MISSION READINESS RANGE

Enabling Skill Mastery Through Scenario-Driven Mission Rehearsal

Powered by Capture the Packet™

IMTS
INNOVATIVE MANAGEMENT & TECHNOLOGY
SERVICES

Table of Contents

Introduction

The **Mission Readiness Range™,** part of the **ITI Government Training Cetner of Excellence™,** is a world-class training platform and skill assessment suite, designed and enhanced over the last 15 years to prepare individuals and teams for real-world challenges across cybersecurity, infrastructure, and insider threat domains. With mission rehearsal at its core, the platform enables participants to develop and validate critical skills in immersive, scenario-driven environments.

With more than a decade of proven performance, the Mission Readiness Range is trusted by governments, corporate entities, and all branches of the U.S. military—including members of the Intelligence Community and international governments. This platform has been deployed worldwide, serving as a cornerstone for mission-critical training and assessment.

Overview

Sophisticated Challenges and Professional Competitions

Renowned for creating the most sophisticated challenges in the industry, our platform's content is developed by experts with years of experience designing custom scenarios. Beyond cutting-edge training solutions, we bring unmatched expertise in running professional competitions and events at prestigious conferences such as DEF CON, Black Hat, Cyber Shield, Cyber Gauntlet, Code Blue Japan, and RSA.

Supporting ITI's Master and Expert Certifications

As the foundation for ITI's **Master and Expert Certifications**, this SaaS-based platform delivers rigorous, standards-aligned training. Participants engage in dynamic, scenario-driven exercises that bridge theory and practice, ensuring both individual excellence and team cohesion.

Full NICE and DCWF Integration

The Mission Readiness Range combines the power of gamified training with comprehensive alignment to the **NICE Cybersecurity Workforce Framework (NICE)** and the **Defense Cyber Workforce Framework (DCWF)**. Participants gain role-specific, standards-aligned training by leveraging mapped work roles and tailored content, ensuring they acquire the precise knowledge, skills, and abilities (KSAs) required for success.

Effortless Challenge Navigation

Our intuitive challenge menu makes selecting training scenarios fast and seamless. Participants can sort content by challenge type, difficulty level, challenge ID, or by specific roles and KSAs defined by frameworks such as NICE and DCWF. This streamlined approach ensures training is both targeted and relevant, maximizing the impact of each session.

As one of the few training platforms offering such deep integration, the Mission Readiness Range empowers organizations to achieve critical workforce development goals while ensuring their teams are equipped to excel in dynamic, real-world environments.

Mission Readiness Range Scale and Types

Mission Rehearsal at Scale

Designed for both individual skill-building and team-based exercises, the Mission Readiness Range can scale to support hundreds or even thousands of participants. Its versatility ensures readiness for organizations of any size, making it the ideal solution for collaborative mission rehearsal and operational training.

Deployment Options

The Mission Readiness Range offers flexible deployment options to meet diverse training needs and security requirements. These include a scalable **Software-as-a-Service (SaaS)** model and portable **Physical Appliance** deployments, ensuring accessibility in any environment, from open networks to secure classified spaces.

Software-as-a-Service (SaaS)

- Train securely from anywhere with scalable capacity, supporting individual users or thousands of participants simultaneously.
- Accessible from government networks and compatible with a range of security infrastructures.
- Flexible licensing options, including single licenses and month-to-month plans.
- Cost-effective solutions with volume discounts to meet organizational budgets.

Physical Appliance

- Portable and deployable in environments with strict security requirements, including TS/SCI spaces with polygraph protocols.
- Operates independently of the internet, ensuring secure training within classified spaces.
- Integrates seamlessly with existing range equipment to support large-scale or custom scenarios.
- Compact and lightweight design for easy transport, including via commercial airlines.

These deployment options allow organizations to maximize the impact of mission rehearsal and operational training, regardless of location or infrastructure constraints.

Challenge Categories and Formats

The Mission Readiness Range offers a comprehensive array of challenge categories tailored to develop and assess skills across various domains, including cybersecurity, infrastructure, and notably, insider threats. This platform uniquely features ready-to-deploy insider threat scenarios, making it an essential resource for the Insider Threat mission space. Each challenge is meticulously crafted to align with real-world scenarios and meet organizational needs.

