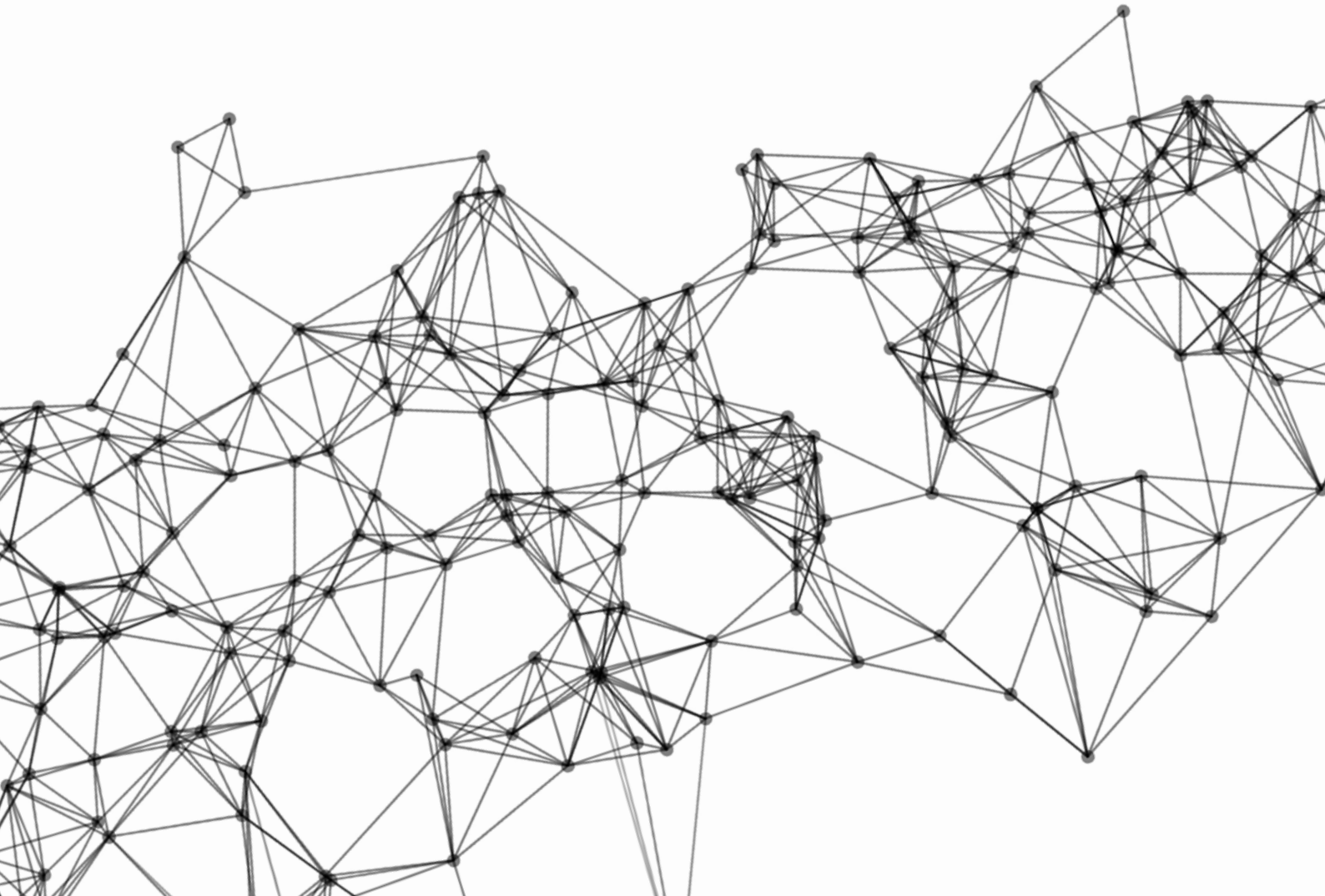
SafeBreach
Stop Tomorrow's Breach. Today.

Whitepaper

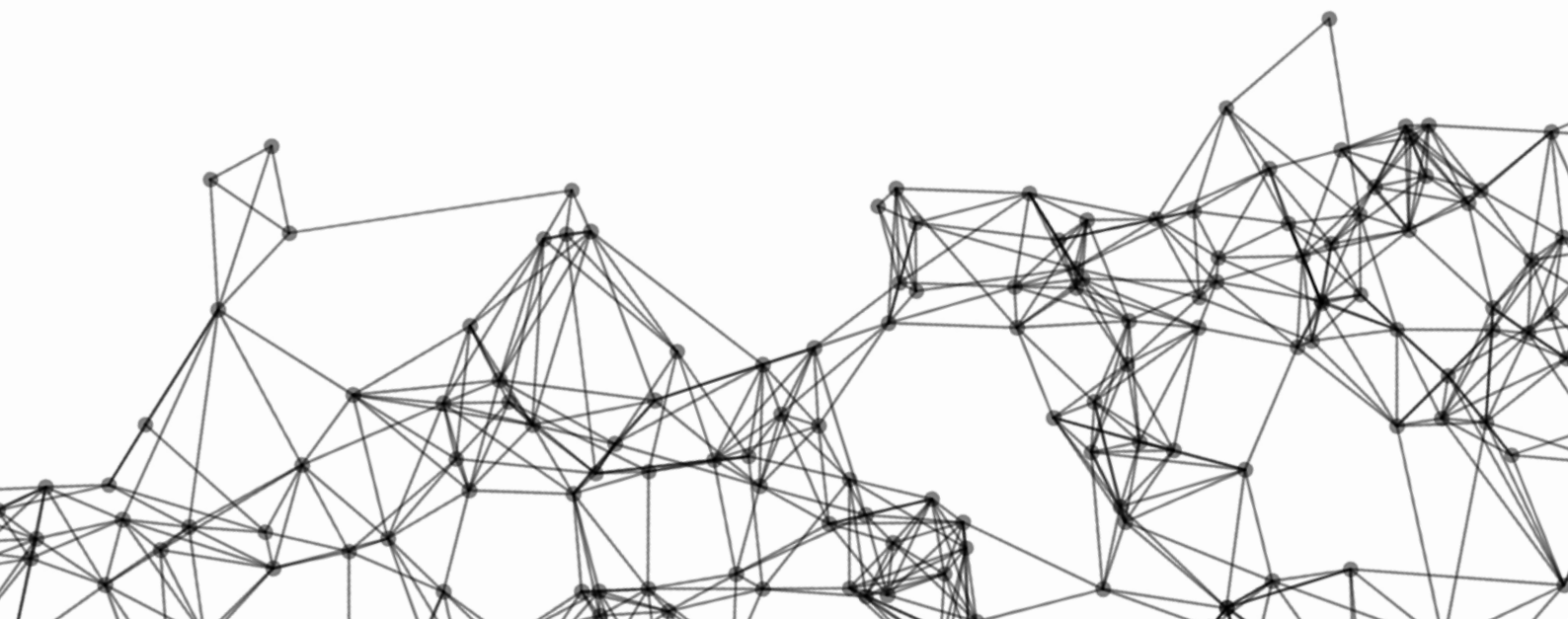
Learning From Hackers

Understanding Your Adversaries For Better Security



SafeBreach
Whitepaper

Table of Contents



“Know your enemy and know yourself,
and you need not fear the results of a hundred battles”

Sun Tzu, The Art of War

In November 2015, during the RSA Conference in Europe, Amit Yoran President of RSA and former cybersecurity director at the U.S. Department of Homeland Security proclaimed “Infosec is fundamentally broken. ”He said, “Infosec is an industry that wastes billions of dollars on firewalls and policing network perimeters, things that “make us feel safe” but don't address real problems. Look at the major breaches of recent memory and you will find companies that were attacked despite using next-generation firewalls and high-level software that, for all their cost and promise, allowed massive, embarrassing and harmful breaches.” Is it true? Certainly there continues to be breaches in the headlines despite more than $70B in annual cybersecurity spending.

