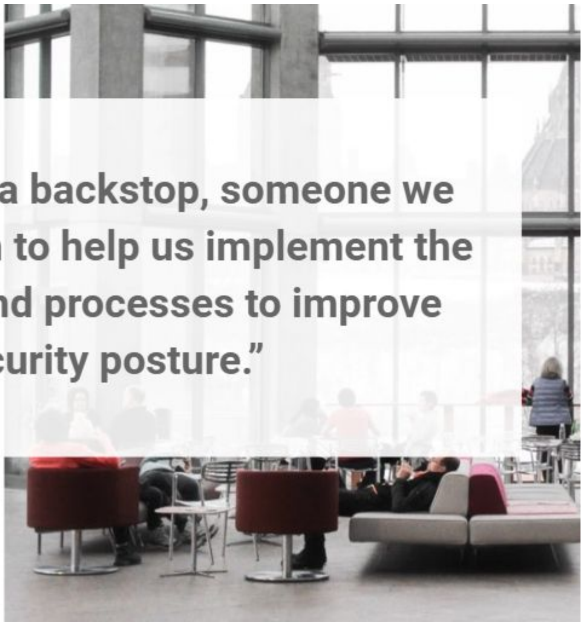
GuardSight Helps AFEX Double Threat Detection Rate

Experienced cybersecurity as-a-service provider enables financial services company to improve cybersecurity posture and boost team morale

Background

When it comes to cyber attacks, financial services companies fall in two camps, according to a PwC 2018 report.[1] Those that come under fire. And those that will.

So it’s no surprise that AFEX, a mid-sized financial services company with a global customer base, wanted to be battle ready. But it faced challenges. It had only a small team of junior security analysts, and they lacked the support, both in knowledge and expertise, to manage IT security operations efficiently.



“We needed a backstop, someone we could rely on to help us implement the right tools and processes to improve our cybersecurity posture.”

“We needed a backstop, someone we could rely on to help us implement the right tools and processes to improve our cybersecurity posture,” said the AFEX information security director.

To carry out its mission, AFEX turned to GuardSight, an established provider of cybersecurity threat detection and response services.

Solution

Cybersecurity Assessment

AFEX first asked GuardSight to perform an assessment of the financial firm’s cybersecurity vulnerabilities.

Over the next two to three weeks, the GuardSight team worked closely with AFEX analysts to evaluate the firm’s software and hardware for weaknesses as well as technical flaws that could potentially be exploited by cyber attackers.

The assessment revealed vulnerabilities in the firm’s customer-facing web applications, some of them critical. As a result, GuardSight offered remediation solutions that AFEX could deploy to fix the problem. However, a retest performed by GuardSight following the remediation showed the vulnerabilities were still present.

Cybersecurity Assessment
Cybersecurity Operations
Increased Threat Detection Rate
Improved Team Morale
A Successful Partnership

By then, AFEX had made its own assessment. The company determined that GuardSight’s capabilities would help AFEX improve its cybersecurity posture. It also realized that GuardSight’s culture of discipline and commitment to the work could have a positive impact on its young analysts.

At that point, AFEX decided to hire GuardSight as a managed security services provider (MSSP) and support AFEX’s internal security operations (SECOPS).

Cybersecurity Operations (SECOPS)

The GuardSight team took a methodical, systematic approach when implementing SECOPS for AFEX.

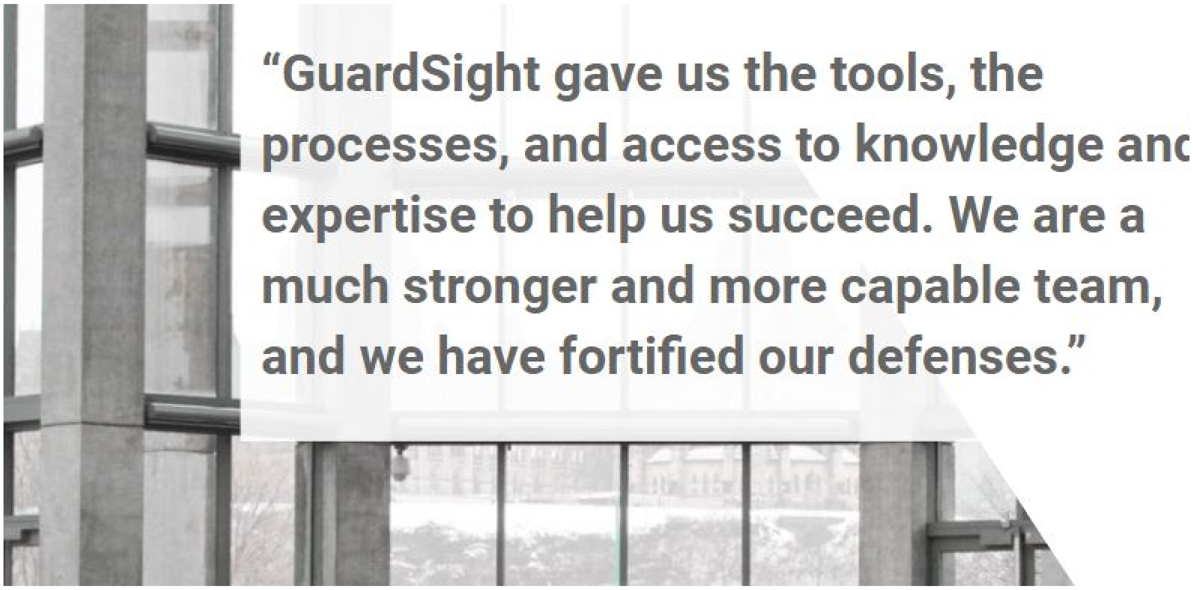
One of the first tasks GuardSight carried out was designating a 24/7 handler on duty (HOD) from the GuardSight team to manage, escalate and coordinate responses to incoming alert data. The HOD was on the scene almost immediately to ensure no cyber threat went undetected.

At the same time, GuardSight deployed an arsenal of tools and systems, which it refers to as cyber weapons, to help AFEX more effectively monitor, prioritize, and respond to cyber threats. These tools complemented AFEX's existing tools and were put in place within 72 hours.

With the necessary security established, GuardSight began the next phase of the project: collaborating with the AFEX team to proactively hunt down and isolate threats. Machine learning played a significant role by helping to prevent and detect unique attacks. For more severe attacks, GuardSight deployed a quick reaction force of senior analysts to investigate and manage containment.

Throughout the process, GuardSight continuously tested all cyber weapons – both AFEX's and its own -- for functionality, availability, performance, and integrity. These weapons included endpoint detection and response systems, intrusion prevention systems, web application firewalls, central logging systems, and security information and event management systems, to name a few.

GuardSight gauged the implementation's success by tracking key performance indicators and key risk indicators, such as the number of security alerts according to intent and severity, daily averages, and response times. The two teams used this information to guide security enhancements and reduce risk.



“GuardSight gave us the tools, the processes, and access to knowledge anc expertise to help us succeed. We are a much stronger and more capable team, and we have fortified our defenses.”

Success also relied on following industry standards and best practices. GuardSight used the Cybersecurity Capability Maturity Model and Cybersecurity Framework to measure AFEX’s cybersecurity maturity and readiness.

Results

AFEX benefited from the SECOPS implementation in multiple ways.

Increased Threat Detection Rate

First, AFEX doubled its threat detection rate. “GuardSight increased our capacity tremendously,” said the information security director, “just by keeping an eye out for threats, bringing in new tools, and augmenting our existing tools.”

Tools don’t work on their own, however. GuardSight helped AFEX manage and prioritize threats through a choreography of processes. This enabled AFEX to separate the signal from the noise, so the firm could determine which threats were important and respond more quickly than before.

GuardSight’s own responsiveness and availability had an impact as well. GuardSight’s ability to act fast has enabled AFEX to contain critical threats. “When I need to bring in someone with a high level of expertise to take care of a problem, that’s a big plus,” the information security director said. “I get enormous value from that.”

Improved Team Morale

GuardSight's knowledge and experience had a positive impact on the whole AFEX team.

"I have good analysts, but they don't have the years in the trenches that the GuardSight team has," the information security director said. "GuardSight fostered a culture of commitment and passion for cyber. My staff has learned a great deal from working with GuardSight's senior analysts, and they now have more confidence."

AFEX has benefited from GuardSight's expertise, too. It regularly bounces ideas off the GuardSight team and gets recommendations on tools that GuardSight uses with enterprise clients.

A Successful Partnership

GuardSight continues to serve AFEX as an MSSP, and the two parties have a great working relationship.

"GuardSight gave us the tools, the processes, and access to knowledge and expertise to help us succeed," said the AFEX information security director . "We are a much stronger and more capable team, and we have fortified our defenses."

John McGloughlin, GuardSight CEO, agreed. "AFEX has vastly improved its threat detection rates and its ability to investigate alerts related to threats. They also understand that ultimately, this is warfare, and the enemy never gives up. They can't ever let their guard down."

---

[1] Top financial services issues of 2018, PwC, https://www.pwc.com/us/en/financial-services/research-institute/assets/pwc-fsi-top-issues-2018.pdf

---