SOLUTION BRIEF

Threat Simulator: Proving You're Safer Than You Were Yesterday

Part of Keysight's Security Operations Suite

Get Ahead of Attacks and Continuously Optimize Your Cybersecurity

Security operations (SecOps) teams face a constant barrage of threats, both intentional and accidental. But simply buying and plugging in a new security device doesn't make problems magically disappear. The reality is, IT security is a process, not a destination—maintaining optimum security takes a constant investment in time and resources to get the most out of the technology and deployed products.

You can't manage what you can't measure, and security effectiveness is notoriously difficult to measure. How do you know if your network is safe? If your security products are configured correctly? If you're making the right investments? How do you justify the need for a new device?

50% of companies were breached because their cybersecurity solution was not working as expected.[1]

Be a Hero, Not a Headline

You need to continuously test your network defenses, find and fix vulnerable misconfigurations, and prove you're safer than you were yesterday. Keysight can help. With Threat Simulator, a breach and attack simulation tool, you can safely simulate attacks on your production network and probe your security stack for vulnerabilities. Boasting a patented recommendation engine, Threat Simulator gives you detailed, easy-to-follow instructions to close potential gaps and optimize your security posture.

KEYSIGHT TECHNOLOGIES

A software-as-a-service (SaaS) tool, Threat Simulator is as easy to deploy as it is cost effective. An intuitive dashboard shows vulnerabilities, audit status, and security measurement over time. However, flexibility is important, too. That's why Threat Simulator makes it easy to run assessments on a fixed schedule or automatically when a change is detected (security policy, new malware release, etc.). You'll see which attacks you're vulnerable to, how to address them, and what steps to take if your existing solutions can't block them.

Alarmingly, 65% of companies do not verify that their security solutions are defending correctly.[1]

How It Works

Don't worry, your network is completely safe. Threat Simulator never interacts with your production servers or endpoints. Instead, it uses isolated software endpoints across your network to safely exercise your live security defenses. Keysight's Dark Cloud, our malware and attack simulator, connects to these endpoints to test your security infrastructure by emulating the entire cyberattack kill chain — phishing, user behavior, malware transmission, infection, command & control, and lateral movement. Additionally, Threat Simulator can also validate protection of your AWS-deployed services and perform policy testing for different types of networks (including gambling, shopping, and others).

Threat Simulator analyzes the detection and blocking capabilities of your entire security array, quantifies your exposure to specific threat vectors, and shows attacks that got through and how to fix the problems based on your particular firewall.

1. Keysight Security Scrimmage Survey, November, 2019

Network Security Assessments, Powered by Threat Simulator: Validate Security Posture, Identify Vulnerabilities, and Prioritize Fixes

Are you looking to improve security operations, but lacking the personnel to do so? We get that. When your team is constantly fighting fires, it can be hard to make time for anything else.

That's why we offer a full range of network security assessments, powered by Threat Simulator. Whether you're looking for recurring monthly assessments or a one-time engagement, our trained professionals can give you a detailed analysis of your security posture without the hassle and complexity of adding another tool to your stack. We can safely simulate attacks on your production network, reveal vulnerable misconfigurations, and give you specific, step-by-step instructions to remediate and prioritize fixes.

Our standard assessment covers the entirety of your defensive deployment. However, you can also choose from a variety of tailored audits to drill down on specific focus areas, such as the following:

- branch security
- email security
- WAF security
- DDoS attack resilience

No matter what you choose, our assessments are quick and cost-effective — complete with personalized reports and remediation guidelines. With our team's detailed analysis, you gain actionable insight into the flaws a malicious actor is likely to exploit, enabling you to immediately implement fixes to protect your network, users, and applications.

Keysight Knows Security Operations

Keysight has been in the business of testing and improving network security for more than 15 years. Since 2005, we've helped make the world a safer place by testing some of the most popular security tools on the market — including firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS). At the same time, our Application and Threat Intelligence (ATI) Research Center collects and analyzes threats from across the globe in real time — and is a trusted partner of SecOps teams and top security vendors alike.

That's why we've taken our leadership in network and security test and built a collection of tools for enterprise SecOps teams. Along with Threat Simulator, Keysight's Security Operations Suite also includes:

- ThreatARMOR: a threat intelligence gateway

When it comes to network security, your best defense is a good offense. Get ahead of attackers with Threat Simulator. Simulate attacks, find and fix vulnerabilities, and prove you're safer than you were yesterday.

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