DATA SHEET

Intelligence Capability Assessment

Establish a baseline for your threat intelligence operation

HIGHLIGHTS

- Baseline functional capabilities of intelligence against five maturity domains
- Understand gaps around people, process, and technology that limit your ability to realize the full potential of cyber threat intelligence
- Plan a strategic growth path for the intelligence function to ease communications with program sponsors and stakeholders
- Validate current program maturity and use assessment results to adjust your plan

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 Intelligence Capability Assessment evaluates core CTI capabilities as well as your ability to integrate intelligence with security operations and the broader business.

Why assess intelligence capabilities

CTI capabilities enable efficient cyber threat and risk management. When organizations are challenged to fully realize their CTI value proposition, they often use CTI in an ad-hoc way, or they overlook opportunities to apply it strategically across all cyber defense and business functions.

Table 1. FireEye Intelligence Capability Assessment Framework.

Domains	Capability Areas	
Cyber Threat Intelligence Core	• Organizational role of intelligence • Analytic practices • Technology integration	• Intelligence products and services • Intelligence process lifecycle • Analyst capability and expertise
Identify and protect	• Strategy and policy • Vulnerability management • Security controls	
Monitor and detect	• Security monitoring • Threat detection	
Respond and recover	• Response and recovery planning • Incident mitigation and recovery	
Reduce risk	• Exposure analysis • Threat and risk communications • Strategic advancement	

Many organizations are tasked to scale CTI operations so they can consistently deliver their full CTI value proposition. In some cases, it can be difficult to focus the intelligence operation on the relevant threats and stakeholder needs. In other cases, the scalability design has flaws that contribute to inefficient execution. Organizations can also experience tactical breakdowns in analysis processes and workflows. Such challenges inhibit mature practices and capabilities required to proactively produce and deliver intelligence across the business

You need a baseline to understand current CTI capabilities, identify gaps and understand the steps needed to realize your full CTI value and potential. The Intelligence Capability Assessment is the benchmark and planning step required to build a mature intelligence function and helps prioritize strategic initiatives over the long term.

How it works

Consultants identify your current capabilities and current maturity, and make recommendations based on identified gaps using the following process:

- **Conduct Discovery:** Build an understanding of your current intelligence function and capabilities through documentation review, workshops, and roundtable discussions.
- **Assess Core CTI Function:** Assess ability to drive accurate, timely and relevant intelligence to appropriate audiences throughout your organization.
- **Assess Integration Capabilities:** Assess your ability to integrate intelligence into security operations and across your business.
- **Plan Target State:** Define an end state for your CTI function based on organizational circumstances, your vision and best practices.
- **Develop Strategic Roadmap:** Build a custom roadmap to achieve the intelligence vision for your organization.
- **Deliverable Review and Finalization:** Work with your teams to ensure there are no gaps in the assessment, and focus on providing actionable recommendation and guidance to enable meaningful and measurable growth.

Figure 1. Engagement overview.

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.

FIREEYE™