MANDIANT

WHITE PAPER

Validation for Security Effectiveness

Five critical steps to prove the return on security investments

> Security validation allows you to know whether you’re competent, and it gives you a way to clearly communicate that competency to your executives.
>
> **– Kevin Mandia, CEO, FireEye**

Introduction

Cyber security has evolved over the last several years, shifting from a compliance-driven mandate to being recognized as critical to business continuity and profitability. Now CEOs, boards of directors and shareholders not only want to understand the relevance of security, but also ask their IT leadership to demonstrate its value and overall contribution to the business.

For CIOs and CISOs tasked to respond, security validation is an impactful way to both attain empiric evidence that security controls are working as they should and report to the CFO office and business leadership that the company is achieving and improving its accepted level of risk.

Security validation enables CIOs and CISOs to answer questions such as:

- How does risk stemming from targeted threats impact the business? What threats are relevant? Can we effectively stop them?
- How can we maximize the return on our security investments? What is the right amount of focus in spending, time and resources?
- If a breach occurs, how will the company do in a third-party assessment?
- In times of crisis, how do we maintain operations and deliver the products and services our customers need? Can we securely support a remote workforce?
- Ultimately, how does the security team prove its value and instill confidence from across the company?

Impact of Cyber Security Effectiveness

Four areas of the business are acutely impacted by security and must be considered when measuring and reporting on cyber security performance: business continuity, asset protection, regulatory and compliance requirements and spend justification.

Business Continuity

The industry definition of business continuity has evolved from describing an organization's ability to recover from disasters to becoming a priority metric of an organization's ability to maintain operations in a high-stakes security event, such as a ransomware attack. Recent breaches and attacks worldwide have reinforced the importance of validating that established controls, people and processes are working properly because the consequences can range from temporary downtime to permanent debilitation.

Asset Protection

Corporations rely on their assets—intellectual property (IP), research and development, customer and patient data, operational intelligence—being accessible and protected to maintain operations. Generating evidence that firmly demonstrates how the organization protects those assets has become an important function of the security organization. And the critical difference between success and liability or loss requires the ability to prove that controls are effective against infiltration, exfiltration and compromise.

Regulatory and Compliance Requirements

Reporting on adherence to regulations and compliance continues to evolve beyond a static report to generating ongoing proof of effectiveness. Having verifiable evidence that will support compliance with regulations such as GDPR, PCI, SOX and HIPAA will put an organization in a position of strength when faced with the need to demonstrate compliance.

Spend Justification

Rising security costs put greater demands on security leaders to not only demonstrate the value of their organization's investments but to justify their spend. Tightening budgets only accelerate focus in this area.

The three questions security leaders must answer more often:

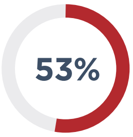
- Can I prove that I'm getting the full potential and ROI out of my security stack and specific products?
- Do I have evidence of capability overlap to prove that divesting one technology will not detrimentally impact our overall security posture?
- Can I empirically demonstrate evidence of risk and justify the need for expanded investment?

Security validation can help meet critical business mandates related to these areas and prove value to company executives. As security validation becomes a more essential capability for companies worldwide, organizations that embrace and adopt the needed capabilities will be in a better position to defend against the rising tide of ransomware and phishing attacks, data breaches and other forms of malicious threats while they sustain, or even improve, operational performance.

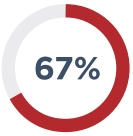
The Need for Security Validation

The recently published Security Effectiveness Report 2020, A Deep Dive Into Cyber Reality, revealed statistics that point to the need for continuous security validation to ensure optimal performance.

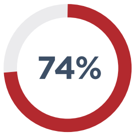
The results of testing conducted by the Mandiant Security Instrumentation Platform in enterprise production environments, compiled by the Mandiant Solutions research team, echo the need for improving security effectiveness:



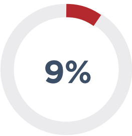
53% of organizations are unaware that an attack is active in their environment



More than 67% of attacks executed are not prevented



Roughly 74% of the attacks tested in production environments go undetected



Only 9% of attacks detected are correlated by SIEMs and generate an alert

The reasons for these security breakdowns are most often attributed to misconfigured tools, particularly as changes in the IT environment impact performance of the security stack. Security teams don't always have proper visibility when changes are made in the environment and are therefore unable to proactively address how those changes impact security performance.

Research shows that the global median dwell time, the duration between the start of a cyber intrusion and its identification, is 56 days. Cyber security practices have improved greatly since 2011, when the global median dwell time was 416 days, but still—a sophisticated attacker needs only a few days to gain access to a company's critical assets, so there is significant room for improvement.[1]

Of all the malware families Mandiant experts observed in 2019, 41% had never been seen before.

Furthermore, 70% of the samples identified belonged to one of the five most frequently seen families, which are based on open source tools with active development. This demonstrates that not only are malware authors innovating, but cyber criminals are also outsourcing tasks to monetize operations faster. Of the attacks that Mandiant professionals responded to, most (29%) were likely motivated by direct financial gain through extortion, ransom, card theft and illicit transfers. The second most common type of attack (22%) was data theft, likely in support of intellectual property or espionage end goals.

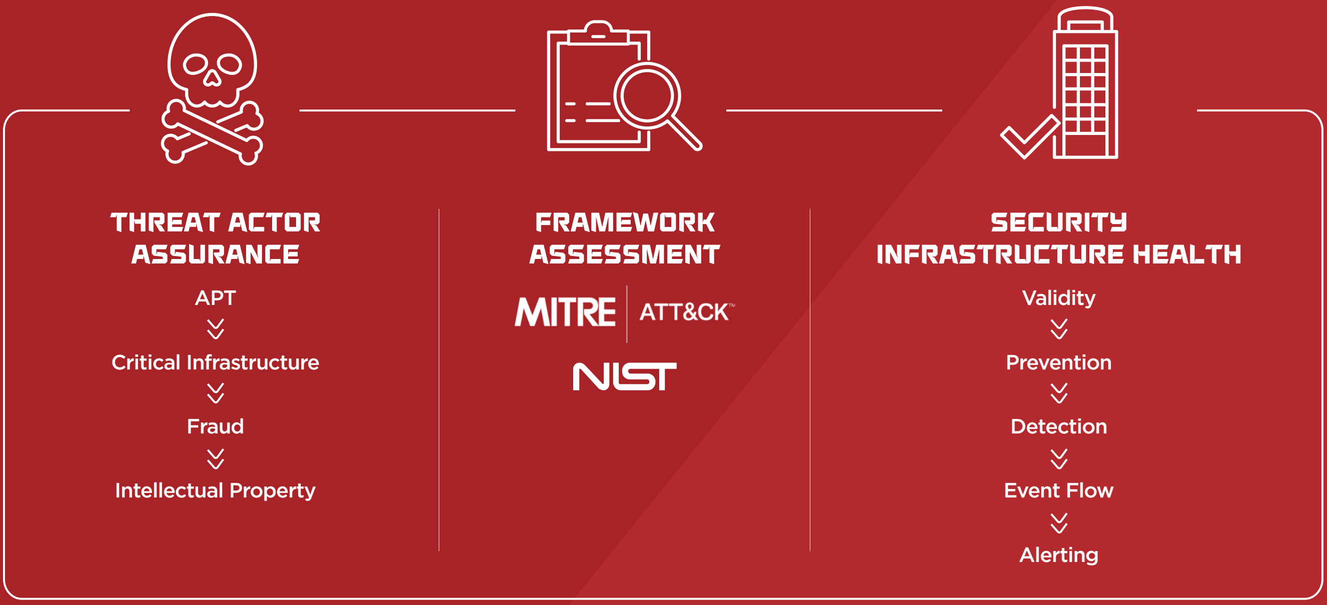
Both reports offer proof that while security investments are going up, attackers are getting smarter and a lack of security effectiveness means that threat actors are still finding ways to penetrate corporate networks and devices. This has the potential to come at the significant expense of a company's brand reputation and financial strength.

