CYJAX

Maximising the Value of Threat Intelligence

A tactical guide for CISOs and their teams

A quarter of ‘cyber-mature’ businesses reported 11 or more cybersecurity incidents in the past year

Law enforcement agencies worldwide face an evolving and increasingly complex cybercrime landscape. The rapid emergence of new fraudulent schemes, the global reach of online criminal networks, and the technical sophistication of cybercriminals create significant challenges. The anonymity afforded by modern technology further complicates police investigations, making it difficult to identify, track, and apprehend perpetrators.

Threat intelligence has become more important than ever due to the rising scale and sophistication of cyber threats. Attacks are not only increasing in frequency, but they’re also becoming more complex, often targeting supply chains and exploiting emerging technologies. At the same time, Chief Information Security Officers (CISOs) face mounting pressures, from limited resources and regulatory demands to burnout and the growing need to communicate cybersecurity risks clearly to non-technical stakeholders.

The rapid advancement of generative AI further complicates the landscape, enabling threat actors to create more complex phishing campaigns, deepfakes, and automated malware. These evolving tactics make it harder for traditional security approaches to keep up, increasing the need for real-time, context-rich threat intelligence.

In this environment, effective threat intelligence provides a crucial advantage. It allows organisations to anticipate attacks, prioritise risks, and respond quickly with accurate, actionable insights. As cyber threats grow more unpredictable and resource constraints tighten, leveraging advanced platforms like Cyjax’s Cymon® becomes essential for maintaining a strong security posture and reducing operational strain.

For CISOs striving to maximise the value of their threat intelligence investments, this guide provides a clear roadmap to transform information into impact and keep their organisations one step ahead of cyber threats.

Table of Contents

The growing importance of threat intelligence

"There are a lot of misnomers around what is and isn't threat intelligence. The majority of information sold or gathered as 'intelligence' is in fact data or information. To be classified as intelligence, the information needs to be augmented with context (the 'so what?') so that it can be effectively used to manage risk." David Sandell, CEO of CI-ISAC Australia

The concept of threat intelligence has evolved alongside the growth of digital networks and the increasing sophistication of cyber threats. In the early days of cybersecurity, threat information was largely reactive, focusing on post-incident analysis and forensics. As these types of attacks grew in frequency and complexity, the need for more proactive and predictive approaches became evident.

By the 2000s, the emergence of dedicated threat intelligence platforms enabled security teams to aggregate and correlate data from multiple sources, providing a more comprehensive view of the threat landscape. The adoption of frameworks like the MITRE ATT&CK and the use of Indicators of Compromise (IOCs) helped standardise threat detection and response practices.

Today, modern threat intelligence goes beyond simple data collection. It involves advanced techniques like machine learning, behavioural analytics, and real-time threat hunting. These innovations allow organisations to identify emerging threats faster, prioritise responses based on risk, and adapt their defences to an ever-changing digital environment.

By 2027, 17% of cyberattacks are expected to involve Generative AI

Key drivers of the growing importance of Threat Intelligence

Rising Cyber Threats

The frequency, scale, and sophistication of cyberattacks continue to increase, posing significant challenges to organisations across industries. From ransomware to advanced persistent threats (APTs), the need for timely and accurate threat intelligence has never been more critical.

Increasing Pressure on CISOs

CISOs face mounting demands, including resource limitations, regulatory compliance, and the need to provide clear, actionable insights to senior leadership. The high-stress nature of the role often leads to burnout, making efficient and effective threat intelligence vital.

The Impact of Generative AI

Threat actors are leveraging AI-driven tools to accelerate phishing attacks, deepfakes, and automated malware, increasing the importance of adaptive and intelligent defence strategies.

Traditional Approach Limitations

Traditional threat intelligence methods often struggle to keep pace with developing threats. Static indicators and delayed reporting lead to slow response times, while the sheer volume of data can overwhelm security teams.

As cyber threats continue to evolve, so too must the capabilities and strategies of threat intelligence. Effective implementation of threat intelligence not only enhances an organisation's security posture but also reduces the operational burden on security teams, ensuring that limited resources are focused on the most pressing risks.

