CSA+

Course Outline

Module 1: Threat Management

1.1 Introduction
1.2 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 1
1.3 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
1.4 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
1.5 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 4
1.6 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 5
1.7 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 6
1.8 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 7
1.9 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 8
1.10 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 9
1.11 Given a scenario, analyze the results of a network reconnaissance Part 1
1.12 Given a scenario, analyze the results of a network reconnaissance Part 2
1.13 Given a scenario, analyze the results of a network reconnaissance Part 3
1.14 Given a scenario, analyze the results of a network reconnaissance Part 4
1.15 Given a scenario, analyze the results of a network reconnaissance Part 5
1.16 Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 1
1.17 Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 2
1.18 Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 3
1.19 Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 4
1.20 Explain the purpose of practices used to secure a corporate environment Part 1
1.21 Explain the purpose of practices used to secure a corporate environment Part 2
1.22 Explain the purpose of practices used to secure a corporate environment Part 3
1.23 Explain the purpose of practices used to secure a corporate environment Part 4

Module 2: Vulnerability Management

2.1 Given a scenario, implement an information security vulnerability management process Part 1
2.2 Given a scenario, implement an information security vulnerability management process Part 2
2.3 Given a scenario, implement an information security vulnerability management process Part 3
2.4 Given a scenario, implement an information security vulnerability management process Part 4
2.5 Given a scenario, implement an information security vulnerability management process Part 5
2.6 Given a scenario, implement an information security vulnerability management process Part 6
2.7 Given a scenario, implement an information security vulnerability management process Part 7
2.8 Given a scenario, analyze the output resulting from a vulnerability scan Part 1
2.9 Given a scenario, analyze the output resulting from a vulnerability scan Part 2
2.10 Compare and contrast common vulnerabilities found in the following targets within an organization Part 1
2.11 Compare and contrast common vulnerabilities found in the following targets within an organization Part 2
2.12 Compare and contrast common vulnerabilities found in the following targets within an organization Part 3

CSA+

Course Outline Cont.

Module 3: Cyber Incident Response

3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 1
3.2 Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 2
3.3 Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 3
3.4 Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 1
3.5 Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 2
3.6 Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 3
3.7 Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 4
3.8 Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 5
3.9 Explain the importance of communications during the incident response process
3.10 Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 1
3.11 Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 2
3.12 Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 3
3.13 Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 4
3.14 Summarize the incident recovery and post-incident response process Part 1
3.15 Summarize the incident recovery and post-incident response process Part 2
3.16 Summarize the incident recovery and post-incident response process Part 3
3.17 Summarize the incident recovery and post-incident response process Part 4

Module 4: Security Architecture and Tool Sets

4.1 Explain the relationship between frameworks, common policies, controls, and procedures Part 1
4.2 Explain the relationship between frameworks, common policies, controls, and procedures Part 2
4.3 Explain the relationship between frameworks, common policies, controls, and procedures Part 3
4.4 Explain the relationship between frameworks, common policies, controls, and procedures Part 4
4.5 Given a scenario, use data to recommend remediation of security issues related to identity and access management Part 1
4.6 Given a scenario, use data to recommend remediation of security issues related to identity and access management Part 2
4.7 Given a scenario, use data to recommend remediation of security issues related to identity and access management Part 3
4.8 Given a scenario, use data to recommend remediation of security issues related to identity and access management Part 4
4.9 Given a scenario, review security architecture and make recommendations to implement compensating controls Part 1
4.10 Given a scenario, review security architecture and make recommendations to implement compensating controls Part 2
4.11 Given a scenario, review security architecture and make recommendations to implement compensating controls Part 3
4.12 Given a scenario, use applications security best practices while participating in the Software Development Life Cycle (SDLC) Part 1
4.13 Given a scenario, use applications security best practices while participating in the Software Development Life Cycle (SDLC) Part 2
4.14 Overview
4.15 Conclusion

Course Duration: 17 hours 54 minutes