Data security: Looking at the big picture

As cyber threats grow more sophisticated, context holds the key to data defense

Capgemini

Organizations that fail to adequately protect their data should not be asking if they will experience a cyber-attack, but rather when it will happen.

We live in a digital world fueled by data – and data is valuable. Even more valuable than gold or oil, according to some. And, like anything valuable, there is a risk of theft. Unfortunately, cyber-attacks are occurring with alarming frequency. In the year 2022, ***83% of organizations found themselves victims of more than one data breach[1].*** In just the first three months of 2023, ***over six million data records were exposed globally due to data breaches[2].*** The loss of confidential information can lead to identity theft, damage to company reputation, loss of customer trust, and regulatory consequences such as fines or legal action. Data breaches also result in substantial financial losses. ***The average cost of a data breach in 2023 was $4.45 million USD[3].***

With the cybersecurity threat level at an all-time high, all organizations have security measures in place to some extent. However, they often fall short when it comes to identifying all potential vulnerabilities and seeing how these vulnerabilities might be connected.

As technology becomes more ingrained in various facets of our lives, combating cybercrime demands an extensive strategy that leverages a comprehensive understanding of cyber threats and the environments in which they unfold, with particular emphasis on the integration of threat intelligence. This requires an approach that incorporates threat intelligence and analysis of cyber-attacks into the broader strategy for preventing cybercrime.

What is threat intelligence?

Threat intelligence is the collection, analysis, and sharing of information about potential and actual cybersecurity threats. But it's more than just taking data and transferring it from one computer to another; it is a comprehensive approach that provides context and information that can be used to identify and prevent cyber-attacks, improve security measures, and reduce risk exposure.

Threat intelligence should serve three purposes: strategic, operational, and tactical. At the strategic level, it provides organizations with the insights they need to make informed decisions. In operational scenarios, like threat hunting, threat intelligence can provide a better understanding of an organization's vulnerabilities, the possible entry points that an attacker can use to gain unauthorized access to a computer system or network, and what is being sold on the dark web through malware information stealers.

In the event of a data breach, threat intelligence can be used tactically to help retrieve malware logs, revealing all the information that the information stealer has taken from a particular computer system. This includes password lists, browser history, OS information, and running 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.

[1] ***The Devastating Business Impacts of a Cyber Breach,*** Harvard Business Review, May 2023
[2] Number of data records exposed worldwide from 1st quarter 2020 to 1st quarter 2023, ***Statista,*** June 2023
[3] Average cost of a data breach in the United States from 2006 to 2023, ***Statista,*** September 2023

Prevention is the best form of protection

Ideally, potential attacks will be detected and prevented before they occur. It is the job of an offensive security team to proactively test an organization's network or system to review its security measures and raise awareness of possible attacks. Their primary objective is to identify vulnerabilities and weaknesses in the organization's defenses that can be exploited by real-world attackers. The team may use a variety of techniques, such as penetration testing, social engineering, and breach and attack simulations (BAS). These simulations mimic real-attacker behavior to measure the effectiveness of security controls and help improve incident response capabilities. By looking at the most immediate threats, they can gain a clear understanding of potential vulnerabilities and can develop more effective strategies for preventing, detecting, and responding to them.

Using a threat intelligence-driven approach when running a BAS lets organizations see the threat landscape from a wider perspective. It does this by providing detailed and timely information about the types, tactics, and evolving nature of cyber threats. This information is collected from a variety of sources. It helps organizations understand the interconnections between different types of cyber threats, as well as the relationships between different threat actors. This understanding allows organizations to better anticipate and respond to emerging threats, as well as to collaborate more effectively with other organizations in the community to share threat intelligence and develop more robust defense strategies.

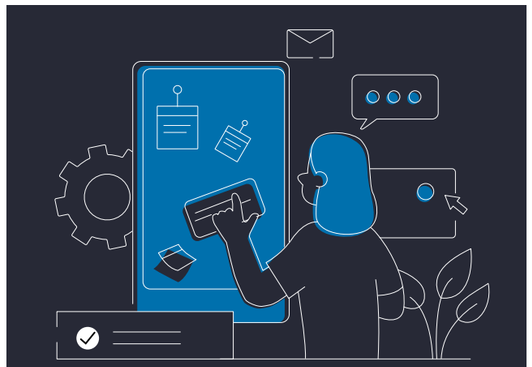
Cyber safety comes from taking a proactive approach

Imagine this: an offensive security team successfully identifies a point of vulnerability in the client's system, managing to bypass existing security controls. This outcome could suggest that the threat actor they simulated has either been there before or is actively executing such an attack. This discovery prompts a shift towards threat hunting. Threat hunting is a proactive and intelligence-led approach to cybersecurity. It involves actively searching for potential threats or indicators of compromise (IoCs) within an organization's network or systems. Unlike traditional security measures, which primarily focus on detecting and responding to known threats, threat hunting aims to identify previously unknown or advanced persistent threats (APTs) that may be hiding in an organization's environment. Threat hunters use various techniques, such as behavioral analysis, machine learning, and information taken from other threat intelligence teams, to identify anomalies and potential threats. The ultimate goal of threat hunting is to reduce the dwell time, which is the amount of time an attacker remains undetected in a network, and to minimize the impact of any breaches.

Threat hunting is highly targeted and specific. It typically involves using a standardized model for understanding and responding to cyber threats like the MITRE ATT&CK framework; a cybersecurity model that categorizes attack techniques, tactics, and procedures (TTP) to help organizations detect and respond to advanced threats.

If artifacts or evidence of an attack are found, a Digital Forensics and Incident Response (DFIR) team will be called upon to contain, eradicate, and recover from the cybersecurity incidents. DFIR teams aim to minimize the impact on the organization's operations and reputation. DFIR teams use various tools and techniques, such as forensic imaging, analysis of log files, and memory analysis, to identify the nature and extent of the incident, as well as to gather evidence for legal and regulatory purposes.

There is strength in the collaboration between these teams. At each stage of this process, threat intelligence can provide additional insights based on the collective findings of all the teams involved.



Quickly detecting data leaks

When a major incident occurred in the Nordics in early 2023, a Digital Forensics and Incident Response (DFIR) team was urgently called upon to swiftly identify data that had been leaked. To confirm if data was being sold, the DFIR team scoured forums and dark web marketplaces; looking for any indicator that that data was up for sale. They also analyzed communication between threat actors – individuals or groups that seek to exploit vulnerabilities in computer systems, networks, or databases with malicious intentions – to determine the perpetrators' identity, modus operandi, and intentions.

Day-to-day threat intelligence operations involves actively monitoring the dark web for references to an organizaton, keeping a close eye on new vulnerabilities, and determining whether there is a proof of concept out there that would allow the exploitation of a particular vulnerability.

Real-time monitoring

Threat intelligence not only used to respond effectively 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. 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 immediately receive common vulnerabilities and exposures (CVE) identifiers. Threat intelligence fills this gap, informing prioritization based on real-world threats.

This further illustrates the fact that threat intelligence is not a standalone service. Rather, it's a force multiplier that enhances various aspects of cybersecurity. It assists in resource augmentation, offering expertise, manpower, technology, and reach. It encompasses not only the consumption of standard threat intelligence sources but also insights from DFIR teams who often encounter emerging threats during their investigations.

A highly adaptable threat intelligence service

Cyber threats can come in various forms, from cybercrime and espionage to insider threats from rogue employees, or even accident threats caused by human error. When a crisis strikes it must be dealt with swiftly and comprehensively, regardless of the cause of the threat.

Threat intelligence is the linchpin that ties together various aspects of cybersecurity, providing crucial insights, enhancing preparedness, and facilitating rapid responses in the ever-evolving landscape of digital threats. This can only be achieved through a pragmatic approach that draws on the skills of specialists in different areas and quickly communicates information from various sources.

Capgemini offers a threat intelligence service that goes beyond a one-size-fits-all approach. It's a versatile service that can be easily adjusted to examine supply chains. By analyzing a list of key suppliers who have access to infrastructure, we can monitor for any suspicious activities, such as dark web chatter or financial irregularities. We can also investigate their customers or employees. If, for example, there is a suspected rogue insider, we can create a profile and look for any signs of unusual spending patterns.

At Capgemini, we provide customized 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're backed by our cyber experts in 50+ locations worldwide to help us prevent attacks effectively.

Find out more

Get in touch with our experts to learn more about our threat intelligence solutions and services.

Billy Camlin
UK Computer Security Incident Response Team (CSIRT) Lead, Capgemini
billy.camlin@capgemini.com

Lesson learning at the earliest opportunity

When the news broke in May 2023 about a huge cyber-attack with Capita, clients who work with Capita were understandably concerned. Capgemini's DFRI teams were vigilant and responded rapidly. They monitored not only news outlets and social media but also dark web platforms and Capita's share price, looking for some kind of indicator of what type of incident was taking place.

A client with Capita-managed infrastructure came to Capgemini early, seeking assistance; the DFIR teams provided them with immediate information about the threat actor involved: the Black Basta ransomware group. This was a full rundown and deep dive into the Black Basta group and included their tactics, techniques, and procedures. Our rapid response allowed us to assist our client even before the full details of the situation became public knowledge. We keep a running dossier on ransomware groups which meant that – within a few hours – we were able to supply our client with the group's attack chain tools, the techniques, tactics, and procedures that they were using, and we were also able to provide them with threat hunting guidance.

We also shared this information with other clients, fostering a proactive approach to security.

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

GIS_042024_SC