CYBER THREAT INTELLIGENCE SERVICES

TRANSFORM YOUR SECURITY OPERATIONS FOR INTELLIGENCE-LED ADAPTIVE DECISION MAKING ACROSS THE ORGANIZATION

OVERVIEW

Mandiant has over a decade of experience at the forefront of cyber security and cyber threat intelligence (CTI). This has enabled us to build unparalleled intelligence operations collecting, analyzing and disseminating threat intelligence to our customers, as well as helping organizations develop their own intelligence-led security operations. Based on expertise, Mandiant has developed the Cyber Threat Intelligence Services to help organizations build, mature and sustain intelligence-led security operations customized to their unique needs.

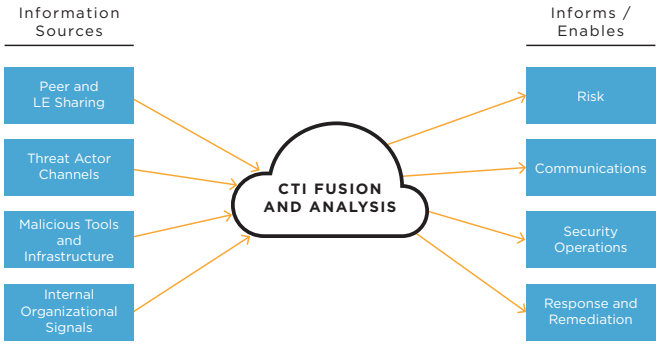


FIGURE 1. FUSING DISPARATE SIGNALS TO DRIVE INTELLIGENCE VALUE ACROSS THE ORGANIZATION

Transforming How You Use Threat Intelligence

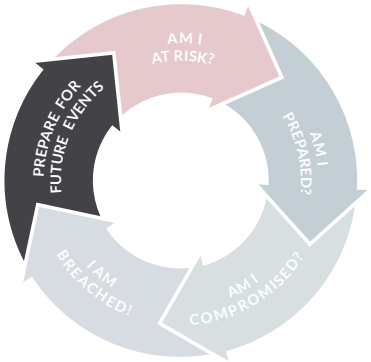
Cyber Threat Intelligence Services design and build cyber threat intelligence (CTI) solutions and capabilities within your security and business operations to optimize your ability to consume, analyze and apply cyber threat intelligence to protect the business. Our services focus on strategic planning, threat communications, technical solutions and workforce expertise required to implement an intelligence-driven cyber security program by:

- Assessing the maturity of existing threat intelligence programs and helping to create a strategic plan focused on achieving a level of maturity in line with organizational goals and budget
- Developing an operations framework including processes, workflows, technologies, necessary relationships and expertise to guide implementation of intelligence programs
- Developing CTI communications to meet cross-functional needs
- Enhancing workforce expertise and knowledge of analytic tradecraft and intelligence-led hunt missions to solve the most complex problems and proactively reduce threat exposure

Scope and Approach

Cyber Threat Intelligence Services 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 identify, contextualize, adapt to, anticipate and communicate the threats it encounters.

MANDIANT®
A FireEye® Company



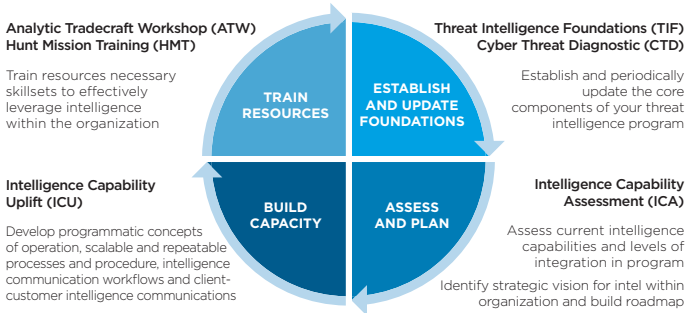
BENEFITS

- Anticipate, identify and prioritize active and nascent threats to reduce exposure and adapt defenses
- Inform risk assessment and management by determining adversary motivation, capability and impact
- Contextualize and communicate cyber threats across business operations and drive informed decision-making
- Align security capabilities and resources appropriately, based on the most relevant and impactful threats

FireEye®

Enhanced capabilities include:

- **Programmatic CTI Consumption and Integration**
  Develop the ability to implement a set of CTI practices, capabilities or an entire program, capable of consuming and applying CTI to reduce long term risk and integrate CTI into key cybersecurity capabilities.
- **Strategy and Process**
  Develop a strategic roadmap to enhance security maturity using an intelligence-driven methodology. Key security and business process components recognize and include threat intelligence.
- **Threat Awareness and Skill Enhancement**
  Teams and individuals within the organization have a greater understanding of the threats it faces, with enhanced skills related to consuming, analyzing, applying and communicating threat intelligence.



Cyber Threat Intelligence Service Offerings

Cyber Threat Intelligence Services is a framework of six offerings that, when combined or delivered separately, support the development of an organization's CTI program.

Threat Intelligence Foundations (TIF)

Threat Intelligence Foundations provides you the basic building blocks for developing threat intelligence practices and capabilities with three primary objectives:

- Inform organizations about the most relevant and impactful cyber threats relative to their sector organizational type and operational profile
- Identify how various stakeholders within the organization can consume and apply CTI within security and business operations
- Provide a framework for prioritizing and developing pragmatic threat intelligence practices, communications and cybersecurity use cases

Cyber Threat Diagnostic (CTD)

A Cyber Threat Diagnostic provides a baseline threat profile that includes the motivations, intentions and capabilities of the actors targeting the business. This profile is built by analyzing threat activity evident within network logs as well as underground observations indicating threat actor interest relevant to our customers. Periodically baselining your threat profile is a key component of building and maintaining an intelligence-led security strategy.

Intelligence Capability Assessment (ICA)

An Intelligence Capability Assessment evaluates an organization's core threat intelligence capabilities as well as the effectiveness of the program to integrate intelligence across multiple information security-related domains and disciplines. It provides a comprehensive understanding of current intelligence capabilities through detailed reporting, observations and determinations made during assessment activities. Recommendations for program maturation are also provided.

Intelligence Capability Uplift (ICU)

An Intelligence Capability Uplift focuses on defining a world-class threat intelligence program. We work with you to develop a programmatic concept of operations that includes scalable and repeatable processes and procedures for the collection, analysis and dissemination of intelligence throughout the organization. ICU addresses the full range of factors needed to support a successful intelligence-led mission: strategy organizational function, expertise, process, technology, levels of service, intelligence products and supporting resources, using core cyber security domains to guide integration across the security organization.

Analytic Tradecraft Workshop (ATW)

The Analytic Tradecraft Workshop is a one-day workshop that enhances the analytical skillsets necessary to support an organization's threat intelligence capability. Skills learned can be applied directly to a specific CTI process component, capability or practice. The workshop's curriculum directly aligns with the concepts and approach of other Cyber Threat Intelligence Service offerings. This provides an enablement aspect to the broader CTIS offering: giving threat intelligence analysts a pragmatic, core set of skills that can be applied within operations.

Hunt Mission Training (HMT)

The Hunt Mission Training workshops provide a tactical, technically-focused curriculum that enables intelligence-driven, proactive identification of active or nascent threats. Curriculum is tailored for SOC, IR and tactical intelligence analysts responsible for advanced threat detection activities.

For more information on FireEye, visit:
www.FireEye.com

About FireEye, Inc.

FireEye® is the leader in intelligence-led security-as-a-service. 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 has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye