ANOMALI

GUIDE

Six Steps to Smarter Threat Intelligence and Proactive Defense

Six Steps to Smarter Threat Intelligence and Proactive Defense

Security teams are drowning in alerts, many of them meaningless. A March 2023 study of 1,000 SOC team members commissioned by IBM and completed by Morning Consult[1] revealed some startling statistics, including:

- The majority of the alerts that respondents reviewed daily were low-priority or false positives.
- Participants reported spending almost a third of each typical workday investigating/validating incidents that were not actual threats.
- The volume of unnecessary work prevented study respondents from processing 50% of the alerts they were tasked with reviewing on a typical workday.

It doesn't take a statistician to ascertain that, given these numbers, attackers who breach a network have a one-in-two chance of slipping under the radar. Yikes!

It doesn't have to be this way, and the good news is that solutions are available.

[1] "Global Security Operations Center Study Results," Morning Consult/IBM, March 2023.

1. Smarter Threat Intelligence: Enhancing Intel with AI/ML

Artificial intelligence (AI) and machine learning (ML) are addressing the threat intelligence platform (TIP) information overload and helping analysts identify the alerts that truly matter. This new generation of "smarter" threat intelligence provides insights, automates time-consuming tasks, and helps security teams make more informed decisions faster.

Key Features of AI/ ML-Enhanced Threat Intelligence

1. **Threat confidence analysis:** AI-powered systems can assess the reliability and relevance of threat indicators with unprecedented accuracy. By analyzing vast amounts of data and identifying patterns, these systems predict emerging threats, helping analysts prioritize their efforts more effectively.
2. **Automated false-positive detection:** One of the most significant advantages of AI/ML in threat intelligence is its ability to flag false positives automatically. This capability saves analysts substantial time and resources, allowing them to focus on genuine threats rather than chasing down misleading alerts.

3. **Dynamic severity analysis:** Advanced AI algorithms can evaluate the potential impact of threats in real time, considering factors such as the affected assets, the current security posture, and the broader threat landscape. This dynamic severity analysis enables more informed and timely decision-making.
4. **Intelligent threat summarization:** AI-driven platforms can generate high-quality threat bulletins and finished intelligence products automatically. These summaries distill complex threat data into clear, actionable insights that can be easily shared with stakeholders across the organization and beyond.
5. **MITRE ATT&CK® framework mapping:** Cutting-edge threat intelligence platforms leverage AI to automatically map threat data to the MITRE ATT&CK framework. This provides a standardized view of adversary tactics and techniques, enhancing threat modeling and defensive strategies.
6. **Advanced threat scoring:** AI/ML algorithms can perform sophisticated threat scoring, accounting for multiple factors, such as relevance, freshness, and source reliability. This nuanced scoring system helps prioritize threats more accurately than traditional methods.
7. **Intelligent deduplication:** Smart deduplication powered by AI ensures that analysts aren't overwhelmed by redundant information. By identifying and consolidating duplicate threat data, these systems present a cleaner, more manageable intelligence feed.

Participants reported spending almost a third of each typical workday **investigating/ validating incidents that were not actual threats.**

The Impact of Smarter Threat Intelligence

The integration of AI and ML into threat intelligence platforms is revolutionizing cybersecurity operations:

- **Enhanced efficiency:** By automating time-consuming tasks like false-positive detection and threat summarization, AI allows security teams to operate more efficiently.
- **Improved accuracy:** ML models can process and analyze data at a scale and speed impossible for humans, leading to more accurate threat assessments.
- **Contextual understanding:** Advanced AI can provide richer context around threats, helping organizations understand not just what is happening, but why, and what it means for their specific environment.
- **Rapid operationalization of threat data:** Enriched threat data translates into faster action — enabling you to immediately enhance your existing security controls.
- **Proactive defense:** AI-driven systems can identify emerging threats and attack patterns before they become widespread, enabling proactive, rather than reactive, security measures.
- **Continuous learning:** ML models continuously improve as they process more data, ensuring that the TIP becomes more effective over time.

2. Aggregating and Enriching Threat Intelligence

The first step in building a comprehensive view of the security landscape is to create a central repository for curated threat intelligence and ingest it from a wide array of sources, including open-source intelligence (OSINT), commercial feeds, government agencies, industry information sharing and analysis centers (ISACs), and high-quality proprietary research. Because this intelligence will come in various data formats (structured, unstructured, and semi-structured), effective analysis and correlation requires normalization to convert it to a common format.

Augmenting insights with data enrichment

Raw threat data often lacks the context necessary for informed decision-making. Advanced TIPs use AI to analyze multiple sources of intelligence and enrich it with additional context, including:

- Attacker profiles and information about their campaigns
- Adversary tactics, techniques, and procedures (TTPs)
- Integration with vulnerability assessment data for risk prioritization
- Malware signatures
- MITRE ATT&CK mapping to add depth and meaning to raw indicators
- ML-based scoring and prioritization based on factors like relevance, credibility, and potential impact.

By providing this rich context, curated feeds enable security teams to focus less on false-positive alerts and spend more time on the alerts that really matter.

3. Delivering Global Visibility without Delay

To reduce the inordinate amount of time analysts spend researching false positives and non-threats, it's essential to invest in high-quality threat intelligence. The place to start is with curated feeds.

The Importance of Curation

Feed curation is the process of collecting, organizing, and enriching threat data from various sources to provide security teams with relevant, reliable information. The goal is to transform raw data into actionable intelligence, enabling analysts to make informed decisions quickly and effectively.

Diverse Source Integration

Best-in-class TIPs serve as centralized libraries of threat intelligence, offering a wide array of base feeds out of the box. These include OSINT feeds, research from dedicated threat analysis teams, and feeds from reliable third-party vendors.

The true power of a TIP lies in its flexibility, providing:

- **Customizable intelligence**: Organizations can integrate feeds specific to their industry, geographic location, or unique threat landscape.
- **Extensible libraries**: TIPs often feature marketplaces or trial feeds, allowing security teams to evaluate and incorporate new sources of intelligence easily.

This flexibility ensures that organizations can select intel feeds directly relevant to their industries and exclude those that don't.

Intelligent Filtering and Prioritization

The hallmark of effective feed curation is the ability to separate the signal from the noise. Leading TIPs employ advanced algorithms and ML techniques to filter and prioritize threat data. This intelligent processing dramatically reduces the time spent on false positives and low-priority alerts, so security teams can focus on what's truly important.

The benefits of properly curated threat feeds go beyond efficiency to fundamentally transform how organizations approach threat intelligence:

- **Accelerated triage and response:** Pre-filtered, contextually rich intelligence significantly speeds up the process of triaging alerts and responding to incidents.
- **Improved risk prioritization:** Integration with vulnerability assessment data allows security teams to focus on relevant vulnerabilities actively being exploited in the wild.
- **Enhanced collective defense:** Some TIPs facilitate information sharing among organizations. This collective approach amplifies the value of curated feeds, creating a network effect that strengthens the overall security posture of entire industries.

Transparent Sourcing

In the world of threat intelligence, the credibility of information is paramount. Well-curated feeds provide clear visibility into threat data origins. Whether the intelligence comes from trusted industry circles, commercial feed providers, or individual researchers, knowing the source allows security teams to assess the reliability and relevance of the information quickly.

4. Collaboration and Sharing

Cyber threats are evolving in complexity, often striking multiple organizations across sectors. Enhanced defensive capabilities stem from collaboration and intelligence sharing among trusted entities. For example, when one financial institution sounds the alarm after an attack, the entire community benefits.

How Leading TIPs Enable Collaboration

Despite the advantages of information sharing, establishing secure and effective collaboration channels remains a challenge. The organizations involved may be market competitors who might be reluctant to collaborate in other settings or situations.

To facilitate sharing, a TIP provider must enable private, secure communities of industry peers or supply chain partners with shared interests who want to work together to strengthen their collective cybersecurity posture. For example, grocery chains in California, such as Safeway, Sprouts, Whole Foods, and Grocery Outlet, share threat intel, even though they are separate companies.

In other cases, one parent or umbrella organization (these may be private/corporate or government) shares essential threat intelligence data with a select set of companies “downstream.” This is a one-way sharing model, meaning that the downstream participants do not exchange data with each other. One example is the Walt Disney Corporation, which shares threat intelligence with its child companies, including ESPN, ABC, FX, and Hulu. Another example is the State of California, which shares intel with agencies, local cities, and charities funded by the state.

A Neutral Ground to Cultivate Trust

ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. Typically nonprofit organizations, ISACs reach deep into their sectors, collecting, analyzing, and disseminating actionable threat information and best practices to their members, promoting situational awareness. ISACs may also provide members with tools to mitigate risks and enhance resiliency.

The following are some examples of U.S.-based ISACs:

- Aviation (A-ISAC)
- Communications ISAC (NCC)
- Defense Industrial Base (National Defense ISAC)
- Emergency Services (EMR-ISAC)
- Electricity (E-ISAC)
- Energy Analytic Security Exchange (EASE)
- Elections Infrastructure (EI-ISAC)

5. Flexible Orchestration and Unified Security Operations

Threat intelligence is only as valuable as an organization’s ability to use it effectively. While collecting and analyzing threat data is crucial, the real challenge lies in applying this intelligence across an organization’s security infrastructure. Best-in-class TIPs offer robust integration capabilities that transform raw intelligence into actionable insights, enhancing the entire security workflow.

The Power of Integration

Integration features in modern TIPs serve as a critical bridge between threat intelligence and an organization’s security tools. These capabilities allow you to:

- **Infuse intelligence into incidents and alerts:** By automatically enriching security events with relevant threat data, integration tools provide context that helps analysts quickly understand and respond to potential threats.

- **Operationalize threat intelligence:** Integration allows you to put your threat intelligence to work, enabling real-time automated blocking and monitoring based on the latest threat data.
- **Customize data feeds:** Advanced integration tools allow you to tailor threat feeds for various security tools within your infrastructure, ensuring each system receives relevant and actionable intelligence.
- **Centralize intelligence distribution:** Acting as a broker between the TIP and other security tools, integration features ensure consistent and timely dissemination of threat intelligence across your entire security stack.

Benefits of Seamless Integration

- **Faster response times:** Automatically enriching alerts with threat intelligence enables analysts to quickly prioritize and respond to the most critical threats.
- **Improved accuracy:** Integration reduces false positives by providing additional context to security events.
- **Proactive defense:** Automated blocking based on the latest threat intelligence helps prevent attacks before they can impact your systems.
- **Efficient resource utilization:** By automating the distribution and application of threat intelligence, your security team can focus on high-value analysis and response activities.
- **Comprehensive visibility:** Integration ensures that threat intelligence is consistently applied across all security tools, providing a unified view of your security posture.

Considerations for Effective Integration

When evaluating threat intelligence platforms, consider the following aspects of their integration capabilities:

- **Breadth of integrations:** Look for platforms that offer native integrations with a wide range of security tools, including SIEMs, firewalls, endpoint protection systems, and more.
- **Customization options:** The ability to customize intelligence feeds for different tools without additional charges can significantly enhance the value of your threat intelligence investment.
- **Automation capabilities:** Advanced automation features, such as automated blocking and monitoring based on threat intelligence, can greatly enhance your security team's efficiency.
- **Scalability:** Ensure the integration solution can handle your organization's volume of security data and grow with your needs.
- **Ease of use:** Look for intuitive interfaces and straightforward configuration options to minimize the learning curve for your team.

6. Threat Models

Threat modeling is a process for projecting the probable nature of a threat, including the attacker profile, likely attack vectors, and probable target assets. This systematic exercise helps security teams prepare in advance by directing their attention to vulnerabilities in their network ecosystems so they can proactively shore up defenses.

Without realizing it, most people go through an analogous process of threat modeling in their daily lives. An example might be after hearing about burglaries in your area, you might research how the intruder entered the burgled homes and what they stole. Then you'd think through the similar ingress points and high-value assets in your own home, so you could take appropriate measures to protect yourself from a similar attack.

Threat modeling with a TIP is comparable, involving some variation of the following steps:

- **Organize threat intelligence:** Categorize and organize threat data from various sources, making it easier to search, filter, and analyze.
- **Contextualize threat information:** Link different threat models together to provide context and insights into the relationships between various threats.
- **Support investigations:** Help analysts investigate security incidents by providing a framework for understanding the attacker's motives, methods, and potential targets.

