CLOUD RANGE

Single Cyber Attack Training Mission

WHAT IS IT?

A single cyber attack training mission is an à la carte session where customers can train on a scenario featuring a simulated cyber attack. Choose from a variety of attack scenarios, with custom scenarios available as well. New scenarios are added regularly to keep your team up-to-date as the threat landscape becomes increasingly complex.

WHO IS IT FOR?

OT and IT SOC and incident response teams

FEATURES

- Choice of dozens of different scenarios with customizable levels of complexity
- Each session can accommodate up to 20 participants
- Onsite or remote training available
- Optional live instructors (virtual or on-premise)
- IT/OT environments
- Alignment to MITRE ATT&CK and NICE Cybersecurity Workforce frameworks
- Includes the same licensed security tools that your team uses every day

YOUR SECURITY TEAM WILL LEARN

- How to swiftly identify, detect, investigate, and respond to cyber attacks in real-time
- SIEM and firewall management & analysis
- Incident response
- Windows and Linux system management
- Advanced endpoint controls

EXAMPLE SCENARIOS

Ransomware
Phishing
DNS Tunneling
Website Defacement
OT/ICS PLC Attack
Remote Access Trojan
Web DDOS
OT/ICS Reconnaissance
Powershell Empire Attack
Spearphishing (Fin7)
Bitcoin Mining
Log4J Attack
Cyber Espionage
Supply Chain Attack
And more!

How to Purchase & Schedule Your Single Cyber Range Training Mission

1. Choose Your Mission

Select the scenario from the Cloud Range Scenario Library, which is continuously updated based on new threat vectors.

2. Choose Your Training Format

Live remote training or onsite - both are instructor-led.

3. Select Number of People

Up to 10 participants are included. More participants may be added at an additional cost per person.

4. After You Order

A Cloud Range representative will work with you to schedule your session, either onsite or remote, based on your selection.

Contact us for more information at info@cloudrangecyber.com.