

APÊNDICE A AO TERMO DE REFERÊNCIA

REQUISITOS MÍNIMOS EXIGIDOS EM CADA CURSO

1. ITEM 01 – CURSO ISC/SCADA CYBERSECURITY

- 1.1 Introdução à Defesa de Rede ICS/SCADA;
- 1.2 TCP/IP 101;
- 1.3 Introdução ao Hacking;
- 1.4 Gerenciamento de Vulnerabilidades;
- 1.5 Padrões e Regulamentações para Segurança Cibernética;
- 1.6 Protegendo a rede ICS;
- 1.7 Preenchendo o Air Gap; e
- 1.8 Introdução aos Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS).

2. ITEM 02 – CURSO E | DRP - DISASTER RECOVERY PROFESSIONALS

- 2.1 Introdução à Recuperação de Desastres e Continuidade de Negócios;
- 2.2. Gestão de Continuidade de Negócios (BCM);
- 2.3. Avaliação de RiscoAnálise de Impacto nos Negócios (BIA);
- 2.4. Planejamento de Continuidade de Negócios (BCP);
- 2.5. Estratégias de Backup de Dados;
- 2.6. Estratégias de Recuperação de Dados;
- 2.7. Recuperação de desastres baseada em virtualização;
- 2.8. Recuperação do Sistema;
- 2.9. Recuperação de Sistema Centralizado e Descentralizado;
- 2.10. Processo de planejamento de recuperação de desastres; e
- 2.11. Teste, Manutenção e Treinamento BCP.

3. ITEM 03 – CURSO C | SA - CERTIFIED SOC ANALYST

- 3.1 Operações e Gerenciamento de Segurança;
- 3.2 Compreendendo ameaças cibernéticas, IoCs e metodologia de ataque;
- 3.3 Incidentes, Eventos e Registro;
- 3.4 Detecção de Incidentes com Segurança da Informação e Gestão de Eventos (SIEM);
- 3.5 Detecção Aprimorada de Incidentes com Inteligência de Ameaças; e
- 3.6 Resposta a Incidentes.

4. ITEM 4 – CURSO E | CIH - EC - COUNCIL CERTIFIED INCIDENT HANDLE

- 4.1. Introdução ao Tratamento e Resposta a Incidentes;
- 4.2. Processo de Tratamento e Resposta a Incidentes;
- 4.3. Primeira Resposta;
- 4.4. Tratamento e resposta a incidentes de malware;
- 4.5. Tratamento e resposta a incidentes de segurança de e-mail e rede;
- 4.6. Tratamento e resposta a incidentes de segurança de aplicações web e na nuvem;
- 4.7. Tratamento e resposta a ameaças internas; e
- 4.8. Tratamento e resposta a incidentes de segurança de endpoint.

5. ITEM 5 – CURSO C | TIA - CERTIFIED THREAT INTELLIGENCE ANALYST

- 5.1. Introdução à Inteligência de Ameaças;
- 5.2. Requisitos, Planejamento, Direção e Revisão;
- 5.3. Coleta e Tratamento de Dados;
- 5.4. Reporte e Divulgação de Inteligência;
- 5.5. Segurança na Internet; e
- 5.6. Metodologia de Ameaças Cibernéticas e Kill Chain.

6. ITEM 6 – CURSO C | HFI - CERTIFIED HACKING FORENSIC INVESTIGATOR

- 6.1. Computação Forense no Mundo de Hoje;
- 6.2. Processo de Investigação Forense Computacional;
- 6.3. Noções básicas sobre discos rígidos e sistemas de arquivos;
- 6.4. Aquisição e Duplicação de Dados;
- 6.5. Derrotando Técnicas Antiforenses;
- 6.6. Análise Forense do Windows, Linux e Mac;
- 6.7. Análise Forense de Rede;
- 6.8. Investigando ataques na Web;
- 6.9. Análise forense da Dark Web;
- 6.10. Análise Forense de Banco de Dados;
- 6.11. Análise forense em nuvem;
- 6.12. Investigando Crimes por E-mail;
- 6.13. Análise Forense de Malware;
- 6.14. Análise Forense Móvel; e
- 6.15. Análise forense de IoT.

7. ITEM 7 – CURSO COMPTIA CYBERSECURITY ANALYST (CYSa+)

- 7.1. Operações de segurança;
- 7.2. Gestão de vulnerabilidades;
- 7.3. Resposta e gestão de incidentes; e
- 7.4. Relatórios e Comunicação.

8. ITEM 8 – CURSO COMPTIA SECURITY+

- 8.1. Conceitos gerais de segurança;
- 8.2. Ameaças, vulnerabilidades e mitigações;
- 8.3. Arquitetura de segurança;
- 8.4. Operações de segurança; e
- 8.5. Gestão e Supervisão do Programa de Segurança.

9. ITEM 9 – CURSO TH-200 - FOUNDATIONAL THREAT HUNTING (OSTH)

- 9.1. Conceitos e práticas de caça a ameaças;
- 9.2. Visão geral do cenário de atores de ameaças;
- 9.3. Comunicação e relatórios para caçadores de ameaças;
- 9.4. Caça com dados de rede;
- 9.5. Caça em Endpoints; e
- 9.6. Caça a ameaças sem IoCs.

10. ITEM 10 – CURSO SOC-200 - FOUNDATIONAL SECURITY OPERATIONS AND DEFENSIVE ANALYSIS (OSDA)

- 10.1. Introdução à Metodologia de Ataque;
- 10.2. Introdução ao Windows Endpoint;
- 10.3. Ataques do lado do servidor Windows;
- 10.4. Ataques do lado do cliente do Windows;
- 10.5. Escalonamento de privilégios do Windows;
- 10.6. Persistência do Windows;
- 10.7. Introdução ao Linux Endpoint;
- 10.8. Ataques do lado do servidor Linux;
- 10.9. Detecções de rede; e
- 10.10. Alertas e Evasão de Antivírus.

11. ITEM 11 – CURSO IR 200 - FOUNDATIONAL INCIDENT RESPONSE (OSIR)

- 11.1 Visão geral da resposta a incidentes;
- 11.2. Fundamentos de resposta a incidente;
- 11.3. Fases da resposta a incidentes;
- 11.4. Resposta a incidentes e planos de comunicação;
- 11.5. Técnicas de ataques comuns;
- 11.6. Detecção de incidentes e Identificação;
- 11.7. Perícia digital para incidente respondedores;
- 11.8. Caso de resposta a incidentes e gerenciamento;
- 11.9. Contenção de incidentes ativa;
- 11.10. Erradicação de incidentes e recuperação;

11.11. Avaliação de impacto inicial; e

11.12. Relatórios post-mortem.

12. ITEM 12 – CURSO EXP - 301 - WINDOWS USER MODE EXPLOIT DEVELOPMENT (OSED)

12.1 Tutorial WinDbg;

12.2. Stack buffer overflows;

12.3. Exploiting SEH overflows;

12.4. Superando as restrições de espaço: Egghunters;

12.5. Shellcode do zero;

12.6. Bugs de engenharia reversa;

12.7. Stack overflow e desvio DEP / ASLR;

12.8. Ataques de especificador de string de formato; e

12.9. Cadeias ROP personalizadas e decodificadores de carga útil ROP.

13. ITEM 13 – CURSO PEN-200 - PENETRATION TESTING WITH KALI LINUX (OSCP)

13.1. Ficar confortável com o Kali Linux;

13.2. Diversão na linha de comando;

13.3. Ferramentas práticas;

13.4. Bash Scripting;

-13.5. Coleta passiva de informações;

13.6. Coleta ativa de informações;

13.7. Verificação de vulnerabilidades;

13.8. Ataques a aplicações Web;

13.9. Introdução ao Buffer Overflows;

13.10. Estouros de buffer do Windows;

13.11. Estouro de buffer do Linux;

13.12. Ataques do lado do cliente;

- 13.13. Localização de exploits públicos;
- 13.14. Correção de exploits;
- 13.15. Transferências de arquivos;
- 13.16. Evasão antivírus;
- 13.17. Escalonamento de privilégios;
- 13.18. Ataques de senha;
- 13.19. Redirecionamento e escavação de um túnel do porto;
- 13.20. Ataques ao Active Directory;
- 13.21. A Estrutura Metasploit;
- 13.22. Império PowerShell
- 13.23. Montagem das peças: Quebra do teste de penetração; e
- 13.24. Tring Harder: Os laboratórios

14. ITEM 14 – CURSO EXP-401 - ADVANCED WINDOWS EXPLOITATION (OSEE)

- 14.1. Ignorar e evitar mitigações de segurança do modo de usuário, como DEP, ASLR, CFG, ACG e CET;
- 14.2. Manipulações de heap avançadas para obter execução de código junto com escapes de convidado para host e sandbox;
- 14.3. Desarmar as mitigações de WDEG e criar independência de versão para armamento;
- 14.4. Engenharia reversa de driver do kernel do Windows de 64 bits e descoberta de vulnerabilidades; e
- 14.5. Ignorar as mitigações de segurança do modo kernel, como kASLR, NX, SMEP, SMAP, kCFG e HVCI.

15. ITEM 15 – CURSO ADVANCED EVASION TECHNIQUES AND BREACHING DEFENSES (PEN-300 - OSEP)

- 15.1. Teoria do Sistema Operacional e Programação;

- 15.2. Execução de código do lado do cliente com o Office;
- 15.3. Execução de código do lado do cliente com JScript;
- 15.4. Processo de injeção e migração;
- 15.5. Introdução ao Antivírus Evasion;
- 15.6. Evasão Avançada de Antivírus;
- 15.7. Aplicação Whitelisting;
- 15.8. Ignorando filtros de rede;
- 15.9. Pós-exploração do Linux;
- 15.10. Quiosque breakouts;
- 15.11. Credenciais do Windows;
- 15.12. Movimento lateral de Windows;
- 15.13. Movimento lateral do Linux;
- 15.14. Ataques Microsoft SQL;
- 15.15. Exploração do Active Directory;
- 15.16. Combinar as peças; e
- 15.17. Trying Harde: Os laboratórios.

16. ITEM 16 – CURSO WEB-300 - ADVANCED WEB ATTACKS AND EXPLOITATION (OSWE)

- 16.1. Script Persistente entre Sites;
- 16.2. Sequestro de sessão;
- 16.3. Desserialização LÍQUIDA;
- 16.4. Exfiltração de dados;
- 16.5. Ignorando Filtros de Extensão de Arquivo;
- 16.6. Hashes mágicos;
- 16.7. Extensão PostgreSQL e Funções Definidas pelo Usuário;
- 16.8. Contornar restrições de REGEX;
- 16.9. Falsificação de solicitação entre sites;
- 16.10. Digite malabarismo;

- 16.11. Injeção cega de SQL;
- 16.12. Ignorar restrições de upload de arquivos;
- 16.13. Comparações soltas;
- 16.14. Contornar restrições de caracteres;
- 16.15. Objetos grandes do PostgreSQL; e
- 16.16. Depuração de assemblies .NET.