CYWARE™

Buyer's Guide

Choosing a Threat Intelligence Management Platform That Allows UK Government Organisations to Defend as One



Contents

Executive Summary....03

What Is a Threat Intelligence Platform (TIP)?....04

Why UK Government Agencies Need a Threat Intelligence Platform Now....05

Core Capabilities to Look for in a Threat Intelligence Platform 06

Implementation Best Practices....08

Choosing a Vendor....09

Questions to Ask Vendor....09

Vendor Shortlisting Tips....09

Case Studies and Testimonials....10

Conclusion....11

Annex A: Threat Intelligence Platform RFP Template....12

Annex B: Evaluation Criteria for UK Government Buyers....15

Executive Summary

There is an awareness across every industry that threats are moving beyond the ability of what human threat analysts can detect. When looking at the UK government and critical infrastructure organisations, the problem becomes even more pronounced.

The Growing Cyber Threat Landscape for the UK Public Sector

These entities are the target of intensifying attacks, geopolitical aggressions, and organised cybercrime activities. And yet, UK public sector entities fight to obtain cybersecurity funding while inhibited by slow and clunky legislative norms.

Without the ability to move fast or make split-second hiring decisions, these essential organisations are left to work with the security resources they have. In a world that values "more data," many have turned to threat intelligence solutions that promise results but only offer nothing but a deluge of alerts in return. Once teams are done vetting, assembling, and enriching, the threats have materialised, and a compromise has occurred.

Why Centralised, Automated Threat Intelligence Management Matters

Strapped government agencies don't need more threat intelligence. They need more organised threat intelligence, and they need it packaged in a format that is comprehensive, human-readable, and actionable.

That's not too much to ask from modern technology, and it is exactly what threat intelligence management solutions deliver.

Through automation and orchestration, threat intelligence platforms (TIPs) streamline the back-end process of traditional threat hunting, removing both human burden and human error. They reduce response times, lift analyst burden, and systematically eliminate risks to national safety.

Selecting the TIP That's Right for You

By taking away 80% of what used to consume threat hunters' time, TIPs allow strapped public sector entities to hunt down the risks that matter – and stop them at scale. No wonder AI-driven threat intelligence platforms are one of the leading trends in cybersecurity today.

The only question is: How to choose the TIP that's right for you?



What Is a Cyber Threat Intelligence Platform?

A Threat Intelligence Platform (TIP) is a comprehensive cybersecurity software solution that enables government organisations to proactively identify, analyse, and respond to cyber threats before they cause harm. It gathers and organises threat data from multiple sources into clear, actionable insights, helping teams detect risks faster and prioritise responses. By integrating with existing tools, a TIP enhances an agency's ability to more effectively protect critical infrastructure and public services.



Centralising threat intelligence

Pulling together data from government advisories, corporate partners, public threat feeds, and internal sources to create a "single source of truth."



Automating correlation and analysis

Assigning risk scores, identifying malicious patterns, enriching threats, and finding relationships busy human analysts might miss.



Orchestrating real-time response

Autonomously responding to a wide range of security threats based on pre-approved playbook plays and reducing SOC workload.



Continuously learning and improving

Machine Learning capabilities improve TIP accuracy and customisation over time, learning from human-handled incidents and user feedback.



Alerting in real-time

Notifying SOCs of emerging threats and supporting alerts with business context, prioritisation, and enriching context.

Disparate tools create visibility gaps that slow awareness, halt response, and give attackers a head start. Threat intelligence platforms automate redundant and time-consuming tasks, helping teams stay ahead of emerging threats.

Why UK Government Agencies Need a Threat Intelligence Management Platform Now

Critical UK public sector organisations are in the eye of a perfect storm: limited resources, budget constraints, compliance requirements, and cybersecurity staffing shortages combine to put highly valuable assets at risk.

According to a January 2025 press release by the National Audit Office (NAO), "The cyber threat to the UK government is severe and advancing quickly; the government must act now." The spending watchdog suggests that cybersecurity staffing shortages are largely to blame, citing the following statistics:

33%

of all government cybersecurity roles are filled by temporary staff or left vacant.

50+

of all cyber roles were vacant within certain departments.

70%

of those filling specialist security architect roles are temporary staff.

The severe cyber staffing shortage among UK government entities exacerbates another salient challenge: the threat intelligence that comes into these departments originates from disparate sources, and practitioners must sort through it by hand; time-consuming work. For public sector agencies that are shorthanded as it is, a lot of this work may simply go undone.

TIPs do the threat intelligence management work that under-staffed government SOCs could not do on their own. They provide a way for these organisations to not only utilise every piece of critical information that passes through their internal systems but also leverage external threat data from other government agencies, critical infrastructure organisations, the National Cyber Security Centre (NCSC), public threat feeds, and more.



Core Capabilities to Look for in a Threat Intelligence Management Platform

When choosing a threat intelligence management platform, it is important that public sector organisations maximise their limited investment. The goal is to put time back on the clock for threat hunters. To do so, the following core capabilities are required.

Category	Capabilities
 **Data Ingestion and Integration**	• Automatic and manual ingestion from multiple sources: internal security tools, open-source threat feeds, commercial threat feeds • Support structured, semi-structured, and unstructured formats • Integrate with existing tools: SIEM, SOAR, protective DNS, and more
 **Parsing and Standardisation**	• Auto-parsing into STIX 2.1 objects • Normalisation of diverse data sources • Legacy format conversion (OpenIOC, STIX 1.x)
 **Automation and Orchestration**	• Automated tagging, scoring, enrichment • Rule-based enrichment and correlation • Automated workflows for triage, alerting, and sharing
 **Enrichment and Contextualisation**	• Built-in and external data enrichment capabilities • Analyst-added and system-driven context • Relationship mapping between TTPs, actors, vulnerabilities
 **Tagging and Metadata Management**	• System/user-defined tags, hierarchy, sharing rules • Sensitivity, sharing, and visibility tagging • Custom tagging logic and rule creation
 **Scoring and Prioritisation**	• Confidence, severity, and relevance scores • System-defined and analyst-defined scoring rules • Dynamic reprioritisation based on context
 **Search, Query, and Correlation**	• Advanced search and filtering • Data pivoting and IOC traceability • Link analysis and cross-data correlation

Visualisation and Dashboards	• Out-of-the-box and custom dashboards • Support for IBM i2-style and Maltego-style visualisations • Visual representation of actor, IOC, and campaign relationships
Collaboration and Sharing	• Role-based and attribute-based access controls • Multi-tenant support with selective cross-sharing • Built-in collaboration features and report generation
Reporting and Metrics	• Intelligence report creation and distribution • Operational dashboards and tool performance metrics • Federated reporting across agencies and tenants
Security and Compliance	• Data encryption at rest and in transit • Phishing-resistant MFA, RBAC/ABAC, data segmentation • Support for zero trust, audit trails, and chain of custody
Scalability and Architecture	• Cloud-native, multi-tenant scalability • API availability for automation and third-party integration • On-premises/cloud/hybrid deployment options



Implementation Best Practices

While these are elements of the implementation phase, they should be considered before buying. Roadblocks at implementation can be enough to undermine the value of even the most promising upgrades.

Phased Rollout

It is important to keep continuity when transitioning over to a comprehensive threat intelligence management platform. Because no critical infrastructure entity can afford to be blind to threats for any amount of time, a phased rollout approach is recommended.

Training and Onboarding

Analyst training and onboarding needs should be a factor in the decision-making process. This will take more time away from security teams already struggling to stay ahead of daily security demands and can put valuable assets at risk. Look for a TIP solution with easy deployment and low time-to-value. A difficult-to-use tool can result in underutilisation, misconfigurations, and ultimately shelfware.

Integration Capabilities

Integration with existing cybersecurity infrastructure should be a key consideration, especially for government organisations operating on limited budgets. Without the ability to overhaul the entire security stack, and with little guarantee of the next funding boost, it is important to keep and maximise the tools you already have. Find a TIP that works within your current parameters and integrates across all existing solutions.



Choosing a Vendor

Questions to Ask Vendors

Prior to purchasing, it is important to speak directly to vendors about a few key elements that can shape your threat intelligence experience going forward. Three strategic questions include:

How is automation configured and customised?
Working within the skillsets and solutions your agency has in place allows you to build on current wins. Find out what goes into configuration and customisation within your current ecosystem and ensure there is no unnecessary burden.

What other public sector entities currently use your platform?
Knowing this could enable you to reach out to those customers and get a firsthand account of that vendor's TIP solution in action.

How do you handle data sovereignty and inter-agency sharing?
Threat intelligence sharing is a requirement of increasing compliance frameworks today. The process must be as close to effortless as possible, and data should be processed in its country of origin to avoid compliance fines.

Vendor Shortlisting Tips

When making close decisions between competing vendors, the following criteria could help tip the scales:

Seek out government and public sector references and case studies.
Seeing these tools in environments similar to yours can answer specific questions and address niche concerns.

Look for NCSC and other national compliance alignment.
Vendors whose threat intelligence management platforms already adhere to national cybersecurity standards put you ahead of the compliance game and eliminate one more security burden.

Request a live demo tailored to your environment.
Doing so will enable you to see the level of security expertise required to run a particular TIP. This can help determine the right fit for the cybersecurity maturity level of your organisation.

Ask if onboarding assistance comes standard.
The purpose of an advanced TIP is to reduce the workload on your government agency. Look for a vendor that supports you through the onboarding process.

Optimise with ongoing support.
Avoid minimising your investment by leaving the leading features of your TIP solution underutilised. Optimise platform functionality with a vendor that offers ongoing support.

Case Studies and Testimonials

Government organisations have unique challenges that tend to revolve around compliance, scalability, and outdated mechanisms. Seeing a threat intelligence platform at work within one of these environments can help other government institutions visualise potential impact.

A UK healthcare entity was tasked with collecting and processing vast amounts of threat data within disparate systems. Aggregating the intelligence and circulating it to all industry stakeholders as part of the Defend as One approach was essential to maintaining compliance with the government standard and securing the healthcare community at large.

The organisation needed a complete Threat Intelligence Sharing Platform to help them run their day-to-day operations. 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.

Read the full case study here.



Conclusion

The threat landscape will only intensify as AI and emerging technologies drive new risks. And as cyberwarfare continues to evolve, government entities will only become more tantalising targets. Government entities must make a choice: stay in the status quo and increase their manual workload, or invest in a platform that prioritises automation, orchestration, and ease-of-use. By doing the work of ingesting, analysing, normalising, and prioritising threat data, TIP solutions empower:

- **Enhanced decision-making**
- **Improved threat visibility**
- **Reduced alert fatigue and SOC burden**
- **Bolstered compliance**
- **Increased ROI on security investments**

The limits of current government cybersecurity resources demand new solutions that force-multiply the assets on hand. By adopting a threat intelligence management solution that goes beyond collecting alerts, public sector agencies can spend less time managing and more time hunting.

Contact the Cyware team to learn more about threat intelligence platforms and how the right solution can support your requirements and align with your strategic objectives.

Ready to get started?

Check out the RFP templates on the following pages.

For more information, email us at europe@cyware.com, and our team will get in touch with you.

