CUSTOMER CASE STUDY:

ANOMALI EMPOWERS STATE GOVERNMENTS AGAINST THREAT ACTORS

ANOMALI

CHALLENGE

State governments need to track different threat actors targeting their network and share intelligence quickly and efficiently to defend against cyberattacks. The state cybersecurity operations team quickly realized it needed to massively improve its ability to share and operationalize threat intelligence across a platform because different threats hit different departments and the team did not have enough time or resources to properly pursue those threats.

SOLUTION

Anomali ThreatStream surfaced all the relevant threats the state government faced, which allowed the team to properly investigate each threat. The state government found a fast, automated method of communicating through Anomali's solution so that they could detect attacks in real time.

RESULTS

- Complete visibility into threat landscape
- Time savings for security professionals
- Faster, more accurate threat detection and alerting
- Reduced malware infections
- Successful blocking and detection of ransomware

Overview

State governments in the United States are the target of many cyberattacks. State governments maintain and operate many of the most fundamental infrastructures, including energy, water, and transportation. State governments also store vast amount of confidential information such as social security numbers and licenses. Even though they provide critical services and store sensitive information, they often do not provide a high level of cybersecurity protection for their IT systems. These features make them a very compelling target for threat actors.

State Government Challenge

Securing all this infrastructure, data, and systems against cyberattacks is typically the responsibility of understaffed and underfunded cybersecurity teams. In fact, some of the most difficult areas to defend against these cyberthreats exist at the state and local levels. With only a small cybersecurity team overseeing the systems, the state recognized the need for stronger cybersecurity solutions. State governments have to protect sensitive information and infrastructure while operating under financial and staffing constraints.

> "The only way that we can win is by putting automation in place, doing the things that can free up the analysts and engineers to focus on more unique threats and their secret sauce that's happening at each individual organization" said the CISO.

The Anomali Solution

The state government turned to Anomali to solve for these challenges in automation, lack of threat intelligence, and sharing capabilities. Anomali's solutions include multiple integrations with leading malware sandboxes, endpoint protection solutions, and other controls to accelerate investigations and response.

The state government found that it was conducting faster investigations and creating threat intelligence that could be operationalized into existing security controls for automated and immediate detection and blocking across its environment.

Anomali ThreatStream seamlessly integrated into their existing technologies, so staffers did not need to reroute their analysis process and could implement early investigations from a single centralized platform. The dashboard features, which allow security operations to see what intelligence it is ingesting and integrating across its infrastructure, were extraordinarily helpful in increasing productivity for the cybersecurity team.

The Anomali Impact

One of the biggest key challenges in cybersecurity is information overload. Relevant information is needed so that they can act quickly without being overwhelmed with unrelated issues. Prior to Anomali, the state government cybersecurity operations team had no way of knowing if it was receiving and integrating relevant threat intelligence needed to detect and block threats it was facing.

In one of many instances that the state government realized huge benefits was a hacking incident that came through the cloud against another department in the state. The state CISO was able to quickly lock down the case, share the relevant indicators of compromise on Anomali ThreatStream, and provide them to the other local entities that were also worried about a similar attack happening to them. Not only did Anomali save the SecOps team essential time, but it also provided a secure means to share those indicators fast in what was a major attack that made national news.

With Anomali, this state government has achieved numerous, measurable results. It has managed to avoid being breached, successfully detected and blocked ransomware attacks, saved staffing time cost, and elevated their threat visibility.

> "We're limited at every level on the number of cybersecurity resources we have. So it might be that the CIAC, our information analysis center, can handle one incident and the secretary of state's office is going to handle a different incident depending on resource availability. So Anomali gave us a platform where we could all help each other and come together when we needed it on a bigger issue" stated the CISO.

About Anomali

Anomali offers intelligence-driven extended detection and response solutions that help organizations quickly identify and respond to threats in real-time by automatically correlating ALL security telemetry against active threat intelligence to expose "(un)known" threats. Anomali Match uses automation to correlate tens of millions of threat indicators against your real time network activity logs and up to 5 years of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred.

ANOMALI