PURPLE RANGE LAB

Offering Advanced Cyber Range Solutions

www.qostechnology.in

INTRODUCTION

Organizations worldwide are facing a critical shortage of Cyber Security personnel that have the skills required to defend against new age cyber-attacks. This urgent situation is made worse by the weaknesses and vulnerabilities that continue to pervade critical IT infrastructures—despite billions of dollars that have been invested in cyber security measures. Addressing these problems requires Internet-scale simulation environments, along with a comprehensive training curriculum and proven methodologies, to develop the skills necessary to defend and recover from attacks against the IT infrastructure.

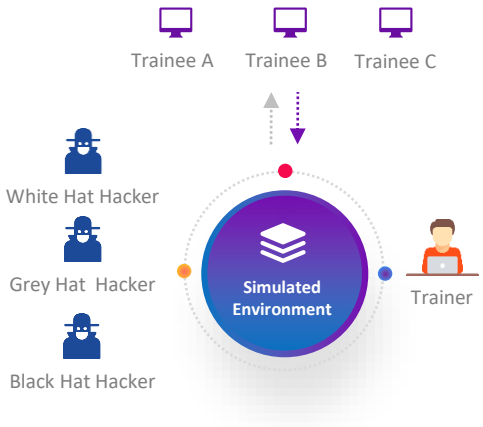
One way to mitigate the problem is to conduct training so that network security engineers can at least recognize the basics of an attack. This can save hours, maybe days, of diagnostic time. For instance, it is one thing to read a driver's manual on how to operate a car but a completely different situation to be able to successfully drive the car after only reading the drivers manually. You may know what the gas and brake pedals look like, but understanding how much pressure to apply and when to apply the pressure makes all the difference between a safe start/stop and causing an accident. You need realistically simulated, if not actual, experience to fully understand how to operate the car.

Purple Range, a Cyber Range solution, designed and developed by QOS Technology Pvt Ltd, is a training platform on cyber-attack/defense that allows organizations to increase the skills of their teams in the attacking/defensive side of their network infrastructures. Prevention exercises allow organizations to re-evaluate their business continuity plan in an event of a cyber-attack. Purple Range Lab, once deployed can be accessed over the Internet via any secure means such as VPN.

FEATURES

The range enables security professionals to learn best Infosec skills and knowledge in a controlled 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 operations against enemy targets.
- Simulate and conduct defensive operations to protect critical infrastructure Components.



CYBER RANGE USERS

The main factor of cyber range is how we make a successful outcome within the people who are going to use it. The purple range Lab has been prepared to keep this in mind and is the most important part and core philosophy of the range. The cyber Range thus can be used by four target group of people:

- **Trainees/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 Cyber Security Certifications.
- **Trainers/Educators:** Trainers/Educators can use Cyber Ranges as a classroom for evaluating their students cyber-attack and defence skills.
- **Professionals:** They can be from different groups such as information technology, law enforcement, cyber security incident handlers that use Cyber Ranges for improving individual and team knowledge and skills.
- **Organizations:** They can use Cyber Ranges for evaluating their own proficiency, training their team and test new methods.

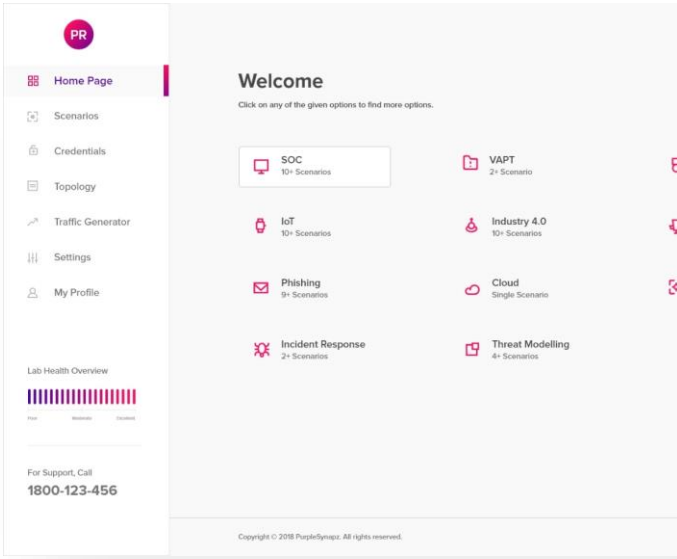
info@qostechnology.in

COMPONENTS OF PURPLE RANGE

Purple Range setup is completely built on a virtual platform and has most of the critical Datacentre Infrastructures/setup. 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.



The scenario is the central element of every training session. As a matter of fact, the main purpose of the Cyber Range is to stage scenarios that meet the training requirements. A Cyber Range team typically consists of three different teams Red, Blue and Green.

There are many scenarios built in the Purple Range setup that is designed to cover a wide range of the latest Attack Strategies. Currently 20 + scenarios are included in the lab solution:

- Basic SQLi + Local File Inclusion.
- WebShell Upload through SQLi, Privilege Escalation.
- SQLi through Cookies.
- SQLi Bypassing Filters.
- SQLi, Command Injection and Privilege Escalation.
- Enumeration, Exploiting using.
- Publicly available exploits and Metasploit (earlier Metasploit and Privilege Escalation using Exploits).
- Metasploit and Privilege Escalation using Perl Shell.
- Buffer Overflow FTP server Crash + Buffer Overflow FTP server Shell.
- Metasploit Post-exploitation and Pivoting.
- POST DOS.
- DOS Layer 7 HTTP GET Flood.
- Port Scanning.

BENEFITS

- Purple range enables security teams to practice identifying and responding to threats in a real-world environment using a variety of technologies and run-books.
- Purple Range offers an environment for teams to train collectively, improve their cyber defence skills and gain critical insight into a variety of stakeholder actions within the organization.
- Training in an authentic but controlled environment can help security teams deal with crisis situations in a rapid manner.

TRAINING OPTIONS

Purple Range Lab can be used to provide following training.

- Blue team
- Red team
- CXO breach response
- Threat Hunting
- Incident response
- Cloud Security
- CTF
- Custom

LAB SETUP OPTIONS

Based on the requirement, Customer can choose from any of the following 3 option for setting up the lab.

BRONZE

SILVER

GOLD

Purple Range solutions can also be customized to meet specific enterprise requirements

For additional information, write to **info@qostechnology.in**