

### **Maturing Cybersecurity Infrastructure** with Intelligence-Driven Operations

Equipping a Multinational Cloud Computing SaaS Provider with a **Foundation that Scales** 

It's not hard to imagine the cybersecurity challenges of a global cloud computing network, providing applications and services to businesses who depend on accessing their data as well as maintaining visibility and control of their information. Cyber risk is an evolving landscape, and there is no shortage of regular attacks by malicious actors who steal or ransom data, or those who simply misuse or fail to maintain control of data and find themselves out of compliance with an industry requirement.

What is hard to imagine is a global security operations center that is primarily using manual methods to handle security alerts and triage. A recent Forbes<sup>1</sup> article calls it a "dirty little secret" that two-thirds of tasks are not automated across IT functions. and especially so in a large enterprise organization.

There are many reasons why this is the case, from implementation challenges and costs, to complexities within the technology stack, or the silos that widen when using disparate tools and technologies across teams.

For one of the world's leading computer technology companies, 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.

# **PROFILE:**

**CUSTOMER'S** 



**CUSTOMER SINCE:** 2020





TEAM: Geographically Dispersed **Security Teams** 

**Customer Challenge** 

## ThreatConnect's Solution

stack with multiple silos

**Immature security** 

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.

ThreatConnect removes silos around data and connects processes between SOC analysts, Incident Responders,

and Cyber Threat Intelligence analysts by providing a common platform for them to execute daily tasks and

ThreatConnect's Collective Analytics Layer or CAL™ helps teams learn about the reputation of IOCs and

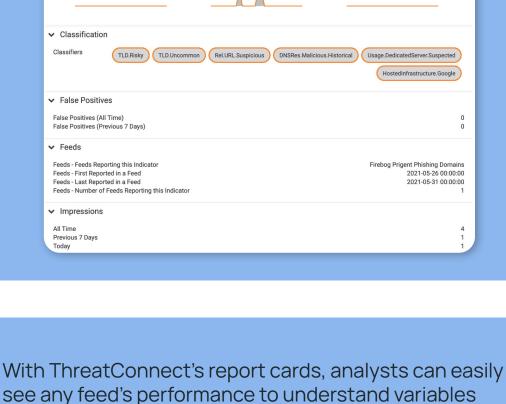
track Indicators of Compromise (IOCs)

manual methods to

**Primarily using** 

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. CAL™ Insights ✓ Trends Daily False Positives Daily Impressions Daily Observations



credible

A solution that allows

easily shared between

a Threat Intelligence

**Team and a Security** 

information to be

Lack of context around

understanding what is

**OSINT** feeds and

Bambenek TLD.Uncommon TLD.Risky TorExitNode PrivateNetwork

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.

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

**Operations Team** 

Manage and analyze the collected threat data

prioritize into actionable

threat hunting, incident

threat intelligence for

to characterize and

#### 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

An intelligence driven approach provides intelligence

informs how you build and configure your orchestration

on an adversary's capabilities, attack patterns, and

to be more effective, resilient, and adaptive.

response, or security defense tools.

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.



#### MAKING THE LANDSCAPE MANAGEABLE Even for the most skilled teams, keeping up with the threat landscape, complex IT

**ENHANCE INTELLIGENCE WITH GLOBAL CONTEXT** 

providing global context that has never before been available.

ThreatConnect's CALTM is an innovative architecture that distills billions of data

points, offering 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,

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. They were looking for a partner to come alongside them, helping them recognize and set critical benchmarks for their processes and programs as it grows and changes over time. ThreatConnect's Customer Success team is committed to helping to minimize risks and maximize the value that an integrated TIP and SOAR platform brings. The Customer Success team helped them as they defined their strategic and tactical objectives, and worked alongside them to configure and deploy their instance and required integrations. Ultimately, 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.

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



ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and Al-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights, and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

3865 Wilson Blvd., Suite 550 Arlington, VA 22203

sales@threatconnect.com +1 (800) 965.2708

Learn more at <u>www.threatconnect.com.</u>

ThreatConnect.com