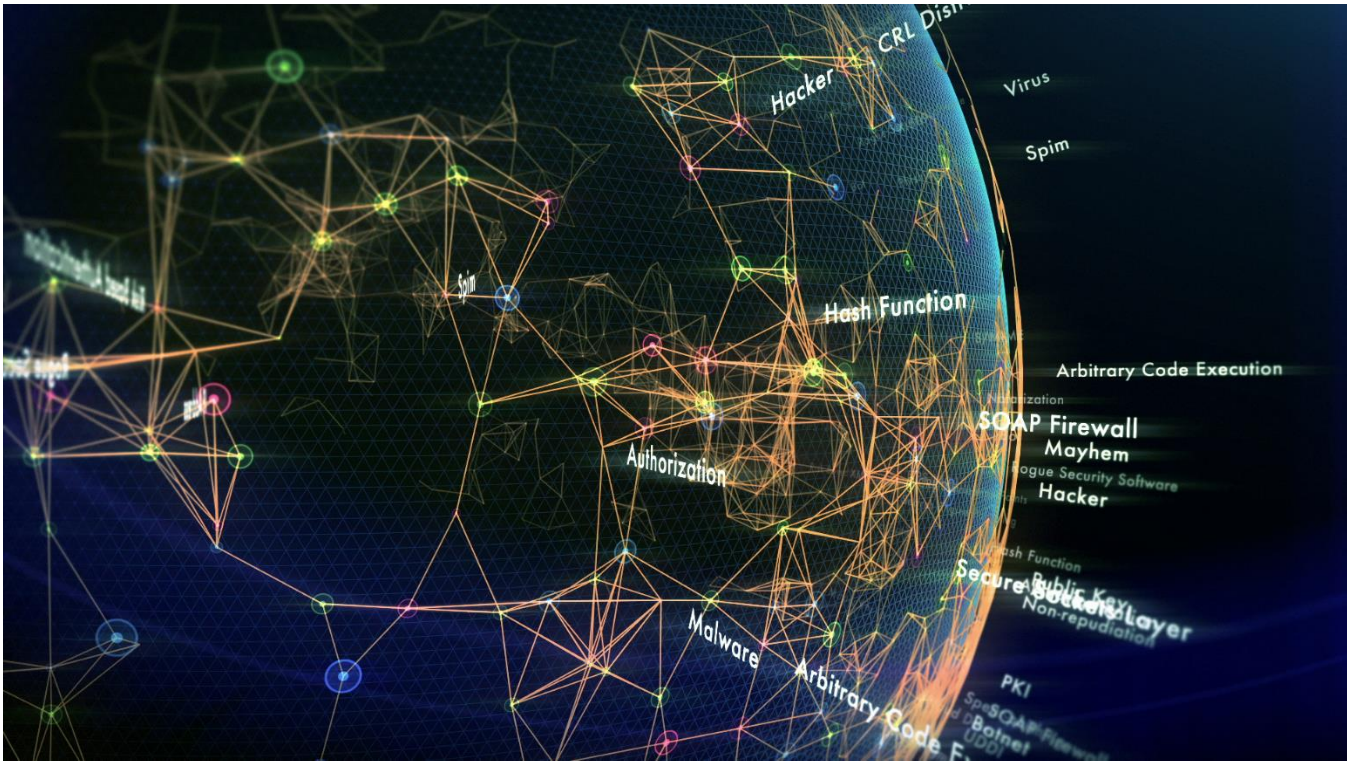
ARCHITECTURE TECHNOLOGY CORPORATION
SPECIALISTS IN COMPUTER ARCHITECTURE

cyrin



CYRIN® CYBERSECURITY TRAINING

Corporate Headquarters
Architecture Technology Corporation
9971 Valley View Road
Eden Prairie, MN 55344
www.atcorp.com
info@atcorp.com

