GOHACKING SECURITY OPERATION CENTER FOUNDATIONS

(GHSOC)

GoHacking

CYBER SECURITY TRAININGS

NÍVEL BÁSICO / INTERMEDIÁRIO

Carga Horária: 40hs

GoHacking

(GHSOC)

Bruno Guerreiro Diniz

Cyber Security Executive

Executivo de Segurança Cibernética com mais de 15 anos de experiência em Segurança da Informação. Forte experiência na liderança de equipes e serviços de operações cibernéticas, com mentalidade liderada por inteligência e pensamento de negócios.

Atualmente responsável pelas ofertas e entrega de Detecção e Resposta Gerenciada (MDR) e Gerenciamento de Vulnerabilidade e Conformidade Técnica (VM/Hardening), dando suporte a Líderes Técnicos de SOC e direcionando o roteiro de serviços.

FORMAÇÃO:

Bacharel em Ciências da Computação
UNINOVE

CERTIFICAÇÕES:

Modulo Certified Security Officer
MCSO

Linux Professional Institute Certified Security Specialist
LPI 303

ITIL Foundation
ITIL

COBIT Foundation
COBIT

GoHacking

(GHSOC)

O curso GoHacking Security Operation Center Foundations (GHSOC) fornece uma visão geral de um Centro de Operações de Segurança Cibernética (CSOC ou SOC), utilizando frameworks e metodologias consagradas como NIST CSF, MITRE ATT&CK, Cyber Kill Chain, SOC-CMM, CMMI, DeTT&CT, RE&CT entre outros.

As ameaças cibernéticas estão cada vez mais avançadas ao ponto de grandes empresas e nações serem vítimas constantes de ataques mais elaborados. Isso nos leva a dura realidade de que, mais cedo ou mais tarde, sua organização será atacada e comprometida em algum nível. Desta forma, é imprescindível planejar, estruturar e gerenciar um Centro de Operações de Segurança Cibernética com capacidade de Monitorar, Detectar e Reagir à incidentes cibernéticos.

Para isto é fundamental entender: O que é um SOC? Por que ele existe? Quais atividades ele proverá? Como ele estará organizado? Quais recursos serão necessários? Quais as principais ferramentas e processos de apoio? O que posso esperar deste SOC? Essas e outras perguntas serão respondidas nesse treinamento que possui uma abordagem mista entre teoria, exercícios de mesa e prática, apoiada por uma bateria de exercícios.

MÓDULO 1 - Introdução

1. Entendimento da Expectativa:
• *Minority Report*
2. Etimologia e Convenções de Nomenclatura:
• SOC (Security Operation Center), Cyber SOC, Cyber Defense, Intelligence Center.
3. Ameaças Cibernéticas e a Sociedade Moderna:
• Evolução das Ameaças, Evolução dos Impactos, Crime Cibernético, Impacto nãocibernético.
4. Gestão de Risco como Conceito Fundamental:
• Ativos, Valor, Ameaças, Fragilidades, Controles e Tipos de Controles.
5. Missão, Visão e Objetivos:
• *NIST Cybersecurity Framework*, SOC, NOC (Network Operation Center), CSIRT (Computer Security Information Response Team), MDR (Managed Detection and Response), MSS (Managed Security Services)
• Objetivos Estratégicos e Táticos, *Insourcing / Outsourcing*.

GoHacking

(GHSOC)

MÓDULO 2 - Planejamento

1. Capacidades & Maturidades de SOC:
• Intelligence Driven Defense, Atividades de SOC, Processos e Prioridades, Consulting, Operations & Subscription, CMMI, SOC-CMM
2. Recursos de SOC:
• Data Sources e Ferramentas: Volume, Capacidade de Detecção, Categorias
• Recursos Humanos: Cyber Skill Gap, Burnout & Turnover, Planejamento de Pessoas
3. SOC KickStart:
• Avaliação, Planejamento, Execução e Medição
• Exercício em Grupo: Consciência Situacional e Planejamento de SOC
4. Laboratório:
• Consciência Situacional

MÓDULO 3 - Detecção e Resposta

1. Objetivos:
• Papéis e Responsabilidades, Fluxo Principal
2. Plataforma Tecnológica:
• Visão Geral, Elementos Fundamentais
3. Problemas de Detecção e Resposta:
• Dimensões, Expectativa e Realidade

