FireEye
SECURITY REIMAGINED

FireEye Incident Investigation Solution

Moving from alerts to real-time answers

SOLUTIONS BRIEF

HIGHLIGHTS / BENEFITS

- **Comprehensive Context to Build an Effective Remediation Plan**
  With context built by covering the network to the endpoint, malware objects to full packets, and nodes both on-and-off premises, organizations can ensure that there aren't any blind spots when responding to an alert. For remote or smaller locations, organizations can apply FireEye Threat Intelligence to events and logs captured from the security infrastructure.

- **Integrated Workflow to Accelerate Time-to-Response**
  To accelerate response, organizations must fuse the workflow from detection through response. The solution technologies provide integration points with the FireEye Threat Prevention Platforms, the FireEye Central Management System, and 3rd-party SIEMs. These integrations ensure the rapid recognition of a targeted threat that is directly correlated to an initial alert.

- **Immediate Response to Limit Impact**
  Between the time an attack is detected, and before it is resolved, organizations are at risk of losing sensitive and confidential information and suffering infrastructural damage. The only way to limit the impact is to validate and quarantine targeted nodes. FireEye Threat Intelligence draws on a global threat intelligence ecosystem and incident response analysis to uniquely and quickly identify threat actors and IOCs allowing you to then instantly quarantine affected nodes.

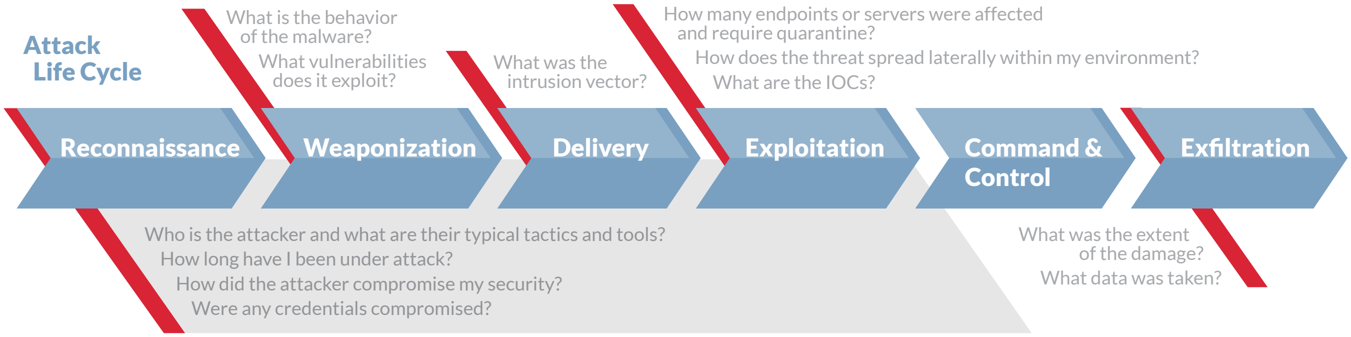
THE CHALLENGE

Organizations increasingly recognize that they must complement their perimeter defenses with strong analysis and incident response capabilities to investigate and remediate threats. As recent cyber security breach headlines reveal, the key to minimizing the impact of a security incident is not only quick detection, but also early and swift investigation.

A typical organization can take a month or more to respond to and remediate a breach*. This can dramatically disrupt day-to-day operations, extend sensitive data loss, negatively impact revenue and customer retention while exposing the organization to legal and regulatory action. Typical risks include:

- Ineffective Response Tactics – Organizations often take the approach of going from detection to remediation by "wiping" compromised systems. However, today's threat actors spread quickly and establish deep footholds into the organization before a typical cleanse. Without a well thought out and thorough remediation strategy, an attacker can maintain their presence within the organization.

INCIDENT INVESTIGATION SOLUTION: What you need to know to be effective



Attack Life Cycle

Reconnaissance

Weaponization

Delivery

Exploitation

Command & Control

Exfiltration

What is the behavior of the malware?
What vulnerabilities does it exploit?

What was the intrusion vector?

How many endpoints or servers were affected and require quarantine?
How does the threat spread laterally within my environment?
What are the IOCs?

Who is the attacker and what are their typical tactics and tools?
How long have I been under attack?
How did the attacker compromise my security?
Were any credentials compromised?

What was the extent of the damage?
What data was taken?

- Prolonged Attacker Access to Sensitive Assets—Without the ability to validate whether an alert has resulted in a successful breach, organizations cannot define a plan of action or determine whether one is necessary. This gives an attacker more time to cause damage.
- Damage to Organizational Reputation—Ineffective incident response raises questions about an organization's quality of management, trustworthiness, and competence. This negatively impacts customer, investor, employee, and media sentiment.
- Compliance and Legal Liability Exposure—Poorly managed security incidents can lead to legal action and noncompliance with regulations and industry standards. In addition, lack of visibility into causes and consequences of a breach can result in lawsuits and claims of negligence and sloppy practices.
- Disclosure and Risk Management- At the outset of a breach, organizations need to properly quantify the impact, while accurately disclosing the scope and scale of a breach. Failure to do so can result in tangible impacts such as fines, as well as intangible damage to organizational reputation.

Existing solutions are often slow and ineffective during high pressure incident response activities. They suffer from being disparate and disconnected from the detection and alerts while lacking a comprehensive view of the attack narrative. They also lack actionable threat intelligence to understand the identity, motivation, and objectives of the attacker, critical information to inform any response.

THE SOLUTION

The FireEye Incident Investigation solution provides real-time answers to validate alerts, and includes information on the scale, scope and methodology of an attack. This information helps organizations respond quickly and effectively to minimize losses.

HOW IT WORKS

The FireEye Incident Investigation solution provides full visibility across the security infrastructure in real-time, and at scale. It includes context from FireEye's proprietary repository of threat intelligence that is based on the millions of network and endpoint based sensors, hundreds of IR engagements, and billions of security events analyzed daily.

- Endpoint Threat Prevention Platform (HX Series): Pivot seamlessly from an alert to rapidly investigate and validate whether on- and off-premise endpoints have been affected. If necessary contain the threat to just that endpoint while performing deep forensic analysis of the endpoint to understand impact and behavior of attacks, including lateral spread. By reducing detection and response latencies, defenders limit damages and quickly restore normal operations.
- Enterprise Forensics (PX and IA Series): After detection, build the broader context of an attack (who-what-where-how) and expedite effective incident response. Gather critical information along the way, such as: length of attack, extent of infrastructure damage, data loss, and whether lateral spread has occurred. This information that allows you to go back in time accelerates remediation and mitigates potential risks to enterprise assets, reputation, and customers.
- Malware Analysis (AX Series): Stay a step ahead of the attacker by safely executing and profiling malware in a virtual environment to simulate the attack lifecycle. Gain an understanding of the malware's network and endpoint behavior as well as the overall attack methodology.
- Threat Analytics Platform (TAP): Quickly search through billions of events within seconds, and correlate event logs with FireEye Threat Intelligence to discover the presence of a threat or previously identified indicators of compromise (IOCs) in other parts of the network.
- Threat Intelligence: Obtain context in-line with the detection and analysis components of this solution. This speeds triage and response by understanding the identity, motivation, and objectives of the attacker. Further, knowledge of a threat actor's tactics helps establish a proactive security posture to protect against future threats.

Visit the Incident Investigation solution page for more information.

* Source: FireEye M-Trends Report