CYBLE®

REPORT

This Year in Cyber Threat Intelligence: AI Keeps Organizations on Top of Growing Threats

The sheer number of cyberattacks and vulnerabilities has made one security technology uniquely positioned to address the challenge – and has also made companies offering it attractive acquisition targets. A look back at the evolution of cyber threat intelligence (CTI) in 2024, and what to look forward to in 2025.

Table of Contents

Overview 3

CTI Vendors Become Attractive M&A Targets 4

How Threat Intelligence Evolved in 2024 – And What's Coming in 2025 5

The Evolution of Threat Intelligence in the Age of AI 6

AI-Powered Threat Intelligence Behind Drop in Data Breach Costs 7

How to Get More from Threat Intelligent Platforms 8

How Third-Generation Threat Intelligence Works 9

Conclusion 10

Overview

Cyber threat intelligence (CTI) has undergone an astonishing evolution in the age of AI, in the process evolving into a comprehensive cybersecurity solution standing guard over all of an organization's external assets, from the network edge to the cloud and beyond.

As threat intelligence market leaders have evolved into comprehensive external attack surface management (EASM) solutions, they have become increasingly desirable acquisition targets, particularly for legacy cybersecurity companies. As a result, half of the leading CTI companies have been acquired in recent years by larger cybersecurity companies looking to expand their offerings outside the firewall to include EASM.

This report will look at the many ways threat intelligent platforms have evolved in 2025, and what may be coming in 2025 – along with ways that users can get more value from their CTI platforms.

CTI Vendors Become Attractive M&A Targets

A flurry of acquisition activity has left only a handful of independent cyber threat intelligence companies remaining. There have been eight major acquisitions of CTI companies in the last three years – and three of those have occurred just in the last few months as the trend has accelerated. Acquisitions have included:

- Google-Mandiant
- Mastercard-Recorded Future
- Fortinet-Volon Cyber Security
- Check Point-Cyberint
- ReliaQuest-Digital Shadows
- Bitsight-Cybersixgill
- Haveli Investments-ZeroFox
- Netcraft-FraudWatch

What's behind those acquisitions is a growing realization by legacy security vendors and service providers that cybersecurity requires a 360-degree view of the attack surface – and that leading cyber threat intelligence companies are best-positioned to provide that view, with solutions that span the cloud, the edge, third-party risks, the dark web, the Internet of Things (IoT), operational technology (OT), and beyond.

Building a threat intelligence company is an enormous undertaking requiring investment in technology, expertise and infrastructure, so for deep-pocketed companies, it's easier to buy than build.

Mastercard's recent acquisition of Recorded Future was particularly ground-breaking, as it demonstrated the growing awareness by financial companies of the strategic importance of threat intelligence for securing sensitive environments. Because of the extreme sensitivity and value of financial data and assets, the banking and financial sector has historically been a leader in cybersecurity. Mastercard's acquisition of Recorded Future suggests that other financial services companies may begin to offer threat intelligence services to customers and partners – and may even acquire CTI companies to do that.

The CTI acquisition trend also highlights the evolution of threat intelligence platforms into comprehensive External Attack Surface Management (EASM) solutions. EASM sees an organization's vulnerabilities much the same way that attackers do – from the outside – and provides guidance for reducing that attack surface.

The technology has been popular with security product buyers. The EASM market is projected to grow at around a 30% compound annual growth rate (CAGR) through 2030 – more than twice as fast as the security market as a whole.

In the process of its evolution into EASM platforms, threat intelligence has become a core – and cost-effective – cybersecurity technology, able to respond agilely as new threats emerge. That evolution continued in 2024 as CTI providers responded to rapidly developing threats.

How Threat Intelligence Evolved in 2024 – And What's Coming in 2025

At the forefront of new features this year have been Executive Monitoring and Deepfake Detection, in addition to rapid takedown procedures for those and other threats.

While part of executive monitoring is scanning for impersonations on the web, social media and elsewhere – including AI-generated deepfakes detected through Facial Recognition and other advanced technologies – physical safety has also become an increasingly important concern for high-profile executives. As a result, some CTI platforms have added capabilities for tracking online threats, along with physical risks as CEOs and other top executives travel.

These services also fit under the broader category of Brand Intelligence – ensuring that fraud and anything else that could damage a company's reputation and business is addressed quickly. AI-powered logo detection, negative mentions, and copycat websites, apps and social media accounts can be addressed with the click of a button.

If a security threat made headlines this year, chances are good that the top CTI platforms added coverage for it. Another new innovation in 2024 has been Hiring Scam Detection, after nation-state threat groups were discovered infiltrating IT companies by impersonating job applicants with sought-after skills.

Cyble went further than most this year by adding Cloud Security Posture Management (CSPM), revealing the extent to which EASM solutions increasingly incorporate standalone security products that can be personalized to address threats in specific environments.

You can expect more of the same for 2025, including rapid responses to emerging threats. Cyble, for example, limits its product roadmap to three months so the company can respond to emerging threats and urgent customer needs. Security needs change as new threats arise, and an agile threat intelligence partner is critical for effective cyber defense.

Given the vast reach of the leading CTI platforms, if there's a need that falls within the external attack surface, there's a chance that threat intelligence companies are working on a solution for it, and standalone tools like CSPM will increasingly become part of CTI platforms. Expect cloud security offerings in particular to continue to evolve.

And as the AI arms race between attackers and defenders heats up, threat intelligence platforms will continue to play a central role in defending organizations against AI threats, whether those threats take the form of increasingly sophisticated fraud, scams, spoofing, deepfakes or other cyberattacks.

Business Risk Management and Threat Intelligence Increasingly Align

A Cyble survey of top CISOs earlier this year found that aligning cybersecurity with business risk is one of the most important priorities for CISOs. Look for threat intelligence platforms to increasingly provide this capability.

CISOs are charged with defending an organization's most critical assets. Integrating threat intelligence with organizational risk management processes would help achieve that goal by prioritizing risk reduction efforts to those threats most likely to disrupt critical business processes, regardless of where those threats reside, whether inside or outside the network, in the cloud, or with third parties.

The Evolution of Threat Intelligence in the Age of AI

Evolving through the era of Big Data and now AI, threat intelligence platforms have become trusted partners that watch over the threats and exposures in specific environments, scanning the network perimeter, web applications, the cloud and the dark web to provide actionable insights that guide organizations to stronger security and peace of mind.

Now in their third generation, cyber threat intelligence platforms incorporate and automate many security tools and processes, in the process also making them one of the most cost-effective security defenses while prioritizing actionable intelligence and ease of use.

Cyble, for example, incorporates and automates technologies like Vulnerability Assessment and Penetration Testing (VAPT), Cloud Security Posture Management (CSPM), Third-Party Risk Management (TPRM) and other critical functions, and integrates them with an organization's IT environment and security tools to create a comprehensive range of services that include:

- **Attack Surface Monitoring:** Includes web application and asset discovery; network vulnerability detection; domain and certificate expiry; domain, subdomain, IP and DNS zone monitoring; DMARC issue detection; exposed port, network and IoT device detection, and more.
- **Cloud Security Posture Management:** In addition to scanning for vulnerabilities, exposures and misconfigurations, Cyble benchmarks compliance against nearly 30 cloud, security and regulatory frameworks, with scores letting users know specific fixes that need to be applied.
- **Dark Web Monitoring:** Discovering exposed data, files, and code repositories; leaked credentials; compromised payment cards, endpoints and cookies; and monitoring threat actor discussions and dealings.
- **Brand Intelligence:** Uncovering deepfakes, copycat apps, websites, social media and executive impersonators and negative mentions, including built-in rapid takedown capabilities.
- **Threat Intelligence:** The latest research on threat actors, ransomware groups, malware families and exploitation tools; real-time attack data across IT and operational technology (OT) environments; and indicators of compromise (IoCs), file hashes and threat detection rules for automating detection. Cyble, for example, has added nearly 4,000 detection rules and 25,000 file hashes this year, data that can be used to strengthen an organization's existing detection tools.
- **Third-Party Risk Management:** Applying the same security metrics to vendors to alert users of potential risks that partners may be exposing your organization to.

Cyble scans the entire IPv4 space – 4.3 billion IP addresses – every 24 to 48 hours and alerts customers of any exposed assets or vulnerabilities. That level of threat protection is possible only with massive compute power and AI. The vast power, automation, threat coverage and prioritization that AI provides may be the biggest threat intelligence development of recent years.

AI-Powered Threat Intelligence Behind Drop in Data Breach Costs

One bit of good news in 2024 was that escalating data breach costs finally got a break – thanks to AI. The annual IBM-Ponemon Cost of a Data Breach report found that while the average cost of a data breach increased to a record $4.88 million, that cost dropped by 45%, or $2.2 million, when AI and automation were used across prevention workflows.

The security tools that most lowered the cost of breaches were:

- Employee training
- AI- and machine learning-driven insights
- SIEM systems
- Incident response planning
- Encryption
- Threat intelligence

AI-powered threat intelligence platforms play a key role in all those areas by identifying weaknesses, directing response and threat hunting efforts, and increasing the effectiveness of SIEM tools, making them the rare security tool with measurable ROI.

How to Get More from Threat Intelligent Platforms

It is a truism in cybersecurity that big events start from small ones, and the quickest way to good security is to develop a culture where small events are prioritized and addressed quickly.

Internet-facing devices and web applications with vulnerabilities are where many breaches start. Threat intelligence platforms can scan the network perimeter for exposed assets and vulnerabilities, and can be as simple to use as plugging in an IP address or domain or connecting to an API to scan and monitor. Automated reporting and remediation recommendations can help resolve issues quickly.

Leaked credentials, whether from an on-premises environment or a cloud bucket, can be an important early warning signal that often presages ransomware attacks and data exfiltration. In fact, leaked and stolen credentials are the most common attack vector used by hackers and cybercriminals. Dark web monitoring services can detect leaked credentials as soon as they appear, in addition to files, code, endpoints, cookies and other critical exposures, enabling rapid containment of breaches.

Third-Party Risk Management (TPRM) can alert organizations to security shortcomings in partners so they can take action before these weaknesses become supply chain attacks and data breaches.

How Third-Generation Threat Intelligence Works

Third-generation cyber threat intelligence platforms work by leveraging predictive analytics, real-time threat hunting, and automated response mechanisms to stay ahead of adversaries.

Predictive Analytics and AI: Anticipating Threats Before They Strike

Predictive analytics is at the heart of next-gen threat intelligence. By harnessing the power of advanced algorithms and machine learning, cybersecurity systems can analyze vast amounts of data to identify patterns and anomalies that indicate potential threats. This helps organizations anticipate attacks before they occur, changing from a reactive stance to a proactive one.

Threat Hunting: Actively Seeking Out Hidden Dangers

Gen3 cyber threat intelligence greatly boosts the power of threat hunting – the proactive search for threats within an organization's environment. Cybersecurity professionals use sophisticated tools and techniques to uncover hidden threats that might bypass conventional defenses, and next-gen threat intel platforms can guide and automate those investigations in ways not previously possible.

Automated Threat Response: Speed is Essential

One of the most significant advancements in these new CTI platforms is the integration of automated threat response systems. These systems can act in real-time to neutralize threats as soon as they are detected. By minimizing the time between detection and response, automated systems help contain and mitigate damage, reducing the overall impact and cost of cyberattacks. APIs and integrations extend the value of these CTI systems further by incorporating threat data and alerts into SIEM systems and other monitoring and management tools, ensuring unified and coordinated cyber defenses and investigations.

Contextual Awareness: Understanding the Big Picture

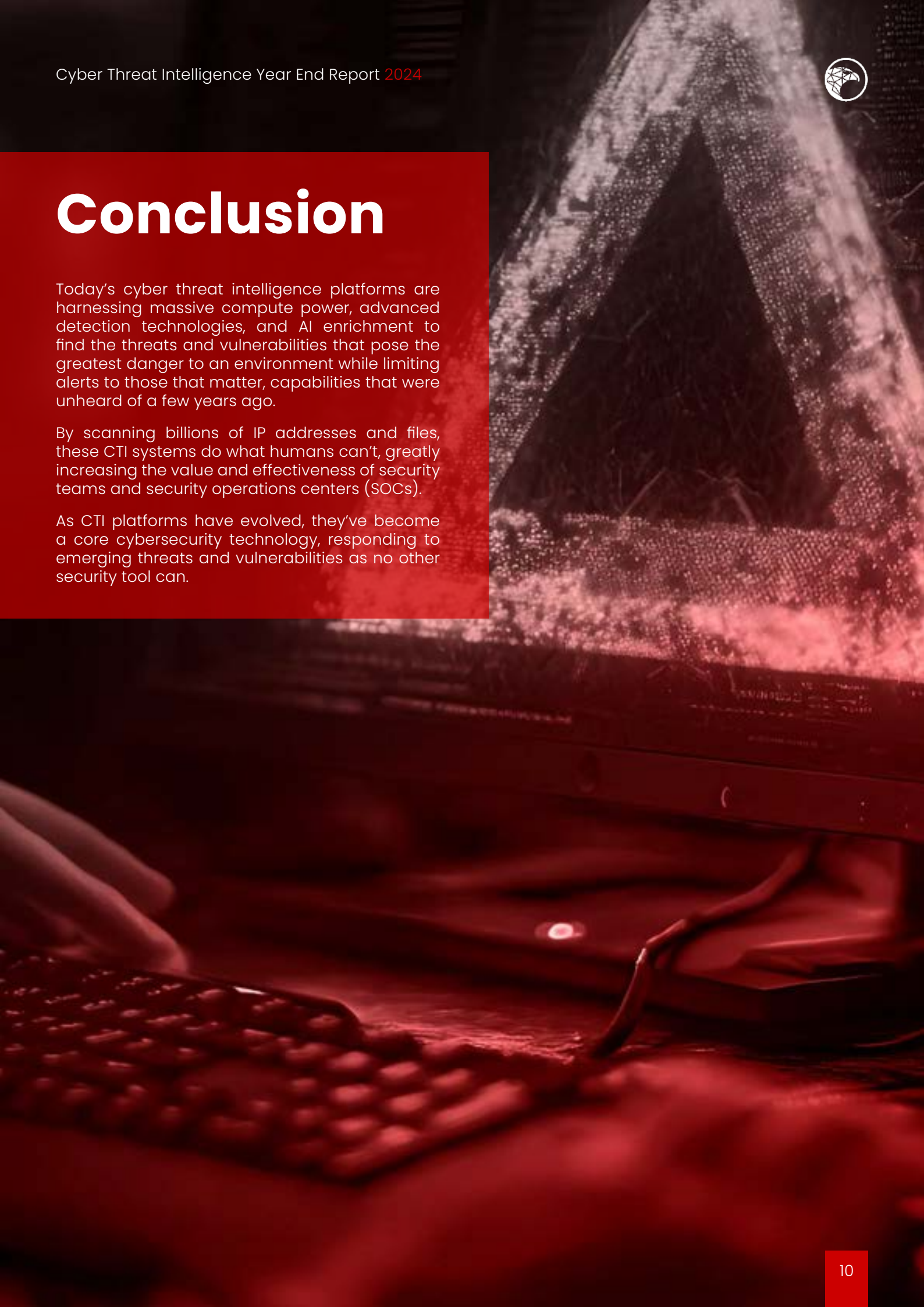
Understanding the context of a threat is critical for formulating effective defense strategies. Gen3 cyber threat intelligence provides deeper insights into threats by incorporating information about threat actor motives, techniques, and potential impacts. This context helps organizations tailor defenses to the specific nature of a threat, enhancing overall security posture.

Conclusion

Today's cyber threat intelligence platforms are harnessing massive compute power, advanced detection technologies, and AI enrichment to find the threats and vulnerabilities that pose the greatest danger to an environment while limiting alerts to those that matter, capabilities that were unheard of a few years ago.

By scanning billions of IP addresses and files, these CTI systems do what humans can't, greatly increasing the value and effectiveness of security teams and security operations centers (SOCs).

As CTI platforms have evolved, they've become a core cybersecurity technology, responding to emerging threats and vulnerabilities as no other security tool can.



About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067