FireEye iSIGHT Threat Intelligence

Forward-looking threat intelligence with highly contextual analysis

BENEFITS

- Get actionable threat intelligence tailored to your security mission

- Protect your organization from all categories of threats, including cyber espionage, cyber crime and hacktivisim

- Gain insight into the extended cyber attack lifecycle by FireEye's unmatched view across adversaries, victims and networks worldwide

- Choose the level of threat intelligence integration and support best suited to your needs

Overview

FireEye iSIGHT Threat Intelligence subscriptions deliver comprehensive, actionable intelligence to help you proactively defend against new and emerging cyber threats and align your security program with corporate risk management goals. We tailor intelligence to your security mission and staff, giving both mature and growing security teams critical context on attacker intent and activity.

The FireEye iSIGHT Threat Intelligence Advantage

FireEye iSIGHT Threat Intelligence is unique in the industry. More than 150 FireEye security researchers and experts around the globe apply decades of experience to gathering forward-looking, high-fidelity, adversary-focused intelligence. With an unmatched view into adversaries, victims and networks worldwide, iSIGHT threat intelligence delivers visibility across the extended cyber attack lifecycle to all levels of your business.

"Knowledge about your enemies will help you win. Thus, treat threat intelligence with the respect it deserves and use it to protect your organization from all the relevant adversaries."

How to Collect, Refine, Utilize and Create Threat Intelligence
Gartner, October 2016

FireEye iSIGHT Threat Intelligence Subscriptions

iSIGHT Threat Intelligence subscriptions offerings are tailored to the needs of your organization.

Fusion Intelligence delivers comprehensive, situational awareness of the global threat landscape with insights into ongoing, past and predictive threat activity. It empowers your team with a deep understanding of past, present and future adversary activities, including trends and typical tools, tactics and procedures (TTPs). The subscription equips organizations with processes, defense scenarios, deep dives and industry analysis to enable a proactive security posture. It includes Operational Intelligence.

Fusion Intelligence is used by advanced security operations center (SOC) or incident response (IR) team members who proactively hunt for adversaries and want details about threat actors, their motives and TTPs.

Cyber Espionage Intelligence delivers deep intelligence analysis and insights into adversaries who target corporate and government entities for strategic advantage. This subscription provides profiles of emerging adversaries' policies, strategies, doctrines and operational arts.

Cyber Espionage Intelligence is used by advanced SOC or IR team members who proactively hunt for adversaries and want details and TTPs of threat actors with an espionage motivation.

Cyber Crime Intelligence delivers deep intelligence and technical analysis that enable improved responses to abuses of computer systems, cyber crime operations and the targeting of victims' money, goods or services. With this subscription, you'll gain a better understanding of credential theft operations, ransomware, distributed denial-of-service (DDoS) attacks, network compromises and malware, including point-of-sale (POS) and mobile malware.

Cyber Crime Intelligence is used by advanced SOC or IR team members who proactively hunt for adversaries and want details and TTPs of threat actors with a cyber crime motivation.

Operational Intelligence gives security analysts actionable context for alerts that enable them to prioritize and inform their responses. It provides access to the full FireEye library of malware intelligence reporting, as well as actor overviews and indicator reports.

Operational Intelligence is used by SOC or IR teams who want to understand which threats to focus on and when.

Executive Intelligence conveys organizational risks to decision makers who direct security investment and strategy. It includes intelligence analyses of industries, regions and threats to enterprise networks. It improves executive-level communication on security topics relevant to your enterprise.

Executive Intelligence is used by C-level executives, such as chief information security officers (CISOs), who want to understand the business risks associated with cyber threats.

Vulnerability Intelligence prioritizes patch management workflows based on active and evolving exploits of vulnerabilities in your critical business systems. This subscription helps you identify unaddressed vulnerabilities, prioritize patch cycles and increase patch effectiveness and more. Reports include all threat intelligence and vulnerabilities related to critical infrastructure.

Vulnerability Intelligence is used by IT professionals and vulnerability analysts who want to improve efficiency and focus their time on top priorities.
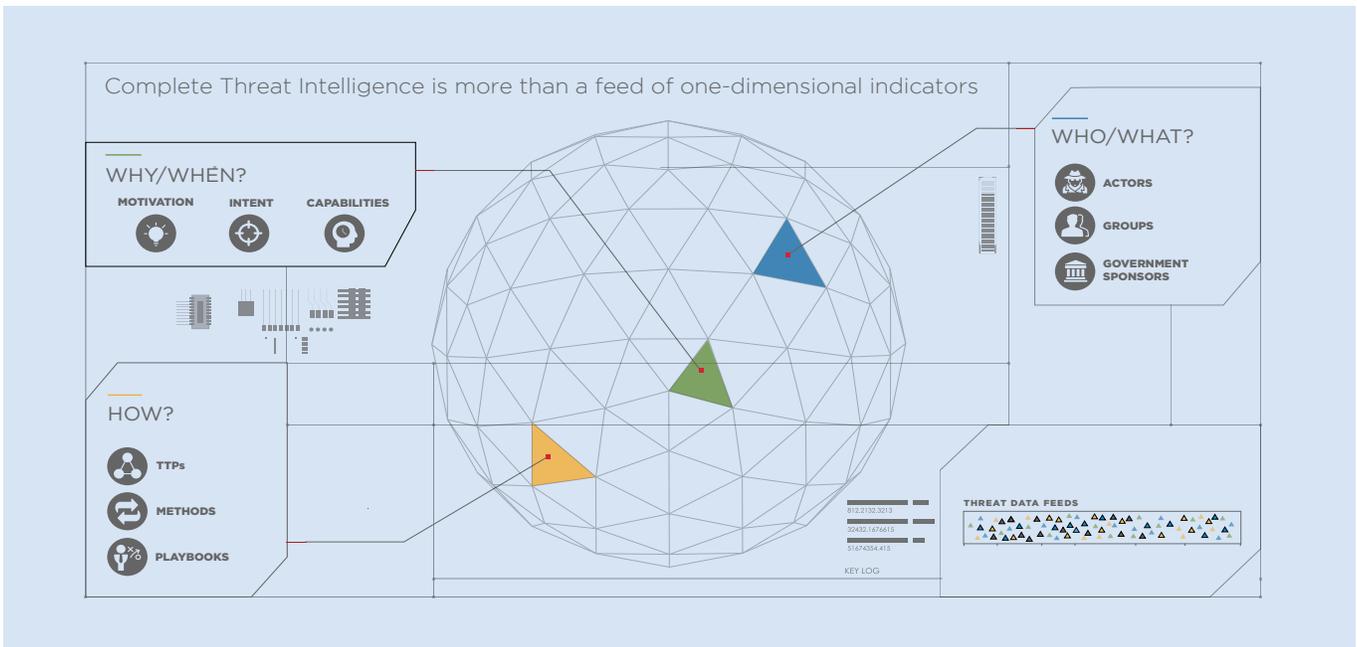
iSIGHT Threat Intelligence Delivery Mechanisms

Intelligence and reports from iSIGHT Threat Intelligence subscriptions can be accessed in many ways.

Email Alerts and Digests deliver designated resources via email, as configured through the iSIGHT Portal.	**Threat Media Highlights** delivers a daily email that tracks current security stories, answers inbound questions from business executives and includes proactive analyses of important events to your executives and board members. This email correlates highlights with iSIGHT Intelligence reports to give you a detailed understanding of the security landscape.	**iSIGHT API and SDK** enables you to use our intelligence with your security infrastructure and risk and compliance management technologies.
Intelligence Portal provides on-demand access to the complete online library of historical reporting for your specific subscription.		**Browser Plugin** scans webpages for technical indicators (IP, domain, hashes) and query the iSIGHT API for relevant iSIGHT intelligence.
Onboarding and Provisioning provisions users and API/browser plugin keys, as well as a formal annual business review.		**Analysis Tools** enable the receipt of contextual information on domain names, IP addresses and threats, and upload suspect files for analysis.

iSIGHT Threat Intelligence Enablement and Integration

Your analysts can tap into iSIGHT Intelligence to make inquiries, conduct extended research and perform detailed analyses. There are three levels of enablement:

Level 1: Onboarding and Provisioning equips you with the materials and engagement you need to use our intelligence solutions, including a self-service portal, customer support desk and API provisioning. It is included in the purchase price of all subscriptions.	**Level 2: Intelligence Coordination** provides you with a designated FireEye Intelligence Account Manager who serves as a concierge, guide and facilitator for your FireEye investment.	**Level 3: Intelligence Optimization** provides you with a designated Intelligence Account Manager and a Threat Analyst who help you integrate FireEye iSIGHT Threat Intelligence with you security operations. It includes three intelligence workshops per year.

Table 1. iSIGHT Threat Intelligence Enablement Levels			
Service Provided	**Level 1** Onboarding and Provisioning (Included with subscriptions)	**Level 2** Intelligence Coordination	**Level 3** Intelligence Optimization
Onboarding	Yes	Yes	Yes
Self Service Portal	Yes	Yes	Yes
Customer Support Desk	Yes	Yes	Yes
Collection of Threat Concerns			Yes
iSIGHT API Provisioning	Yes	Yes	Yes
Formal Business Reviews	Remote	Remote	Remote or onsite
Analyst Access Clarification		Yes	Yes
Analyst Access Original Requests		10 per quarter	25 per quarter
Priority Analyst Access Requests			2 per quarter
iSIGHT API Technical Integration		1 hours for 1 use case	4 hours for 2 use cases
General Threat Brief		Yes	Yes
Focused Threat Brief			Yes
Intelligence Workshops			3 per year

To learn more about FireEye, visit: **www.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 has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®