44% of CISOs reported missing a data breach in the past 12 months with existing tools

Common challenges in threat intelligence management

Despite the clear benefits of threat intelligence, many organisations encounter significant obstacles when trying to implement and maximise these capabilities. Understanding these challenges is crucial to developing more effective strategies and leveraging the full potential of threat intelligence.

Overwhelming alert fatigue

"We are getting too many alerts, many of which are false positives meaning our team is wasting time investigating the wrong things and things are slipping through the net."

One of the most pervasive issues facing security teams is the sheer volume of alerts generated by threat intelligence platforms. As many as 75% of these can be false positives, leading to wasted time and effort while increasing the risk of real threats slipping through unnoticed. Security teams often find themselves stretched thin, struggling to prioritise and respond to the most critical incidents.

Solution: Advanced analyst enrichment and intelligent linking can help reduce noise by providing context and prioritisation for alerts. By enhancing the quality of threat data and correlating information across multiple sources, organisations can focus on the most relevant and high-risk threats.

Delayed detection and response

"We aren't getting alerted on time and are slow to detect, and then respond."

Challenge: Speed is critical in cybersecurity, yet many organisations suffer from slow data collection and alerting processes. Delays in identifying and responding to threats increase the risk of significant damage, from data breaches to operational disruptions.

Solution: Real-time data collection and faster alerting mechanisms enable quicker detection and response. By minimising the time between threat identification and action, security teams can mitigate potential damage more effectively.

Managing expansive and evolving supply chains

"Our supply chain is big and changes all the time, we are struggling to identify compromises in a timely manner."

Challenge: Modern supply chains are vast and constantly changing, making it difficult to monitor for potential compromises. Third-party vulnerabilities often serve as entry points for attackers, increasing organisational risk.

Solution: Specialised feeds, such as ransomware intelligence, can provide timely updates on supply chain threats. By maintaining visibility over third-party risks, organisations can identify and address potential compromises before they escalate.

Resource Constraints

"There is just too much to monitor for, and we are struggling to find the time, expertise and budget to invest in everything we feel we need to to protect the organisation."

Challenge: Many organisations face a lack of time, expertise, and budget when it comes to implementing comprehensive threat intelligence strategies. The wide range of potential threats often overwhelms limited security teams.

Solution: Tools like the MITRE map offer structured and prioritised views of threat data, helping organisations allocate resources more efficiently. By focusing on the most pertinent risks, security teams can maximise their impact even with limited capacity.

Adapting to a Dynamic Threat Landscape

"Our attack surface and threat landscape are large and constantly changing, we need a solution tailored to us that can rapidly and dynamically adjust to these changes."

Challenge: The fast-changing nature of cyber threats requires solutions that can evolve alongside them. Static, one-size-fits-all approaches often fail to provide the flexibility needed to address shifting attack surfaces.

Solution: Tailored dashboards and keyword-driven monitoring allow organisations to customise their threat intelligence approach. Dynamic adjustments ensure continued relevance and efficacy as the threat landscape evolves.

Communicating cybersecurity insights to non-technical stakeholders

"We are getting an increasing amount of interest and requests regarding cybersecurity topics from senior, non-technical stakeholders and struggle to find the time to provide digestible but pertinent responses."

Challenge: CISOs are increasingly called upon to provide cybersecurity insights to senior, non-technical leadership. Balancing technical depth with clarity and relevance can be a significant challenge.

Solution: Visual dashboards and enriched analyst reporting offer accessible yet detailed overviews of threat intelligence data. These tools facilitate informed decision-making without requiring technical expertise.

Demonstrating compliance and intelligence utilisation

"Regulators and cyber/data protection bodies are requiring a demonstration of the utilisation and actioning of cyber intelligence, we are struggling to demonstrate this in a meaningful way."

Challenge: Regulatory bodies and data protection authorities often require evidence of effective threat intelligence use. Proving the actionability and impact of collected data can be cumbersome.

Solution: Board-level reports and compliance documentation streamline the demonstration of threat intelligence utilisation. Clear, structured reporting satisfies regulatory requirements while showcasing proactive security measures.

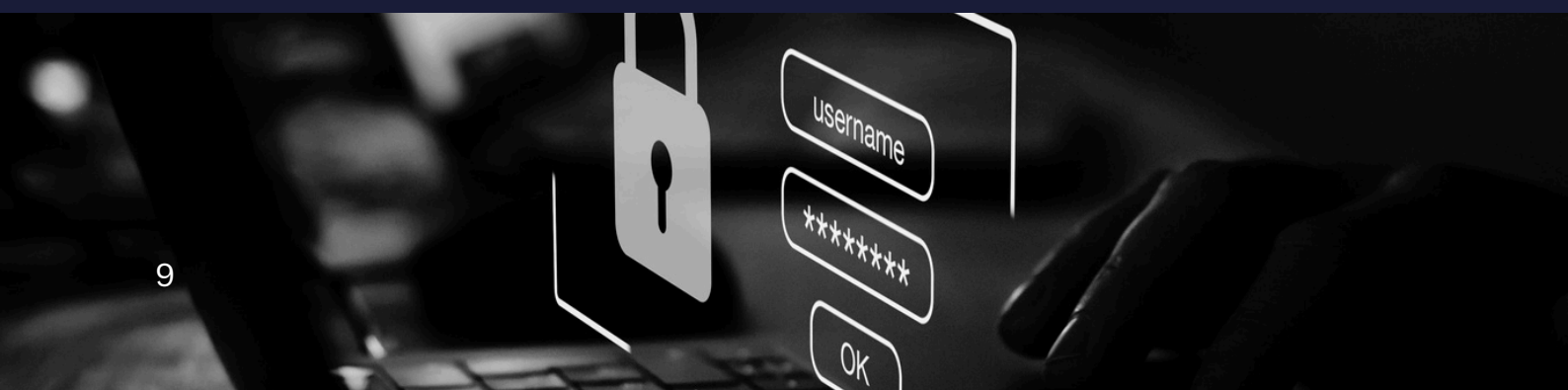
Addressing these challenges requires a combination of advanced technology, strategic alignment, and effective communication. In the following sections, we explore how Cyjax's solutions empower organisations to overcome these obstacles and unlock the full potential of their threat intelligence capabilities.

Make threat intelligence work for your organisation

To truly harness the power of threat intelligence, organisations need a strategic approach that translates data into effective security action. This section outlines practical tactics for optimising threat intelligence operations:

- **Prioritising alerts with enriched context:** Providing context and prioritisation ensures security teams focus on genuine risks while minimising time spent on false positives.
- **Accelerating response with real-time threat insights:** Real-time data collection and alerting capabilities reduce the time between threat detection and response, allowing quicker containment and mitigation.
- **Strengthening supply chain monitoring and incident response:** Specialised intelligence feeds, like ransomware monitoring, help identify third-party vulnerabilities, contributing to more proactive risk management and faster incident response.
- **Using intelligence-driven threat prioritisation:** Mapping threats to adversary behaviours using tools like the MITRE ATT&CK framework helps prioritise response efforts based on potential impact and likelihood.
- **Customising intelligence feeds for your unique risk profile:** Tailored dashboards and keyword-driven monitoring aligns threat intelligence with the organisation's changing needs, threat landscape and risk profile.
- **Automating and simplifying cyber risk communication:** Automated reporting tools transform complex data into accessible, digestible insights for non-technical stakeholders, streamlining communication and enhancing organisational awareness.
- **Meeting compliance and regulatory requirements with actionable intelligence:** Advanced reporting capabilities simplify demonstrating effective threat intelligence utilisation, supporting compliance with regulatory demands and audit requirements.

"Many boards and C-suites now require or need further knowledge into potential threats, security vulnerabilities, risk scenarios and actions needed for greater resilience."
Emily Mossburg, Cyber Leader, Deloitte Global



Optimised threat intelligence in action

OSINT (Open-Source Intelligence)

A British-Swedish pharmaceutical company partnered with Cyjax to cut through overwhelming false positives and protect sensitive data. Over a decade, Cyjax provided timely, actionable threat intelligence 12 to 36 hours faster than previous vendors, reducing alert fatigue and enabling the internal team to focus on real threats, significantly strengthening the company’s security posture.

Enhancing resilience

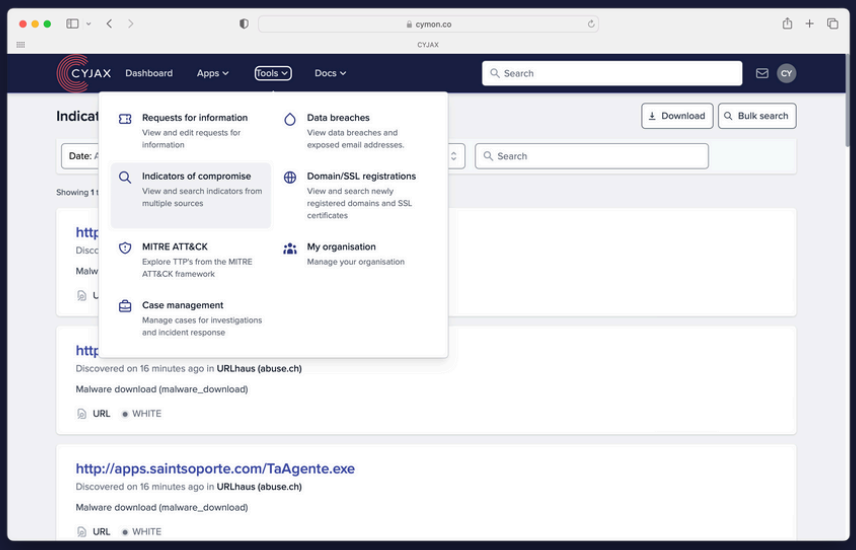
A UK non-ministerial government department wanted to combat online brand misuse and reputational threats. Utilising the Cymon® platform and a dedicated analyst team, Cyjax provided daily intelligence reports and established a ticketing system for in-depth investigations. This proactive approach significantly reduced reputational damage and streamlined the client's threat response process.

The value of speed and accuracy

A Middle Eastern utility provider was in need of strengthened cybersecurity and recognised the urgent need for rapid, validated, and reliable threat intelligence. Over a 12 month period, Cyjax provided 43,184 validated IOCs and 46 ransomware alerts, improving threat response times and securing critical infrastructure.

What is Cymon®?

Cyjax's Cymon® platform turns vast amounts of raw data into clear, actionable threat intelligence. It brings together insights on threat actor activity, dark web monitoring, ransomware incidents, and data leaks into one unified, easy-to-navigate interface. With customisable dashboards and advanced filtering, users can focus on the most relevant and high-risk issues. Its seamless API integration allows it to work smoothly alongside existing security systems, strengthening operational efficiency without disrupting workflows.



Transforming challenges into advantages with Cymon®

- Start strong with the essential insights required to establish an effective threat intelligence programme.
- Uncover hidden threats and vulnerabilities through access to restricted and hard-to-reach sources.
- Streamline high-level reporting with intelligence tailored to tactical, operational, and strategic needs.
- Cut through the noise to highlight the most critical threats, keeping your attention on what matters most.
- Enhance your team's capabilities with expert analysis and support, bridging gaps in in-house resources.
- Stay ahead of evolving regulations with contextual intelligence that supports compliance and proactive adaptation.

Key takeaways

The current threat landscape is complex and rapidly changing, and the need for timely, contextual, and actionable threat intelligence has never been greater. This whitepaper has underscored both the opportunities and the challenges that come with implementing robust threat intelligence capabilities. By addressing common pain points, such as alert fatigue, resource constraints, and supply chain visibility, organisations can transform raw data into meaningful insights and proactive security measures.

Cyjax's advanced solutions, particularly the Cymon® platform, stand out by offering enriched context, real-time threat insights, and customisable dashboards. These features empower security teams to prioritise risks, accelerate response times, and maintain a resilient security posture. By adopting a strategic and tailored approach to threat intelligence, businesses not only enhance their defence capabilities but also reduce operational strain and support compliance requirements.