While advances in malware and hacking techniques against a backdrop of underinvestment in security departments have created the perfect storm, there are several reasons why cybersecurity has become one of the biggest challenges for organizations today:

Changing risk profile- There exists a never-ending challenge of new and evolving users, endpoints and applications that need to be secured

Complex point products- Point security products by different vendors to address specific security problems make it difficult to understand the security posture for the entire organization. In addition, with the complexity and lack of cyber talent, most security solutions are not properly optimized or configured correctly. As described by a participant in the NYSE and Veracode survey (Cybersecurity in the Boardroom), “The more you increase security, the less user friendly the product becomes.”

Unclear prioritization of risks- The current reactive approach of patching systems and vulnerabilities (CVEs) is not scalable, and may not be the right approach. Vulnerability-based models prioritize recent weaknesses in systems and infrastructure, without evidence that these specific weaknesses are important to an attacker.

In fact, security attacks come from living, breathing opponents that exhibit specific characteristics. They are thinking outside the box, using sophisticated breach methods and taking advantage of a very collaborative ecosystem. Traditional security solutions are point solutions that deliver very specific defenses while attackers use a blend of techniques.

How Do Hackers Think?

How can organizations work smarter by understanding attackers and learning from them? The good guys have to get it right all the time to avoid being hacked. The bad guys only have to find one hole. The advantage appears to be on their side, unless security teams move from just understanding environments to understanding adversaries.

It's time to supplement security defenses with a hacker-centric security paradigm. But, first, let's put ourselves in the hacker mindset – how do they think?

Reality-bound- The first is that they are bound by rules and boundaries within any network. There is no way for them to change reality. If there are specific protocols allowed in a network, those are the ones attackers will likely leverage. They can be creative with their methods and malware, but are challenged to manipulate the network, security configurations or protocols to avoid detection. In other words, they are as resourceful as they are allowed to be.

Persistent, patient and resourceful- Hackers are persistent and relentless-- they spend time understanding the organizational structure and the network; they will actively investigate the best way to infiltrate an organization. Whether they are cause- or financially-motivated, they've evolved from the equivalent of the cyber purse snatcher to the great cyber heist.

Playbook of breach methods- Malware today has become much more sophisticated, it can exhibit specific behaviors based on user activity, and is sophisticated enough to lie latent when necessary to bypass security solutions. Yet, the majority of breach methods are limited, and are being replicated across organizations. According to the Verizon Breach report, 92% of cyber attacks in the past ten years can be linked to just nine basic attack patterns. Of these, most companies have to face only between two and four. These are the ones that hackers will try first. These are the ones that security teams must continually validate, instead of just focusing on the "cool zero-day".

Asset and objective-oriented- Every action performed by an attacker may look like a singular incident, but is actually a phased progression towards their objective. Hackers will adjust their methods based on success and failures; they also tend to reuse tools and infrastructure. The ability to look at the entire cohesive view of what an adversary is doing (the complete attack kill chain), and their techniques is critical to not only to detect today's attack but understand their modus operandi for future attacks.

Developing An Offensive Security Mindset

How do the characteristics outlined above help organizations? It tells us that any hacker-centric cybersecurity program must incorporate the following:

1. Continuous validation- In the software development lifecycle, continuous validation are unit tests that allows a developer to test the basic input and output of a software methodology. In the security world, your infrastructure, users and even security solutions are constantly evolving. The only way to properly battle relentless and highly-motivated attackers is by constantly validating and monitoring an environment.

2. Break the cyber kill chain- The cyber kill chain documents the various phases that attackers use, from reconnaissance, weaponization, infiltration, exploitation, lateral movement to exfiltration. By understanding this attack lifecycle, security teams can prioritize specific programs that are going to be more successful in their particular environment. For example, instead of just focusing on security awareness programs to combat phishing attacks, security teams can direct resources towards proper segmentation to break the lateral movement phase or inspecting of outbound Internet traffic for breaking the exfiltration phase.

