Organizations worldwide are facing a critical shortage of skilled cybersecurity personnel to defend the new age cyber-attacks. This urgent situation is exacerbated by the weaknesses and vulnerabilities that continue to pervade critical IT infrastructures despite billions of dollars being invested in cybersecurity measures. Addressing these problems requires Internet-scale simulation environments, along with a comprehensive training curriculum and proven methodologies.

To reduce the impact of cyber adversaries, organizations need to bet on human capital to improve the security posture of their digital infrastructure, as equipment alone is not enough to build a solid defense. In order to develop robust teams, a versatile and simulation-rich platform is required to teach right infosec skills and knowledge that allows teams to react to real-world cyber threats in a controlled environment. Such platform will not only provide them better exposure to attacks but also increase their confidence and response capabilities at the times of real cyber assault.

Purple Range™ Solutions
Purple Range is a hyper-realistic simulation lab that allows participants to build the skills and experience necessary to combat today’s most ruthless cyber attacks. The platform uses simulation as its foundation to mimic any infrastructure and cyber attacks, thus providing security teams a controlled and war-game like environment to grow and innovate by playing a role of both attacker and defender.

**Purple Range™ Advantages**

**Build the right skills & experience**
The range offers a unique and immersive attacking and defensive training experience for teams to learn new skills and knowledge, preparing them to withstand and defeat any cyber attack.

**Mimic modern infrastructures**
Purple Range is capable of mimicking modern infrastructures and attack, thus enabling participants to build better response capabilities.

**Evaluate your Team’s readiness**
The platform provides a clean scoring mechanism, making it easy for moderators/trainers to evaluate the performance of participants and judge their response aptness.

**React against real-world cyber threats**
With 20+ inbuilt real-world attack scenarios, the range can be leveraged to launch a variety of realistic cyber attacks to test team readiness and approach.

**Test your defense capabilities**
With a variety of attacks and other scenarios, the organizations can test the resistance of their defense team by pushing it to its maximum capabilities.

**Build a Purple Mindset**
The range establishes its foundation on a Purple Theme to allow participants to learn both red and blue skills, thus preparing them to build a resilient defense architecture while anticipating every move of a hacker.

---

*Figure 1: Purple Range Simulated Environment*
Features
The range enables security professionals to learn best Infosec skills and knowledge in a controlled and hyper-realistic environment.

- Recognize patterns for security threats and compromise.
- Recognize threats faster and practice responding to them properly.
- Simulate critical infrastructure components, including computer servers and clients.
- Simulate and conduct offensive and defensive operations against enemy targets to protect critical infrastructure components.

Purple Range™ Users
Cyber Range is highly instrumental in shaping the future of infosec training, and the platform is versatile enough to benefit everyone associated with building a strong cyber defense.

Participants: To apply their theoretical knowledge in a simulated network environment, improve cyber skills, work as a team for solving cyber problems and preparing for cybersecurity certifications.

Mentors: Trainers/Educators can use Cyber Range as a classroom for evaluating students’ cyber-attack and defense skills.

Professionals: They can be from different groups such as information technology, law enforcement, cyber security incident handlers that use Cyber Range for improving individual and team knowledge and skills.

Organizations: They can use Cyber Range for evaluating their own proficiency, training their team and testing new methods.

Purple Range™ Components
This lab consists of the following technologies and depicts a real-world datacentre. If needed, the entire Purple Range lab environment can be deployed on-premises using a high-end physical server or the same can be hosted in a public cloud (AWS/Azure).

Cyber Security Technologies used:
- End Point Security
- SIEM
- Threat hunting Platform
- WAF (Web Application Firewall)
- Firewall
- IPS
- DLP
- Web Proxy
- Anti-Virus
- Sandboxing
- Other real-world technologies, like Windows AD, Web Servers, Open Source Technologies, Database Servers, etc. have been used as well to replicate a real-world two-tier production setup.

There are many scenarios built in the Purple Range setup that are designed to cover a wide range of the latest attack strategies.

Currently, 20 + scenarios are included in the lab solution.

Next Step
Get in touch with our advisors for more information:

USA: Richmond, VA 23060 E info@qostecnology.net P +1 (804) 426-1694

India: Bangalore, 560052 E info@qostecnology.in P +918043700809

Website: www.qostecnology.net