BITSIGHT

EBOOK

CTI: a formidable weapon in cyberwarfare

A look at the top use cases for threat intelligence.

Table of contents

Introduction

Cyber threat intelligence (CTI) plays a starring role in helping organizations around the globe bolster their security posture. CTI provides information and insights about what threat actors are doing, what they're targeting, and their tactics, techniques, and procedures (TTPs) for carrying out attacks, empowering cyber defenders to battle adversaries more effectively.

With comprehensive, real-time CTI that factors the organization's unique attack surface and assets, security professionals can proactively identify threats and vulnerabilities that pose the most significant risk to the business and remediate issues before they become large-scale incidents.

This eBook offers an overview of CTI and how it can be used to proactively defend organizations against emerging threats, detect a breach and determine the extent of any damage caused as a result of an attack.

The use cases detailed include:

- **Threat detection and prevention**
- **Vulnerability management**
- **Threat hunting and automated monitoring**
- **Third-party and supply chain compromise**
- **Threat actor profiling**
- **Cyber governance and compliance**

01

Why companies need cyber threat intelligence

01 Why companies need cyber threat intelligence

Today, cybercrime is big business. As the frequency, scale, and sophistication of cyberattacks continue to increase, the financial impact on organizations is a growing concern.

Companies of any size can be targeted by cybercriminals motivated by financial gain and political causes or simply a need to cause chaos and disruption in the business world. In addition, highly complex enterprise IT environments, ever-expanding attack surfaces, the adoption of innovative technologies like cloud computing and Internet of Things (IoT) devices, third-party security programs and increasingly sophisticated methods to launch attacks are exposing organizations to risk of attack.

To fight cyber warfare effectively and keep companies and their assets safeguarded from bad actors, security leaders must be able to identify the threats that pose the greatest risk to their organizations. Cyber threat intelligence (CTI) delivers the critical insights into the emerging tactics, techniques, vectors, and procedures that could expose their network to attack. As such, CTI forms the foundation of every cybersecurity activity from threat detection, mitigation and remediation.

Gartner describes threat intelligence as "Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Further, Gartner notes that the value of threat intelligence depends not only on the information's relevance and timeliness but also — and more importantly — on the context provided. To be truly effective , threat intelligence must support the risk assessment process with critical context surrounding threat actor groups, tactics, techniques and procedures, vulnerability exploits, indicators of compromise (IOCs), and more. Gartner recommends that organizations look for vendors that offer context-rich threat intelligence that can be customized and tailored for their unique threat landscape.

Gartner notes that the value of threat intelligence depends not only on the information's relevance and timeliness but also — and more importantly — on the context provided.

02

Threat Detection & Prevention

Threat Detection & Prevention

Threat detection and prevention is important to organizations of any size across industries and geographies. Typically, this function is performed by the incident response team. Comprehensive, automated real-time threat intelligence is essential to benefit from the vast collection of data and insights from across the digital landscape, including surface and underground web sources, to help security teams detect potential threats and incidents at the earliest stage of the malicious supply chain.

Inform and improve threat detection and prevention

Threat detection and prevention is essentially the first line of defense. By providing rich contextual insight into the nature, source, immediacy, and severity of each threat, security teams can discover emerging and ongoing threats that are relevant to the organization's attack surface and assets, conduct thoroughinvestigations to pinpoint issues, and take preventive measures to stop threats from becoming full-fledged, costly attacks.

When CTI is refined with the organization's internal business context, security teams are better able to investigate and triage IOCs and potential incidents quickly. This is achieved with attack surface management, leveraging vulnerability and exploit intelligence to continuously monitor their complete asset inventory exposure across the deep, dark, and clear web. The result: faster mean time to detect the most critical threats and respond with the necessary preventive actions to stop threat actors in their tracks.

Comprehensive, automated real-time threat intelligence collected from the clear, deep and dark web is essential to help security teams detect potential threats and incidents at the earliest stage of the malicious supply chain.

Case Study

A global financial services enterprise with over 5,000 employees and over 2,500 branches across 20 countries faced severe challenges stemming from its CTI solution. Previously, the firm had only two manual threat intelligence feeds containing week-old information resulting in telemetry full of false positives and an intelligence bottleneck. This resulted in a reactive security posture and a team that lacked context and visibility into the attacker's mindset, placing the organization at risk.

