Eric Reed
Email: eric@ericreedlive.com
Phone: 707-722-7333
Mobile: 404-277-0506

CYSA+ Course Outline

1 - Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

2 - Analyzing Reconnaissance Threats to Computing and Network Environments

- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Social Engineering

3 - Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

4 - Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

5 - Managing Vulnerabilities in the Organization

- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans
- Conduct Penetration Tests on Network Assets

6 - Collecting Cybersecurity Intelligence

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

7 - Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis

8 - Performing Active Asset and Network Analysis

- Analyze Incidents with Windows-Based Tools
- Analyze Incidents with Linux-Based Tools
- Analyze Malware

- Analyze Indicators of Compromise

9 - Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Prepare for Forensic Investigation as a CSIRT

10 - Investigating Cybersecurity Incidents

- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

11 - Addressing Security Architecture Issues

- Remediate Identity and Access Management Issues
- Implement Security During the SDLC