Threat Intelligence and Hunng – 360 h

Um profissional de segurança cibernética precisa entender as ameaças, os agentes de ameaças e ter uma compreensão clara de onde os invasores estão tentando tirar proveito das vulnerabilidades. Threat Intelligence e Hunting os alunos terão uma visão de onde existem vulnerabilidades em software, nuvem e outras superfícies de ataque. Ao longo do curso, o aluno explorará como classificar ameaças, trabalhar com vulnerabilidades e usar metodologias de avaliação comuns. O curso também abordará a compreensão das ameaças contra a Internet das Coisas (IOT), sistemas operacionais em tempo real e ambientes baseados em nuvem.

Disciplinas:

- Segurança Defensiva e Resposta a Incidentes
    - Introdução a segurança defensiva
    - Quem é o inimigo e Como hackers atuam
    - Mitre & Attack
    - Exploit Database
    - APTs
    - Malwares
    - Processo de Contratação de ferramentas
    - Gestão de ferramentas de segurança
    - Conhecendo uma rede corporativa de grande porte
    - Proteção contra malwares
    - Windows Internals
    - AMSI bypass
    - UAC Bypass
    - Sysmon Bypass
    - ETW bypass
    - Análise Heurística de ameaças
    - EDR x AV convencional
    - MSS
    - Firewall Next Generation x Firewalls convencionais
    - Ferramentas de detecção de Ameaças
    - Machine Learn em defesa cibernética
    - Micro Segmentação
    - Nano Segmentação
    - Publicação segura de serviços e recursos
    - WAF - Web Application Firewall
    - Vazamento de dados
    - DLP e CASB
    - Proteção de Domínio
    - Phishing e Spear Phishing
    - Security Awareness
    - DevSecOps e APP sec
    - Correlação de eventos
    - SIEM
    - SOAR
    - IDS/IPS
    - IOCs
    - Threat Intelligence
    - Análise de Malware
    - Maldoc

    - Introdução a engenharia reversa
    - Resposta a Incidentes
    - Cadeia de Custódia
    - First responder
    - Como a memória ram funciona
    - Dump de Memória
    - FTK-Imager
    - Análise de Memória
    - IPED - Polícia Federal

- Analista de SOC (Security Operation Center)
    - Introdução ao SOC
    - SIEM
    - Criando um SOC
    - Frameworks e Acesso Físico
    - Plano de comunicação e Threat Intelligence

- Malware Hunting
    - O que é uma Threat (Ameaça)?
    - Malwares, Vulnerabilidades e Exploits
    - Cenário Atual
    - Entendendo alguns ataques
    - Ameaças Avançadas Persistentes (APTs)
    - DNA de uma APT
    - Etapas de uma APT
    - Sandbox
    - Threat Hunting
    - Qual me eu deveria ter
    - Empoderando meu SOC
    - Incidentes de Segurança
    - Monitoramento de Segurança em Camadas
    - Gerenciamento de Incidentes
    - Encodings

- Estratégias de Segurança Cibernéticas
    - Introdução à Segurança Computacional
    - Introdução à Privacidade e Proteção dos Dados
    - Governança
    - Ataques e suas características
    - Ferramentas e Processos

- Detecção de Intrusão, Configuração de Perímetro e Análise de Logs
    - Segurança da Informação
    - Pilares da Segurança da Informação
    - Governança de Tecnologia em Segurança da Informação
    - Incidente de Segurança da Informação
    - Sistemas de Detecção de Intrusão
    - Pós-detecção
    - Exemplos e sistemas de detecção de intrusão

- Gestão de Segurança da Informação
    - Normas e Padrões em Segurança da Informação (ISO/ NIST /PCI)

- ISO 27001
- A estruturação de Seções
- NIST 800-53
- Ameaças, Vulnerabilidades, Riscos e Tipos de Ataques em Segurança
- Segurança em Internet das Coisas, Ciberataques e Ransomware
- Segurança em Cloud Computing
- Segurança em dispositivos móveis e pessoais

- Gerenciamento de Projeto de Redes de Computadores
  - Arquitetura de Camadas
  - Ciclo de Vida de Uma Rede
  - Planejamento de uma Rede
  - Disponibilidade de rede
  - Projetar uma Rede de Computadores
  - Tipos de Redes
  - Topologias de Redes
  - Segurança de rede
  - Dimensionamento de links
  - Implantação de Redes
  - Operar e Otimizar Redes
  - Conectores de Cabos e Guias de identificação de Ferramentas

- Cyber Threat Intelligence: Prevenção e a Redução de Ataques
  - Fases do ciclo e ameaça
  - Ferramentas utilizadas em inteligência de ameaça
  - Inteligência de Ameaça como operação
  - Responsabilidades da equipe SOC
  - O volume crescente de alertas
  - Inteligência de Ameaça como Resposta a Incidente de Segurança
  - Desafíos continuos
  - Um Gap de Competências
  - O Tempo de Respostas
  - O Aumento no Tempo de Resposta
  - Uma Abordagem Fragmentada
  - Qual o Problema da Reatividade?
  - Minimizando a Reatividade em Resposta de Incidentes
  - Identificação de Prováveis Ameaças
  - Identificar as Prováveis Prioridades
  - Fortalecendo a Resposta a Incidentes com Inteligência de Ameaças
  - Características Essenciais da Ameaça Inteligência para Resposta a Incidentes
  - Inteligência de Ameaças para Gerenciamento de Vulnerabilidades
  - O Que é o Problema da Vulnerabilidade em Números
  - Dia Zero não Significa Prioridade Máxima
  - Tempo Deve Ser Utilizado de Forma Essencial
  - Avalie o risco com base na explorabilidade
  - As Classificações de Gravidade Podem ser Enganosas
  - Banco de vulnerabilidades
  - Explorabilidade Versus Exploração
  - Inteligência de Ameaças e os Reais Riscos
  - Verificação de Vulnerabilidade Interna
  - Matriz de Risco para Vulnerabilidades
  - Comunidades Criminosas

- Condomínios Fechados
- Frameworks para Análises de Inteligência de Ameaças
- A Estrutura MITRE ATT&CK™
- Categorizar o Comportamento do Invasor

● Threat Intelligence: Strategic, Tactical, Operational and Technical
- INTRODUÇÃO A INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS
- Fundamentos sobre Inteligência de Ameaças Cibernéticas
- Ciclo de Vida da Inteligência de Ameaças Cibernéticas
- O que são Threat Actors
- CTI NA PRÁTICA
- Os Tipos de Threat Intelligence
- Ferramentas de Threat Intell
- Frameworks de Threat Intell

- ESTRATÉGIAS DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS
- Técnicas de Segurança Operacional - OpSec
- Técnicas de Infiltração e Engenharia Social
- Técnicas de Contrainteligência

- OPERAÇÃO TÁTICA: ANÁLISE DE DADOS
- Técnica e Análise de Dados
- Relatórios de Inteligência de Ameaças

- CONCLUSÃO, DICAS E INDICAÇÕES
- Pirâmide da Dor
- Certificações
- Fundamentals & Indicações

- DICAS:
- Certificações
- Fundamentals & Indicações