GoHacking

(GHSOC)

MÓDULO 4 - Contexto e Inteligência

1. Inteligência Interna e Externa:
• Contexto Organizacional, Inteligência de Ameaças, Iterações de Atualização
2. Inteligência Cibernética:
• Fluxo de Inteligência, Inteligência de Ameaças Cibernéticas e Fusion Center
3. Frameworks Importantes:
• Cyber KillChain, MITRE ATT&CK

MÓDULO 5 - Processos de SOC

1. Metodologias e Organização:
• Feedforward e Feedback, OODA Loop Framework
2. Onboarding:
• Dados, Informações, Inteligência e Ação

MÓDULO 6 - Engenharia de Casos de Uso

1. Engenharia de Casos de Uso
• Construção: Modelagem de Ameaças, SIGMA, Cyber Threat Intelligence Mapping, MaGMa Framework, DeTT&CT, Simulação de Adversários, Plano de Testes e Tipos de Regras de Detecção
2. Laboratório: Modelagem de Ameaças
• CVSS e STRIDE

GoHacking

(GHSOC)

MÓDULO 7 - Processos de Apoio

1. Threat Hunting & TaHiTI:
• Threat Hunting baseado em Cenário/Desafio, Threat Hunting contínuo
2. Gestão de Conteúdo (Knowledge Base)
3. Cyber War Gaming

MÓDULO 8 - Tratamento e Resposta a Incidentes Cibernéticos

1. Cyber Incident Response
• Organização, Framework RE&CT
2. Runbooks e Playbooks
• Playbooks, Runbooks e Automações
3. Turnos e Escalas Operacionais
• Horário de Trabalho, Checklists de Qualidade
4. Fluxo e Dinâmica escalar
• Volume de Atividades e Planejamento de Capacidade de Atendimento

MÓDULO 9 - Recursos Humanos

1. Habilidades/Capacidades (Skills):
• Ned Herrmann Model, Hard and Soft Softskills, Skill Sets and Learning Paths
2. Paradigmas de Gestão:
• Performance e Confiança, Círculo Dourado
3. Organização:
• Equipes, Lideranças e Papéis e Responsabilidades na Operação

GoHacking

(GHSOC)

MÓDULO 10 - Tecnologias de SOC

1. Evolução e Maturidade:
• Visão Geral, Evolução e Maturidade
2. Ferramentas de Dados:
• Central Log Management, Security Data Lakes e SIEMs
• LOG Archives: LOG Rewind e LOG Recover
3. Ferramentas de Inteligência de Ameaças Cibernéticas:
• Threat Intelligence Platforms
4. Ferramentas de Apoio:
• Security Orchestration, Automation and Response (SOAR)
• Honeypots e Deceptions
• Endpoint/Network Detection and Response (EDRs / NDRs)
• Forense Digital: Online (Live) e Offline Forensics

MÓDULO 11 - Laboratório de Ferramentas

1. Wazuh: Endpoint Monitoring
2. Graylog: Central LOG Management
3. Velociraptor: Remote Live Forensics
4. MISP: Threat Intelligence Platform
5. The Hive: Case Management

GoHacking

(GHSOC)

MÓDULO 12 - Gestão de SOC

1. Visão Geral de Processos de Gestão
2. Indicadores:
• Operacionais
• Táticos
• Executivos
3. Balanced Scorecard
• Objetivos, Metas, Indicadores e Projetos estratégicos

MÓDULO 13 - Caso Prático

1. Caso Prático:
• Exercício de Construção de um Projeto de SOC

PRÉ-REQUISITOS

- **Conhecimentos em Sistema Operacionais**
- **Conhecimentos em Rede de Computadores e Serviços de Rede**
- **Familiaridade com procedimentos e soluções de proteção cibernética**
- **Familiaridade com avaliações de LOGs e Troubleshooting utilizando telemetria**

GoHacking

(GHSOC)

PÚBLICO ALVO

- Especialistas/Arquitetos em Segurança da Informação
- Líderes Técnicos de Segurança
- Membros de CSIRT
- Analista de SOC
- Gestor de Segurança da Informação
- Gestor de Operações de TI
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS)
- