FIREEYE™

SOLUTION BRIEF

Threat Intelligence Use Case Series

Security operations center (SOC) analysts

SOC ANALYST CHALLENGES

As the volume of alerts, alarms and events generated by security tools expands exponentially, SOC analysts struggle to understand which ones are most important, which are part of campaigns and advanced attacks, and which require immediate attention. They must grapple with the task of separating impactful threats from noise and determining where to focus limited incident response resources. Some of the most difficult challenges include:

- The near impossibility of combing through anywhere from tens of thousands to millions of alerts and alarms daily to determine the most significant threats.
- A scarcity of information to separate invalid, unreliable or irrelevant alerts and alarms from those posing a serious risk to the enterprise.

Tools to aggregate logs and correlate related alarms can reduce the number of alerts that must be evaluated, but SOC Level 1 analysts still remain highly overburdened.

How SOC level 1 analysts use cyber threat intelligence

Advanced security operations centers (SOCs) are employing cyber threat intelligence to prioritize and validate alerts and quickly determine which ones might represent real threats to the enterprise. By shrinking the problem and providing immediate access to threat context, cyber threat intelligence enables Level 1 analysts to make better, faster decisions about which alerts and alarms should be escalated to incident response (IR) teams for detailed analysis and action.

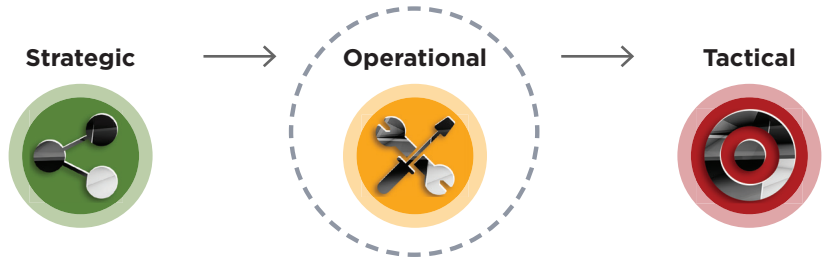

Table 1. Use Cases—SOC Level 1.

Use case	Key objective	Intelligence needed
Machine-based Prioritization	Automate the initial triage process by helping SIEM and analytics tools correctly prioritize the alerts and alarms presented to SOC analysts.	Machine readable threat data: threat indicators with severity ratings, and with tags linking them to attacks targeting specific industries, geographies, applications, etc.
Alert/Event Triage	Quickly determine which alerts and events should be investigated first	Threat indicators linked to summary threat data that provides context and situational awareness
Alert/Event Analysis and Validation	Validate events and decide which to escalate to the IR teams for in-depth remediation	Threat data that connects individual indicators with campaigns, threat actors, and techniques and other context.

Machine-based prioritization: Let technology do the heavy lifting

Among thousands (or millions) of alarms, alerts, and events, which ones really matter? Many of the alarms that SOC teams encounter are false positives: threats that won't impact the business, or that will be thwarted by existing defenses. By matching alarms and events with threat intelligence, SIEMs, log management and security analytics tools can perform first-cut alarm prioritization at machine speed. This relieves SOC Level 1 analysts from the labor-intensive task of sorting through tens of thousands of low-level and irrelevant alerts each day.

For example, SOC teams can create SIEM rules that match observable threat indicators found on the corporate network (e.g., domains and IP addresses, ports and protocols, file hashes or registry settings) with threat intelligence that connects those indicators with threat actors or campaigns that target the enterprise's industry, geographical areas of operation, software applications or infrastructure components. When matches are found, the SIEM will automatically increase the priority rating of that alert or event, ensuring that SOC teams have "eyes on" the threats relevant to their enterprise.

Event and alert triage: Accelerate human prioritization

Although machine-based prioritization can do much of the heavy lifting, SOC analysts are still faced with the laborious tasks of figuring out which alerts and alarms are actually dangerous. Cyber threat intelligence can speed up this process by providing SOC teams with summary threat data that provides context and "situational awareness."

This threat data can take the form of tags and summary descriptions that link individual indicators with threat actors and targets, or of longer narrative descriptions that place the indicators in the context of campaigns and multi-stage attacks.

For example, if malware is associated with an alarm, threat intelligence can tell the SOC analyst quickly if that malware has been linked to cyber crime or espionage activity. If an alert points to suspicious communication with an IP address on the Internet, linked threat intelligence can provide a fast answer as to whether that IP addresses is associated with actors known to be targeting the enterprise's industry or countries where it operates.

Analysis and validation: Assemble evidence and select the incidents to escalate

Threat intelligence can also help SOC Level 1 analysts further analyze threats and validate events. It enables them to answer questions such as: "Could this event be associated with a threat that poses a significant risk our business? Are these events isolated or part of a more complex targeted attack?"

Context associated with alerts can include lists of associated malware families, domains and IP addresses, and information about the behavior of malware samples, phishing attacks and other attack techniques. Intelligence maintained in a cyber threat knowledge base can provide additional detail and narrative, for example attribution of malware or phishing messages to a specific group or threat actor, analysis of the steps used in a multi-stage attacks and recommended options for mitigation.

These cyber intelligence resources can help SOC analysts quickly assemble evidence to determine if alerts and events should be characterized as incidents that pose serious threats to the organization and should be escalated to the incident response team for immediate in-depth investigation.

The bottom line

Today's SOC teams are inundated with raw data. Reliable, actionable, context-rich intelligence from FireEye can help your SOC Level 1 analysts:

- Shrink the problem of an overwhelming number of security alerts and events.
- Eliminate the inefficiencies of sorting through massive volumes of invalid and low-priority alerts.
- Rapidly identify alerts associated with relevant threats to the enterprise.
- Quickly assemble and assess evidence and make better decisions about which incidents to escalate.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™