Diverse Skill Areas

Challenges focus on defensive and offensive cyber operations and support, including but not limited to roles that support SOC operations, open-source intelligence, forensic analysis, and red team tactics, spanning dozens of categories and scenarios aligned with DCWF and NICE requirements.

Custom Content Development

Challenges are developed in-house to ensure data privacy and tailored solutions that meet specific customer requirements. This focus on customization allows the range to offer scenarios that are directly relevant to the threats and technologies faced by today's cybersecurity professionals.

Continuous Updates

Content evolves regularly based on changes in the operational landscape and customer feedback, ensuring relevance and cutting-edge training. This dynamic update process keeps the training material fresh and reflective of current and emerging cyber threats.

Walkthrough Integration

Training is enhanced with walkthroughs, providing in-depth explanations to improve subject matter understanding. These guided tutorials support learners in grasping complex concepts and applying them in practical scenarios effectively.

Crowdsourced Content

Feedback-driven content creation ensures a dynamic library of challenges, addressing shared needs across the user base. This approach allows the platform to adapt and expand its offerings based on direct input from its community of users.

Key Training Categories

Advanced Persistent Threats (APT)

Develop strategies to detect, counter, and mitigate persistent adversarial activities. This focus equips learners with the skills to handle sophisticated and prolonged cyber threats effectively.

Insider Threats

Simulate scenarios involving unauthorized access and malicious insider activity. This training focuses on detecting and mitigating risks posed by potential insider threats, crucial for professionals tasked with safeguarding sensitive information and maintaining organizational security.

Web Attacks and Penetration Testing

Identify, mitigate, and defend against common vulnerabilities in web applications. This training is crucial for professionals aiming to secure web environments against a range of attack vectors, enhancing their ability to protect critical online infrastructure.

System Forensics

Investigate and recover critical data from compromised systems. This training is essential for forensic analysts who must retrieve and analyze data following cybersecurity incidents.

File Forensics

Analyze files for signs of tampering, malware, or unauthorized changes. Essential for professionals tasked with ensuring the integrity and security of data files, this training equips learners to detect and respond to sophisticated digital threats effectively.

Network Forensics

Perform packet analysis, traffic inspection, and anomaly detection to uncover threats. This category provides critical skills for analyzing network data to detect, investigate, and mitigate security incidents in real-time.

Reverse Engineering and Malware Analysis

Dissect software to understand its design, functionality, or malicious intent. Analyze and interpret executable files and documents to uncover hidden functionality or malicious behavior.

Internet of Things (IoT)

Learn to secure interconnected devices and networks from emerging IoT-specific threats. As IoT devices proliferate, understanding how to safeguard these systems is crucial for cybersecurity specialists.

Misconfigured Devices

Detect and remediate common configuration errors that create security vulnerabilities. This training is crucial for professionals responsible for maintaining system security and integrity, providing them with the skills needed to identify and correct potential security flaws before they can be exploited.

Wide Area Networks (WAN)

Secure and optimize complex, distributed network environments. raining focuses on managing and protecting extensive network systems that span multiple locations, essential for professionals tasked with ensuring robust network security and performance.

Local Area Networks (LAN)

Address challenges in configuring, managing, and securing network infrastructure. Essential for professionals tasked with maintaining organizational connectivity and security.

Cryptography

Build expertise in encryption protocols, cryptanalysis, and secure communication practices. This category is vital for professionals working to protect data integrity and privacy in various digital communications.

Legacy Protocols

Understand and secure outdated or legacy systems still in use across many industries. This category focuses on the unique challenges associated with older technologies, providing the skills needed to maintain security without disrupting existing infrastructures.

Voice over IP (VoIP)

Address vulnerabilities in voice communication systems and protocols. Training focuses on securing VoIP infrastructure from eavesdropping, denial of service, and other cyber threats, essential for professionals managing modern communication technologies.

