ThreatConnect.

Whitepaper

How ThreatConnect Enables

Cyber Fusion Operations

Introduction

Cyber threat intelligence is essential to defending an organization from cyber attacks. Applying threat intelligence is a journey. Many organizations start by collecting internal data from their various security tools to understand attacker motives, targets, tactics, techniques, and procedures. Other organizations start with open source intelligence sources or by purchasing a commercial threat intel service. Whichever way an organization starts, it's important that a threat intelligence operations (TI Ops) team have an agreed destination when they start the journey, and a plan to get there.

As an organization matures their TI Ops, adding more data sources to get a more comprehensive view of their threat landscape, they all too often fall considerably short on operationalizing that threat intel to help them become more proactive and strengthen their defenses. Even when they master the process of intelligence gathering and management, too many organizations lack standardized, repeatable procedures to operationalize the data. They need a consistent, well-defined process to drive critical security decisions based on comprehensive intelligence gathering and institutional knowledge.

Unfortunately, many cybersecurity teams act unilaterally and are not collaborating with each other to impart and share knowledge. True operationalization of threat intelligence requires that TI Ops teams share information and infuse it into their cyber defense operations (vulnerability management, threat monitoring and detection), offensive security (penetration testing, red teaming) incident response, and threat hunting. Anything less increases risk for the organization. With that in mind, organizations should take concrete steps that enable security teams to be optimized for producing, consuming, and collaborating on threat intel.

Organizations should establish a cyber fusion operations model, what ThreatConnect calls Intelligence-Powered Security Operations.[1] This model centralizes Threat Intelligence Operations at the core of a cyber fusion operations "center" or organization, that is highly integrated into a wide-range of security operations teams and tools. And for the cyber fusion center to operate at its best, organizations should invest in a cybersecurity platform that promotes sharing of threat intelligence and collaboration by unifying and automating operations.

[1] Security leaders are still in the dark with asset visibility while a lack of insight is driving control failures

01 Separation Anxiety

Cybersecurity operations unfortunately have emulated a long-running pattern in IT operations. As new capabilities are added, new teams with specialized expertise come into existence. Those teams tend to focus on specific mandates, such as threat analysis or incident response, without much thought or coordination with other teams responsible for their own areas of cybersecurity.

The result is the creation and propagation of silos that act independently, keeping to themselves the threat intelligence they use in their decision making. The absence of consistency and collaboration inevitably causes operational inefficiencies as teams duplicate effort, perpetuate ineffective approaches, and fail to share best practices. Even worse, the insular approach to completing tasks enables conditions that weaken the security posture and widens the target for threat actors.

By one estimate[2], **ransomware attacks occur every 11 seconds,** contributing to an annual global cost of $20 billion.

The problem intensifies as organizations grow, undergo digital transformation, and expand their attack surfaces. Unless organizations enact cohesive growth management and security strategies, they suffer a side effect that often results from the addition of technology and expansion of IT environments – the propagation of technology and security silos.

The more silos a company has, and the wider its attack surface becomes, it creates more opportunities for threat actors to successfully exploit exposures and vulnerabilities. Attackers never relent from identifying new targets and refining their methods. For example, as organizations coped with pandemic-related restrictions by setting up work-from-home (WFH) environments, attackers saw that as a new opportunity. Ransomware attacks, including one that disrupted fuel distribution[3] along the Eastern seaboard in May 2021, have intensified as threat actors get bolder and demand higher ransoms.

With these kinds of threats looming over security teams, it has never been more critical to approach threat intelligence strategically by finding ways to operationalize it and maximize its impact across all of security operations.

[2] Ransomware Statistics in 2022: From Random Barrages to Targeted Hits
[3] Colonial Pipeline hack explained: Everything you need to know

Uncoordinated Efforts

Maximizing the impact of threat intelligence comes down to having well-defined and prioritized requirements, investing in dedicated cyber threat analysts, and having clear processes for analyzing, interpreting and acting on data insights. Standardized processes drive efficiencies and enable collaboration. However, achieving these benefits requires tackling cybersecurity's big data problem, which stems from collecting too much information from too many tools. Security operations teams have access to dozens of open source threat intelligence sources, and there are dozens of commercial ones too.

Why?

79% of security teams feel overwhelmed by alerts.

Organizations have an average of

76 security tools[4].

Without a centralized, single source of threat intelligence truth, the number of duplicate alerts and false positives generated creates a tremendous amount of noise leading to wasted efforts and a lack of focus on the most critical alerts that matter.

Those tools include:

- firewalls
- SIEM platforms
- endpoint protection
- and myriad other solutions that are generating alerts that need to be triaged and investigated.

[4] Security leaders are still in the dark with asset visibility while a lack of insight is driving control failures

As security teams attempt to make sense of all the data that finds its way to their dashboards, they have to contend with a number of challenges:

- An unclear picture of the risks faced by the organization due to data overload
- Inability to contextualize risk, making it difficult to communicate it to management
- Misalignment between security and business, which companies typically don't realize until they've been attacked
- Uncoordinated efforts by siloed teams charged with analyzing and interpreting threat intelligence from point tools
- Lack of a centralized threat intelligence and shared visibility, further inhibiting the ability to coordinate effort
- A flurry of alerts and false positives that keeps teams busy and ineffective – 79% of security teams[5] feel overwhelmed by alerts
- Manual, repetitive tasks that are time-consuming and prone to error

ThreatConnect helped a company who received 200 million SIEM events per month or, **50 million per week.** With ThreatConnect those events were narrowed down to **12 per month, or only 3-4 per week.**

Cybersecurity leaders need to embrace a new approach that modernizes security operations and adapts to digital business, changing attack surfaces, and a more hostile threat landscape.

