TechData

CYBER RANGE

An interactive cyber playground with the guidance of elite cyber experts.

Our goal is to equip our Partners with the skills necessary to design holistic cybersecurity solutions and services that will mitigate against the most advanced cyber threats in the industry.

Brushing up On Security Strategies With the Tech Data Cyber Range

If your company is connected to the internet, it's hackable. To prepare for this, companies need access to the resources that will help mature their cybersecurity practice.

This e-book will introduce you to the driving reasons why you need a resource that lets your team practice the skills needed to combat network exploits in the real world. Cybersecurity is a stressful business – one with lots riding on every decision. Proper, thorough preparation is the best way to overcome that stress. **The Tech Data Cyber Range, the first cybersecurity training facility ever offered by an IT distributor, can help you and your IT teams gain the skills needed.**

> **I am convinced that there are only two types of companies: those that have been hacked and those that will be.**

ROBERT S. MUELLER, III
Former Director
Federal Bureau of Investigation

Overcoming Cybersecurity Stress Requires More Than a Few Skills

In a survey of 489 cybersecurity professionals conducted in 2021 by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), 31% of respondents listed “the overwhelming workload” as the most stressful aspect of their job, with 30% citing “constant emergencies and disruptions” as the second most stressful.[1]

Further, 57%, indicate that the cybersecurity skills crisis has impacted their organization, with respondents citing an increasing workload, unfulfilled job requisitions and high burnout among staff.[1]

It’s clear that the cybersecurity industry needs a steady diet of trainings and skill enhancers. In fact, 91% of respondents agreed with the statement, “Cybersecurity professionals must keep up with their skills or the organizations they work for are at a significant disadvantage against today’s cyber-adversaries.”[1]

In the meantime, millions of open positions remain unfilled and existing professionals all agree that every effort must be made to keep skills current with the tools available to confront the constantly changing and growing threat landscape.

Cybersecurity Isn’t Getting Better

As early as 2016[1], the FBI reported rising incidents of ransomware – and its prevalence has only grown since then. The FBI Internet Crime Complaint Center (IC3) reports receiving 791,790 complaints from the American public in 2020, totaling over $4.1 billion in losses; a 69% increase over 2019.[2] The report also cites 241,342 complaints about phishing scams, incurring losses of more than $54 million, and separates out 2,474 ransomware incidents.[2]

Another report from CyberCrime Magazine estimates that today’s global ransomware damage costs up to $20 billion, with a new attack occurring every 11 seconds.[3] They predict that ransomware attacks will reach $265 billion by 2031, with a new attack occurring every 2 seconds.[3]

The Importance Of Hands-On Training

ESG and ISSA believe that hands-on experience is the most important factor in cybersecurity career development. This is confirmed by the fact that only 1% of professionals surveyed believe security certifications are more important than hands-on experience, while 52% know that hands-on experience is the most important driver behind cyber preparedness.[3]

1. ESG & ISSA. The Life and Times of Cybersecurity Professionals. Vol. 5. July 2021.
2. Federal Bureau of Investigation. Incidents of Ransomware on the Rise: Protect Yourself and Your Organization. April 29, 2016.
3. FBI Internet Crime Complaint Center. Internet Crime Report. 2020.
4. Braue, David. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. CyberCrime Magazine. June 3, 2021.

Stop Selling Fear – Focus on Prevention

The old saying “an ounce of prevention is worth a pound of cure” may be out of scale. With the financial losses we’ve witnessed over the past few years, it’s more like “an ounce of prevention is worth a ton of cure.” This is a message the distribution channel delivers to our customers often.

However, some may take it too far: it’s one thing to deliver a cautionary tale about others who have neglected their due diligence and ended up spending an enormous sum to remedy their situation, it’s quite another to instill the famous fear, uncertainty, and doubt into customers with horrific warnings and exhortations.

What you want as a professional service provider is to deliver your customer the best advice, the best protection, and the least business disruption possible. **The most effective way to achieve that is to get ahead of attacks and provide preventative services** – and it is possible to explain this to your customers in compelling, unthreatening ways.

Cyber Readiness

Help your customers embrace the reality that being alert, prepared and having a protected environment to the best of their ability in the event of a malware attack is key. It’s important to ensure that staff knows exactly what to do to stop and eradicate the threat, then safely return to full function. The bottom line? **Be the agent of change that ends a customer’s history of reactive measures that take too long and cost too much.** Help them become proactive, regularly testing all the preventative measures they have in place to keep disasters from impacting them.

Welcome to the Cyber Range

The Tech Data Cyber Range is the first ever cybersecurity training facility hosted by an IT distributor. It’s made to serve as a platform for cybersecurity demonstration and training. By leveraging the Cyber Range, Tech Data’s channel partners will be equipped with the skills necessary to design holistic cybersecurity solutions and services that mitigate the most advanced cyber threats in the industry.

Even beyond the highly valuable and necessary certification training that cybersecurity professionals must obtain, there’s a widely recognized need for hands-on learning opportunities The Cyber Range provides the opportunity to practice techniques in locating, isolating and resolving cybersecurity threats by leveraging multiple technologies and experiences.

Solutions from the Cyber Range

The Cyber Range offers a multitude of different experiences, where visitors can focus on specific security challenges they are confronting. Plus, they can engage with several exercises and simulations to get their hands on a variety of threats and exploits. The following are previews of several of the offerings:

Incident Response Experience – The Most Popular Cyber Range Service

The advisories and alerts that a company may see mean nothing until someone reviews the alerts and acts upon them. In today's information climate, you must be prepared to not only quickly locate and identify an attack in progress, but to immediately attempt to counter it before it can cause damage. This requires tight coordination and a well-prepared team.

In this experience, your new and experienced security professionals will step into a real-world exercise modeled along an actual event or one that has been predicted to happen. This is a group mission where the team will be confronted with realistic scenarios that could occur in a cyberattack. To ensure all organizational parties are tested, this exercise also includes executive-level decision makers and other technical positions. Post-exercise debriefing helps participants evaluate their own incident response capabilities.

Battle Fortress

Learn by playing Battle Fortress, provided by RangeForce. Line up in red and blue teams and play the cybersecurity equivalent of "Capture the Flag." Find yourself in intense battle with real-world attacks as you learn to defuse threats to protect your fortress, which is your network infrastructure.

In the Battle Fortress, you'll find yourself in a complete IT environment armed with security tools. You'll experience malware attacks, which you'll combat in a collaborative approach and learn how it truly takes a team to win these battles.

After the battle, you'll receive a quantitative and qualitative analysis reviewing your teamwork. It will examine the decisions you made together and evaluate whether there were better strategies you could have followed. You cannot help but learn more about yourself and your team's cybersecurity know-how in the Battle Fortress.

ISAO Threat Feed

In this experience, you'll receive a demonstration of the Information Sharing and Analysis Organizations (ISAO) threat feed in the Cyber Range. In 2015, President Barack Obama ordered the creation of ISAO. ISAO allows the formation of communities composed of security professionals from the private sector, local governments and security professionals to collaborate, share intelligence and deliver valuable training and other high-value security-related content. It's covered under a non-disclosure agreement (NDA) that protects everyone's privacy and allows all members to freely participate.

Remote Ranges

Can't travel all the way to Arizona to experience the Tech Data Cyber Range? We've created a series of **Remote Ranges** that participants can use to increase their hands-on cybersecurity skills. They can also try to "hack" our networks and try their own penetration testing skills. Remote ranges are available for beginner, intermediate and advanced Range users.

Resources

Gain a better understanding of fundamental security concepts and come to better understand vulnerabilities and prepare for challenges out in the wild.

Cyber Essentials Series –
This free, instructor-led video series allows participants to obtain new computer skills and discover a variety of security technologies. These courses provide participants with the cybersecurity knowledge needed to better understand system vulnerabilities and how to strengthen their cybersecurity posture.

Demonstration Videos –
Cyber Range engineers demonstrate the capabilities of various vendor products and platforms.

30 Minutes with a Hacker Podcast –
Our engaging monthly podcast series delivers insightful and thought-provoking discussions on current cybersecurity events and technologies.

Demonstrations and Supported Technologies

The Cyber Range provides partners with access to the most advanced cybersecurity technology available on the market to demonstrate to their customers. Use the Cyber Range as your solutions center, where you can try various solutions, introduce new platforms and help your customers envision the security environment you will build for them. Vendors with technologies featured in the Cyber Range include:

AREA 1 · BLUECAT · CARBONITE | WEBROOT · Check Point SOFTWARE TECHNOLOGIES LTD. · CISCO · Cyberinc · ERICOM Access Done Right · Fluency · FORTINET · IBM Security · kaspersky · McAfee · Microsoft · RANGEFORCE · SEAGATE · SONICWALL · storONE THINK RESULTS · Symantec A Division of Broadcom · TREND MICRO · VERITAS · vmware · WatchGuard

Courses and Partnership Training

The Cyber Range and several of its affiliates offer a wide range of general cybersecurity training courses, most with a duration of 20 hours. Topics include Incident Response, Ethical Hacking, Threat Hunting and more.

Many vendors whose products are featured in the Cyber Range also provide cybersecurity training related to their technologies.

"The Cyber Range provides partners with access to the most advanced cybersecurity technology available on the market.

The Passage Program

As cyber threats continue to grow in sophistication, organizations face a persistent challenge in recruiting skilled cybersecurity professionals capable of protecting their systems against the threat of malicious actors.

According to a recent cybersecurity professional survey conducted by the Center for Strategic and International Studies (CSIS) and the Information Systems Security Association (ISSA):

56%
are impacted by the cybersecurity skills gap

61%
believe half of cybersecurity applicants are not qualified

76%
indicate difficulty in finding qualified cybersecurity talent

> The Passage Program, delivered through the Cyber Range, is a professional service designed to bridge the skills gap for upcoming and established cybersecurity professionals.

> **Analysts estimate that by 2025, roughly 3.5 million global cybersecurity jobs will be unfilled."**
>
> Cybersecurity Jobs Report 2021,
> Cybersecurity Ventures

Passage Program Components

There are two core offerings of the Passage Program:

Placement Initiative

The Placement Initiative supports the development of **new** cybersecurity talent and places candidates in **new job roles** by providing resources and hands-on skills.

It's designed for two target audiences: **candidates**, who are looking to be placed in new job roles in cybersecurity, and **employers**, who are looking to hire candidates who have completed the program.

Upskill Initiative

Most organizations find it increasingly difficult to develop newly hired talent, retain tenured personnel, and maintain the requirements of day-to-day security operations. Investing in the professional development of cybersecurity personnel is a key factor in both the operational success of an organization and the long-term retention of staff.

The Upskill Initiative is designed to develop **participants** in their **current job role** by providing the resources and skills needed to succeed. The initiative can provide the necessary bandwidth and proficiency to support the development of currently employed, qualified individuals.

While not an accrediting body, these initiatives will help accomplish this need through hands-on experience and professional consulting. Both initiatives focus on the same cybersecurity job roles but are directed toward an individual's current skill and experience level.

Hands-On Cybersecurity Skill Development

Both the Placement Initiative and Upskill Initiative develop individuals in the roles of SOC Analyst 1 and Junior Penetration Tester.

SOC Analyst 1

A Tier 1 SOC Analyst position is a core job role in defensive cybersecurity. This role is responsible for the **monitoring** and **investigation** of security alerts and incidents in a Security Operations Center (SOC).

The Passage Program will provide job-readiness (Placement Initiative) and current skills development (Upskill Initiative) through testing and training on the following topics:

· Data search procedures
· Fundamentals of Windows
· Identification and recognition of vulnerabilities
· Interpretation of collected information and logs
· Malware identification
· Report writing
· Utilization of protocol analyzers

Junior Penetration Tester

A Junior Penetration Tester is responsible for the reconnaissance, **enumeration** and **documentation** of security vulnerabilities.

The Passage Program will provide job-readiness (Placement Initiative) and current skills development (Upskill Initiative) through testing and training on the following topics:

· Pre-engagement analysis
· Reconnaissance and information gathering
· Enumeration
· Introduction to exploitation
· Post-exploitation and engagement cleanup
· Remediation guidance
· Vulnerability analysis
· Report writing

Benefits of The Passage Program

Candidate/Participant Benefits

· Hands-on skills training directly related to the career role.
· Real-world cybersecurity skills and knowledge assessments.
· Support with career path development, either as a new role (Placement Initiative) or building skills in your existing role (Upskill Initiative).

Employer Benefits

· Eliminate onboarding time constraints.
· Expand your internal security departments.
· Gain confidence in hiring qualified candidates (Placement Initiative), or in developing your existing cybersecurity professionals (Upskill Initiative).

If you are an employer or candidate interested in the Passage Program, visit our website to learn more at cyberrange.techdata.com/passage-program

Comprehensive Professional Services

Delivered by Third Parties and Vetted by Tech Data

Tech Data offers comprehensive professional services to help evaluate the technical security of a customer's network outside of the Cyber Range environment. **A significant challenge in selecting a service provider is ensuring they are vetted properly for quality and reliability. Tech Data has already done the heavy lifting for you, conducting comprehensive vetting of third parties to validate their integrity, professionalism and cost of delivery.** Our service providers are committed to the core principles of the partner/customer relationship.

Incident Response Services

Plan Development, Readiness Review and Emergency Services

In today's information climate, you must be prepared not only to quickly locate and identify an attack in progress, but to immediately move to counter it before any damage is caused. However, if you're just launching your cybersecurity practice, or want to build on an existing practice with some outside help, turn to Tech Data to deliver the services your customers need:

Incident Response Plan
Preparing to respond quickly and decisively to any incident alert begins with the development of a detailed Incident Response Plan that describes the steps every team member must take to respond to an incident alert. This includes documenting who needs to do what, who needs to be notified and how recovery can be achieved in the shortest time possible.

When you provide your customer with Tech Data's Incident Response Plan development services, our experts work directly with you and your customer to create everything they'll need, from policies to playbooks. We also offer the guidance necessary to properly put the plan in place.

Incident Response Readiness Review
Are your customers ready for a cyberattack? Our service providers carefully examine their state of cyber readiness and make recommendations as to what remedial steps need to be taken to improve their security posture. If your customer currently lacks an incident response plan, or if they haven't performed an incident response readiness review in more than one year, this is a great place to start!

Incident Response Emergency Service
Breaches happen, even despite the best preparation and planning. Our incident responders provide rapid breach remediation assistance. They will address the overall impact of the incident and cut the time it takes to return to normal business. We know time is critical in these moments, and engagement can begin within a few hours of signing a statement of work.

> **In today's information climate, you must be prepared not only to quickly locate and identify an attack in progress, but to immediately move to counter it before any damage is caused.**

Vulnerability Assessment and Penetration Testing

Our assessments are fee-based services that evaluate the technical security of a customer's network in the form of vulnerability assessments or penetration testing. These services identify security weaknesses and exploitable vulnerabilities with objective results and clear recommendations. They'll also deliver a roadmap to help your customers identify and deliver appropriate products and services to best fit their needs.

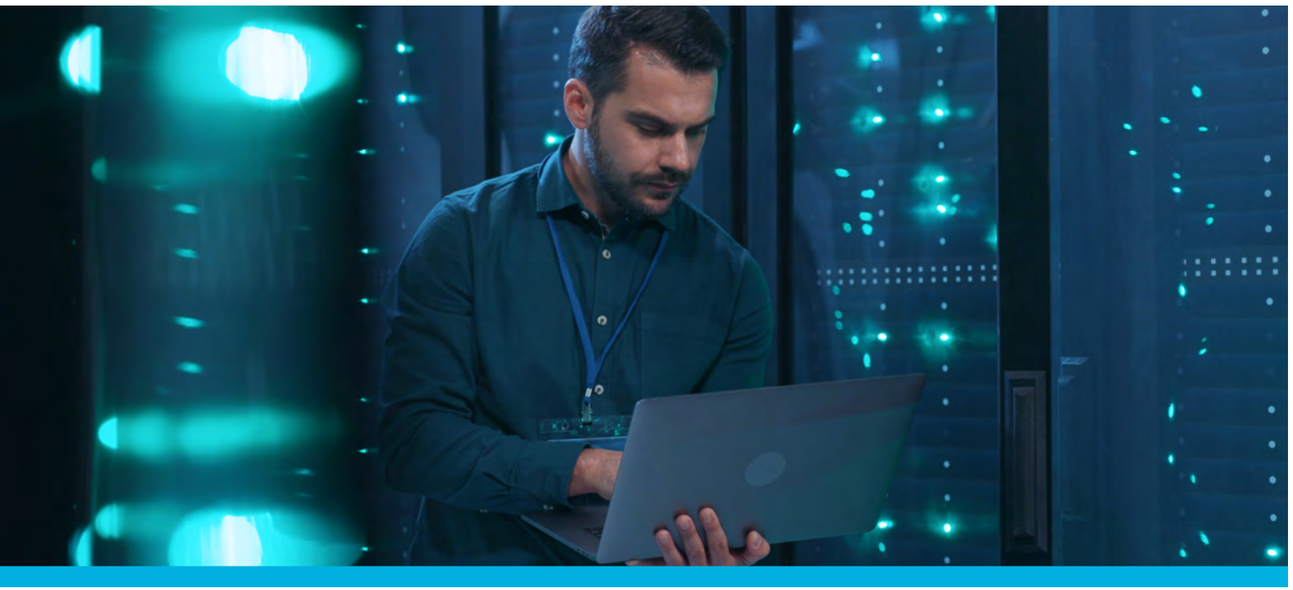
Vulnerability Assessments

- Comprehensive view of technical vulnerabilities
- Identifies common misconfigurations that attackers exploit
- Identified vulnerabilities are evaluated and scored based on their prioritization and likelihood to be exploited
- Provides evidence to efficiently allocate limited resources

Penetration Testing

- Demonstrates necessary conditions and methods used to exploit vulnerabilities
- Reveals pathways that lead to sensitive data disclosure
- Allows realistic evaluation of defensive posture
- Proves which vulnerabilities are exploitable to prioritize for remediation

For more information on Tech Data's Professional Services, please contact us at SecurityServices@techdata.com.



Develop and Practice Your Skills at the Cyber Range

The Tech Data Cyber Range helps partners practice and develop cybersecurity skills, leveraging multiple technologies and experiences. As the only Cyber Range in the distribution channel, we encourage our partners to utilize our expertise and vendor technologies to improve their cybersecurity posture.

To engage with the Tech Data Cyber Range or to sign up for one of our many security offerings, reach out to us at **cyberrange@techdata.com** or visit our website at **cyberrange.techdata.com**