ANOMALI®

Managing Threat Intelligence Playbook

Your Guide to Evaluating, Selecting, Managing and Ultimately Optimizing Your Threat Intelligence Platform (TIP)

Index

1 Introduction

2 What Challenges Do Threat Intelligence Platforms Address?

3 What to Look for in a Threat Intelligence Platform?

4 How Threat Management Fits into the Security Lifecycle

5 Anomali®

6 Case Studies

7 Conclusion

Chapter 1. Introduction

What Is a Threat Intelligence 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 platform (TIP) is a solution that automates much of the manual labor of threat intelligence research, reduces time to detection, and enables analysts to investigate and respond to cyber threats in a consolidated environment that empowers collaboration with teams throughout your enterprise.

Using Threat Intelligence to Improve Detection

A recent survey of IT professionals by the Ponemon Institute asked respondents about their use of threat intelligence for detection.

- 85% of respondents to the Ponemon survey say **threat intelligence is essential** to a strong security posture, but only 41% of them say they are **effective at detecting external threats**.
- Less than half or 48% of respondents to the Ponemon have a **dedicated threat intelligence platform**.
- Only 33% of respondents to the Ponemon said they **have adequate budget for threat detection**.

Source: The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies, Ponemon Institute, 2019

Chapter 1. Introduction

How a Threat Intelligence Platform Is Different Than Other Security Solutions:

- ***Aggregation of intelligence from multiple sources***—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 TI analysts with more comprehensive insights into known or suspected threats.
- ***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, upgrading the output of all of 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

Threat Data Sources at a Glance

Threat intelligence 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.

Typical Data Sources Include:

- ***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 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 organization, as well as increasing the time value of such investigations.
>
> ***IT Professional | Aerospace & Defense***

Chapter 2. What Challenges Do Threat Intelligence Platforms Address?

Automating Threat Data for Faster Insights

The number and sophistication of cyber security 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 a number of 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.

350,000 cybersecurity positions are currently open and the global shortfall of 3.5 million cybersecurity jobs is predicted by 2021

Source: Cyber Security Ventures

Chapter 3. What to Look for in a Threat Intelligence Platform?

Frequent Users of Threat Intelligence

Threat intelligence platforms are designed to give analysts back time that would otherwise be spent manually managing information. 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 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 to Look for in a Threat Intelligence Platform?

Data Aggregation and Curation

Threat intelligence 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 to Look for in a Threat Intelligence 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 to Look for in a Threat Intelligence 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 to Look for in a Threat Intelligence Platform?

Integration

TIPs act as a middleman between information 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 to Look for in a Threat Intelligence 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 Company***

While **59%** of respondents say their organizations share threat intelligence with others, **56%** cite possible misuse of their data as to why they are reluctant to share threat intelligence.

Source: The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies, Ponemon Institute, 2019

Chapter 4. How Threat Management Fits Into the Security Lifecycle

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 have to 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 or not 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 Threat Management Fits Into the Security Lifecycle

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 off of 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 more quickly inform remediation and response efforts. 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 Threat Management Fits Into the Security Lifecycle

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. Anomali®

Managing Threat Intelligence with Anomali

Anomali harnesses threat data, information, and intelligence to drive effective cyber security decisions. It is a platform that automates detection, prioritization, and analysis of the most serious threats to your organization. With machine learning, automation, and an expansive partner ecosystem, Anomali empowers your analysts to leverage threat intelligence for better insights and response to cyber attacks.

The following three components are part of the Anomali platform.

- **ThreatStream®** is the threat intelligence platform built for analysts to create threat intelligence and investigate security incidents. Collect, contextualize, and risk rank complex, high-volume indicators with machine learning to prioritize alerts and guide security strategy.
- **Anomali Match™** is a threat detection engine purpose-built to automate and speed time to detection in your environment. Anomali Match correlates twelve months of metadata against active threat intelligence to expose previously unknown threats to your organization.
- **Anomali Lens™** enables threat and security analysts to make faster and more accurate decisions. Anomali Lens provides instant access to strategic and tactical intelligence from any mobile or browser page. Analysts at all levels are empowered with real-time scores and context that accelerates decision making. Executives can easily access threat intel on their devices to stay informed about the latest threats to their business.

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

> Anomali has enabled us to march to the next level of security operations, in terms of keeping us updated on the cyber threat intelligence with all required attributes of it. Thus, enabling us to defend our organization against emerging threats.
>
> ***IT Manager | Computer Services Company***

Chapter 6. Case Studies

Colorado Threat Intelligence Sharing (CTIS) Case Study

In 2017, the State of Colorado formed the Colorado Threat Intelligence Sharing network (CTIS) in partnership with Anomali, connecting state, county, municipal, and tribal governments to enable security teams to share, analyze and better respond to threats.

Challenge

The State of Colorado struggled to create a secure portal for local communities to share vital cybersecurity information. The previous method of sharing information via email was insecure, uncollaborative, and not expedient enough for emergency situations. Without seamless, secure threat sharing, state departments lose critical information to prevent and contain cyber attacks.

Solution

The State of Colorado partnered with Anomali to provide a comprehensive threat sharing and analysis platform, allowing all state government departments to share confidential information in one central location. This portal provides greater visibility for local governments to instantaneously share data around potential threats within a trusted circle of fully vetted users.

Key Benefits

- Seamless and secure threat sharing, accessible to all local, tribal, county and state departments across Colorado.
- Ability to collaborate and share intelligence with other states via the Multi-State ISAC.
- Powerful threat investigation toolset, enabling security analysts to rapidly evaluate and understand attacks.

“We developed CTIS across the State of Colorado to address a critical need to drive broader cyber threat sharing,” said Trevor Timmons, Chief Information Officer for the State of Colorado. “We’ve seen rapid adoption at all levels of government within the state, with different departments and counties actively collaborating. We strongly encourage all states to implement cyber threat sharing programs to enhance their security posture.”

Get the Whitepaper »

Chapter 6. Case Studies

Federal System Integrator Case Study

This Federal Systems Integrator (FSI) is a proven provider of information solutions, engineering, and analytics for the US Intelligence Community, US Department of Defense and other federal agencies. With more than 40 years of experience, the FSI designs, develops and delivers high-impact, mission-critical services and solutions to overcome its customers' most complex problems.

Challenge

Working primarily as a systems integrator with clients in sensitive intelligence and security communities, this FSI's intellectual property (IP) contains critical high-value information. This IP, essential to the US government, must remain protected and secure.

Solution

This FSI turned to ThreatStream for an automated cyber threat intelligence solution. The ThreatStream™ platform counters adversaries by fusing actionable intelligence with existing security infrastructure.

Key Benefits

- Consolidating and curating multiple threat intelligence sources while eliminating redundancies
- Providing cross-validated analysis
- Rapidly operationalizing intelligence with high confidence

"Working with ThreatStream has helped us be much more effective at defending against the simplest threats all the way to the most advanced threats that attempt to compromise our company assets on a daily basis." Federal Systems Integrator CISO.

Read the Complete Case Study »

Chapter 6. Case Studies

UAE Banks Federation (ISAC) Case Study

The UAE Banks Federation (UBF) is a not-for-profit organization representing 50-member banks operating in the United Arab Emirates (UAE) and the leading industry association for the UAE banking sector.

Challenge

Cyber attacks are ever increasing in frequency and sophistication, presenting significant challenges for organizations and entire verticals which must protect their data and systems from capable adversaries. As cyber threat actors and groups share their tools, techniques, and procedures (TTPs) to attack and infiltrate organizations, those defending corporate networks and critical infrastructure must do the same by collaborating with peers in a trusted, secure, and effective manner.

Solution

The UBF Tasharuk initiative launched in September 2017, powered by Anomali flagship product, ThreatStream. The platform is used by the UAE Banks Federation membership to share relevant, timely, and actionable intelligence across regional financial institutions. A value-added component of the Anomali commitment to Information Sharing and Analysis Centers (ISACs) is the intelligence research team known as “Anomali — Threat Analysis Center (A-TAC)”.

Key Benefits

- Enhanced situational awareness of cyber threats to the UAE banking sector
- Centralized vetted community of practitioners focused on collective security objectives
- Improved security posture and resilience against cyber attacks for the entire vertical

“ With the launch of Tasharuk, we have been able to streamline anti-cybercrime efforts of participating banks and inform them about potential malicious threats in order to enhance their defense system.” HE Abdul Aziz Al Ghurair, Chairman of UAE Banks Federation.

Check Out the Blog »

Chapter 7. Conclusion

Cybercriminals, nation-state actors, and hacktivists are working overtime to target organizations for exploitation. Your organization benefits from understanding your vulnerabilities, staying ahead of threats and remediating events quickly.

But while your organization may have gathered large amounts of data from internal security systems and external threat feeds, manually pouring through all this data expends massive resources forced to sift through vast numbers of false positives and false negatives. Investigating all these incidents can quickly overwhelm a security team already stretched thin due to a growing cybersecurity talent shortage.

A TIP automates the process of bringing together and analyzing internal and external threat data, information, and intelligence in a way that provides actionable threat intelligence, speeding and simplifying the entire security lifecycle. Whether identifying relevant IOCs and preparing to address them, monitoring, detecting and analyzing threats, responding to events, or looking to improve security operations, a TIP provides the context needed to prevent and address threats more rapidly and effectively.

Anomali is the equivalent of adding two full-time employees by reducing our false positive rate by 80%.

IT Director | Health Care

Let Anomali help you achieve your threat intelligence and management goals.

LEARN MORE

ANOMALI WEEKLY THREAT BRIEFING

FREE STIX/TAXII: STAXX

REQUEST A DEMO

ANOMALI®

Website: www.anomali.com

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

Anomali® delivers intelligence-driven cybersecurity solutions. Organizations rely on the Anomali platform to harness threat data, information, and intelligence to make effective cybersecurity decisions that reduce risk and strengthen defenses. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The Anomali platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com and follow us on Twitter @Anomali.

808 Winslow Street, Redwood City, CA 94063