CYCOGNITO

SOLUTION GUIDE

Understanding the Technology: Threat Intelligence & Exploit Intelligence

Overview

There's little doubt that threat intelligence is a critical function for enterprise-grade security programs. However, all too often, organizations struggle to translate threat intelligence into something that's actionable. What's needed is tailored, highly-relevant context on the way vulnerabilities impact a specific organization and its assets. Combining threat intelligence and context results in Exploit Intelligence, which gives security teams a truly actionable, prioritized view of risk. In this guide, we'll take a closer look at each of these technologies.

The Importance of Context

Today's defenders face challenges ranging from increasingly sophisticated and nefarious threat actors to a longstanding shortage of talent. On a daily basis, they also confront information overload – enormous volumes of alerts and events – with too few hours in the day to investigate or mitigate everything.

Threat intelligence was created to help solve some of these problems: what if defenders pooled their knowledge and shared resources so that everyone could better understand the current threat landscape? Wouldn't defenders be able to make better decisions if they knew which steps cybercriminals were planning to take next?

There's little doubt that threat intelligence is a critical function for security programs, and there's no question that information sharing can help to counter the world's most pressing cyber threats. But all too often, organizations struggle to translate threat intelligence into something that's actionable. What's needed is additional, highly relevant context. This can help security teams leverage threat intelligence to make faster, better-informed decisions and meaningfully reduce real-world risks. This combination of threat intelligence and context results in Exploit Intelligence.

To maximize its usefulness, threat intelligence should be readily accessible and applicable. In this guide, we'll take a closer look at both threat intelligence and Exploit Intelligence as well as the difference between them. Here is a snapshot:

All too often, organizations struggle to translate threat intelligence into something that's actionable. What's needed is additional, highly relevant context.

Comparison Chart

Capability	Threat Intelligence	Exploit Intelligence
Security testing for a broad range of issues that are not limited to specific threats and known attack sequences	No	Yes
Prioritization of what to remediate immediately based on a comprehensive view of the organization's entire attacker-exposed IT ecosystem	No	Yes
Current intelligence curated from one or more open source, proprietary or bespoke threat data sources	Yes	Yes
Requires normalization, contextualization and labor-intensive manual analysis	Yes	No
Provides a broad overview that can help decision-makers understand broader trends in the threat landscape	Yes	No

What is Threat Intelligence?

Threat intelligence is data that's been gathered with the express purpose of helping defenders mitigate cyber risk. Gartner defines threat intelligence as "evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing menaces or hazards to assets."

Threat intelligence can be obtained from a wide variety of sources ranging from cybersecurity researchers' blogs and mainstream media outlets to open-source and proprietary threat intelligence feeds that provide an ongoing stream of data about current or potential cyber threats. As a category, it's enormously broad. To make threat intelligence easier to leverage and consume, many organizations turn to threat intelligence platforms (TIPs) that consolidate and classify this informationin an effort to make it more useful in event triage, risk analysis or vulnerability management.

If you want threat intelligence to be relevant and actionable, you need to ask the right questions. Thoroughly understanding your organization's assets, network and attack surface is essential to make threat intelligence actionable.

4 things to understand about TIPs and other threat intelligence sources:

01 Most available threat intelligence is broad in nature

Typically, the more specific the threat intelligence, the more difficult it is to obtain. But the more general the insights are, the less likely they are to be actionable – or relevant to your individual organization.

02 Tailoring threat intelligence requires skill and expertise

The organizations that are most successful at deriving value from threat intelligence are those that have dedicated threat intelligence analysts on their teams. These analysts often need to collaborate closely with TIP vendors to triage and prioritize the information they provide.

03 If you want threat intelligence to be relevant and actionable, you need to ask the right questions

Thoroughly understanding your organization's assets, network and attack surface is essential. The vast majority of threat intelligence data concerns vulnerabilities that aren't present in your environment. Only by understanding what your attack surface and assets are can you ask the right questions about what your biggest risks are.

04 Threat intelligence generally cannot tell you which vulnerabilities to patch first

While threat intelligence can help to guide overall defensive strategies, it's rarely specific enough to enable you to prioritize particular activities within your security program. The best TIP vendors invest heavily in curating information to increase its relevance for their clients, but their efforts are based on what you told them about your own environment and assets.

Most threat intelligence isn't immediately applicable and is focused more on general trends than specific vulnerabilities that exist in your environment. For the average organization that has only a limited number of security hours available, monitoring threat intelligence feeds may not be the most useful way to spend your limited time.

