FIREEYE™

SOLUTION BRIEF

Threat Intelligence Use Case Series

Incident responders

CHALLENGES FACING THE INCIDENT RESPONSE TEAM

Incident responders are frontline defenders against cyberattacks. They are responsible for investigating suspected compromises, identifying and reverse engineering advanced attacks, conducting forensics, and remediating damage. Incident response (IR) team members typically are experienced security analysts and could be a part of the security operations center (SOC) group as a Level 2 and/or 3 SOC analyst.

Challenges facing incident responders today include:

- Urgent requirements to validate which incidents represent real threats and to prioritize incidents based on the level of risk they pose.
- Difficulty connecting incidents to specific threat actors and campaigns.
- The need to perform laborious searches through databases and knowledge bases to find details about sophisticated attacks and the TTPs of threat actors.
- Trouble translating security issues to business language that executives can understand and act on.

In one survey, enterprises reported spending an average of $1.27 million annually responding to erroneous alerts.

How incident responders use cyber threat intelligence

Incident responders use cyber threat intelligence to improve the detection of serious threats, to quickly answer questions about the who, what, why, when and how of attacks, to speed up response and remediation, and to uncover evidence of advanced attacks that have dwelled unseen on the corporate network.

Table 1. Use Cases—IR Teams

Use case	Key objective	Intelligence needed
Incident Validation and Prioritization	• Determine which incidents are likely to pose a risk to the enterprise and prioritize those with the hightest potential for negative impact on the business	• Threat indicators linked to summary threat data
Incident Analysis	• Answerquestions about the who, what, why, when and how of attacks • Determine if attacks are still in progress and identify their effects	• Threat indicators with links to context about campaigns, threat actors and targets • An intelligence knowledge base with detailed information about attack histories and techniques
Containment and Remediation	• Disrupt attacker communications • Remove malware and reverse changes • Eliminate vulnerabilities	• Intelligence knowledge base with detailed information about attack histories and techniques
Hunt Missions	• Uncover previously undiscovered attacks related to current incidents or to threats targeting the enterprise's industry, geographical locations, applications, etc.	• Threat indicators with links to context about campaigns, threat actors and targets • An intelligence knowledge base with detailed information about attack histories and techniques

Incident validation and prioritization: Assess potential business impact

When SOC Level 1 analysts escalate incidents to the IR team, the incident responder must prioritize those incidents and decide which ones merit detailed investigations. Cyber threat intelligence can help them identify which incidents are most likely to be connected with attacks that target their organization, and assess which attacks have the highest potential for negative impacts on the business.

Cyber threat intelligence can speed up the process by providing threat data that links the indicators of the attack to context such as likely threat actors, their motivations (financial, competitive, and ideological), their targets, and the impact of their previous attacks. This summary threat data helps incident responders de-prioritize incidents that are targeting other types of enterprises (or consumers) and save scarce incident analysis resources for attacks that actually threaten important business processes or valuable information assets.

Incident analysis: Reverse engineer attacks

Incident responders need to pivot from initial incidents to determine if the attacks are still in progress, to pinpoint changes made to systems and applications, and to identify possible damage in terms of stolen data and disrupted operations. Cyber threat intelligence helps them answer questions (who, what, why, when and how) to develop a complete picture of attacks.

Cyber threat intelligence enables the IR team to connect alerts and indicators with related events and artifacts. For example, if a malware sample is detected, is there an IP address it is known to contact? Threat intelligence might show that malware indeed contacts an IP address that is used as a command and control server by a cybercriminal organization. Incident responders can then check network logs to find other corporate systems that have communicated with this server and are likely to be compromised.

If a repository of threat intelligence is maintained in a knowledge base, incident responders can use that knowledge base to find detailed information about the identities and techniques of attackers, their targets, their TTPs, and the impact they have on targeted enterprises. That information tells the IR team where to look for evidence about who is attacking, what they have done, how they did it, and whether the attack is still in progress.

Containment and remediation: Stop the bleeding and eliminate vulnerabilities

Incident responders need to supply information to other IT groups to help them contain attacks and remediate damage.

A threat intelligence knowledge base provides information on the motivation, techniques and infrastructure of threat actors associated with incidents. That can help block attacks in progress, for example by disrupting communications with external command and control servers and by disabling user credentials compromised by phishing attacks.

Information about how specific threat actors target systems and the behavior of the malware they use can help IT groups identify infected systems, remove malware, reverse changes to registries and files, and eliminate vulnerabilities to prevent attacks from recurring.

Hunt missions: Proactively uncover hidden attacks

Today most enterprises assume that some attacks will penetrate their protection and detection systems and dwell unnoticed on their network. Hunt missions are efforts to proactively uncover these attacks.

Reactive hunt missions use cyber threat intelligence to search for undiscovered attacks related to current incidents. For example, if a current incident involves a phishing campaign, threat intelligence might show that this campaign is used by a particular adversary that also employees other phishing campaigns and a type of "watering hole" attack. Since there is a strong probability that the group will use more than one type of attack, the hunt team can track down evidence of the other phishing campaigns and employees who have visited the adversary's watering hole website.

Proactive hunt missions start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Threat intelligence, particularly a comprehensive intelligence repository, gives the hunt team an accurate, detailed source of information on the actors most likely to threaten them, and about where to look for evidence of their presence in the corporate network.

How FireEye Threat Intelligence Helps Incident Responders

- Comprehensive intelligence available on the market Highly validated intelligence and associated indicators
  - Context rich intelligence about adversaries, campaigns, TTPs
  - Broad adversary coverage from crime to espionage and hacktivism
  - Globally sourced and analyzed
  - Eight-year historical database
- Robust API enabling integration with your tools and processes
- Partner integrations with key incident response tools
  - Analytics: Splunk, BAE, Palantir, Maltego
  - Endpoint: Tripwire and Ziften
  - TIPs: ThreatConnect, Anomali, ThreatQuotient
  - IR: Resilient Systems, and many others

The Bottom Line

Reliable, actionable, context-rich intelligence from FireEye can help your incident responders make fast, informed decisions in order to:

- Identify events that should be investigated immediately.
- Connect isolated indicators with threat actors and campaigns in order to quickly understand the source and targets of attacks.
- Perform in-depth investigations more accurately and completely and answer questions about the who, what, why, when and how of attacks.
- Block attacks in progress sooner, reducing their impact on the business.
- Prevent the same types of incidents from recurring in the future.
- Perform hunt missions to uncover attacks that are dwelling undetected on your network.

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™