Components of a Threat Model

Regardless of the framework an organization may adopt, threat models typically include the following information:

- **Actors:** Threat actors, groups, or individuals involved in malicious activities. It includes information like their aliases, motivations, targets, and associated TTPs.
- **Campaigns:** Coordinated cyberattacks or campaigns with a specific objective. This includes information like the campaign's name, timeframe, targeted sectors, and associated threat actors.
- **Incidents:** Specific security incidents or breaches. This includes details about the incident, affected systems, attack vectors, and related threat actors or campaigns.
- **Malware:** This includes the different types of malware, such as viruses, worms, trojans, and ransomware, as well as specific malware names, hashes, functionality, and associated threat actors.
- **Vulnerabilities:** These are specific weaknesses attackers have targeted, such as outdated software versions, lack of encryption, misconfigurations, and more. Where possible, vulnerability lists include CVE numbers, affected systems, severity levels, and related exploits.
- **Attack Patterns:** Common attacker TTPs, including the attack pattern's name, description, and associated threat actors or campaigns.
- **Exploits:** This category includes the specific ways attackers have exploited a vulnerability. It may include exploit code, affected systems, and associated vulnerabilities.

Rising to the Challenges with Anomali ThreatStream

Anomali ThreatStream is a best-in-class TIP that effectively addresses the key challenges organizations face in operationalizing threat intelligence.

1. **Advanced ML:** Anomali goes beyond basic threat scoring, using advanced ML to analyze threat data, identify patterns, and predict emerging threats.
2. **Comprehensive threat intelligence enrichment and aggregation:** Anomali ThreatStream aggregates threat intelligence from a wide range of sources (internal, external, open source, and premium) and uses ML to enrich it with context and actionable insights, ensuring more precise threat detection and prioritization.
3. **Global threat visibility:** Anomali provides access to the largest curated repository of global threat data, pulling from multiple premium and OSINT threat intelligence feeds, providing industry-leading threat visibility.
4. **Enhanced collaboration and sharing:** ThreatStream's Trusted Circles feature enables secure sharing of threat intelligence and collaboration with trusted partners and communities, helping improve collective security. Organizations can define their own trusted networks to enhance threat awareness across industry sectors, geographies, or other criteria.
5. **Unified security operations:** Anomali ThreatStream integrates seamlessly with SIEM, SOAR, and XDR solutions, providing a centralized platform for managing and automating security operations. This unified approach offers a more holistic view of the threat landscape and streamlines security workflows.
6. **Flexible orchestration and threat intelligence dissemination:** Anomali Integrator automates and orchestrates the distribution of threat intelligence across various security tools and workflows, enhancing overall security effectiveness and operationalizing indicators of compromise and attacker TTPs.
7. **Threat models:** ThreatStream provides detailed detailed information regarding actors, attack patterns, campaigns, courses of action, identities, incidents, infrastructure, intrusion sets, malware, signatures, threat bulletins, tools, TTPs, and vulnerabilities.

Intelligent Threat Intelligence, Actionable Everywhere

Anomali ThreatStream doesn't just make threat intelligence actionable — it ensures it gets actioned by pushing it to endpoints, such as firewalls, SIEM systems, proxy, DNS, messaging systems, and endpoint protection platforms for blocking or other automated incident response. By providing curated access to extensive threat data, streamlining investigation processes, and enhancing overall cybersecurity posture, ThreatStream empowers organizations to stay ahead of emerging threats.

The Anomali advantage goes beyond addressing current challenges. With the integration of Anomali AI-Powered Copilot and Security Analytics, the platform leverages advanced AI to enhance threat detection, investigation, and remediation capabilities. The Anomali Security and IT Operations Platform allows organizations to analyze vast amounts of historical data with unprecedented speed and scale, identifying patterns that suggest potential threats even before they manifest as known attack signatures.

50%

The volume of unnecessary work prevented study respondents from processing 50% of the alerts they were tasked with reviewing on a typical workday

A powerful, flexible, and intelligent TIP is more important than ever. Anomali ThreatStream offers the comprehensive solution organizations need to navigate the complex world of cyber threats today and in the future.

Ready to discover how ThreatStream can transform your threat intelligence operations? Schedule a demo today and learn how Anomali can help your organization build a resilient and adaptable security strategy for the future.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI