Customer Case Study

Federal Systems Integrator

Federal Systems Integrator

"Working with ThreatStream has helped us be much more effective at defending against the simplest threats all the way to the most advanced threats that attempt to compromise our company assets on a daily basis."

Federal Systems Integrator CISO

Product:
ThreatStream Optic™

Industry:
Government

ABOUT FEDERAL SYSTEMS INTEGRATOR

This Federal Systems Integrator (FSI) is a proven provider of information solutions, engineering and analytics for the U.S. Intelligence Community, U.S. Department of Defense and other federal agencies. With more than 40 years of experience, this FSI designs, develops and delivers high impact, mission-critical services and solutions to overcome it's customers' most complex problems.

THE PROBLEM

Working primarily as a systems integrator with clients in sensitive intelligence and security communities, this FSI's intellectual property (IP) contains critical high-value information. This IP, essential to the U.S. government, must remain protected and secure.

On a daily basis, this FSI receives hundreds of Indicators of Compromise (IOCs) from multiple sources, and each IOC requires evaluation of the level of confidence behind the intelligence. Analysis of the data must:

- Consolidate important threat intel data
- Put the intel into context
- Decide if intel is pertinent and reliable
- Show where to focus and take action

The volume of IOCs combined with the need for accurate assessment created a significant challenge for this FSI—threat data management is time consuming and crucial, and yet is not the core mission of the company. This FSI needed to scale operations and use manpower resources more efficiently.

This FSI needed a way to speed threat intelligence validation and integration, and to do it without compromising information security. The company sought an automated threat intelligence solution that would work with this FSI's existing security information event management (SIEM) tools while reducing the time spent analyzing and operationalizing threat intelligence data.

THE THREATSTREAM SOLUTION

This FSI turned to ThreatStream for an automated cyber threat intelligence solution. The ThreatStream Optic™ platform counters adversaries by fusing actionable intelligence with existing security

infrastructure by:

- Consolidating and curating multiple threat intelligence sources while eliminating redundancies
- Providing cross-validated analysis
- Rapidly operationalizing intelligence with high confidence

"ThreatStream comes with a valuable reputation for providing quality intelligence in a timely manner, and their automated capability works seamlessly with the various cybersecurity tools you already have in your environment."

Before ThreatStream, this FSI staff spent thousands of hours annually to collect intelligence, sift through IOCs, validate intelligence and then operationalize that data by writing rules and actions into security infrastructure.

This FSI deployed ThreatStream Optic and immediately reduced the amount of time it took to not only identify valid threat intelligence, but also operationalize that threat intel by injecting it directly into this FSI's existing security tools. ThreatStream Optic connects with this FSI's SIEM through a single, cloud-based portal, consolidating, normalizing and validating intelligence. This seamless integration also eliminates the time and resource-intensive process of manually de-duplicating information from multiple feeds.

This FSI chose ThreatStream because the ThreatStream Optic platform, unlike other threat feeds, provides the additional benefit of cross-validation analysis. This FSI is able to take the threat intel received from ThreatStream and other sources and use ThreatStream Optic to determine with a high degree of probability what is valid intelligence, and act accordingly. ThreatStream allows this FSI to act on threat intel with a high degree of confidence.

The efficiencies created by ThreatStream Optic also allow this FSI to redeploy valuable human resources, which saves this FSI countless hours and thousands of dollars per year.

"Rather than taking us days to implement threat intelligence into our cybersecurity tools, with Optic, we can do it in minutes."

IMPLEMENTATION

ThreatStream provided this FSI integrations for multiple sets of technology architecture, ensuring a smooth implementation. This FSI's SIEM tools easily connect with ThreatStream's server to pull down and inject data directly into this FSI's security architecture stack. The threat intelligence provided by ThreatStream is viewed and used at this FSI's highest levels.

"The reliability of the data and depth of information the ThreatStream solution provides is top-notch. ThreatStream only delivers data that's been fully vetted, rich with context and insights, allowing us to take immediate action."

A PARTNERSHIP

"Working with ThreatStream is really a partnership. We have regularly scheduled discussions, and if we need anything, it's only a phone call away. It's easy to communicate with our ThreatStream team, and they are very receptive of what we ask of them."

ThreatStream Optic is the first threat intelligence platform that manages the entire life cycle of threat intelligence from multi-source acquisition to operational integration across the entire ecosystem of existing security devices. ThreatStream Optic enables enterprise and government organizations to seamlessly aggregate and analyze threat intelligence and automatically inject the information into their security infrastructure.

Organization

Federal Systems Integrator

Industry

Government

Challenge

Working primarily as a systems integrator with clients in sensitive intelligence and security communities, this FSI's intellectual property (IP) contains critical high-value information. This IP, essential to the U.S. government, must remain protected and secure.

Solution

This FSI turned to ThreatStream for an automated cyber threat intelligence solution. The ThreatStream Optic™ platform counters adversaries by fusing actionable intelligence with existing security infrastructure by:

Results

- *Consolidating and curating multiple threat intelligence sources while eliminating redundancies*
- *Providing cross-validated analysis*
- *Rapidly operationalizing intelligence with high confidence*