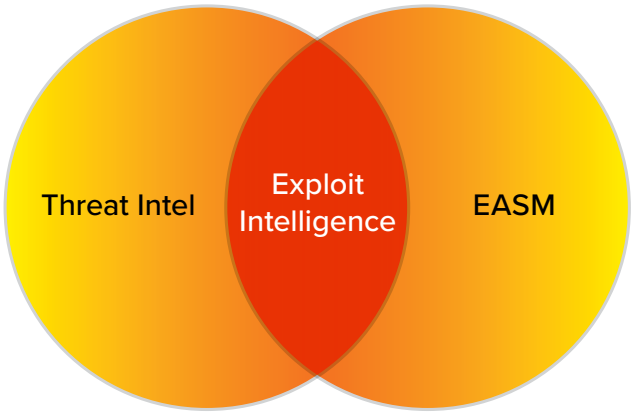
What is External Attack Surface Management and how does it benefit your use of threat intelligence?

> EASM is also able to contextualize assets – meaning it can automatically attribute them to the business entity that owns them – and can prioritize the risks that assets pose.

Threat intelligence is of the greatest value when it's actionable and immediately relevant to your organization. But understanding which feeds will be most relevant requires foundational knowledge of which assets are present within your environment. In addition, threat intelligence is most valuable when it's disseminated to the appropriate stakeholders. To achieve this, you'll need to understand the business context of the threat intelligence. Executives can benefit from an understanding of the current cyber risks that are germane to decision-making. Practitioners can benefit from becoming able to craft better detections or mitigate or prevent currently prevalent threats. Threat intelligence can also give them the capability to behave like real-world threat actors when simulating attacks.

External attack surface management (EASM) enables you to see your environment exactly as attackers do. They're continuously surveying and testing the attack surface to find the path of least resistance into your environment. EASM performs comprehensive ongoing reconnaissance across the entire IT ecosystem from an attacker's point of view, so that you can understand which vulnerabilities are present. This allows you to understand whether indicators of compromise (IOCs) in threat intelligence are pertinent to your organization. With this comprehensive understanding of what's present in your environment – and which gaps are there – you can leverage the threat intelligence that's most relevant.

Risk = TVC



Exploit Intelligence

What is Exploit Intelligence?

Exploit Intelligence expressly tailors threat intelligence to your organization's unique attack surface and its vulnerabilities using machine learning and natural language processing to alleviate the demands on already overstressed analysts. Real-world attackers don't consult the Common Vulnerability Scoring System (CVSS) before deciding which security gaps to exploit. Instead, they try to find the path of least resistance, figuring out what's likely to be easiest to target, following the trends, or repeating common patterns of behavior. Exploit Intelligence layers an understanding of how vulnerabilities are currently being exploited in the wild onto a map of the vulnerabilities in your attack surface. In other words, it is a sophisticated combination of curated threat intelligence and next generation external attack surface management.

Why Leverage Exploit Intelligence?

Exploit Intelligence empowers you to focus on the most impactful issues on your attack surface – those which are being actively exploited.

Together with vulnerability intelligence (identifying which software or asset configuration vulnerabilities are present in your environment), Exploit Intelligence lets your team know where to focus first. Plus, Exploit Intelligence includes step-by-step guidance on how to safely simulate real-world attacks, enabling your team to see how your countermeasures stand up against actual adversarial behaviors.

Exploit Intelligence also includes information on what the asset does, who owns it and where it's located. Together with the prioritization information that's part of EASM, this dramatically speeds patching.

The Reality: Threat Intelligence and Exploit Intelligence

Let's take a closer look at what bringing together threat intelligence and Exploit Intelligence makes possible:

- On their own, threat intelligence feeds and platforms can seem like an overwhelming fire hose of information. When combined with Exploit Intelligence, threat intelligence can be presented as a set of specific advisories that tell you which of your assets are impacted by a threat – and which have already been patched or are otherwise invulnerable.

- Unlike threat intelligence, Exploit Intelligence is immediately applicable in red teaming or security testing, since vulnerabilities are presented along with a set of step-by-step instructions that tell you how to validate the finding in an easy-to-follow procedure. Exploit Intelligence also lets you know whether it's safe to try to validate the finding, or whether doing so will impact your systems adversely.

- Exploit Intelligence also includes information on what the asset does, who owns it and where it's located. Together with the prioritization information that's part of EASM, this dramatically speeds patching.

In Summary

Figuring out which vulnerabilities attackers are currently exploiting – or which they're most likely to target in the future – should be a cornerstone activity within your vulnerability management program. Threat intelligence can indeed help you answer this question. However, it's likely that you're not approaching the problem in the most efficient way if your starting point is a set of intel feeds or a TIP. Instead, you need to start with a thorough and comprehensive understanding of your organization's attack surface. Exploit Intelligence is applied, relevant threat intelligence. It's tailored to your environment and designed to expedite validation and remediation of the most critical risks in your attack surface.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO