ANOMALI

Managing Threat Intelligence Playbook

Your Guide to Evaluating, Selecting, Managing, and Ultimately Optimizing Your Threat Intelligence Management Platform

Index

Chapter 1. Introduction

What Is a Threat Intelligence Management Platform?

Threat actors are constantly evolving and advancing their attacks. Organizations seek to gain context on these attacks by leveraging threat intelligence, which is actionable information about adversaries and their Tactics, Techniques, and Procedures (TTPs). A Threat Intelligence Management Platform, also known as a Threat Intelligence Platform (TIP), is a solution that helps orchestrate and automate intelligence workflows by aggregating, processing, and disseminating raw and finished intelligence to help reduce time to detection, and enable analysts to investigate and respond to cyber threats in a consolidated environment that empowers collaboration with teams inside and outside of your enterprise.

Using Threat Intelligence to Improve Detection

A 2021 survey of IT professionals by SANS asked respondents about their use of cyber threat intelligence for detection.

- **85%** of respondents to the SANS survey say ***they produce or consume cyber threat intelligence***, but only **44%** of them ***have resources dedicated to focusing on it.***
- Only **28%** of respondents to the SANS survey have a ***dedicated threat intelligence platform.***
- **50%** of respondents to the SANS survey said ***lack of funding*** inhibited their organization from implementing CTI effectively.

Source: 2021 SANS Cyber Threat Intelligence (CTI) Survey

Chapter 1. Introduction

Why Do You Need Threat Intelligence?

Threat Intelligence Platforms (TIPs) are designed to take advantage of numerous sources of threat data that vary in format and focus. Security teams select threat feeds and determine which are best suited to inform them of threats relevant to their organization.

Typical Customer Challenges Include:

- ***Continuous Attack Triage***—Security teams spend too much time "activating" global threat intelligence in a way that is useful that allows them to detect the occurrence of a new threat in their environment based on global indicators.
- ***Threat Hunting Prioritization***—Organizations struggle collaborating across security silos and prioritizing threat hunting activities.
- ***Security Control Tuning***—Customers require the ability to update their security controls and monitoring tools constantly and automatically with relevant global threat intelligence.
- ***Reliant on Manual Processes*** —Inability to streamline data collection and cyber threat research to identify relevant threats.
- ***Streamline Investigations***—Unable to operationalize and correlate unstructured data into the investigations process.

> **Anomali has been one of the only platforms we've seen that allows us to tag our own intelligence, apply confidence ratings, and collaborate with other intel sources to get a better picture of the attacker infrastructures, etc. at play in cyber attacks.**
>
> *Cyber Security Specialist | Transportation*

Chapter 1. Introduction

Why Do You Need a Threat Intelligence Management Platform?

- ***Aggregation of intelligence from multiple sources for a quicker response***—Most security solutions focus only on information internal to their environment. A mature Threat Intelligence Platform consumes and correlates data from external and internal sources, providing threat intelligence analysts with more comprehensive insights into known or suspected threats to enable a quicker response.
- ***Automated curation, normalization, enrichment, and risk scoring of data***—The process of manually creating threat intelligence reports, bulletins, and profiles from individual indicators of compromise is burdensome and time-consuming. A Threat Intelligence Platform automates much of this process, so analysts spend less time assembling data and more time focused on providing high-fidelity intelligence in support of proactive defense.
- ***Integration with existing security systems***—Many security vendors seek to displace other systems. A TIP works in concert with existing solutions and makes them better, upgrading the output of all your security solutions.
- ***Analysis and sharing of threat intelligence***—The creation of threat intelligence is meaningless unless it's shared with other analysts. Securely sharing threat intelligence creates more comprehensive, reliable outputs that can be used to quickly respond.

Threat actors reuse many of their TTPs and strategies to target similar organizations and infrastructures. The more information and context around malicious actors you have, the quicker and easier it will be for your security team to prevent them from doing significant harm.

Chapter 1. Introduction

Where Can You Find Relevant Data Sources?

Threat Intelligence Management Platforms are designed to take advantage of numerous sources of threat data that vary in format and focus. Security teams select threat feeds and determine which are best suited to inform them of threats relevant to their organization.

- ***Third-Party Premium Feeds***—Security vendors sell feeds with specific focuses such as nation-state actors or deep and dark web. These feeds usually consist of more comprehensive and difficult to acquire information.
- ***Open-Source Feeds***—Open-source intelligence is free information that comes from security researchers, vendor blogs, and publicly available blacklists or whitelists.
- ***Threat Sharing Groups***—Threat sharing groups such as Information Sharing and Analysis Centers (ISACs) share industry-relevant threat data with vetted members.
- ***Open-Source Analysis Platforms***—MISP is an open-source Malware Information Sharing Platform. Although lacking in the full functionality of a Threat Intelligence Platform, MISP is ideal for those starting to gather, share, store, and correlate Indicators of Compromise (IOCs).
- ***Community Knowledge Bases***—One of the more popular knowledge bases for cybersecurity today is the MITRE ATTACK™ framework. It is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This framework is also used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

> **The quality of data and analysis received from Anomali has improved and educated our users. Thereby, allowing them to more accurately identify internal and external threats to our organizations, as well as increasing the time value of such investigations.**
>
> *IT Professional | Aerospace & Defence*

Chapter 2. What Challenges Do Threat Intelligence Management Platforms Address?

Automating Threat Data for Faster Insights

The number and sophistication of cybersecurity attacks increases every day. Organizations need to know exactly what threats they face so they can address them proactively and determine how to respond to incidents more effectively.

Analysts will look for evidence of an attack by examining alerts from various security solutions, typically a Security Information and Event Management (SIEM) system. However, because SIEMs were built to process and store all of an organization's data, many alerts that are generated are not real threats. These false positives, although not actually malicious, often waste valuable resources required to investigate the alert.

With an already limited staff, this can be crippling to the effectiveness of a security team. Threat intelligence helps analysts filter through these alerts and validate them by correlating curated threat intelligence with internal threat markers.

Threat intelligence itself can present several challenges. IOCs can number in the millions and the process of identifying which are relevant is labor intensive. Threat intelligence platforms are designed to automatically correlate inputs for significantly faster insights into cyber threats.

According to a report by (ISC)2, the number of unfilled cybersecurity positions now stands at **4.07 million.**

Source: Dataconomy

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Relevant Users of Threat Intelligence Management Platforms

Threat Intelligence Management Platforms are designed to automate manual processes to empower analysts and enable them to prioritize and focus their efforts. Raw data is transformed into finished intelligence that is easily understood, readily shareable, and most importantly—actionable. With intelligence, automation, and integration with existing security tools, organizations are able to understand threats that are relevant to them. The most frequent users of Threat Intelligence Management Platforms include:

- Threat Intelligence Analysts
- Security Operations Center (SOC) Analysts
- Cyber Threat Hunters
- Incident Response (IR) Analysts
- Chief Information Security Officers (CISOs)

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Data Aggregation and Curation

Threat Intelligence Management Platforms automatically collect threat data, information, and intelligence from numerous sources. Security analysts should have the flexibility of setting up customized imports of data while also being able to quickly ingest information from vendors or trusted third parties. This repository of intelligence is then funneled into investigations and other security tools.

Many of the inputs to a TIP may be duplicated, no longer malicious, or not enough of a threat to merit action. TIPs have machine learning algorithms to sort the information and weight the individual IOCs based on a multitude of factors that are relevant to cyber threats. Curated indicators are presented in an easy-to-read format with a risk score and associated intelligence.

> **Our ability to ingest information, enrich, and cluster based on relational tags and IOC types has greatly enhanced our threat intel side of our SOC. Once we layered on automation integration the gain was exponential.**
>
> *SOC Supervisor | Energies & Utilities*

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Investigation

Threat intelligence analysts are responsible for investigating threats and creating new threat intelligence to guide security strategy. This kind of analysis typically requires dozens of tools and countless hours.

A TIP enables analysts to conduct investigations through automated, scalable workflows and collaborate with different teams. Analysts can manage known IOCs and pivot to investigate unknown threats. Within the same investigation, analysts can associate indicators with intelligence, produce relevant observables and threat bulletins, and identify threat actors and their TTPs.

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Automation

Threat Intelligence Platforms are designed to take advantage of the strengths of machine and human capabilities. Automation reduces human error, spares analysts from "alert fatigue," and gives security teams the time and information necessary to make advanced judgement calls on cyber threats.

Laborious or repetitive processes that involve massive amounts of data are fully automated. This includes removing duplicate data, consolidating different formats into easy-to-read information, enriching indicators with additional data, and integrating security solutions.

> **Anomali allows us to address the large amount of data generated from multiple intel resources and identify the threats that are relevant to our organization. We can now more quickly, import threat data, correlate the risk, and then export only the needed indicators to our SIEM for proactive threat management and mitigation.**
>
> *Intelligence Analyst | FinServ*

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Integration

Threat Intelligence Management Platforms act as a middleman between relevant threat data and your existing security solutions, eliminating the need to manually configure a connection. Indicators are sent to firewalls and intrusion detection systems for active blocking, correlated against information in SIEMs and endpoint solutions to prioritize alerts, and sent to orchestration platforms to improve workflows.

The flexibility of these integrations rapidly improves the ability of a security team to identify and counter threats. This holds true whether an organization's security stack is entirely cloud-based, on-premises, or any combination of the two.

Chapter 3. What's Required In a Threat Intelligence Management Platform?

Collaboration and Sharing

Organizations are better able to anticipate attacker strategies, identify malicious actions, and block attacks with detailed and contextualized threat intelligence. Security teams can advance their defenses by collaborating with other teams to create this intelligence and protect the community through sharing.

TIPs facilitate collaboration on investigations and enable instantaneous, bi-directional sharing of intelligence. Sharing groups such as Information Sharing and Analysis Centers (ISACs) will commonly leverage threat intelligence platforms to align companies in similar industry verticals and help organizations to benefit from diverse resources and expertise.

> **Anomali automation has allowed us to research and share malicious actor information with industry partners quickly and securely. In addition, intelligence we receive from trusted organizations is automatically populated into our tools for alerting.**
>
> *IT Professional | Energy & Utilities*

48% of organizations interact with or are members of an ISAC.

Participation in ISACs and other government sharing programs and the perceived value they provide has increased year over year.

Source: 2021 SANS Cyber Threat Intelligence (CTI) Survey

Chapter 4. How Global Threat Intelligence Fits Into Cyber Resilience

Establishing a strong security posture is an iterative process. However, it can be overwhelming to try to improve everything that goes into the security lifecycle, such as planning, monitoring, detection, analysis, response, remediation, and feedback. Threat intelligence supports each of these phases by providing context to help guide those actions so they are faster and more targeted.

Planning

Security teams must plan for every possibility. They assess what threats their organization is most likely to face based on what product or service they produce, their geolocation, their political affiliations, and more. Threat intelligence enables these teams to prove or disprove their theories. Analysts gain more visibility into what threats are relevant to them and how those threat actors operate. Beyond analysis of this data, information, and intelligence, TIPs enable analysts to select and utilize what tools will be most effective for prevention and mitigation.

Monitoring and Detection

There are a few different ways to detect and monitor for malicious behavior, but incorporating threat intelligence is the only way to proactively defend against these threats. Pulling in external, verified context on threat actors and their TTPs eliminates

the need for security analysts to do the previous research to determine what is and isn't malicious. Organizations can quickly identify whether those malicious indicators are present by correlating threat intelligence with data from their existing security systems. Anything identified as suspicious can be automatically sent to integration points for monitoring. This empowers tools and personnel to block threats ***before*** they enter the network.

Chapter 4. How Global Threat Intelligence Fits Into Cyber Resilience

Investigation and Analysis

Once malicious entities are uncovered, analysts conduct investigations to determine impact to their organizations. TIPs provide a workbench for analysts to examine evidence where they can link different pieces of information. Analysts pivot from individual IOCs to look up WHOis information, PassiveDNS, and more to uncover previously unknown threats.

Response and Remediation

During an incident, a TIP helps analysts identify patterns and associated threat actors to inform remediation and response efforts more quickly. For example, a TIP can inform an analyst that a particular actor is known to use a specific tool or tactic, powering a more targeted incident investigation.

> **Anomali allows us automation of indicator ingesting, thereby giving the analyst more time to investigate and contextualize incidents with additional data provided in Anomali.**
>
> *Intelligence Analyst | FinServ*

Chapter 4. How Global Threat Intelligence Fits Into Cyber Resilience

Feedback

The feedback phase is critical for improving on your current security. Threat Intelligence Platforms are useful for assessing where to improve because they sit in between tools and information.

Key areas to consider are:

- ***The monitoring phase***—to determine which sources of information are most helpful for identifying and blocking threats.
- ***The detection and analysis phase***—to document how long it took to reach a conclusion.
- ***The response and remediation phase***—to determine whether the right information was possessed and how long it took to react. For example, if a malicious actor successfully infects a system, a TIP user can see whether information about that threat was already available in the repository or, if not, what other source contains that information.

Chapter 5. The Anomali Solution Suite

Managing Threat Intelligence with Anomali

Anomali integrates the world's largest intelligence repository with an organization's security telemetry to deliver extended detection and response capabilities to quickly uncover covert activity to stop attackers and help prevent breaches.

The following three components are part of the The Anomali Solution Suite.

- **ThreatStream®** is a Threat Intelligence Management Solution that automates the collection and processing of raw data and transforms it into actionable threat intelligence for security teams.
- **Anomali Match™** is an intelligence-driven extended detection and response XDR solution that helps organizations quickly identify and respond to threats in real-time by automatically correlating ***all*** security telemetry against active threat intelligence to expose unknown and known threats.
- **Anomali Lens™** is a powerful browser extension that helps operationalize threat intelligence by automatically scanning web-based content to identify relevant threats and streamline the lifecycle of researching and reporting on them.

Anomali Benefits

- Identify targeted threats to your organization
- Automate detection and analysis of threats
- Improve response with insights into threat actors and behaviors
- Save time and resources by reducing the impact of attacks
- Allow for collaboration between internal and external CTI groups

Chapter 6. Case Study

Bank of Hope Case Study

Bank of Hope needed a way to simplify the threat intelligence lifecycle process so it could make better use of its analysts' bandwidth to work deeper into the forensics and incident response process.

Challenge

Bank of Hope needed a way to easily investigate potentially risky IPs without having to log in to multiple security product dashboards. The bank depends on its security information and event management (SIEM) tool as the heart of its incident response program, but when the SIEM flagged a potential problem IP address the analysts needed to spend up to a half hour confirming its reputation.

Solution

ThreatStream offered Bank of Hope a way to sync its actionable intelligence with the organization's SIEM tool and provide analysis with minimal effort.

Key Benefits

- Powerful threat investigation toolset, enabling security analysts to rapidly evaluate and understand attacks.
- Reduced mean time to know to enable faster investigations.
- Integrated automations helped increase capacity without increasing overhead costs.

"The SIEM is a critical component of our environment and the heart of our program. It pulls in logs from a variety of different systems and correlates those indications to determine whether an activity is malicious or not," Bose says. **"Integrating ThreatStream in our SIEM portal means we don't have to go into five different systems but can look at the validity of an IP or executable from a single place. The solution has minimized much of the team's overhead."**

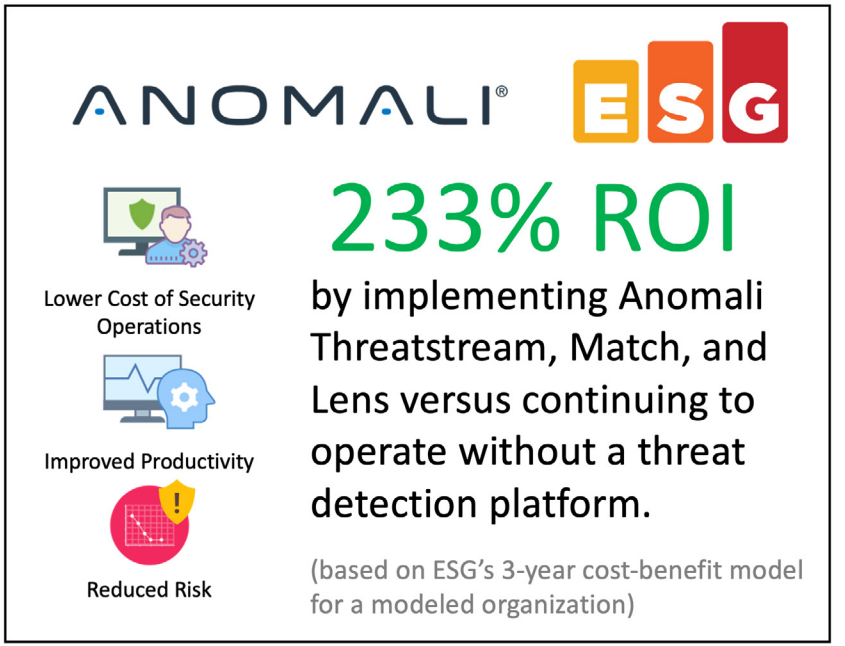
Arindam Bose, Senior Vice President & Security Officer for Bank of Hope

Chapter 7. Conclusion

ESG Executive Summary

Never before has it been so critical for enterprises to effectively empower an increasingly remote workforce with access to applications and resources across a number of geographic regions, networks, and devices. Enterprises have been forced to quickly implement solutions, ease restrictions and policies, and remove barriers to entry, placing an even greater burden on their security teams to operate effectively and efficiently to protect the organization and its assets. Security teams must work smarter and more efficiently to incorporate as much threat intelligence information as possible to identify and remediate threats.

ESG validated that Anomali's suite of intelligence-driven security products has helped to streamline security operations, automate workflows, reduce false positives, improve internal and external collaboration, and reduce time to detection and remediation. ESG validated the benefits that Anomali's customers had experienced through a series of interviews and used the information to create a modeled scenario that shows how an organization can save $93K per month through improved productivity, avoidance of risk, and value gained from included products. ESG's model predicts a return on investment of 233% and a payback period of only 11 months for an organization with a security team of 10 individuals choosing to implement Anomali versus continuing to operate without a threat intelligence platform.



Chapter 7. Conclusion

Cybercriminals, nation-state actors, and hacktivists are working overtime to target organizations for exploitation. Organization's need threat intelligence data and insights to fully understand their vulnerabilities to stay ahead of threats and respond to events quickly.

While gathering large amounts of data from internal security systems and external threat feeds is a start, manually pouring through all this data and investigating all these incidents can quickly overwhelm a security team already stretched thin due to a growing cybersecurity talent shortage.

An effective Threat Intelligence Management Platform provides the context needed to prevent and address threats more rapidly and effectively. By automating the process of collecting and analyzing internal and external threat data, information, and intelligence, security teams are able to view actionable threat intelligence quickly. Whether identifying relevant IOCs and preparing to address them, monitoring, detecting, and analyzing threats, responding to events, or looking to improve security operations, a Threat Intelligence Management Platform can help improve cyber resiliency.

> **Anomali is the equivalent of adding two full-time employees by reducing our false positive rate by 80%.**
>
> *IT Director | Health Care*

LEARN MORE

ANOMALI CYBER WATCH

FORRESTER THREAT INTEL TECH TIDE

REQUEST A DEMO

Website: www.anomali.com

Contact Us: **+1 844-4-THREATS** (847328)
+44 8000 148096 (International Toll Free)

Anomali is the leader in global intelligence-driven cybersecurity. Our customers rely on us to see and detect threats, stop breaches, and improve the productivity of security operations. Our solutions serve customers around the world in every major industry vertical, including many of the Global 1000. We are a SaaS company that offers native cloud, multi-cloud, on-premises, and hybrid technologies. As an early threat intelligence innovator, Anomali was founded in 2013 and is backed by leading venture firms including Google Ventures, IVP, General Catalyst, and several others. Learn more at www.anomali.com.

808 Winslow Street, Redwood City, CA 94063