MANDIANT®

DATA SHEET

Security Instrumentation Platform

Know the true measure of your security

HIGHLIGHTS

- **Prioritize threats that matter** based on timely and relevant cyber threat intelligence
- **Assess current security tools efficacy** against real adversary attacks
- **Discover undetected gaps and overlaps** in your security infrastructure
- **Measure your team's time** to detect and respond
- **Identify the greatest opportunities** for optimization
- **Quantify improvement** to defenses over time
- **Rationalize value** of investments to executives with evidence
- **Simplify communications** on state of security posture across the business

In today's increasingly dynamic threat environment, CISOs and their teams are challenged to keep corporate assets secure. They are expected to know, and provide evidence of, the value of their cyber security investments and the effectiveness cyber defenses against current and emerging adversary attacks.

Penetration tests, red teaming, and breach and attack simulations are not enough—they do not deliver the quantifiable proof that CISOs and business leaders require to understand risk exposure and their cyber readiness. Without evidence based on performance data, security teams are hindered from successfully optimizing defenses and reporting on their security posture with confidence.

The Mandiant Security Instrumentation Platform, a critical element of Mandiant's intelligence-led controls validation technology, delivers the evidence you need. The Security Instrumentation Platform is a cyber security risk assessment and management platform that enables teams to ensure their critical assets are always protected.

Improved Efficacy of Controls

The Mandiant Security Instrumentation Platform is powered by Mandiant global threat intelligence and incident response data—unique and unparalleled threat data and adversary visibility that represents what the attackers are doing right now. This combination of Mandiant threat intelligence and security validation technology arms security teams with a validation strategy based on knowledge of who and what are likely to target their organization.

Mandiant intelligence-led security validation technology starts by prioritizing critical, relevant threats and then safely assesses and captures discrete, quantified evidence of the effectiveness of your overall security architecture against real adversary attacks. The results highlight specific individual attacks and even entire areas in the extended kill chain that defeat or bypass your security technologies. You can use these insights to determine where and how to optimize your controls, working with specific performance data and vendors as needed, and ultimately transform your entire program.

With the Mandiant Security Instrumentation Platform, you can rapidly quantify and prove the effectiveness of your security program against the latest sophisticated adversaries around the world. This technology can be used with on-premises, cloud, and hybrid architectures.

Quantifying your efficacy improvements makes it possible to prove the value of your security investments against the company's risk tolerance to business leadership.

With Mandiant Security Instrumentation Platform, the process is automated and continuous, allowing you to focus on defending your business more strategically while the platform vigilantly monitors and measures your overall security effectiveness.

Gain Confidence in Your Security Posture
Mandiant Security Validation experts work with you to quickly configure the platform, connecting actors, an alert source and any specific controls for additional depth. Through ease of integration, you can visualize the performance of your defensive stack when attack behaviors are safely executed.

Once configured, you can select discrete tests or preconfigured sequences of tests from Mandiant's vast library of real attacks, from adversary techniques, tactics and procedures, and various types of malware. As these tests are safely run, you can immediately and continuously validate that specific controls are working properly. Dashboards populate in real time to show you detection, alert, miss and prevention rates as tests run.

The platform also validates that events are properly timestamped and correctly parsed, and if correlation rules and threat models are defined, events generate appropriate alerts. Reports are available to view and export outlining your overall security effectiveness over time. Through continuous, ongoing validation, you gain the proof needed to achieve and maintain confidence in your program, not only for yourself, but also for your executives and the board.

Platform Details
Mandiant's open, customizable and extensible platform offers automated controls discovery and an architecture that allows the use of real attack binaries to safely test security controls. It includes six core components.

Director
This central controller and manager of continuous validation across your dynamic production environment is available a cloud-based (security-as-a-service) platform or on-premises as a virtual appliance or installable software.

Actors
These safely perform tests in production environments to validate the effectiveness of network, Windows, MacOS and Linux endpoint, email and cloud security controls and ensure your infrastructure is configured correctly.

Integrations
Rich, out-of-the-box integrations with defensive technologies and security infrastructure can accomplish deeper controls validation.

Attack Library
The content library represents thousands of attacks in every stage of the adversary lifecycle, including the extended kill chain and based on current and emerging adversary attack behaviors and TTPs informed by Mandiant global threat, adversary and breach intelligence.

Frameworks
Attacks are aligned to MITRE™ ATT&CK and NIST frameworks to easily tie effectiveness into your security assessment programs. Mandiant Security Validation is unique because its content both provides insight into which attack framework tactics are relevant to an organization and can be used to run validations against MITRE ATT&CK tactics to ensure comprehensive, relevant testing and accurate results.

Dashboards and Reports
Live graphical display with results of tests run in your environment, and reports of efficacy improvements over time containing real, quantitative data that can be used to inform your executives (Fig. 1).

Figure 1. Dashboard helps validate security controls across the full attack lifecycle to pinpoint areas of risk.

Intelligence-Led Validation Methodology

Mandiant Security Instrumentation Platform performs complete, continuous monitoring, validation and optimization of security controls with automated environmental drift detection. This continuous validation process is conducted through a five-step intelligence-led methodology (Fig 2.)

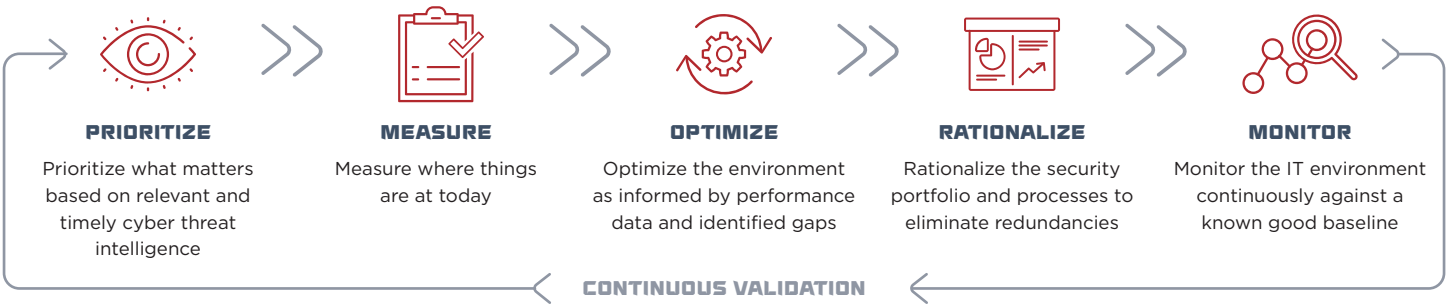

Figure 2. Mandiant five-step intelligence-led validation methodology.

Advanced Capabilities

- **Threat Actor Assurance Module (TAAM):** makes threat intelligence actionable so it's possible to test controls performance against real threat actors, particularly those most likely to target an organization. TAAM integrates with third party industry-leading intelligence feeds (Fig. 3).
- **Automated Environmental Change/Drift Analysis (AEDA):** enablement of continuous monitoring of the IT infrastructure to eliminate environmental drift and drive continuous validation against defensive regressions to ensure health of an organization's security infrastructure.
- **Protected Theater:** validates controls efficacy of the endpoint by safely executing malware, ransomware, and other destructive attacks to enable proactive protection against the latest and emerging threats.
- **Email Theater:** tests the controls offered in email security platforms.

Figure 3. Threat Actor Assurance Module (TAAM).

The Mandiant Security Validation portfolio includes multiple deployment options:

- **Customer Owned and Managed Model:** Cloud-based (SaaS) or deployed as a virtual appliance on-premises.
- **Fully Managed and Co-Managed Models:** Based on a customer's desired business outcomes, Mandiant teams build validation programs to fit particular use cases, providing detailed reporting to customer stakeholders on an ongoing basis.
- **Validation On-Demand:** Enables customers to purchase a single use case for a one-time assessment of their ability to block/prevent against a pre-defined attack or threat actor, and gain recommendations on further investigation needed to improve defenses and reduce risk exposure.

Security Validation Informed by Mandiant Threat Intelligence

Over the past 15+ years, through investigations, incident consultancy and red team exercises around the globe, Mandiant has created and curated a unique portfolio of threat intelligence which is constantly updated with new evidence data, human expertise and unique analytic tradecraft. Mandiant now dominates the field of cyber threat intelligence through the following balanced set of sources:

- **Breach intelligence** collected via Mandiant Consulting incident response engagements
- **Adversarial intelligence** obtained by Mandiant researchers
- **Machine intelligence** from FireEye security products
- **Operational intelligence** derived from Mandiant Managed Defense services

To learn more about Mandiant Solutions, visit **www.FireEye.com/validation**

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

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®