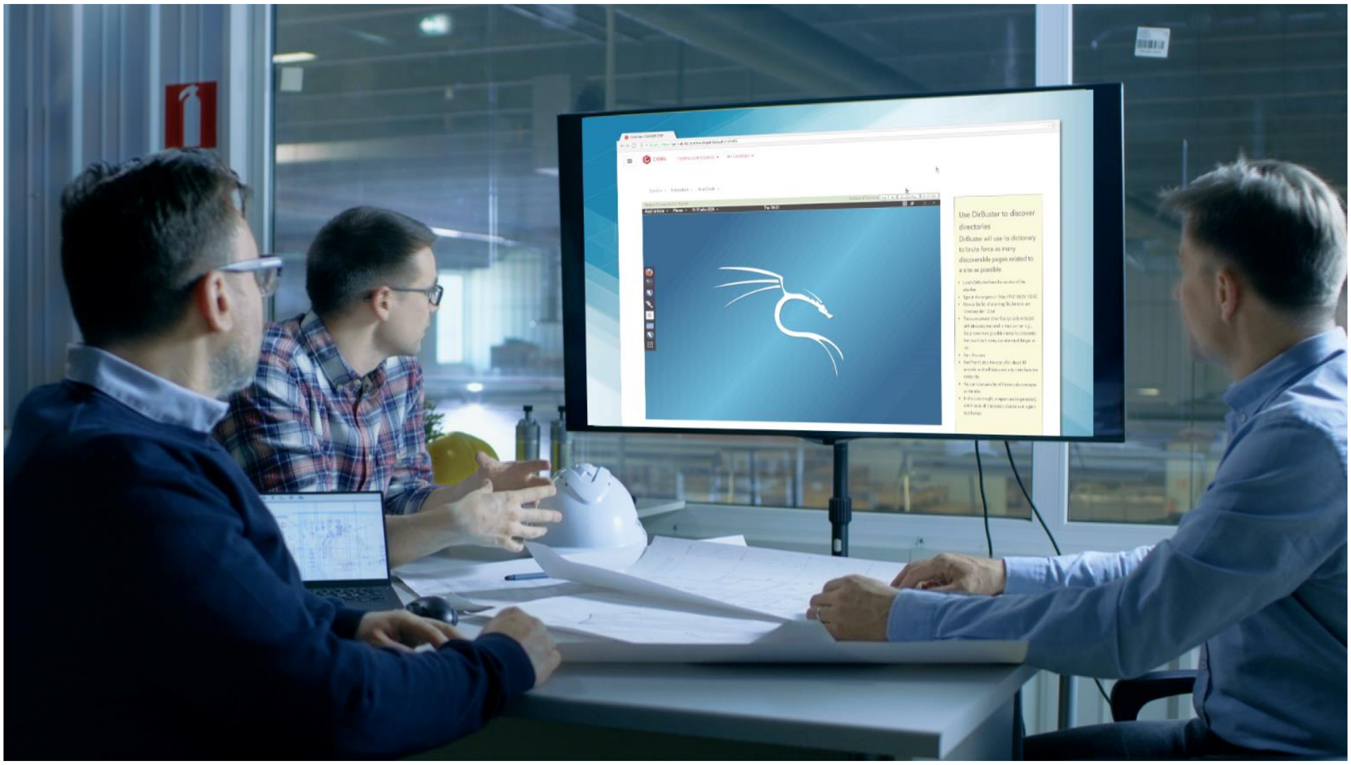
CYRIN Platform Headquarters
ATC-NY
P.O. Box 422
Trumansburg NY 14886
https://cyrin.atcorp.com/utilities
info@cyrintraining.com

Washington DC Sales Office
Indian River Advisors
1717 Pennsylvania Avenue
Suite 1025
Washington, DC 20006
www.ir-advisors.com
Office: 202.559.9123

CYRIN – VIRTUAL ADVANCED CYBER TRAINING NOW WITH THREE LEVELS OF TRAINING DESIGNED FOR THE UTILITY INDUSTRY

CYRIN – is the online, always on, always available Cyber Range Training Platform. We've trained thousands of people on how to monitor and keep their networks safe. Most importantly, training can save your organization from a disastrous cyber attack.

For those pondering the Internet of Things (IoT) and its future impact, recognize that time is of the essence. Your organization's survival could depend on it.


Use DirBuster to discover directories
DirBuster will use its dictionary to brute force as many discoverable pages related to a site as possible

Are You Ready?

CYRIN is a next-generation cyber-range where you use real tools, real attacks, and real scenarios to hone your skills in a virtual environment. Secure a Linux server system, analyze the security of a web application, or respond to a denial of service attack in a controlled environment. Practice on your own schedule using your web browser—no custom software or travel necessary! Now with new programs, new virtual attacks, specifically designed for the Utility Industry.

