NAVIGATING CYBERSECURITY FRONTIERS

A DEEP DIVE INTO A CYBER RANGE

WHITEPAPER

Executive Overview

In an era of escalating cyber threats, ensuring robust cybersecurity preparedness is paramount for organizations across sectors. A cyber range offers a dynamic platform for professionals to hone their skills and confront evolving threats effectively. This whitepaper delves into the intricate landscape of a cyber range, providing a detailed analysis of leading providers and their offerings. From military applications to educational initiatives and commercial deployments, this exploration aims to equip organizations with the insights needed to navigate the cyber range terrain and fortify their cybersecurity posture.

Key Takeaways:

01

Diverse Deployment Models

02

Comprehensive Cyber Range Types

03

Real-World Training Scenarios

04

Leading Solution Providers Analyzed

A Cyber Range and ItsTypes

A cyber range can be defined into three broad categories: Commercial, Educational and Government cyber range, which are all in operation today.

Based on their purpose of utilization, the cyber range are as follows:

Military, Defense and Intelligence: Consumed by military organizations and government agencies, this is a cyber range that enables cyber warriors with skills to counter cyber terrorism. They are aimed at finding weaknesses and vulnerabilities. Military uses of a cyber range are mostly focused on enabling development and deployment of cyber testing capabilities and facilitating the scientific use of cyber testing methods.

Education: In 2015, using a Cyber Range for education started taking shape. The intent was to provide training on methods required by professionals to learn or enhance their skill sets for cyber-attack defence and detection, developing certifications, collaborate with industries and carry out research. The goal is to provide training so that students can imitate to be network administrators and study-simulated attacks.

Enterprise and Commercial: Enterprises and commercial organizations use cases for deploying a cyber range to strengthen cyber security capabilities of their organization and teams. They need a superior and advanced way to develop ranges to be at par with the exponential growing technologies, threats, applications and traffic. They provide a cyber range solution which simulates operationally relevant environments that replicate and enable sophisticated simulations.

Service Providers: These are solution vendors who offer a cyber range as a Service. This range is hosted on the cloud and help organizations simulate specific near like scenarios imitating their real-time environments and offer training and simulations ensuring advanced training and testing services.

Open-Source: Security professionals need to gain expertise to perform multiple activities in different environments which may include production networks. These may lead to serious consequences. A few open-source ranges have been hosted on the cloud. These ranges provide free, internet accessible and a safe environment for novices and experts to test their skills and conduct security practices.

A Cyber Range and Its Deployment

A Cyber range is deployed using three main models: Hosted Cloud, On-Premises, and Hybrid. Each deployment model offers unique advantages, allowing organizations to choose based on their specific requirements, support needs, scalability, and cost considerations:

Hosted Cloud Cyber Range: Provided as a service by vendors, hosted cloud cyber range offer flexible pay-per-use or subscription-based models. Vendors manage infrastructure, curriculum, and customization, making them accessible from anywhere with an internet connection. These ranges are ideal for organizations seeking scalability, flexibility, and ease of access.

On-Premise Cyber Range: On-premise cyber range is installed and operated within an organization's premises. This deployment model offers greater customization options and control over infrastructure, catering to organizations with specific security or compliance requirements. An on-premise range is suitable for organizations that prioritize data sovereignty, regulatory compliance, or confidentiality concerns.

Hybrid Cyber Range: A hybrid cyber range combines elements of both hosted cloud and on-premise models, offering added flexibility and scalability. Organizations can leverage the benefits of both deployment approaches, seamlessly transitioning between cloud-based and on-premise environments as needed. Hybrid ranges are ideal for organizations with dynamic or fluctuating demand for a cyber range resource.

Examples of a Leading Cyber Range & its Solutions:

A cyber range solution caters to different industry needs and deployment preferences. Below are examples, each offering unique functionalities and capabilities:

Hosted Cloud Cyber Range:

1. Accenture Cyber Range: Hosted as a service, with locations in Houston, Washington, D.C., and Essen, Germany, Accenture Cyber Range primarily targets Industrial Control Systems (ICS) security. It enables organizations to test, stage, and mitigate vulnerabilities in critical infrastructure, offering readiness against advanced cyber threats, application security advisory services, cyber investigation, forensics, and threat intelligence.

2. Cloud Range: This is a cyber range that delivers a SAAS-based model, offering simulated scenarios for training cybersecurity teams and assessing organizational readiness. With next-generation technology and industry-specific scenario planning, it supports thousands of simultaneous users and offers customized training environments accessible from anywhere without physical infrastructure requirements.

3. CRUD11 - Cyber Range at the University of Delaware: CRUD11 is an exclusive cyber range for student skill development, offering practice in security flaws testing, coding, attack response, and countermeasure techniques. It conducts individual and group exercises, including Capture The Flag (CTF) events, with plans to expand capabilities for multi-facility activities and cloud infrastructure support.

4. Cyber Czech (KYPO CYBER RANGE PLATFORM): Developed for practical cybersecurity training, Cyber Czech leverages cloud technology for scalability and automation. It provides affordable and cost-efficient training with human-readable data serialization languages, emphasizing community building and sharing of training resources. It offers emulated virtual environments for cybersecurity training and practical exercises, focusing on scenarios such as penetration testing, malware analysis, and log analysis.

5. CYBER-RANGES by Silensec: Silensec's cyber range harnesses cloud technology to manage realistic cyber scenarios, catering to individuals and enterprises for training, testing, and evaluating cybersecurity readiness. It offers a wide range of scenarios, including penetration testing, reverse engineering, malware analysis, and computer forensics, supporting single-user and multi-user environments.

On-Premise Cyber Range:

1. Arkansas Cyber Range: Established for educational training purposes, Arkansas Cyber Range offers a dedicated cyber range for students at the University of Central Arkansas. It enables simulation of various network configurations and attack scenarios, facilitating hands-on learning and practical skill development tailored for academic use.

Hybrid Cyber Range:

1. Arizona Cyber Warfare Range: Providing hands-on cybersecurity training and innovation, the Arizona Cyber Warfare Range emphasizes real-world scenarios and practical learning. It offers live-fire cyber warfare exercises, open to submissions for real-world security assessments, and remote access options for users. Focused on fostering a community of white-hat hackers and cybersecurity enthusiasts, it offers training within the US and allied countries.

2. Austrian Institute of Technology (AIT) Cyber Range: AIT Cyber Range provides IT security training tailored for individuals and organizations, focusing on different skill levels and incident response processes. It offers realistic virtual environments for simulating critical IT systems, incident response training, and security process validation, catering to IT security managers, specialists, IT professionals, and government entities, with certification of knowledge and processes.

3. Baltimore Cyber Range: This is a cyber range that helps prepare IT professionals for hands-on security operations center (SOC) training, focusing on workforce development and real-world attack scenarios. It offers customized training for entry-level, journeymen, and advanced students, covering CompTIA certifications and SOC simulation exercises. Deployed as instructor-led training, it emphasizes hyper-realistic virtual network environments and real-world threat simulations.

4. Cyber Range and Training Environment: CRATE provides security competitions and exercises, utilizing many virtual machines in a controlled environment for realistic cyber scenarios. It offers a web-based interface for network design and deployment, facilitating logging, monitoring, and traffic generation tools for emulating user behavior. With scalability starting with donated servers, it now comprises 800 servers, facilitating the deployment of diverse network configurations and operating systems.

5. Georgia Cyber Range: Hosted at the Georgia Cyber Center, the Georgia Cyber Range provides a versatile platform for cybersecurity education, training, research, and development. Leveraging open-source components and a kinetic framework, it offers reproducible environments for advanced research and training across various technologies and domains.

6. Raytheon Technologies CODE Center: Raytheon's Cyber Operations, Development, and Evaluation (CODE) Center is a cyber range for testing mission-critical systems against cyberattacks. It enables organizations to assess technology resilience, simulate cyber exercises, and evaluate emerging techniques for cyber protection.

7. Vector Synergy CDeX: Vector Synergy's CDeX cyber range solution offers advanced training simulations for IT security teams, available as both cloud and on-premise deployments. With features like team training, complex network infrastructures, and interactive solutions, it enhances organizational resilience and improves team coordination and communication.

A cyber range solution caters to specific industry needs and deployment preferences, offering diverse functionalities for training, testing, and evaluating cybersecurity readiness. Whether hosted on the cloud, on-premise, or hybrid environments, these platforms empower organizations to enhance their cybersecurity posture and stay ahead of evolving threats.
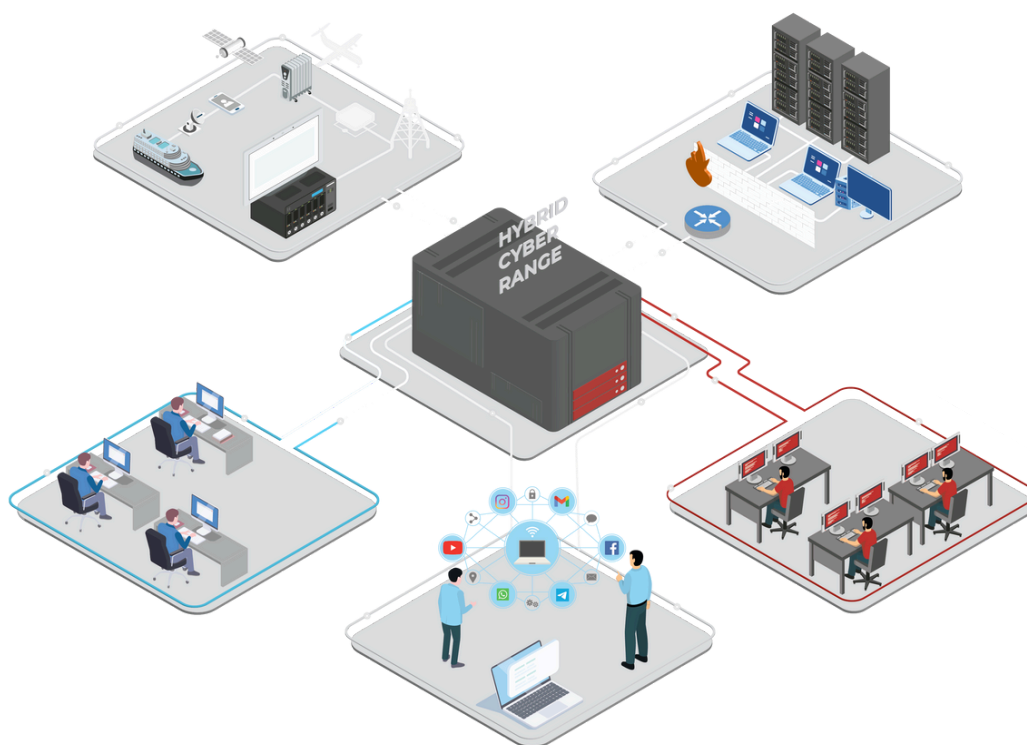
CONCLUSION

In an ever-evolving landscape of cyber threats, cybersecurity preparedness is paramount for organizations across all sectors. A cyber range offers a dynamic platform for professionals to hone their skills and effectively confront these threats. This whitepaper has provided a detailed analysis of a cyber range and its leading providers and their offerings, categorizing them into Military, Education, Enterprise, Service Provider, and Open-Source categories. Additionally, it explored the deployment models of a cyber range, namely Hosted Cloud, On-Premise, and Hybrid, offering insights into their advantages and considerations.

By understanding the types of a cyber range and their deployments, organizations can make informed decisions to fortify their cybersecurity posture. Whether hosted on the cloud, on-premise, or in a hybrid environment, a cyber range empowers organizations to stay ahead of evolving threats and ensure robust cybersecurity preparedness.

CyberKshetra provides organizations the platform to train, practice, and improve their cyber skills, offering organizations a beacon to fortify their cybersecurity defense and enhance cyber resilience. At its core, CyberKshetra is a secure training environment simulating real-world cyber threat scenarios, paving the way for a more secure digital future and more prepared cybersecurity professionals.