
# STRENGTHENING LAW ENFORCEMENT WITH PROACTIVE INTELLIGENCE

*A Practical Guide to Threat Intelligence for Modern Policing*

# Executive Summary

Criminal networks are becoming increasingly complex and sophisticated, driven by rapid technological change and adapting to the modern digital world. To stay ahead, law enforcement agencies must leverage timely and actionable threat intelligence to safeguard communities and combat crime effectively. This whitepaper provides a comprehensive guide for law enforcement leaders on building and using a robust threat intelligence framework. It explores best practices for gathering, analysing, and operationalising intelligence data to pre-empt criminal activity and enhance investigative capabilities. With real-world case studies and strategic insights, this guide equips agencies to make informed decisions and strengthen public safety.

*"The real value of threat intelligence lies in what you do with it. Turning insight into action is where resilience is built."*

**Jonathan Bennett**
*Chief Executive Officer at CYJAX*

# Table of Contents


The role of intelligence in modern policing 04

Sourcing and validating threat data 06

From data to action: operationalising intelligence 08

Real-world applications of threat intelligence 10

Building a threat intelligence program 12

Key pillars of intelligence integration 14

Strengthening law enforcement with proactive intelligence 16

Endnotes 18

# The role of intelligence in modern policing

**2024 saw 3x more “severe” attacks on UK organisations and companies**

With criminal activity increasingly enabled by digital technologies, intelligence-led policing has become essential for modern law enforcement. The rise of cyber-enabled threats, ranging from online fraud and ransomware to radicalisation and organised cybercrime, demands a proactive, data-informed approach.

This shift requires moving beyond reactive enforcement models towards the systematic collection and analysis of intelligence to guide decisions, allocate resources, and prevent harm. Effective policing in this environment begins with a clear understanding of the different forms of intelligence and their role in operational strategy.

Intelligence can be broadly categorised into three levels: strategic, operational, and tactical. Strategic intelligence offers a high-level view of long-term risks and emerging trends, supporting planning and inter-agency coordination. Operational intelligence bridges strategy and frontline action, providing insights into specific threat actors, campaigns, or incidents. Tactical intelligence is immediate and action-oriented, used by officers or analysts to inform arrests, disruptions, and incident response.

*“Intelligence agencies shouldn’t be organized around their traditional structures, they need to be organized against the threats they’re countering and the safety of the populations they serve”*

**Sir Jeremy Fleming**
Former Director of GCHQ

A further distinction must be made between cyber threat intelligence and traditional physical threat data. Cyber threat intelligence focuses on digital indicators such as malware signatures, phishing infrastructure, command-and-control domains, and activity on the dark web. While physical threats, such as smuggling routes, weapons caches, or hostile surveillance, remain central to many investigations, digital intelligence is increasingly critical to understanding the broader context in which criminal networks operate.

Aligning the right intelligence to the right operational context enables law enforcement to detect patterns, disrupt criminal activity, and respond with greater precision. In doing so, agencies also reinforce wider public safety goals. By identifying emerging risks, such as disinformation campaigns or threats to critical infrastructure, law enforcement can engage earlier, mitigate harm, and build public confidence.

As criminal networks evolve in sophistication, intelligence-sharing and collaboration become indispensable. Establishing a shared, cross-agency picture of threats is vital to tackling serious organised crime at scale. In this context, threat intelligence is not a niche capability but a foundational element of modern policing.

# Sourcing and validating threat data

The value of threat intelligence depends not only on its analysis but on the integrity and relevance of the data on which it is built. For law enforcement, sourcing threat data from a broad range of inputs is essential, but so too is the ability to validate that information and ensure it can be trusted to inform critical decisions.

**Internal sources** form the foundation of most intelligence efforts. These include incident reports, patrol data, and investigative findings such as first-hand records of criminal activity and operational response. This data provides essential local context and often reveals behavioural patterns, recurring targets, or emerging risks within specific communities or regions

**External sources** expand situational awareness and enable agencies to identify threats beyond their immediate jurisdiction. Commercial threat intelligence feeds can provide timely alerts on digital risks, including malware campaigns, phishing infrastructure, and threat actor movements. Open-source intelligence (OSINT) such as social media monitoring allows agencies to track sentiment, identify disinformation, or detect coordinated harmful activity, while community tips, whether submitted through hotlines, online portals, or local outreach, remain an invaluable form of human intelligence, particularly in early warning scenarios.

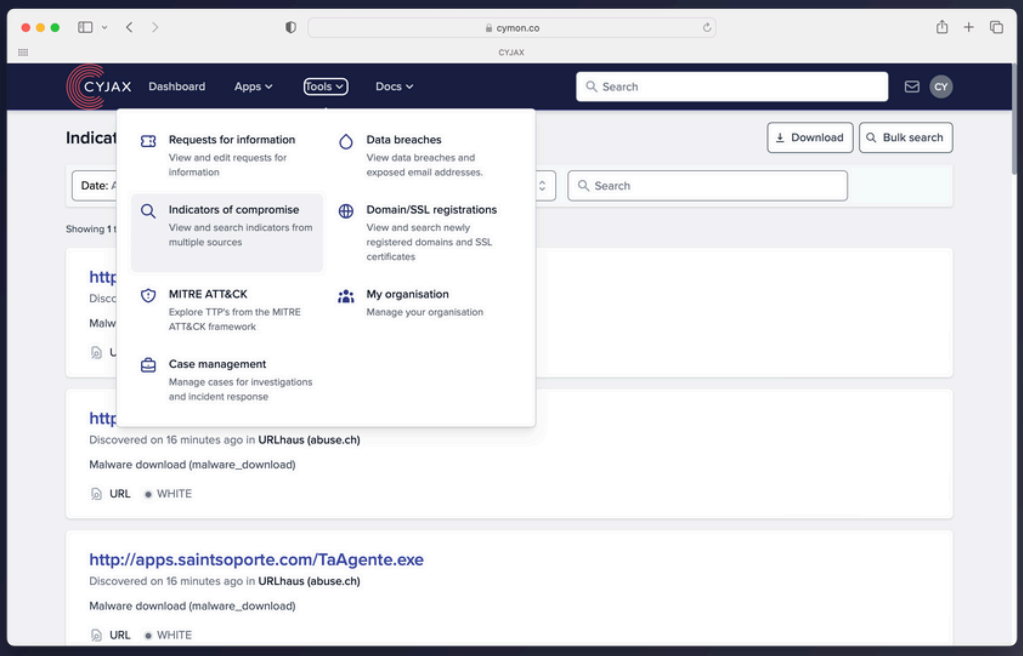
Additionally, signals intelligence (SIGINT), often derived from intercepted communications, offers powerful insights but is technically and legally complex to obtain.

However, not all data sources are equal in reliability, and the prevalence of false or manipulated information, especially in open-source and social media environments, can undermine investigations or divert operational resources. Verification processes are therefore essential.

To ensure data reliability, agencies must establish clear protocols for vetting sources, corroborating key claims, and contextualising new information. This may involve cross-referencing with trusted databases, assigning confidence scores, or integrating human review into automated processes. Timeliness is also a factor; outdated or stale information can be as damaging as incorrect data if it leads to misinformed priorities.

Commercial providers such as Cyjax offer support in this area by not only collecting data across a wide spectrum of sources but also applying rigorous validation and enrichment processes. Their role is increasingly valuable for agencies facing resource constraints or information overload, helping to separate signal from noise and ensure that intelligence is both timely and actionable.

Ultimately, the ability to distinguish credible intelligence from background noise is critical to operational success. In an era defined by both data abundance and disinformation, rigorous sourcing and validation practices are essential to building trust, reducing risk, and supporting informed, intelligence-led policing.



# From data to action: operationalising intelligence

The effectiveness of threat intelligence is measured not only by the quality of the data collected but by how well it is integrated into day-to-day law enforcement operations. Intelligence that is siloed, underused, or poorly disseminated offers limited value. To support proactive policing and informed decision-making, intelligence must be centralised, accessible, and operationalised across all levels of an organisation.

A key first step is the centralisation and correlation of data from diverse sources—internal reports, open-source intelligence, commercial feeds, and partner agencies. Bringing this information together in a unified platform enables a more comprehensive understanding of threats, exposing links between incidents, identifying patterns of behaviour, and highlighting previously unseen vulnerabilities.

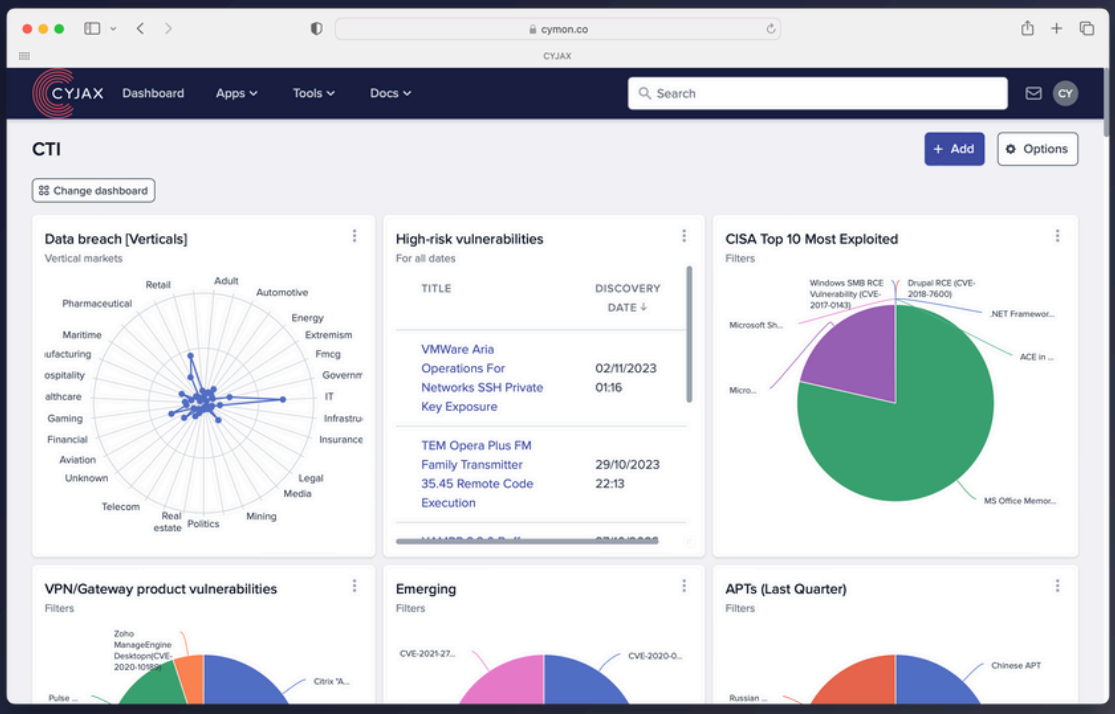
To support this, many agencies now rely on digital platforms that enable secure intelligence sharing and real-time collaboration. These tools facilitate coordination across departments, jurisdictions, and even national borders, reducing duplication of effort and accelerating response times. Platforms designed for interoperability also allow for structured analysis and threat scoring, which is essential for prioritising limited resources.

Integrated intelligence enhances situational awareness by providing decision-makers with timely, relevant insight. Whether in a control room, during an investigation, or at the scene of an unfolding incident, officers benefit from a clear, data-informed picture of risks, enabling faster and more accurate decisions. When supported by real-time feeds and geospatial data, this can significantly improve the precision and impact of tactical operations.

Beyond immediate response, intelligence also plays a central role in assessing risk and prioritising threats. Structured analysis can reveal which actors, tactics, or locations pose the greatest danger to public safety, allowing agencies to allocate resources accordingly. This process of threat prioritisation is particularly important in high-pressure environments, where multiple issues compete for attention and operational capacity.

Longer term, integrated intelligence supports strategic planning and policy development. Insights drawn from historical data, emerging trends, and recurring vulnerabilities can guide investments, shape community engagement strategies, and inform national security priorities. Intelligence-led agencies are better positioned not only to respond to crime, but to prevent it, adapt to new threats, and build public trust.

By embedding threat intelligence across operational workflows—from frontline response to strategic planning—law enforcement agencies can transform information into action. The result is a more agile, informed, and resilient policing model, capable of keeping pace with the complexity and speed of today's threat landscape.



# Real-world applications of threat intelligence

Integrating threat intelligence into law enforcement operations has demonstrably enhanced the effectiveness of crime prevention and response strategies. Several case studies and expert insights underscore the tangible benefits of such integration:

## Operation Venetic and EncroChat

In 2020, European law enforcement agencies collaborated to dismantle EncroChat, an encrypted communication network used by organized crime groups. This operation, known as Operation Venetic, led to over 1,000 arrests across Europe, the seizure of significant quantities of drugs and firearms, and the prevention of violent crimes. The success of this operation highlighted the critical role of centralized data correlation and intelligence sharing in disrupting criminal networks.

## INTERPOL's Operation Serengeti

In a two-month operation across 19 African countries, INTERPOL coordinated efforts that resulted in 1,006 arrests and identified over 35,000 victims, including those trafficked. The operation targeted various cybercrimes, including ransomware and online scams, demonstrating the effectiveness of international collaboration and intelligence sharing in combating cyber threats.

## Australian Federal Police's Operation Ironside

In 2021, the Australian Federal Police (AFP), in collaboration with international partners, executed Operation Ironside, which involved the infiltration of an encrypted communication platform used by criminals. This operation led to over 800 arrests globally and the seizure of 3.7 tonnes of drugs, 104 firearms, and $45 million in cash. The operation showcased the AFP's ability to enhance situational awareness and decision-making through real-time intelligence.

## NYPD's Intelligence & Counterterrorism Bureau

The New York Police Department's Intelligence & Counterterrorism Bureau (ICB) has been instrumental in disrupting over 60 terrorist plots since its inception post-9/11. Deputy Commissioner Rebecca Ulam Weiner leads this specialized unit, which utilizes extensive resources, including intelligence analysts, surveillance technology, and undercover operatives, to proactively address threats. This approach underscores the importance of integrating intelligence into both tactical operations and long-term strategy development.

Evidently, intelligence-led policing provides a structured process for anticipatory crime mitigation through the collection and analysis of information, allowing agencies to proactively address and mitigate threats. These case studies and insights collectively demonstrate that the integration of threat intelligence into law enforcement operations enhances situational awareness, informs decision-making, supports tactical operations, and contributes to the development of effective long-term strategies and policies.

# Building a threat intelligence program

*"We need to be as innovative, adaptable and technologically driven as the criminals we pursue."*

**Graeme Biggar**
Director General of the National Crime Agency (NCA)

Establishing a dedicated threat intelligence capability requires more than technology or data access, it demands a structured, strategic approach that aligns with the wider mission of law enforcement and meets the specific operational needs of the agency. A well-designed programme enables intelligence to be embedded into day-to-day policing while maintaining ethical standards, legal compliance, and public trust.

### Define objectives and mission alignment

The first step is to define clear objectives. Whether the priority is preventing organised crime, identifying cyber threats, enhancing community safety, or improving inter-agency coordination, the programme must be purpose-driven. Aligning threat intelligence efforts with organisational goals ensures that resources are directed towards actionable outcomes and that intelligence supports, rather than operates in parallel to, core policing functions.

01

### Identify key stakeholders and operational needs

Identifying the right stakeholders early on is equally critical. This includes senior leadership, investigative units, cybercrime teams, frontline officers, legal advisors, and IT specialists. Understanding their respective needs and workflows helps shape a programme that delivers relevant intelligence in a usable format—whether for real-time tactical deployment or strategic planning.

02

### Establish a framework for data collection and analysis

Once objectives and stakeholders are defined, the next step is establishing a framework for data collection and analysis. This includes setting protocols for sourcing, vetting, storing, and sharing intelligence, and determining how internal and external data will be integrated. Interoperable systems and clearly defined workflows reduce duplication, improve speed, and ensure intelligence is consistent across departments.

03

---

### Build expertise in threat analysis and intelligence use

Developing in-house expertise is a long-term investment that underpins the effectiveness of any intelligence programme. Analysts must be equipped not only with technical skills—such as data correlation, threat mapping, and link analysis, but also with contextual understanding of criminal behaviour, adversary tactics, and geopolitical drivers. Equally, officers who use intelligence operationally must be trained in interpreting and acting on intelligence products with accuracy and confidence.

04

---

### Training and capacity building

Ongoing training is essential. As threats evolve, so too must the skills of those tasked with identifying and responding to them. Regular upskilling sessions, joint exercises with partner agencies, and scenario-based learning all help ensure that both analysts and officers remain responsive and informed.

05

---

### Ensuring ethical use and data privacy compliance

Finally, any threat intelligence programme must uphold the highest standards of ethics and data privacy. Intelligence-led policing depends on access to sensitive information—but this access must be governed by legal frameworks and handled with care. Agencies must implement strict access controls, audit trails, and data minimisation principles to protect individual rights and maintain public trust. Transparency around how intelligence is collected and used can further reinforce legitimacy and accountability.

06

---

By taking a structured and principled approach, agencies can build a threat intelligence programme that is both operationally effective and publicly defensible. This foundation supports not just better investigations and faster responses, but a more adaptive, accountable model of policing for the digital age.

# Key pillars of intelligence integration

To maximise the value of threat intelligence, it must be fully embedded into law enforcement operations, supporting everything from day-to-day policing to strategic planning and crisis response. Effective integration depends on the ability to centralise data, enable secure collaboration, and build a strong network of trusted partners.

A key priority is the centralisation and correlation of intelligence data. Law enforcement agencies routinely gather information from a wide range of internal and external sources, incident reports, surveillance footage, digital monitoring, and commercial threat feeds. Consolidating this information within a unified system enables a more comprehensive and contextual understanding of threats. Correlation tools can reveal patterns, connect disparate events, and help identify individuals or networks of interest more quickly and accurately.

Technology platforms play a critical role in enabling intelligence sharing and collaboration. Modern tools, such as shared threat dashboards, secure messaging environments, and integrated case management systems, allow officers, analysts, and command teams to access and act on intelligence in real time. Structured workflows and standardised formats ensure that intelligence is timely, consistent, and actionable across teams and departments.

Equally important is the ability to collaborate beyond organisational boundaries. Effective threat intelligence depends on a robust ecosystem of partners. This includes collaboration with other law enforcement agencies, intelligence services, and national security bodies. Cross-border and inter-agency intelligence sharing enhances situational awareness, reduces duplication of effort, and allows for coordinated responses to transnational threats.

Private sector intelligence providers, such as Cyjax, are also vital contributors to this ecosystem. These organisations offer access to specialised threat data, advanced analysis, and global coverage, extending the capabilities of public sector agencies. Engaging with private partners helps agencies keep pace with fast-moving threats, particularly in the digital space, where criminal tactics and technologies evolve rapidly.

The integration of intelligence into operations enhances situational awareness at every level. Whether during an unfolding incident or a routine patrol, timely and relevant intelligence improves decision-making and reduces operational risk. In strategic contexts, it supports better resource allocation, threat prioritisation, and long-term planning.

Ultimately, embedding threat intelligence into workflows, supported by strong partnerships and shared platforms, creates a more agile, coordinated, and informed policing model. In an increasingly complex threat environment, this approach is essential for delivering effective and accountable public safety outcomes.

***Integrating threat intelligence into law enforcement operations***

---

**Centralising and Correlating Data**

Unify intelligence data to provide a comprehensive view

**Tools and Platforms for Intelligence Sharing and Collaboration**

Enable real-time access to and collaboration on intelligence

---

**Building Partnerships and Information Sharing Networks**

Collaborate with other law enforcement, government, and private sector partners

**Enhancing Situational Awareness and Decision Making**

Improve understanding and response to threats

# Strengthening law enforcement with proactive intelligence

*What was once a comparatively minor threat - people hacking for fun or for bragging rights - has turned into full-blown economic espionage and extremely lucrative cyber crime.*

**Christopher A. Wray**
Director of the FBI

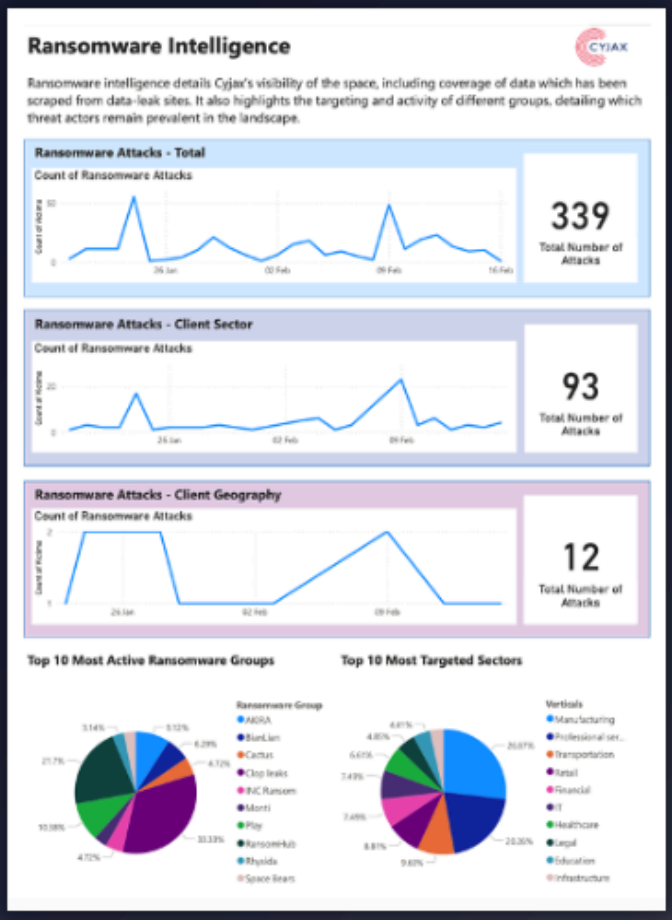
As the line between physical and digital threats continues to blur, law enforcement agencies must adapt, regardless of whether they operate at a regional, national, or international level. This whitepaper has explored the essential role of threat intelligence in enabling proactive, data-driven policing that is both operationally effective and strategically informed.

We have examined the value of intelligence-led policing in today's context, the different types and sources of intelligence available to agencies, and the processes required to validate, centralise, and integrate this intelligence into real-world operations. From supporting tactical decision-making and risk prioritisation to informing long-term strategy and policy development, threat intelligence is no longer a peripheral capability, it is fundamental to modern policing.

Key to success is the ability to build structured, scalable threat intelligence programmes. This includes defining mission-aligned objectives, developing analytical expertise, investing in secure collaboration platforms, and fostering partnerships across the public and private sectors. Just as importantly, these efforts must be grounded in strong ethical principles and a commitment to privacy and transparency.

Law enforcement cannot afford to remain static while the threats it faces continue to evolve. The ability to anticipate, understand, and act on emerging risks is central to protecting communities, maintaining public confidence, and delivering on the promise of public safety. By embracing intelligence as a core capability, agencies can become more agile, more collaborative, and better prepared for what lies ahead.

Agencies that invest in threat intelligence today are not only improving their operational capacity, they are laying the foundations for more resilient, responsive, and future-ready policing. Cyjax is ready to support this mission, providing the insight, expertise, and tools to transform intelligence into operational advantage. Discover how now.



# Endnotes


1. https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53
2. https://therecord.media/british-former-spy-chiefs-shakeup
3. https://www.nationalcrimeagency.gov.uk/news/operation-venetic
4. https://www.afp.gov.au/about-us/history/unique-stories/operation-ironside
5. https://www.nyc.gov/site/nypd/bureaus/investigative/intelligence-counterterrorism.page
6. https://www.nationalcrimeagency.gov.uk/news/director-general-graeme-biggar-launches-national-strategic-assessment
7. https://www.fbi.gov/news/speeches-and-testimony/digital-transformation-using-innovation-to-combat-the-cyber-threat

# About CYJAX

CYJAX is an award-winning technology company and provider of digital threat intelligence services to international corporations, law enforcement agencies and the public sector.

Using our state of the art technology and our world-class team of analysts, CYJAX monitors the Internet to identify the digital risks to your organisation from cyber threats, reputational risk, and the Darknet.

CYJAX provides an Incident Response and Investigation service that provides a calming and structured approach in helping organisations when a breach does occur.

Our proactive methodologies make sense of the noise and help make intelligence decisions, securing the future for our customers.

2025 Winner Global Business Tech Awards

FSQS REGISTERED

Crown Commercial Service Supplier

bsi ISO/IEC 27001 Information Security Management CERTIFIED

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

**SEE CYJAX IN ACTION NOW**