CYWARE™ | Case Study

Major US State Leverages Cyware to Reinforce Cyber Defenses with Unified Threat Intelligence Management

State, Local, Tribal, and Territorial (SLTT) entities in the United States are tasked with processing and enriching over a million observables weekly to deliver actionable threat intelligence to state agencies. Overwhelmed by the enormity of the task and constrained by time-sensitive deadlines and specific threat intelligence requirements, one of the largest state entities turned to Cyware when their existing Threat Intelligence Platform (TIP) was not performing as expected.

The Cyber Risk Challenge: Phishing Triage at Scale

In accordance with security operating procedures, phishing scams and other suspicious email communications received by the State's agencies are forwarded to a designated cyber threat team for analysis. This team must ingest, process, and analyze these messages, then return the underlying intelligence and any recommended actions back to the reporting agency for action.

Challenges included creating effective and actionable intelligence feeds and enrichment at the scale of hundreds of thousands per week, and sharing this information with various public sector entities. The intelligence needed to be clear and concise to avoid overwhelming state agencies with irrelevant data.

Additionally, the cyber threat team used the new threat intelligence to update its own security posture, integrating threat information into tools such as Cisco FMC, Gravwell SIEM, and Tipping Point SMS.

Technical Barriers Preventing Protection

Prior to adopting Cyware, this cyber threat team struggled to handle their threat intelligence demands at scale. The team curated the intelligence received based on specific requirements and needed to disseminate the finished threat intelligence reports within a timeframe that allowed state agencies to act on it effectively. This hindered the team's ability to properly triage phishing emails and campaigns targeting public sector agencies, leaving state agencies vulnerable to attack.

Additionally, the cyber threat team's current TIP had difficulties connecting via STIX/TAXII with both internal and external tools.

Leveraging Cyware to Remove Response Roadblocks

After hearing about Cyware from their Information Sharing and Analysis Center (ISAC), the cyber threat team decided to adopt two Cyware solutions, Cyware Orchestrate and Cyware Intel Exchange, to meet their unified threat intelligence processing and response goals.

It quickly became clear that Cyware directly addressed the challenges the cyber threat team faced prior to adoption. Bespoke TAXII support and strong STIX mappings made threat intelligence exchange much easier, features that had notably not worked as needed from the state's previous TIP.

Bespoke TAXII support and robust STIX mappings

Advanced automation capabilities

Seamless dissemination of actionable intelligence at scale

A true force multiplier for cyber threat detection and response

Cyware Orchestrate provided advanced automation beyond what typical TIPs could support, handling unique use cases and creating enrichment pathways where custom integration was necessary. Cyware Orchestrate also included Intel Management tools to help expand overall logical workflows.

Additionally, the speed at which Cyware Intel Exchange ingested, processed, enriched, and disseminated threat intelligence allowed the cyber threat team to significantly increase output.

Ultimately, it was the combination of Cyware tools and Cyware's tailored attention to the cyber threat team's needs that made the difference.

> **"We did a major version upgrade and were extremely happy with Cyware's open communication about expectations and rapid response to resolve a couple of issues," said one key practitioner on the cyber threat team. "Our former TIP vendor never did this."**

Timing in the Turnaround: The Ultimate Proof

Cyware's implementation was a complete success. As noted by a key stakeholder from the state,

> "We were able to connect the Cyware platform with external intelligence exchanges and our own internal tools via STIX/TAXII in one hour. We accomplished more in one hour than we did with our previous TIP provider in one year."

About Cyware

Cyware is leading the industry in Operationalised Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, as well as hyper-orchestration and automation—eliminating silos and enabling organisations to outmanoeuvre adversaries faster and more effectively.

Learn More

Request a Demo Today