Customer Case Study:

State of Maryland

Background:

CUSTOMER NAME:
State of Maryland

INDUSTRY:
Government

LOCATION:
United States

Overview:

The State of Maryland has an outsized presence in the cybersecurity domain due to its proximity to Washington DC and all the associated security entities that operate in the area. In spite of this, the state's cybersecurity programs are relatively new, and the state is also responsible for coordination across multiple government levels (state, local, etc.). The state has always been (and will continue to be) a high-profile target, so the implementation of a robust and cohesive cybersecurity program is critical.

Customer Pain Point:

The state suffered several significant cyber incidents, which drove the need for executive (state government level) oversight. They were also subject to complex cybersecurity implementation models (Centralized, Federated, or Decentralized) depending on the specific entity involved. Because of this, there was often poor internal security alignment across government entities.

The senior cybersecurity team knew they needed to invest in advanced security solutions but ran into issues rationalizing it at the executive level. Because of the variances in implementation models, Shadow IT was also a significant challenge, effectively driving how often new vulnerabilities were introduced into the system.

Anomali Products:

- **ANOMALI MATCH SECURITY ANALYTICS**
- **ANOMALI THREATSTREAM**
- **LENS +**
- **INTEGRATOR**
- **THREATSTREAM COMMUNITY (POWERING MD-ISAC)**

Results:

The state essentially began its cybersecurity program from a blank slate, so the improvement in its security posture with Anomali was immediate, noticeable, and effective. The implementation of a strong cybersecurity program was critical in addressing threats from asymmetrical and nation-state cyber adversaries. They also had the advantage of strong support at the executive level of government but were also expected to show results quickly.

Benefits:

Incident response times are now measured in minutes rather than weeks, and the state now has integration and contextualization of a broad range of data feeds (including OSINT and Premium).

ANOMALI

Competitors:

The State of Maryland has been using Recorded Future, which the state sees as complementary to Anomali. Overall, they were looking for a way to leverage a broad range of threat intelligence feeds that were coupled with premium data. By bringing in Anomali they were able to leverage and significantly accelerate their existing security investments.

The Anomali Impact:

The state IT Department has hit its objective of a response time measured in seconds. While they are still in the process of rolling this technology across the state, there have been significant, measurable overall improvements. At this point, the state has far better visibility into threats, coupled with better communication across government entities to review threats. They also leveraged Anomali to create an MD-ISAC, which has had significant, positive effects across multiple levels of government.

> "Creating actionable intelligence and then acting on it is the most effective tool that we have to defend ourselves against all classes of cyber adversaries, from nation states to hacktivists."

– ANONYMOUS, STATE OF MARYLAND

ANOMALI