Mandiant

OPTIMIZING THE SECURITY OPERATIONS CENTER USING INTELLIGENCE

Security Operations Centers (SOCs) are typically assigned with monitoring for, detecting, and investigating cyber threats. One of the most well-known challenges in this space is the overwhelming volume of alerts and events these teams must triage daily.

Read Time: 7-10 Min

Threat intelligence has long been sought to remedy this problem, helping teams prioritize alerts and events that may represent a higher severity of threat.

Sometimes overlooked as a key success factor is the application of strategic threat intelligence within the SOC. Analysts can gain a significant edge over the adversary when they have a wider view of the threat landscape and a deeper understanding of the TTPs being deployed against them.

These two concepts may sound simple, but there are few things to carefully consider when implementing this use case, which we will explore in this article.

Reduce Noise and Enhance Efficiency

The role of the SOC is to monitor for and investigate potential cyber threats. These are often represented as "alerts" or threat "events" produced by some detective or preventive technical security control.

Threat event criteria (rules), thresholds, and escalation conditions drive detection activities, and the volume of these events can be overwhelming for security operations centers (SOCs).

An optimized SOC team can leverage threat intelligence to manage, evaluate and prioritize their daily operations.

The SOC can also use threat intelligence to maintain a better understanding of the threat landscape and the TTPs adversaries are employing against them.

Objectives and Key Actions

Within the SOC, threats are detected based on security alerts and rules, and intelligence can be used to correlate known indicators of compromise with detected activity. Alerts and rules can then be prioritized accordingly.

Intelligence can also be used to enhance the understanding of attack targets, methods, and impact of potential security events. More strategically speaking, the organization's security monitoring strategy can be informed, supported, and enhanced by intelligence.

These principles ensure the right approaches are employed to identify and investigate the most critical threats, but we need specifics in order to implement them. Here are some common questions this use case helps answer:

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Where should we look for threats within our environment?
- What types of activity or behavior are we looking for?
- How will we prioritize or determine criticality of threats when they emerge?
- What types of intelligence do we need to anticipate emerging threats?
- What types or level of threat intelligence will we need when something is detected?

In order to answer these questions, consider the following activities.

Evaluate Current Alert Volume, Team Workflows, Log Sources, and Rules

As a first step, SOC teams need to understand their current state and perform a gap analysis to determine what specific alerts or related processes are not serving the organization's objectives. Understanding alert volume and the sources of alerts will help identify resource and visibility challenges. The workflows related to how alerts are queued and processed by analysts (and their actual current workload or level of effort) can uncover issues around efficiency and performance. Finally, understanding and comparing how current alerts are prioritized can help determine better integration points for intelligence.

Review Current Threat Intelligence or Threat Profile and Validate Tracking of Related Threat Data and TTPs

Discussed in a separate use case, perhaps the most important intelligence product for an organization is a cyber threat profile. The SOC should be a primary consumer of this product and become familiar with the top threats they face. Beyond a firm understanding of the threat landscape, the prioritization of security alerts can be driven or derived from the threat profile. The SOC should ensure threat data (for example, indicators of compromise) are being collected against the most current and significant threats. This will drive integration of intelligence in security monitoring technology, providing important context and correlation to observed threat activity.

High-confidence, validated indicators should be published and made available in a structured data format. An enterprise-grade data feed of this type can usually be deployed from a Threat Intelligence Platform (TIP) or equivalent solution. STIX version 2.1 is a commonly accepted standard, but the top consideration is that this data is structured so that it can be processed, stored, and transmitted efficiently across different technology types. The expected outcome is that monitoring technology is configured for near-real time detection and prevention of threats as they emerge.

Analyze a Comprehensive Set of Alert Rules and Apply a Prioritization Schema

The SOC should perform independent analysis to determine alerts and related rules that are most valuable, rather than only accepting vendor technology or detection tool defaults. Correlation of alert data with intelligence should be a key consideration to provide context to detection teams.

The following criteria could be considered when prioritizing security alerts based on intelligence and related indicators of compromise.

- Position of Observable in Kill Chain: Where in the kill chain is a specific indicator or observable found?
- Other Related IOCs Found: Have other linked IOCs have been detected?
- Indicator Value: IP addresses, file hashes, and domains all have different baseline values within detection activities (for example, a file hash is often more determinative than an IP address).
- Attribution: Is the alert related to an adversary known to be targeting the organization?
- Sophistication: Is the alert an indication of an APT group's activity, or otherwise linked to a known sophisticated adversary or TTP?
- Asset Criticality: Is the alert related to a business or mission critical application, asset (host), or data set?
- Criticality of Vulnerability Exploited: Is the alert linked to a known zero day or critical vulnerability?

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Threat Relevance: Is the alert related to activity observed and specific to the organization, industry, sector, or geography?
- Persona Impact: Will the alert indicate activity affecting or targeting an individual with heightened privilege, or access to critical or sensitive data.
- Transitivity: Will the alert be indicative of other related activity, observed in other parts of the kill chain that may indicate success or scope of an attack?
- Indicator Age: How long ago have we known about the indicator(s) related to the alert? When was the last time it was observed?

Test and Deploy Revised Alerts

Testing new alerts or rules in non-production environments is recommended when possible. This helps ensure they can be deployed without overloading resources, causing processing errors, or affecting the availability of existing technology.

After testing, teams can deploy new rulesets, but it may not be beneficial to act on new detections based on the alert rules. Teams should spend extra time when new alerts are deployed to monitor and validate rules are being triggered as expected.

Re-align Security Team Process and Workflows

Adoption of new detection rulesets by teams and their respective processes are the final step. When new alerts based on intelligence are configured, tested, and validated, monitoring and detection teams can begin to re-align their daily workflows or procedures to process new detections.

When security alerts and events are validated, providing background and linkages to intelligence are important to support more in-depth investigations. Analysts should use intelligence to prioritize initial analysis and investigation and escalate as appropriate. As alerts and events are escalated upwards in priority, more detailed intelligence is typically needed to make determinations and take additional actions to mitigate the threat.

When events are escalated to incidents, having good threat intelligence from the SOC investigation can help expedite an effective response effort.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.