

A Resilience Manager's Guide to Threat Intelligence



The deteriorating cyber environment for businesses

Cyber warfare isn't new. Whether perpetrated by state-backed or private actors, cyber-attacks have been around for quite some time now.

However, the growth in digital systems and the increasing reliance on third-party based providers have exacerbated cyber risk. Add to that, the popularization of remote working arrangements since the pandemic now means that malicious actors have a larger attack surface with which to exploit, while corporate IT has even more territory to defend.

What's been the effect? A dizzying array of cyber incidents, including high-profile breaches like MOVEit, T-Mobile, and MailChimp.

What's been the most common attack type, though? The 2023 IBM-sponsored Threat Intelligence Index found that the deployment of backdoors was the most common adversary action on objective, occurring in 21 per cent of all reported incidents, followed by ransomware at 17 per cent, and business email compromise (BEC) at six per cent. Meanwhile, malicious documents, or maldocs, spam campaigns, remote access tools, and server access were discovered in five per cent of cases each.

What were their impacts? The same IBM-sponsored study found that more than one in four incidents aimed to extort victim organizations, with observed extortion cases most frequently achieved through ransomware or BEC, but also often including the use of remote access tools, cryptominers, backdoors, downloaders, and web shells.

Data theft was the second most common impact, at 19 per cent of incidents. And credential harvesting leading to stolen usernames/passwords and requiring corresponding mitigations accounted for 11 per cent of incidents.

For their part, impacts to brand reputation, e.g., disruption to the services clients provide to their customers, accounted for nine per cent of incidents.

The **2023** IBM-sponsored **Threat Intelligence Index** found that the deployment of backdoors was most common adversary action objective, occurring in **21%** of all reported incidents, followed by ransomware at **17%**, and business email compromise (BEC) at **6%**.

What is threat intelligence? And what isn't threat intelligence?

Given this deteriorating cyber climate, we've been hearing a lot more about threat intelligence. But what is threat intelligence, exactly?

The definition put forth by the National Institute of Standards and Technologyⁱ (NIST) is threat information that's been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Analyst firms have come up with similar definitions. Gartner, for instance, has classified threat intelligence, or TI, 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"ⁱⁱ.

In other words, threat intelligence isn't just idle data.

Far from it. To be intelligent, threat information must be actionable. By that metric, threat intelligence isn't:



A list of indicators without additional context



Dated information that fails to help an organization protect itself or understand its attackers



An ignored data source

Internal and external threat intelligence

Contextualization is key to turning threat information into threat intelligence. But where does threat intelligence come from in the first place?

Well, according to the SANS Instituteⁱⁱⁱ, there are two types of threat intelligence. They include internal threat intelligence and external threat intelligence.

Internal threat intelligence, as the name suggests, includes data points and information collected from within the organization, then organized into meaningful content.

Conversely, external threat intelligence consists of intelligence acquired from outside the organization. Given the variety of information this can include, external threat intelligence tends to fall into the following categories:



Data subscriptions or feeds. Often vendor-provided information which comes from a delivery mechanism for specific types of data provided at pre-determined intervals. The value of this type of feed is usually only realized when the receiving organization implements the data into its own tools.



Commonality or communal information (by industry or geographic location). Organizations with similar interests often create industry-specific groups that facilitate the sharing of threat information.



Relationships formed with government entities and law enforcement. This is threat intelligence that comes from relationships with government and law enforcement.



Crowdsourced platforms. Information that comes from platforms that have funneled information from a large group of people.

How do these two types of threat intelligence differ in the context of cyber resilience management?

Well, internal threat intelligence sources, by their very nature, tend to yield more relevant information. Meanwhile, external sources, even though they will force companies to assess relevance and applicability, point up information that organizations aren't currently aware of.

Learning from both sets of sources, as such, is integral to fortifying an organization's security posture. After all, threat intelligence, deftly used, can often shorten the time from attack infection to detection and from detection to remediation.

But for this to happen, companies will have to submit both sets of sources to differing tests.

Of external sources, companies should ask:



What is the fidelity level of the information provided?



Is the intelligence provided relevant to operations? To the industry?