Challenge Formats

Multiple Choice

Provides scenario-based questions to test decision-making and technical knowledge. These challenges help assess learners' understanding and quick thinking in response to security dilemmas, making them a staple in cybersecurity training.

Matching

Reinforces familiarity with technical data like port maps, protocols, and error codes. This format is essential for professionals who need to rapidly identify and address network issues or security breaches accurately.

Downloadable Artifacts

Offers contained training scenarios while preparing users for live environments through realistic materials. This format is designed to enhance practical skills and ensure readiness for real-world applications.

Live Services

Presents interactive, real-time systems for tasks like scanning open ports or assessing vulnerabilities, creating hands-on learning opportunities. . This dynamic format is crucial for honing operational cybersecurity skills in a controlled, yet realistic setting.

Syntax-Based

Focuses on mastery of command-line syntax, improving proficiency with system commands. This format is vital for IT professionals who require deep technical knowledge to manage complex systems and respond to incidents effectively.

Hybrid Challenges

Combines multiple formats to deliver a comprehensive and versatile training experience. This innovative approach allows participants to engage in diverse learning activities that mimic the multifaceted nature of cybersecurity threats.

These categories and formats ensure that participants are equipped to meet the demands of both individual roles and collaborative team missions.

Modes and Features

The Mission Readiness Range delivers versatile modes and features that adapt to a variety of training objectives and engagement strategies, ensuring an impactful learning experience.

Scenario-Based Training

Participants solve progressively challenging tasks that develop both offensive and defensive skills. Ideal for both individual and team-based learning, this mode encourages critical thinking and tactical adaptation in dynamic scenarios.

Team-Based Competitive Training

Teams operate in dynamic environments with their own networks, where they secure their systems and assess vulnerabilities in a collaborative yet competitive setting. This setting mirrors real-world cyber operations, enhancing strategic and operational skills.

Key Features

Gamified Training

Realistic, interactive scenarios boost engagement and facilitate advanced skill development. Gamification adds a compelling layer of realism and excitement, making learning both effective and enjoyable.

Traffic Generator

Simulates realistic network traffic and live threats in controlled environments, providing hands-on experience with essential tools and techniques. This feature is crucial for preparing trainees to handle real cybersecurity incidents effectively.

Tool Agnostic

Allows trainees to use their daily operational tools, ensuring seamless translation of skills into real-world applications. This flexibility supports a wide range of cybersecurity practices and tools, enhancing adaptability and proficiency.

Anti-Collusion Measures

Encourages teamwork and problem-solving while preventing unauthorized sharing of solutions. This feature fosters a culture of integrity and independent problem-solving among trainees.

Single Sign-On (SSO)

Simplifies access through integration with popular SSO platforms, including military CAC systems. This convenience enhances user experience and security, streamlining the training process.

Knowledge Base and Hints

Built-in expert resources and guided hints ensure continuous learning and support. This repository is invaluable for reinforcing training materials and providing additional insights on complex topics.

Targeted Content

Challenges can be customized by difficulty, subject matter, or specific job requirements to deliver tailored training experiences. This adaptability ensures that training is relevant and closely aligned with trainee needs and industry standards.

Flexible Training Packages and Prices

The Mission Readiness Range offers four flexible tier packages tailored to meet the needs of individuals and organizations.

Essentials Tier (Bronze)

Focused on foundational knowledge and introductory training, this tier provides 3-month access to the Mission Readiness Range and over 100+ curated CTI courses designed to build core cybersecurity skills.

Advanced Tier (Silver)

Building on foundational skills, this tier adds over **100+ hands-on labs** to reinforce practical knowledge in real-world scenarios, integrating interactive exercises with CTI courses.

Pro Tier (Gold)

Expanding on the Silver Tier, the Pro Tier introduces the **Tech Pro Library**, offering advanced resources, to include a subscription to the EC-Council Learning Pro+ catalog, to support professional development, career advancement, and certification preparation.

Elite Tier (Platinum)

Combining all features of the Pro Tier, this package adds full access to the **EC-Council On-Demand Catalog**, including all courses with certification exams.

