Whitepaper

Breach and Attack Simulation: A Novel Cybersecurity Validation Approach

1. Executive Summary

Until the point that a cyber threat is used in a successful attack, it is just another threat amongst millions of others. Organizations keep investing in security to fight against that threat that could be used in an attack with a probability that is unknown. This is an unfair game, where the good guys often are left to fight blindfolded and subsequently are blindsided by new attacks.

A 2020 report by Accenture shows that 69% of cybersecurity stakeholders think that "staying ahead of attackers is a constant battle and the cost is unsustainable". They list as many as 17 different technological categories where the cost of investment has increased significantly.[1] This necessitates massive investment and requires continuous effort.

69% of cybersecurity stakeholders think "staying ahead of attackers is a constant battle and the cost is unsustainable".

Security vendors continually develop and improve their prevention technologies. These technologies are great at seamlessly stopping a multitude of adversary actions with easy to identify artifacts and characteristics, and this takes away a huge burden.

When it comes to sophisticatedly crafted and targeted threats, let's refer to this category as "advanced threats", security teams need to step in to boost the capabilities of their existing technologies. This is easier said than done. There are far too many security technologies to manage and advanced threats do not necessarily reveal themselves easily. This leaves cybersecurity stakeholders overwhelmed with a significant operational workload, the risk of getting breached and compliance requirements to address. On the technology side, investments are by far underutilized.

In this paper, we delve into how different validation technologies support cybersecurity stakeholders in their quest to remain resilient against advanced threats. Our view is that widely adopted vulnerability management, penetration-testing and red-teaming are not enough to produce the results that meet the "sense of urgency" requirements that cybersecurity teams face. Even though their capabilities have enhanced in recent years thanks to the new threat centric approach that the market embraces, these solutions do not empower relevant stakeholders to deal with advanced threats 24 x 7 x 365.

"Which validation solution is best for achieving continuous threat readiness visibility and gaining immediate mitigation capabilities?"

Breach and Attack Simulation has emerged as the front runner of threat centric validation approach. It fills an important gap and offers the possibility of handling security in tranquil waters. This is a comfort long time overdue and cybersecurity teams deserve on all levels.

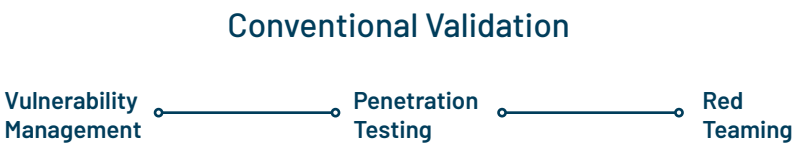
1 https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience*

2. Introduction

The cybersecurity function as a whole is the entity that protects the business against threat actors, in slightly more technical terms, protecting business applications against cyber-threats. If cybersecurity teams can build the capability of linking the two ends of this battle, the potential attacker and the potential victim, they can then gain the upper hand to invalidate cyber threats before they arrive in their networks.

Clearly, this hypothesis is not new or original. cybersecurity is a mature domain with a good number of security validation tools, technologies and services that attempt to establish the link mentioned above. On the other hand, the speed and sophistication of the ever-changing threat landscape and modern business dynamics have reduced the effectiveness of these.

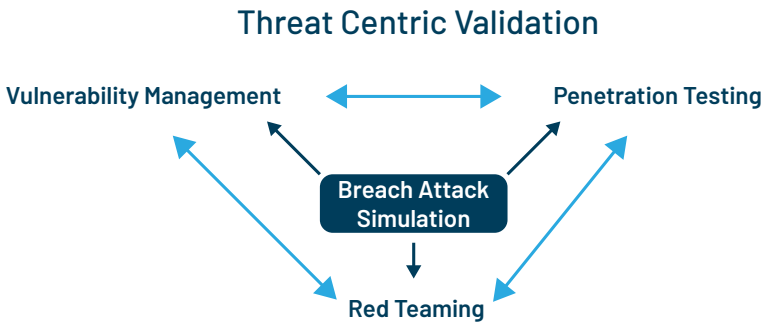
In the last couple of years, we see that a pragmatic and feasible validation approach has emerged, which the market calls a "threat-centric" approach. This approach is built on a strategy that focuses on certain threats and threat groups instead of trying to address all threats. The threat-centric approach is transforming the validation market. Vulnerability scanning becomes Threat & Vulnerability Management. Penetration testing has started offering goal oriented and threat-group focused assessments. The gap between penetration testing and red teaming is narrowing. Organizations are increasingly adapting new threat-centric frameworks such as Gartner's CARTA or MITRE's ATT&CK. The need to place threats in the center has resulted in the formation of a novel assessment domain: Breach and Attack Simulation.



In this paper, we discuss the value that threat-centric validation delivers and where each technique stands in terms of contributing to readiness against advanced threats 24x7. Advanced threats are defined as:

- threats that recently breached other organizations,
- threats identified as currently active and dangerous by the cyber-security and intelligence community.

Section 3 focuses on the requirements for effective security validation against advanced threats. Section 4 examines how vulnerability management, penetration testing and red teaming exercises score against these requirements. Section 5 discusses how Breach and Attack Simulation can help enterprises deal with advanced threats.



3. Requirements for Effective Security Validation Against Advanced Threats

If security operations are not aware and controls are not ready when an advanced threat is imminent, the chance of eliminating the risk it poses becomes more difficult and less likely. Creating the capabilities to be proactive in the fight early on is the only way to prevent and contain attacks. For such capabilities to be acquired five requirements are needed and are outlined below:

Requirement 1: Ability to Utilize Imminent Advanced Threats

The capability of being able to link potential attackers to potential victims requires security validation platforms to simultaneously manage both ends of this battle. Therefore, validation tools should contain and utilize a rich set of threat and technique samples, not only the potential victim inventory. Security assessments without the context of 'in-the-wild' samples may reveal some weaknesses such as policy mistakes or vulnerabilities, but they cannot identify readiness against advanced threats that flourish in an evolving threat landscape.

Requirement 2: 24 x 7 x 365 Validation

Security assessments for advanced threats must run 24 x 7 x 365. Threat adversaries skillfully bypass control infrastructures by continually introducing new advanced techniques. Adding into the mix that business systems and related infrastructure constantly change, having only point in time validation is not sufficient.

Requirement 3: Assessing Existing Control Capabilities

Validation processes should be inclusive of existing controls and their readiness status. In this way, the relevance of identified gaps can be understood, and prioritized. The absence of this condition can result in thousands of uncontextualized links between threats and possible victims at any given time, leading to teams that are overwhelmed by this flow of rogue information.

Requirement 4: Immediate Mitigation

Cybersecurity teams need to be empowered with the right tool set to be able to mitigate identified breach vectors in a matter of minutes. Having the visibility but not being able to quickly remediate risk gaps diminishes the objective of the overall effort.

Requirement 5: Enable Team Communication and Collaboration

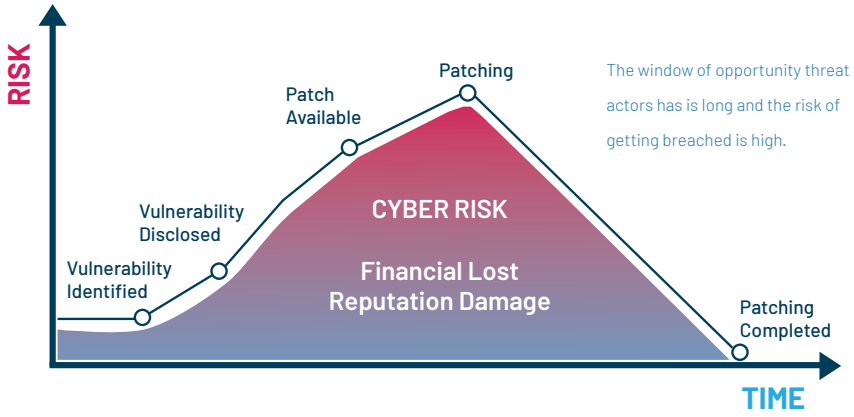
Cybersecurity organizations are comprised of many different functions and departments with different priorities and skill sets. Not every piece of information will receive the same priority across these disparate groups. The possible attacker and victim links should be in binary precision in terms of the risks they pose for every different scenario. In this way different cybersecurity departments can be involved, partnering as a team to come up with optimal mitigation or response scenarios.

In the next section we will evaluate vulnerability management, penetration testing and red teaming from the perspective of the afore mentioned requirements. This paper does not intend to compare these alternative solutions in their entirety but rather discuss their suitability for validating readiness status against advanced threats. In the last section, we will examine how Breach and Attack Simulation, as a new security assessment category, differs and addresses the requirements outlined in these categories.

4. A Brief Assessment of Vulnerability Management, Penetration Testing, Red Teaming

Vulnerability Management

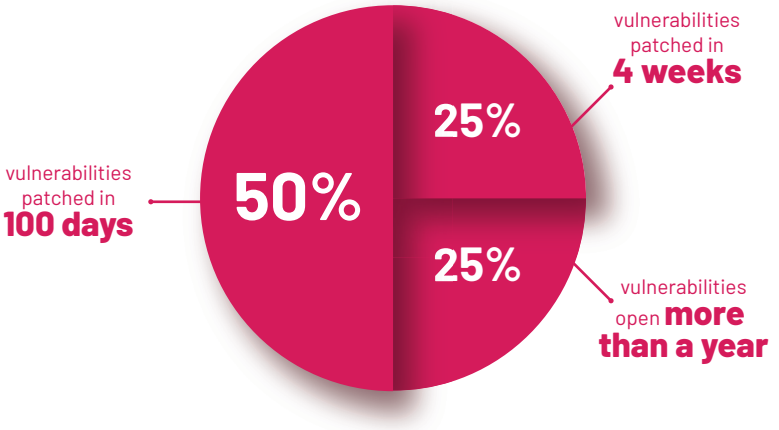
Often post cyber-breach analysis includes some commentary on how the exploited vulnerability was known many months prior to the breach and despite this publicly available knowledge, a cybersecurity team "failed" to patch that vulnerability.



Cybersecurity professionals know that prioritizing and patching vulnerabilities are lengthy, difficult and sometimes impossible processes. Based on a report by Kenna Security, in 2019, 25% of vulnerabilities were patched in 4 weeks, 50% of vulnerabilities were patched in 100 days and 25% of vulnerabilities remained open more than a year.

According to the ENISA State of Vulnerabilities 2018/2019 report[2], most of the exploits are published on average during the ±20 day period of the date that the vulnerabilities were published. This number was 12 days for critical vulnerabilities. The duration for vulnerability identification, prioritization and patching cycles is long and doesn't keep up with the speed of adversaries.

2 https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/*



Vulnerability Management is a 25 year-old technology. It has evolved significantly over the years to address the shortcomings mentioned above. Existing alternatives have acquired threat context and offer automation. Threat & Vulnerability Management, Predictive Prioritization, and Vulnerability Prioritization Platform are some of the new terms used by the vendors of this technology. Despite all the progress achieved, this domain delivers value only within its own framework, not in the framework of tackling and advanced threat in a matter of minutes.

Vulnerability management versus the 5 requirements for effective security validation against advanced threats:

Ability to Keep Up With & Utilize Imminent Threats	○
24/7/365 Validation	◐
Assessing Existing Control Capabilities	○
Immediate Mitigation	○
Enable Team Communication and Collaboration	◐

Penetration Testing

The UK's National Cyber Security Center (NSCS) describes penetration testing as "a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."

Clearly, the idea that a trusted third party challenges a network for the aim described above, resonates strongly for many cybersecurity stakeholders. This natural strong acceptance, compliance requirements (esp. PCI DSS) and increasing cybersecurity concerns have contributed to the growth of the Penetration Testing Market, which reached $920M in 2018 and is expected to grow with a CAGR of 14.9% until 2025, 50% higher than the CAGR of the overall cybersecurity market.[3]

However, penetration testing has three major shortcomings when it comes to dealing with advanced threats. Even though there are some automated penetration testing technologies, the majority of penetration testing is conducted within a certain time frame and may be repeated monthly, quarterly, etc. Penetration tests validate security on the day of the test. The customers remain on their own after the tests are completed. Secondly, most of the penetration tests are completed within a specific scope. There is no focus on revealing the efficacy of the overall control infrastructure. Finally, penetration testing does not offer any specific mitigation insight other than some general recommendations.

Penetration testing versus the 5 requirements for effective security validation against advanced threats:

Ability to Keep Up With & Utilize Imminent Threats	○
24/7/365 Validation	○
Assessing Existing Control Capabilities	●
Immediate Mitigation	○
Enable Team Communication and Collaboration	●

Red Teaming

Where penetration testing focuses on revealing weakness and vulnerabilities that may be exploited due to the security gaps within the scope of the test, red teaming takes this effort a couple of steps further. Red teams can run real threats with full attack scenarios and challenge very specific capabilities with a multi-disciplinary approach. The findings of red teams generally initiate mitigation tasks for security control teams, in other words, the blue teams.

Many organizations with mature security operations include red team practices in their security and risk management processes, either having internal teams or external engagements. Red team practices often focus on achieving specific goals with the aim of understanding organizational capabilities and ensuring that necessary corrective actions are taken on their end.

Although much more comprehensive and closer to real world scenarios, red team practices by nature cannot be fully automated and they may involve lengthy processes. Having 24x7 readiness visibility across the entire new and changing advanced threat surface cannot be achieved by relying only on red-team exercises.

Red teaming versus the 5 requirements for effective security validation against advanced threats:

Ability to Keep Up With & Utilize Imminent Threats	○
24/7/365 Validation	○
Assessing Existing Control Capabilities	●
Immediate Mitigation	◐
Enable Team Communication and Collaboration	●

3 https://www.marketwatch.com/press-release/penetration-testing-market-size-to-grow-extensively-with-149-cagr-by-2025-2019-04-09*

5. Breach & Attack Simulation: A Novel Cyber-Security Validation Approach

Breach and Attack Simulation (BAS) is the newest member of the security validation domain. In the last couple of years, a good number of publications have been released by various research companies and some vendors, with the aim of explaining how BAS differs from pen-test, red-teaming and others. This paper may seem to have a similar approach even though instead of merely comparing these different assessment tools, we intend to look at which solution is the best fit to identify and tackle advanced threats that are lurking just around the corner, ready to attack enterprise networks.

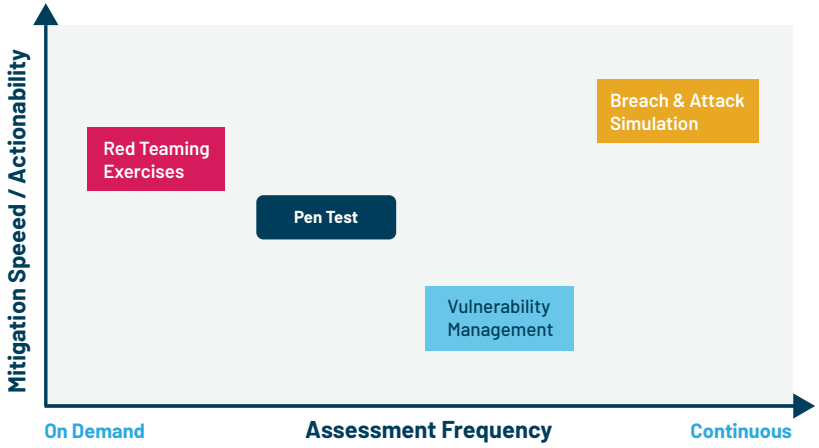
It is worth noting that BAS solutions available today have different characteristics. Some provide a rich feature set, but do not offer a comprehensive library of threat scenarios. Some have been designed to address a specific attack vector, for instance end point or web gateway. Some vendors have designed their solutions more with consultancy in mind, whereas some others are geared toward continuous validation. Some offer automated pen-testing but market it as a Breach and Attack Simulation solution. As this new market matures, the confusion will clear and these differences will become more easily discernible.

Adversaries constantly attack their targets using automated tools. Advanced threats combine sophisticated techniques and constantly introduce new variants to try to evade defenses. Keeping up with a large number of fast-moving threats requires a novel unique validation approach.

In this novel approach, a validation solution should contain:

Requirement 1: Ability to Keep Up With & Utilize Imminent Threats	A subset of the threat landscape, consisting of real threat samples and techniques, crafted meticulously and continuously to represent the actual threat landscape.
Requirement 2: 24 x 7 x 365 Validation	An automation infrastructure to keep security infrastructure under challenge 24x7, as cyber-criminals do, using the subset of the threat landscape.
Requirement 3: Assessing Existing Control Capabilities	A rich visibility output that continually reveals prevention and detection capabilities and limitations.
Requirement 4: Immediate Mitigation	A comprehensive, precise and easy to apply mitigation guidance for each threat sample, linked to every detection and prevention technology that is in use.
Requirement 5: Enable Team Communication and Collaboration	A comprehensive and easy to use platform that could produce information for different teams.

It is only by combining all the criteria outlined above that cybersecurity teams are able to manage an infrastructure that actively adapts to the threat landscape. BAS embraces these principles and is the only realistic approach to empower cybersecurity stakeholders, align processes and boost the performance of control technologies on an ongoing basis.



6. Conclusion

Security validation solutions are invaluable in keeping control technologies and mechanisms ready against cyber risks. Each different type of validation tool can provide benefit for a certain scope. Objectives of the related stakeholders should define the validation tool that is to be used. These objectives can range from finding vulnerabilities, misconfigurations, architectural mistakes, licensing non-compliance to measuring security control effectiveness, findingthird party risks, ensuring regulatory compliance and others. These elements correspond to different business objectives. One other factor in choosing a validation tool is related to the amount of time the tool will be in use, whether it is for a one-off, periodic or continuous use.

The four validation technologies discussed in this paper are complementary solutions. Vulnerability Management is key for ultimately keeping the possible target assets free from vulnerabilities. Penetration testing and red teaming can help measure the resilience of the security infrastructure against specific threat scenarios, for specific environments, under specific conditions, at the time the test is performed and with a good level of detail.

Breach and Attack Simulation is the best approach for continuous and consistent validation of security control efficacy. A key difference when compared with other tools is that BAS gets tightly integrated into security operations due to its automated architecture for continuous visibility and its focus on quick mitigation. BAS offers the chance to replicate real adversary behavior continuously, as it happens in real life. The agility that BAS offers allows organizations to build additional capabilities to empower security stakeholders, to align processes across different departments, to maximize investment utilization and to swiftly eliminate risks.

About Picus Security

Picus Security provides an intelligence driven "Breach and Attack Simulation" solution. The Picus platform empowers cybersecurity stakeholders by validating the cyber threat readiness of controls and operations 24x7, identifying gaps and providing mitigation guidance built on the largest technology alliance ecosystem in the industry.

Address:
San Francisco, USA
London, UK
Ankara, Turkey

306.001.V1 EN