SOLUTION BRIEF

FireEye

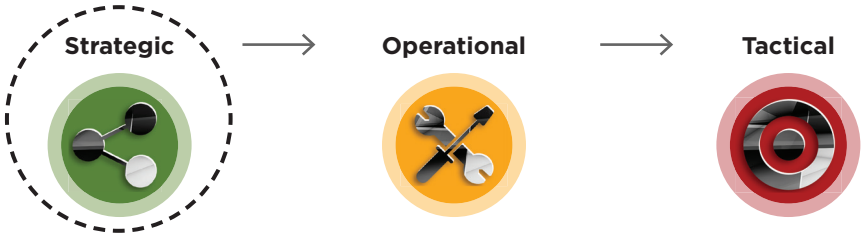
Threat Intelligence Use Case Series

CISO and senior IT executive

THE FOUR FACES OF THE CISO

- **Strategist:** Drive business and cyber risk strategy alignment, innovate and instigate transformational change to manage risk through valued investments
- **Advisor:** Integrate with the business to educate, advise, and influence activities with cyber risk implications
- **Guardian:** Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program
- **Technologist:** Assess and implement security technologies and standards to build organizational capabilities

Cyber threat intelligence for CISOs and senior IT executives
Chief Information Security Officers (CISOs) and senior IT executives make strategic decisions about cybersecurity. They need to allocate human and technical resources to where they can have the biggest impact reducing risks. That means they have to understand who is most likely to attack their enterprise and what assets those attackers will target. They also must be able to separate genuine threats from hype, and communicate with the CEO and board about how the IT organization is responding.



Challenges facing CISOs
The challenges facing today's CISOs and senior IT executives include:

- Judging competing budget requests to determine what investments in programs, staff and technology are strategic for reducing risk.
- Sifting through a continuous deluge of reports, analysis and hyperbole from media, analysts and vendors, in order to prioritize threats relevant to their specific enterprise.
- Communicating with top executives and board members to keep them appraised about threats to their enterprise and the IT organization's response to those threats.

About iSight partners

Since 2007, iSIGHT Partners has been recognized as the leader in cyber threat intelligence. Through its established intelligence team made up of over 300 different experts in 18 different countries, the iSIGHT Partners team focuses exclusively on analyzing and understanding the global threat ecosystem, to include threat sources and the methodologies they employ, and partners with its customers' security and intelligence operations to empower an intelligence-led security strategy that connects intelligence directly to their business.

Table 1. Use Cases – IR Teams

Use case	Key objective	Intelligence needed
Risk Prioritization	• Identify who is targeting the industry sector, geography and company • Determine the information assets most at risk and business impact of compromise	• Threat analysis customized for the industry or enterprise • Threat diagnostics identifying the threat sources, the assets they target, and how they exploit stolen assets
Risk Assessment of New Initiatives	• Determine risks to new markets, regions, industries and technologies	• Threat analysis of new markets, regions, industries and technologies • Custom queries with cyber security
Planning, Budgeting and Staffing	• Assess current security programs, technologies and staff against current and emerging threats	• Threat analysis customized for the industry of enterprise • Intelligence knowledge base of threat actors and their techniques • Custom queries with cybersecurity researchers
Executive Communications	Communicate with the CEO and board: • What headlines are relevant to us? • How do we respond to current incidents? • How well are we prepared to counter emerging threats?	• Assessments of media reports • Threat analysis • Custom queries with cybersecurity researchers

How CISOs & executives win with cyber threat intelligence
CISOs and other senior IT executives are using cyber threat intelligence to identify and prioritize risks to the business, to make better strategic decisions on plans, budgets and staffing, and to communicate with the CEO and board in business terms about operational and financial risks, threats and security preparedness.

How cyber threat intelligence helps

1. Risk Prioritization: Protect Against the Most Damaging Threats
Cyber threat intelligence helps CISOs and senior IT executives cut through the noise and focus on the threats most likely to have a major impact on their enterprise. Threat reports provide information on threat actors targeting specific industries, geographies and enterprise types, as well as on their tactics, techniques and procedures (TTPs). Threat diagnostics identify an organization's threat profile, highlighting the threat sources actively targeting their assets and associated tactical and strategic implications. This knowledge enables CISOs and senior executives to prioritize risks to a given enterprise and identify appropriate policies, process improvements, and technologies for managing them.

2. Risk Assessment of New Initiatives: Prepare Before you Leap
Entering (or exiting) new markets and regions or adopting new technologies involve unforeseen risks. Cyber threat intelligence prepares enterprises for new initiatives by pointing out unanticipated threats, such as the cybercriminals who are active in new markets, hacktivists (and sometimes governments) that target companies operating in certain regions, and attacks that exploit vulnerabilities in new applications and technologies. This type of information can be obtained from threat analysis of new markets, regions and technologies, and from customized queries and discussions with cybersecurity researchers.

3. Planning, Budgeting and Staffing: Spend and Hire Wisely

Cyber threat intelligence can give CISOs and senior IT executives a strategic picture of their "threat landscape." This includes a high-level view of the threat actors and threats they face, the information assets being targeted in similar enterprises, and available countermeasures. This information helps top managers assess their current security posture and make key decisions about investing in security programs, new technologies, and security staff with new skills.

4. Executive Communications: Keep Everyone on the Same Page

Today, CEOs and board members are bombarded with media reports about cybercriminals, hacktivists, and catastrophic data breaches. CISOs and senior IT executives need to be proactive about keeping top executives informed about genuine threats to the enterprise and why the IT organization is investing in specific programs, technologies and staff.

Threat intelligence can help CISOs and senior IT executives communicate with non-technical top executives in terms of risks and threats to the business and the financial and political goals of threat actors. It can help them respond quickly and accurately to questions about incidents publicized in national and industry media, as well as cybersecurity priorities. When incidents occur, threat intelligence can help IT executives better inform the CEO and board about potential responses, so everyone can agree on appropriate next steps.

The bottom line

- Reliable, strategic, actionable intelligence from iSIGHT Partners can help the CISO and IT executives:
- Identify and prioritize risks based on threat intelligence that's relevant to your enterprise.
- Assess the risks of new business initiatives with more confidence.
- Make better strategic decisions on security budgets and staffing.
- Respond effectively to incidents through a better understanding of threat actors and their tactics, techniques and procedures.
- Keep top management aligned about risks, threats, security preparedness and responses.

To learn more about FireEye, visit: **www.FireEye.com**

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