cybersixgill

Mastering Your Cyber Threat Preparation

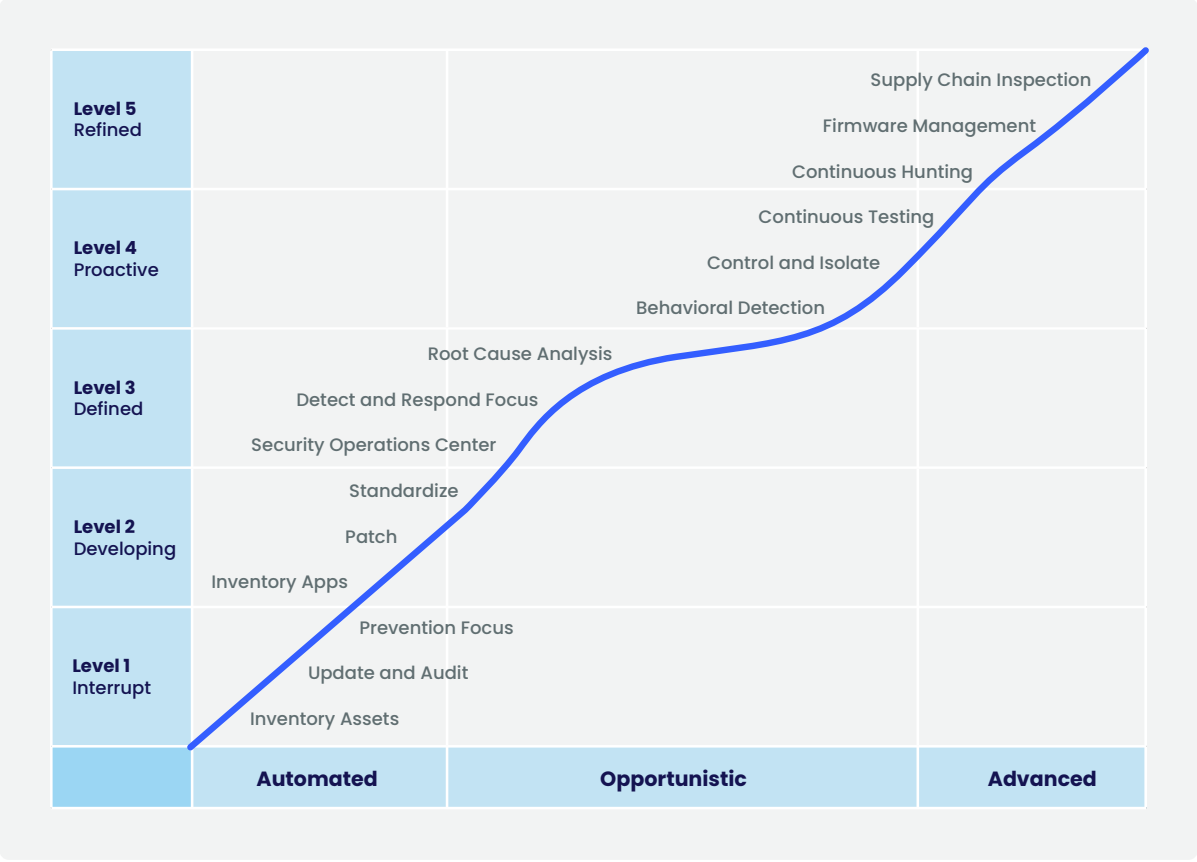
Part 2: The 5 Levels of Cyber Threat Intelligence Maturity

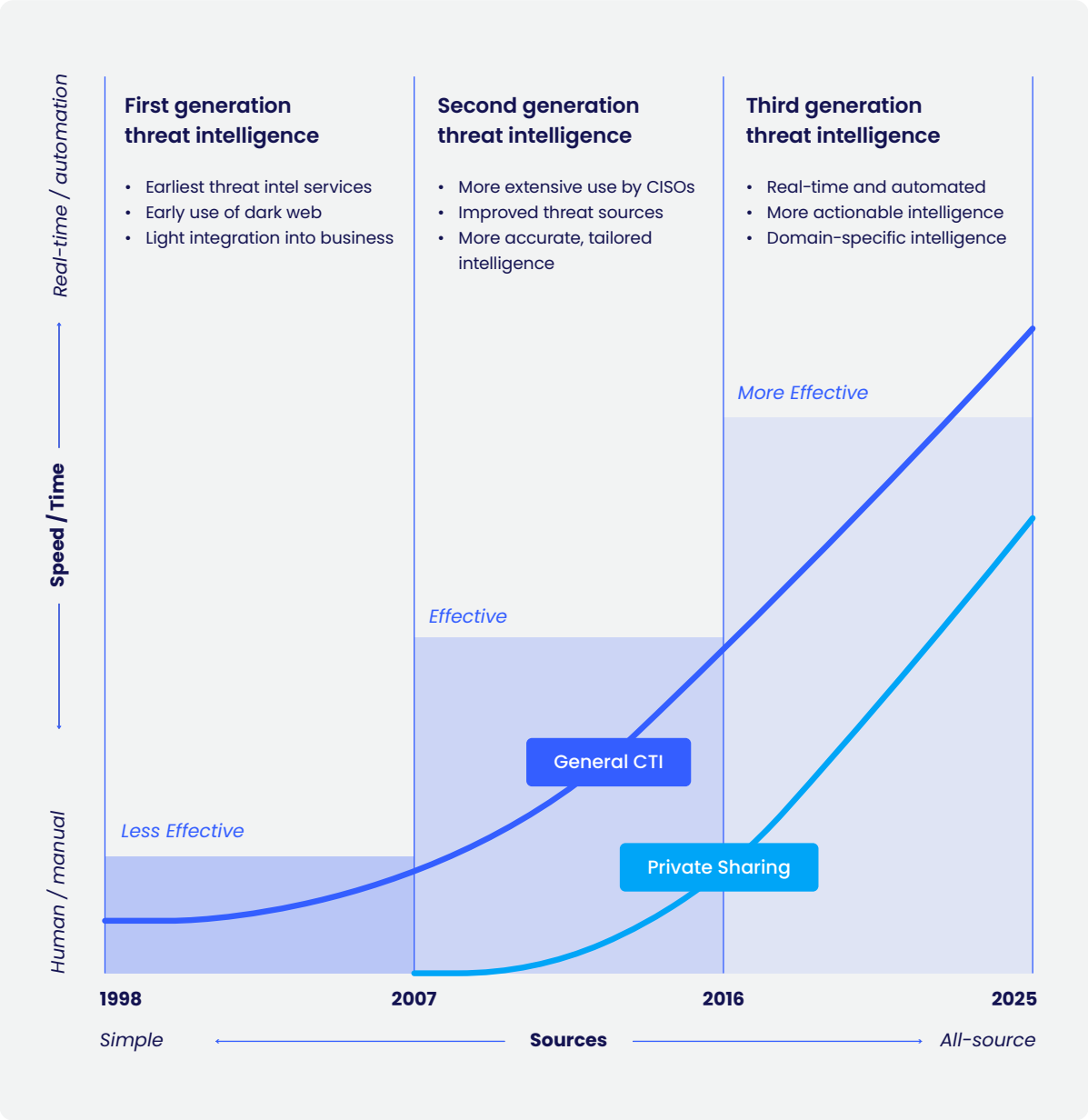
Gartner defines Cyber Threat Intelligence (CTI) as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." While easy to define, such an objective is difficult to achieve.

Comprehensive cyber threat intelligence should be any organization's first line of defense. Without a thorough understanding of the threats that pose the most significant risk to its brand, digital assets, and supply chain, companies are highly limited in their ability to protect against the ongoing onslaught of cyber warfare. But to better understand the varying levels of CTI maturity.

The Dark Web: Models of Response According to Cybersecurity Maturity Level

In organizations whose security teams are already overwhelmed with the never-ending stream of cybersecurity threats from just the clear web alone, the more pressing dangers posed by those who frequent what's known as the "dark web" are often overlooked. The dark web is at the heart of the underground cybercriminal, home to countless criminal marketplaces for illegal goods and services, constituting the wellspring of most cyber-attack methods. For example, malicious threat actors were recently able to gain access to the codes and networks of game developer Electronic Arts (EA), infiltrating the system by purchasing an EA member's ID, which had been stolen and resold on the dark web for a mere $10. After they bought an ID on the underground marketplace, the cybercriminals reached out to EA's IT team through the company Slack channel. They used the stolen identity information to pose as the employee and request a multifactor authentication token, which allowed them access to EA's corporate network.





Cybersixgill's solutions are designed to detect and respond to threats emerging from the dark web and those inhabiting it, providing invaluable threat intelligence sourced for that purpose.

Level 1: Unstructured

In an immature organization, when faced with a threat from the dark web, the response would most likely resemble an emergency room - detecting imminent threats and responding immediately to address them. However, with Cybersixgill's solutions, organizations enjoy automated alerts of incoming threats, such as:

- **Brand protection**
  Customers receive automated alerts warning of abuse of their brand, such as rogue applications on app stores
- **Phishing detection**
  Customers are informed of new domains trying to impersonate their company and attributions to underground chatter if it exists.
- **Data leaks**
  Customers receive automated alerts regarding leaked customer data, including OCR-extracted text from images to identify logos and designs.
- **Compromised credentials**
  Customers receive automated alerts in the event of leaked employee credentials.
- **Executive/VIP monitoring**
  Customers receive automated alerts if their executives are being targeted by a cyber or physical threat, including spear-phishing attacks, CEO scams, doxing, etc.
- **Credit card detection**
  Customers, receive automated alerts if their credit card credentials are leaked or compromised, sold on underground credit-card markets, IM apps, and IRC chats.