3. Automation wins- In an offensive security model, automation is the only way to keep up with the efficiencies that attackers are enjoying. To more efficiently combat persistent attacks, organizations must be able to model the hacker, and automate the process to find security deficiencies.

The move towards a hacker-centric security paradigm is already taking place in the cybersecurity world. Offensive security techniques like practicing cyber war games, and using ethical hackers to break systems and infrastructure have been around for many years. Many large organizations are also creating bug bounty programs to reward hackers for finding flaws in their product/systems and infrastructure.

While these programs are important to complement existing defensive security solutions, they have a dependency on the human element/expertise. In many cases, as with consultancy services and ethical hackers, the results provide only a perspective of security at a point in time and may vary depending on the skillset of the consultant. In order to optimize efforts against hackers and support evolving risks from new users, endpoints and applications, a platform that automates the actions of a hacker and execute breach methods across the entire kill chain in a continuous fashion is needed.

Introducing SafeBreach

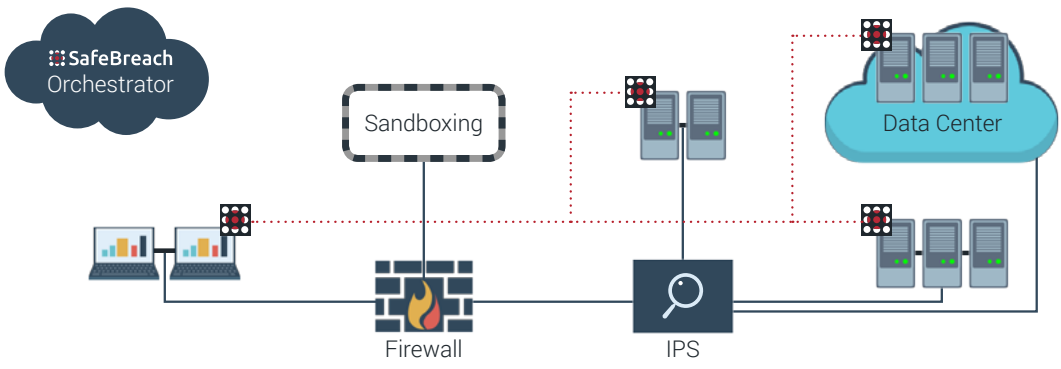
SafeBreach is defining a new market category – continuous security validation. Also, known as "attack simulation" or "attack modeling", this new category of security aims to automate adversary actions and find breach scenarios before an attacker does. For many years, cyber war game practices, military operations and commercial pilots have utilized simulated games or exercises to expose weaknesses in time to be remediated ; the goal with continuous security validation is similar.

The SafeBreach platform executes breach scenarios, first simulating breach scenarios to find holes in the network and then recommending fixes based on the attacks found. It allows organizations to quantify actual attack risks, validate security controls and support SOC (security operations center) efforts.

Organizations can deploy SafeBreach simulators in various parts of the organization's infrastructure, simulating the virtual hacker. Because breach scenarios are executed only among SafeBreach simulators, there is no impact to the organization's users or infrastructure. At the same time, these simulators sit in a real-world environment while security systems like firewalls, intrusion prevention systems and web application firewalls are in place, allowing security controls to be validated and real risks to be measured.

SafeBreach offers unique benefits:

- Simulates hacker breach methods backed by real security research to keep up with the evolving techniques developed by attackers.
- Delivers continuous validation to ensure understanding of the organization's security posture at any point in time
- Allows Chief Information Security Officers (CISOs) to provide boards with insights into their risks, justify existing security investment and focus their resources on the issues that matter, not just the easy ones.



SafeBreach Platform Components

Next Steps

If you would like to get a FREE assessment of your security risks, please email: contact@safebreach.com or fill out our form at info.safebreach.com/assessment.