Cybersecurity and the distributed grid: A double-edged sword

As the Internet of Things merges with grid edge technology, experts say the power sector is both more vulnerable and more secure.

DOE cybersecurity report reveals 7 'gaps' in power sector defense capabilities

The assessment warns restoration following a cyberattack "could be more challenging than previously experienced," in part due to the unprecedented nature of such an incident.

In 2018 The U.S. Department of Energy released an August 2017 report that concluded there are more than a half dozen "capability gaps" in the power sector's ability to respond to a cyberattack on the electric grid. A power outage due to a cyberattack has never happened in this country, but hacking attempts are on the rise and a recent focus on industrial control systems (ICS) by would-be intruders has upped the ante.[1]

Electricity generation is vital to the commerce and daily functioning of the United States. The U.S. electric grid has operated historically with a high level of reliability; however, the various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events. The bulk power system faces new and evolving cybersecurity threats. Cyber threats can come from direct attacks aimed at electric grid or other critical infrastructure that could impact the operations or security of the grid.

Arguably, the greatest cyber threats to the grid have been intrusions focused on manipulating industrial control system (ICS) networks. Cyber intrusions on the electric grid have resulted in malware on ICS networks with the capability of causing damage or taking over certain aspects of system control or functionality. Recent concerns have extended to Internet of Things (IoT) devices connected to networks. IoT devices have been increasingly targeted by botnet malware (whereby the hacker takes over the operation of a large number of infected devices) to launch denial-of-service or other cyberattacks. If such IoT cyberattacks were able to access electric utility ICS networks, they could potentially impair these systems or cause electric power networks to operate based on manipulated conditions or false information. [2]

[1] https://www.utilitydive.com/news/doe-cybersecurity-report-reveals-7-gaps-in-power-sector-defense-capabilit/524706/

[2] https://fas.org/sgp/crs/homesec/R45312.pdf

CYRIN Subscription Levels & Pricing

LEVEL 1: CYRIN Enterprise Instructional Labs	**LEVEL 2 {New}: War Gaming Scenarios & Instructional Labs**	**LEVEL 3 {New}: Utility Under Attack, War Gaming & Instructional Labs**
Cybersecurity Labs: A growing catalog of cyber defense training labs in these critical areas:	Includes all Level 1 labs PLUS access to two current capture-the-flag scenarios AND one new CTF/war-game scenario each quarter...	Includes all Level 2 war games and Level 1 labs, PLUS four IT/OT attack scenarios with a new scenario each quarter!
Secure Network Setup, (Labs in this category help you gain experience with common network security practices, intrusion detection systems, and firewall policies.)	…let your team compete head-to-head in attack/defend games!	Experience and mitigate live cyberattacks on a virtual network representing a power generation/ transmission/ distribution company! Each utility gets a dedicated virtual network with mock enterprise (IT) and operational (OT) networks.
Incident Response, (Labs in this category guide you through approaches to addressing and managing the aftermath of an attack or security breach.)	Test your team's abilities with virtual capture-the-flag, defacement, and denial of service scenarios!	Attacks can include Internet-originating malware such as spear-phishing, insider threats, and supply chain compromises. Users sign in via a web browser or, as of Summer 2019, can "bring their own tools" with a direct VPN connection to their exercise network.
Web Application Security, (Labs in this category focus on detecting and understanding vulnerabilities in your web-based applications—penetration testing for the web.)	Prerequisites: Familiarity with the Unix/Linux command line Basic networking concepts (TCP/IP, DNS, etc.)	Prerequisites: Familiarity with SCADA system concepts (HMI clients, PLCs, Modbus, etc.) Basic networking concepts (TCP/IP, DNS, etc.) Basic network attack/defense and troubleshooting.
Network Monitoring and Recon, (These Labs explore how to identify network systems and the services they provide – intention-ally, through misconfiguration, or by malicious action.)	Each scenario comes with step-by-step instructions for successful attacks or can be completed without instructions for a greater challenge!	Each scenario comes with step-by-step instructions for finding the source of the attack, or for a greater challenge, have your team figure it out on their own!
Vulnerability Scanning, (Labs in this category focus on systems-level scanning and exploitation.)	Architecture Technology Corporation will publish at least one new war game per quarter.	Architecture Technology Corporation will publish at least one new attack scenario on this network per quarter
$1995 - Annual Subscription*	$3995 - Annual Subscription* (includes all labs from Level 1)	$5995 Annual Subscription* (includes all three levels)

