FireEye iSIGHT Threat Intelligence

Scalable Threat Intelligence for Added Context across The Organization

RESPONSE TO THE THREAT ENVIRONMENT

Organizations continue to fight an asymmetric battle on the cyber front. 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 discover.

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 that make it nearly impossible to detect attacks and provide a false sense of security. The right threat intelligence can help organizations improve detection and response capabilities and business efficiencies.

Rich context to mitigate threats

FireEye iSIGHT® Threat Intelligence is unique in the industry. It is developed by more than 150 FireEye security researchers and experts around the globe who apply decades of experience to deliver knowledge about adversaries and their motivations, intentions and methods. They help organizations:

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

Threat Intelligence is mainly derived from three areas:

- Deep within the attacker's development environment before attacks are even launched
- First responders to the world's most advanced cyber threats
- 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.

Flexible threat intelligence suite to meet your requirements

FireEye helps operationalize your intelligence with standalone iSIGHT Threat Intelligence and intelligence integrated with FireEye technology, which includes Dynamic Threat Intelligence (DTI) and Advanced Threat Intelligence (ATI).

HIGHLIGHTS

- Improve investigations and response plans with contextual intelligence that provides answers
- Gain visibility into the attack life cycle with pre- and post-attack threat intelligence
- Consume actionable threat intelligence tailored to your security mission

STANDALONE THREAT INTELLIGENCE

FireEye iSIGHT Threat Intelligence can be integrated with any FireEye security solution as well as with any of your existing infrastructure and tools. It is a comprehensive offering that provides tactical, operational and strategic intelligence. It goes beyond the basic information that data feeds provide and adds the forward-looking and highly contextual information you need to build proactive defenses, prioritize alerts and resources and improve incident response.

It includes various consumable intelligence streams as well as direct access to analysts and dedicated client support. Intelligence is available in:

- 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

Intelligence can be tailored to the role or function of the personnel using it, empowering both mature and growing security teams with critical context on the intents and activities of their attackers. FireEye iSIGHT Threat Intelligence subscriptions can be customized across these five functional use cases: tactical, operational, fusion, executive and vulnerability.

INTELLIGENCE INTEGRATED WITHIN FIREEYE TECHNOLOGY

Threat intelligence subscriptions for your FireEye technology can enhance your detection, investigation and response capabilities. Two intelligence variants are offered as add-on subscriptions for FireEye detection and investigation products: DTI and ATI.

Dynamic Threat Intelligence (DTI)

This intelligence facilitates unsurpassed detection with machine learning and analytics that codify attacker intent and tactics, techniques and procedures (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 the context required 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 that can be used to search for the attackers in your environment.

How FireEye threat intelligence is different

The FireEye iSIGHT Threat Intelligence portfolio provides extensive insight into adversaries and their motivations, intentions and methods:

- **Deep and broad visibility** into the extended attack lifecycle and attacker's motives, tools and procedures. Early visibility and access to information on 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 sixteen million virtual 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.

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.

TABLE 1. Visibility of Extended Kill Chain.

	DTI	ATI	iSIGHT Intelligence
Stage of an attack where intelligence comes from	Attack	Attack	Pre-attack, attack, post-attack
Type of intelligence	Tactical	Contextual	Broad, comprehensive intelligence and analysis tools
Detection from FireEye appliances	X		
Detection profiles for FireEye appliances		X	
FireEye alert correlation to geolocations and industry verticals		X	
Attribution of FireEye alerts to known threat actors		X	
Threat group profiles			X
Industry profiles			X
Malware family profiles			X
Media highlights			X
Threat indicators via API			X
API and SDK for integration into non-FireEye tools			X
iSIGHT browser plugin for scanning, querying and pivoting into iSIGHT intelligence			X
Attribution of iSIGHT Threat Indicators to known threat actors			X
Extended coverage of threat actors			X
Executive intelligence			X
Business system vulnerability tracking			X
Critical infrastructure vulnerability tracking			X
Exploitation tracking			X
Context for alerts across the existing IT infrastructure			X

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

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

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. 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 has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye