WHITE PAPER

How to Create an Effective Breach Defense Strategy

Creation of a proper breach defense strategy is paramount to every government agency and enterprise. Various entities (like nation states, terrorist organizations, or individual hackers) can launch network attacks. Government agencies and businesses must be prepared for attacks from these sources that consist of both prolonged and sporadic durations.

This means you need a strong defense that you can routinely verify is working. However, network security is very hard to measure – what works and what does not? Breach and attack simulation (BAS) solutions solve this problem. This type of solution gives you actual metrics and instrumentation to objectively measure the effectiveness of your security tools and assess the real value of your security solution spending.

Specifically, a BAS security solution will help you with the following actions:

- create a security architecture that aligns with the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework
- understand your threat landscape and security gaps
- provide recommendations that align with the cyber kill chain model to remediate identified security gaps
- decrease your security risk and vulnerabilities

Red Helix

KEYSIGHT TECHNOLOGIES

How to Develop a Formidable Breach Defense

When creating a formidable breach defense strategy, the NIST Cybersecurity Framework[1] is a good place to start. While use of the architecture is mandated for United States Federal government agencies to use, it is also completely applicable to any civilian business or other international government network — as the architecture is based upon sound cybersecurity principles.

The NIST cybersecurity architecture has five core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

The Identify function helps develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Key activities here include asset management, governance, and risk management. This is obviously the foundation of any breach defense solution because you need to know what data and assets you must protect and the capabilities you have to do so.

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. This is the critical first line of defense and includes the ability to: actively stop attacks, block incoming and outgoing network communications to hackers, perform decryption to analyze incoming IP packets for threats, and perform threat blocking using inline security solutions.

The Detect function enables timely discovery of cybersecurity events. Examples of this category includes: anomaly and events detection, continuous security monitoring, and other threat detection processes.

BAS solutions are a key and necessary part of this function. BAS lets you respond to a simulated security incident rather than waiting for the real thing. These solutions enable you to tell if your Detect and Protect functions are working or not. This step includes the data collection process as well as the creation of actionable intelligence that can pass on to a security information and event management (SIEM) for better threat correlation and detection. For instance, is the connection from the detection device to the SIEM functioning as designed? This provides actionable intelligence as to what you can detect vs. block.

1 NIST Cybersecurity Framework. https://www.nist.gov/cyberframework.

The Respond function supports the ability to contain the impact of a potential cybersecurity incident. This includes communication of incidents to the management team, analysis of attack vector, mitigation of any damage, and the creation of network improvements to prevent a similar attack in the future. Access to detailed and accurate threat intelligence will be important to the creation of a fix and the timely mitigation of any damage.

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. This includes recovery planning, architecture and equipment improvements, and communications. A key step not to overlook during this stage is that you need to proper test any fix before you deploy it into the network. The last thing you want is a self-inflicted loss of service or to advertise that the problem is corrected, when it may not be.

Test Your Production Network

Once you have your security architecture in place, a BAS solution can immediately test your security defenses. This is an incredibly important activity. Numerous studies about network breaches over the last 10 years have proved one thing for sure—your network will be tested for weakness by a hacker at some point in time. Therefore, either you test it first or they will test it for you. It is your choice, but the legal and financial consequences should be far less devastating if you test the defenses first.

This means you need a strong defense that goes beyond the standard compliance checkbox. It requires building an offensive strategy that enables you to continuously verify that your security controls are working and optimized for maximum protection. To successfully manage and improve your security posture, you first need to measure it and identify opportunities to improve it. However, measuring your security posture in a production environment has been notoriously difficult. *And when you can't measure security, it becomes harder to manage and improve it*.

For instance, can you quickly identify sensors that go dark and fail to report security events to SIEM? Can you tell if the latest security signature provides protection as advertised? Can you identify environment drifts between the current state and last week? Are you protected from newly released malware? Unless you have a BAS solution, answering those questions is extremely difficult. BAS solutions solve this problem by providing organizations with the evidence needed to measure, manage, and improve their cybersecurity effectiveness.

When conducting a security threat analysis, your BAS solution should perform the following:

- Assess the security of your production network.
- Identify potential problems, gaps, and environmental drift.
- Recommend specific remediation actions to close any identified gaps

- Generate alerts that can pass on to your SIEM solution to close the validation loop from both prevention and alerting perspectives.

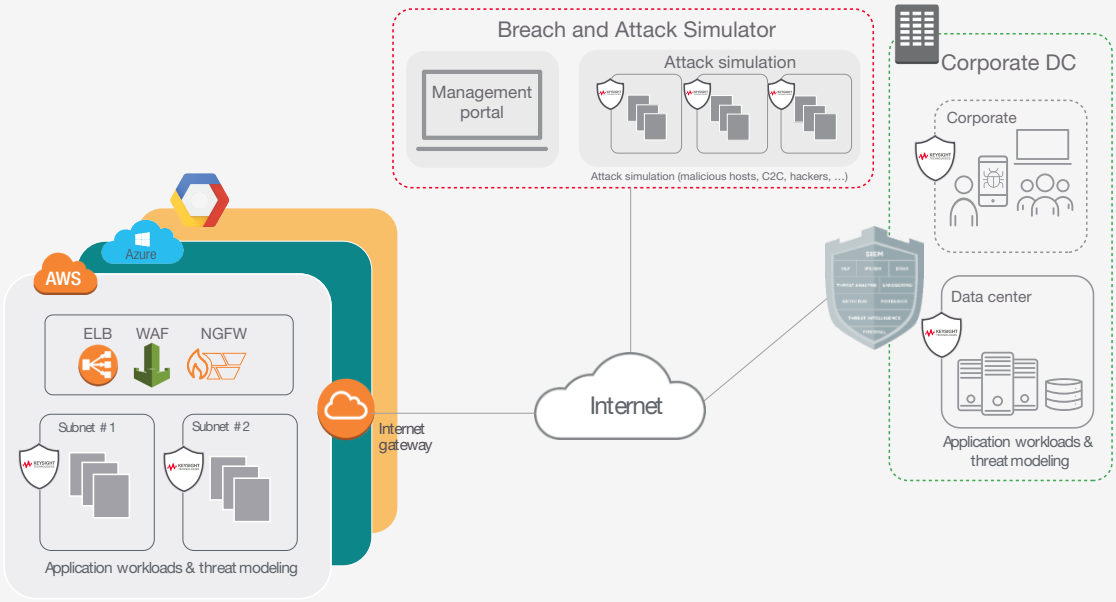

Figure 1. Overview of a BAS solution

Assess

During the testing phase, the BAS solution is set to attack the network to determine weaknesses. If a good product (like Keysight's Threat Simulator) is used, your network is completely safe from the threat simulator. The threat simulator never interacts with your production servers or other equipment. Instead, it uses isolated software endpoints across your network to safely exercise your live security defenses.

During the test effort, the threat simulator automatically scans your perimeter defenses, web application firewall (WAF), and web policy engines to identify any vulnerabilities. A malware and attack simulator then connects to the software endpoints to test your security infrastructure by emulating the entire cyberattack kill chain — phishing, user behavior, malware transmission, infection, command & control, and lateral movement. This will allow it to analyze the detection and blocking capabilities of your entire security array, quantify your exposure to specific threat vectors, delineate attacks that got through, and show how to fix the problems based on your particular firewall (if the BAS solution supports this feature).

In addition, the threat simulator should also be able to validate your web-based infrastructure including AWS- and Azure- deployed services. It also performs policy testing for different types of user policy controls (gambling, shopping, and so forth).

Identify

Once weaknesses are determined, they can be analyzed to see what is really a problem and what might just be a testing anomaly. Most threat simulator solutions are software solutions with software-as-a-service (SaaS) management. An intuitive dashboard shows vulnerabilities, audit status, and security measurement over time.

Security operations center (SOC) teams should run assessments both on a fixed schedule and automatically when a change occurs (security policy, new malware release, etc.). This will let you see which attacks you're vulnerable to, how to address them, and what steps to take if your existing solutions cannot block them.

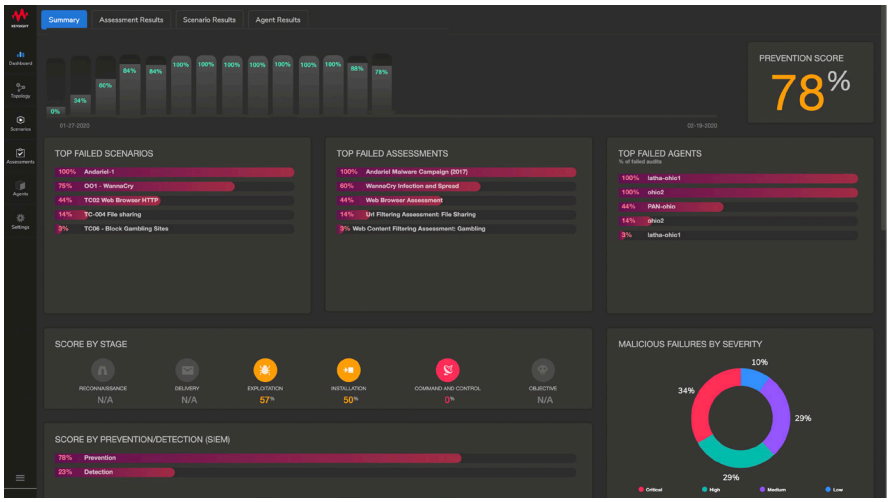

Figure 2. Example of a BAS dashboard

Alert

Finally, using tight SIEM integration, real threats and information from the simulation can pass to a SIEM for analysis. This allows your SIEM to analyze the detection and blocking capabilities of your entire security array and quantifies your exposure to specific threat vectors. This also allows your SOC team to see what an actual attack looks like so they can understand how to recognize a real one in the future. Most teams only get to see and identify the traces of an attack once a real one has already breached their defenses.

The threat simulator should provide specific recommendations on how to optimally configure your existing security products, improving your security without increasing equipment expenditures. It will also identify gaps in your coverage which your current products can't block. The recommendations include detailed instructions in clear, easy-to-follow instructions on how to better configure your security products to close the noted security gaps. A good threat simulator solution automatically reassesses your environment, so you are continuously aware of your security effectiveness even when the environment or threat landscape changes.

Know Thy Enemy

Part two of a successful breach defense strategy is to subscribe to a threat intelligence feed that gives you clear and understandable information about security attacks – how do they function, how do they move within the network, and so forth.

A proper threat intelligence feed should include a constantly updated database of malicious threats. This data is correlated into a summary, referred to as a “Rap sheet” in this document, that contains details about each and every documented threat. Figure 3 is an example of a Rap sheet form.

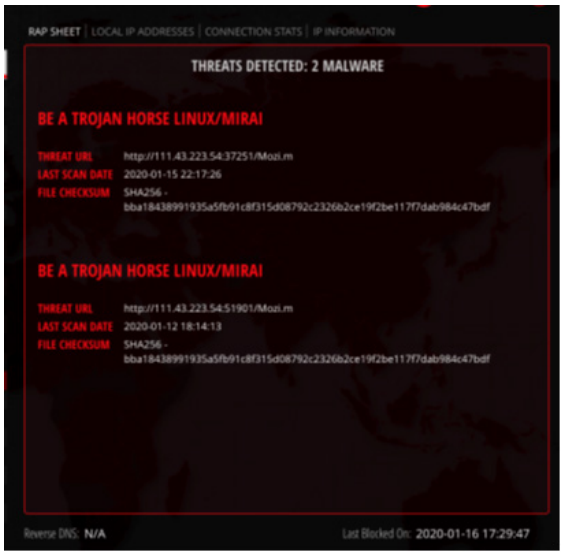

Figure 3. Rap sheet example for malware

Research

When it comes to threat intelligence feeds, the right research is crucial. For example, Keysight’s Threat Intelligence solution is an always-on database of real-world threats backed by Keysight’s ATI Research Center. All Keysight database sites have 100% proof of recent malicious activity. SOC teams can access the full database to research threats and understand evidence of malicious activity, including automated SIEM access.

Understand

For any threat intelligence feed, the research needs to be clearly and easily understandable. This allows the SOC team to recognize and understand whether the threat is malware, a botnet, hijacked IP, phishing activity, or some other exploit. If suspicious activity is correlated to a particular site, it’s helpful to know the observed malicious activity. Is it a botnet controller? A phishing site? Is it distributing malware? Is it trying to exploit vulnerable internet of things IoT devices? Understanding the proven, recorded history of a site’s malicious activity helps to provide context to understand what malicious actions a given site may be undertaking

on your network. And beware of “IP Reputation” feeds with confidence scores, as they can complicate decision-making with uncertainty. Ideally you want information such as last-scan date, extended DNS information, and screen shots.

Analyze

Once you have the correct data, you have actionable information. This lets you indirectly or directly take actions on the data. One example of an indirect action is that most next-generation firewalls (NGFW) can import a limited amount of threat intelligence information to conduct automated blocking of malicious, exploit, and botnet sites based upon that data.

Direct activities include:

- Detecting and stopping IoT attacks
- Tagging suspicious or rogue applications and monitoring them for unusual activity
- Tracking traffic to or from unauthorized geographies
- Tracking questionable file transfers and brute-force attacks

Real-time Threat Prevention

The third part of a formidable breach defense strategy triad is to be able to block as many threats from getting into the network as possible. This includes malware, viruses, worms, Trojans, and other attacks. The most important activity you can perform is to reduce your attack surface. If you limit the amount of bad (malicious) traffic coming into your network, you automatically limit your threat landscape.

The most common approach against this threat is to deploy a firewall. This is absolutely correct. You will want to configure a firewall and its ports to block all known and unwanted traffic. Unfortunately, bad actors understand how firewalls work as well—it is a well-known technology deployed for years.

Therefore, most successful bad actors have adapted and changed their tactics as follows:

- they only use a particular address for a certain period of time
- they use IP addresses from different countries
- they create different variations of malware
- some have even shifted their business model to sell hacking software (malware and such) to other bad actors on the Dark web and make money that way, rather than engaging in hacking activities directly themselves

To combat this newest version of the threat landscape, you need a solution that automatically updates with the latest and greatest threat information, like known bad IP addresses. This is the role that a threat intelligence gateway can perform. While almost

no one can discover bad IP addresses instantly, there are companies like Keysight that focus on scouring the Internet for bad actors and documenting such IP addresses. This allows for the distribution of such information as fast as possible to threat intelligence gateways to block incoming and outgoing traffic to those (now known) bad IP addresses.

IT security teams currently try to sift through the mountains of SIEM alerts, firewall logs, and IPS alarms to find and stop malware infections, ransomware, and data breaches before they wreak havoc — a time-intensive chore. But the Ponemon Institute has documented that the nonstop flood of alerts means that only 29% of security alerts go through analysis. Vital clues and malicious threats sneak by[2].

As the following diagram shows, the threat intelligence gateway should be installed in the network using an inline implementation combined with the Layer 2/3 firewall.

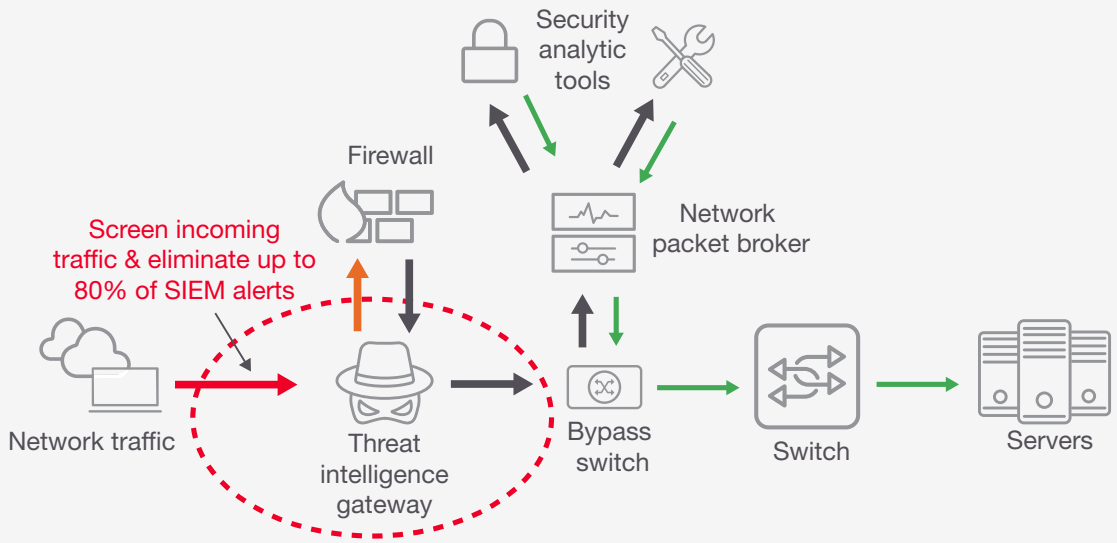

Figure 4. Deployment of a threat intelligence gateway for incoming traffic

Inspect

The first thing a threat intelligence gateway will do is inspect the incoming or outgoing addresses for IP packet data. This means deploying a solution that is capable of handling billions of sites with no performance impact. The threat intelligence gateway must perform at full line-rate.

Next-gen firewalls are great at DPI and threat detection, but they are not optimized for massive-scale blocking of malicious, hijacked, and untrusted IP addresses. Even if they can import a threat intelligence feed, their performance suffers dramatically when trying

2 Ponemon Institute, "The State of Malware Detection & Prevention," March 16, 2016. http://www.ponemon.org/blog/the-state-of-malware-detection-prevention

to block the potentially tens of millions of IP addresses required—assuming you are blocking phishing sites and hijacked IP's. A threat intelligence gateway complements next-gen firewalls by offloading massive-scale blocking so that they can allocate more resources to content inspection, user policies, virtual private network (VPN) termination, and other features while generating fewer security alerts. This makes your security operations more efficient by eliminating up to 80% of SIEM alerts once the threat intelligence gateway starts blocking malicious traffic.

Of course, there are many ways to get malware into a network—thumb drives and bring your own device (BYOD) feature prominently in the threat list. However, most malware actually starts with a small "loader" component that wakes up, registers with a botnet controller, and downloads additional code and information. Those controller sites are often used across multiple botnets, so having a threat intelligence gateway which blocks connections to those can protect you from breaches even if live malware enters your network. This includes outgoing communications such as command and control back to the hacker or the exfiltration of actual network data. Even if the malware is active, if the threat is caught in time, it may be that no network data is exfiltrated and that no breach occurred. An alert can let you know about the infected systems.

It is also important that the solution have a dashboard like the following that provides an intuitive, on-screen display of blocked sites, countries of origin, and statistics. This allows you to easily see what is happening within the gateway and how your network is being attacked.

Figure 5. Threat intelligence gateway dashboard example

Recognize

The next step is to obviously analyze the data collected. You can choose two different modes: report-only or blocking mode for otherwise unrecognized threats. Suspect IP addresses are compared to Rap sheet data for matches. Black list or white list strategies enable blocking for countries and other IP addresses as well.

The dashboard will deliver clear on-screen proof of malicious activity for any blocked sites and the performance of the threat intelligence solution. Data matching applied to individual Rap sheets can generate detailed information, enabling information to pass to the SIEM for integrated and correlated analysis. It's often best practices to simply ignore blocked inbound attack attempts, as once they're blocked no further action need be taken, while analyzing and responding to outbound connection attempts such as those to botnet controllers.

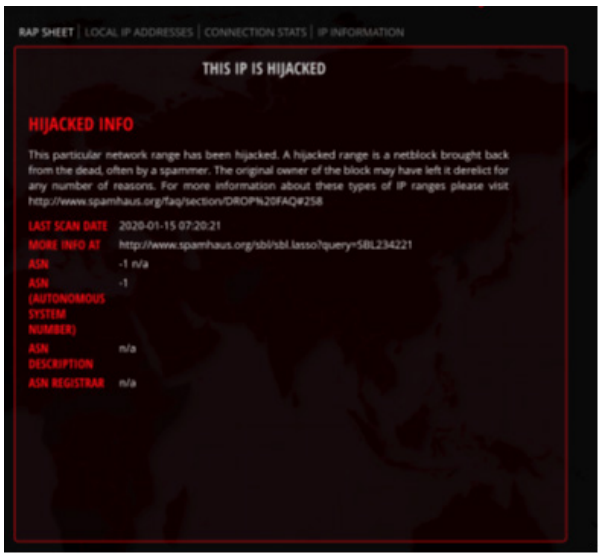

Figure 6. Rap sheet example for known bad IP address

Kill

The last key step in the process is to kill off all incoming or outgoing traffic to known bad IP addresses. This means blocking connections from known malicious IP addresses and untrusted countries while preventing phishing replies and botnet connections.

A threat intelligence solution provides remediation and optimizes security in ways traditional tools can't. The blocking function has a phenomenal impact on the rest of the network. By reducing this malicious traffic, up to 80% of SIEM alerts are eliminating that reduces 'alert fatigue' for SIEM and security tools.

Conclusion

Breach defense solutions are a critical component to any cybersecurity architecture, whether you have a legacy architecture or have redesigned your network around the NIST cybersecurity architecture. The all-important key is to put the proper solution in place that can collect actionable intelligence, provide proper analysis of that intelligence, and then help you act upon the intelligence.

This includes deploying the following three breach defense components:

- a breach and attack simulation solution to continuously test your defenses and provides the evidence needed to measure, manage, and improve your cybersecurity effectiveness
- a threat intelligence feed that provides you detailed insight into active threats which may attack your network so that you can recognize and respond to them
- a threat intelligence gateway that actively blocking communications to known bad IP addresses (whether the communication is incoming or outgoing)

These three functions are what will enable your SOC to respond appropriately to security attacks and identify any security breaches. In the end, a proper BAS solution allows you to go beyond the instrumentation level to provide remediation steps that improve the cybersecurity effectiveness of the organizations and help offset security engineer skillset shortages.

Learn more at: www.redhelix.co.uk

For more information on Keysight Technologies' products, applications or services, please contact **Red Helix**

Red Helix

KEYSIGHT TECHNOLOGIES