FIREEYE THREAT INTELLIGENCE

UNMATCHED VIEW ACROSS ADVERSARIES, VICTIMS AND NETWORKS WORLDWIDE

OVERVIEW

Organizations continue to fight an asymmetric battle that they are ill-equipped to win. Attackers are sophisticated, well-funded, well-organized and use highly targeted techniques. Security teams routinely struggle to understand which cyber threats pose the greatest risk to them and how to prioritize those they do face.

Most organizations stake their security efficacy on legacy, signature-based tactical intelligence feeds that can't anticipate attacks or provide context to guide response. Instead these feeds increase alert volumes with false positives making it nearly impossible to detect attacks and providing a false sense of security. The right threat intelligence can help organizations improve detection and response capabilities while lowering the total cost of ownership.

FIREEYE ISIGHT THREAT INTELLIGENCE: CONTEXT RICH TO MITIGATE THREATS

FireEye iSIGHT® Threat Intelligence is a nation-grade offering that provides tactical, operational and strategic intelligence. It delivers knowledge about adversaries and their motivations, intentions, and methods to help organizations:

- Proactively assess and manage the risks that they face,
- Detect and prevent attacks,
- Build attack context for the alerts that they face.

FireEye Threat Intelligence is derived from three main areas:

- From deep within the attacker's development environment before attacks are even launched
- From first responders to the world's most advanced cyber threats
- From MVX-driven technology that identifies never-before seen attacks.

By providing comprehensive intelligence that is immediately actionable, organizations can better manage their risk and response to today's attacks.

HIGHLIGHTS

- Access comprehensive threat intelligence from the tracking of over 16,000 threat actors, decades of incident response cases and thousands of global deployments
- Gain visibility into the attack life cycle with pre- and post-attack threat intelligence
- Subscribe to over 100 reports each month that include strategic intelligence related to attacker motives
- Improve investigations and response plans with contextual intelligence that provides answers

FireEye® SECURITY REIMAGINED

FLEXIBLE SET OF THREAT INTELLIGENCE PRODUCTS TO MEET YOUR REQUIREMENTS

Depending on the requirements of your security program, FireEye delivers a flexible set of options to operationalize your intelligence:

Standalone Threat Intelligence:

FireEye iSIGHT threat intelligence can be integrated to existing infrastructure and tools. This intelligence is a nation-grade level offering that provides tactical, operational and strategic intelligence. It goes beyond the basic information that "data feeds" provide with forward looking and highly contextual information you need to build proactive defenses, prioritize alerts and resources as well as improve incident response.

Offered with various consumable intelligence streams and direct access to analysts and dedicated client support. Ways to consume standalone iSIGHT threat intelligence is through:

- Machine-to-machine format via the iSIGHT API
- Human readable format through the MySIGHT Portal
- iSIGHT Threat Media Highlights, a daily analysis of the top global security news stories.

Organizations can subscribe to over 100 intelligence reports each month which include deep strategic intelligence tied to attacker motivations, tactical and operational intelligence streams. These reports enable multiple levels within a security team to stay on top of important issues and ahead of the inbound questions driven by executive management.

Intelligence Integrated within FireEye Technology

Enhance your detection, investigation and response capabilities with threat intelligence subscriptions for your FireEye technology. This intelligence is offered as add-on subscriptions when purchasing FireEye detection and investigation products and comes in three variations.

Dynamic Threat Intelligence (DTI)

Unsurpassed detection with machine learning and analytics that codify attacker intent and TTPs through the FireEye Multi-Vector Virtual Execution (MVX) engine. DTI provides hourly updates to ensure that your organization is finding the most recent attacks FireEye has seen across its global network of customers.

Advanced Threat Intelligence (ATI)

When FireEye detects an attack ATI provides you with the context to prioritize resources and develop an appropriate response. Available intelligence includes who the associated threat actor is, what their likely motives are, industry and global views information about the malware and other indicators you can use to search for the attackers in your environment.

ATI+

Benefit from 24/7critical alert and detection efficacy monitoring by FireEye.

ATI+ also provides access to foundational dossiers, trends, news and analysis on advanced threat groups as well as profiles of targeted industries, including information about the types of data threat groups target.

How Our Threat Intelligence is Different

- Deep and broad visibility into the extended attack lifecycle and attacker's motives, tools and procedures. Early visibility and access to the latest and most sophisticated threats from hundreds of embedded analysts deep within the adversary's development ecosystem, decade-long visibility at the front lines of major cyber attack investigations, and a global network of eleven million threat detection nodes through codified understanding of the attacker intent.
- Flexible and scalable analysis engine to track an ever-evolving attacker. 125+ million node mathematical graph database that dynamically models the relationships between the tools and tactics cyber threat groups use, the operations they conduct, and their sponsors.
- Subject matter experts from diverse domains who rigorously track and analyze the financial and political dimensions of over 16,000 cyber threats worldwide

This breadth of visibility and understanding of the adversaries and their motivations, intentions, and methods is provided to organizations through the FireEye Threat Intelligence portfolio. With this type of threat intelligence security teams shrink the attack surface and move from a resource-intensive, alert-reactive security posture to a proactive one that addresses threats significantly more effectively and efficiently.

	DTI	ATI	ATI+	ISIGHT INTELLIGENCE
Stage of an attack where intelligence comes from	Attack	Attack	Attack	Pre-attack, attack, post-attack
Type of Intelligence	Tactical	Operational	Foundational Strategic	Contextual Intelligence and Analysis Tools
Detection from FireEye Appliances	✓			
Detection Profiles for FireEye appliances		✓		
FireEye Alert Correlation to Geolocations		✓		
Attribution of FireEye Alerts to Known Threat Actors		✓		
Alert Monitoring			✓	
System Health Monitoring			✓	
Threat Group Profiles			✓	✓
Industry Profiles			✓	
Malware Family Profiles			✓	
Media Highlights			✓	✓
Threat Indicators via API				✓
API & SDK for Integration into non-FireEye Tools				✓
iSIGHT Broswer Plug-in for scanning, querying & pivoting into iSIGHT intelligence				✓
Attribution of iSIGHT Threat Indicators to known threat actors				✓
Extended Coverage of Threat Actors				✓
Executive Intelligence				✓
Business System Vulnerability Tracking				✓
Critical Infrastructure Vulnerability Tracking				✓
Exploitation Tracking				✓
Context for Alerts Across the Existing IT Infrastructure				✓

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye