



Keysight Cyber Training Simulator

Knowledge Toughened on Reality

Train Students on the Real-World Threat Simulation Platform

There's no shortage of bad actors in cyberspace. But there is a serious shortage of trained professionals to counter them. Businesses, government agencies, education institutions, and other critical organizations have openings they're anxious to fill—immediately.

Keysight Cyber Training Simulator (KCTS) prepares your students with the same market-leading tool used by the professionals in the world's foremost enterprises and government agencies: BreakingPoint, Keysight's emulation platform. With hands-on experience powered by BreakingPoint, students will be ready to jump quickly into careers in cybersecurity.

Demand for Industry-ready Professionals is Intense

Hackers are wreaking havoc across every facet of our business and personal lives: the destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. By 2025, cybercrime will cost the world 10.5 trillion USD annually, estimates Cybercrime Magazine.

More than half of the 2020 (ISC)2 Cybersecurity Workforce Study respondents said cybersecurity staff shortages were putting their organizations at risk. As cybersecurity jobs grow by more than 30% annually, the need for highly skilled graduates prepared to step into roles in cybersecurity has never been more urgent.

Industry needs professionals who are ready to hit the ground running.

- Produce students who are in demand by today's top cyber teams.
- Realistic scenarios that are just like the real world. Because they come from the real world.
- A well-rounded curriculum, because attacks come from all sides.

The Cyber Range with Enterprise DNA

Keysight Cyber Training Simulator (KCTS) is a complete, turnkey cyber range designed to prepare students for the real-world challenges employers confront daily. It's the cyber range with a critical difference:

KCTS is informed by Keysight's ongoing, real-world engagements with global enterprises and government agencies and powered by the same trusted tools currently deployed by professionals at the forefront of cybersecurity.

Keysight Cyber Training Simulator (KCTS)

Keysight is a global leader in advanced design and validation solutions. Our cybersecurity solutions are trusted around the world for mission-critical, financial, and military as well as consumer applications. We participate in developing standards in nearly every industry we serve, keeping our customers a step ahead in emerging technologies and security threats.

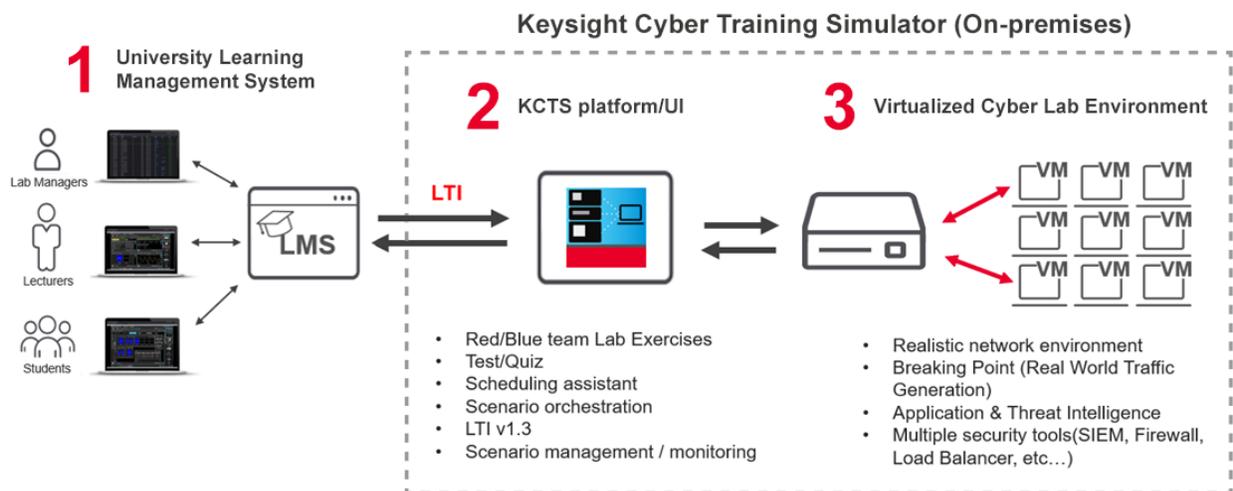


Figure 1. Components of the Keysight Cyber Training Simulator (CY101KCTS)

The Keysight Difference: BreakingPoint



Teach with BreakingPoint. Because real threats are unscripted.

KCTS enables students to develop and sharpen their skills in the same realistic environment used by professionals in government and defense, banking and finance, and other enterprises. Our educational solution is based on Keysight BreakingPoint, the gold standard for application and security emulation in enterprises and government agencies worldwide.



Stay one step ahead of the bad guy.

The cyber threat landscape is constantly changing. Many educational solutions offer limited, pre-prepared training scenarios for both attack (red team) and defense (blue team) strategies. Keysight's Global Application and Threat Intelligence (ATI) Team feed KCTS the very latest updates—just as they do for the professionals who depend on us to stay one step ahead of the bad guys. Your students train on realistic scenarios that reflect the real world—because they come from the real world. Students graduate from the course with more than book skills. They're practiced at thinking on their feet to respond to ever-shifting challenges



BreakingPoint. The professional's real-world threat simulator.

BreakingPoint simulates real-world attacks, using legitimate traffic, DDoS, and malware, so students learn from actual scenarios, not scripts. Simulating good application traffic along with malicious and malformed traffic, BreakingPoint immerses students in the same environment they will face on the job in "real" life, post-graduation.

- Simulates more than 450 real-world application protocols
- Allows for customization and manipulation of any protocol, including raw data
- Generates a mix of protocols at high speed with realistic protocol weight
- Supports more than 46,000 attacks and malware
- Delivers from a single port all types of traffic simultaneously, including legitimate traffic, DDoS, and malware
- Regular Application and Threat Intelligence (ATI) updates ensure your students are trained on the latest threats



Master the Cyber Kill Chain.

KCTS built-in lab exercises drill students in the Cyber Kill Chain, the theoretical model of an attack's structure that's become the standard approach in cybersecurity. Our hands-on exercises are based on one or more of the simplified kill chain stages in either the Red Team or Blue Team classifications, depending on the threat scenario objectives. So, students are armed with industry-ready skills when they enter the workforce.

Easy to Deploy. Easy to Manage. Easy on the Instructor.

With full Learning Tools Interoperability, teachers and students can take full advantage of the university's Learning Management System. One of the common frustrations for faculty is when third-party teaching tools have limited or no integration with the University Learning Management System (LMS). In designing Keysight Cyber Training Simulator, we made sure to correct that. KCTS features Learning Tools Interoperability (LTI) to ensure that you can take full advantage of your university's LMS investment and that your and your student's experience is simple and smooth.

Easy to deploy the platform

KCTS seamlessly integrates with your university's Learning Management System (LMS).

Save time provisioning courses

Lab scheduling and completion are easy, with scores updated to your LMS

Assessment simplified

Out-of-the-box Lab Exercises with pre-defined red and blue team exercises challenge students while freeing the instructor to focus on teaching.

Customize to fit your requirements

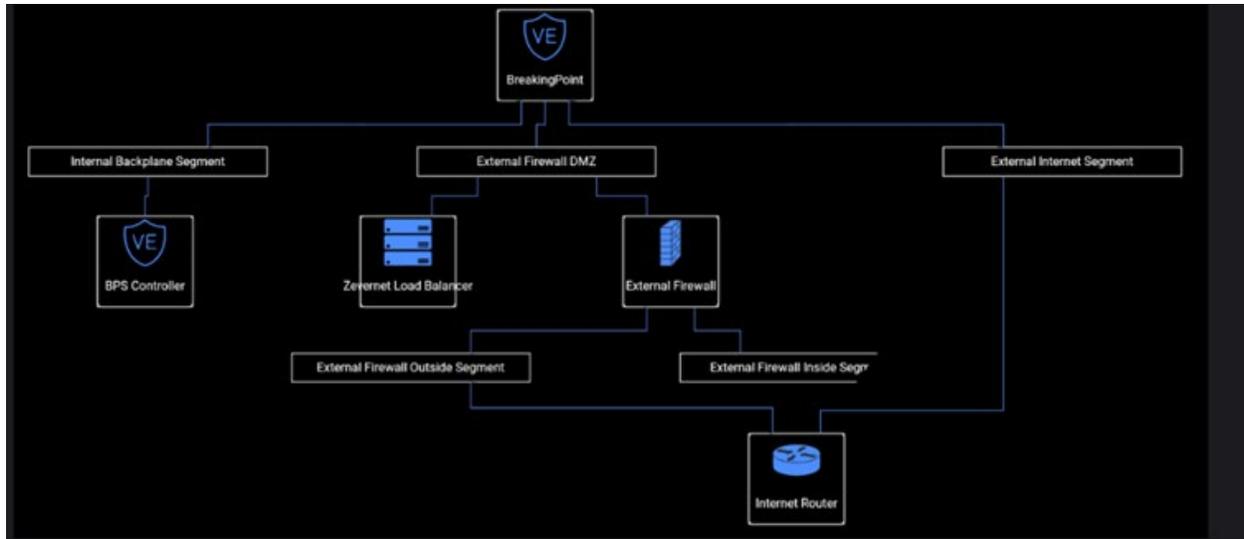
Create, edit, clone, and delete scenarios as needed for your syllabus.

You're in charge

The instructor has full ownership and control of which labs to teach and in which course.

Prepare for the Known. Train for the Unexpected.

Students learn in a hands-on environment that reproduces the challenges of the real world.



Know the enemy

Gain insights into the myriad threats that are out there. Hone the techniques required to detect and mitigate threats.

Anticipate the enemy

Understand typical security threats that exploit vulnerabilities in web applications. Anticipate and counter online outlaws.

Think like the enemy

The expression “it takes one to know one” was never truer. Understand typical techniques used to breach defenses and evade common defense mechanisms.

Outsmart the enemy

Learn how to perform analysis and forensics using real-world vulnerabilities and threat actors. Spot attacks faster, pinpoint intrusions and block attackers at scale.

Why Keysight?

Benefits for students and instructors



Produce students who are in demand by today's top cyber teams.

- Theory plus real-world challenges equal front-line readiness
- Students learn using industry-relevant tools
- KCTS is powered by Keysight BreakingPoint, the application and security traffic generator currently deployed by foremost global enterprises and governments



Realistic scenarios that are just like the real world. Because they come from the real world.

- KCTS is backed by Keysight's industry-recognized expertise including our Global Application and Threat Intelligence (ATI) Team
- KCTS's realistic network emulation is constantly updated by ATI with the latest cyber scenarios confronting industry professionals today
- Students graduate from the course with more than book skills. They're ready to think on their feet to respond to the unpredictable challenges they'll face on the job.



A well-rounded curriculum because attacks come from all sides.

KCTS covers the core skills of a capable cyber defender:

- Ethical Hacking
- Cyber Defense
- Web Application Security
- Forensic and Analysis

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com