DigitalXRAID
CYBER SECURITY EXPERTS

CYBER SECURITY

Threat Intelligence

The Fast Response
to Cyberattacks

Why Cyber Threat Intelligence is Important

Cyber criminals will attack any organisation, regardless of size. While enterprises typically rebound from customer confidence problems and other issues that come after a data breach, some small and medium-sized businesses (SMBs) never recover. Within 6 months of a data breach, 60% of businesses are forced to shut down.

Many businesses are understaffed, underfunded and don't have the time or expertise to defend against malicious actors. Managed security service providers (MSSPs) can provide the threat data, intelligence, experience, expertise, and focused attention needed, to identify and control attacks.

Threat intelligence is a popular term in the security industry and has become a catch-all phrase for a range of technologies and approaches. Threat intelligence is the essential output of an organisation's threat research and analysis process that includes actionable information about attackers, their tools, infrastructure, and the methods to detect threats in the network - and most importantly how to prioritise the response to those threats.

Threat intelligence works by focusing the organisation on the most important threats facing their systems and networks at any given time. This will allow an organisation to defend against, and deal quickly with, ongoing data breaches and detect and respond to cyberattacks, often before they happen. Maintaining a threat intelligence program provides your business with the necessary information to help to identify unknown adversaries and decreases the likelihood of the attack being successful - as well as limiting the severity of any attack.

Threat intelligence comes in many forms. Some of the forms that we commonly see today include IP addresses, domain names, DNS (Domain Name Service) servers, URLs, file hashes, network signatures, attack patterns, and occasionally written profiles of attackers.

Most IT teams lack the technology and resources to automate the data correlation and analysis process. They often rely on the simple collection of log files for their threat analysis. Compounding this challenge is the fact that, for any IT team, security is often just one of many essential responsibilities to the organisation. The IT team likely does not have the time or even the technologies to manage and sort through the mountains of log data collected by all of their critical systems. They also lack the time needed to perform the necessary research to understand the latest techniques and infrastructure used by attackers, in order to detect today's emerging threats.

Gathering intelligence data from the multiple sources needed to paint a complete picture is a constant and never-ending process, which can be a huge drain on internal resources. Having a managed security service provider (MSSP) in place that can produce in-depth threat intelligence and protection is critical to staying ahead of digital threats, as well as providing the capabilities to respond to potential security breaches quickly.

From a proactive perspective, threat intelligence monitors events inside and outside of your network. This helps to identify suspicious activity and find patterns in cyberattacks that help to determine what security features should be implemented next and to stop attacks before they happen. Fully managed cyber security services are invaluable, especially in organisations where even just a few hours of downtime could have serious consequences for the business.

Threat intelligence comes in many forms. Some of the forms that we commonly see today include IP addresses, domain names, DNS (Domain Name Service) servers, URLs, file hashes, network signatures, attack patterns, and occasionally written profiles of attackers.

Within 6 months
of a data breach,

60%
of businesses are forced to shut down

The 4 Types of Cyber Threat Intelligence

There are four key types of cyber threat intelligence that fit into the overall intelligence lifecycle. Each form of intelligence plays a key role in the information gathering process.

Strategic Intelligence

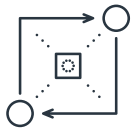
Strategic threat intelligence offers a high-level view of the threat landscape. Strategic intelligence is often the most complete form of intelligence and is presented as a report or series of options that are less technical in nature. This intelligence often highlights risk factors, groups involved, attack patterns, and other high-level insights that are derived from specific business requirements and questions.

Tactical Intelligence

Tactical intelligence investigates the specific techniques that actors use to carry out a cyberattack. This information can help prepare organisations to defend key assets, bolster security posture in specific areas or distribute learning material to help keep staff informed of new threats as they occur. Even if an attack does occur, good tactical intelligence will help to speed up the remediation.

Technical Intelligence

Technical intelligence is much like tactical intelligence but relies more on the exact technical execution of the attacks. This type of intelligence often outlines the Indicators of Compromise (IoC), which serve as clues as to exactly what was put at risk, and how a threat gained access. This detailed information is often used by malware researchers and cyber security professionals to match the attack to known strings of malware, and to document the breach based on the attack characteristic and digital evidence left behind.