Visit us at cyware.com

Annex A: Threat Intelligence Platform RFP Template

Requirement	Description	Must Have	Nice to Have	Not Needed	Vendor Response
Automatic and manual ingestion from multiple sources	Support ingestion from internal tools, open-source and commercial threat feeds				
Support structured, semi-structured, and unstructured formats	Enable parsing of all major data types for flexibility in threat intake				
Integrate with existing tools	Compatibility with SIEM, SOAR, protective DNS, and other security systems				
Auto-parsing into STIX 2.1 objects	Support for parsing threat intelligence into STIX 2.1 format				
Normalisation of diverse data sources	Ability to standardise threat data from multiple heterogeneous sources				
Legacy format conversion	Convert legacy formats such as OpenIOC, STIX 1.x into modern formats				
Automated tagging, scoring, enrichment	Automatically apply tags, scores, and enrichment data to indicators				
Rule-based enrichment and correlation	Apply rules to correlate and enrich data automatically				
Automated workflows	Trigger workflows for triage, alerting, and sharing of threat intelligence				

Built-in and external data enrichment capabilities	Support integration with internal and external enrichment services				
Analyst-added and system-driven context	Allow both manual and automatic addition of contextual data				
Relationship mapping	Map relationships among TTPs, actors, and vulnerabilities				
System/user-defined tags	Allow creation of tags by users and system with hierarchical rules				
Sensitivity, sharing, and visibility tagging	Tag intelligence based on sensitivity and sharing permissions				
Custom tagging logic	Enable rule creation for automated tagging behaviour				
Confidence, severity, and relevance scores	Assign multi-dimensional scores to threat intelligence				
System-defined and analyst-defined scoring rules	Allow both default and customised scoring models				
Dynamic reprioritisation	Update threat scores dynamically based on evolving context				
Advanced search and filtering	Support complex queries and advanced filtering options				
Data pivoting and IOC traceability	Trace back indicators and pivot between related data				

Link analysis and cross-data correlation	Correlate and visualise links across various data sources				
Out-of-the-box and custom dashboards	Provide standard and customisable dashboards				
Support for IBM i2-style and Maltego-style visualisations	Enable link analysis visualisation styles				
Visual representation of relationships	Visualise relationships among actors, IOCs, campaigns				
Role-based and attribute-based access controls	Control access based on user roles and data attributes				
Multi-tenant support with selective cross-sharing	Enable collaboration across tenants with access control				
Built-in collaboration features	Support annotation, commenting, and report generation				
Intelligence report creation	Create and distribute intelligence and incident reports				
Operational dashboards and performance metrics	Display system and operational performance				
Federated reporting	Support consolidated reporting across tenants and organisations				
Data encryption at rest and in transit	Ensure secure storage and transmission of data				

Phishing-resistant MFA, RBAC/ABAC, data segmentation	Provide modern access control and segmentation				
Support for zero trust, audit trails	Support for compliance and auditing frameworks				
Cloud-native, multi-tenant scalability	Scalable architecture suitable for multi-tenant cloud environments				
API availability	Expose APIs for automation and integration				
Deployment options	Support on-prem, cloud, and hybrid deployment scenarios				

Annex B: Evaluation Criteria for UK Government Buyers

When all major functionality boxes are checked, it is important to consider the weight that each criterion carries for your particular government agency.

Criteria	Description	Weight (%)	Score (1–5)	Weighted Score	Vendor Response
Total Cost of Ownership (TCO)	Total cost of acquiring, operating, and maintaining the platform throughout its lifetime				
Cost of Licensing Models	The expense associated with purchasing or subscribing to the product license				

Deployment Complexity and Time	How long to get the system fully operational, including employee training time				
Integration Capabilities	Ability to integrate with our current systems, data sources, and threat intelligence tools				
Vendor Support	Availability of customer service for troubleshooting and technical concerns				
Government References	Has this tool been used and recommended by other government agencies				

Instructions for Use

- Assign a **weight (%)** to each criterion based on importance (total should equal 100%)
- Score each vendor on a scale from 1 (Poor) to 5 (Excellent)
- Calculate the **Weighted Score:** Score × Weight
- Sum the weighted scores across all criteria to compare vendors



CYWARE™

Get in touch with the Cyware team to learn more about threat intelligence platforms and how the right solution can support your requirements and align with your strategic objectives.

Request Demo

Visit Website