CUSTOMER CASE STUDY:

ANOMALI

Anomali Centralizes Threat Intelligence for a Global Financial Markets Infrastructure Provider

OVERVIEW

INDUSTRY
Financial Services

SIZE OF COMPANY
25,000+, 100 in the SecOps team

LOCATION
United Kingdom

Anomali Products:

Threatstream

- The core driver of the customer's threat intelligence, ThreatStream, allowed them to ingest, process, deduplicate, and distribute on a massive level without any scalability challenge.
- ThreatStream delivered standardized models for parsing and distributing via API integrations, which enabled a one-click model to consume and ingest data.

ANOMALI MATCH SECURITY ANALYTICS

- Anomali Match Security Analytics is used for IOC (indicators of compromise) matching, which had previously been a challenge since 90% of their threats were known. Match Security Analytics allows security analysts to more e ciently separate signals from noise and focus on high-priority events, which can be particularly challenging as the organization scales up.
- Anomali Match Security Analytics is also a better and far more resilient option than a traditional SIEM (security and information event management), which struggles to match millions of indicators. Additionally, running millions of IOCs on a SIEM is not only significantly more expensive, SIEM is also far more constrained due to storage limitations.
- The customer is able to run Match Security Analytics out of a single AWS instance. Splunk by comparison would require a minimum of 4 instances just to get the process started.

Customer Pain Point:

The customer, a global financial information company, had a core requirement to centralize threat intelligence while being able to support a broad range of premium third-party feeds, which meant integration was a critical security enabler. Their SIEM (security information and event management) solution struggled to correlate the quantity and historical relevance of threat information that was entering their system, which put significant constraints on their threat-hunting capability.

Solution:

Anomali directly addressed the need for actionable intelligence delivered in minutes, rather than weeks, by effectively taking the customer's security infrastructure to the next level in terms of identifying and contextualizing threats and automating security workflows via SOAR integrations: QRadar, Splunk, Intezer, and ThreatWorx (via ThreatStream).

"We need to on-board and off-board vendors that are / aren't performing and do it quickly—with Anomali we don't need to build our own parsers. It's not just about cost, but the complexity of on-board/of-board."

– CUSTOMER (ANONYMOUS)

Results:

The results associated with the Anomali implementation have been successful to the point where any new security technologies are required to integrate with Anomali prior to implementation. The automation enabled by Anomali provides a central source of Cyber Threat Intelligence workflows supporting Security Operations, connecting the right intelligence sources to an actionable operational framework.

The Anomali Impact:

For this global financial markets infrastructure and dataprovider, the ability to ingest all intel data in one platform is a significant time saver—ThreatStream provides near real-time access to threat models (actors, campaigns, TTPs), as well as intelligence enrichment, coupled with theability to send high-fidelity indicators to different security tools, driving actionable visibility across the organization.

The customer has integrated Anomali Match Security Analytics with their D3 SOAR instance via Anomali APIs and script actions, which increases the fidelity of information feeding into automated workflows. Between the use of ThreatStream and Match Security Analytics, the customer now has the ability to match significantly larger amounts of both current and historical data in a timeframe measured in minutes, rather than weeks.

The customer's partnership with Anomali has elevated its operational intelligence capabilities via a near real-time threat model correlation, enabling them to quickly answer the question "Have I been affected?" and triggeringautomated workflows to both implement an immediate incident response and disseminate critical security information across the organization.

Through Anomali, the customer is able to see which threat actors and malware initiatives are targeting them by correlating all tra c (including blocked). This capability allows for further analysis using Anomali to understand MITRE ATT&CK techniques and overlaying security controls to understand risk and perform risk reduction initiatives.

"We found information in the news media that a Tier 1 threat actor was targeting us. This was quickly validated by Match Security Analytics and contextualized by ThreatStream. This enabled a security control to not only stop the threat but also provided the context to execute the right next steps to ensure we are continually protected. We found lots of vendors who made promises, but only Anomali delivered."

– CUSTOMER (ANONYMOUS)

Why Anomali?:

The financial services company started with an in-house solution that had integrations into several competitive solutions. As their needs grew and security challenges became sharper, they assessed the need for something better suited to their increasingly complex requirements.

After an exhaustive review, Anomali was chosen as the best option; there were no technical limitations, and Anomali offered a high-stability platform that does not slow down when new feeds are integrated into the system. This choice was validated in its performance; the customer has millions of IoCs entering the system per week, and there have been absolutely no performance issues. As a side note, this customer is also the largest Anomali Match Security Analytics user by volume.

Anomali is headquartered in Silicon Valley and is the Leading AI-Powered Security Operations Platform that is modernizing security operations. At the center of it is an omnipresent, intelligent, and multilingual Anomali Copilot that automates important tasks and empowers your team to deliver the requisite risk insights to management and the board in seconds. The Anomali Copilot navigates a proprietary cloud-native security data lake that consolidates legacy attempts at visibility and provides first-in-market speed, scale, and performance while reducing the cost of security analytics. Anomali combines ETL, SIEM, XDR, SOAR, and the largest repository of global intelligence in one efficient platform. Protect and drive your business with better productivity and talent retention.

ANOMALI

© Copyright 2024 Anomali®. All rights reserved.
ThreatStream® is a registered trademark of Anomali Inc. Anomali Match™ ("Match") and Anomali Lens™ ("Lens") are trademarks of Anomali Inc.