ThreatConnect.

Whitepaper

Smarter Security and Maximum Impact from

Intelligence-Powered Security Operations

Introduction

The cyber risks that today's businesses face are more plentiful and severe than ever. The U.S. Federal Bureau of Investigation[1] stated that cyberattack volumes saw an "unprecedented increase" over the course of 2021, far outstripping 2020's already high levels. In 2021, the FBI's Internet Crime Complaint Center (IC3) received a record 847,376 complaints from American businesses and consumers, resulting in potential losses in excess of $6.9 billion dollars.

Ransomware, business email compromise (BEC) and large-scale data theft abound, with criminal activities costing their victims — and insurers — dearly. The cost of the average data breach soared to a new 17-year high of $4.24 million[2] in 2021 at the same time that the total number of breaches climbed past the previous record[3] before the year was even out.

Business leaders are aware of the seriousness of these threats. In PwC's most recent Annual Global CEO Survey[4], for instance, cybersecurity risks were ranked first among the worries keeping corporate leaders up at night, surpassing pandemic-related health concerns and economic volatility. As a result, cybersecurity budgets are growing. Recent research from IDG[5] shows that a majority of CIOs (59%) expect to see their budgets increase at pre-pandemic rates for 2022.

But it isn't immediately obvious which investments will do the most to stave off the rising tide of cyberattacks. Certainly the imperative to manage ever-increasing risks has added to the pressures that security operations (SecOps) teams face, with human consequences for cybersecurity professionals that are severe. In a recent survey of security leaders and practitioners[6], nearly one-third (32%) of respondents reported being "very stressed" in their current job, and more than two-thirds said they'd personally experienced work-related stress symptoms like headaches, fatigue and insomnia. 36% said they'd seen their colleagues feeling overwhelmed and unable to cope.

It is clear that many enterprise security programs are currently in a dire situation, confronting too many events and alerts, with too little talent and not enough time to investigate everything that's worthy of attention. This situation leads to stress and burnout, of course, but it also results in a reactive approach that's doomed to failure, leaving SecOps teams struggling to organize internal processes and resources instead of anticipating and preventing the latest threats. Without the bandwidth to become more proactive, defenders are restricted to playing an endless game of catch-up with cyberattackers — one that they're unlikely to win.

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[2] https://www.ibm.com/reports/data-breach

[3] https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/

[4] https://www.pwc.com/ceosurvey

[5] https://foundryco.com/tools-for-marketers/research-state-of-the-cio/?utm_campaign=2022%20State%20

[6] https://threatconnect.com/resource/threatconnect-white-paper-cybersecurity-under-stress/

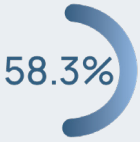
What's needed instead is a smarter way of making decisions, being more efficient, and improving collaboration in security operations. What we call **Intelligence-Powered Security Operations** makes it possible for security teams to do just that.

31% increase

in attack volumes from 2020 to 2021.
Source: Accenture

9.8% increase

in the cost of the average data breach from 2020 to 2021.
Source: IBM Security/Ponemon Institute



58.3% of security

programs today are consuming published threat intelligence.
Source: SANS Institute

79% of security teams

feel overwhelmed by the volume of threats and alerts they face.
Source: Enterprise Management Associates

35.4% of organizations

have documented intelligence requirements.
Source: SANS Institute

Broadly speaking, we define "Intelligence-Powered Security Operations" as what results when threat intelligence is a keystone of security operations. Infusing threat intelligence into activities across the entirety of security operations – whether that's prioritizing Common Vulnerabilities and Exposures (CVEs) or building start-to-finish incident management and response workflows– makes it possible for security teams to apply their efforts where they'll have the biggest impact against the most dangerous threats and the most prevalent attack tactics. And by orchestrating and automating processes, they can empower themselves to work effectively and efficiently, further driving down risk.

In the remainder of this white paper, we'll take a deeper dive into the concept of Intelligence-Powered Security Operations, exploring what it is, why it's needed and how to apply it in real-world enterprise security programs today.

01

Why Taking an **Intelligence-Powered Approach** is Imperative Today

The value of threat intelligence is broadly understood among enterprise security program stakeholders, and a majority of organizations already consume cyber threat intelligence (CTI) — as many as 93%, according to a recent SANS Institute[7] survey, although fewer than half (47%) have dedicated CTI teams in-house.[1]

However, many security programs struggle to operationalize the threat intelligence that they consume. According to the SANS Institute survey cited above, less than half (35%) of the organizations that use CTI have formally documented their requirements for threat intelligence. Many lack a means to translate threat intelligence into a form that's readily sharable or actionable. 73% simply disseminate the information through email, presentations or spreadsheets.

The ability to put threat intelligence to practical use often increases as a security program matures. While most try to leverage threat intelligence, less mature security programs do so in ways that are ad hoc or product-specific. More mature security programs tend to be better at operationalizing the information, but many still struggle to do so in a way that's consistent and centralized. And most organizations that consume threat intelligence report ongoing challenges with the quantity and quality of the data.

By and large, threat intelligence poses all of the classic "big data" problems: the information arrives in such great volumes, at such rapid velocities, and with such enormous variety that it's inherently difficult to apply it in ways that create value. It's also difficult to figure out which threat information is accurate and relevant.

Given the challenges with managing and operationalizing CTI, many organizations opt to not have a formal CTI function and instead take an ad-hoc approach or rely on a "decentralized" model where the CTI function is effectively turning on threat feeds that come with their security tools or using a single commercial threat feed across those tools. In some organizations, the CTI function is strictly part of the SOC and only used for threat investigation purposes, i.e., CTI is not disseminated to, and used by, other SecOps teams. The consistent theme is the view that keystone CTI is not a function that deserves to be elevated to the same level in the SecOps organization as the SOC or the vulnerability management team.

Given the breadth and seriousness of the threats that security programs currently confront, however, it needs to be. Applying threat intelligence is what will enable security leaders and practitioners to make the best possible choices about which activities will have the greatest impact on the biggest risks to the business.

It's imperative that today's security teams adopt this approach because it's the only way to move towards being a proactive, rather than reactive, organization, overcome resource and expertise scarcity and get ahead of the constant scale to keep up with daily responsibilities. These things have become endemic in the industry, but they work together to make a proactive approach impossible.

Putting Threat Intelligence to Work:

Top 3 Ways to Maximize the Value of Threat Intelligence within Security Operations

1) Enhance Prevention and Detection: Correlate data from your tools with threat intelligence for more accurate alerting, blocking and threat quarantining

2) Improve Response Time: The more knowledge you have about a particular threat, the faster you can respond to it

3) Inform Security Policy and Controls: Ensure that your organization has the right defenses in place

02

What does **Intelligence-Powered Security** Look Like?

It entails becoming able to focus your limited resources where they'll have the greatest impact on the business' top priorities. And it involves relying on knowledge and evidence to drive every decision you make and every action you take.

This isn't a small change. It requires midset shifts from stakeholders across the organization. It also demands new tools and operational processes. It's not the case that you can just buy a new threat intelligence platform (TIP) - or other solution - and expect it to magically alter your security program. Instead, you need to take a multifaceted approach to transformation.

Balancing people, processes and technologies is the key to successful organizational change. This is just as true when it comes to building an intelligence-powered security operations program.

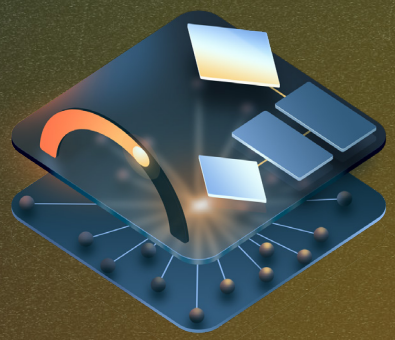
Infusing intelligence into every aspect of security operations means **going from a reactive to a proactive** approach to security.

The Intelligence-Powered Cyber Fusion Center

1) Build with operationalized cyber threat intelligence at the core and uses it to inform every aspect of security operations

2) Represents an evolutionary stage that comes after the traditional security operations center (SOC)

3) Enables highly collaborative and agile security operations across protection, detection, and response functions



Here's how people, processes and technologies interact in an **intelligence-powered** SecOps program.

Inputs

- Business risk appetite
- Business critical processes, and assets
- Regulatory concerns
- Cybersecurity maturity
- Threat intelligence
- Vulnerabilities
- Attack surface

Outputs

- Higher effectiveness through prioritizing the most critical threats
- Accelerate threat detection and response
- Optimize security operations spend
- More efficient, productive, and happier staff with less churn
- Increased internal and external collaboration, and information sharing

People

An organization needs to dedicate adequate resources to threat intelligence. This means making CTI into a core security operations function, just like threat monitoring, detection engineering, incident response and vulnerability management are.

CTI analysts should have a seat at the table. Their output should be made use of by all security teams, but it should also be given credence outside of security, including by DevOps and CloudOps teams as well as organizational leadership.

In fact, when it comes to organizational mindsets, intelligence-powered operations shares some key similarities with the DevOps philosophy. There's an overarching emphasis on collaborative relationships and breaking down barriers between traditionally siloed functions and departments within security. There's also an emphasis on shared learning and collaborative workflows.

Process

Security teams have long been struggling to keep up. There are too many threats to investigate, too many disconnected tools to maintain, too many assets, environments and third parties to monitor, and too many vulnerabilities to remediate. Intelligence-powered security operations teams work smarter and more effectively because they begin with the ends in mind.

Intelligence-powered operations starts with the identification of the most important risks to the business. This enables security leaders and practitioners to identify and prioritize the required outcomes. With this information in hand, they can then begin identifying all the use cases within SecOps where threat intelligence should play a major role. This allows an organization to properly define their priority intelligence requirements (PIRs) for their CTI function and sustain them over time.

Where Security Teams Must Go

Security leaders whose organizations leverage threat intelligence will be better positioned to mature their organizations away from reactive mode to being proactive. operationalizing threat intelligence allows security operations teams to anticipate and take action against potential threats before they are able to wreak havoc on the business. This allows ciso to demonstrate a high level of assurance to Business Leaders, customers, partners, and suppliers.

Threat intelligence analysts within an intelligence-powered secops program will not only be able to curate and disseminate the most relevant information, but also work to continuously operationalize threat intelligence and fuse it across all secops activities, leveraging a common data model, building a threat Library, threat scoring, and automating tasks and processes.

When **SOC analyst** make use of threat intelligence, they'll be able to triage alerts and events more quickly and accurately. They'll have access to relevant data on which threats are being observed in other organizations, as well as which poses the greatest risk to theirs.

In intelligence-powered security operations, **incident responders** will become more efficient by making use of automated tasks and playbooks that have high fidelity threat intelligence built right in. This enables them to operate more decisively and efficiently, with a better understanding of attackers tactics, techniques and procedures or which vulnerabilities are most likely to be exploited.

Threat hunters can not only rely on threat intelligence as a starting point for hypothesis- driven hunts, but also leverage their organization's threat library to discover which indicators of compromise (IoC) might serve as evidence of ongoing malicious activity that previously went undetected.

Technologies

Putting the right technologies in place is essential for becoming an intelligence-powered SecOps program, but such technologies can only be implemented successfully after the other aspects (people, processes) are in place.

In order to operationalize threat intelligence management successfully, a platform-driven approach is key. A central, integrated platform enables you to harness all the capabilities of a plethora of security tools and technologies in one place. This approach reduces the operational overhead necessary for maintaining the security architecture at the same time that it makes it quicker and easier to gain insights. This way, practitioners can focus on understanding context, making decisions and taking action, rather than monitoring and maintaining technologies.

Essential platform capabilities for operationalizing threat intelligence and fusing it across security operations activities:

- Common data model that's shared across the architecture
- Threat intelligence library
- Threat scoring that includes community-powered insights
- Automated tasks and playbooks
- Case management tools
- Unified workflows across the entire incident lifecycle

03

Putting Intelligence-Powered Security Operations **into Action**

We've talked about how Intelligence-Powered Security Operations can transform the ways in which security teams work, enabling them to become more effective — even with limited resources — by directing their efforts where they'll have the greatest impact on business risk. We've said that infusing intelligence across security operations requires the right resources, process and mindset shifts, and a technology platform that supports centralized intelligence management as well as automation and orchestration. And we've discussed the fact that this is a significant shift. But how do you put these principles into practice in the real world?

In this section, we'll take a deeper dive into three specific uses

We'll show how:

1) Establishing and sustaining a threat library

2) Triaging alerts

3) Prioritizing vulnerability management

Are different in intelligence-powered security programs.

1) The Role of the Threat Library

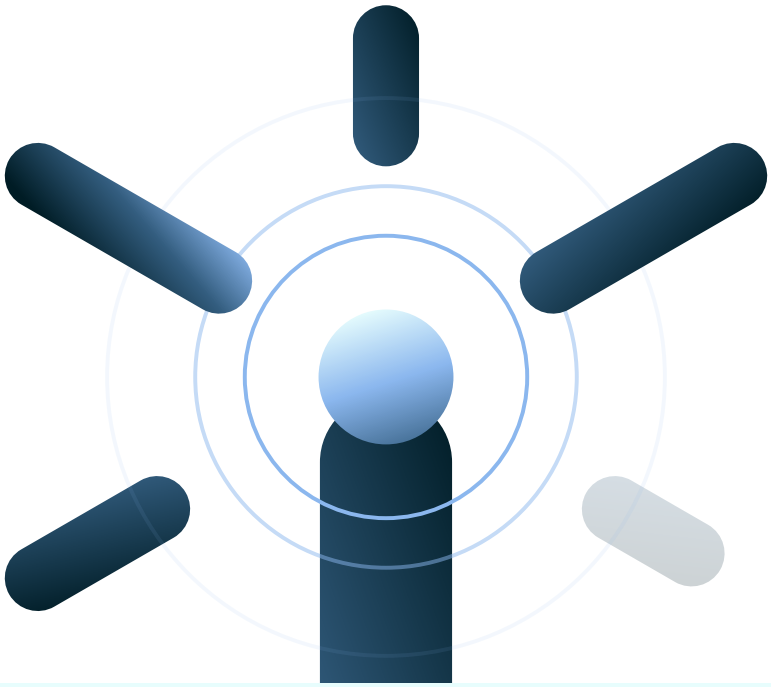
Attackers' tactics and techniques continue to grow in sophistication, often at a faster pace than defenders' tools are evolving. With a threat library, security teams have access to a canonical system of record documenting the threats that are most relevant to their individual organization. This provides a holistic view of the threat landscape in one place, supporting faster decision-making and more efficient operations.

Intelligence-powered security operations teams can leverage their threat library to better understand which threats are currently the most relevant. These insights can then inform defenders' strategies for identifying, detecting and responding to attacks. Using the ThreatConnect Platform as your Threat Intelligence Platform (TIP) will significantly reduce the amount of time it takes to build a threat library and use analytics, crowdsourced data and machine learning to identify the most pertinent information within it.

2) Automating Alert Triage for Faster Response

Today's security analysts are inundated with alerts. They receive thousands if not millions of them on a daily basis, and as many as 45% of alerts end up being false positives, slowing down workflows and making analysts less efficient. In desperation, many analysts simply ignore alerts: 35% of respondents to a recent IDC Research[8] survey say they have no choice but to ignore alerts when their queue gets too full.

When a security program fuses threat intelligence into its alert triage processes and workflows, analysts can quickly cross-check alert data with current sources of threat intelligence such as technical blogs as well as open source and premium intel feeds, giving them the most current and complete information it's possible to have. Plus, bi-directional integrations make it possible to share this information with your security information and event management (SIEM) system, influencing what triggers an alert in the first place, and ultimately bringing down false positive rates.



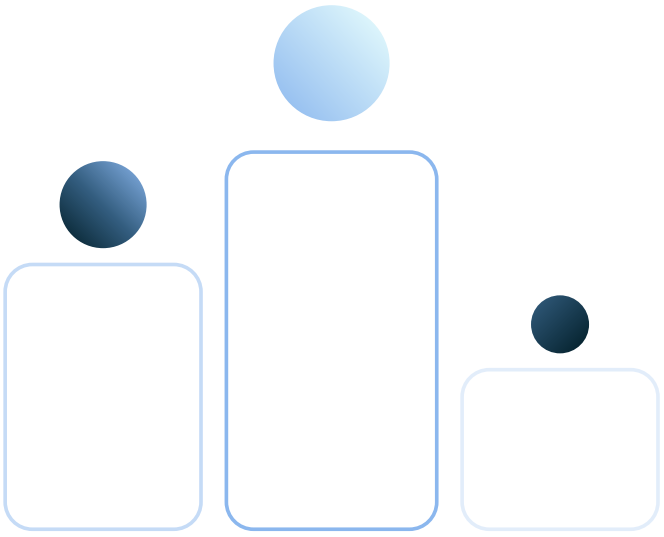
8 https://www.securitymagazine.com/articles/94614-three-quarters-of-security-analysts-suffer-from-fomi

3) Prioritizing Vulnerabilities

In the past, security teams have typically focused on remediating the vulnerabilities with the highest Common Vulnerabilities Scoring System (CVSS) severity scores first, but this is a problematic strategy for several reasons.

Security teams struggle to keep up with the volume and pace at which patches are being released by software vendors. **77% of security practitioners polled in a recent Ponemon Institute[9] survey said their organization simply lacked the resources to keep up with patching.** The rate at which vulnerabilities are being publicized is accelerating, with the total number of vulnerabilities having grown 36% year over year annually since 2015. The total number of vulnerabilities reported in 2020 was a whopping 183% higher than it had been in 2015. CVSS scores are often a poor match for which vulnerabilities attackers will ultimately exploit. These scores are based on how easily a particular vulnerability could be exploited and how much impact its exploitation would have, but they don't consider individual industry-specific risks, let alone unique business context. Given the large volumes of vulnerabilities with CVSS scores of 9 or 10 that they currently confront, it's critical for security teams to find better strategies for prioritization.

77% of security practitioners say their **organization lacks resources**



An intelligence-powered security program will leverage threat and vulnerability intelligence to determine which vulnerabilities are currently being exploited by attackers in the wild, which ones were recently widely exploited but have since gone out of fashion, and which cybercriminals are talking about targeting next. But security programs can also go a step further. They can leverage cyber risk quantification (CRQ), like ThreatConnect RQ, to rank vulnerabilities by the potential financial impact that their exploitation would have on the business. This enables vulnerability management teams to work smarter instead of harder, but it also demonstrates how their patching efforts are driving down overall business risk to the company — enabling clear communication to executive leadership, board members and other key stakeholders.

[9] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf

04 How **ThreatConnect** Can Help

ThreatConnect delivers a single platform that was purposefully designed to empower security teams to forge a path to better security by infusing threat intelligence into every aspect of their operations. The ThreatConnect Platform makes it easy to automate the collection and analysis of threat intelligence from a variety of sources and disseminate it through easy-to-understand dashboards and reports as well as seamless integrations with a broad array of today's most popular security tools and solutions.
To make it easier to operationalize threat intelligence, the ThreatConnect Platform leverages a robust threat data model that can be shared across your entire organization. This makes it possible to normalize threat data from a variety of sources, add context and readily infuse the resulting insights into your mission-critical activities and use cases.

The ThreatConnect Platform also makes building a threat library simple. With the platform, it's easy to aggregate, normalize and correlate threat intelligence, so that you can take incoming threat data in a variety of formats and levels of quality and translate it into something that's ready to disseminate and operationalize. This aids in centralizing knowledge management, and ultimately empowers security teams to build automated playbooks and workflows to act upon the platform's embedded wisdom.

In an intelligence-powered security operations program, every member of the team needs to be speaking the same language. The ThreatConnect Platform's standardized threat scoring system makes this possible, ensuring that everyone in your security program — and, indeed, across all ThreatConnect intelligence-sharing communities — applies a universal system for scoring threats and researchers' confidence levels. ThreatConnect also provides a single numeric scale for assessing the criticality of every IoC. The goal is to keep your entire security team on the same page when it comes to task prioritization and impact.

Plus, ThreatConnect's CAL™ - AI and ML-powered analytics[10] - provides a way to understand how many times particular threats were identified across thousands of participating Platform instances. This empowers security teams to leverage insights that have been distilled from billions of data points to understand how widespread and relevant a threat is from a global perspective.

[10] https://threatconnect.com/solutions/collective-analytics-layer/

Conclusion

Today's security leaders and analysts need a real-time control tower view of their operations and activities, outlined against the backdrop of the current threat landscape, to be able to understand whether they're working efficiently and effectively. This is exactly what infusing intelligence into security operations makes possible.

For too long, security teams have wasted effort, losing the battle to the attackers, because they spend their time firefighting threats, with too many disconnected tools, and without understanding how their time and expertise could be applied to proactively mitigate the most critical risks to the organization.

In Intelligence-Powered Security Operations, risk and threat intelligence is combined with human expertise and machine power to deliver better outcomes to the business as a whole. Ultimately, intelligence-powered security operations programs will deliver smarter security and better results.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 -or- **ThreatConnect.com/Request-a-Demo**

ThreatConnect.

ThreatConnect enables security operations and threat intelligence teams to work together for more efficient, effective, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse threat intelligence and cyber risk quantification into their work, allowing them to orchestrate and automate processes to respond faster and more confidently than ever before. Nearly 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their most critical systems.
Learn more at www.threatconnect.com.

ThreatConnect.com
3865 Wilson Blvd., Suite 550 Arlington, VA 22203
sales@threatconnect.com
+1 (800) 965.2708