intelligence

Hornblower is the nation's largest private vessel company with over 70 vessels. Since the company's founding in 1980, they have focused on delivering premium tourist and entertainment excursions for local and international tourists. In addition to hospitality cruises in California and New York, Hornblower services national park destinations such as Alcatraz and the Statue of Liberty. Hornblower is also the official Canadian operator of boat tours to Niagara Falls.

As the company has grown and added multiple ports of destination, their small IT team found it increasingly difficult to gain visibility into their security posture. Like many mid-market companies, the IT team was extremely lean and focused primarily on running the business. Hornblower had the traditional perimeter and endpoint defenses in place, but the company leadership recognized that these could easily be

"My Arctic Wolf security engineer is truly an extension of my IT team, and has detected phishing attacks that bypassed our existing prevention tools twice in the first few weeks. I could not have achieved visibility into our security posture within my budget without Arctic Wolf."

Tim Johnson, Director of IT, Hornblower Cruises & Events

bypassed by today's highly advanced and targeted attacks. They had IT staff consisting of operational experts in areas such as networking and telecom, who focused almost exclusively on making sure that the day-to-day operations were running smoothly. However, Hornblower did not have dedicated security staff, nor the budget to build out a dedicated security team with all of the tools required to implement a robust security strategy.

AWN CyberSOC – the best choice for mid-market companies

There is currently a scarcity of security engineers, and competition to hire them is extremely high. Many mid-market companies are unable to hire and retain security personnel to build a scalable security operations center in-house. Effective security operations include not just managing security infrastructure and handling security events, but also vulnerability assessment, threat hunting and security data triage.

Hornblower realized that the key to any comprehensive security strategy was coverage and consistency. They evaluated options from several large security vendors and realized that those products and services were primarily designed for large enterprises with dedicated security operations teams. After a presentation from one of the largest security vendors, the conclusion was that the solution was like "killing a mosquito with a sledgehammer."

In the end, Hornblower selected AWN CyberSOC because it was the fastest way for them to gain a security operations center. They also liked that the service was specifically developed for mid-market companies. For an affordable monthly subscription, the service is customized to fit with the way Hornblower operates. Security information is thoroughly investigated and communicated with context rather than just thrown over the wall to Hornblower's team for investigation and remediation.

AWN CyberSOC provided Hornblower with a dedicated Concierge Security Engineer (CSE) who monitors their security data and events 24x7. Unlike other services, each Arctic Wolf customer is always serviced by the same CSE, who intimately understands the customer's security policies and operational policies. As a true extension of Hornblower's IT team, the CSE helps them fully understand any security issues and expertly advises on the necessary steps for remediation.

AWN CyberSOC includes

- Dedicated Concierge Security Engineer
- Managed SIEM
- Machine learning
- Monthly vulnerability assessments
- Threat feed subscriptions
- Regular security reviews

No more tiers – virtual security operations team

In addition to day-to-day operational support, AWN CyberSOC includes monthly vulnerability scans and quarterly security reviews. The reviews provide Hornblower's team with an understanding of their security posture with concrete recommendations for addressing any shortcomings.

AWN CyberSOC includes a managed SIEM and three different kinds of machine learning integrated with third-party threat feed subscriptions. Despite the sophistication of the technology, the installation process occurs in minutes and was described by Hornblower as "Fantastic!"

Getting Started: A preconfigured AWN Sensor was shipped to Hornblower and placed inline behind their firewall. Once installed, the sensor began analyzing network traffic data and scanning endpoints to assess whether there was any abnormal behavior. Deeper insights and protection were then enabled by using the sensor to collect system logs, Active Directory Information and other data such as NetFlow.

AWN CyberSOC detects threats missed by FireEye

Almost instantly, AWN CyberSOC provided value by detecting threats that had bypassed Hornblower's existing perimeter defenses. Shortly after being deployed, the Arctic Wolf CSE detected that a server was sending encrypted traffic to a known malicious website. Further investigation revealed that the server had been infected with malware, and this infection was not previously detected. Despite Hornblower having both a firewall and antivirus software, a key server had been infected, and the team would never have known without AWN CyberSOC.

Another security incident demonstrated AWN CyberSOC's ability to detect advanced targeted attacks. In a span of two weeks, the Arctic Wolf CSE detected two phishing attacks that were not detected by a FireEye EX appliance. The two separate incidents were part of the same phishing attack, highlighting the need to actively monitor indicators of compromise rather than assuming that one-time detection results in ongoing protection. The attacks were detected and remediated within four minutes of detection, and any potential loss or disruption was avoided.

Arctic Wolf is a True Partner

Hornblower selected Arctic Wolf because AWN CyberSOC is the industry's easiest threat detection and response service to install. Arctic Wolf is a trusted security partner to hundreds of mid-market companies. Companies serving large enterprises tend to have a static offering that is inflexible or requires hundreds of thousands of dollars of professional services. Arctic Wolf works with each customer to understand their business and the best way to work with the business. Being a small IT shop, Hornblower really needed to minimize their administrative overhead, and AWN CyberSOC fulfilled that requirement.

Arctic Wolf does not just design a solution and leave it for the customer to manage. They work with a customer's existing infrastructure and provide the robust monitoring and detection required for vigilant cybersecurity. Hornblower now has peace of mind knowing their security operations have the consistency and coverage of a 24x7 SOC, and they were able to achieve this for a fraction of what it would have cost to do it themselves internally.

Arctic Wolf Networks, Inc. / 111 West Evelyn Ave., Suite 115, Sunnyvale, CA 94086 / T 1.888.272.8429 / www.arcticwolf.com