THREATCONNECT®

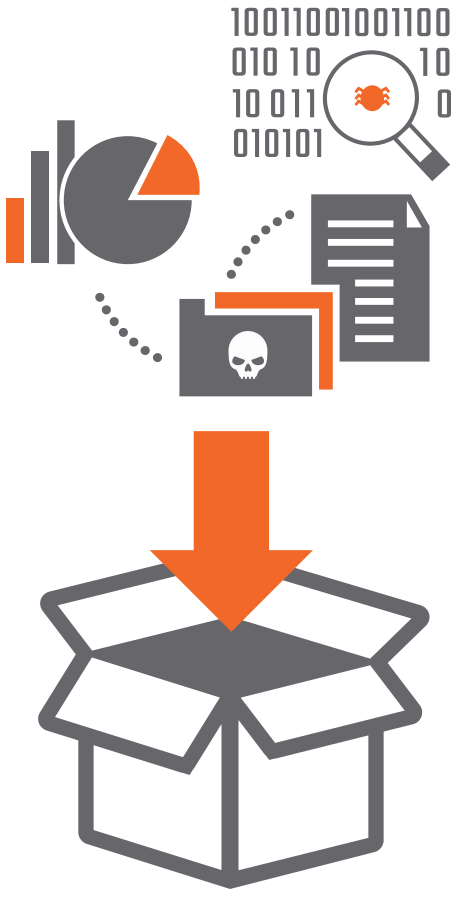
The Tao of Intel Driven Security

How to implement an intelligence-driven defense by uniting your threat intelligence and orchestration

The need to improve security teams' efficiency, integrate technologies, and speed up incident response has spurred the demand for orchestration and automation.

Intelligence-driven orchestration goes a step further -- it takes things like environment, situational awareness, and circumstances into account, empowering you to be proactive in mitigating threats to your organization.

This is a big deal for the security industry because automation or orchestration informed by threat intelligence enable any organization with a network security function to realize an **intelligence-driven defense**. And you're going to need it. If you are trying to operate your organization in the twenty-first century without awareness and preparedness against the digitally based threats to your business processes, relying on purely compliance-based security, then you stroll blindfolded and willfully ignorant into a minefield of unmeasured risk (pardon the drama).



So what is so great about an intelligence-driven defense? Honestly? There is nothing amazing about it; it's common sense. What's astonishing is that it is so sparsely adopted. In order to understand the concept better, let's break it down to its components.

Intelligence de-Hyped

First, let's talk once again about what threat intelligence (TI) should mean. The hype machine has put TI in a box; it's largely misunderstood as merely referring to indicator of compromise (IOC) feeds. These feeds have their place to support defensive operations, but they are far from a complete and accurate picture of what TI can be. Most IOC feeds are better characterized as information not intelligence. Conjuring the **DIKW Pyramid** (data, information, knowledge, and wisdom): intelligence is not raw data, it is not merely information, it is knowledge of threats you can use to inform decisions and possibly gives you the wisdom to predict future circumstances or events.

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708

Intelligence and Operations

Intelligence does not exist for its own sake, as stated above: it exists to inform decisions. Threat intelligence, therefore, specifically exists to inform decisions for security operations, tactics, and strategy.

This relationship is not one way. Intelligence and operations as functions of the security team should be cyclical and symbiotic. Intelligence informs decisions for operations and then actions are taken based on those decisions. Those actions (such as cleanups, further investigations, or other mitigations) will beget data and information in the form of artifacts such as lists of targeted or affected assets, identified malware, network based IOCs, newly observed attack patterns, etc. These artifacts can be refined into intelligence that can thus inform decisions for future operations. While many organizations do not have a formally defined intelligence function, the concept of using what you know about your threat-space to inform your operations exists in all organizations regardless of whether or not they employ threat intelligence analysts. The relationship between intelligence and operations is fundamental and exists in all security teams.

Intelligence

Intelligence informs decision making

- Correlation of incidents: IOC, TTPs
- Global pattern recognition
- Recommendations on COA

Operations

Operations beget knowledge of adversary

- Incident management and artifacts captured
- Threat investigations/research
- IOC observations/FP metrics

Implementing an Intelligence-Driven Defense

If there is so much value to be gained with implementing an intelligence-driven defense, why aren't more doing it? There are some significant challenges for organizations of all sizes to do it right. Fundamentally, these challenges are all rooted in fragmentation that inhibits clear access to relevant information by those who need to act. Organizations can implement an intelligence-driven defense by focusing on addressing the fragmentation problem across information, people, technology, and process.

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708

Information: In order for relevant information to be refined into usable intelligence, it must be available to be correlated, enriched, and contextualized. You must remove the silos segmenting the data by creating a common source of record for it. Aggregating internal and external information normalized to a common data model can refine it into intelligence usable for informing decisions. Internally sourced information, details of an IR investigation, notable events from the SOC, or even curated intelligence from an in-house team, are often the most valuable parts of the feedback loop enabled by aggregation.

People: Like data, the various functional teams within your security organization (IR, SOC, Intel, Risk, etc.) also need the silos taken down around them. They need access to relevant information from other teams, and intel sharing communities outside your organization. They also need to be able to work seamlessly together with a dynamic workflow. Allowing teams to provide tips and tasks to each other, create and funnel intelligence to relevant functional organizations, and create reports for executive decision makers based on threats to the organization, facilitates this.

Technology: Most organizations today have a very heterogeneous and disconnected set of point defensive technologies. Coordinating action across them for most means coordinating tickets between IT and various facets of the security teams. A good Threat Intelligence Platform (TIP) enables organizations to coordinate intelligence-driven action across a library of integrations.

Process: Once you have removed the silos between information, people, and technology, you can streamline your processes with Playbooks that leverage both internal and external intelligence to inform action for your teams and your technology, as well as learn from past experiences.

Many products perform Security Automation and Orchestration, but they rely on intelligence as simply a lever with little or no regard to its veracity, and certainly do not enable adaption for future runs of their Playbooks. Some Threat Intelligence Platforms allow for aggregation of external “intelligence” (often better characterized as information), creation of internal intelligence, and even have many connectors to defensive products.

A TIP that truly delivers an intelligence-driven defence focuses on getting the most value out of your threat intelligence by enabling cross team coordination and workflow around it, or the ability to orchestrate action between technologies with it.

Once you have one in place, you can start to make more informed decisions about your security operations and strategy.

About ThreatConnect®

ThreatConnect arms organizations with a powerful defense against cyber threats and the confidence to make strategic business decisions. Built on the industry’s only intelligence-driven, extensible security platform, ThreatConnect provides a suite of products designed to meet the threat intelligence aggregation, analysis and automation needs of security teams at any maturity level. More than 1,600 companies and agencies worldwide deploy the ThreatConnect platform to fully integrate their security technologies, teams, and processes with actionable threat intelligence resulting in reduced detection to response time and enhanced asset protection.

www.ThreatConnect.com

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708