[1] FireEye (Feb. 2020) – M-Trends 2020

The Fundamentals of Security Validation

Given existing challenges and research, CISOs and CFOs must be able to validate performance of their security investments. Validation is about aligning a cyber security program with desired business outcomes, such as cutting costs, reducing risk or protecting the brand, particularly when measured against the threats most likely to target the company. It's about taking a deep look at the health of the security infrastructure to establish a baseline from reliable data so the organization can prioritize and maintain a steady, continuous process for monitoring effectiveness.

BUILDING AN EFFECTIVE SECURITY VALIDATION PROGRAM



THREAT ACTOR ASSURANCE

APT

Critical Infrastructure

Fraud

Intellectual Property

FRAMEWORK ASSESSMENT

MITRE | ATT&CK™

NIST

SECURITY INFRASTRUCTURE HEALTH

Validity

Prevention

Detection

Event Flow

Alerting

Threat Actor Assurance

After establishing a baseline and prioritizing needs against industry frameworks, security teams should communicate ongoing activity to business leadership and continuously validate against an evolving environment. Overlaying adversary-centric testing in a security effectiveness program enables a security team to use context about adversaries to proactively test the organization against typical attack tactics. As a result, the organization can focus on validating that it is protected against specific criminals and nation state threat actors that it specifically sees and that typically target the organization's industry. The organization should be sure to consider external intelligence from solutions already paid for so the security team doesn't have to waste time trying to write and debug code to parse and load data into the system. Look for an open and extensible platform that can easily integrate with extant tools in the security stack.

Framework Assessment

After establishing a baseline of health, organizations should understand how they are performing relative to industry frameworks such as MITRE ATT&CK or NIST. However, coverage on its own is not enough; it's not sufficient to have one defense covering each attack stage because the security stack should be resilient against adversaries that change and adapt quickly. To fully represent the variety of actions an adversary might take during an attack and prioritize those relevant to the target environment, a security team needs access to a deep library of techniques across the attack lifecycle that represent the full adversary landscape. There are hundreds of areas to focus on—the ability to map to tactics or techniques that are most relevant to the target organization requires a detailed knowledge of likely attackers and their motivations.

Security Infrastructure Health

A security validation program requires the establishment of a baseline for the health of the organization's system of systems. If the environment is not healthy, whether due to misconfigurations or environmental drift, then you cannot generate reliable results and actionable outputs. Even in the most mature, enterprise environments, 53% of attacks infiltrate and only 9% of them generate alerts.[2] An accurate baseline is critical for security tools' effectiveness.

[2] FireEye (May 2020) - Security Effectiveness Report 2020, A Deep Dive Into Cyber Reality

How to Implement a Continuous Security Validation Program

Proper execution of a continuous security validation program requires a five-step methodology through which security leaders can prioritize, measure, optimize, rationalize and monitor the security stack. Through this process, security validation shows where vulnerabilities exist in relation to relevant and timely threat intelligence and where to optimize tools to improve the ability to defend and respond to attacks. The combined result allows you to achieve realistic security objectives for the organization given its risk tolerance.

Security validation done right 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. There are several steps to implementing a reliable security validation program:

Prioritize what you are going to measure based on relevant and timely cyber threat intelligence

Measure where you are today

Optimize your environment as informed by the identified gaps

Rationalize your portfolio and processes to eliminate redundancies

Monitor your environment continuously against a known good baseline

Validation vs BAS

A Breach and attack simulation (BAS) solutions are widely used to test how security controls respond to specific exploits. BAS vendors may claim that these solutions are security validation, but they are not. The methodology for BAS solutions is to target the environment with simulated—not real—attacks to generate binary pass/fail ratings. This approach is useful if a company wants to answer the question, “Is my environment susceptible to attacks?” However, BAS does not answer questions such as: “How did the threat get inside? How did my controls behave? Where and what can I do to correct the issue so a real attack doesn’t get through?” BAS products don’t focus on how a security program reacted to attacks and what to do about security controls.

True security validation provides security teams with detailed information about how security controls behaved during the attack across the entire attack lifecycle, what happened and what must be done to fix it. It also allows the continuous measurement of an organization’s security posture to determine if it is regressing or improving over time, and again, what to do about it. Validation is not only “point in time” analysis; it is a continuous practice that every security team should adopt.

1. PRIORITIZE

Use threat intelligence to understand what threats matter most

Operationalized threat intelligence integrated within the security validation process can help a company prioritize resources to focus on defenses against threats to which it is most susceptible. By identifying the most relevant and impactful threats targeting your organization, you can test against the same behaviors your adversaries use to breach other companies.

This enables you to:

- **Proactively identify threats**
- **Influence investment by aligning business risk and security programs**
- **Align cyber security technology, security programs and resources against the most likely threats and actors**

1. PRIORITIZE

Considerations

Should you test with real attacks or simulations?

Using real-world adversary tactics, techniques, and procedures proves true security effectiveness. Simulated, incomplete, and defanged attacks are not genuine and provide a false sense of security. Blocking a pseudo-attack isn't the same as blocking a real one.

What does comprehensive threat coverage include?

Effective validation requires an equal focus on both technical attacks and adversary tactics across multiple attack vectors. When there is imbalance you can end up with a limited or biased assessment of your controls. These three examples of imbalance illustrate this point:

- A limited focus on malware excludes testing on real-world techniques like the use of what's already on the system, such as PowerShell, also known as "living off the land."
- A limited focus on one attack vector, such as endpoint, means you're only focusing on part of your attack surface.
- Overly focusing on the latest attacks leaves out a large number of attacks still successfully being used by adversaries.

Required capabilities

Open & extensible platform

Effective technology platforms are open and extensible in order to make it as easy as possible for users to accomplish all of their objectives. Critical tools in security validation are direct integrations to easily interoperate with existing security technologies, the means to add custom content, and the ability to interact with a bi-directional API and SDK. Leveraging real indicators of compromise and the means to upload and edit malicious network packet captures into safe actions also demonstrates extensibility.

Automated controls discovery

With just a SIEM or log source integration in place, the platform should automatically discover your security controls. This allows for rapid onboarding and capture of high-level effectiveness for these controls and helps you get value from the platform more quickly.

Operational & infrastructure health

Adding additional technologies and processes typically increases cognitive load with additional maintenance required to keep it operating. The platform should minimize maintenance work and highlight unexpected changes, ensuring it is operating correctly on an ongoing basis, presenting users with an operational readiness dashboard that helps onboard quickly and monitors the platform to ensure it is functioning correctly. A focus on infrastructure health will confirm, for example, that time is in sync across an organization and that networks haven't changed unexpectedly.

2. MEASURE

Test against known adversaries

When it comes to cyber intelligence and adversary visibility, a critical aspect of security validation is the ability to execute real attacks safely in a production environment across the full lifecycle of the attack kill chain. Real attacks provide a clear view of how well technologies are performing independently and alongside policies, processes and people; how they see and interact with the aspects of attack binaries that attack simulations simply can't do. To properly measure effectiveness, the ability to test against adversary techniques and technical attacks is critical.

2. MEASURE

Considerations

- How can the relevance of threat intelligence and exposure to a likely attack be measured?
- How can an accurate quantified baseline of the effectiveness of a company's current cyber security level be set, given the existing technology stack, policies, and people?
- How will you gather qualitative evidence to demonstrate effectiveness?
- How will you use the qualitative evidence of controls behavior and performance to drive improvement?
- How will you accurately assess security infrastructure health?

Required capabilities

Execution of real attack binaries

Robust testing requires the ability to safely execute attack binaries (that are not altered, neutered or simulated), behaviors, files, ransomware, malware, sequences and permutations within a production environment, and authenticate actors. This potentially enables the full lifecycle of an attack to be observed, both pre- and post-exploit.

Complete kill chain visibility

Rather than relying on a reverse engineered or neutered form of an attack, it is better to execute actual binary of attacks, behaviors, ransomware and malware to enable full visibility and analysis across all stages of the kill chain versus the limited results of just a post exploit perspective.

Open content platform

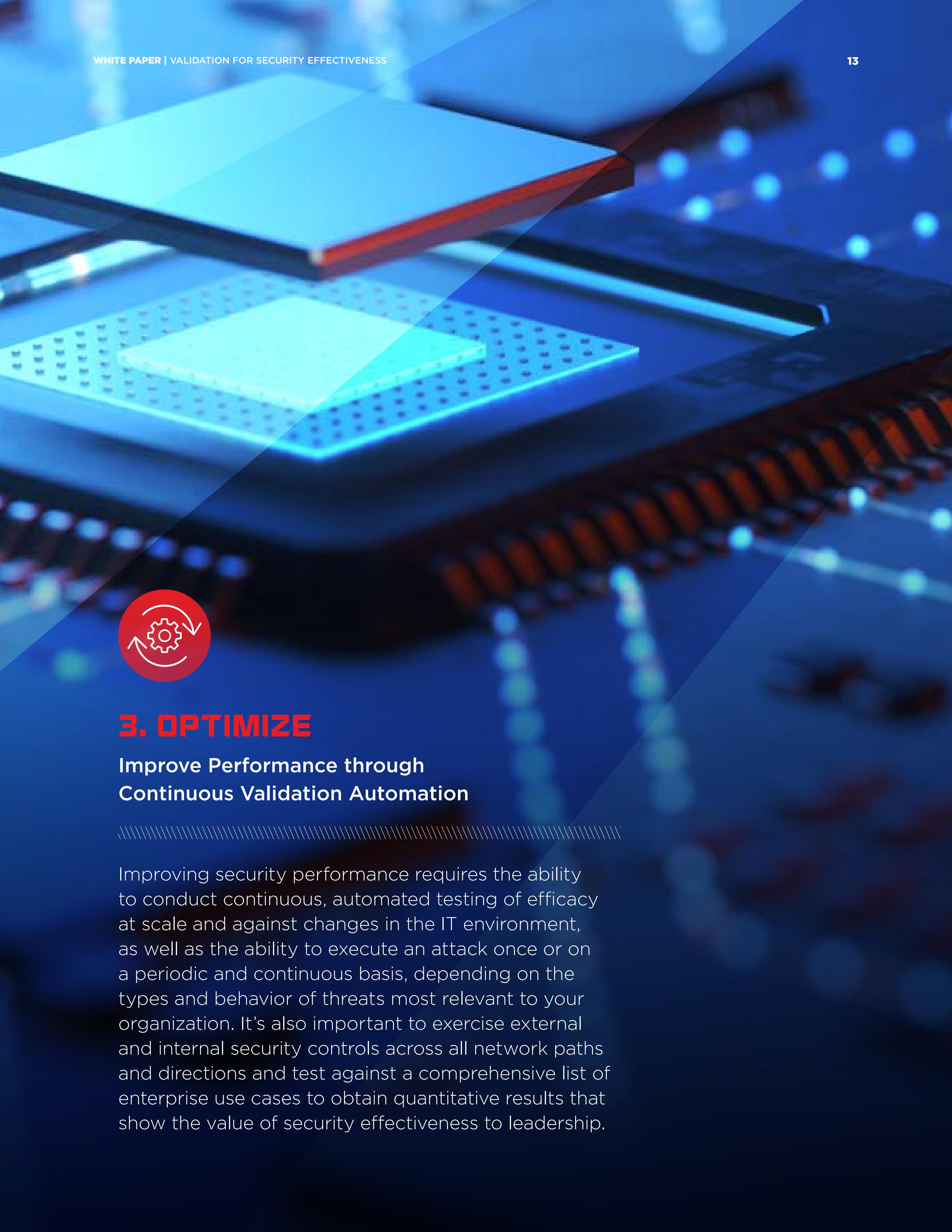
An open content platform should deliver the ability to consume custom attacks through Python and Powershell; ingest, weaponize and execute PCAPs in a live routable attack session; import threat intelligence to weaponize and execute over the platform, emulating actual actor-known techniques and tactics; provide mechanisms to share actions, simulations, PCAPs and other content via import and export functionality; and offer the ability to export all testing results.

Execution of multi-layered and multi-staged attacks

The platform should demonstrate tunneling, encoding, and multiple layer attack models in a production environment.

Execution of individual behaviors and attacks

It should be possible to execute or deliver individual or isolated attack actions, behaviors, files, sequences and scenarios. It should also be possible to chain such items to create attack sequences including kill chain scenarios.



3. OPTIMIZE

Improve Performance through Continuous Validation Automation

Improving security performance requires the ability to conduct continuous, automated testing of efficacy at scale and against changes in the IT environment, as well as the ability to execute an attack once or on a periodic and continuous basis, depending on the types and behavior of threats most relevant to your organization. It's also important to exercise external and internal security controls across all network paths and directions and test against a comprehensive list of enterprise use cases to obtain quantitative results that show the value of security effectiveness to leadership.

3. OPTIMIZE

Considerations

- After clearly identifying gaps and shortcomings, or in response to corporate changes in the business' risk profile, how can effectiveness be maintained or increased?
- Now that you have specific controls-based visibility, where will you pinpoint improvements across people, processes, and technology?
- How will you shift to proactive testing with real, full lifecycle attacks?

Required capabilities

Controls assurance rather than attack success

Use specific performance data for each control to inform the actions needed to increase its ability to detect, block and alert.

SIEM correlation rule analysis

Optimization technologies should provide automated SIEM correlation rule analysis and content tuning visibility that delivers evidence of execution or triggering of SIEM correlation rules based on detection, blocking, alerting and other notification of malicious behavior or attack. There should also be prescriptive correlation rule syntax for erroneous or missing correlation rule definition based on findings.

RESTful API integrations

It is critical to integrate with various technologies and capabilities, such as SIEM, SNORT, proxy, IDS, firewall, DLP, NGEN+, endpoint protection and malware analysis tools, as well as orchestration, change management and ticketing platforms. It should be possible to directly import content into the management server and work with security appliances and log data to validate attacks. Analysis of third-party products should show how well they block, prevent, detect, alert and report to the SIEM across network, endpoint, email and cloud platforms.

Threat actor assurance

The ability to consume third party threat intelligence feeds and execute genuine attack techniques and tactics helps make threat intelligence actionable and correlates validation efforts with specific actors, threats, behaviors and malware families.

Validation across IT infrastructure

Validation efforts should apply to and affect the entire network, endpoint actions, email and cloud deployments.

Correlation and alignment to frameworks

Effectiveness metrics and controls' performance should be aligned to various frameworks such as MITRE ATT&CK, NIST, ISO and PCI.

4. RATIONALIZE

Achieve Measurable Business Metrics to Quantify Effectiveness

After you have prioritized, measured and optimized, you can obtain the metrics you need to calculate business risk and the value of your investments. This also means you can gauge the implications of changes to controls and adjustments to security infrastructure, calculate efficacy of security controls detection and prevention, and show improvements on return after optimization. You can also pinpoint overlap in controls capabilities and calculate the dollar potential of consolidation and recouped investment.

4. RATIONALIZE

Considerations

- How can a financial value be attached to cyber security effectiveness?
- How can financial and resource spend be justified, costs reduced, duplication and waste eliminated, while simultaneously maintaining or increasing security effectiveness in key areas from executive communications to remote working protocols to customer data protection?
- How can financial rationalization demonstrate the alignment between the efforts of the cyber security technology stack, policies, and people with the desired outcomes, priorities, costs, and risk profile of the company?

Required capabilities

Controls-specific assurance visibility
Visibility should encompass specific metrics of assurance that show the attack posture and ability of each technology and control being evaluated to detect, block and alert on specific triggers.

Detailed flow and event evidence
Effectiveness metrics derived from raw logs, common detection alerts and suspicious events indicate where to best optimize security controls.

Ability to gauge threat families, tying back to ROI evidence

5. MONITOR

Continuous Monitoring and Testing for Environmental Drift

Environmental drift refers to changes in the IT environment—addition or removal of systems and platforms—that impact security performance. These must continually be monitored and measured. After prioritization, measurement, optimization and rationalization, you can establish a known good baseline to use for ongoing testing and ensure controls effectiveness even through environmental drift.

5. MONITOR

Considerations

- Knowing that the overall cyber security environment as well as a company's risk profile are not static, how can effectiveness and performance be monitored to inform proactive response?
- Can you maintain confidence with operational effectiveness?
- There will always be changes in the environment; how will you avoid deviations in performance?
- How will you inform the business with automated monitoring and reporting?

Required capabilities

Continuous monitoring of effectiveness

To continuously monitor the current security posture and effectiveness of controls, you need the ability to execute attack behaviors, malware, ransomware, actions and sequences based on frequency, environmental conditions or events. This will also enable you to monitor attacks and actions executed individually or in batches.

Automated alerts on environmental drift

It is critical to receive timely alerts on any environmental changes through periodic testing of network and security zones, including monitoring across physical controls, policy, configuration consistency. Any changes in the effectiveness of security controls should be immediately alerted and assessed for source and associated security risk.

Automated controls discovery

The automated discovery of security controls should include SIEM, SNORT, proxy, IDS, firewall, DLP, endpoint protection and malware analysis tools. Auto discovery of security technologies should include awareness of unknown technologies through endpoint actors' communications.

Segmentation validation

Automating the awareness of segmentation enforcement and the ability to limit communications and lateral access within the network helps discover proven communication paths across the network infrastructure.

Platform Evaluations

In addition to the five-step security validation methodology, you can ask probing questions of your potential vendors to identify the tools and platforms you will need:

- Is the solution proven in large complex environments?
- Does the vendor offer a global support team and program to ensure customer success?
- Can the solution be safely deployed in a live production environment?
- Does the solution offer flexible deployment options such as on-premises or cloud-based, or as a fully or co-managed managed service?

Measurable Business Benefits

There are several examples of measurable benefits to the business as a result of security validation, which ultimately affect the bottom line.

Mergers and Acquisitions

Security validation offers an understanding of how companies undergoing a merger or acquisition may have overlaps or gaps in controls. Through rationalization of spending, companies 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

Rather than simply look at the number of years of experience when hiring talent, CIOs can use a security validation methodology to assess an individual's potential for learning, the type of experience they have and how well certain skill sets match an organization's environment. For example, 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 employees know how to respond in a real-world attack and validate the applicability of each team member's knowledge and skills.

Brand Protection

When security effectiveness is validated, a company is at much less risk of experiencing a breach or attack, which helps preserve its brand reputation and customer loyalty.

Data Privacy and Protection

Protection of customer data and compliance with other regulatory mandates are rooted in a sound cyber security program. Through validation of effectiveness, companies can be assured that corporate governance standards are met.

Conclusion

The need to improve how companies validate security effectiveness in today's business climate is clear: attacks are on the rise, the targets of those attacks are expanding, adversaries are more motivated and their tactics are increasingly insidious. A combination of business drivers and security validation methodology (prioritize, measure, optimize, rationalize and monitor) create a powerful defense for organizations against cyber attacks, from both the technology and financial standpoints. With intelligence-led security validation you gain justified confidence in your ability to reduce risk, prove effectiveness and improve ROI.

To learn more, visit: **www.FireEye.com/validation**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.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.