Security Validation

Prove the Value of Cyber Security

CISOs Must Prove Security Effectiveness

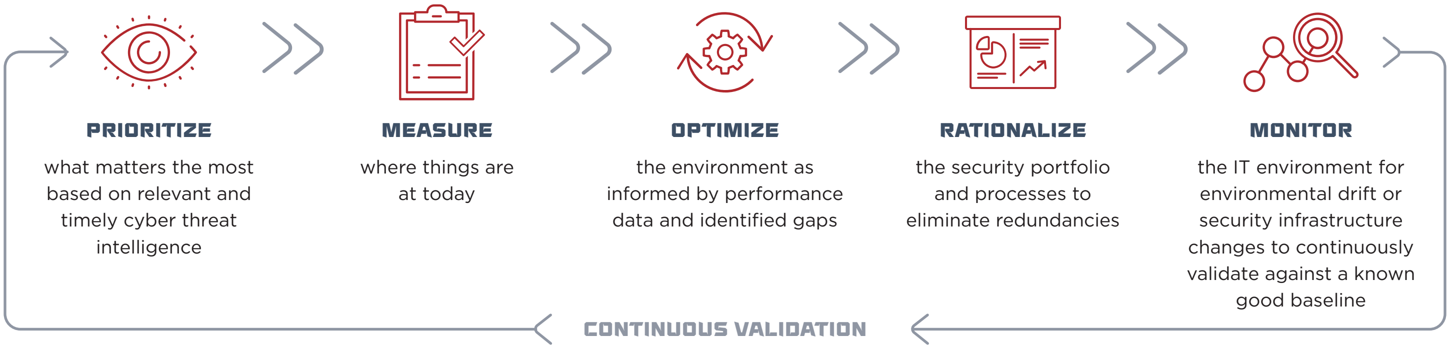
Today's risk-aware business environment is putting unprecedented pressure on CISOs and their teams to secure corporate assets and protect the financial posture and brand value of their organizations. They must prove to leadership the value of their cyber security investments and their effectiveness at preventing adversaries from compromising critical systems.

But lacking the tools needed to validate the effectiveness of security, quantify risk, and exhibit operational competency, they rely on vulnerability scanners, penetration tests, red teams or breach and attack simulations. Because of inherent limitations, these approaches do not sufficiently assess effectiveness or provide relevant, timely insights into specific, high-priority threats to the organization.

The solution is Mandiant Security Validation, a continuous, automated, intelligence-led portfolio made up of unique performance modules and the Mandiant Security Instrumentation Platform.[1]

Prove Effectiveness and Quantify Your Cyber Security Program

Security validation done right is based on a five-step methodology that provides insight into what is most important to test against and how to optimize defenses based on the knowledge of who and what might be targeting an organization or industry.



PRIORITIZE
what matters the most based on relevant and timely cyber threat intelligence

MEASURE
where things are at today

OPTIMIZE
the environment as informed by performance data and identified gaps

RATIONALIZE
the security portfolio and processes to eliminate redundancies

MONITOR
the IT environment for environmental drift or security infrastructure changes to continuously validate against a known good baseline

CONTINUOUS VALIDATION

Figure 1. Mandiant five-step intelligence-led validation methodology.

[1] Formerly Verodin Security Instrumentation Platform.

The methodology requires the ability to leverage threat data in real time. Mandiant Security Validation uses Mandiant threat intelligence and incident response data for unparalleled adversary visibility that reveals what attackers are doing right now. With intelligence-led Security Validation, security teams can identify high-priority threats to their organization and create a validation strategy based on the knowledge of who or what poses a threat to the organization. With Mandiant, security leaders and their teams can perform complete, continuous validation of security controls across technology, processes and people.

Mandiant Security Validation uses the Security Instrumentation Platform, its controls validation technology, to help security teams execute real attack behaviors against security controls to rapidly quantify and prove the effectiveness of their security program and ability to defend against the most sophisticated adversary attacks.

The Mandiant Security Instrumentation Platform basic functionality:

- Prioritize the threats and adversary controls that matter most
- Measure efficacy of security controls against real adversary attacks
- Safely execute relevant attacks informed by unparalleled Mandiant threat intelligence and incident response data
- Discover undetected gaps in the organization's security infrastructure
- Identify the greatest opportunities for optimization
- Quantify improvement to defenses over time
- Rationalize value of investments to executives with quantifiable evidence

The Mandiant Security Implementation Platform features advanced functionality:

- **Threat Actor Assurance Module:** 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.
- **Advanced Environmental Drift Analysis:** 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.

The Mandiant Security Validation portfolio includes multiple deployment options:

- **Customer Owned:** Cloud-based (security as a service (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 or prevent a pre-defined attack or threat actor, and gain recommendations on further investigation needed to improve defenses and reduce risk exposure.

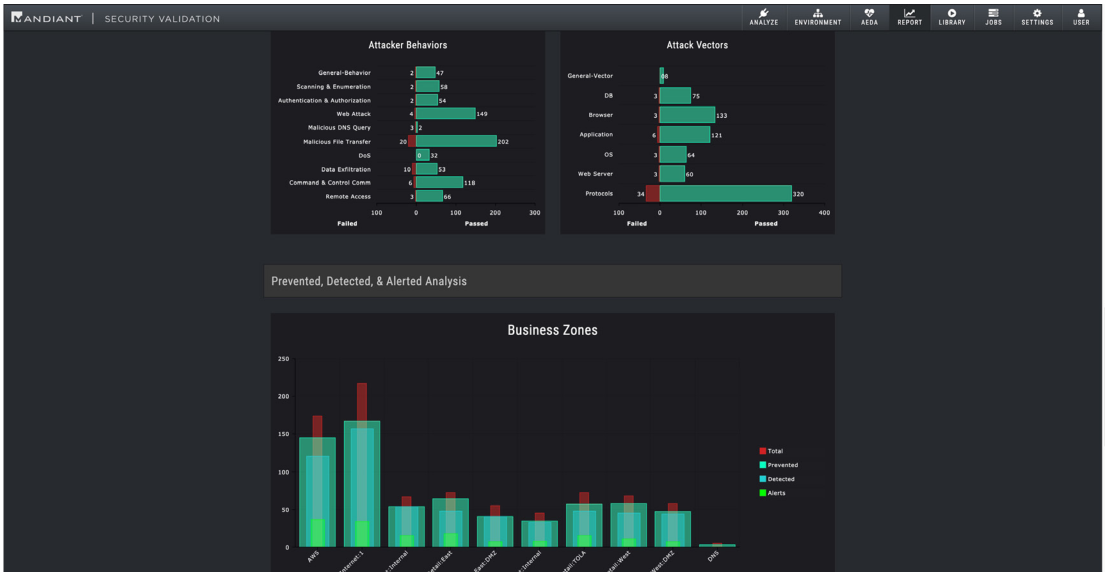


Figure 2.

Platform helps visualize and generate proof that your controls are protecting critical assets.

Business Benefits of Security Validation

Measure Effectiveness and Return on Investment (ROI)

Gain quantifiable data that helps determine the investment required to increase security effectiveness against prioritized attack types and quantify your overall risk profile. Security teams can also use this evidence to rationalize the value of security investments with executive leadership and the board.

Mergers and Acquisitions

Clearly grasp how companies undergoing a merger or acquisition may have overlaps or gaps in controls. Through rationalization of spending, you can calculate the dollar amount potential for consolidation and the level of risk they may be taking on as a result of the merger.

Hiring and Training of Security Talent

Look past years of experience and assess a security professional's potential for learning, the type of experience they have and how well their skill sets match your organization's environment within real-world scenarios. By safely executing real attacks across their production environment, IT leaders can monitor how prospective applicants respond and react. IT leaders can also conduct regular assessments as training exercises to see whether teams demonstrate acceptable response times and required skills in real-world attack scenarios.

Brand Protection

Proactively and continuously measure security effectiveness to reduce the risk of experiencing a breach or attack and preserve your brand reputation and customer loyalty.

Data Privacy and Protection

Protect customer data and ensure compliance with regulatory, corporate and third-party mandates.

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.