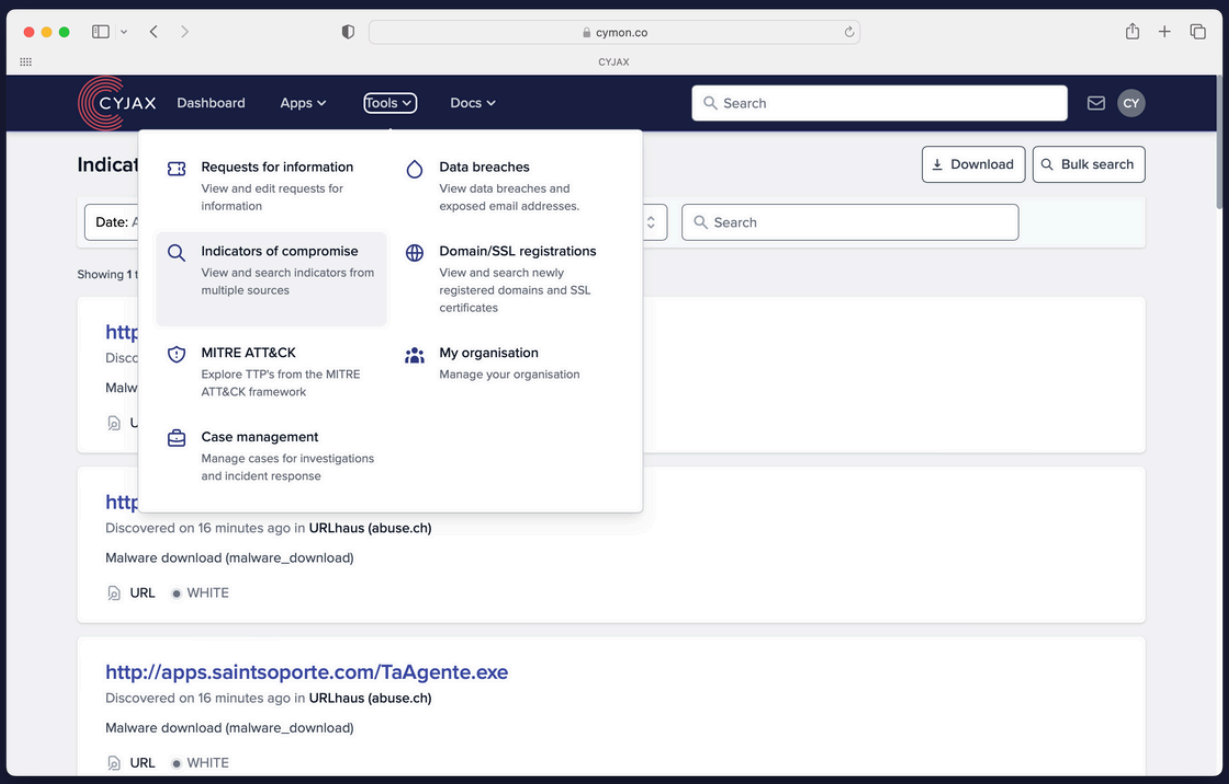
As threats become more intricate, staying ahead requires more than just information but actual intelligence. With Cyjax, organisations gain a trusted partner in their journey toward greater security maturity and operational efficiency. Start optimising your threat intelligence strategy today, and equip your team with the tools they need to safeguard the future.

Endnotes

1. https://www.deloitte.com/global/en/about/press-room/deloitte-global-future-cyber-survey.html
2. https://www.cyjax.com/cymon/\
3. https://www.csoonline.com/article/653990/the-value-of-threat-intelligence-and-challenges-cisos-face-in-using-it-effectively.html
4. https://www.cyjax.com/resources/blog/what-is-the-mitre-attck-framework/
5. https://www.cyjax.com/resources/case-study/global-pharmaceutical-company/
6. https://www.securityweek.com/inside-the-mind-of-a-ciso-survey-and-analysis/
7. https://www.cyjax.com/resources/blog/the-need-for-contextualised-threat-intelligence/
8. https://securityintelligence.com/articles/cisos-drive-intersection-between-cyber-maturity-and-business-continuity/
9. https://www.cyjax.com/resources/case-study/uk-government-department/
10. https://www.cyjax.com/resources/case-study/case-study-enhancing-cybersecurity-resilience-for-a-leading-utility-provider/
11. https://www.cyjax.com/resources/blog/the-use-of-artificial-intelligence-in-threat-intelligence/

CYJAX

CYJAX delivers contextual and actionable threat intelligence leveraging advanced AI and human analysts



Trusted by enterprises like AstraZeneca, Disney, UK Power Networks, Viatris, HM Revenue & Customs, and more...

SEE CYJAX IN ACTION NOW