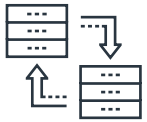
Operational Intelligence

Operational intelligence covers detailed, inside knowledge of how a cyber threat conducts its attack. This type of intelligence contains lists of command-and-control servers, email servers, aliases, and potential targets. It often consists of both technical and non-technical details that detail how an organised cybercrime group carries out an attack. Operational intelligence identifies countermeasures needed which can range from blacklisting groups of hostnames and IP addresses, to reinforcing areas of a network where attackers are known to try to gain access.

The 5 Steps of Cyber Threat Intelligence

Direction

The first step is to define what information is needed to make informed decisions in the shortest time frame. This helps to define objectives that are based on the evidence gathered, such as the nature of the attack, devices involved, and what was compromised.



Collection

This can include audit logs and IP addresses, and any other data sources needed, depending on the nature of the attack. At scale, data collection can exceed terabytes of space, meaning proper planning, storage, and processing will need to be considered.

Processing

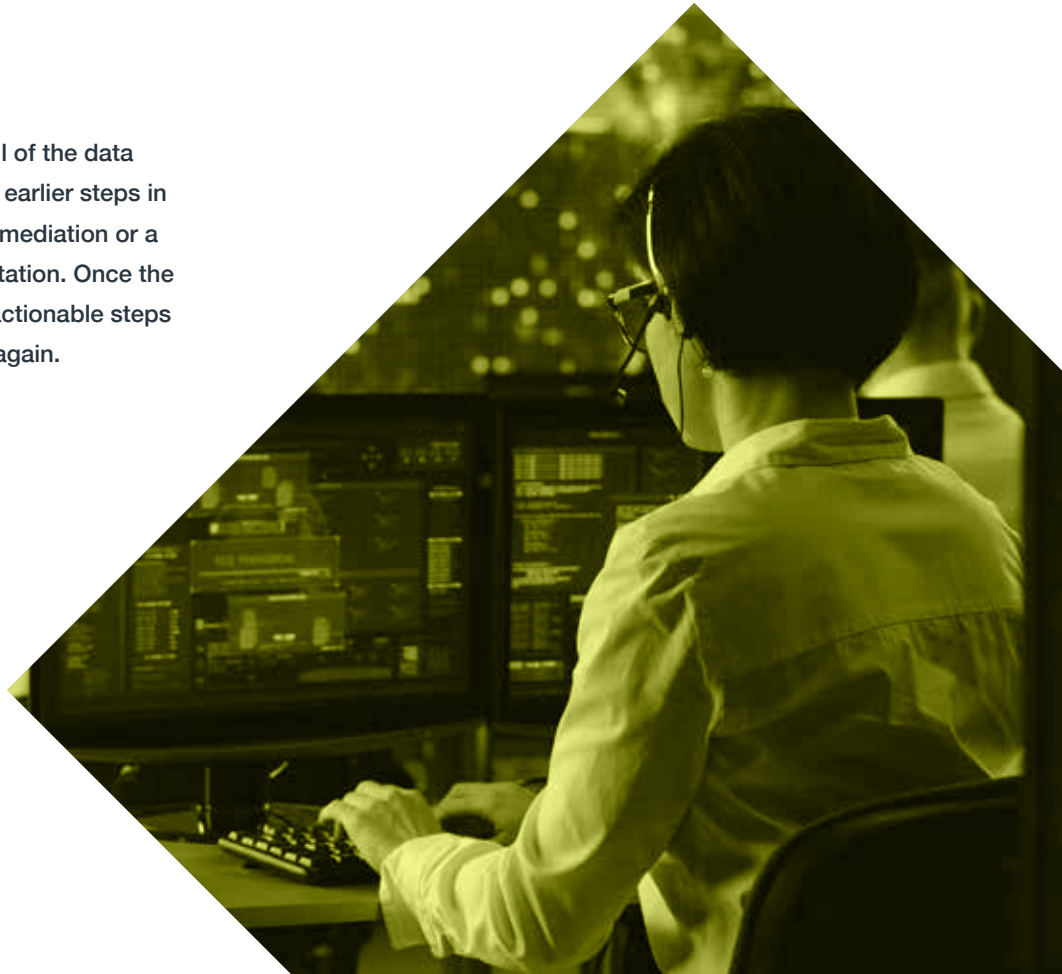
Raw data is processed into a more concise, actionable form. This can involve decoding information, organising raw data into groups, or tagging information that fits a specific context or source.

Analysis

A timeline of the attack must be proven using collected data, and contradictory information must be analysed and compared further. At this stage, patterns and other evidence may appear, requiring even further analysis. This is often one of the most time-consuming stages of the cycle and is almost always led by a specialist analyst who is aided by tooling.

Action

Any action is taken based on all of the data gathered and analysis from the earlier steps in the cycle. This could include remediation or a new security system implementation. Once the feedback has been given and actionable steps completed, the process starts again.



DigitalXRAID
CYBER SECURITY EXPERTS

Complete Protection for Your Business With an Outsourced Security Operations Centre

For a more resilient threat detection and response system, organisations need to find a way to move from a dependence on simple Indicators of Compromise (IoC) to real-time tracking of the underlying tactics, techniques, and procedures (TTP) that indicate malicious behaviour. This shift from IoC-based detection to TTP-based detection is driven by how quickly threat actors change attack infrastructure characteristics, like IP addresses and malware code, to evade detection.

Unfortunately, most traditional systems and even some of today's SIEM (Security Information and Event Management) platforms still limit their correlation rules to simple IoC. This is because they cannot handle the overwhelming log data being fed into them. If organisations are going to keep up with or stay ahead of attackers, they're going to need to integrate more sophisticated detection mechanisms into their security tool kit. These include mechanisms such as intrusion detection systems (IDS) which help to build a full threat intelligence picture alongside other tools such as SIEM and Log Management, Endpoint Detection and Response, Dark Web and Vulnerability Monitoring. However, these tools, their upkeep, and the monitoring needed, can be expensive. All of that, plus the amount of time and in-house expertise needed to be able to read and act on the threat intelligence data generated. Businesses, especially SMBs, are looking to MSSPs to help them manage threats by outsourcing their organisation's cyber security to a fully managed Security Operations Centre (SOC).

IT teams and businesses shy away from sharing information about security attacks and breaches they have experienced. However, a managed security service provider will benefit from aggregate value. The more data and telemetry a SOC has, the better incident detection, response and remediation the SOC team can provide. MSSPs remove the issues around a lack of skills and expensive tools – with highly qualified security professionals and the best of breed tooling available, all delivered at a lower total cost of ownership for your business. This effectively outsources your threat intelligence gathering process, which can save your internal team a lot of time and resources.

With advanced features such as 24/7/365 proactive security monitoring, security orchestration, and automation, you can quickly set up or scale a world class security program by implementing a fully managed SOC, without the cost and complexity of building it yourself.

A fully managed Security Operations Centre will:

- Continuously and intelligently collect data from across all environments
- Analyse and correlate data from across many security controls installed within those environments
- Fuel analysis through integrated, continuous threat intelligence about attacks going on outside the organisation
- Include automation and orchestration functionality to streamline threat response after malicious activity has been detected

How to Choose the Right Provider for Your Business

Cyber security is rarely an organisation's primary focus. In a world plagued by constantly evolving cyber threats, outsourcing cyber security to a managed security service provider is a smart decision for any business.

The Main Benefits of Outsourcing Cyber Security

Experience and Skill

The skills shortage in the cyber security industry is well documented. Finding and keeping one top-rated accredited cyber expert, let alone a whole team, is a challenging task. Outsourcing removes the worry of recruiting fully skilled and experienced cyber experts.

Time and Cost

Hiring and maintaining an in-house cyber security team is expensive. Recruitment tariffs, salaries, retention and training budgets mean the costs can escalate quickly. By outsourcing your cyber security management, your business can get 24/7 access to the expertise of highly trained professionals, familiar with the ever evolving and complex threat landscape.

Risk Management

A managed security service provider delivering a Security Operations Centre service will identify and assess your existing vulnerabilities and advise on how to mitigate the potential for future attacks. This partnership takes the uncertainty out of your next move to a more secure posture.

There are some questions that you should answer as an organisation to make the case for cyber security and to be able to choose a managed security services provider who can support all of your needs:

Can we afford a breach, reputationally as well as financially?

Do we have the systems and in-house skills to know if we're under active attack?

Are we meeting the minimum government approved cyber security standards?

How does the size of our business impact our cyber security requirements?

Do we understand our current exposure to risk and how this could impact our supply chain and customers?

Do we have the resources to protect our key systems and services 24/7/365?

Do we understand what is at risk if our business is not protected?

The right provider will get to know your organisation, understand the challenges you face, and implement the correct combination of services, tailored to your needs. By partnering with the right cyber security service provider for your business, you gain the highest level of threat intelligence and security protection and can avoid the time, cost and damage associated with a data breach.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

---

info@digitalxraid.com digitalxraid.com