MANDIANT®

DATA SHEET

# Security Validation

## Know the true measure of your security

### BENEFITS

- Assess current security tools efficacy against real adversary attacks
- Discover previously undetected gaps in your security and infrastructure
- Measure your team's time to detect and respond
- Identify the greatest opportunities for optimization
- Improve configurations to target and eliminate specific weaknesses
- Determine which controls are most and least valuable
- Quantify improvement to defenses over time
- Augment team with automated, continuous efficacy monitoring
- Rationalize value of investments to executives with proof

**CISOs Are Measured On Their Effectiveness**

Security teams protect critical assets for their organizations, a challenging charter with difficult odds in today's dynamic threat environment. These teams make major investments in security technologies to defend their organizations, doing so in many cases without being empowered to effectively demonstrate or validate these capabilities to deliver on their promises to prevent adversaries from compromising their systems and networks.

Some teams try to close this gap by relying on limited tests from overstretched staff or outsourced red teams with significant time constraints. Others count on limited technologies like vulnerability scanners and automated penetration tests that don't fully and accurately represent the real threat environment.

The future success of security teams calls for a new shift in cyber security management—continuous security controls validation. This new approach of measurement and optimization of cyber security is Mandiant Security Validation, accompanied by the Mandiant Security Instrumentation Platform, a cyber security risk assessment and management platform that enables teams to ensure their critical assets are always protected.

**Improved Efficacy, Delivered Immediately**

With the Mandiant Security Instrumentation Platform, you can rapidly quantify and prove the effectiveness of your security program and ability to defend against the expanding threat landscape of the latest sophisticated adversaries around the world. This technology can leveraged whether your architecture is wholly on-premise, hybrid or in the cloud.

Start by safely assessing and capturing 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 leverage these insights to optimize your controls, working with specific performance data and vendors as needed, and ultimately transform your entire program.

Quantifying your efficacy improvements makes it easier to demonstrate results and rationalize your investments within a business framework to your executives.

All this is continuous, automated and repeatable, allowing you to focus on defending your business more strategically while the platform vigilantly underpins your overall security effectiveness.

**Be Confident In Your Security Posture**
Quickly configure the platform, connecting actors, an alert source and any specific controls for additional depth. Graphically add your high-level infrastructure.

Select discrete tests or preconfigured sequences of tests from the vast library of real attacks from adversary techniques and malware. Safely run these tests immediately and continuously to validate specific controls are working properly. Dashboards populate in real time with 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 build proof for you, your executives and your board to achieve and maintain confidence in your program.

**Key Components**

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

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

**Integrations**
Seamlessly and directly integrate with defensive technologies and infrastructure to extensively validate how effective controls are and identify improvements to implement where they are misconfigured.

**Attack Library**
Thousands of attacks in every stage of the adversary lifecycle, including the extended kill chain; the platform is open, customizable and extensible, and powered by Mandiant global threat intelligence and incident response data.

**Frameworks**
Attacks are aligned to MITRE ATT&CK and NIST frameworks to easily tie effectiveness into your security assessment programs

**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.


Foundational steps for a continuous security validation program.

To learn more about Mandiant Security Validation, 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®