SightGain

Case Study

How SightGain Helped a Military Cyber Team Find and Fix Gaps in Their Defenses

The Threat of Zero Visibility

The U.S. military's technology assets are constantly threatened by sophisticated cyber actors, but its defensive capabilities are often not adequately tested. From weapon systems to classified data, these unknown gaps in cyber performance represent a very real danger to military branches and throughout the Department of Defense (DoD).

The Air Force launched new Mission Defense Teams (MDTs) responsible for protecting systems throughout the Air Force. These Air Force teams were setting up their cyber vulnerability assessment (CVA) technology and establishing processes from scratch. Their leadership needed to know how to optimize processes and technology to effectively repel attacks and train their analysts.

An Opportunity for Empirical Insight

Early versions of SightGain's Continuous Readiness processes and technology provided the right combination of live-fire testing and real-time analysis to evaluate the Air Force's prevention, detection, response, and remediation capabilities. A team from SightGain, Verodin, and Deloitte worked together to identify the Air Force's level of cybersecurity readiness within one of its MDTs, 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. Empirically document the accuracy and timeliness of Air Force cybersecurity analysts.
4. Implement an automated system to continuously monitor and *improve* cybersecurity readiness.

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

"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."

— AIR FORCE LEADER

Testing Performance in a Live Environment

The project team collaborated with Air Force leadership to integrate its solution into the internal cyber defense system for the MDT 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 Air Force'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."
>
> **— AIR FORCE LEADER**

UNITED STATES AIR FORCE

From Assumptions to Accuracy

SightGain was installed within a few hours, and within two days it was generating surprising and crucial operational insights. In fact, Air Force MDT leaders were stunned. Given the investment into their 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 the Air Force's defenses. First, the team found and corrected an issue in the configuration files on the Intrusion Detection System. Then, the team continued to test and tune to improve the results. The findings from the engagement ultimately transformed the MDT'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 Air Force MDT within days:

- 89% faster threat identification
- 68% improvement in detection
- Zero detrimental effects on the production system

Today, teams within the Air Force 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 Air Force has stopped guessing how prepared they are; instead, they're equipped to measure their readiness with precision.

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