How Breach and Attack Simulation Can Improve Your Security

In this paper:

- Organizations are deploying a number of different tools in order to protect their users and data
- Breach and attack simulation helps organizations automate and scale how they test their defenses
- XM Cyber’s BAS solution assesses risks on production systems, cloud or on-premise, by simulating attacks

Year after year, organizations of all sizes are faced with myriad technical challenges. Whether it’s moving to the cloud, enabling mobility, or simply making sure everything works as users expect.

One of the biggest challenges for any organization is security.

The security landscape is full of all manner of tools and services that organizations acquire and deploy to help solve different issues. Many organizations start with tools that aim to provide a degree of control over their IT operations.

For basic network security and perimeter defense, firewalls remain a cornerstone technology. Endpoint security is another core area of concern, with a variety of tools that are used to help identify threats and protect endpoints. Access control is another area of investment for many, with Identity and Access Management (IAM) services receiving a great deal of attention. Application security is also top of mind; as is cloud and mobile security.

Beyond control points, there are monitoring and logging tools, as well as threat intelligence and threat-hunting functions that organizations often use. Then there is testing, which has its own subset of options, including penetration testing, red teaming, and bug bounties, as well as Breach and Attack Simulation (BAS) services.

**Breach and Attack Simulation (BAS)**

Simply deploying a laundry list of security controls and tools is not enough to actually secure an organization. There can be gaps in the coverage of the various tools and there can also be misconfigurations that can potentially expose companies to risk.

Looking beyond the tools, security is often a function of technology working alongside people and processes. Even when the technology is properly deployed and configured, there can be risk coming from other areas.

Testing and validating security is a critical, foundational component.

Penetration testing usually involves a security consultant who is contracted by a company actively attempting to gain access to resources. Red teaming is an approach where a group within the company acts as an adversary, attempting to get past defenses put up by a company’s blue team defenders. With bug bounties, third-party researchers are provided a financial reward for reporting flaws in an organization’s infrastructure or applications.

Breach and attack simulation represents a different approach to helping organizations test and validate their security posture. BAS is focused on how organizations can automate and scale how they test cybersecurity defenses.

**Next Steps:**

- Visit the [XM Cyber website](#).
- Technology journalist Sean Michael Kerner [speaks](#) with Gus Evangelakos of XM Cyber (14 min).
BAS offers the opportunity to expose where risks exist. Just because an organization has 99 percent of your devices patched doesn’t mean an attacker can’t take down the network.

BAS platforms have become an important capability for any organization to have in its toolbox. As the need for these capabilities that BAS provides is so great, the market for tools is also growing rapidly.

**BAS and Compliance**

There are many reasons why a company will invest in a particular cybersecurity tool or service. One of the biggest drivers is compliance with regulatory and policy requirements.

Regardless of the regulation or policy, compliance is something that requires time and resources. Compliance is often centered on collecting different results and then documenting everything in a formal report. BAS can play a key role in aiding IT staff as they prepare for compliance audits, helping to remove some of the manual processes that waste time and resources.

One of the more common compliance regulations is the Payment Card Industry Data Security Standard (PCI DSS). One business that needed to comply with PCI DSS required that a subnet within its network be locked down and only be accessible by devices in the same subnet.

By implementing XM Cyber’s BAS solution, the business was able to see where firewall rules needed to be updated, after first demonstrating how a potential attacker could gain access via a variety of different means.

Also among the attack vectors exposed by XM Cyber were a pair of service accounts that were part of the SQL administrators’ role. An attacker that could compromise the systems where the service accounts were located could also gain access to the areas of the network where PCI DSS compliance was required.

———

The term BAS is relatively new and began gaining in popularity in 2017 and 2018. It attracted analyst attention with Gartner stating in its *The Hype Cycle for Threat-Facing Technologies* report that, “the ability to provide continuous and consistent testing at limited risk is the key advantage of BAS technologies.”

The consistency of testing is a critical attribute of BAS that helps to differentiate it from other approaches, such as penetration testing, which is only a point-in-time test. After a penetration test is completed and flaws are remediated, it only takes only one configuration change to create new problems.

Given the scale and distributed architecture of modern IT, which include both on-premises and cloud resources, it’s exceedingly complex for a penetration tester to accurately test an entire environment. There is also a real need for organizations to assess the risk as the network changes.

**Why Organizations Need to Consider BAS**

BAS technology runs in a continuous and automated manner, providing users with the ability to identify potential risks in real-time.

By identifying risks as they emerge, it’s possible for management and IT security professionals to make better decisions. Rather than just collecting metrics about a particular security control,
How XM Cyber’s BAS Solution Works

When testing for security risks, there is a need to make sure that BAS technology isn’t just tested in a lab or on only a few systems. It is imperative that BAS assesses risks on real systems and looks at all resources, wherever they are located, including on-premises and in the cloud.

The elements of the environment that will put a company at risk, after all, are in production, as are the changes that create new risks.

In the XM Cyber BAS solution, sensors are deployed in the cloud and metadata is collected from devices. Using this wealth of information, the solution can simulate how attacks are possible. Going a step further, XM Cyber conducts checks on existing security controls, such as firewall rules, to confirm that the simulated attack would actually work. The whole simulation is done in a safe manner in production and does not actually put IT assets or devices at risk.

Looking beyond the ability to identify risks, there is a need to also enable users with the information required to remediate problems.

XM Cyber provides users with a report that explains how to fix identified problems, whether that involves investing in a new technology or if there are configuration changes that need to be made, or patches that were missed.
Securing the Hybrid Cloud with BAS

It’s also important that BAS examine the combination of both on-premises and cloud deployments. A reality of modern cloud deployment is that some development and access occurs on-premises.

A common attack vector is for a hacker to pivot from one compromised system to gain access to a higher-value target.

For example, if an attacker is somehow able to gain access to an on-premises system that has access tokens for the cloud, it’s possible the attack could pivot to compromise cloud resources.

Securing the public cloud on its own is important, but it’s not enough. XM Cyber links BAS across both on-premises and cloud assets to automatically and continuously access hybrid cloud risk.

Forward-Looking Protection

While IT is constantly changing, one thing that seems fairly certain is that security will continue to be a challenge for organizations for the foreseeable future. Attacks will not stop anytime soon as attackers continue to find targets to compromise.

Among the many cybersecurity concerns for organizations is the risk that results from changing network configurations and the seemingly endless expansion of IT resources with data that sits everywhere.

Understanding what might be missing in an IT organization’s cybersecurity posture is a crucial risk that organizations need to manage. A key part of the solution to this problem is having visibility into all the IT assets in the organization, wherever they might be. No organization can successfully block all of the threats it faces, so it’s best to be prepared with the right approach to IT hygiene, talented people and proven process in place, and BAS can help.