DATA SHEET

Cyber Threat Intelligence Workshops

Develop the skills you need to gather, utilize and manage cyber threat intelligence

HIGHLIGHTS

- Prepare teams to effectively consume and apply intelligence
- Learn how to better collect, analyze, and disseminate CTI
- Enable teams to use CTI to hunt for threats within your organization
- Inform security operations of the latest threat activity, with context relevant to specific stakeholders

FireEye Intelligence Capability Development (ICD) services are designed to help organizations realize the true value of their cyber threat intelligence (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 .

The Cyber Threat Intelligence Workshops give your organizational staff the skills they need to carry out your CTI mission and use CTI within the context of their specific roles.

Workshop Engagement
Our workshops ensure that participants gain practical skills they can apply immediately by using the following principles:

- **Interactive:** Facilitators engage participants to discuss their roles and responsibilities to help adapt the content and make it sticky
- **Organizationally Relevant:** Before the workshops, consultants meet with you to understand your specific circumstances and use cases to effectively relate to participants.
- **Enablement:** Consultants help participants understand, adapt knowledge and apply concepts to their roles.
- **Industry Best Practices and Expertise:** Workshop topics and content is derived from over 15 years of experience building a proven, industry-leading CTI function, helping others build their intelligence functions and curating intelligence community best practices.

Security practitioners just starting to use CTI may often be confused and overwhelmed about how to apply it in security operations. Traditional training and education formats do not always adapt concepts into use cases they can understand. Challenges unique to an organization can further complicate CTI application and adoption. Tight budgets and limited resources can make it difficult to spend significant funds and time on formal training.

The collaborative experience offered by these workshops enable more beneficial situation-specific education for participants. Our consultants work to understand special circumstances, and then enable participants to apply relevant concepts to their unique situations long after the workshop concludes.

Table 1. Available workshops.

	Analytic Tradecraft	Hunt Mission	Intelligence Jumpstart
Description	The Analytic Tradecraft Workshop provides the core analytical skillsets needed to support CTI capabilities. Participants should be able to apply intelligence to organizational concerns and create timely, accurate, and relevant intelligence communications to stakeholders at the conclusion of this engagement.	The Hunt Mission Workshop provides an intelligence-led approach to discovering threats. Participants should be able to understand how to use intelligence to plan for and execute hunts within their network, and how to organize findings and feed them back into the intelligence lifecycle.	FireEye Threat Intelligence Jumpstart helps ensure that you get the most out of your threat intelligence investment. This interactive, one-day workshop introduces you to the knowledge, methodology and best practices needed for an effective threat intelligence capability.
Topical Areas	• The intelligence lifecycle • Stakeholder analysis • Intelligence as a risk mitigation tool • Role-based intelligence • Threat landscape identification • Indicators of compromise management • Structured techniques for analysis (diamond model, challenge analysis, logic models, etc.) • Intelligence augmented kill chain • Technical writing primer • Workflows for organizational threat communications	• Hunt mission value model • Prerequisite core operational drivers • Integration of hunt capability into conventional cyber security operations • Hunt mission process framework • Use case development • Hunt mission scenario—Capstone	• Understanding your cyber threat landscape • Core threat intelligence capabilities • Threat intelligence foundations • Essential analytic techniques • Best practices for threat communications • Technical intelligence integration and managing threat data • Threat actor attribution • Threat hunting • Improving risk management with threat intelligence

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 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.