MARYLAND RANGE
Cyber Security Training & Simulation Center

Cyber Security Operations Specialist

In the current cyber threat landscape, knowledge is important but no longer sufficient.
Equip yourself and your team with the right skillsets and competencies to keep an organization secure. **Cyber Security Operations Specialist (CSOS)** focuses on building cognitive and analytical abilities of participants through operational-centric training.

Cyber Security Operations Essentials

Cyber Defense Knowledge Build-up
Build-up your foundation through understanding of cyber security Concepts

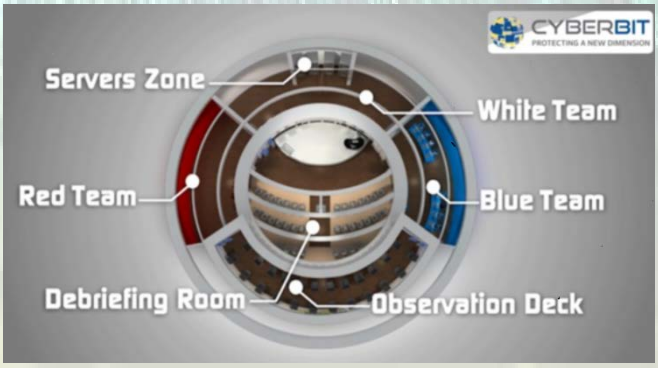
Security Tools Hands-On Exercise
Be familiarized with functionality of various security products3.

Scenario-based Training
Enhance your operational proficiency through the experience of the entire kill-chain of cyber-attack(s) in a controlled environment

Training Benefits

Cyber Security Training based on Maryland CSTR Cyber Security Center Cyber Trainer System benefits trainees by enhancing their ability to:

- Appreciate the entire kill-chain of various cyber-attack
- Develop improved response to cyber attacks
- Enhance decision-making in the event of cyber-attacks
- Enhance the collaboration between teammates working together



Who Should Attend

- Cyber Security Professionals looking to upskill their level of security operations proficiency
- IT Professionals / Engineers looking to multi-skill themselves in cyber security operations or looking to take on a cyber-security related job role
- System / Network Administrators requiring a better understanding of cyber security operations
- Information Security Managers and Executives involved in cyber security operations
- Project Managers, Risk Managers and Compliance Managers who require an understanding of cyber security operations processes and outcomes

OFFICE ADDRESS: 8 Market Place, Baltimore Maryland 21202
WEBSITE | www.MarylandRange.com | Email: info@MarylandRange.com

Course Structure

Day One	
a.	**Cyber Security Imperatives** ▪ Cyber threats, trends, terms and terminologies ▪ CIA, AAA, standards, audit, compliance and regulations ▪ Cryptography and applications
b.	**Network Technologies and Security** ▪ Introduction to network systems, types and devices ▪ Secure network protocol (SSL/TLS, SSH) ▪ Introduction to network security devices (Firewall, IPS/IDS, SIEM, etc.)
c.	**Server Systems and Logs** ▪ Types and functions of servers (web, database, mail, AD, etc.) ▪ OS, servers and their event logs (Windows, Linux,IIS, Apache, Mssql, sendmail and etc.)
Day Two	
d.	**Attack Methodology and Types** ▪ Attack phases ▪ Types of vulnerabilities and attacks ▪ Web-based attack (OWASP top 10)
e.	**Security Operations Centre and Incident Response** ▪ Different types of information security incident ▪ Information security incident management framework ▪ Overview to SOC concepts and operations ▪ Threat identification, threat correlation, threat aggregation, threat filtering (through applications and server logs) ▪ Incident handling, response management, notification and reporting
f.	**Security Products and Hands-On** ▪ Checkpoint Firewall, Security Information and Event Management(SIEM) ▪ Monitoring tools such as Wireshark, Process Monitor
Day Three to Five	
g.	**Security Operations Centre Cyber-Attack Scenario-based Exercises** ▪ Exposure to real-world cyber-attack scenarios ▪ Developing detection, and response skills through team-based exercises