EXPERT TIPS INSIDE

BREACH & ATTACK SIMULATION 101

Brought to you by ATTACKIQ

STUDY PLAN

OBJECTIVES

1. What is the definition of breach and attack simulation (BAS)?
2. How does BAS work?
3. Why would you use the MITRE ATT&CK® framework with BAS?
4. What is security optimization and what does it have to do with BAS?
5. What are the primary use cases of a security optimization platform?
6. Why is a security optimization platform a critical component of a threat-informed defense?

STUDY PLAN

STRUCTURE

1. Learn how a BAS platform functions, plus the capabilities it offers to cybersecurity teams.
2. Examine how the BAS practice has evolved over time.
3. Identify the meaning of security optimization and its role in threat-informed defense.
4. Outline 26 critical security optimization use cases, as well as their benefits to cybersecurity and risk teams.

PRIMER: WHAT IS BREACH AND ATTACK SIMULATION?

The official definition of **"breach and attack simulation"** technologies:

Gartner defines breach & attack simulation (BAS) technologies as tools ***"that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means."*** [1]

[1] Gartner, Hype Cycle for Threat-Facing Technologies 2017, Greg Young, 17 July 2017

FUNCTIONALITY OF BREACH AND ATTACK SIMULATION

- Allows enterprises to automatically emulate comprehensive, multi-stage adversary campaigns using software agents, virtual machines, and other means.
- Provides a detailed summary of results and efficacy of security controls, as well as the personnel that support them.
- Enables security analysts to find protection failures and capability gaps, strengthen security posture, and improve incident response capabilities.
- Assesses readiness and validates that enterprise security systems are performing as originally intended, guaranteeing a return on investment.
- Provides automation that enables platforms to work autonomously and at scale to support business growth.
- Enables analysts to see in real time how changes to configurations or administration can open new risks.

"Most security leaders are unsure if their implemented cybersecurity tools are working as expected. With tighter budgets, security leaders must choose, implement, and configure security tools wisely. Thus, it is critically important that the security capabilities deployed are effective, efficient, and meeting expectations. Testing controls against the known attacker behaviors that are most likely to impact the organization ensures any potential gaps are identified and can be fixed before bad actors find and exploit them."

- Stephan Chenette, AttackIQ CTO and Co-Founder

INDUSTRY CHALLENGES CREATING THE NEED FOR SECURITY CONTROL VALIDATION

- Security controls fail everywhere, and they do so constantly and silently.
- Companies deploy on average 47 different cybersecurity solutions and technologies.[2]
- 82 percent of enterprise breaches should have been stopped by existing security controls but weren't, Verizon estimates.[3]
- When a cybersecurity control fails, either through misconfiguration or operational execution, it can go unnoticed for months.
- The only way to assess cybersecurity effectiveness is, therefore, with an unquantified assessment, a **"finger in the air"** of how the program feels on a given day.

As a result, security teams are faced with three critical obstacles...

[2] https://www.businesswire.com/news/home/20190730005215/en/Ponemon-Study-53-Percent-of-IT-Security-Leaders Don%E2%80%99t-Know-if-Cybersecurity-Tools-are-Working-Despite-an-Average-of-18.4-Million-Annual-Spend
[3] https://enterprise.verizon.com/en-nl/resources/reports/dbir/2020/results-and-analysis/

1 COMPLEXITY AND INEFFICIENCY

On average, companies deploy 47 different cybersecurity solutions and technologies in their environment. There's no good way for them to ensure they're working efficiently and cost effectively without a breach and attack simulation platform.

2 THE ALTERNATIVE TO BAS FOR PENETRATION TESTING AND CONTROL VALIDATION – "RED TEAMING" – IS VERY PEOPLE INTENSIVE

Without a proper BAS platform, most organizations have a red team either on their own staff or contracted externally. Red teaming is the process of testing technologies, policies, systems, and assumptions by adopting an adversary's approach.

The challenge is that red team testing is infrequent, and the coverage delivered is therefore limited by personnel hours; as a result, coverage is unfortunately smaller than the scale of the security team's defenses. Humans can also only cover limited terrain compared to an automated solution.

3 LACK OF AN AUTOMATED CONTROL VALIDATION PLATFORM LEADS TO BREACHES

Manual control validation is also a common tactic that often leads to silent failure of controls. Security teams who rely on this tactic only leave the organization more vulnerable to breaches.

WHY BREACH AND ATTACK SIMULATION IS IMPORTANT FOR CYBERSECURITY TEAMS

A Gartner blog post pointed out that the quantification companies use to present risk and security is often expressed in terms of money and likelihood of damage. These calculations, Gartner contends, **"are often based on assumptions and 'expert opinion' that essentially dictate the result, rather than real quantitative business assessment. Using the veneer of quantification to get what you want does not support improved cybersecurity."**[4] We agree; cybersecurity teams need real quantification.

This is where breach and attack simulation comes in. It emulates real-world attacks so that organizations can test and validate how their security controls (composed of people, processes, and technologies) perform against existing threats.

- BAS is an emerging technology that is gaining attention among security professionals, according to 451 Research.

- Last year, 451 Research added BAS (along with quantum computing) to the list of selected **"emerging technologies"** highlighted in Voice of the Enterprise Digital Pulse: Budgets & Outlook 2020 study, which also includes artificial intelligence, data analytics, zero trust, and edge computing.[5]

Furthermore, as adversaries have accelerated attacks, a paradigm shift is occurring. Chief information security officers are putting a strategic emphasis on proactive prevention and insights using automation, rather than relying only on reactive detection and response controls. Regulation is increasing significantly with each year, which leads to more intrusive processes (including questions and assessments) by regulators.

[4] Smarter with Gartner, "Security Experts Must Connect Cybersecurity to Business Outcomes," 11 May 2020
[5] Report: Voice of the Enterprise: Digital Pulse, Budgets and Outlook – Quarterly Advisory Report," 451 Research 2020

By automating control validation, security teams benefit from a **"force multiplier"** effect that enables them to conduct more simulations, more quickly, and with greater insights that can be shared across red, blue, and risk teams. By taking a purple team approach, teams are able to continually improve the effectiveness and efficiency of their security programs in a dynamic and fast-paced threat landscape.[6]

> ***"The AttackIQ platform will provide a lot of value to our security program. We will have evidence that our IDS, IPS, and endpoint solution are working great. Or, if they're not, we'll know that too — and before the bad guys discover it."***
>
> - Paco Rosas-Moreno, CISO, Morgan State University

THE EVOLUTION OF BAS, FROM SECURITY CONTROL VALIDATION TO SECURITY OPTIMIZATION

The first instances of breach and attack simulation tools were relatively straightforward in their purpose: to test and validate security controls. This might include activities like validating that a firewall is configured according to company standards or testing a relevant set of controls to verify compliance with a particular standard (e.g., ISACA).[7] Breach and attack simulation platforms have evolved from threat emulation and security testing to quantifying risk management and regulatory compliance effectiveness, especially when a BAS platform is used against a compliance framework like the National Institute of Standards and Technology (NIST) 800-53 framework or sector-specific frameworks like the Payment Card Industry Data Security Standard (PCI-DSS).

[6] https://www.securityweek.com/fact-vs-fiction-truth-about-breach-and-attack-simulation-tool
[7] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/continuous-security-validation

THE EVOLUTION OF BAS, FROM SECURITY CONTROL VALIDATION TO SECURITY OPTIMIZATION (CONT.)

As cybersecurity risks have continued to increase, budgets remain uncertain, and the socio-economic impacts of the COVID-19 pandemic linger, BAS is no longer considered a tool for breach and attack simulation or security control validation exclusively — but as a way to provide business value by maximizing resources and decreasing management burdens on teams. Organizations are leveraging a new generation of innovative platforms built on BAS technology to maximize the effectiveness and efficiency of their cybersecurity program as a whole through security optimization, from technical effectiveness to regulatory compliance.

SECURITY OPTIMIZATION REQUIRES COMPETENCE IN THREE AREAS:

1. Identifying and quantifying cybersecurity risks by measuring the performance of existing security controls against actual threats;
2. Prioritizing measurements and security investments based on a **“threat-informed defense”** strategy that measures security program performance against known threat actor tactics, techniques, and procedures;
3. Continuously calibrating staff skills, processes, and technology to maintain the desired security posture, given existing budget constraints.

KEY FEATURES OF A BAS PLATFORM:

- Administrative console
- Automation software
- Test point agents for production and test environments
- An underlying security framework
- Scenarios for testing which use the framework
- Risk analysis reporting
- SIEM integration
- SOAR integration
- An extensible API or API-1st
- Ticketing system and a case management system
- Direct security technology integration

BENEFITS OF AUTOMATING BREACH AND ATTACK SIMULATION

As the security landscape has become increasingly volatile, BAS gives cybersecurity teams a new way to respond.

TOP 3 BENEFITS OF AUTOMATING SECURITY CONTROL VALIDATION

1. **Enhanced Insights**
   A reliable BAS platform will generate insights and improve decisions across the complete security organization, from risk to operations and compliance — and offer a rich depth of use cases to improve effectiveness across the security program. The three pillars of insight of a threat-informed defense strategy are known threats (aligned to the MITRE ATT&CK® framework), security control efficacy, and risk management on the basis of key compliance frameworks (like NIST 800-53).

2. **Better Business Decisions**

   - Make better decisions about people, processes, and technologies.
   - Maximize return on investments and inform future investment decisions.
   - Identify control and organizational weaknesses so your program performs as planned.

3. **Real Security Outcomes**
   BAS verifies security capabilities across your entire enterprise, raising efficiency, productivity, and effectiveness by measuring security program performance against known threat behaviours.

INTRODUCING THE ATTACKIQ SECURITY OPTIMIZATION PLATFORM

Despite years of investment in cybersecurity, today security leaders lack tangible data about the real-world effectiveness of their security programs. Lacking data-driven performance insights, security leaders struggle to achieve effectiveness and make smart decisions.

The AttackIQ Security Optimization Platform builds on the MITRE ATT&CK framework of adversary tactics, techniques, and procedures (TTPs) and emulates those TTPs to exercise security controls in the same way an adversary does, in production. It provides a comprehensive means to measure effectiveness across your organization and elevate business value.

The MITRE ATT&CK framework is a globally available, free, open framework of known adversary tactics, techniques, and procedures (TTPs). Built and released in 2015 by the MITRE Corporation, a federally funded non-profit research and development organization, the ATT&CK framework has gained significant momentum in the public and private sectors as a globally-vetted, all-source repository of adversary behavior. ATT&CK has given organizations a stable framework against which they can design their defenses. By understanding how adversaries target your data, you are in a better position to secure yourself. A natural next step is for organizations to deploy automated adversary emulations to test their cyberdefenses. That is why AttackIQ is closely aligned with MITRE.

AttackIQ takes customers on a journey from initial automated testing to comprehensive security optimization. The company has so far identified at least 26 distinct use cases for deploying the AttackIQ Security Optimization Platform and MITRE ATT&CK framework across the cybersecurity and risk organization. These include:

(continued on next page)

INTRODUCING THE ATTACKIQ SECURITY OPTIMIZATION PLATFORM (CONT.)

- **Security Testing**
  - **Red Team Augmentation** — achieve far greater reach at a fraction of the cost
  - **Blue Team Security Control Validation** — optimize your security control configurations and avoid protection failures
  - **Purple Team Integrated Workflow and Testing Program** — bring together red and blue into an integrated threat-informed defense process
- **Control Framework Assessment:** Test control framework effectiveness (i.e., NIST 800-53) to identify which control framework is most effective.
- **Investment Decision Support:** Use comprehensive performance data to assess your overall security strategy and determine necessary divestments and investments.
- **Security Pipeline Validation:** Assess security sensors in the enterprise, including event logs, network security controls, and the SIEM, to ensure effectiveness.

A full list of all 26 use cases can be found here.

AttackIQ works with customers to maximize the use of the AttackIQ Security Optimization Platform across customers' entire security program. With the adoption of multiple use cases, CISOs can further reduce the overall total cost of ownership of the security optimization platform, while improving the productivity and efficiency of their cybersecurity and risk teams, thus increasing the strategic nature of their cybersecurity posture.

CONCLUSION

- Breach and attack simulation technology allows enterprises to emulate multi-stage, comprehensive adversary campaigns against their entire enterprise.
- Historically, BAS was largely focused on running attacks and red team augmentation and, as it evolved, to security control validation. Today, the objective is to maximize the effectiveness of the cybersecurity program as a whole.
- Ultimately, a security team armed with a BAS platform that helps optimize its entire security program will improve its overall effectiveness and efficiency.
- Founded on BAS technology, the AttackIQ Security Optimization Platform is a **"force multiplier"** for cybersecurity teams — essentially taking the efforts of red and blue teams, plus security controls, and amplifying their effectiveness and efficiency. The result is a better way to test people, processes, and defensive technologies with a threat-informed defense.

"AttackIQ enables us to make sure our security approach is working. If we see news stories about emerging threat actors, we can test right away to be sure our systems will hold up in the face of such an attack."

– Kumar Chandramoulie, Vice President of Cyberdefense, Data, and Threat Management at AmerisourceBergen

TEST YOUR KNOWLEDGE!

1. **Which of the following is not a functionality of BAS?**

   a. Provides detailed status and performance of security controls
   b. Enables security analysts to find performance gaps
   c. Acts as an intermediary between users and cloud service providers
   d. Assesses readiness

2. **What was the original purpose of breach and attack simulation tools?**

   a. Security control validation
   b. CI/CD
   c. Establishing security training and awareness programs
   d. Deep packet inspection

3. **BAS emulates real-world attacks so that organizations can test and validate how their security controls perform against existing threats.**

   ☐ TRUE
   ☐ FALSE

4. **How many security controls does a company have to manage on average?**

   a. 66
   b. 32
   c. 91
   d. 47

TEST YOUR KNOWLEDGE!

5. Which three challenges do security teams most often face because of security controls failure?

a. Cost limitations; blue teams have difficulty stopping red teams during adversary simulation exercises; lack of scalability

b. Lack of visibility; insecure cloud data transmission; compliance risks

c. Complexity and inefficiency; the alternative to BAS, "red teaming," is very people intensive; lack of an automated control validation platform leads to breaches

d. Managing firewall changes; proving where things stand; keeping up with rules and regulations

6. AttackIQ builds on the NIST Cybersecurity Framework and focuses on risk analysis and risk management.

☐ TRUE

☐ FALSE

7. Which of the following is not a use case for deploying the AttackIQ Security Optimization Platform and MITRE ATT&CK framework?

a. Manual testing

b. Control framework assessment

c. ML/AI training

d. Pre-sales enablement

TEST YOUR KNOWLEDGE!

8. Fill in the blank: BAS should be focused on _____ as a comprehensive practice.

a. Security control validation
b. Security optimization
c. Penetration testing
d. Risk assessments

9. All BAS solutions available in the market today are basically the same.

☐ TRUE
☐ FALSE

10. What are the top three benefits of BAS?

a. Detailed data analytics; better business decisions; reduced overhead
b. Firewall automation; increased revenue; real security outcomes
c. Enhanced insights; more security certifications; single-pane-of-glass
d. Enhanced insights; better business decisions; real security outcomes

PAGE LEFT BLANK INTENTIONALLY

Test answers on next page.

ANSWER KEY

1. Answer: C
2. Answer: A
3. Answer: True
4. Answer: D
5. Answer: C
6. Answer: False
7. Answer: A
8. Answer: B
9. Answer: False
10. Answer: D

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com.
Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.