Security Validation

THOUGHT LEADERSHIP PAPER

AUGUST 2025

Contents

1

INTRODUCTION

It is crucial that organizations adapt to the rapidly changing threat landscape to almost the same extent. Dynamic nature of cyber threat, emerging threat vectors and evolution of cyber threats have a significant impact on this rapid change. With the addition of complexity to this rapid change, it becomes significant for organizations to keep up with alteration at the same speed.

Traditional security measures are increasingly inadequate against the evolving techniques used by cybercriminals. Threats such as phishing, ransomware, and insider attacks have become more sophisticated, often bypassing conventional defenses. Additionally, attackers are leveraging artificial intelligence (AI) and machine learning to craft more targeted and effective cyberattacks. Organizations must stay vigilant and adopt proactive measures to safeguard their operations from these complex and evolving threats and must recognize the need for continuous threat monitoring and adaptive security measures to mitigate these risks effectively.

"Organizations must stay vigilant and adopt proactive measures to safeguard their operations from these complex and evolving threats […]"

We can see many cyber incidents that occur in such situations and result in high costs. In 2019, Capital One experienced a significant data breach that affected over 100 million customers. The breach was a result of a misconfigured firewall in their cloud infrastructure, which allowed an unauthorized individual to access sensitive data stored in Amazon Web Services (AWS). This incident underscored the importance of securing cloud environments, particularly in the configuration and monitoring of cloud resources. UK's postal service the Royal Mail was attacked by ransomware and data was stolen by the attackers in January 2023.[1] The service revealed it had experienced enormous financial costs because of the attack, including large revenue losses. Another example is T-Mobile confessed that 37 million customers had their personal and account information accessed by a malicious actor via an API attack which began on November 25, 2022, and incident was not discovered until January 5, 2023.[1] In a separate incident, T-Mobile USA informed customers of another breach of personal and account data that occurred in February and March 2023.

Problem Statement

Cybersecurity is a crucial aspect of any organization's digital infrastructure, as it protects the data and assets from malicious actors. However, many organizations are not sure if their cybersecurity solutions are adequate to protect them from the evolving threat landscape, or if they are being protected appropriately. Cybersecurity solutions may have vulnerabilities or gaps that expose the organization to potential breaches or may not be able to detect or prevent some types of attacks. Therefore, it is essential for organizations to discover any such vulnerabilities, and continuously monitor and test their security holistically, prioritizing issues based on their business requirements, and optimizing their cybersecurity controls.

The breach and attack simulation (BAS) concept aims to help organizations achieve this goal. It simulates realistic cyberattacks on the organization's network and devices and evaluates the performance and response of the existing cybersecurity solutions. By doing so, it provides insights and recommendations on how to improve the security level and reduce the risk of compromise. BAS concept also helps organizations to demonstrate their security readiness to stakeholders and customers, and to benchmark their security posture against industry best practices. With this, organizations can gain confidence in their cybersecurity and focus on their core business objectives.

2

SOLUTION

Testing

High-level Information

Given the context outlined above, cyber security testing emerges as the overarching solution. Here is a detailed explanation of testing from our unique perspective.

Cybersecurity testing involves evaluating the robustness of digital systems against potential threats. It serves as a proactive defense mechanism, akin to fortifying a stronghold against various forms of intrusion. Rather than waiting for breaches to occur, testing anticipates and prepares for potential vulnerabilities.

The essence of testing lies in its ability to unveil the hidden chinks in the armor of an organization's digital infrastructure. Through comprehensive penetration testing, vulnerability scans, and ethical hacking simulations, testers emulate real-world attack scenarios to unearth weaknesses that malicious actors might exploit. By identifying these vulnerabilities proactively, organizations gain invaluable insights into areas that require fortification, enabling them to bolster their defenses before an actual breach occurs.

Testing is indispensable for organizations facing an increasingly sophisticated threat landscape. It not only helps meet regulatory compliance but also mitigates risks by identifying and rectifying vulnerabilities proactively. In today's digital age, where cyber-attacks are pervasive, robust testing practices are paramount for maintaining operational resilience.

In conclusion, testing forms the foundation of cyber resilience by empowering organizations to stay ahead of potential threats. It fosters a culture of proactive defense, ensuring that systems remain fortified against evolving cyber risks. Embracing comprehensive testing strategies is not just a strategy but a necessity for safeguarding organizational assets and sustaining stakeholder trust in an increasingly interconnected world.

Organizations employ a variety of methodologies to conduct testing, ensuring the robustness and resilience of their digital infrastructure. These methods include but are not limited to security validation, penetration testing, red teaming vulnerability assessments and continuous monitoring mechanisms. By leveraging these diverse approaches, businesses can proactively identify and mitigate potential security risks, safeguarding their data assets and maintaining operational continuity in an ever-evolving cyber landscape.

7 Criteria

The criteria to do comparative analysis of security assessment methods are given in Figure 1.

Figure 1: Criteria of comparative analysis in security assessment methods

Efficiency and Resource Optimization (Automation)	•Maximizes operational efficiency by automating repetitive tasks, freeing up human resources for strategic initiatives
Proactive Defense through Continuous Assessment (Continuous Assessment)	•Ensures a constant state of readiness against threats by adapting to new vulnerabilities and threats as they appear, minimizing the window of opportunity for attackers.
Comprehensive Security Posture Enhancement (Assessing Security Controls)	•Strengthens overall security by thoroughly testing and improving every layer of an organization's defenses, addressing weak points comprehensively.
Streamlined Mitigation Planning	•Accelerates the remediation process with clear, actionable guidance, reducing the time to fix vulnerabilities and enhancing security resilience.
Holistic Threat Visibility (Assessment Scope)	•Provides a complete view of security vulnerabilities across the cyber kill chain, enabling preemptive action and strengthening defensive measures at each potential breach point.
Agility in Threat Response (Quick Response to New Threats)	•Enhances the organization's agility in responding to emerging threats by rapidly adapting defenses, keeping security posture robust in the face of new vulnerabilities.
Safe and Non-Disruptive Evaluation (Risk-free Assessment)	•Maintains business continuity with seamless and non-disruptive evaluations, protecting operational integrity while strengthening security measures.

3

METHODOLOGY

As a proactive approach, security validation focuses on detecting and mitigating cyber threats and risks before adversaries can exploit them. Rather than waiting to react to a security incident, this approach helps organizations prioritize exposures and reduce their attack surface by identifying and fixing weak points in systems or networks. By understanding risks upfront, businesses can protect critical assets efficiently and allocate resources effectively.

The security validation methodology has four main steps: Discover, Validate, Prioritize, and Optimize.

> "The security validation methodology has four main steps: Discover, Validate, Prioritize, and Optimize."

Discover

The first step of the security validation approach is to discover the organization's entire attack surface. The attack surface represents the sum of all possible entry points that attackers could exploit to gain unauthorized access, steal sensitive data, or disrupt business operations. In the Discover step, security teams carefully examine any system, application, or other assets and identify vulnerabilities that make up the attack surface.

The Discover step starts with creating an asset inventory and cataloging assets based on their confidentiality and business criticalness. The asset inventory mainly includes three types of assets.

- **Infrastructure assets**: Endpoints, servers, routers, switches, firewalls, printers, etc.
- **Software assets**: Applications, services, databases, cloud resources, operating systems, etc.

- **Data assets**: Financial records, PII and PHI data, intellectual property, proprietary information, etc.

Organizations should also consider ancillary assets and dependencies like third-party vendors, cloud services, and other external entities when creating and maintaining an asset inventory. Since the asset inventory of enterprise networks can be extensive and dynamic, security teams should be thorough in the Discover step and scan for new assets continuously.

Next, the Discover step continues with scanning the asset inventory to identify any vulnerabilities, deviations, or misconfigurations that could expose the organization to potential risks. Security teams often use automated tools such as vulnerability scanners and port scanners and supplement them with manual inspections to uncover security issues that may be overlooked by automated tools alone, providing a more comprehensive assessment of the attack surface.

The Discover step is concluded by documenting the identified security gaps and their severity. This documentation will be a valuable resource for guiding the security validation process in later steps.

Validate

Once the attack surface is discovered and documented, organizations can move on to the second step, Validate. In this step, security teams assess and validate the effectiveness of their organization's security controls in mitigating the potential threats and vulnerabilities within their attack surface. This step seeks to answer the question: "How well is the organization protected against potential threats?" and ascertain whether documented security gaps are exploitable and can jeopardize the organization's security posture.

In the Validate step, security teams should use automated and continuous solutions like Breach and Attack Simulation (BAS). This solution is designed to replicate real-world scenarios and attack vectors, providing insight into how well the organization can withstand potential cyber threats by mimicking adversary tactics, techniques, and procedures (TTPs). Manual and periodic approaches, such as penetration testing and red teaming, are not preferable for this step since the rapidly evolving threat landscape requires organizations to use a comprehensive and agile solution that extends beyond traditional manual security assessments.

The Validate step helps security teams better understand the risk posed by the identified security gaps and eliminate ones that are practically impossible to exploit. Throughout the Validate step, security teams carefully document their findings, including details about exploited vulnerabilities, successful attack vectors, and any weaknesses or gaps in security defenses.

Prioritize

Enterprise networks often have a broad attack surface they need to protect, and not every asset in an organization requires the same level of security and attention. The ideal approach should be to identify and prioritize the most critical areas of an organization's attack surface for focused security attention. The Prioritize step helps security teams determine which security gaps within the attack surface pose the greatest risks to the organization and warrant immediate action. This step enables organizations to allocate resources effectively, address high-risk areas first, and maximize the impact of their security efforts.

This step starts with security teams considering the potential impact and likelihood of exploitation associated with validated vulnerabilities in the attack surface. The potential impact depends on several factors, including the sensitivity of the data or systems involved, the criticality of the affected business processes, and the potential financial or reputational damage resulting from a successful cyber attack. On the other hand, the likelihood of exploitation depends on the prevalence of known vulnerabilities, the ease of exploitation, and the level of exposure to external threats.

Organizations commonly use risk-scoring frameworks and methodologies to quantitatively assess and prioritize security gaps. These frameworks assign numerical scores to vulnerabilities based on their impact and likelihood, allowing organizations to rank them in order of priority. Security teams should also consider the organization's overall risk tolerance and security objectives. Organizations may have specific risk tolerance levels or regulatory requirements that influence their prioritization decisions.

The Prioritize step is an iterative process that evolves over time based on changing threat landscapes, business priorities, and security requirements. As new vulnerabilities are discovered, threat intelligence is updated, and business needs evolve, security teams need to ensure their security efforts remain aligned with current risks and objectives.

Optimize

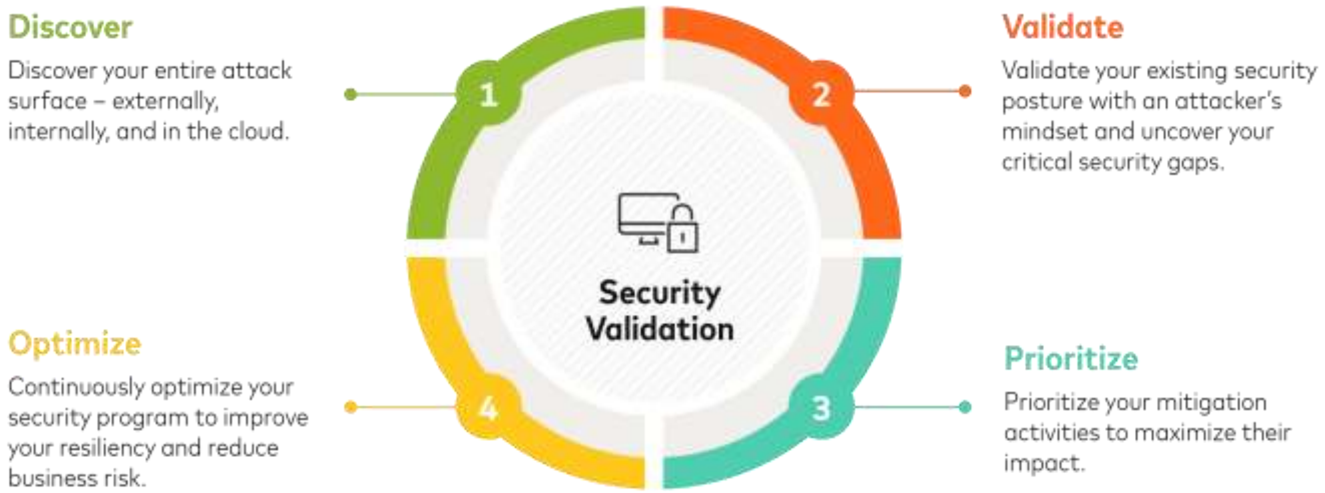
Now that security gaps in the attack surface are discovered, validated, and prioritized, it is time to remediate them and strengthen the organization’s overall security posture. The Optimize step involves addressing and mitigating vulnerabilities, weaknesses, and exposures within an organization's attack surface. In this step, security teams implement corrective actions, security measures, and controls to reduce the risk of exploitation and the potential impact of security threats.

The Optimize step starts with developing a remediation plan outlining the specific actions needed to address prioritized and validated vulnerabilities. The remediation plan may include a combination of technical controls, security patches, configuration changes, and procedural measures designed to mitigate the identified risks effectively. The goal is to implement controls that reduce the organization's attack surface and minimize the likelihood of successful exploitation by malicious actors. Implementation of remediation measures requires coordination and collaboration across various departments within the organization, including IT, security, operations, and business units. Effective communication and stakeholder engagement is essential to ensure that remediation efforts are prioritized, resourced appropriately, and executed efficiently. Additionally, organizations may leverage automation tools and technologies to streamline the remediation process and enhance its effectiveness.

Once remediation measures are implemented, organizations conduct validation and testing to verify their effectiveness and ensure that identified vulnerabilities have been adequately addressed. This may involve retesting systems, applications, or networks to confirm that security controls have been properly implemented and that vulnerabilities have been remediated successfully. Validation efforts help organizations identify any residual risks and fine-tune their remediation efforts as needed.

Similar to previous steps, the Optimize step is an ongoing process that requires continuous monitoring, evaluation, and adaptation to evolving threats and vulnerabilities. Organizations must remain vigilant and proactive in identifying and addressing new security risks as they emerge. By adopting a proactive and iterative approach, organizations can strengthen their security posture, reduce the likelihood of successful cyber attacks, and better protect their valuable assets and data from potential cyber threats.

Figure 2: Security Validation Cycle



Discover

Discover your entire attack surface – externally, internally, and in the cloud.

Validate

Validate your existing security posture with an attacker's mindset and uncover your critical security gaps.

Prioritize

Prioritize your mitigation activities to maximize their impact.

Optimize

Continuously optimize your security program to improve your resiliency and reduce business risk.

4

SECURITY ASSESSMENT METHODS COMPARATIVE ANALYSIS

In this chapter, we explore a range of cybersecurity assessment strategies, drawing analogies to familiar scenarios like home security systems to enhance understanding. By comparing and contrasting various assessment methods, such as Security Validation, Penetration Testing, Red Teaming, and Vulnerability Assessment, we provide insights that enable cybersecurity professionals to choose the most suitable and effective techniques for defending their organizations in a dynamic threat environment.

Efficiency and Resource Optimization

Imagine you have a smart home security system that automatically checks all locks and other defenses that protect your doors, windows, and other attack surfaces of your home and make sure they are locked and secured. That's the same as Security Validation, which automates cyberattack simulations against defenses without any effort on your part. Using such a method within an organization would help in using human resources for other important tasks, which boosts efficiency. On the other hand, Penetration Testing and Red Teaming are more like hiring a security expert to manually check your home. However, these approaches are more time-consuming and costly. The other security assessment method, Vulnerability Assessment, is much more like having a quick automated checkup in which common issues might be identified, but in-depth real-time testing of your security defenses like that done with Security Validation will not be conducted.

Continuous Assessment for Proactive Defense

Think about how quickly technology and possible threats to your home protection change. A system that continuously checks its defenses can keep you ahead by being able to locate and fix gaps before attackers have the opportunity to use these gaps to compromise your home. This constant vigilance is far superior to the periodic checks typical of both Red Teaming and Penetration Testing, which – by its very nature, since it is so labor-intensive – cannot be done on a continual basis. Checks are allowed on an ongoing basis by using Vulnerability Assessment, but it doesn't provide the proactive defense posture of Security Validation, making it essential for staying ahead of both internal changes and external threats.

Comprehensive Security Posture Enhancement

To make sure your home is safe from all sides, you need a full review of your security measures, like what Security Validation does. It's the same as having a security expert check each lock and alarm and monitor to make sure they all work well together. This all-around approach is better than Red Teaming, Penetration Testing, and Vulnerability Assessments, which only look at certain weaknesses, systems, or networks and don't give a full picture of how secure an organization is.

Streamlined Mitigation Planning

When you do find gaps in your security, you need clear and immediate steps to fix them. Security validation is that useful guide that actually tells you what to do, such as recommending specific mitigation recommendations for vendors of locks on your doors. This is more useful than the vague or overly technical advice you might get from a red team or a penetration test. In the case that you are sitting with an unpatchable vulnerability, such precise guidance might make the remediation process substantially quicker.

Holistic Threat Visibility

Now, think about deploying a 360-degree surveillance camera in your home. Security Validation simulates the full cyber kill chain in a way that illuminates everything and allows defense competency assessment for each step. This overall visibility ensures that no potential threat is missed, whereas Red Teaming, Penetration Testing or Vulnerability Assessments may be scoped broadly and still have blind spots.

Agility in Threat Response

Agility is key in this fast-paced world of cyber threats; get on the defense immediately when a new attack comes up. Security Validation takes it a step further in less than a day by simulating and mitigating the new threats. It is almost like a security system that will keep updating to stay ahead of hackers. The speed of this reaction is much better than that of Red Teaming and Penetration Testing, which take longer.

Safe and Non-Disruptive Evaluation

Lastly, it is very important to make sure that security checks don't get in the way of normal business. Security Validation works without getting in the way of normal activities. It's kind of like a quiet alarm test that makes sure everything works without waking up the neighbors. In contrast to Red Teaming and Penetration Testing, which can be more invasive and leave the front door unlocked, this careful balance keeps you safe and up and running.

In conclusion, as seen in the below table, Security Validation stands out as the most thorough, effective, and efficient way to check that defenses are up-to-date and working properly when these cybersecurity review methods are compared. This method takes a proactive, all-around, and flexible approach to cybersecurity, giving businesses the tools they need to stay ahead in a threat environment that is always changing.

Table 1: Benchmark among security validation methods

	Security Validation	Red Teaming	Penetration Testing	Vulnerability Assessment
Efficiency and Resource Optimization	✓	✗	✗	✓
Continuous Assessment for Proactive Defense	✓	✗	✗	✓
Comprehensive Security Posture Enhancement	✓	Limited	✗	✗
Streamlined Mitigation Planning	Ready-to-Use Mitigation Content	Limited with Generic Suggestions	Limited with Generic Suggestions	Limited with Software Patches
Holistic Threat Visibility	Entire Kill Chain	Limited by Predefined Objective	Limited by Predefined Scope	Limited by Predefined Scope
Agility in Threat Response	Testing New Threats in 24 Hours	No Response Until New Engagement	No Response Until New Pentest	Plugin Updates Happen Within 3-5 Days
Safe and Non-Disruptive Evaluation	✓	✗	✗	✓

5

USE-CASE

One of the success stories from a Cyber Front user is how they discovered a major gap in their detection capabilities. The user, a large financial institution, had deployed Cyber Front to continuously assess their security posture and validate their security controls. Cyber Front revealed that they were not getting any logs of what was happening on the PowerShell and command prompt on their web application servers, where attackers could execute malicious commands and scripts. Cyber Front helped them identify and fix this issue and provided them with actionable recommendations to improve their overall security hygiene and resilience.

Another success story from a Cyber Front user is how they improved their firewall protection and reduced their exposure to web attacks. The user, a leading e-commerce platform, had deployed Cyber Front to continuously monitor their network traffic and detect any malicious or anomalous activity. Cyber Front revealed that their firewall was not configured properly and was allowing certain protocols i.e. HTTPS to bypass inspection. This meant that they were vulnerable to attacks that could exploit encrypted traffic and various attack vectors including steal sensitive information or disrupt their services. Cyber Front helped them fix this issue by providing them with vendor-specific recommendations to adjust their firewall settings and ensure that all traffic was inspected and filtered. Cyber Front also provided them with best practices to optimize their firewall policies and prevent future breaches.

6

WHY MASTERCARD & HOW MASTERCARD HELPS

Cyber Front leveraged by Picus platform – High level information

Cyber Front is a breach and attack simulation platform that helps users validate their cybersecurity controls. This is achieved by creating an isolated space within the customer network to be a target of attacks. Cyber Front can simulate attacks designed to infiltrate customer network and email infrastructure, exploit vulnerabilities in web applications, perform malicious activities on endpoints, and attempt to exfiltrate data outside the network. Additionally, Cyber Front helps users mitigate the shortcomings detected in these simulations by generating vendor-specific signatures, queries, and related information.

Mastercard-Cyber Front-Practice Information

Mastercard Cybersecurity Team can help you with Cyber Front to continuously define and enhance security gaps and misconfigurations, settle responses and improve your defences with the most relevant simulation scenarios for your organization.

Contact us to learn how Mastercard's Enterprise Cybersecurity Platforms supports the full ecosystem resilience cycle with Cyber Insights, Cyber Quant, RiskRecon, Cyber Front, Cyber Crisis Exercise and Threat Protection.

Contributors

Süleyman Özdoğan, Ph.D.
Co-founder and Vice President
Picus Labs

Eda Boltürk, Ph.D., Assoc. Prof.
Director, Product Management, Risk & Resilience
Mastercard

Sergei Rumiancev
Manager, Software Engineering
Mastercard

Kenan Kural, CISM, CISA, CEH, CDPSE
Director, Solutions Consulting
Mastercard

Hüseyin Can Yüceel, CISSP, OSCP
Security Research Lead
Picus Labs

References

[1] *https://www.infosecurity-magazine.com/news-features/top-cyber-attacks-2023/*