

FIREEYE ISIGHT THREAT INTELLIGENCE

SCALABLE THREAT INTELLIGENCE FOR ADDED CONTEXT
ACROSS THE ORGANIZATION

OVERVIEW

FireEye iSIGHT Threat Intelligence delivers comprehensive, actionable intelligence to help align your security program with corporate risk management goals and proactively defend against new and emerging cyber threats. 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. iSIGHT Threat Intelligence subscriptions can be customized across these five functional use cases: tactical, operational, fusion, executive and vulnerability.

The FireEye iSIGHT Threat Intelligence Advantage

FireEye iSIGHT Threat Intelligence is unique in the industry. More than 160 FireEye security researchers and experts around the globe apply decades of experience to gathering forward looking, high fidelity, adversary-focused intelligence. They have an unmatched view across adversaries, victims and networks worldwide to deliver visibility across an 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

Oct 2016, Gartner, Inc.

HIGHLIGHTS

- Consume actionable threat intelligence tailored to your security mission
- Broad, comprehensive threat intelligence across all categories of threats (cyber espionage, cyber crime, hacktivism, critical infrastructure and more)
- Delivers visibility over an extended cyber-attack life cycle based on an unmatched view across adversaries, victims, and networks worldwide
- Choose the level of threat intelligence integration and support your program is prepared for

FireEye iSIGHT Intelligence subscriptions

iSIGHT Intelligence subscriptions are offered for five distinct roles:

- **Tactical Intelligence** enhances your alerts and helps prioritize them with intelligence-driven indicators. It improves the overall efficiency of your tactical security requirements and team.

TARGETED FOR: TACTICAL, TECHNICAL USERS THAT WANT ALERTS ON ADVANCED, RELEVANT THREATS.

- **Operational Intelligence** provides actionable context such as malware and actor profiles alongside alerts and detected threats. It provides a prioritization filter that helps security teams focus on what matters most. Operational Intelligence includes both Tactical Intelligence and access to the Intel Portal which gives you online, on-demand access to all your historical intelligence reports.

TARGETED FOR: SECURITY OPERATIONS CENTER (SOC) OR INCIDENT RESPONSE (IR) TEAMS THAT WANT TO UNDERSTAND WHICH THREATS TO FOCUS ON AND WHEN.

- **Fusion Intelligence** delivers comprehensive, situational awareness through insights into ongoing, past and predictive threat activity tailored to your organization's cyber risk profile. It empowers your team with contextual understanding of past, present and future adversary activities, including trends and typical tools, tactics and procedures (TTPs). Fusion Intelligence equips organizations with processes, defense scenarios, deep dives and industry analysis to enable a proactive security posture. Operational Intelligence included.

TARGETED FOR: ADVANCED SOC OR IR TEAM MEMBERS THAT PROACTIVELY HUNT FOR ADVERSARIES AND WANT DETAILS ABOUT THREAT ACTORS, THEIR MOTIVES AND TTPS.

- **Executive Intelligence** conveys your organization's true risk profile to security and C-level staff to better inform security investment decisions, develop strategy and anticipate industry threats. Available as a standalone or add-on offering.

TARGETED FOR: EXECUTIVE USERS, CISOS AND ABOVE, THAT WANT TO UNDERSTAND THE BUSINESS RISKS ASSOCIATED WITH THE THREATS.

- **Vulnerability Intelligence** prioritizes patch management workflows based on active and evolving exploits of vulnerabilities in your critical business systems. Identify unaddressed vulnerabilities, prioritize patch cycles, increase patch effectiveness and more. Available as a standalone or add-on offering.

TARGETED FOR: INFORMATION TECHNOLOGY USERS AND VULNERABILITY ANALYSTS THAT WANT TO IMPROVE EFFICIENCIES AND FOCUS THEIR TIME ON TOP PRIORITIES.

FIREEYE ISIGHT INTELLIGENCE



Multiple ways to access your intelligence

- **Intel Portal** provides online, on-demand access to the complete library of historical reporting for your specific subscription (Note: Tactical users do not have portal access)
 - Email Alerts and Digests: intel portal can be configured to push new reports or digests via email alerts to your designated resources.
- **Threat Media Highlights** is a daily email that tracks current security stories, answers inbound questions from business executives and proactively sends analyses of important events to your executives and board members. The highlights are correlated with iSIGHT Intelligence reports to go beyond the headlines to deliver you a true, detailed understanding of the security landscape.
- **The Application Programming Interface (API) and Software Development Kit (SDK) for iSIGHT Threat Intelligence** lets you fuse our intelligence with your security infrastructure and risk and compliance management technologies. FireEye technology partners already use our API to build out-of-the-box integrations with their platforms.

INTELLIGENCE ENABLEMENT

Integration and support for your security program

Three levels of intelligence enablement make it possible for you to maximize your intelligence investment through analyst access (AA) for inquiries, extended research and detailed analysis.

- **Level 1: Self-Service** equips you with the materials and basic engagement needed to use our intelligence solutions.
- **Level 2: Intelligence Coordination** enhances the operational relationship between you and FireEye with a designated Intelligence Account Manager.
- **Level 3: Intelligence Optimization** integrates FireEye iSIGHT Threat Intelligence with your security operations via a designated Intelligence Account Manager and a Threat Analyst. It also includes three intelligence workshops per year.

ACTIVITY	INTELLIGENCE SUPPORT LEVEL		
	Level 1	Level 2	Level 3
Onboarding	✓	✓	✓
Self Service Portal	✓	✓	✓
Customer Support Desk	✓	✓	✓
Collection of Threat Concerns			✓
iSIGHT API Provisioning	✓	✓	✓
Analyst Access Clarification	✓	✓	✓
Formal Business Reviews	Remote	Remote	Remote and Onsite
Analyst Access Original Requests	1 (1 per Q)	✓ (10 per Q)	✓ (25 per Q)
Analyst Access Priority Requests			✓ (2 per Q)
iSIGHT API Technical Integration		<2hrs / 1 use case	<4hrs / 2 use cases
General Threat Brief		✓	✓
Focused Threat Brief			✓
Intelligence Workshops			✓

About FireEye

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.

Visit the FireEye iSIGHT Threat Intelligence [web page](#) or contact your sales representative for more information.

FireEye, Inc.

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

www.FireEye.com