DATA SHEET

Cyber Threat Diagnostic

Make informed security decisions to manage your risk

HIGHLIGHTS

- Align organizational resources against the capabilities and tactics of relevant threats
- Anticipate changes to your organizational risk profile based on changing threat factors
- Prioritize daily operations and program improvements by understanding what relevant threats can do and what they're after

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 Cyber Threat Diagnostic assesses the motives, intents and tactics of threat actors targeting your organization. The resulting threat profile provides cyber risk clarity and enables overall cyber risk management.

Why build a cyber threat profile?
Compliance and technology-based security approaches can establish a solid security baseline. However, they do not normally consider security alongside organizational risk. Leaders must periodically baseline and update the cyber security risk profile under which their organizations operate. With an assessment of the cyber threat landscape, they can determine:

- Are threat actors targeting the organization?
- What are their motivations? Why are they targeting the organization?
- What are their intentions? What assets are they targeting?
- What are their capabilities? What tactics, techniques and procedures (TTPs) should the organization be aware of? How sophisticated are the actors?

Answers to these (and related) questions provide context to help identify and clarify cyber risk. And by combining a periodic analysis of your organization's threat profile with the global threat intelligence perspective from FireEye you can create a bridge between security operations and organizational risk. This enables you to align security operations decisions based on risk rather than best practices, or instinct.

How it works
Consultants use an intelligence-led approach to develop relevant threat profiles based on evidence in network logs, external observables relevant to organizational concerns and a comparative analysis of threat activity focused on your industry sector or vertical.

FireEye consultants will identify threats relevant to your organization through the following steps:

- **Scope:** Identify relevant logs that produce potential signals of threat activity and determine an appropriate timeframe for the assessment. Threat activity findings may vary depending on the time of year, where technology sits within the network, specific business operations or public-facing activity.
- **Collect:** Work with your security teams on the best way to transfer log sources that can help identify threat activity.
- **Task:** Identify external observables relevant to your organization's threat profile.
- **Correlate and validate:** Based on Intelligence, observed data and analysis, determine the validity of insights to ensure high fidelity, actionable findings.
- **Analyze and contextualize:** Establish the nature, motives, intentions, capabilities, scope of operations and targets of a threat.

Multiple data collection options

- **No touch via historical log collection:** Clients can collect and provide scoped event log data via a number of physical transfer options.
- **Low touch:** Technology-enabled using the FireEye Helix platform to ingest enterprise event log data in real time, eliminating the burden of log collection and transfer and enabling and live "snapshot" of the network.
- **Moderate touch:** Clients can deploy a system within their enterprise to collect relevant data, which consultants can then access to perform the assessment. This is ideal for organizations that operate under tight data sovereignty restrictions.
- **Technology-enabled using FireEye Network Security and FireEye Email Security:** Use existing FireEye technologies or deploy technology to capture evidence of initial intrusion attempts with MVX sandboxing technology.

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™