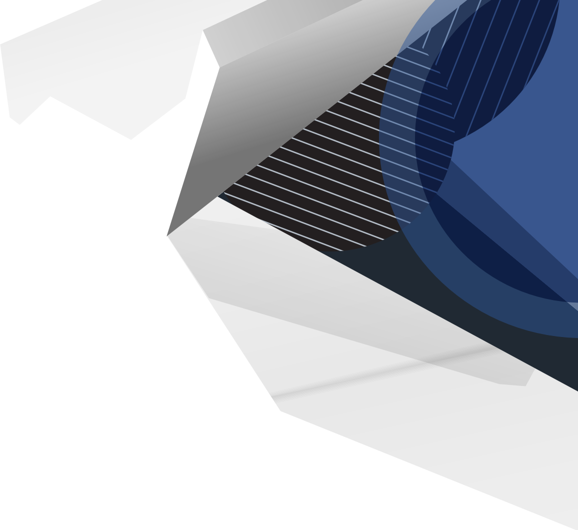


FIREEYE™

DATA SHEET

Intelligence Capability Development

Optimize your threat intelligence capabilities

HIGHLIGHTS

- Optimize your ability to consume, analyze and apply threat intelligence within your cyber security operations
- Call on the 12+ years experience building government and commercial intelligence capabilities
- Baseline existing intelligence capabilities and plan improvements
- Determine the cyber risk your organization faces, the intelligence you need to fight that risk and who will use it
- Map out your strategic, operational and tactical use cases for the application of intelligence
- Participate in workshops to improve CTI capabilities and use CTI more effectively in your day-to-day activities

Cyber attackers are better trained, better funded and better staffed than many security organizations. As a result, cyber attacks have become more complex and the resulting damage more severe. Finding and retaining even a single qualified security professional is tough, but getting all the professionals you need is often cost prohibitive.

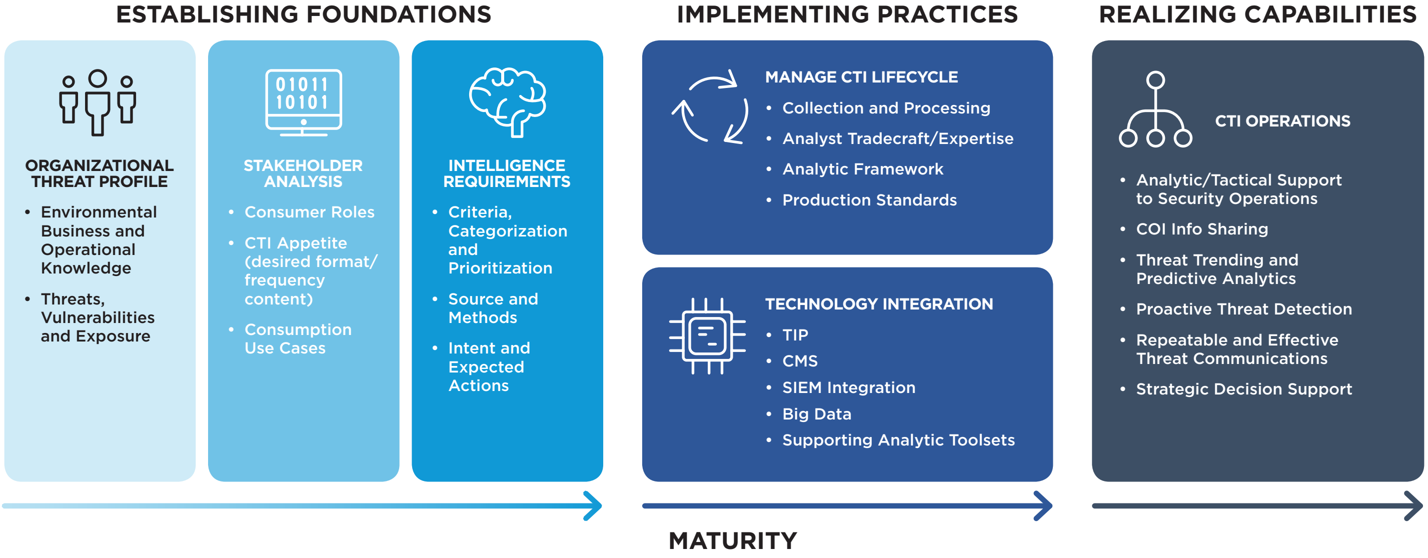
For these reasons, more organizations look to reduce their risk and augment their security with cyber threat intelligence (CTI) services. However, many organizations don't know where to start, while others jump in without understanding what threat intelligence they need or how it should be used. The results are generally ineffective and costly. Organizations need to know how to get a better return from their CTI investments.

FireEye Intelligence Capability Development (ICD) services are designed specifically to help organizations realize true value from CTI. Over the last decade, hundreds of organizations have worked with FireEye ICD consultants as trusted advisors to build best practices for the consumption, analysis and practical application of CTI. As a result, they have increased the effectiveness and efficiency of their security programs.

How it Works

ICD has developed a suite of CTI services that use a standardized framework to **assess** the current state of your intelligence program and threats, **design** an optimized program to meet your organizational and regulatory requirements and **enhance** the capabilities of your staff with regard to analytical skillsets and applying threat intelligence to specific use cases.

This framework defines the most critical components of an effective CTI program.



ESTABLISHING FOUNDATIONS

ORGANIZATIONAL THREAT PROFILE

- Environmental Business and Operational Knowledge
- Threats, Vulnerabilities and Exposure

STAKEHOLDER ANALYSIS

- Consumer Roles
- CTI Appetite (desired format/ frequency content)
- Consumption Use Cases

INTELLIGENCE REQUIREMENTS

- Criteria, Categorization and Prioritization
- Source and Methods
- Intent and Expected Actions

IMPLEMENTING PRACTICES

MANAGE CTI LIFECYCLE

- Collection and Processing
- Analyst Tradecraft/Expertise
- Analytic Framework
- Production Standards

TECHNOLOGY INTEGRATION

- TIP
- CMS
- SIEM Integration
- Big Data
- Supporting Analytic Toolsets

REALIZING CAPABILITIES

CTI OPERATIONS

- Analytic/Tactical Support to Security Operations
- COI Info Sharing
- Threat Trending and Predictive Analytics
- Proactive Threat Detection
- Repeatable and Effective Threat Communications
- Strategic Decision Support

MATURITY

ICD services address all aspects of the framework and range from limited scoped engagements focused on specific use cases to large-scale intelligence program implementations. All outcomes are focused on increasing an organization's ability to maximize the value of their external cyber threat intelligence. Specific offerings include:

- **Threat Intelligence Foundations**
  Establishes the basic building blocks for developing threat intelligence capabilities. This includes identifying relevant threats, the stakeholders who would benefit from using threat intelligence and the pragmatic practices for effective delivery and consumption. [Assess]
- **Cyber Threat Diagnostic**
  Identifies and documents your organization's threat landscape by analyzing your current processing environment for malicious attacks. The threat landscape is a critical part of intelligence-led security because it enables you to better align your defenses and prioritize your actions based on the motives and intentions of the threat actors targeting your business. [Assess]
- **Intelligence Capability Assessment**
  Evaluates the effectiveness of your current threat intelligence capabilities and how well intelligence is integrated into your security program. A detailed gap analysis accompanies a strategic roadmap for addressing those gaps with people, processes and technology. [Assess]
- **Intelligence Capability Uplift**
  Develops the blueprint for how you can implement a world-class threat intelligence program that includes scalable, repeatable processes for the collection, analysis and dissemination of intelligence throughout your organization. [Design]
- **Intelligence Jumpstart**
  Introduces many of the subject areas covered by in-depth consulting services. This interactive one-day workshop draws on the expertise of our strategic and tactical intelligence practitioners to map out technical and operational use cases for the application of intelligence within your organization. [Design]
- **Analytic Tradecraft Workshop**
  Enhances the analytical skillsets your team needs to support in-house threat intelligence activities. Core CTI concepts, structured analytic techniques, threat communication skills and links to threat and risk management are covered in this one-day workshop. [Enhance]
- **Hunt Mission Workshop**
  Introduces your team to a threat hunting framework that can be used to standardize the way threat hunting is done within your organization. You can analyze your current methods to identify a set of repeatable processes that represent threat hunting best practices. Curriculum is tailored for SOC, incident response, and tactical intelligence analysts responsible for threat detection activities. [Enhance]

The FireEye Advantage

A strategic partnership with FireEye will ensure your people, processes and procedures are prepared to meet the demands of an evolving threat landscape—at any scope and scale.

The FireEye Intelligence Capability Development (ICD) group has more than a decade of experience building industry-leading CTI capabilities. This experience includes all of the lessons learned and the best practices identified through working with FireEye Threat Intelligence. Forrester Research recently identified FireEye as the only threat intelligence vendor in the "Leader" category in its report, "The Forrester New Wave™: External Threat Intelligence Services, Q3 2018."

FireEye has spent the last decade working with companies across industry verticals to effectively adopt and integrate CTI into their security operations. These experiences have helped build and refine a set of services adaptable to any organizational need and mission. Media, government and private sector organizations worldwide depend on FireEye intelligence leadership and offerings.

Whether combined or delivered separately, ICD services support the development and maintenance of a comprehensive threat intelligence program.

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.