ThreatConnect

SUCCESS STORY

Transforming Cyber Threat Intelligence Operations at a Top 5 Global Software Company

Maturing Cybersecurity Infrastructure with Intelligence-Powered Operations:

Protecting the attack surface of a global software leader from a myriad of threat actors and attacks is no small feat. Given massive and increasing volumes of sophisticated threats, traditional approaches to operationalizing cyber threat intelligence (CTI) simply would not be effective.

Pain Point 1

Sophisticated threat actors are increasingly targeting software vendors as a way to infiltrate other companies from one environment to another attack surface.

Pain Point 2

A variety of technologies and workflow complexity leads to a lack of visibility and coordination across the entire organization, lowering defenses and increasing the risk of being breached.

Pain Point 3

As SaaS organizations grow and mature, they face the same challenges as large Enterprises face around defending cloud environments.

For one of the top 5 software companies in the world, they found themselves in exactly this situation - with teams spread out geographically, using a myriad of informal processes and tools, with no standardized method for collecting threat intelligence and operationalizing their actions. They needed a way to unify and manage their cybersecurity operations within a cohesive, scalable platform that could grow with them as the organization matured with its people, processes, and technology.

CUSTOMER'S PROFILE:

CUSTOMER SINCE: 2020

REVENUE: $40 Billion

INDUSTRY: Software

TEAM: Geographically Dispersed Security Teams

Customer Challenge

Primarily using manual methods to track Indicators of Compromise (IOCs)

Lack of context around OSINT feeds and understanding what is credible

Immature security stack with multiple silos

A solution that allows information to be easily shared between a Threat Intelligence Team and a Security Operations Team

Manage and analyze the collected threat data to characterize and prioritize into actionable threat intelligence for threat hunting, incident response, or security defense tools.

ThreatConnect's Solution

ThreatConnect's Collective Analytics Layer or CAL™ helps teams learn about the reputation of IOCs and apply classifiers to help facilitate faster decision making by prioritizing what matters most. CAL can help remove junk IOCs, determine credibility of IOCs, and identify which feeds to enable, equipping the team with the information needed to have a proactive defense.

ThreatConnect aggregates hundreds of OSINT and commercial sources of threat intelligence and allows teams to create their own prioritized threat landscape with internally derived threat intelligence as well. However, we don't stop there. Context on IOCs and known threat groups is critical.

With ThreatConnect's report cards, analysts can easily see any feed's performance to understand variables such as a feed's reliability rating and unique indicators, when it was first reported, and its scoring disposition. These insights are designed to help make better decisions during threat analysis and investigation.

ThreatConnect removes silos around data and connects processes between Cyber Threat Intelligence analysts, SOC analysts, and Incident Responders by providing a common platform for them to execute daily tasks and manage their workflows together.

When the team is freed up from focusing on manual and mundane tasks, morale improves and existing technology investments are able to be leveraged more strategically, and productivity and effectiveness can scale to meet the business needs.

10 OUT OF THE BOX SOLUTIONS

Creates a centralized repository of threat data to collect, contextualize and disseminate data to the security team and their tools. With ThreatConnect's SOAR, organizations can record, analyze, and interact with all of the information related to a case from one place. With this, teams can enrich cases leveraging internal and external threat intelligence and add learned intelligence back into the platform itself. This ultimately creates a feedback loop to ensure information is constantly being both gathered and applied for smarter decision making.

Free the team from mundane data collection tasks to focus on analysis and response. Leveraging the power of an integrated TIP & SOAR, this organization was able to harness the power of intelligence-driven operations to be more effective, resilient, and adaptive.

An intelligence driven approach provides intelligence on an adversary's capabilities, attack patterns, and informs how you build and configure your orchestration capabilities to defend your network better. Intelligence and orchestration together provide the situational awareness and context that is needed when trying to extract meaning from data and apply it within a changing environment.

ENHANCE INTELLIGENCE WITH GLOBAL CONTEXT

The ThreatConnect® Platform already helps you identify threats with your own data, but with ThreatConnect's CAL™, an innovative capability that distills billions of data points, it offers immediate insights into the nature, prevalence, and relevance of a threat. CAL provides global context that leverages anonymously shared insights from ThreatConnect users, open-source intelligence, malware intelligence and more, providing global context that has never before been available. This helps CTI teams to manage the number of false positives for threat monitors and identifies pockets of intelligence that are fertile hunting grounds for teams of all sizes and maturity levels.

MAKING THE LANDSCAPE MANAGEABLE

Even for the most skilled teams, keeping up with the threat landscape, complex IT environments, evolving regulatory environments and constant security alerts is not easy to achieve, much less quickly. This organization recognized their need to mature their security operations and chose their solution based on the concept of leveraging intelligence-driven operations. It was imperative that they have flexibility to control the right levels of automation and having the ability to automate entire actions or specific aspects of actions fit their unique needs.

Leveraging ThreatConnect's Playbooks to automate and solidify their processes, and Case Management capabilities to memorialize and structure their workflows, they were able to reduce the time it takes to uncover relevant threat intelligence while working cases and mitigate the risks of spending significant time chasing false positives. Using customizable dashboards, they were able to visualize the data and monitor security operations and intelligence across teams, which enabled them to quantify their return on investment of automating and orchestrating their activities over time.

A PARTNERSHIP TOWARDS MATURITY

Reaching their strategic goals of maturing their security operations is not an overnight transformation. By reducing the amount of repetitive manual tasks, analysts are able to collaborate cross-functionally, including those outside the security team, and support multiple teams all in the same platform that provide a single source of truth that can be easily shared and operationalized. This enables teams to work together seamlessly regardless of geography, timezone, or job function, leading to a unified organizational cybersecurity defense. ThreatConnect laid the foundation for intelligence-based decision-making and cross-team collaboration, equipping them with an infrastructure they can build upon for years to come.

1 https://www.forbes.com/sites/forbestechcouncil/2021/02/25/its-dirty-little-secret-manual-processes-are-still-prevalent/

About ThreatConnect®

ThreatConnect enables security operations and threat intelligence teams to work together for more efficient, effective, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse threat intelligence and cyber risk quantification into their work, allowing them to orchestrate and automate processes to respond faster and more confidently. Nearly 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their most critical systems. Learn more at www.threatconnect.com.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

Call 1.800.965.2708 or visit threatconnect.com/request-a-demo/

ThreatConnect

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708