Can the intelligence be followed up on with the provider?



How is the information provided?

Meanwhile, internal threat intelligence can yield important answers. However, businesses will have to ask the following questions:



What we know?



How have we been attacked?



What are we/have we been protecting?

Challenges to making threat information actionable

The fact that organizations must ask these questions of their threat intelligence suggests that there's more to threat intelligence than just having it. And indeed, there is.

Companies sit on a massive trove of information; they have even more at their disposal, much of which could become actionable threat intelligence. Why it doesn't speak to the common challenges in making threat information actionable.

For one, too much threat information can overwhelm threat analysis. Often the quality of the threat information leaves much to be desired, as well.

This is often the case in companies with relatively immature threat intelligence capabilities, i.e., those companies who've failed to adequately define what threat intelligence is and how to use it to mitigate associated problems.

How to go about mitigating these challenges?

For one, researchers have suggested that companies break out of the mindset that fast sharing of threat intelligence is enough to avoid targeted attack^{iv}. Instead, trust must be seen as a key factor in the effective sharing of information between organizations.

Add to that, organizations should come up with a common, standardized format for sharing threat information, to minimize the risk of losing high-quality threat data. Here, choosing the best threat intelligence tool, as we will discuss later, can help.

What to do with threat intelligence?

But before we get to what digital tools help make threat intelligence more actionable, let's discuss what companies should be doing with their threat intelligence in the first place.

That's where incorporating threat intelligence into the corporate security posture comes in, i.e., the policies and procedures needed for a business to protect itself.

Here, threat intelligence can help businesses in the following ways:



Understand which areas of the business attackers are most likely to target



Use that insight to more effectively protect key assets



Identify potentially critical assets that weren't previously perceived as vulnerable

What's more, threat intelligence should also be incorporated into the information security and incident response team's daily activities. That's because when an incident does occur, useful threat intelligence can help businesses better understand the threat actor's thinking and how that actor is conducting the attack.

How to systematize the above? That's the role of the threat intelligence lifecycle. That lifecycle comprises the following six stages:

1

Direction. In the direction phase, organizations determine which threats to focus on. This involves assessing the risk that different threats pose to an organization and prioritizing those that are most serious.

Here, the most actionable threat intelligence is highly focused on specific events or activities; and so, it's advisable to avoid broad, open-ended threats. Organizations, for their part, can use a variety of different methodologies to determine which threats to focus on:

- Threat risk assessments. Threat risk assessments involve assessing the likelihood and impact of a threat happening. This information can be used to create a risk profile for an organization and determine which threats are most serious.
- Threat prioritization matrices. Threat prioritization matrices are used to compare different threats against each other to determine which ones are most important.
- Threat severity ratings. Threat severity ratings are used to measure how severe a threat is and determine how much attention it requires.

2

Collection. The collection phase involves gathering information about threats. This can be done through various methods, including open-source intelligence (OSINT), network scanning, and consulting subject matter experts. OSINT is the process of collecting information from publicly available sources, e.g., social media, news reports, blogs, and websites. Meanwhile, network scanning entails using tools to identify hosts and services on a network. The resultant information can be used to determine which systems are vulnerable to attack.

- 3 Processing.** This phase is all about organizing and analyzing collected information, which involves sorting through data, identifying patterns, and extracting meaning from it. Data mining, data analysis, and threat modeling are the most common methods employed to process data. Information yielded by each method should then be used to create mitigation plans and make decisions about security controls.
- 4 Analysis.** In this phase of the threat intelligence lifecycle, data is transformed into intelligence, at which time professionals review the collected information and distill it into actionable intelligence about the identified threat from the direction phase.


- 5 Dissemination.** This phase is all about sharing intelligence with the relevant stakeholders. The best-practice for the presentation of analysis at this stage is contextually tailoring it based on the technical experience of the audience in question.
- 6 Feedback.** The final feedback stage involves receiving feedback on the provided report to determine whether adjustments should be made in future threat intelligence priorities. Indeed, priorities might change, or the disseminated report might raise new questions that need to be addressed in the next report.


