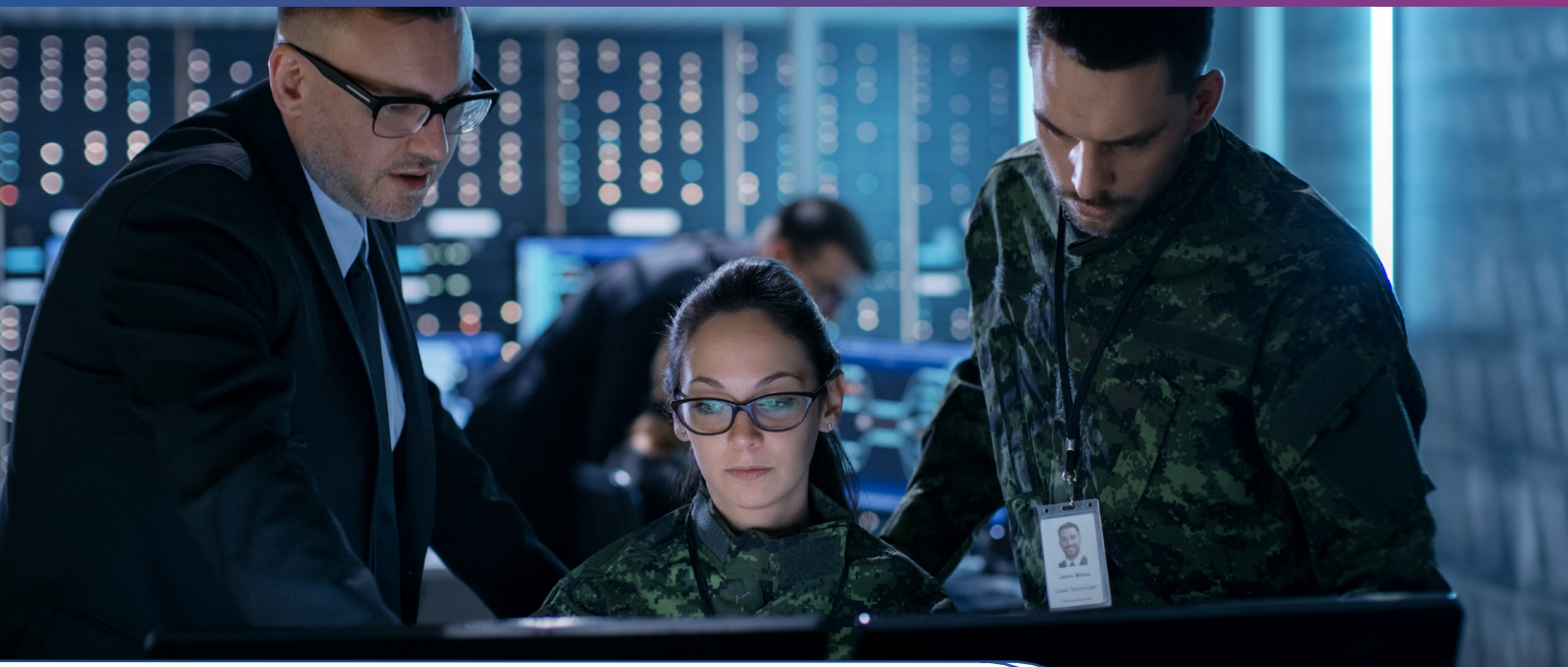

CASE STUDY

Keysight's BreakingPoint Equips US Army National Guard's Cyber Shield 2020 Cyber Training For Defending Nation's Information Infrastructure

Cyber range exercises are the most realistic way for warfighters to 'train as they fight'. These are live exercises where cyber attackers (red teams) attempt to disrupt information flow within defended environments. The network defenders (blue teams) are tasked with keeping their networks up and running by detecting and mitigating the red team's attacks.

The US Army National Guard's largest yearly event is called 'Cyber Shield'. The 2020 event was run under the command of COL Teri Williams, of the National Guard's 91st Cyber Brigade. More than 800 National Guard soldiers and airmen from more than 40 states signed in for the virtual training to sharpen their skills as network defenders. The exercise was conceived in cooperation with industry network owners and law enforcement partners to ensure it met the demands of defending the nation's at-risk information infrastructures.

As in previous years, Keysight Technologies volunteered its support to Cyber Shield. Keysight's BreakingPoint traffic generators were used in the exercise to provide realistic and random background traffic generation meant to obfuscate cyberattacks.

Organization:

US Army National Guard

Challenges:

- Generate realistic legitimate internet-like network traffic
- Obfuscate malicious actions to challenge analysts in finding cyberattacks

Solutions:

Keysight's BreakingPoint application and security test platform

Results:

Brought "immeasurable realism, context, and value to this year's exercise"

KEYSIGHT TECHNOLOGIES

Traffic realism is one of the most important requirements for cyber range traffic generation. It is not enough for defending teams to observe and mitigate cyber threats. As in the real world, they must 'hunt' the nefarious actors, understand hacker tactics, techniques, and procedures (TTPs), and then mitigate their attacks. These attacks will be part of the normal network traffic landscape and that landscape can be an enormous haystack of traffic. Before trying to mitigate an attack, a blue team must find that attacker, or needle, in this haystack of normal network traffic.

Identifying the threat is as important as mitigating it. Without appropriate background traffic, the red team is easily identified. Nearly as ineffective as no background traffic is bad background traffic. When blue teams start their hunting, they will analyze the traffic for clues to find the attackers. The quality and realism of the traffic is a very important aspect of any cyber range as synthetic traffic can be misleading. Keysight traffic generators provide random and realistic traffic that cannot be easily identified. Red teams now have the cover traffic to perform their operations and blue teams must hunt for their needles in a haystack of random and realistic traffic, just as they must do in the real world.

"We appreciate the unwavering support, cooperation, and technical efforts delivered by Keysight's BreakingPoint system and personnel to Cyber Shield 2020. Specifically, their ability to generate obfuscating malicious actions and to simulate legitimate Internet-like traffic, provided unparalleled training opportunities for our analysts, allowing them to sift through a myriad of simultaneous traffic streams to find the malicious activity. This brought immeasurable realism, context, and value to this year's exercise." — COL Teri D. Williams, Commander, 91st Cyber Brigade (VAARNG)

"Breakingpoint brought immeasurable realism, context, and value to this year's Cyber Shield exercise"

— COL Teri D. Williams, Commander, 91st Cyber Brigade (VAARNG)

Real-World Application Traffic

In Cyber Shield 2020, BreakingPoint's ability to send traffic directly to webservers, fileservers, and email servers residing in the various blue team's network demarcation zones (DMZs) provided the main portion of the haystack. Most initial penetrations of a red team will occur in the DMZ, where red teams establish connectivity, then pivot into other parts of the blue team's network. BreakingPoint conversed directly with these servers, for example interacting with a webserver in the same way a user (or a million users) would interact using a web browser. BreakingPoint easily scales from a few users connecting to a webserver about once a second, to millions of users at 1 gigabit Ethernet (GE) or 10GE line rates or higher. The goal in a cyber range is to emulate actual traffic types and densities that are seen by real networks.

BreakingPoint conversed directly with web file, and email servers in the same way users would interact with them, scaling from a few users connecting to a webserver about once a second, to millions of users at 1GE or 10GE line rates or higher.

In creating the necessary traffic mixes for cyber range exercise, BreakingPoint users have many functions available to them to get higher levels of realism. As an application traffic example, start with a predefined template representing the traffic workloads commonly found on an enterprise data center network, then adjust that template to add additional applications, remove applications that aren't appropriate to the exercise, and adjust the percentage of the types the applications.

Drilling down further, BreakingPoint can control exactly what is being done during the application flow. Is the user just checking their web e-mail or are they sitting on a web application for an hour pulling files or posting pictures? Each traffic component has its own unique and adjustable timeline. A typical use case for multiple application components might be to have one component sending an enterprise traffic mix during normal business hours, a second component surging social media traffic during a simulated lunch hour, and a third component focusing on machine-to-machine flows after the simulated workday.

To create even more realism, BreakingPoint allows full control of the messages used in the flow, customizable to Layer 7. This allows setting different browser types including cellphone browsers, different client operating systems, email content and attachments, using built-in certifications or adding new ones, and many more.

BreakingPoint also includes a gamut of supervisory control and data acquisition (SCADA)-based industrial control system protocols for critical infrastructure traffic emulation. SCADA is emphasized in many military cyber range exercises.

Advanced Cyberattack Traffic

BreakingPoint's cyber security strike traffic is another component that can be used in a traffic generation scenario. Like application components, multiple strike components can be used by themselves or mixed and matched with application traffic components. Also, like application components, strike components can launch traffic according to their own unique timelines. Typically, it is a red team that is launching the attacks at the defending blue teams, but there are use cases where BreakingPoint's security strikes can play an important part. Supporting over 40,000 strike traffic flows (DDoS, malware, exploits, signatures, predefined cyber kill chains, etc.), BreakingPoint can create entire cyber kill chains and act as an automated red team.

More commonly, BreakingPoint strike traffic can be used as 'diversionary' attack traffic, launching port scans or other diversionary attacks to distract blue teams, while the human red teams operate in another area of the defended network. In addition to an extremely large and robust library of cyber security strikes, BreakingPoint provides advanced evasion techniques to obfuscate the attack traffic. Multiple variants of existing attacks and polymorphic attacks are also supported.

In addition to an extremely large and robust library of cyber security strikes, BreakingPoint provides advanced evasion techniques to obfuscate the attack traffic.

Current and Broad Application and Attack Workloads

Application traffic and strike traffic libraries are important to a cyber range but keeping the list up to date and current is also important. Keysight's Application and Threat Intelligence (ATI) research center comprises over 80 cyber security and application researchers. This worldwide team empowers Keysight's application and security products, including BreakingPoint. With application and cyber strike updates delivered bi-weekly and malware updates delivered daily, the ATI team ensures that BreakingPoint users are using the most up to date application and security threat traffic in their training.

Keysight is honored to work with the US Army National Guard as they continue training to fight cyberwarfare to defend the nation's information infrastructure.

About Ixia and Keysight

Keysight Technologies Inc. (NYSE: KEYS) is the world's leading electronic measurement company, transforming today's measurement experience through innovations in wireless, modular, and software solutions. With its Hewlett-Packard and Agilent legacy, Keysight delivers solutions in wireless communications, aerospace and defense, and semiconductor markets with world-class platforms, software, and consistent measurement science. The company's nearly 12,600 employees serve customers in more than 100 countries.

In 2017 Keysight acquired Ixia to accelerate expansion of software solutions and broaden reach within the communications development lifecycle throughout protocol Layers 2 through 7. Keysight's portfolio now includes end-to-end solutions for the development of next-generation technologies, including network optimization and security.

With a complete portfolio of test, visibility, and security solutions, companies trust Keysight to future-proof their networks throughout their entire lifecycle.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES