1. **Metodologia de Ataque e Defesa**

- Introdução
- MITRE ATT&CK
- Cadeia de destruição cibernética
- TÁTICAS, TÉCNICAS E PROCEDIMENTOS
- Metodologia de resposta a incidentes
- Busca proativa
- Análise ao vivo
- Ioc's Vs Ioa's
- Conheça seu processo
- Virtualização e configuração de laboratório do Windows 10

2. **Ameaças e escopo**

- Incidentes baseados em host e rede
- Tipos de ameaças
- Triagem de ameaças
- Visibilidade do sistema operacional
- Transcrição PowerShell e Sid do Usuário

3. **Artefatos de ameaça do endpoint**

- A Sysinternals Suite
- Uso do Process Explorer
- Persistência com Autoruns
- Linha de comando de Autoruns
- Cenário de Exercício – Malware Red Line
- Detecção de binário não assinado
- Procmon para detecção de processos
- Procmon Beautifier
- Exercício Njrat - Detecção e Resposta

- Visualizações de atividade de rede
- Detectar identificador de zona de origem
- Monitor de utilização de recursos do sistema
- Cache RDP
- Cache de atividades

4. Análise de logs do Windows

- Logs de eventos do Windows
- Tipos de logon de evento
- IDs de evento
- Demonstração dos recursos do log de eventos
- Exercício - Cenário de Investigação
- Evtx com TimeLineExplorer
- Sysmon
- Caça de eventos

5. Artefatos de Ameaça de Registro

- Estrutura do Registro
- Aquisição de arquivo de registro
- Ferramenta RegistryExplorer
- Pontos de interesse do registro
- Registro ASEPS
- UserAssist
- ShellBags
- Setupapi

6. Análise de ameaças de rede

- Trabalhando com Wireshark

- Filtros e Adaptações Wireshark
- Estatísticas do Wireshark
- Análise de DNS
- Análise DHCP
- Análise HTTP
- Exercícios de Cenários de Ataque
- Análise SMB e MS-RPC
- Exercício - Cenário de ataque

7. Evidência de Execução

- Jump Lists
- ShimCache
- AmCache