For teams, we offer suite packages that can be customized to include multiple participants, allowing organizations to scale training while tailoring resources to their specific needs. To ensure the Mission Readiness Range is accessible for organizations of any size, we offer straightforward pricing options. Visit **Training.IMTS.Store** for more details on tier packages.

Tech Pro Library Overview

Take your Mission Readiness Range training to the next level with the ***Pro Tier (Gold)***, offering a comprehensive suite of resources under the Tech Pro Library to support continuous learning and professional development in IT and cybersecurity. This upgrade enhances your organization's capabilities by providing the features described below.

Extensive Course Library

Over 600 premium online courses covering IT and cybersecurity topics, from foundational to advanced levels. This library is curated to provide comprehensive knowledge tailored to the needs of modern IT professionals.

Hands-On Applied Labs

Access to more than 15,000 labs and lab demos designed to build practical, real-world experience. These labs are crucial for applying theoretical knowledge in simulated environments that mimic real-world challenges.

Knowledge Assessment

Over 15,500 practice questions to test and reinforce learning. These assessments are designed to gauge progress and ensure understanding of complex topics in cybersecurity and IT.

Structured Learning Paths

Choose from 50+ learning paths for guided, career-focused progression. Each path is structured to guide learners through incremental challenges, ensuring a thorough understanding of each subject.

Certification Preparation

Courses aligned with certifications from top providers such as AWS, CompTIA, EC-Council, ISC^2, Microsoft, ISACA, and more. This preparation is essential for professionals aiming to validate their skills through recognized certifications.

Continuing Education

Continuing Education: Stay current with regular updates reflecting the latest trends, threats, and best practices in IT and cybersecurity. This ongoing education is vital for staying ahead in the rapidly evolving tech landscape.

Exclusive Discounts and Savings

Active subscribers receive a 5% discount on all ITI courses and bundles. Enjoy 20% off CompTIA certification exam vouchers. These savings encourage learners to pursue certification by reducing the financial barrier to entry.

Exam Optional Certification Course Upgrades

Add annual subscriptions to EC-Council's OnDemand catalog or CompTIA courses, complete with exam vouchers. This option provides flexibility for professionals to choose advanced training according to their career goals.

The Tech Pro Library upgrade offers unmatched value for organizations seeking to ensure their teams are fully equipped with cutting-edge skills and knowledge, making it an ideal addition to the Mission Readiness Range package.

Annual Operational Support Agreement

Expand the capabilities of your Mission Readiness Range with our Annual Operational Support Agreement. This essential add-on ensures your system remains at the forefront of cybersecurity training technology, whether you're using our SaaS solution or physical appliances. The agreement covers one calendar year and includes:

- **Core Feature Updates**: Gain access to additional CORE features as they become available, keeping your system cutting-edge.
- **Challenge Crowdsourcing**: Engage with a dynamic community to contribute and benefit from new challenges, scenarios, and themes.

- **Continuous Content Refresh**: Regularly receive new scenarios and challenges, keeping the training environment diverse and up-to-date.
- **Quarterly Software Updates**: For clients using physical appliances, we provide quarterly updates to the main CTP server software, which include bug fixes and enhancements.

This tailored support ensures your training solutions are always aligned with the latest cybersecurity trends and operational requirements. Due to the customized nature of this service, costs may vary. Please contact us to discuss detailed pricing and how this agreement can support your training goals.

Conclusion

The Mission Readiness Range, complemented by the Tech Pro Library Upgrade and Annual Operational Support Agreement, provides an unparalleled blend of cutting-edge cybersecurity training and continuous system enhancement. This integration ensures that individuals and teams not only develop essential skills but also remain at the forefront of technological advancements and best practices in cybersecurity.

By choosing the Mission Readiness Range, your organization gains access to an innovative training environment where complex challenges are addressed in real-time, fostering a culture of continuous improvement and readiness. Engage with us today to see how our comprehensive solutions can transform your cybersecurity capabilities and prepare you for the challenges of tomorrow. Contact us today by visiting our websites or email us at training@imts.us to explore how the Mission Readiness Range can transform your training program and mission readiness.