DATA SHEET

Threat Intelligence Foundations

Plan to put your CTI where it does the most good

BENEFITS

- Align CTI to business priorities to ensure positive ROI
- Take informed security action by applying intelligence where it's needed
- Discover business uses for CTI
- Develop consistent, repeatable and scalable threat intelligence operations
- Optimize your ability to consume, analyze and apply threat intelligence

Cyber threat intelligence (CTI) can enable a more effective and efficient cyber risk management process. Actionable intelligence on the motivations and methods of threat actors likely to target your organization can strengthen your position in strategic, operational and tactical use cases.

But to achieve this, you must get the right CTI to the right stakeholders in the right format. Most intelligence consumers don't know how to make correct and timely use of relevant threat intelligence. CTI functions must be able to focus their operations on relevant threats and deliver actionable communications tailored to end users. If you are mindful of this focus, you can consistently realize the value of your intelligence and ultimately increase operational efficiencies.

Why FireEye Threat Intelligence Foundations

CTI enables efficient cyber risk management. In many cases, you can reduce risk by anticipating and understanding the methods and motives the threat actors targeting your organization. The FireEye Threat Intelligence Foundations consulting engagement helps organizations identify and institutionalize the basic requirements for meaningfully consuming and applying CTI.

Strategic (Threat Profile)	Informs
• Who is targeting me, why? • What are their intentions? • What does this mean for my business? • What can I do to prepare?	• Planning • Messaging • Resourcing
Operational (Campaigns)	**Informs**
• How are these events connected? • What should I prioritize? • Why are these events happening? • How do these actors operate?	• Investigations • Incident Response • SecOps
Tactical (Malware)	**Informs**
• What malware is evident? • How does it operate? • How do I identify it on my network? • How is it getting on my network?	• Infrastructure Ops • Vulnerability Management

How it Works

During the Threat Intelligence Foundations engagement, Intelligence Capability Development (IDC) consultants will work with you to identify the foundational intelligence requirements through the following steps:

- **Discovery:** Build an understanding of your current intelligence function and capabilities through documentation review, workshops, and roundtable discussions.
- **Threat (Landscape) Profile:** Build a profile of threats relevant to your organization based on the results of discovery.
- **Stakeholder Analysis:** Review and interview all relevant potential consumers of threat intelligence to ensure their needs are understood and met.
- **Intelligence Requirements:** Build a set of intelligence requirements based on learnings about relevant threats, organizational concerns and the needs of individual stakeholders to focus your intelligence operations
- **Threat Communication Concepts:** Demonstrate how threat intelligence can be operationalized through stakeholder-specific communications.
- **Intelligence Prioritization:** Prioritize intelligence requirements and collection strategies based on anticipated threat level and organizational risk management preferences.
- **Deliverables Review and Finalization:** Present deliverables that explain how to build, maintain and disseminate core threat intelligence constructs and communications.

FireEye Intelligence Capability Development (ICD) services are designed to help organizations realize the true value of their CTI investments. Over the last decade, hundreds of organizations have worked with FireEye ICD services to improve their security programs through best practices for the consumption, analysis and practical application of CTI.

Figure 1. Threat Intelligence Foundations engagement focus.

Additional FireEye Intelligence Capability Development offerings

Threat Intelligence Foundations: establishes the basic building blocks for developing threat intelligence capabilities.

Cyber Threat Diagnostic: identifies and documents your organization's threat landscape by analyzing your current processing environment for malicious attacks.

Intelligence Capability Assessment: evaluates the effectiveness of your current threat intelligence capabilities and how well intelligence is integrated into your security program.

Intelligence Capability Uplift: develops a blueprint for how you can implement a world-class threat intelligence program that includes scalable, repeatable processes.

Intelligence Jumpstart: offers participants an interactive one-day workshop that maps out technical and operational use cases for the application of intelligence within your organization.

Analytic Tradecraft Workshop: enhances the analytical skillsets your team needs to support in-house threat intelligence activities.

Hunt Mission Workshop: introduces your team to threat hunting as well as a framework that can be used to standardize the threat hunting process within your organization.

THE FIREEYE ADVANTAGE

Experience: Our industry leading cyber threat intelligence function is complemented by 15 years of programmatic knowledge gained from helping a diverse set of customers operationalize cyber threat intelligence.

Best Practices: Our framework and development methodology uses intelligence community best practices to help you improve how you consume and apply intelligence. It also uses information security best practices to guide CTI integration across your business and security operations.

Threat Intelligence: Our industry leading intelligence is sourced from FireEye consulting engagements, Managed Defense services, product telemetry data and FireEye Threat Intelligence operations. We use this powerful, broad and deep visibility across the threat landscape to help customers visualize comparative threats and translate concepts to practice.

To learn more, visit: **https://www.fireeye.com/solutions/cyber-threat-intelligence/intelligence-capability-development.html** and read the **Forrester report**.

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™