CUSTOMER CASE STUDY:

ANOMALI

Anomali Helps the Centers for Medicare & Medicaid Services Reduce Third-Party Risk

Customer Pain Point:

The Centers for Medicare & Medicaid Services (CMS) is the single largest payer for healthcare in the United States. Part of the US Department of Health and Human Services (HHS), CMS administers the Medicare program and works with state governments to administer Medicaid, the Children's Health Insurance Program (CHIP), and health insurance portability standards. Providing health coverage to more than 100 million people, CMS bears a significant responsibility for securing personally identifiable information, financial data, health records, and other highly sensitive data its work involves. The agency's extended operational ecosystem makes it challenging to fulfill this duty.

While relatively small in itself, CMS works with a large number of contractors and suppliers. If any of these third parties are the victim of a phishing attack or the exploitation of a vulnerability, the agency's data can also be at risk of a breach. As the CMS security team works to address a broad range of priorities, from cybersecurity supply chain risk management, control assessments, and continuous diagnostics and mitigation (CDM) to security operations, it must also maintain a high level of visibility and insight to ensure effective incident response and management wherever such events might occur.

To meet this requirement, CMS must bridge traditionally siloed security teams and ensure comprehensive visibility into its security posture across the organization. This includes translating a high volume of raw threat intelligence data into relevant, prioritized insights correlated to its systems and data and distributing this information as security analyst updates for executive leadership, political appointees, and other senior-level personnel.

OVERVIEW

INDUSTRY
Federal Government

SIZE OF COMPANY
6,000 employees

LOCATION
Baltimore, MD
United States

Solution:

Why Anomali? CMS wanted a threat-centric view of their security environment in order to stay ahead of potential and actual threats by automating workflows for two-way information sharing within CMS Cybersecurity Integration Center (CCIC) and CMS's data centers.

CMS adopted an Anomali solution to gather and share threat intelligence throughout its organization effectively. A combined CTI team from CMS and Anomali worked as one to develop strategic goals and implementation tactics for Anomali's threat intelligence solution - ThreatStream. Anomali Engineering worked with CMS Engineering to develop server-hardened, FIPS-enabled systems and integrated the Anomali Threat Intelligence Platform with elements of the CMS security ecosystem.

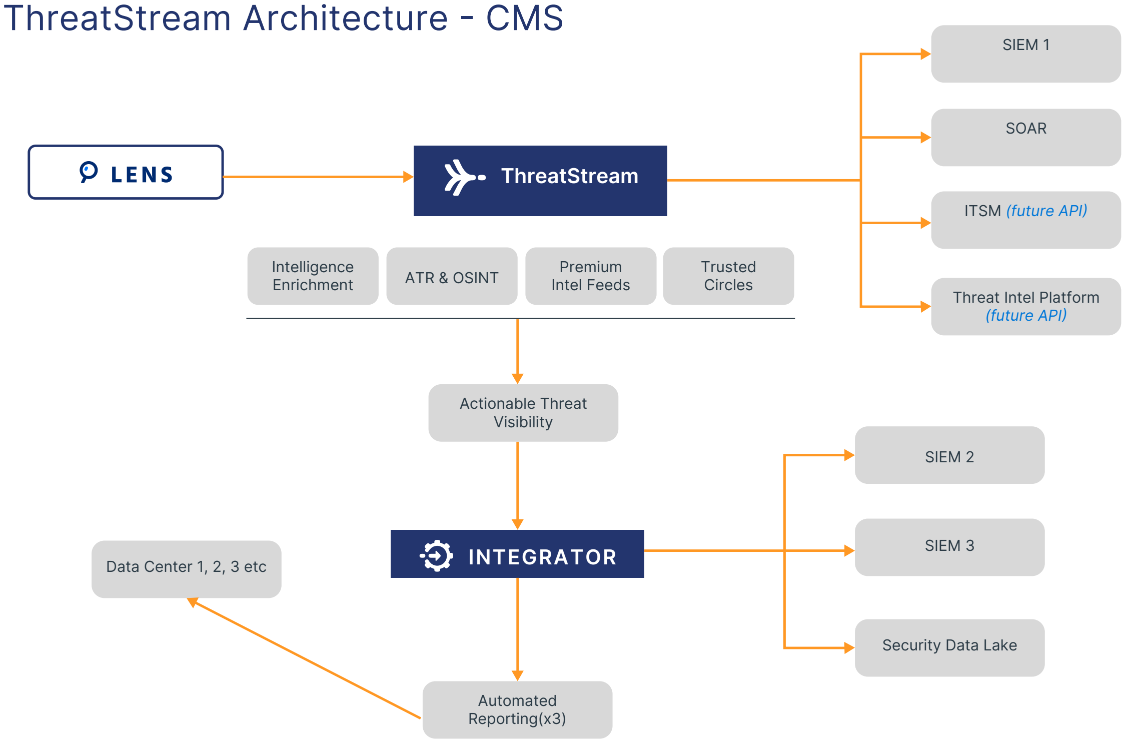
Anomali has integrated with the agency's SIEM and data lake environments.The Anomali Threat Intelligence Platform now provides near real-time threat data as a valuable enrichment source for security operations initiatives. Indicators of compromise (IOCs) and indicators of attack (IOAs) are correlated with relevant security telemetry from the agency's systems to highlight areas where heightened measures or remediation are needed. Anomali intelligence is also fed into the CMS fusion center and used to provide insights to stakeholders throughout the organization.

Anomali Products:

THREATSTREAM

The world's largest threat repository, Anomali ThreatStream captures raw threat data in near real-time for instant correlation across millions of logs, IOCs, and IOAs. The agency uses ThreatStream primarily as an intelligence sharing platform, including both insights for stakeholders and threat data fed directly into other security systems. Integrations include three SIEM systems, a security Data Lake, a SOAR solution, STIX/TAXII, and a global integrator.

ThreatStream Architecture - CMS



Results:

The Anomali solution has performed exactly as CMS intended, helping it share relevant threat information across stakeholders and systems through cyber threat intelligence briefings, status reports, incident response information, a cyber threat intelligence tracker, and collaboration and coordination with internal and external entities.

Anomali ThreatStream is now a key component of the agency's security ecosystem. The agency is currently focused on establishing processes to track retrospective metrics around past security incidents and leading metrics focusing on exploitable vulnerability density and program-specific measurements.

The Anomali Impact:

As CMS improves its security posture, ThreatStream is key in managing its third-party risk and preventing damaging data breaches. Threat data from Anomali ThreatStream is pulled into the agency's security data lake, correlated with SIEM log data, and used to help enrich proactive security initiatives such as threat hunts and compliance assessments. Insights from intelligence feeds are presented in natural language to clearly understand active threats, including tactics, techniques, and procedures (TTPs) and their relevance to the CMS environment. High-quality analyst products can be generated more quickly and efficiently, helping stakeholders at all levels understand the agency's risk and the measures that can be taken to mitigate it. Controls within ThreatStream help the agency meet compliance requirements.

The CCIC reports that the Anomali solution has played a crucial role in its top focus of disseminating intelligence with partners. Integration and automation have made it possible to share timely and valuable information to stop threats and strengthen security across the agency's environment.

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