IBM Security

September 2019

Threat intelligence builds winning teams

How smart companies leverage threat intelligence to improve their security posture

Contents

3 The best offense is a good defense

4 Putting your best team on the field

5 Strengthen your first line of defense

6 Improve threat hunting outcomes

7 Formulating a winning strategy

8 The team’s shared intelligence playbook

8 The final point

The best offense is a good defense

Security analysts aren't simply a part of your company. They're part of a team. Every day, they battle against an intimidating opponent with a seemingly endless array of tools, malware and a team of malicious hackers on their side. At the end of each day, success is defined by a shutout: whether or not they blocked the bulk of those attacks, tackled the cyber threats that snuck past their first line of defense and executed effectively against their security strategy.

In many ways, a security operations center (SOC) team functions like a sports team. You have your tier 1 security analysts as your primary defenders, your tier 2 and tier 3 security analysts who can take the ball and run with it when you need to go on the offensive and your managers who are responsible for crafting a winning strategy and ultimately answering to all stakeholders. And like any successful sports team, the better that SOC teams understand their opponent, the better chance they have of winning.

In the world of sports, scouting reports provide valuable insight into opponents' strengths and weaknesses. In the world of security, threat intelligence serves a similar role. Threat intelligence is complementary to the security intelligence that SOC teams collect from their own network and security tools, providing additional and often valuable insights into the who, what, where and why of cyberattacks. Threat intelligence feeds can be subscribed to or purchased from a variety of vendors and sources and may range from human-generated intelligence created by security experts to machine-generated telemetry data, social media intelligence or industry-specific intelligence.

Most enterprises use external threat intelligence to bolster their security efforts. In fact, it's not uncommon for an enterprise to subscribe to dozens of different threat intelligence feeds. Yet having threat intelligence doesn't automatically translate into a better defense. In fact, too much threat intelligence — or too little actionable threat intelligence — can have an adverse effect on SOC teams, generating more work as analysts react to false alerts and intelligence that isn't relevant for their industry or organization.

Putting your best team on the field

So what does good threat intelligence look like? First of all, it's reliable. It comes from a trusted source that you can base security decisions on with confidence. It's also actionable, allowing security analysts to leverage intelligence immediately to improve real-time security operations and tactics. And it's integrated with the rest of your security ecosystem, so analysts can access threat intelligence quickly from their existing Security Incident and Event Management (SIEM) systems and other security tools without toggling between different screens to find that information.

The goal for SOC teams isn't simply to have more intelligence on their side, but to have more relevant intelligence that can drive better outcomes at the moment of decision. Some threat intelligence partners, such as nonprofit Information Sharing and Analysis Centers (ISACs) and the Department of Homeland Security, are good sources for general threat intelligence. But their intelligence feeds only represent a part of a complete security scouting report. SOC teams also need to consider the intelligence behind the intelligence: Are their security experts better than our guys? Do they see things that we don't, or can't, see? Are they tailoring their intelligence to our industry and environment?

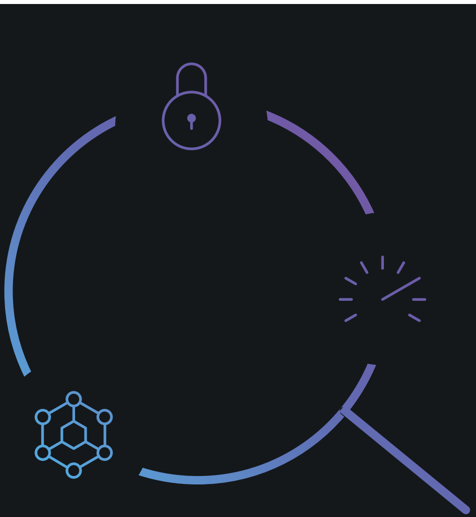
As we'll see in the following pages, the right mix of threat intelligence can help your security team perform better on the field and prevent your opponents (i.e., cyber criminals) from penetrating your defenses. We'll examine **how threat intelligence can make a difference in three critical areas of security: by hardening your frontline defenses, aiding threat hunting efforts and driving more effective security strategies.**

The IBM X-Force Exchange difference

The X-Force Exchange was considered for the "Best Threat Intelligence Technology" category at the 2018 SC Awards Europe.

Watch video

Good threat intelligence is reliable, actionable and integrated.



Strengthen your first line of defense

Enterprise SOC teams receive more than 200,000 security events on an average day.[1] The vast majority of those events are handled by machines and tier 1 security analysts. This mix of human and machine intelligence is an enterprise's first line of defense against cyberattacks. Threat intelligence can play an important role in strengthening this critical line of defense by helping machine-based systems block more attacks and human analysts better identify which events require further investigation.

Depending on the threat intelligence source, this tactical intelligence can include valuable data such as suspicious/malicious domains and endpoints, recent attacks and other Indicators of Compromise (IoCs) from around the globe. This intelligence, in turn, can be fed directly into machine-based security systems to enrich an organization's real-time blocking capabilities, both for inbound network events (e.g., a denial-of-service attack) and outbound network traffic (e.g., an employee clicking on a link to a known phishing site). Similar to a sports team's defensive line, SOC teams must anticipate new strategies and shifting players from their opponents or run the risk of being caught off guard on the next attack.

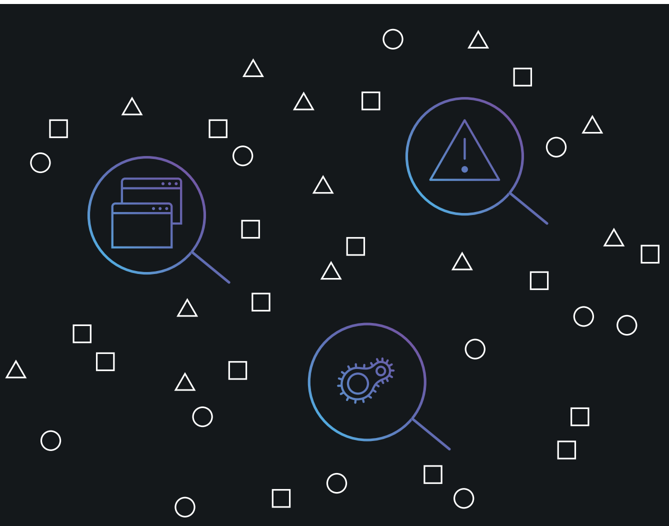
Tier 1 security analysts, however, do more than stop attacks. They also create opportunities for the "stars" of the security team — the tier 2 and tier 3 analysts who orchestrate the response and serve as threat hunters — to take the ball and run with investigations when live threats are potentially in play. Here, **threat intelligence can help front-line analysts triage and prioritize risks for threat hunters based on potential impact to their business,** similar attacks targeted to that industry/region, detected IoCs in the network and other real-time data.

X-Force Exchange Threat Intelligence: Speed Security Investigations

See how security analysts can research, collaborate and act on cyber-threats with the X-Force Exchange, a threat intelligence sharing platform.

Watch video

Tactical intelligence can include suspicious/ malicious domains and endpoints, recent attacks and other Indicators of Compromise (IoCs) from around the globe.



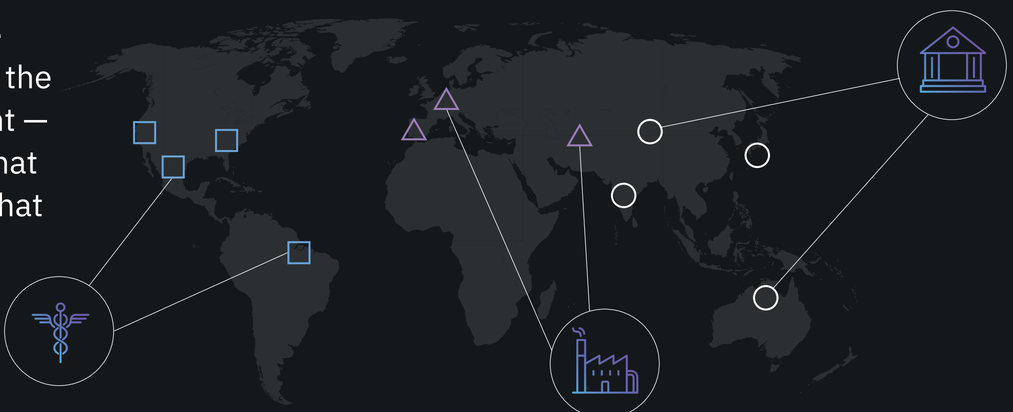
Improve threat hunting outcomes

Threat hunting is as much art as science. It relies on human experience and intelligence in concert with technology to connect security events, come to a conclusion and prescribe the appropriate remediation — all while the clock is ticking. The investigative art of threat hunting relies heavily on clues: Where does a threat come from? Who is the author? What is their intent? Is it working alone or in concert with other malware? SIEMs and other security tools aid in this investigative process, but without external data they can only connect the dots that exist in their own security logs. To make broader and better connections, SOC teams often bring multiple threat intelligence feeds into their SIEMs and threat hunting tools for additional clues and discoveries.

This kind of operational threat intelligence is most valuable when it's most relevant to the threat hunter's unique environment. A bank in Japan, for example, might gain little value from threat intelligence on hospital data breaches in North America, but could benefit immensely from knowing what kind of attacks had recently been experienced by financial services companies in Asia. **The best threat intelligence is contextual: it understands the context of the threat hunter's environment** — what industry they're in, what geography they're in, what kind of data they store, which IoCs are already present in the network — and helps threat hunters speed their investigations by enabling them to connect the right dots faster.

Threat hunters, like all security analysts, struggle with information overload. They may have to maneuver through thousands of security logs, bounce between multiple security tools and juggle information from dozens of different threat intelligence feeds. The ability to separate what's news from what's noise is critical in their jobs, and contextual threat intelligence can help threat hunters reach their goal sooner. If a threat hunter knew, for example, that a ransomware attack had been targeted recently to similar companies in the same industry and that some of the IoCs associated with that attack were detected in their network logs, they could elevate that threat as a top priority. To do this, however, threat hunters would need broad visibility across many different data sources — something they may not have. Adding federated search capabilities to the threat intelligence platform can help SOC teams gain that visibility and provide a critical piece of context — i.e., have we already been affected? — to the threat hunter's decision-making process.

The best threat intelligence understands the context of the threat hunter's environment — what industry they're in, what geography they're in and what kind of data they store.



Formulating a winning strategy

Threat intelligence can also play a strategic role by helping security decision makers plan, manage and build a stronger security posture. Much as a coach is responsible for giving their players the support they need to succeed — whether it's getting the most from existing players or getting more players to help the team — chief security officers, SOC managers and other senior-level security executives are responsible for putting the best people and processes in place to protect their business. If a global manufacturing company, for example, knew that some of its distribution partners had recently been subject to a data exfiltration attack, they might put new data security safeguards in place when sharing data with their partners. Or, if they see a rising trend in ransomware through phishing attacks, they might seek funding for a company-wide training program to educate employees on how to detect and avoid common phishing techniques.

Threat intelligence can also help security teams better understand their adversary. Threat intelligence might reveal who an attacker is, their motivation (e.g., financial, political), their preferred method of attack, known targets and so on. This information can give security teams a considerable advantage when planning where to focus their security efforts. If a company knows they are more likely to be targeted for ransomware or bitcoin theft in the coming year, they may decide to take proactive action by investing in an air-gapped storage solution for sensitive data or re-examining their access control lists every few months to reflect organizational changes in roles and responsibilities. And when it comes time to present the security budget to senior management, good threat intelligence can help support the ask for additional funding, too.

The most effective defense is an agile one. As the opposing players shift their tactics, your defenses automatically shift in response. With the right threat intelligence, security teams can predict how their opponents will respond to certain defensive plays and plan one step ahead. If you know that a certain opponent in a particular region is prone to use DDoS attacks as a smokescreen for data exfiltration, you might update your security processes and policies to automatically block outgoing data transmissions to that country during a DDoS attack.

The team’s shared intelligence playbook

Bringing threat intelligence into your SIEM tools might seem obvious, but what about the other security and business tools you use? By adding contextual threat intelligence to other security and business applications, security teams can ensure that everyone is on the same page of the security playbook. After all, if the goal of threat intelligence is to spot threat actors sooner, more eyes on the field reduce the likelihood that a threat could slip in through a backdoor.

The best way to connect threat intelligence with other applications is through open-source APIs, although not every threat intelligence feed will support this capability out of the box. When choosing a threat intelligence service, ease of integration with other applications should be an important part of the selection criteria. Another consideration is how your security team will mix threat intelligence with security data that may reside on premise and/or in the cloud. As more enterprises move to cloud-based storage and application hosting, the ability to bring these disparate data sources together with threat intelligence into a unified view of security information will be critical to making truly informed, real-time security decisions.

The final point

Threat intelligence is, in many ways, an extra player on the field. It can give security teams a competitive advantage against their opponents (i.e., cyber criminals) and even against their own competitors. A recent Harris Poll found that most consumers — three out of four — will not buy products from companies they don’t trust to protect their data.[2] With a confusing array of threat intelligence feeds currently available from both nonprofit and commercial vendors, security teams should select their threat intelligence with care.

The **most effective threat intelligence supports organizations at tactical, operational and strategic levels,** comes from a trusted source with unique security expertise and data that integrates seamlessly with existing security tools to simplify and strengthen real-time decision-making.

Ready to kick-off your threat investigation with the IBM X-Force Exchange?

Sign up for the IBM ® X-Force ® Exchange, a free threat intelligence sharing platform.

Start your free 30-day trial of the IBM ® X-Force ® Exchange Commercial API.

Learn more about the IBM Security threat intelligence offering:

Products

- IBM X-Force Exchange
- IBM X-Force Exchange API
- IBM X-Force Exchange Software Development Kit (SDK)
- IBM Threat Intelligence Insights

Services

- IBM X-Force Incident Response and Intelligence Services (IRIS)

IBM **Security**

Sources

1. Marc van Zadelhoff, "Cybersecurity's Next Major Challenge: Connecting Human and Machine Intelligence, ibm.com. IBM Corp., April 16, 2018, newsroom.ibm.com/IBM-security?item=30433. (Accessed on June 10, 2019.)

2. "Data Privacy Now A Top Public Priority," SecurityIntelligence. IBM Corp., April 24, 2018, securityintelligence.com/news/data-privacy-now-a-top-public-priority/. (Accessed on June 10, 2019.)

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2019
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

♲ Please Recycle