Digital capabilities to support the threat intelligence lifecycle


Of course, the threat intelligence lifecycle is meant to be an ongoing process. But how to keep it going effectively? That's where having digital capabilities to support the threat intelligence lifecycle comes in handy.


The right resilience management platforms with threat intelligence capabilities can, in fact, reduce the amount of time needed to get skilled responders focused on mitigating an attack. What does the right platform look like, though?

Capabilities to support the threat intelligence lifecycle to consider include:

- 

Monitor alerts about potential threats, receive relevant notifications, capture alerts, and escalate them into incident management
- 

Combine alerts with personnel and asset data to see who and what may be impacted
- 

Trigger notifications to affected personnel and assets, either in-app, via email, SMS, and/or voice messages
- 

Enrich situational awareness during ongoing incidents by adding further intelligence from threat monitoring

It's also worthwhile considering the vendor's threat intelligence options, e.g., AI-driven detection and/or keyword-based filtering. Sources matter, too, whether its hundreds of thousands of public data sources, digital and social media, and/or the deep and dark webs.

These sources can be integrated into a vendor's platform as an add-on. Once up and running, capabilities could look like the following:

- 

Escalating alerts into incidents so that organizations can manage their response
- 

See who and what is affected by an incident
- 

Visualize alert locations alongside people and assets, using the platform's mapping capabilities
- 

Lead personnel through business process, with fully configurable workflows
- 

Turn alerts into actionable insights using notifications and real-time analytics
- 

Bring Crisis and Security teams together in a single platform to consistently manage all prevention, preparation, response, and recovery activities according to business processes

Finally, for resilience managers, understanding what threat intelligence is (and isn't) is crucial to fortify their company's security posture and overall resilience aims. More than ever, that posture is being threatened by the increase in the number and impact of cyber threats.

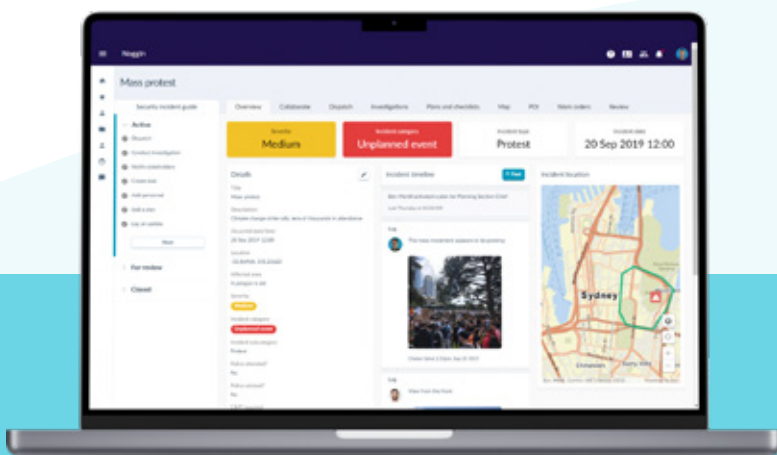
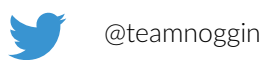
However, developing strategies and procuring digital tools like, Noggin, to make threat intelligence actionable and accessible are key to managing cyber threats and treatments in a consistent, systematic, and easy-to-use way.

Sources

- i. NIST, Computer Security Resource Center: Threat intelligence. Available at https://csrc.nist.gov/glossary/term/threat_intelligence.
- ii. Rob McMillan, Gartner: Definition: Threat Intelligence. Available at <https://www.gartner.com/en/documents/2487216>.
- iii. Matt Bromiley, SANS: Threat Intelligence: What It Is, and How to Use It Effectively. Available at https://nsfocusglobal.com/wp-content/uploads/2017/01/SANS_Whitepaper_Threat_Intelligence_What_It_Is_and_How_to_Use_It_Effectively.pdf.
- iv. Wiem Tounsi and Helmi Rais, Computers & Security: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Available at <https://www.sciencedirect.com/science/article/abs/pii/S0167404817301839>.



Like what you read? Follow Noggin on social media



noggin for Security

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Security gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Security solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: www.noggin.io
or contact: sales@noggin.io