[5] One-fifth of cybersecurity alerts are false positives

02 The Cyber Fusion Center

One of the most decisive, results-driven steps a company can take to improve its security posture is to set up a cyber fusion operations model where teams can work together to maximize the benefits of threat intelligence. A cyber fusion center, whether it's a physical location or a globally-deployed virtual team, enables collaboration between all security operations teams – as well as coordination with IT and business teams – integrated with TI Ops at its core. The center amplifies the duties and responsibilities traditionally associated with SOCs by enabling a more cohesive approach between teams and stakeholders.

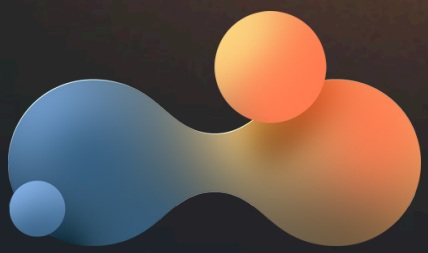
The fusion center concept originated in the intelligence sector. The U.S. Department of Homeland Security adopted it after the release of the 9/11 Commission Report[6] to foster communication and collaboration between various agencies, such as the FBI, CIA, and local police forces.

In the cybersecurity realm, the fusion center pulls together the various teams that handle tasks such as defense (vulnerability management, threat detection and analysis, threat hunting), offense (pen testing, red teaming), forensics and investigations, and incident response, to better coordinate effort and strengthen defenses.

What's Worked in the Past Won't Work for Cyber Fusion Operations

To support threat intelligence being at the core of cyber fusion operations, the approaches and tools have to change. First, just "managing" threat intelligence is not going to work. If threat intelligence is not centralized in a repository using a common data model, it can't be easily and efficiently disseminated and consumed across multiple teams and technologies.

The use of spreadsheets and legacy TIPs will not have the right features, capabilities, flexibility, and scalability required to operationalize threat intelligence to support a cyber fusion operations function.



[6] The 9/11 Commission Report

Operationalizing Threat Intelligence to Enable Cyber Fusion Operations

To enable cyber fusion operations and a fusion center, TI Ops teams need a platform that unifies and fuses threat intelligence across all people, processes, and security tools. Such a platform integrates intelligence with human expertise and machine power, making it fast and easy to aggregate, analyze, and disseminate threat intelligence.

This helps ease the burden on security teams, which are always busy, often overwhelmed and typically understaffed. A unifying TI Ops platform allows teams to work smarter, letting them focus on what they do best – identify and interpret high-fidelity, intelligence-powered insights to drive the right decisions, activities, and actions.

As previously noted, security teams use dozens of separate tools to help defend organizations against cyber threats. Each tool can generate logs and alerts, and provide context, but their effectiveness is seriously compromised when companies fail to integrate them to make them work more harmoniously. With the right platform in place, organizations can integrate all of their disconnected tools into a single solution that provides centralized threat intelligence, and automation and orchestration to maximize the cyber fusion center's efficiency.

30 minutes to 3 minutes

For a Fortune 50 customer, ThreatConnect enabled an average single alert resolution decrease from 30 minutes to 3 minutes - significantly reducing mean-time-to-respond (MTTR).

03

The ThreatConnect Platform

The ThreatConnect Platform integrates an organization's security tools into a single solution and helps operationalize threat intelligence - leveraging apps, workflow, orchestration, and automation, and a native analytics engine (CAL™) to not only automate threat intelligence aggregation and management, but also for the analysis and the ability to act on that intelligence.

With ThreatConnect

Organizations can leverage a variety of threat intelligence sources, prioritize cybersecurity decisions based on financial risk to the business, and leverage institutional knowledge.

In short, the platform:

1. Operationalizes the threat intelligence
2. Captures and applies analyst knowledge and tradecraft
3. Automates and orchestrates activities with machine power

The ThreatConnect Platform is the central repository for threat intelligence, knowledge, and insights gained by TI Ops and other fusion operation teams as they perform their tasks, making the information readily available to analysts and technologies. It delivers a unified view to security leaders and analysts, letting them work in tandem to process the information they need and make decisions to strengthen their organization's cyber defense through machine powered analytics, Threat Graph visualizations, dashboards, reports, and metrics to provide the right level of information, in the right form, to the right people, when they need it. By leveraging the ThreatConnect API and an extensive marketplace of integration applications, cybersecurity teams are able to connect previously isolated tools, drive efficiency and maintain consistency across cybersecurity operations. As such, the ThreatConnect Platform is ideal for managing cyber fusion operations.

For a Global 500 Aerospace and Defense Contractor, one Playbook saved them "over $1,500/day." This drove making Playbooks available for all supported business units across the Organization's threat intelligence base, directly enabling 60+ analysts to do their job more efficiently.

Next Steps

Interested in learning more about how ThreatConnect can help modernize your security operations into cyber fusion operations? Connect with us at **https://threatconnect.com/request-a-demo/** to discuss your goals for making cyber fusion operations a reality.

Contact us to learn more about how ThreatConnect can help you realize Intelligence-Powered Security Operations.

+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