FIREEYE™

DATA SHEET

Threat Intelligence Jumpstart

Maximize the value and impact of your threat intelligence

HIGHLIGHTS

- Learn how to effectively integrate threat intelligence into your security operations
- Understand the importance and value of knowing your organization's threat profile
- Identify your current intelligence practices and how to pragmatically improve them.
- Map out your technical and operational use cases for applying intelligence.
- Maximize your threat intelligence return on investment.

External threat intelligence services can be invaluable in making strategic business decisions, staying ahead of your adversaries and proactively aligning your security defenses against your most likely threats.

But you need to know how to effectively integrate threat intelligence into your security operations to fully realize its benefits.

FireEye Threat Intelligence Jumpstart is designed to 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.

Every customer and organization is unique, with different maturity levels, security challenges and intelligence needs. Because of this, Threat Intelligence Jumpstart offers a modular, topic-based approach you can tailor to fit your organizations's unique requirements and areas of focus.

FireEye Threat Intelligence Jumpstart harnesses the subject matter expertise of our strategic and tactical threat intelligence practitioners around the world. Our experts share that knowledge with you based on their experiences with what has worked in the real world across many types of organizations.

How Threat Intelligence Jumpstart Works

To ensure that your unique use cases for threat intelligence are appropriately addressed, FireEye offers modules on different intelligence subjects. You select which modules need to be included in the workshop. The FireEye team scopes the agenda, helps you identify participants who would benefit from attending and then documents the expected outcome to ensure alignment. The workshop can be delivered onsite, remotely or in a hybrid format. Deliverables include:

- Formal report documenting the content delivered, key observations and recommendations
- Select supporting materials, such as workshop slides and graphics
- Industry references, recommended reading and samples of FireEye Threat Intelligence reports (if applicable)

A follow-up meeting is held 30 days after the workshop to review the status of the recommendations and to discuss your intelligence priorities.

Threat Intelligence Jumpstart Workshop: Intelligence Subject Modules

Here are some of the available topics you can choose to customize your Threat Intelligence Jumpstart workshop:

Table 1.

Workshop Module	Description
Understanding Your Cyber Threat Landscape	Provides an overview of the importance of understanding your unique cyber threat landscape. Introduces methods and use cases for using threat intelligence to develop your organization's cyber threat profile.
Core Threat Intelligence Capabilities	Explains how to identify the essential people, processes and technology needed to effectively consume and apply threat intelligence within your organization. A crtical and essential part of developing threat intelligence capabilities.
Threat Intelligence Foundations	Describes the essential building blocks needed to develop and sustain a threat intelligence capability. This includes inputs typically needed to maintain a cyber threat profile and how teams can conduct stakeholder analysis to understand your intelligence needs.
Essential Analytic Techniques	Introduces basic best practices and techniques used to effectively analyze threat intelligence in a manner that meets organizational or stakeholder needs.
Best Practices for Threat Communications	Establishes best practices and methods for communicating information relating to cyber threats across the organization to different audience types, to achieve specific outcomes.
Technical Intelligence Integration and Managing Threat Data	Orients technically-focused teams with common practices related to the integration of intelligence data into existing procedures, workflows and within your security technology.
Threat Actor Attribution	Explains how intelligence analysts perform attribution at different levels, details associated operational challenges and provides technical and non-technical methods to attribute threat activity to specific actors or groups.
Threat Hunting	Introduces a standardized, intelligence-driven methodology to proactively identify threats within the enterprise. Identifies operational drivers, success factors, and valuable business outcomes related to a formally established and managed threat hunting function.
Improving Risk Management with Threat intelligence	Presents recommended approaches to integrate threat intelligence into broader risk management standards, frameworks and practices.

The Threat Intelligence Jumpstart workshop enables your security programs to gain a foundational understanding of threat intelligence best practices and capabilities, and how they could be implemented within your organization.

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.