Mandiant

EBOOK

# The Definitive Guide to Security Validation

Why the market has evolved beyond Breach and Attack Simulation

# The Evaluation of Security Investments

Many organizations can often underestimate their level of cyber risk or overestimate the strength of their security controls. When it comes to cyber security, they cannot afford to make mistakes because the cost of a data breach is incredibly high. For some organizations, the impact of a breach can cause irreparable financial and reputational damage.

Cyber security effectiveness needs to be objectively measured on an ongoing basis, not only to ensure established systems and tools are reducing an organization's exposure to risk, but also because CISOs are more often being asked to measurably improve and demonstrate the value of their security investments across people, process and technology to their stakeholders.

To identify a solution, you first need to quantify the problem. You cannot improve what you do not measure, just as you cannot fix what you cannot see. Breach and Attack Simulation solutions are not sufficient for gaining detailed visibility into the performance of security tools or for proving the business value of security investments. Thus, they cannot help clearly identify or solve security issues.

To identify a solution, you must first quantify the problem with data-driven evidence—the first step toward identifying any solution.

You cannot fix what you cannot see.

# The Evaluation of Security Testing

Over time, security tools have become more advanced and more automated. For many years, organizations have been able to take advantage of penetration testing, red teaming and breach and attack simulation.

- **Penetration testing** activities authorize personnel to simulate attacks on specific areas of an organization's environment to evaluate security systems. This approach only provides limited insights into a narrow area of a security program at a particular time.
- **Red teaming** exercises mobilize a skilled and authorized security team to act like attackers with concrete objectives to assess cyber risk and expose security vulnerabilities. This approach only offers a snapshot of performance within the boundaries of the authority granted to conduct the exercise.
- **Breach and attack simulation (BAS)** solutions are designed to simulate attack scenarios in an attempt to bypass security control systems and evaluate their ability to detect threats and respond accordingly. This approach lacks the ability to quantitatively measure effectiveness and support business outcomes.

BAS was an important entrant to the market when it was identified by Gartner as a category. But it is no longer sufficient to provide organizations with the insight they need to improve effectiveness.

## Security Validation

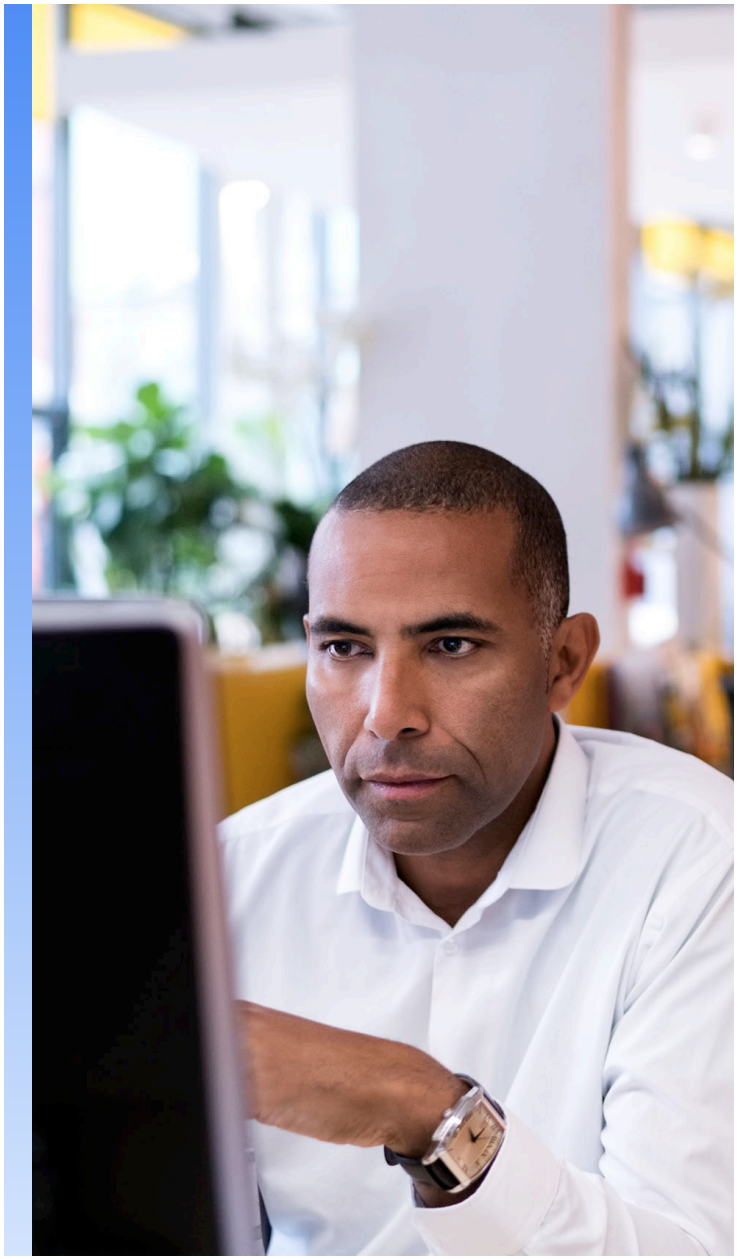
Cyber innovations now enable teams to emulate attackers during the controls testing process. This approach enables security teams to safely deploy real attacks—informed by authentic, relevant and active threat intelligence—in an organization's environment to validate controls against current threats and quantify the degree to which controls are optimized and configured.

The shift to security validation is dramatically changing the security market.

# Moving Beyond the Limitations of BAS

Breach and Attack Simulation is a category of security solutions designed to simulate attack scenarios in an attempt to bypass security control systems and determine if they are detected and/or responded to as expected. BAS tools deliver an analysis of how controls performed against specific attack exploits.

BAS solutions attempt to bypass security control systems, which is not the same as replicating an authentic and active attack. This is a critical weakness of BAS.



# Five Considerations When Comparing BAS with Security Validation

The security industry generally assumed that BAS provided a comprehensive view of an organization's cyber security posture. It does not. While many traditional BAS vendors have begun to label themselves as security validation, effective security validation requires a specific set of capabilities and content to generate the evidence security teams need to confidently prove security effectiveness.

## 1. Simulated attacks are incomplete, reverse-engineered, neutered and not genuine. They are often not recognized by security controls as a threat.

Real attacks matter. When controls see but do not alert on a simulated attack, it can provide security teams with a false sense of security. AI and machine learning only exacerbate the scenario by learning the manufactured behaviors that cause false positives in detection. When the goal is to generate a quantifiable view of effectiveness, organizations need to know whether a solution is simulating or emulating an attack. Otherwise, they risk inaccurate test results and a false sense of security.

## 2. Complete attack lifecycle visibility is a must. BAS solutions are often focused on post-exploit attacks.

To successfully test an enterprise security program, organizations need to be able to safely perform attack behaviors with full attack life cycle visibility. Visualizing how security controls perform against all stages of an attack provides actionable insights to security teams.  A lack of visibility delivers test results that may lack critical information. Without sufficient visibility, security teams must deal with an expanding attack surface that they cannot proactively identify and protect.

### 3. Integration across the security stack enables comprehensive testing of security performance. Traditional BAS solutions have improved integration capabilities, but remain heavily focused on endpoint security controls.

Many BAS vendors emphasize testing endpoint controls and lack comprehensive integrations with the entire security stack. With limited integration, BAS technologies may be able to determine how the an endpoint performs after being compromised, but may not be able to pinpoint the point of entry of an attacker if another threat vector (such as the network) was targeted. For comprehensive testing, integration is required with the entire security infrastructure of network, email, cloud and endpoint.

### 4. Testing content informed by timely threat intelligence is critical to any effective testing technology. BAS lacks content based on authentic and active intelligence.

As with many testing platforms, BAS uses a content and attack library based on attack data; its testing is only as good as its data. Without access to real and active threat intelligence, test results may be inaccurate and limit a team's ability to defend against the threats relevant to their organization.

### 5. Continuous monitoring for environmental drift is critical to ensure security infrastructure health and accurate testing. BAS does not offer this capability.

After fully testing its environment, an organization captures a view of its security posture at a particular moment in time. However, IT environmental drift, or changes to an organization's infrastructure can impact the effectiveness of security controls. When left unchecked, this can present an opportunity for compromise by attackers, increasing organizational risk. Continuous analysis, detection and remediation of environmental drift is a critical success factor that BAS solutions do not provide. Testing with the ability to alert on and remediate environmental drift will significantly enhance an organization's ability to maintain operational competency and manage cyber risk.

# Why Emulation Sidelines Simulation

BAS depends on an inconsistent model of reverse engineering and simulation. These solutions often focus on the replication of post-exploit attacks. This can often result in one-off testing of a security control with limited integration across the security stack.

Conversely, security validation safely runs real attack binaries based on authentic, relevant and active threat intelligence. Threat intelligence and incident response data would contribute unmatched adversary visibility—frontline intelligence on what the attackers are doing right now. Informed with this knowledge of who or what may be targeting their organization, better security validation solutions enable security teams to:

- Access frontline intelligence that informs validation content
- Gain adversary visibility and breach intelligence to provide knowledge of who or what may be targeting an organization, industry or region and shape validation strategy.
- Safely execute attack behaviors and destructive attacks (malware or ransomware) with full attack lifecycle visibility
- Align actionable test results with enterprise business outcomes
- Identify opportunities for optimization and rationalize security investments with real-time performance data
- Gather the evidence required to prove security effectiveness and competency against today's aggressive adversaries and their attacks.

Regardless of perceived similarities between BAS technologies and security validation, and claims by vendors of comparable functionality, the distinction remains clear: attack simulation does not represent a comprehensive assessment of security effectiveness and proof of competency.

# Prove Security Every Day

## Mandiant Security Validation

Mandiant Security Validation is a modern approach to measuring security effectiveness that conducts real attacks across the full attack lifecycle—including pre-and-post-exploitation—to accurately detail the effectiveness of your organization's security posture.

Our intelligence-led validation shows how security controls respond to a real attack. Security Validation provides quantitative insights into gaps, overlaps and opportunities for optimization. Our solution also allows you to monitor environmental drift within IT and enables measurement of improvements.

Security Validation goes beyond point-in-time analysis; it is an automated, continuous practice that delivers quantitative data on the efficacy of security controls across technology, people and processes. It also provides the evidence you need to prove the value of your investments and optimize your cyber security program.

Using Mandiant Security Validation, a U.S. Insurance provider reported an 89% improvement in the execution of Splunk notable events, directly impacting their incident response rates.

# Methodology for Success

Confidence in security effectiveness and the ability to optimize or rationalize a security program can only be gained through continuous, accurate and relevant validation of security controls. Mandiant applies a rigorous approach to security validation.

## Mandiant Security Validation delivers:

**Cost reductions** by highlighting areas of redundancy, which enables teams to streamline their security controls and remove any duplicated tools.

**Proven effectiveness** with evidence on the organization's security posture that teams can communicate to stakeholders across the business.

**Optimized cyber security** as a result of continuous monitoring and alerting on any unexpected changes in your organization's infrastructure; defense regressions can be remediated to ensure security performance.

A U.S. Healthcare provider reported $2.4m of recouped investment due to exposing inefficiencies after deploying Mandiant Security Validation.

## 1. Mandiant Threat Intelligence and adversary visibility

Mandiant pairs unparalleled, to-the-minute threat intelligence with security controls validation technology. This intelligence-led approach to security validation helps you prioritize your resources to defend against the threats that matter most.

## 2. Emulation of Real Attack Binaries

The Mandiant Security Validation platform enables the safe execution of real attacks—binaries, behaviors and malware. Safe detonation of active attack behaviors and destructive malware or ransomware is a unique functionality that enables you to comprehensively measure your organization's security effectiveness across multiple threat vectors. This functionality can renew and legitimately heighten your confidence in your organization's security posture.

## 3. Attacks are conducted across the full attack lifecycle

You cannot effectively assess areas for improvement by testing only one phase of the attack lifecycle. By using active and authentic attacks across the full attack lifecycle—pre-and-post attack exploits—integrated with an organization's entire security infrastructure, you can accurately validate and prove your organization's security posture.

BAS technologies primarily focus on the post-exploitation of attacks and have limited integrations across an organization's security stack. This can lead to inaccurate results which lack the contextual insight needed to report on security posture and shore up defenses.

## 4. Automated monitoring and remediation of IT environmental drift

Changes to the IT environment that are "unseen" by the security team can create opportunities for attackers because these changes can impact the effectiveness of security controls. The Mandiant Security Instrumentation Platform automates the testing of network and security zones with customized frequency to detect and alert on any changes to environmental configurations, ensuring security controls are working as expected.

# Security Validation is informed by Mandiant Threat Intelligence

Over the past 15+ years, through investigations, incident consultancy and red team exercises around the world, Mandiant has created and curated a unique portfolio of threat intelligence which is constantly updated with ongoing threat data, human expertise and analytic tradecraft.

Mandiant now dominates the field of cyber threat intelligence, collating, curating and rating threat data from four sources:

## Breach Intelligence

As the industry's premier incident responder, attending 1000+ incident response engagements annually, only Mandiant has an unrivaled vantage point into the most recent cyber attacks, the adversaries behind those attacks and up-to-the-minute knowledge of their activities.

## Adversarial Intelligence

Mandiant deploys 300+ intelligence analysts and researchers located in 23 countries. We collect up to 1 million malware samples per day from more than 70 different sources. Our intelligence analysts are deeply entrenched where cyber attackers plan, design and execute their attacks, giving our clients early visibility into hacker motives and cyber security trends.

## Machine Intelligence

We have approximately four million virtual guest images deployed globally in 102 countries, generating tens of millions of sandbox detonations per hour, confirming 50,000-70,000 malicious events per hour.

## Operational Intelligence

The Mandiant Managed Defense team performs detection and response services for over 300 customers from four international cyber threat operations centers, ingesting 99 million+ events and validating 21 million+ alerts. This continuous monitoring enables us to identify emerging global threat campaigns within specific organizations or industry verticals.

Google Cloud

For more information visit cloud.google.com
M-EXT-EB-US-EN-000373-04