Threat intelligence

The art of intelligence-led cyber defense

In a hostile cyber environment, the power of threat intelligence is essential to make cyber defense fully ready to face attacks and respond rapidly.

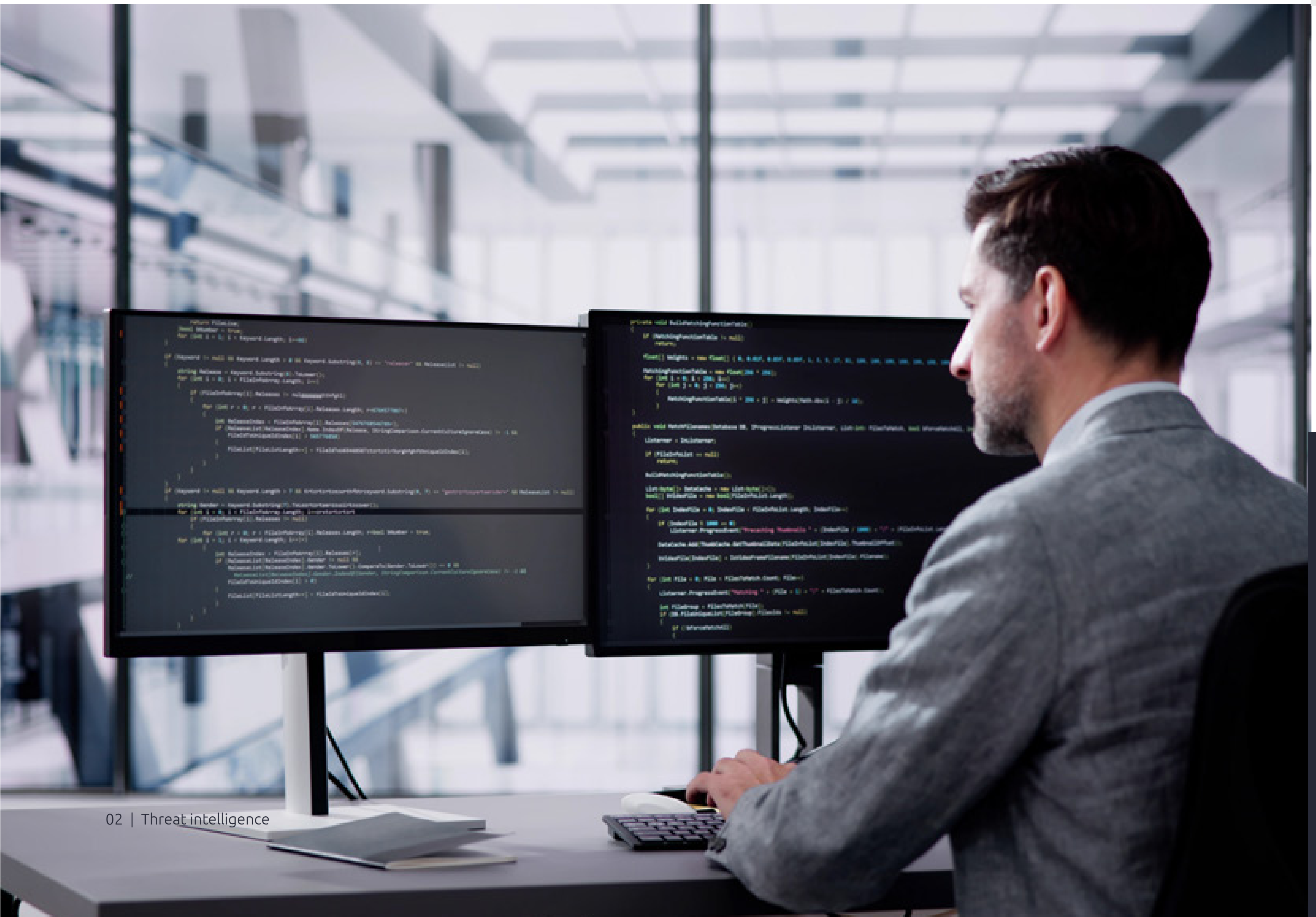
Building an accurate view of the cyber threat environment around an organization is essential for an organization to protect itself effectively.

Combating cyber attacks with full effect requires a strategy that includes understanding the full range of active threats and the surrounding environment. Integrating threat intelligence is a key part of a strategy that aims to keep an organization operational in the face of attacks. This can potentially save millions by protecting revenue and limiting costs of mitigation.

As Sun Tzu, the legendary 6th c. BCE Chinese military strategist put it, “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

Threat intelligence – also known as cyber threat intelligence (CTI) or “threat intel” – is detailed, actionable information about cybersecurity threats targeting an organization. It is gathered and analyzed continuously for insights used to shape overall strategy for cybercrime defense. It is an approach that provides context and specific information to be used to identify and anticipate cyberattacks, improve security measures, and reduce risk exposure.

Regulators now expect threat intelligence to be integrated in organizations’ cyber defense architecture. The European Union’s Digital Operational Resilience Act (DORA), applicable to institutions conducting financial transactions in the EU, has brought increased pressure and urgency to embedding cybersecurity best practices, including threat intelligence.



Threat intelligence serves four strategic objectives:

1 **Enabling proactive defense through data-driven actions to prevent cyberattacks before they occur e.g., making impossible known forms of attack.**

2 **Detecting and responding faster to attacks by understanding threat trends and patterns, security analysts can be prepared for certain attacks and react most effectively.**

3 **Bringing contextual understanding of an organization's specific attack surface vulnerabilities, including identifying the most common tactics used by threat actors, and other indicators of compromise (IoCs).**

4 **Generating actionable insights for security teams, which they can use to evaluate current cybersecurity tools, address vulnerabilities, prioritize threats.**

CTI provides organizations with insights that can direct an organization’s cyber strategy in response to the shifting threat landscape. It can provide a better understanding of an organization's vulnerabilities. This includes the possible entry points for unauthorized access to a computer system or network; and which data, gathered through malware such as infostealers and relevant to cybersecurity, is being sold on the dark web.

In case of a data breach, threat intelligence can be used tactically for “threat hunting”.

This means retrieving malware logs and identifying all information that an information stealer has taken and made available on dark web forums and marketplaces. This can include password lists, browser history, operating system information, and running CPU processes. Immediate tactical action can make a significant difference in reducing the incident response time by hours. At the same time, credential leak monitoring can continue, enabling the identification of any further breaches or evidence of a wider attack.

Infostealers

Infostealers are a category of malware, a malicious trojan designed to extract sensitive information from a system or network. It collects login credentials, browsing history, credit card numbers, and other personal details, and then transmits them to the attacker. These digital spies often infiltrate devices via emails, fake ads, or compromised websites, blending seamlessly into daily browsing. Once inside, they silently siphon off your data. Most are sold on dark web marketplaces and are cheaply available, requiring low technical skill to run them.

Proactive prevention is not optional

Ideally, potential attacks can be prevented or detected early. It is the job of an offensive security team, otherwise known as penetration testers or ethical hackers, to proactively test an organization's cybersecurity system, review its security measures and alert the organization to possible attacks. Their primary objective is to show vulnerabilities and weaknesses in the organization's defenses that can be exploited by real-world attackers.

They use a variety of techniques to bring organizations to a high state of readiness for attacks, including penetration testing, social engineering, and breach and attack simulations (BAS). Simulations mimic real attack behavior based on industry sector and location to measure the effectiveness of security controls and improve incident response capabilities. Using a threat intelligence-driven approach when running a BAS lets organizations see the threat landscape from a wider perspective. By looking at the most relevant threats, they can understand an organization's actual potential vulnerabilities and then develop equivalent strategies for prevention, detection, and response.

The intelligence information is collected from a wide variety of sources, e.g., government, law enforcement agencies, commercial threat intelligence providers, technology vendors, and private and public threat intelligence sources. It is used by cyber security specialists to understand the interconnections between threats, as well as relationships between different threat actors. Organizations can then better anticipate and respond to the latest forms of threats and collaborate effectively with other organizations in the cybersecurity community to share threat intelligence and develop common robust defense strategies. This is done formally, for example, by participating in Information Sharing and Analysis Centers (ISACs) such as the Center for Internet Security[1], and the Health ISAC. These are non-profit organizations that gather information on cyber threats as well as pooling information, knowledge and analysis between private and public sectors about causes, incidents and threats.

[1] https://www.cisecurity.org/isac.

Outpacing cyber attackers

Imagine this: an offensive security team engaged to detect systemic weaknesses successfully locates a point of vulnerability in the client's system and manages to bypass existing security controls. This might suggest that the threat they simulated has either occurred before, or that an attack is currently active. The discovery prompts a shift towards threat hunting, with cyber defense becoming proactive and intelligence-led, highly targeted, and specific in its goals.

Threat hunters use various techniques, such as behavioral analysis, machine learning, and information shared by other threat intelligence teams, to identify anomalies and potential threats. They aim to detect all threats that pose a risk to an organization, looking for initial access brokers (IABs)[2], cybercriminals, hacktivists, and other cyber threat actors. They want to reduce dwell time, which is the amount of time an attacker remains undetected in a network, and to minimize the impact of breaches.

CTI can also be used for attribution of attacks, although this is done primarily by more specialized Digital Forensics and Incident Response (DFIR) teams. If evidence of an attack is found, a DFIR team will be called to contain, eradicate, and recover from the cybersecurity incidents. There is strength in close collaboration between threat intelligence and DFIR teams. At each stage of an incident response, threat intelligence can provide additional insights based on collective findings.

Threat hunters use a standardized model to understand and respond to cyber threats e.g., the MITRE ATT&CK® framework. This model is a method of categorizing attack techniques, tactics, and procedures (TTP) to improve detection of and responses to advanced threats.

[2] IABs seek to procure access to a network and sell it to other threat actors.

Real-time monitoring for indicators of compromise

Threat intelligence is not only used to respond to incidents as they occur. Proactive monitoring is a part of threat intelligence that helps organizations stay ahead of emerging threats.

Security telemetry is the automated continuous collection and transmission of security-related data to provide real-time, comprehensive visibility of potential threats. Artificial intelligence (AI) is already an established part of executing this process quickly and efficiently. Generative AI has multiplied the speed at which threat intelligence reports can be generated and distributed to clients' security information and event management (SIEM) systems, where they are used to generate alerts or activate other security controls. This connected flow of information culminates in faster flagging, blocking, and repositioning of an organization's security posture.

When indicators of compromise (IoCs) are detected, they are passed on to the security operations center (SOC). Security engineers use this information to tackle security issues by delivering patching information and workarounds as soon as they become available. This is especially important because not all vulnerabilities are immediately assigned common vulnerabilities and exposures (CVE) identifiers. After they have been added to a database such as NIST's National Vulnerability Database[3] or MITRE's CVE database[4] , CVEs simplify sharing data across separate network security databases and tools and improve how organizations evaluate their security coverage.

Threat intelligence teams also monitor for:

- I Evidence of vulnerabilities being actively exploited by threat actors
- II Proofs-of-concept published by threat researchers showing how a vulnerability could be exploited
- III The insights of DFIR teams who often encounter emerging threats during their investigations
- IV The latest workarounds and security patches available to clients to protect them from newly discovered vulnerabilities

Threat intelligence's wide-ranging view of the threat landscape illustrates how it is not an isolated service, but one that touches on many aspects of cybersecurity. It is a force multiplier for other cybersecurity resources.

[3] https://nvd.nist.gov/

[4] https://www.cve.org/

Know your enemy

When news broke in May 2023 of a huge cyber attack on Capita, organizations with Capita-managed infrastructure were on high alert. Following an approach from a client, Capgemini's security team gathered detailed threat intelligence and threat hunting guidance.

As the attack proceeded, the team monitored news outlets, social media, dark web platforms and Capita's share price, looking for indicators of what type of incident was taking place.

The team identified the attackers as the Black Basta ransomware group before the attack was public knowledge. They were able to give a full rundown on the Black Basta group's tactics, techniques, and procedures (TTP). This included a description of the attacker's cyber kill chain i.e., their plan of attack, as learned from earlier attacks. When one organization within a supply chain is compromised, an attacker may use this to access other organizations and extend the attack further.

All the intelligence was used as guidance for threat hunting, which allows detection, mitigation and containment of any similar attack within the client's environment, in this case before it was public knowledge.

Once details of the attack were widely known, the security team shared information with other clients, taking a proactive, responsible approach to wider cyber security awareness.

Rapid data leak detection

Day-to-day threat intelligence operations involve constantly actively watching the dark web for references to an organization, keeping a close eye on new vulnerabilities, and deciding whether there is a proof-of-concept in the public domain that would allow the exploitation of a particular vulnerability.

A threat intelligence service should be adaptable, versatile, and agile. For example, it could be oriented to monitor a supply chain. By analyzing a list of key suppliers who have access to infrastructure, a security team is primed for any suspicious activities, such as dark web chatter or financial irregularities. Or where there is suspicion of a suspected rogue insider, the CTI team can create a profile and look for signs of unusual spending patterns; or it could be directed to investigate customers or employee behavior. They can also monitor for mentions on social media and the dark web of high-profile figures, e.g., a CEO, in case this person becomes the focus of an attack.

Dark web credential leak

A cyber threat intelligence team in the UK discovered leaked credentials on the dark web. When reporting this to the client, they then discovered that the user whose credentials had been stolen by infostealer malware was "patient zero" (i.e., the first affected) in an ongoing attack under investigation.

The CTI team was able to find and access the malware logs on the dark web and recover copies of all files and data stolen. This also allowed the client security team to identify what had been stolen, from where, and how. Threat intelligence also gave the client network IoCs that were used to prevent other users from being compromised; and to scan the security system to detect any other users similarly affected.

A highly adaptable threat intelligence service

Cyber threats come in various forms, from cybercrime and espionage to insider threats from rogue employees or accidental threats caused by human error. Threat intelligence offers crucial insights into their nature, enhances preparedness, and aids rapid responses in the ever-evolving landscape of digital threats.

At Capgemini, we offer customized threat intelligence services that help businesses of all types and sizes quickly detect and respond to global threats. With a network of 15 connected Cyber Defense Centers (CDCs) and more on the way, we are a global team of more than 6,200 cyber experts in over 50 locations worldwide to help us prevent attacks effectively.

Find out more

For further information please contact:

Billy Camlin
Threat Hunting Analyst
billy.camlin@capgemini.com

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com

For further information please contact:
cybersecurity.in@capgemini.com