* Annual subscription pricing per user. Discounts are available for multiple users and on an enterprise-wide basis. Customized Training: CYRIN utility networks and attacks can be customized to match your environment for an enhanced training experience. Talk to us about pricing. Call or email Indian River Advisors at 202-494-0360; graham@ir-advisors.com

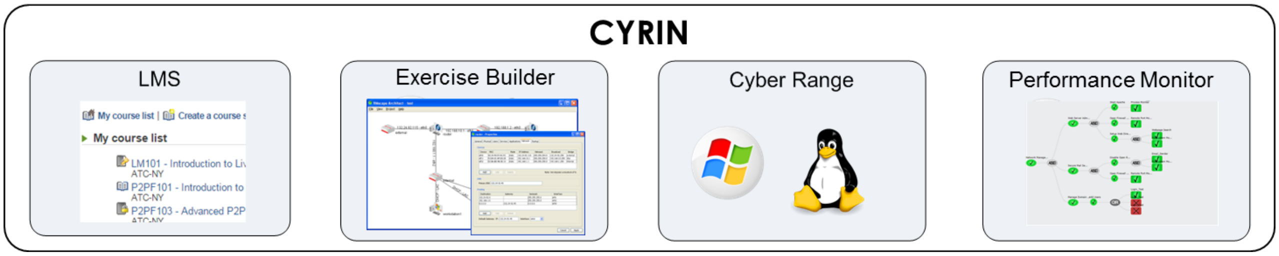
DETAILS

CYRIN is effective training for the next generation of cyber defenders and systems analysts as it requires hands on exercises, where students learn by doing. Traditionally, this has been done with a dedicated set of computer and network hardware on premises and in a dedicated classroom environment. Resource limitations typically prevent individual students or teams from having independent environments for their exercises or from being able to roll back and “try again” if they encounter problems. Further, with current systems, instructors can only evaluate a student’s progress by monitoring them in-person and requiring that they meet an artificial goal, such as capturing a “flag” file. This traditional method is resource-intensive, inflexible, slow, expensive and not very effective.

CYRIN is a next-generation “cyber range” for on-line interactive training and testing. CYRIN is an advanced e-learning platform that integrates instruction, live exercises and performance monitoring and evaluation. CYRIN improves upon existing cyber range systems with these central innovations: (1) a fully interactive, independent on-line exercise environment for each student; (2) comprehensive performance monitoring of student progress against learning objectives within practical exercises; and (3) a catalog of exercises under five major modules designed to train students on offensive and defensive cyber-attack exercises. Combined, these innovations make effective on-line e-learning possible, saving money and time.

THE CYRIN PRODUCT PLATFORM AND SYSTEM REQUIREMENTS

The CYRIN platform consists of an on-demand virtual environment (cyber range) and electronic notebook, exercise creation tools, a learning management system, and an automated performance monitoring/evaluation system using remote agents.



CYRIN is a software suite and catalog of exercises (labs) that runs on Linux using standard 64-bit Intel processors. A small-scale deployment consists of four blade servers: one for the CYRIN control software and web server, one for shared storage, and two to provide compute resources for student “virtual machines” (VMs). As student load increases, CYRIN can be scaled up by adding additional compute servers. Training scenarios can make use of any operating system that runs as a VM on an Intel-based system: Windows XP and newer, Linux, FreeBSD, Solaris, Mac OS X, VyOS, and others. CYRIN’s monitoring agents come pre-compiled for Windows and Linux. For instructors and students, CYRIN is accessed via any modern web browser such as Internet Explorer, Mozilla Firefox, or Google Chrome.

ATTACKS

— Cybersecurity and the Power Grid — Real Attacks

It's not a question of if your system {company} and the grid will be attacked; it's a question of when. Some notable cyber-physical threats[3]

- 2010 💥 Stuxnet, developed by America's National Security Agency, working conjunction with Israeli intelligence, the malware was a computer worm, or code that replicates itself from computer to computer without human intervention. Most likely smuggled in on a USB stick, it targeted programmable logic controllers which govern automated processes, and caused the destruction of centrifuges used in the enrichment of uranium at a facility in Iran.

- 2013 🕵 Havex was designed to snoop on systems controlling industrial equipment, presumably so that hackers could work out how to mount attacks on the gear. The code was a remote access Trojan, or RAT, which is cyber-speak for software that lets hackers take control of computers remotely. Havex targeted thousands of US, European, and Canadian businesses, and especially ones in the energy and petrochemical industries.

- 2015 ⚡ BlackEnergy, which is another Trojan, had been circulating in the criminal underworld for a while before it was adapted by Russian hackers to launch an attack in December 2015 on several Ukrainian power companies that helped trigger blackouts. The malware was used to gather intelligence about the power companies' systems, and to steal log-in credentials from employees.

- 2016 ⚡ CrashOverride, also known as Industroyer, this was developed by Russian cyber warriors too, who used it to mount an attack on a part of Ukraine's electrical grid in December 2016. The malware replicated the protocols, or communications languages, that different elements of a grid used to talk to one another. This let it do things like show that a circuit breaker is closed when it's really open. The code was used to strike an electrical transmission substation in Kiev, blacking out part of the city for a short time.

Experts predict cyber-crime will cost the world $6 trillion annually by 2021.[4] And there's a massive shortage of qualified security professionals. Are you prepared for the cybersecurity challenges ahead?

[3] https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

[4] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

STUDIES

The following quotes are from NBC News reporting on a cyber security study by the Ponemon Institute from July 30, 2018 who interviewed more than 2,000 IT, data protection, and compliance professionals from 477 companies in 15 countries that experienced a data breach over the past 12 months. [5]

The Institute provided NBC News with some of the comments from those interviews.

REAL ATTACKS

“The true cost of the data breach was much higher than what we projected. One of the most expensive elements is the economic impact of the incident on business and IT performance,” said a senior security analyst with a U.S. energy company.

REAL SCENARIOS

“When we first learned [about] the data breach, we were in a state of disbelief. Fortunately, we had training that helped us to know the steps needed to mitigate damages to our company’s brand and reputation,” a chief privacy officer at a U.S. pharmaceutical company said.

REAL TOOLS

IBM Security’s Barlow advises companies to practice being breached
on a quarterly basis.

“This is not something you want to try to learn once the worst happens,” he said.

[5] https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826

SOLUTIONS

Why Training? Not everyone understands different cybersecurity threat levels. However, everyone understands the impact a successful attack can have on the company's bottom line (lost revenue, costs to conduct the forensic investigation of the attack and repair any damage caused, customer lawsuits, etc.). ("Awkward Conversations About Cybersecurity," CSO Online June 17, 2017.)

CYBER TRAINING

Who are we? We are CYRIN – A business unit of Architecture Technology Corporation, headquartered at their ATC-NY cyber security division in Ithaca, NY. We train you in all things CYBER, from potentially leaky Web Applications to Denial of Service attacks to Forensics Investigations. We think the best way to train is to actually do it. We believe that an active defense, an ounce of prevention, is much smarter than cleaning up after a cyber security mess. For the last 15 years we've created these platforms for the military and law enforcement. That's why we've created more than thirty (30) Cyber Security Training Labs that are interactive. That means you learn by doing. They are online and always available.

And there is more to come. We're on our way to creating another group of Cyber Security Training Labs in the next six months. And we've recently developed a whole new skill set just for the Utility Industry including a templated process control network.

CYRIN lets you use real tools, real attacks, and real scenarios to hone your skills in a virtual environment. CYRIN training supports the current generation of cybersecurity professionals while developing the next generation of cybersecurity leaders—and even more importantly, can help save your organization from a disastrous cyberattack. CYRIN, trains you in the next-generation of cybersecurity skills from your own desktop on your own range to help you stay a step ahead of cyber criminals. With virtual cyber-security training in a real-world environment, CYRIN lets you test your cybersecurity skills on your own schedule with no custom software or travel necessary.

CYRIN offers unlimited on-demand training opportunities for you and your team with 30 cyber training exercises and counting and now specific labs for the Utility Industry. Learn more. Come see for yourself. Our site is always open.

Architecture Technology Corporation
Corporate Headquarters
9971 Valley View Road
Eden Prairie, MN 55344
www.atcorp.com
info@atcorp.com

CYRIN Platform Headquarters
ATC-NY
P.O. Box 422
Trumansburg NY 14886
https://cyrin.atcorp.com/utilities
info@cyrintraining.com
video: https://youtu.be/smokjaL2aCw