Once the security team switched to an automated, comprehensive collection of real-time contextual threat intelligence that delivered relevant insights and alerts particular to the organization, the team reduced response times by 75% and detected 7x more threats. By having preemptive, fresh intelligence — within minutes instead of days — they were able to reduce alert fatigue and gain a big-picture view of each threat indicator, including visibility and insight into each threat actor's context, history, and mindset.

The Bitsight Difference

Using Bitsight's Investigative Portal, security teams can easily research and triage alerts, attribute incidents to specific threat actors, and receive the critical insights they need to proactively prevent attacks before they materialize.

Additionally, by harnessing our Attack Surface Management (ASM) module, cyber defenders gain complete visibility into the organization's risk exposure and can leverage our Dynamic Vulnerability Exploit (DVE) Intelligence to quickly prioritize vulnerability remediation efforts with alerts to high-risk CVEs identified within the IT infrastructure. Security engineers can leverage CTI to remediate immediate threats and implement new policies and procedures to help prevent future threats.

03

Vulnerability Management

Vulnerability Management

Most cyber-attacks and breaches stem from a vulnerability that threat actors exploit. Vulnerability prioritization and management is necessary for most organizations' cybersecurity programs, particularly enterprises and SMEs, and applies to companies across industries and geographies. Typically, this function is performed by the SOC, vulnerability management, or GRC teams.

Prioritize and manage vulnerabilities

Every day, vulnerability management teams look for broken or unpatched systems and the available updates or patches as vendors release them. The problem is that these teams often have many systems to patch, and they don't know which ones to handle first based on the vulnerability's potential impact. Additionally, patching a vulnerability might impact other systems and introduce new vulnerabilities. As such, an important aspect of the vulnerability team's responsibility is determining which vulnerabilities are most critical to remediate.

Comprehensive, real-time contextual threat intelligence does more than tell a security team what vulnerabilities the organization has. It indicates the specific vulnerabilities that threat actors are targeting, highlighting those that put the organization at risk — which is critical for prioritizing remediation efforts.

The first step in this process involves discovering and scoping relevant organizational assets (i.e., CPEs) and vulnerabilities (i.e., CVEs) that are of interest and/or significant relevance to the company. Next, by matching the organization's identified CPEs to specific, related CVEs, teams can determine which exploitable vulnerabilities pose the most urgent risk to their systems. This process is further strengthened by mapping related vulnerabilities to the MITRE ATT&CK framework, which offers teams a full understanding of how, when, or why criminals will exploit each vulnerability.

By enriching the organizational context derived from the above-described discovery stage with real-time threat intelligence, security teams gain valuable external threat context, including insights into cybercriminal discourse, activity, capabilities, and intent, complementing internal asset inventory data.

By correlating organizational assets with potential vulnerabilities and real-time CTI from the clear, deep and dark web, organizations can streamline vulnerability management activities, pre-empt risk, and save time and money.

The CTI outputs resulting from these steps give security teams valuable data with which they can evaluate the exploitability of vulnerabilities, gain a more accurate and dynamic assessment of their organization's vulnerability exposure, and prioritize which vulnerabilities to focus their remediation efforts on.

This holistic approach enables security teams to confidently prioritize vulnerability treatment with a comprehensive understanding of the company's risk posture based on a combination of factors. Likewise, they can de-prioritize lower-risk vulnerabilities and address them more strategically and resource-efficiently.

The Bitsight Difference

Bitsight's Dynamic Vulnerability Exploit (DVE) Intelligence is an end-to-end solution that spans the entire Common Vulnerabilities and Exposures (CVE) lifecycle, streamlining CPE to CVE matching, vulnerability analysis, prioritization, management, and remediation. Customers receive a full intelligence picture of the vulnerability, complete with context — including a comprehensive audit trail of the data we have collected on the actors and their discourse, exploit kits, attribution to malware, APT, and ransomware. This includes a score of the likelihood a vulnerability will be exploited over the next 90 days, hours after the CVE is first published.

Unlike the Common Vulnerability Scoring System (CVSS), a widely used industry-standard resource for assessing the severity of vulnerabilities but not the associated risk, our DVE Intelligence score is continually updated in real-time in response to the threat intelligence we gather. Companies automatically gain access to remediation information for each vulnerability directly from NVD, MITRE, and other vendor sites and can continuously monitor CVEs to reduce their organizational risk.

04

Threat Hunting & Automated Monitoring

Threat Hunting & Automated Monitoring

The deep-dive investigative capabilities afforded by comprehensive CTI empower threat-hunting teams to find the highest-priority potential cyber threats. The term "threat hunting" usually refers to the process performed manually, which is inefficient and can drain resources. When CTI automates threat hunting, "threat monitoring" is more appropriate because it refers to the continuous discovery and updating process.

Conduct more effective threat hunting and monitoring

A real-time CTI solution can compile, manage, and monitor the organization's complete asset inventory across the deep, dark, and clear web through automated capabilities. This process identifies potential risks and exposures and helps security teams understand threat actors' potential attack vectors and TTPs to proactively expose and prevent emerging cyber-attacks before they are weaponized. For example, CTI can identify malware when it is initially offered for sale on the dark web, extract the malware in the preliminary phase, and then block it on the corporate firewall, triggering playbooks on the organization's SIEM, SOAR, EPP, or VM platforms before others have a chance to download it.

Threat-hunting activities often span multiple tools and data sets. An effective CTI solution should allow security engineers to integrate and easily cross-reference data between their tools to save time and resources. For example, a security engineer should be able to review logs within their SIEM for suspicious activity or indicators and immediately enrich those indicators with CTI to know whether or not a threat exist.

When combining an attack surface management solution with real-time CTI to constantly monitor an organization's complete asset inventory across the deep, dark, and clear web, security teams can proactively find and prevent emerging cyber-attacks before they are weaponized.

Protecting credentials, credit cards, and data

Threat monitoring is essential to protect credentials, methods of payment, and sensitive data. Continuous monitoring of the company's assets, brand, and employee and customer data across the surface web and cybercriminal underground in real-time ensures that security teams receive early warnings of active threats relevant to the organization as they surface.

Real-time CTI immediately notifies security teams of compromised credentials or credit card data leaked on the deep and dark web, including social media, instant messaging apps, and limited-access dark web forums and marketplaces. When discovered, compromised login credentials or leaked credit cards are made known to security teams immediately so they can take proactive defensive measures to protect the organization, its assets, and customers against threats.

Case Study

A small cybersecurity consultancy had a team of 12 analysts manually collating open-source intelligence to undertake threat risk assessments for their organization and identify stolen credentials and at-risk accounts. By leveraging an automated CTI solution, the team gained access to the deep and dark web, including closed underground sources previously unavailable to their research efforts. The CTI solution now automates many of their investigative functions, delivers advanced analysis to support security operations, and simplifies their ability to conduct broad searches on leaked credentials. Additionally, with a breadth of threat intelligence sources, analysts spend far less time conducting detailed research, which means they can monitor threats for a variety of clients, take appropriate steps for remediation, and ultimately, scale their services as their business grows.

The Bitsight Difference

Bitsight's DVE Intelligence provides security teams with an essential layer of context based on threat actor intent. The solution contains a full audit trail behind each vulnerability, including POC exploit codes for zero-day vulnerabilities – even for vulnerabilities with no CVSS rating.

05

Third-Party & Supply Chain Compromise

Third-Party & Supply Chain Compromise

Most organizations work with external companies — vendors, partners, and suppliers — that become part of the company's larger IT ecosystem and/or supply chain. The organization can be impacted if any third party has weak security measures or suffers a breach. For example, an attack on a supplier that gives threat actors access to the supplier's network can also create an entry point to the organization's systems or sensitive data.

Protect against third-party and supply chain compromises

Third-party and supply chain monitoring is therefore necessary for security programs, regardless of an organization's size or sector. This type of intelligence typically benefits a company's intel and SOC teams, but can also benefit incident response and threat analysts aswell. Supply chain attacks, where attackers target less secure third-party components to infiltrate the main organization, have become increasingly common and pose a significant risk to the company's overall security posture.

Any CTI solution deployed should take into account an organization's third-party partners and supply chain, identifying vulnerabilities or threats targeting those third-party companies as a potential risk. In particular, CTI solutions that integrate with an ASM component can offer complete visibility into the organizational attack surface, including internal and external systems, applications, and devices as well as the risk exposure of associated third-party vendors.

When a threat or risk associated with a third party is detected, the organization's security team gains an early warning of potential and emerging threats so they can take steps to remediate them before they can be weaponized.

Ransomware: Targeting third-party vendors

Ransomware has emerged as one of the most frequent types of cyber-attacks, and the cost to business can be steep. Ransomware often targets third parties and supply chain partners because the payouts can have exponential value for cybercriminals. More recently, we've seen ransomware as a service (RaaS) operators emerge as an effective method of attack for threat actors who lack expertise in this area.

CTI can play a important role in protecting the organization against ransomware attacks and those targeting third parties. For example, when monitoring the clear, deep, and dark web, a CTI solution can see activity on ransomware forums, markets, and dedicated leaks sites (DLS) to provide critical insights. CTI can track threat actor capabilities, specialties, and limitations in ransomware markets, delivering alerts to security teams before an attack is launched.

RaaS operators use ransomware markets to extend their reach and promote their malware on the underground. CTI solutions can also provide valuable insights about RaaS affiliate programs and their revenue-sharing models to help security teams block, analyze, and investigate specific threat actors, their TTPs, motivations, and social networks.

Case Study

An automotive company received an alert of a possible ransomware attack on one of its parts manufacturers through its real-time CTI before the supplier notified its team. This intelligence prompted the team to proactively determine if any sensitive information was leaked in the attack and take immediate action.

The Bitsight Difference

Risk assessments are vital to ensuring a robust security posture. This incorporates an assessment to weigh risks within and across the supply chain against the effectiveness of core security controls. This step is critical given the high-profile software supply chain vulnerabilities in recent years, such as the notorious SolarWinds breach.

CTI helps with ongoing risk assessments by guiding companies on their current risk exposure and the steps needed to minimize that exposure. By considering the impact radius and available security controls associated with each asset, security teams can determine the level of protection in place and whether it needs to be enhanced. With such information, teams can address potential vulnerabilities and blind spots more effectively and proactively enhance the company's defensive mechanisms for business critical assets when limited security controls are in place.

06

Threat Actor Profiling

Threat Actor Profiling

Threat actor profiling, or attribution, is critical to effective cyber defense. It's hard to fight an enemy if you know very little about their motivations, TTPs, targets, and capabilities.

Threat actor profiling: Know your enemy

Real-time CTI offers significant value in this regard, providing details and insights from across the deep, dark, and clear web into threat actor groups and how they're launching attacks. CTI can provide IOCs for specific threat actor groups based on their history of activity and behavior and alert security teams to threat actors they should pay close attention to based on the company's business context.

Threat actor profiles give SOC teams and threat analysts critical information they can use to prioritize their activities. For example, if an organization is currently tracking a few hundred threat actors, threat actor profiling can reveal that a portion of those threat actors are actually the same person or group which helps them better prioritize which threat actors to focus on and which should be consolidated for more effective monitoring.

For example, if a threat actor group such as FIN11 is targeting a certain vulnerability, which is widely known from news articles and other reports. Threat actor profiling enables security teams to dig deeper to determine the level of risk this threat actor group poses to the organization by looking at their IOCs and other attributes. Additionally, attributing attacks to specific actors or groups can aid in identifying future attacks faster so that preventative measures can be implemented.

Threat actor profiling is beneficial to larger enterprises and law enforcement agencies that want to predict an actor's activity or correlate activity with a particular threat actor based on previously observed indicators or patterns. Smaller organizations typically lack the resources to conduct this type of activity, so they might look to an MSSP to handle this for them.

Real-time CTI can offer significant value to threat actor profiling, providing contextual insight into threat actor groups, their motives, tactics, techniques and procedures.

07

Cyber Governance & Compliance

Cyber Governance & Compliance

CTI provides the information and proof needed to help the C-suite and Board understand the scope and scale of organizational risks, the financial impact of cybersecurity efforts, and the tools and resources needed for establishing and maintaining a strong security posture. establishing strong cyber governance practices.

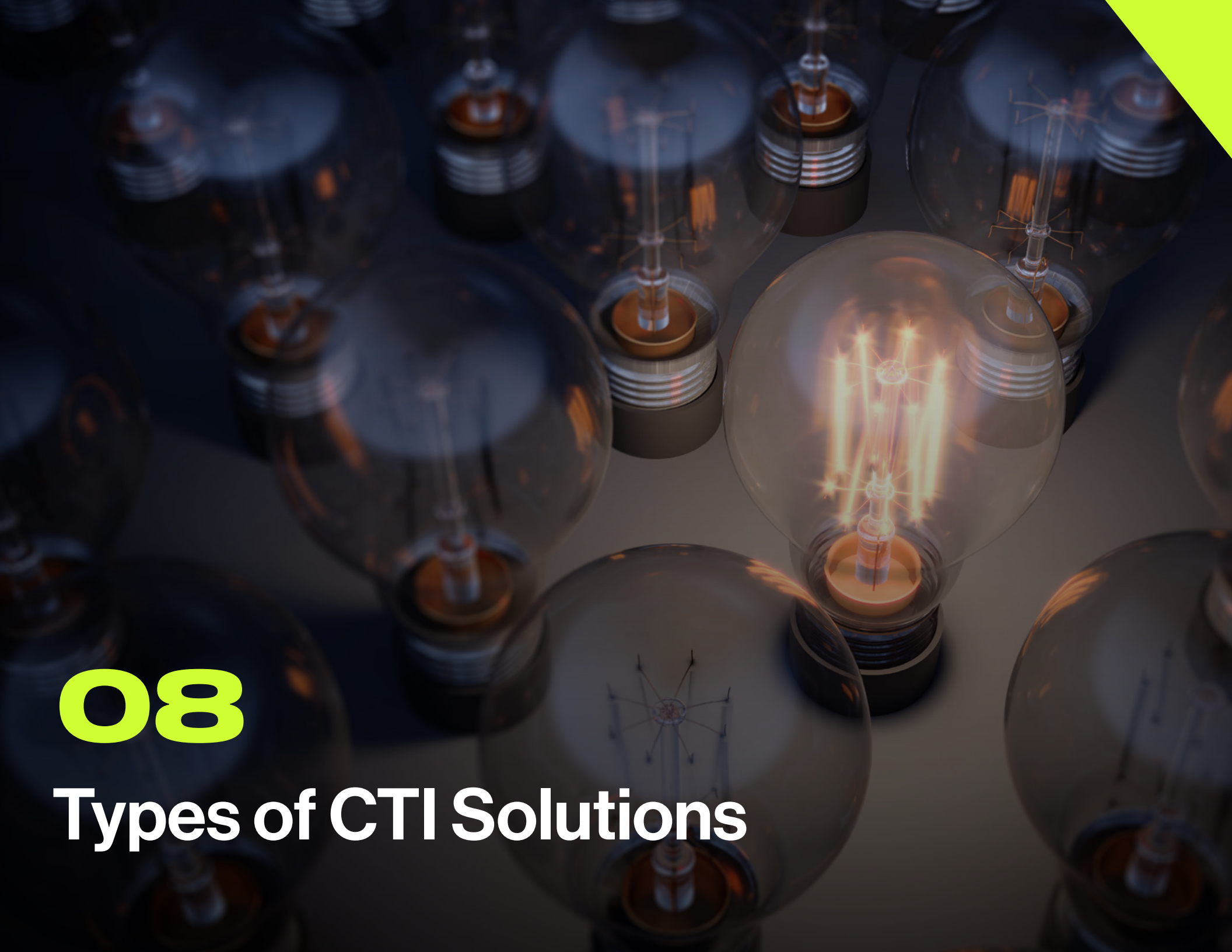
Ensure cyber governance and regulatory compliance

All of this amounts to helping companies comply with government regulations and cybersecurity mandates as well as establishing strong cyber governance practices.

Regulatory requirements state that organizations across industries must have certain systems in place and prove their methods and tools for securing sensitive data against a potential breach. For example, within the recent SEC ruling that regulates how and when companies report cyber incidents, one aspect of the new rules concerns the Board's role in and oversight of risks and threats. When reporting incidents and disclosing their risk management strategy, companies must now describe their cybersecurity policy and management's role — including the C-suite and the Board — in understanding, communicating, and reporting the mitigation and remediation of risk associated with enterprise vulnerabilities.

Government regulations can vary, which makes it challenging for CISOs to understand and implement changes to regulations as they occur — especially for companies that sell products and services into different vertical sectors and countries.As data protection laws and security mandates continue to evolve and strengthen, organizations must also refine their data protection policies, ensure they have the right cybersecurity tools in place, and demonstrate how they safeguard customers' information. However, the burden of information gathering and reporting is significantly lighter with contextual, evidence-based CTI, as CTI data provides multiple levels of assurance on cybersecurity posture and imminent risk to the enterprise. For instance, complying with some government mandates makes it necessary to have evidence-based data available to prove the details of a security breach and to ensure there is full visibility of the enterprise's digital footprint. Having real-time access to intelligence about potential threats targeting the enterprise, taking into account the organization's internal and external attack surface, digital footprint, and other factors, allows companies to prove that they have a complete understanding of the enterprise's risk and are taking proper steps to strengthen cyber defenses.

Contextual CTI also provides a continuous feed of contextual evidence-based data to automate the discovery and exposure of vulnerabilities that could jeopardize the security posture and increase risk after a security incident while helping businesses prove and enforce their mitigation and remediation processes.



08

Types of CTI Solutions

08 Types of CTI Solutions

There are several types of CTI offered by vendors, each with a unique set of attributes.

Open-source intelligence (OSINT)

Open-source CTI is produced from the collection and analysis of publicly available information. OSINT comes from a variety of sources, including social media, news articles, government reports, academic papers and websites providing access to information on a wide range of topics from multiple perspectives. While OSINT can be a more cost-effective option than traditional intelligence tools for organizations with budget constraints, it is not real-time intelligence and can provide data that is inaccurate or outdated. It also only provides a part of the intelligence picture and does not deliver intel from the deep and dark web— where threat actors plan, sell and discuss their next attack.

OSINT is not filtered for business or organizational context, so gaining relevant insights from the overwhelming amount of data, or "noise," can be challenging. Aditionally, OSINT is not "finished intelligence," meaning, it still requires a fair amount of analysis to validate and verify the information – which makes it hard to scale to meet the needs of larger organizations.

Finished reporting

Finished reporting, or finished intelligence, refers to intelligence and insights that are verified, validated, and distinguished from false or misleading information, through human analysis. It provides actionable reporting that can be used by business and security leaders for informed decision-making.

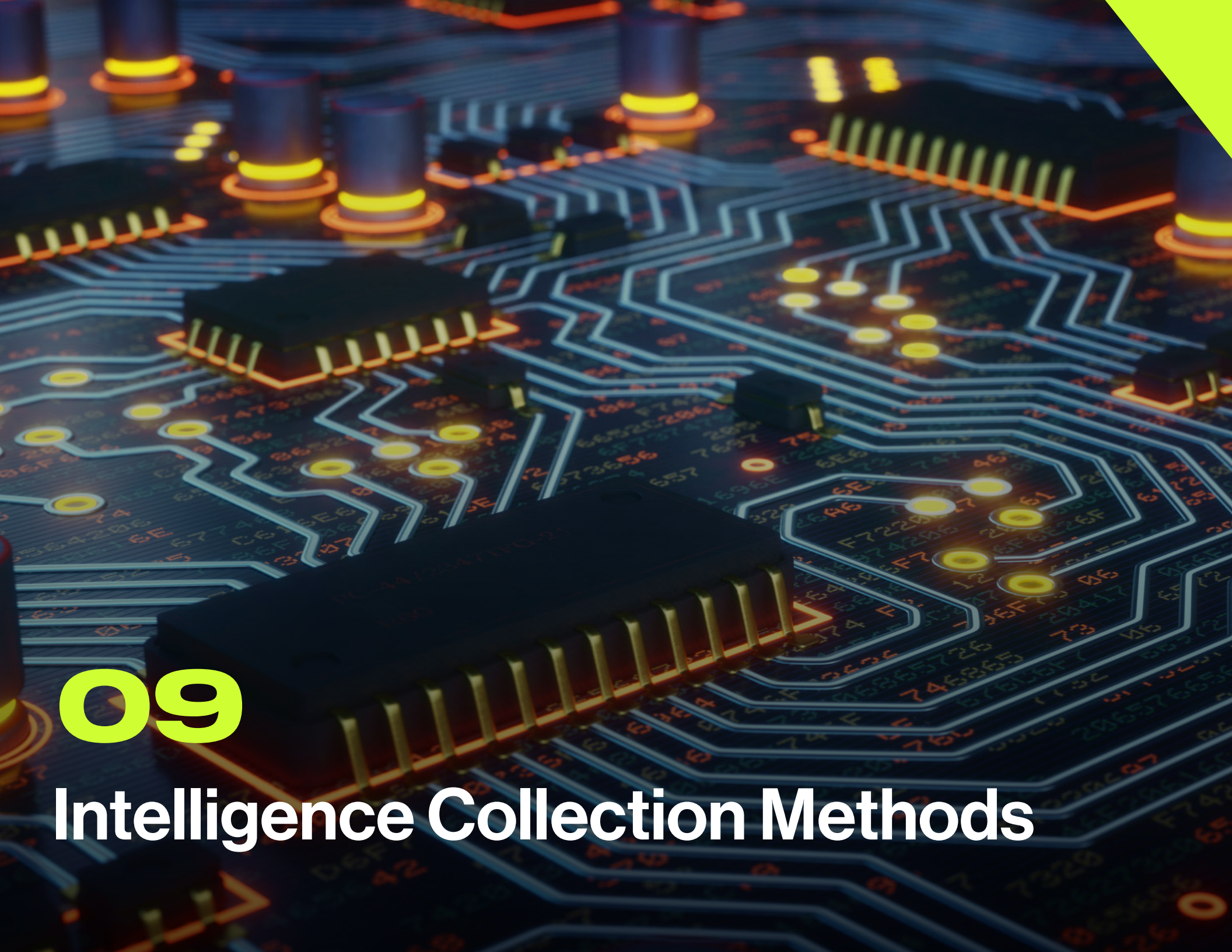
Finished reporting is typically more timely and accurate than open-source intelligence, but it lacks the ability to predict, or offer preemptive intelligence, that can be used to stop an attack before it happens. Without comprehensive, real-time access to dark web sources, many finished reporting vendors offer a limited view of the threat landscape and an organization's risk exposure.

Deep, dark web intelligence

The “deep web” refers broadly to any internet content that is not indexed by search engines – essentially, anything that requires authentication, including university libraries and corporate networks, but can also include personal emails and chat application messages (e.g., WhatsApp, Messenger). Threat actors use deep web platforms such as Telegram to collaborate and transact, making these sources highly relevant for threat analysts.

The “dark web” refers to sites that are only accessible through a special browser such as Tor, which hides a user’s identity and location. The dark web’s focus on privacy makes it popular for hackers and cybercriminals who prioritize anonymity. The dark web primarily comprises a collection of online communities and a space for anonymous commerce and interaction. It’s important to note that not every communication or transaction on the deep and dark web is illegal. Therefore, we also use the term “cybercrime underground” to describe illegal elements in these realms.

Deep, dark web threat intelligence covers an immense volume of platforms and sources, including underground forums, initial access brokers and markets, messaging apps, pastes and code repositories, and more. The types of intelligence found there include chatter about defensive measures and offensive tactics, techniques, and procedures (TTPs), attacks-as-a-service offerings, discussions about news and developments, products for sale, and underground identities. With so many channels and so much activity, it’s fair to say that without a clear understanding of the deep and dark web and how to investigate cyber threats in these arenas, searching for relevant threat intelligence is like finding a needle in a haystack — or millions of haystacks.



09

Intelligence Collection Methods

09 Intelligence Collection Methods

Intelligence data can be collected using manual or automation methods, some vendors deploy a combination of the two.

Manual Collection

Purely manual methods of extracting threat intelligence are not feasible in today's digital age, particularly with the broad range of sources across the clear, deep, and dark web to account for. Manual intelligence doesn't allow for identifying and accessing the right sites to monitor, performing mass keyword searches, or extracting quantitative insights.

Many dark web sites deploy tools to prevent access. Overcoming these roadblocks can be one of the most laborious aspects of dark web investigations. Dark web sources are often unreliable and unstable and may go down without warning. In this case, any data that you've accumulated will instantly vanish.

Hybrid Collection

Hybrid methods combine some amount of manual investigation work with automated intelligence extraction. The more manual labor it requires, the more limited the intelligence will be.

Automated Collection

Automated solutions continuously collect information from a vast range of sources, some such as Bitsight, are able to bypass the barriers and maintain entry to closed forums and limited access markets and can translate data from any language. Depending on the vendor, machine learning and AI can be applied to threat data, enriching each item of intel with context so users can instantly learn more about the threat or threat actor it relates to.

Automated CTI provides actionable and relevant threat alerts in real-time, minutes after activities have surfaced on the underground. By mapping this intelligence to an organization's assets and immediately alerting teams of any suspicious activity, companies can stay steps ahead of threats and stop them from becoming costly attacks.

10

How Bitsight's threat intelligence compares to other vendor

10 How Bitsight's threat intelligence compares to other vendors

Not all threat intelligence is created equal. A vendor automating their threat intelligence collection may not have access to closed forums and marketplaces, or they may not be able to maintain access once granted. Additionally, once the data has been collected, it needs to be processed and correlated for it to be of use to security teams. Since its inception, Bitsight has automated collection from the clear, deep and dark web, processing the data in real time, to deliver meaningful insights to customers. As such, we have the largest, searchable threat datalake available, with intel dating back to as early as the 1990's. The below highlights some of the key differentials of Bitsight's threat intel compared to other major providers.

TITLE	BITSIGHT	OTHER VENDORS
Fully automated threat intelligence collection, extraction and indexing, minutes after it has surfaced	✓	Unlimited
Gains and maintains access to invite-only forums, messaging groups and closed marketplaces	✓	Unlimited
Ability to scrape data sources with complex CAPCHA and posts that have been deleted	✓	✗
Generates detailed profiles on threat actors & groups, including aliases, hours of activity, peer networks, posts and areas of interest	✓	Unlimited
Provides unrestricted access to our complete body of threat intelligence	✓	Unlimited
Generative AI capability embedded throughout all solutions, sourcing intel in real-time from the deep and dark web, providing human-readable, contextual summaries, finished reporting and a personalized AI assistant.	✓	Unlimited

Questions to ask prospective CTI vendors

To benchmark and accurately compare CTI vendors when updating or implementing a new solution, consider asking the following questions:

Consider...

- What types of CTI do you provide?
- Are your collection methods manual, automated or hybrid?
- Do you collect content from limited-access deep and dark web forums, underground markets, invite-only messaging groups, code repositories, paste sites, twitter, Telegram etc.
- How many intel items do you collect daily? (Ideally, this number should be in the millions)
- Do you publish raw data or do you process and correlate data to provide actionable insights?
- Do you give customers access to your complete body of threat intelligence?
- What is the time lag between threat data collection and publishing processed intel?
- How are you monitoring changes in activity across different sources?
- How do you filter through the “noise” to deliver insights that are relevant to my organization?
- Is your intelligence predictive and preemptive, or does it offer a retrospective view after an attack takes place?

11

Conclusion

11 Conclusion

CTI is central to a successful cybersecurity strategy.

While it's not a panacea to fix every security issue, it is a highly valuable tool for the detection and prevention of cyberattacks, delivering the valuable insight and data needed to understand threat actors, identify vulnerabilities, assess risk, and take measures to remediate the most critical issues. Real-time, automated collection of threat intelligence from the clear, deep and dark web enables organizations to take a proactive approach to cybersecurity and aids in better decision-making to strengthen their security posture.

Threat intelligence can be used for multiple purposes across activities within security and governance risk and compliance departments, reducing the time it takes to identify and remediate a threat or breach. However, not all threat intelligence solutions provide the same level, depth, timeliness and quality of information. As such, organizations should ask detailed and probing questions into a vendors' operations, collection methods and capabilities to compare offerings before making their final decision.

About Bitsight

Bitsight continuously collects and exposes the earliest indications of risk by threat actors moments after they surface on the clear, deep, and dark web. Our vast intelligence data lake, derived from millions of underground sources, is processed, correlated, and enriched using automation and advanced AI. Bitsight captures, processes and alerts teams to emerging threats, TTPs, IOCs and their exposure to risk based on each organization's complete attack surface and internal context.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, quickly arming enterprises, government and MSSPs alike with accurate, relevant and actionable insights to proactively block threats before they materialize into attacks.

Learn more at **www.Bitsight.com**

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT