Security Validation

Highlights

- Build a validation strategy based on what Mandiant sees targeting your industry, peers and geography
- Pinpoint undetected gaps, misconfigurations and broken processes before an attack occurs
- Safely use the latest and active attacker behaviors and malware to understand your ability to withstand the next cyber or ransomware attack
- Access and emulate a breadth and depth of attacker TTPs to align with the MITRE ATT&CK framework to improve your security program
- Confidently report quantifiable data on your current security posture
- Capture evidence required to convincingly demonstrate security effectiveness and show the value of your security investments

Know your organization is prepared to defend against attacks

CISOs must prove their security defenses are effective against today's cyber threats

CISOs and their teams are tasked 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 ability to protect critical systems.

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

Mandiant Security Validation, informed by Mandiant frontline intelligence, can automate a testing program to give you real data on how your security controls are performing. This solution provides visibility and evidence on how well your security controls work against threats targeting your organization and quantifiable data to direct improvements to your security environment. Security Validation enables security teams to emulate real attack behaviors against security controls authentically throughout the attack lifecycle and the entire security stack.

Intelligence-led security validation

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.

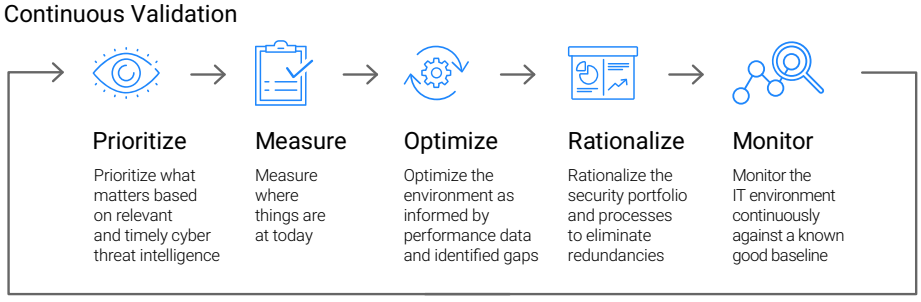

FIGURE 1. Mandiant five-step intelligence-led validation methodology.

Operationalize threat intelligence

Security Validation seamlessly integrates with the Mandiant Threat Intelligence to guide your security validation strategy and provides access to the latest and active attacker tactics, techniques, and procedures (TTPs) for testing. Security Validation arms security teams with the ability to identify and research high-priority threats with Threat Intelligence module. With a click of a button, teams can run security evaluations against their security environment with actual attack behaviors.

Cloud content delivery service

Security Validation is synchronized with cloud content curated from incident response engagements. New validation content is automatically delivered as it is published—there is less wasted time between knowing about a threat and validating your ability to block or detect attacks. Automated content delivery ensures scheduled jobs only run authentic and current evaluations.

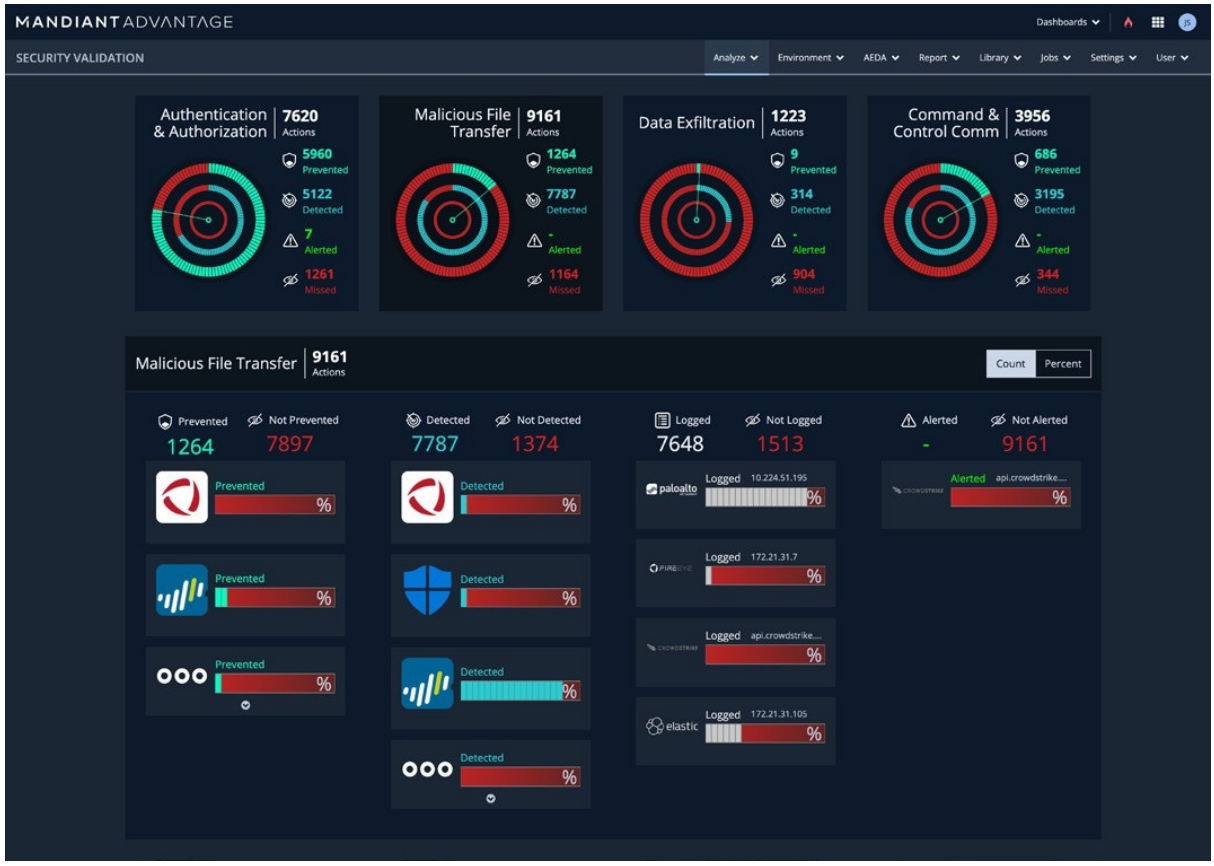

FIGURE 2. Security Validation Dashboards helps visualize how your controls are performing under attack.

Use cases that address critical questions

- **Security infrastructure health** to answer, "Are we prepared?" Through automation and continuous validation, you can capture quantifiable data on the efficacy of your security infrastructure against today's threats and identify gaps, misconfigurations, and areas of improvement before a breach occurs.
- **Attack framework alignment and assessment** to answer, "What is our competency?" Automate your use of the MITRE ATT&CK framework with not only a breadth of coverage of relevant techniques, but also access to a depth of attacker TTPs required to assess your security posture against best practices.
- **Operationalization of threat and adversary intelligence** to answer, "Who is attacking us, and why?" Gain visibility and performance data into how your controls perform against the latest attacks and adversary behaviors. This quantifiable data, with accuracy ensured by active threat intelligence, enables security teams to answer critical questions with confidence.
- **Advanced malware threat defense** to answer, "Can we prevent specific malware?" Safely and proactively test your security defenses to understand if you can withstand malware and ransomware campaigns conducted by a broad range of adversaries and top ransomware families.
- **Cyber security spend rationalization** to answer, "Are our technology investments working?" Gain confidence that your security investments are maximized and redundant controls are consolidated to recoup budget for other needs. Enable data-driven decisions to optimize security effectiveness and make the right investment decisions for the future.
- **Technology evaluations** to answer, "Can we make data-driven technology decisions?" Conduct technology assessment and side-by-side comparisons that capture data on which tools perform best in your security environment.

Security Validation for organizations of all sizes and needs

About the product:

- **Security Validation** is a cloud-based solution that enables your security team to build a continual and automated validation program that tests the security effectiveness of network, endpoint, email and cloud controls across technology, teams and processes. Intelligence-led, Security Validation helps pinpoint gaps, misconfigurations and areas that require immediate attention before an attack occurs.