CYBER THREAT DIAGNOSTIC

UNDERSTAND YOUR THREAT REALITY TO ENABLE AN INTELLIGENCE-LED SECURITY PROGRAM

MANDIANT®
A FireEye® Company

BENEFITS

Develop an efficient security program: Use your threat baseline for informed decision-making in critical areas, including:

- **Resourcing:** Improved alignment of organizational resources against the capabilities and tactics of relevant threats.
- **Forecasting:** Better anticipation of changes to the organizational risk profile due to evolving environmental and organizational factors.
- **Prioritization:** Improved prioritization of daily operations, future plans and security program improvements by understanding the underlying objectives and capabilities of the threat actor.
- **Communication:** Clearer communications to senior management and across the organization by translating technical security events and data to non-technical, threat and risk-focused discussions.

THREAT PROFILES

- Motivation
- Intent

- Capability
- Campaign

- Vectors
- Scope

OVERVIEW

Mandiant has over a decade of experience at the forefront of cyber security and cyber threat intelligence. Our investigative approach has been applied to over a thousand breaches, including many of the most critical and damaging security incidents worldwide. FireEye iSIGHT intelligence collection and analysis capabilities provide the Mandiant team with a global threat perspective through active engagement in forums, marketplaces and other channels.

Cyber Threat Diagnostics uses our industry-leading intelligence and analysis capabilities to provide a unique perspective on the motives, intents and tactics, techniques and procedures (TTPs) of the actors targeting the enterprise. It is part of Mandiant's Cyber Threat Intelligence Services that help organizations build, mature and sustain intelligence-led security operations customized to their unique needs.

Build a threat profile for informed decision-making

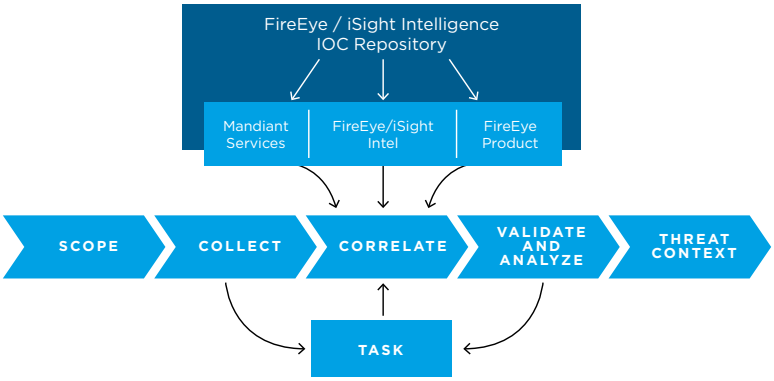
It is becoming increasingly important for leaders to continuously baseline and update their understanding of the threat landscape within which their business operates. While effective at establishing foundational security components, compliance and technology-based approaches to security lack the ability to establish context. Organizations can establish context by seeking to answer the following questions:

1. Am I being targeted by threat actor(s)? Assess whether threat actors are trying to compromise your environment based on analysis of evident threat activity combined with our global threat perspective through active engagement in forums, marketplaces and other channels.
2. If so, what are their motivations? What are their capabilities and what is their modus operandi? Understanding contextual information about threat actors — why they take action, what they seek to achieve and how they carry out operations — enables risk-based alignment of security operations.

Combining a periodic analysis of your organization's threat profile, with FireEye's global threat intelligence perspective creates a bridge between security operations and the organizational risk discussion. This enables a risk-based alignment of security operations focused on the continuously evolving threat environment you do business within.

FireEye®

Approach



Scope: Work with you to scope your Cyber Threat Diagnostic so as to threat concerns and meet business goals. Threat activity may vary depending on the time of year, specific business operations or public-facing activity.

Collect: Mandiant coordinates with your security teams to identify the most effective log sources containing technical observables that are useful for identifying threat activity within an environment.

Task: Work with the FireEye iSIGHT intelligence team to identify external observables relevant to your specific organization's threat profile.

Correlate and validate: Validate results of data correlation to limit false positives and determine where additional analysis or data may be necessary to ensure a high-fidelity threat with actionable insights.

Analyze and contextualize: Validated matches are reviewed for threat context and nature of the threat, identifying key motives and intentions, capabilities supporting operations, scope of operations and target sets.

Data Sources and Collection

Multiple options for collecting the log data necessary for a Cyber Threat Diagnostic assessment:

1. **No touch via historical log collection:** Clients can collect and provide scoped event log data via a number of physical transfer options.
2. **Low touch:** Technology-enabled using FireEye Threat Analytics Platform and Cloud Collector technologies to ingest enterprise event log data in real time, eliminating the burden of log collection and transfer and enabling a live "snapshot" of the network.
3. **Technology-enabled using FireEye Threat Prevention Platforms (NX and EX):** Leverage existing FireEye technologies or deploy NX/EX technology to capture evidence of initial intrusion attempts through employment of the MVX sandboxing technology. This will allow us to rapidly identify initial intrusions and related attempts during the analysis period, even if the malware has not yet been seen or categorized by the industry.

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

Differentiators

Evidence-based approach

Build relevant threat profiles from threat activity evident within network logs, intelligence observables relevant to organizational concerns and a comparative analysis of threat activity within your industry sector/vertical.

Threat Intelligence

Intelligence assembled from Mandiant engagements, FireEye iSIGHT Intelligence operations, FireEye products and FireEye as a Service.

Experience

Mandiant Consultants' industry experience is rooted in thousands of incident response and threat hunting engagements. This experience is augmented by access and collaboration with "best in class" FireEye iSIGHT intelligence analysts, which provides unique capabilities to support identification and contextualization of threat activity.

Services Linkage

Quickly and efficiently pivot to Compromise Assessment and Incident Response services in the event of a suspected compromise or confirmed breach.

WHAT YOU GET

A report documenting actors targeting your organization, related motivations, intentions and capability. The core of the report is designed for a strategic audience but contains addendums including more detailed content, including:

- Specific campaigns identified within the environment, focusing on the common motives, intent, related TTP and supporting infrastructure
- Implicated malicious code and related technical and behavioral indicators, exploitation vectors and implicated hosts within the environment
- Relevant FireEye iSIGHT Intelligence reporting providing deeper dive content on topics discussed within reporting

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