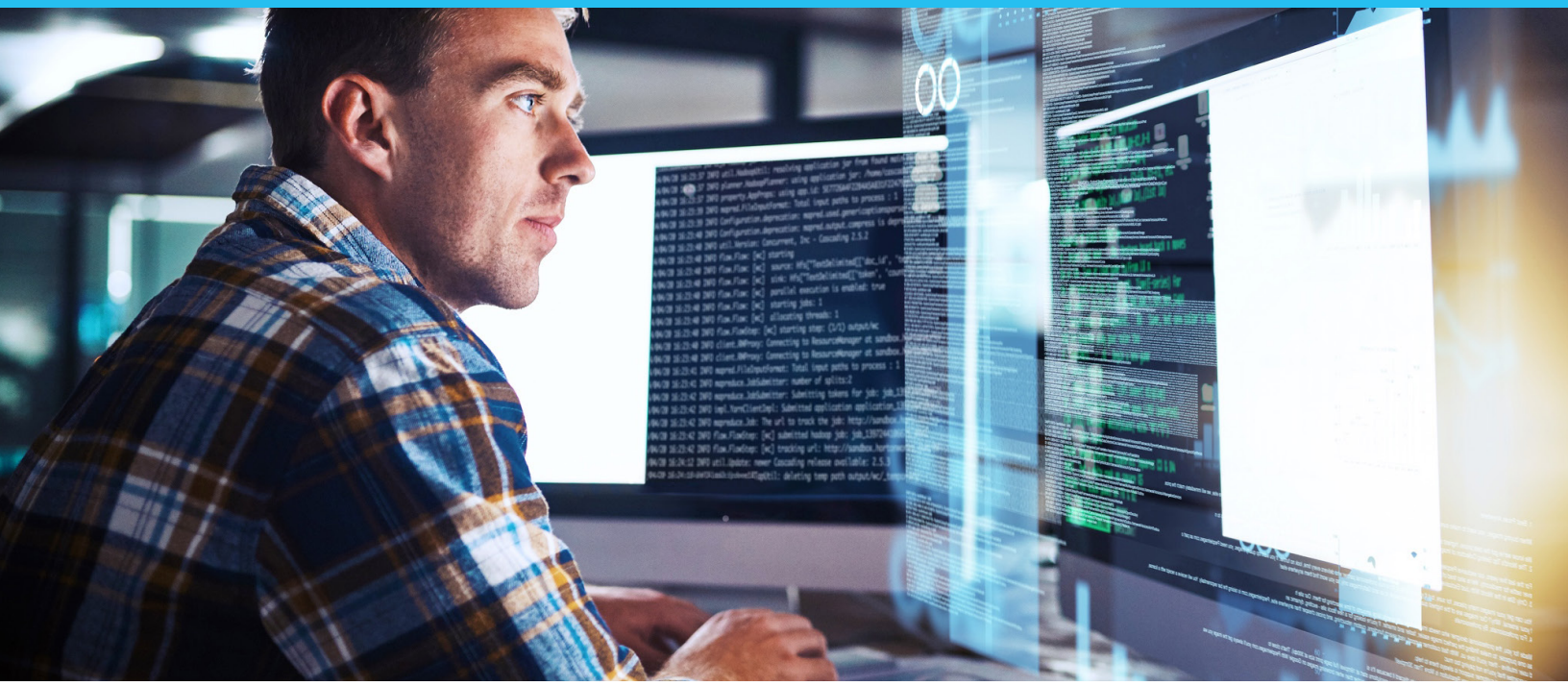
Cybint
BARBRI Cyber Solutions



CSA SIMU-LAB SUITE LAB SCENARIOS

The delivery model of the CSA Simu-Lab Suite is based on the Case Scenario Approach using Accelerated Learning principles.

- Subject matter in contextualized within 10 cyber security lab scenarios that become progressively more complex and challenging. (Additional scenarios are available for advancing curricula).
- Each lab scenario is an authentic/dramatic cyber security event.
- Trainees are limited in their time to resolve the problem.
- Each lab scenario follows the cybersecurity problem- solving sequence:
  - Alert
  - Identify the problem
  - Assess the potential implications
  - Choose and implement the optimal solution
  - Review lessons learned
- Each lab scenario is self-contained, allowing learners to work through them in sequence or according to need.
- Additional scenarios can be added to address specifc skills.

Cyber Security Analyst Simu-Lab Suite Scenarios to enhance your curriculum:

- **Introduction to the Cyber Security Analyst Simu-Lab Suite**
- **Scenario 1:** Getting to know Virtual Machines and Operating Systems
- **Scenario 2:** Off-hour access to relational database triggers an alert
- **Scenario 3:** An endpoint and a server machine try to log-in with the same username and password at the same time
- **Scenario 4:** Suspicious FTP and HTTP traffic to a strange URL
- **Scenario 5:** Port scanning from external unknown IP
- **Scenario 6:** IDS alerts on outbound malicious network traffic
- **Scenario 7:** Endpoint computer issues and possible APT threat
- **Scenario 8:** Suspicious activity by domain administrator user from a VPN connection
- **Scenario 9:** The cloud service server is being attacked
- **Scenario 10:** Write a vulnerability assessment of enterprise's email server
- **Final Scenario 11:** Job interview to a cyber security position
- **Optional:** Penetration testing and/or Threat intelligence

© 2018 BARBRI, Inc. All rights reserved.

Cybint
BARBRI Cyber Solutions

The Subject Matter

The Cybint Simu-Lab Suite covers the following cyber topics (a practical perspective):

IT (INFORMATION TECHNOLOGY) SYSTEMS AND INFRASTRUCTURE WITHIN ORGANIZATIONS	• **Devices** • **Operating Systems** — Microsoft Window (+Sysinternals) — Linux — Protocols and Permissions • **Networks and Domains** — Endpoints — Servers — Network Security and Network Layer Security
DATABASES AND MANAGEMENT SYSTEMS	• **SIEM – Security Information and Event Management** • **SQL – Structured Query Language** • **Reading Logs** • **Big Data**
VIRTUALIZATION	• **Cloud Evolution and Revolution** • **Cloud Solutions** • **IOT – Internet of Things**
CYBER DEFENSE	• **IT Monitoring** • **Digital Certificates and Smart Authentication**
CYBER THREATS AND CYBER ATTACKS	• **Types of Cyber Alerts** • **Types of Cyber Attacks** • **Basic Forensics**
INCIDENT RESPONSE	• **Cyber Security Products (+Metasploit Project)** • **Next Generation Defense Mechanism** • **Liaising with employees, admin, authorities** • **Company Policies / Protocols and Legalities**

Additional scenarios can be added to address specifc skills

© 2018 BARBRI, Inc. All rights reserved.