Level 2: Initial

At this second level, the organization is shifting from a reactionary posture to an anticipatory, analytical stance. Cybersixgill aids this process with such features as:.

- **Vulnerability assessment**
  Cybersixgill's solutions provide customers insight into their organizational threatscape and attack surface, allowing customers visibility across their digital systems, assets, and data, as well as any vulnerabilities emerging from the dark, deep and straightforward web. With an AI-powered scoring engine predicting the likelihood of vulnerability exploitation according to threat actors' intent, the organization can confidently prioritize vulnerabilities for patching.
- **Terror investigations**
  Cybersixgill provides its customers covert visibility into dozens of limited-access terror-related underground forums and thousands of Telegram channels. This information is shared intuitively to give a coherent intelligence picture across various datasets in real time.

Level 3: Managed

At this next stage, the organization progresses from reactionary (ER) to proactive (OR) response, diagnosing and treating threats systematically and strategically. Cybersixgill's solutions also support and enhance this level of cybersecurity preparedness with the following features:

- **Fraud management (root-cause analysis)**
  Cybersixgill provides its customers a breakdown of their leaked credit cards by BINs, geography, issuer, etc. This process enables financial institutions to better implement a root-cause analysis of these leaks and take action to mitigate them.
- **Enriching endpoint protection (IoCs)**
  Providing a feed of indicators of compromise (IoC) appearing in underground channels, enriched with context, Cybersixgill can help organizations prioritize the risks posed by such IoCs.
- **Drugs, smuggling, and weapons investigations and marketplaces**
  Cybersixgill provides its customers access to dozens of weapons for drugs and guns and thousands of IM channels. As with the terrorist investigations feature in level 2, this information is disseminated intuitively to provide a coherent intelligence picture across the various datasets in real-time.
- **Detecting zero-day malware**
  Darkfeed detects malware-based attacks under development before they are deployed in the wild and detected by other security vendors.

Level 4: Repeatable

Risk prevention and planning are the names of the game at this level.

- **Cyber incident prevention, detection, and response**
  Cybersixgill allows its customers to investigate a specific threat or incident across its comprehensive datasets from the dark, deep and straightforward web. This information includes additional context, attributions of incidents to a particular actor of threat, and more.

Level 5: Optimized

At this stage, the organization has expanded its investigatory horizons, looking outside its operations to proactively guard against risks potentially posed by its partners and other third parties.

- **Third-party monitoring**
  Cybersixgill alerts its customers to the risk posed by third-party vendors.

Ready to Step Up to the Next Level?

As you start a CTI program, realize that it will likely take months for your organization to begin showing significant value and reach even the first level of cyber maturity. So be patient: this is a long-term journey, not a single action with immediate gratification.

It may help to set small goals over the first few months, along with key metrics for success. Then, focus on the critical use cases your organization wants to address by order of priority and strive to support these decisions - this is the point of having a CTI program in the first place. As the program matures, there will be more opportunities to handle additional requirements and more challenging problems.

Succeeding in CTI requires aligning the right people for the endeavor, using the most effective tools, and establishing a clearly defined goal for what the team wants to accomplish. A valuable part of any organization, CTI can accelerate the understanding of threats and help scope what actions are required to protect your assets effectively.

Today's organizations face unprecedented challenges in battling cyber threats. A comprehensive threat picture can give you the upper hand. It's time to include actionable intelligence from underground sources to improve your organization's performance.

To see how Cybersixgill's cyber threat intelligence solutions empower you to detect threats quickly, efficiently, and early, schedule a demo today.

BOOK A DEMO

About Cybersixgill

Cybersixgill's fully automated threat intelligence phishing, data leaks, fraud, and vulnerabilities, as well as amplify incident response – in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights and the ability to conduct real-time investigations. Additionally, rich data feeds such as Darkfeed™ and CVE insights from DVE Score™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems. Most recently, Cybersixgill introduced agility to threat intel with their CI/CP methodology (Continuous Investigation / Protection). Current customers include law enforcement entities.

Visit the Cybersixgill Resource Center for more insights.

To learn more about how Cybersixgill solutions can help your organization proactively protect and maximize its security investment with threat intel that makes an impact, email getstarted@cybersixgill.com today.

About the author

Brad LaPorte is a former top-rated Gartner Research Analyst for cybersecurity and Threat Intelligence, veteran US Cyber Intelligence, and product leader at Dell, IBM, and several startups. Brad has spent most of his career on the frontlines fighting cybercriminals and advising top CEOs, CISOs, CIOs, CxOs, and other thought leaders on how to be as efficient and effective as possible. He is currently a Partner at High Tide Advisors, actively helping cybersecurity and tech companies grow their go-to-market strategies.

Follow us

cybersixgill