SightGain

CUSTOMER CASE STUDY

Building an Operationally Effective Cyber Program

The Threat of Zero Visibility

Top-grade, high value technology assets are constantly threatened by sophisticated cyber actors, but their defensive capabilities are often not adequately tested. From boundary protection to critical mission systems, these unknown gaps in cyber performance represent a very real danger to certain organizations and throughout their departments. In this instance, the client launched new cyber defense teams responsible for protecting systems throughout their organization. These teams were setting up their cyber vulnerability assessment technology and establishing processes from scratch. Leadership needed to know how to optimize processes and technology to effectively repel attacks and train analysts.

An Opportunity to Validate Security Spend

SightGain's Threat Assessment processes and technology provided the right combination of live-fire testing* and real-time analysis to evaluate the client's prevention, detection, response, and remediation capabilities. In this case study, a team from SightGain, Verodin, and Deloitte worked together to identify the client's level of cybersecurity readiness within one of its teams, focused on four objectives:

1. Identify any performance gaps in cybersecurity technology, process, and staff, thereby protecting mission-critical defense systems.
2. Verify blocking, detecting, alerting, and correlation procedures.
3. Document the accuracy and timeliness of the client's cybersecurity analysts with empirical data.
4. Implement an automated system to continuously monitor and improve cybersecurity readiness.

Ultimately, organizational leadership hoped to develop a repeatable process to better equip their teams, optimize their technology, and defend high-value assets.

> "It's easy to assume that your systems are ready for detecting or responding to an attack. But you don't know if you're ready until those attacks are actually tested across your network."
>
> — TEAM LEAD

*Live-fire testing involves the execution of actual vulnerabilities against production networks in real-time to gauge the actual efficacy of in-situ teams, technologies, and processes.

Testing Performance in a Live Environment

The project team collaborated with leadership to integrate its solution into the internal cyber defense system for the cyber defense team to safely execute malicious cyber activity. Three software nodes simulated network activity, while a fourth tested endpoint protection. SightGain then recorded the speed and accuracy of the client's response to these threats, developing empirical performance data and uncovering defensive gaps in real-time.

> "The effort with SightGain was our first time coming close to operating with a live adversary. We got to see how the machine responded to an actual attack, and we could be destructive because it was virtualized."
>
> **— CYBERSECURITY LEADER**

From Assumptions to Accuracy

SightGain was installed within a few hours, and quickly it was generating surprising and crucial operational insights. In fact, the client's leaders were stunned. Given their significant investments in cybersecurity defenses, it was assumed that the attacks would be detected. However, of the 125 live-fire attacks, zero were detected by their cybersecurity tools or analysts. This startling discovery informed a new game plan to optimize their defenses. First, the team found and corrected an issue in the configuration files on the Intrusion Detection System. The team then continued to test and tune to improve the results. The findings from the engagement ultimately transformed the team's cybersecurity approach, shifting them from reliance on assumptions to a posture of continuous readiness.

The practical experience with real threats and clear insights provided by SightGain enabled significant performance gains for the cybersecurity team within days:

89% **Faster threat identification**

68% **Improvement in detection**

ZERO **Detrimental effects on the production system**

Today, teams within this organization have virtualized their entire network for training purposes, and new team members learn on the virtual system before transitioning to the production environment. Most importantly, the client has stopped guessing their preparedness and instead know they are equipped to test and continuously improve their cybersecurity performance.

About the SightGain Solution

SightGain's Continuous Readiness Platform is designed to find gaps and redundancies in the performance of people, processes, and technology in cybersecurity systems. It uses live-fire attack simulations to measure, quantify, and optimize cyber defense readiness.

SightGain

Learn more at SightGain.com