DATA SHEET

Intelligence Capability Uplift

Develop and mature your threat intelligence operation

HIGHLIGHTS

- Define intelligence team structure, functions, roles, and expertise
- Develop structured and repeatable intelligence lifecycle processes, practices and capabilities
- Define requirements for the technology stack to support your CTI function
- Create threat intelligence communications formats, production standards, guidance and workflow
- Detail key performance indicators to measure the program, individuals responsible for implementation and intelligence sources.

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 Uplift offering helps you develop scalable, repeatable practices to enable the collection, analysis, production and dissemination of intelligence throughout your organization.

Why Intelligence Capability Uplift

CTI capabilities enable efficient cyber threat and risk management. When organizations are challenged to fully realize their CTI value proposition, they may understand the most impactful threats, but lack the processes, expertise or supporting technology to truly become intelligence-led. The most effective way to realize CTI capabilities is to strategically plan and implement CTI-specific practices related to people, processes and technology. Through programmatic development, organizations can align CTI functions to business needs and ensure sustainability and value.

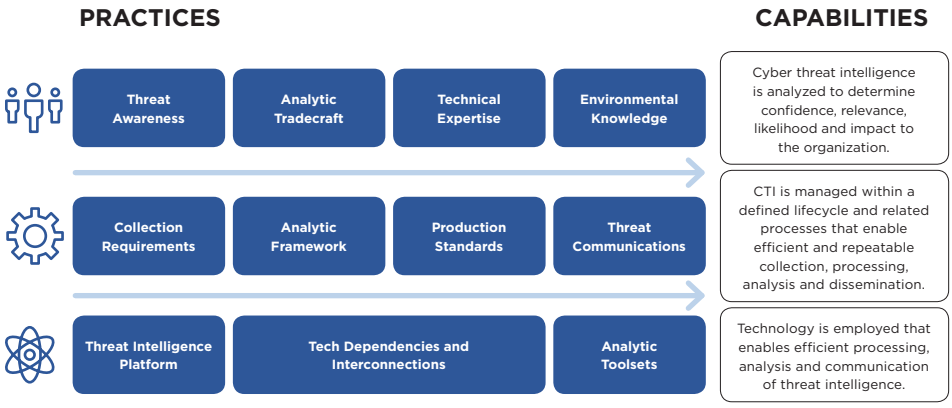

Figure 1. FireEye Intelligence Capability Uplift framework.

How it works
Consultants work to understand your unique organizational circumstances and design a customized CTI program using the following process:

- **Discovery:** Build an understanding of your current intelligence function and capabilities through documentation review, workshops, and roundtable discussions.
- **CTI Core Functions:** Draft core functions based on the mission of your CTI function, and include operational support, communication and analysis of CTI and CTI lifecycle management.
- **Team Structure and Roles:** Define organizational placement, structure, roles and responsibilities based on best practices adapted to your current realities and overall CTI mission.
- **Threat Communications Workflow:** Define workflow, processes and supporting technology required to create and deliver intelligence to stakeholders across your organization.
- **Process Lifecycle:** Develop a process to execute all phases of the CTI lifecycle, including:
  - Planning and requirements
  - Collection and processing
  - Analysis
  - Production
  - Dissemination and feedback
- **Intelligence Product Templates:** Produce organization-specific communications templates.
- **Deliverable Review and Finalization:** Show relationships between all deliverables to ensure your personnel will be able to understand, implement and operationalize CTI practices after the engagement concludes.

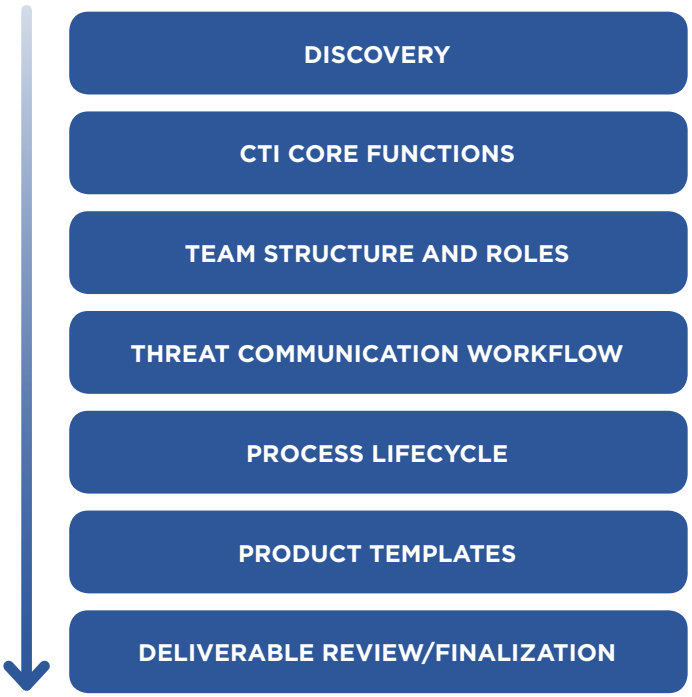

Figure 2. Intelligence Capability Uplift engagement focus.

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 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™