CYWARE™ | Case Study

Major UK Government Organisation Uses Cyware to 'Defend as One' with Unified Threat Intelligence Management

A major UK government organisation was overwhelmed with the need to disseminate vast amounts of threat information to its industry dependents – analysed, relevant to the recipient, and in real-time.

Operating as a critical hub in the "Defend as One" initiative, meeting mandated threat intelligence sharing and collaboration requirements was not only a matter of security, but of compliance.

The Scope of the Challenge

The government organisation was tasked with collecting and processing vast amounts of threat data within disparate systems. Aggregating intelligence and circulating it to all organisational stakeholders as part of the UK Government Cyber Security Strategy's 'Defend as One' approach was essential to maintaining compliance with the government standard and securing its community at large.

Previous methods were manual and decentralised, leading to disparate data sets, slow responses, and a lack of shared awareness of threats and actions.

Global ISAC Recommends Cyware

Upon investigating the issue, the UK government organisation queried their industry ISAC. As with all major global ISACs, this ISAC was using Cyware to analyse vast amounts of threat intel and collaborate with its members, a fact unknown to the organisation at the time.

The ISAC recommended Cyware for their Defend as One compliance needs, and an introduction was made.

Leveraging Cyware Solutions for Real-Time Response

The organisation needed a complete Threat Intelligence Sharing Platform to help them run their day-to-day operations. After a full market analysis, they proceeded with Cyware as the only solution that fit the bill.

Cyware Intel Exchange and Cyware Collaborate were chosen to process the multitude of structured commercial threat intelligence being ingested daily, along with the vast amounts of unstructured intelligence gleaned from other government sources and external industry advisories. These tools normalise, enrich, and process all incoming threat data to collections that are then easily passed on to constituents.

- Cyware Intel Exchange offered a consolidated research portal with all the threat data and investigation tools necessary for them to write their own tailored research and investigations.
- Cyware Collaborate facilitated real-time bi-directional communication by disseminating the written articles and providing a place to effectively communicate back to the central team for help and advice.

The implementation process contributed to a timely transition. The designated Cyware project team worked hand-in-hand with the government organisation to build out use cases and rules, and the service was ready to roll out within four months. Strong engagement continues between the teams as they continue to mature their service.

Game-Changing Results with Cyware

The government organisation is now spending less time analysing threat intelligence and more time collaborating on the findings – the ultimate aim.

Its constituents benefit from increased interaction via a fully branded platform complete with the government organisation's logo and colours.

Able to access the collaborative platform via web portal and mobile app, these stakeholders are increasingly engaged in the Defend as One practices of threat intelligence sharing.

Before, it was a one-way flow of information, mostly via email. Now, analysts and departments have genuine threat intelligence interaction, which has boosted overall satisfaction.

After Cyware, the UK government organisation can:

- Curate industry-specific cyber threat intelligence (CTI)
- Facilitate bi-directional sharing of threat intelligence information between government organisations and departments
- Offer custom self-serve intelligence in line with stakeholders' needs

And perhaps most importantly, other government organisations have now chosen to participate in the agency's collaborative threat sharing efforts as a result of their Cyware partnership.

Prospects for a Collaborative Future

Happy with early positive results and Cyware's meticulous implementation partnership service, this government organisation is discussing plans for taking operationalised threat intelligence a step further. With Cyware's ability to automate workflows – from threat ingestion directly to solutions within members' security stacks – the possibilities are endless.

> "With Cyware, we've gone from manually distributing fragmented intelligence to enabling real-time, bi-directional collaboration across our entire ecosystem. What used to take days now takes minutes. Our stakeholders are finally empowered to act, not just receive."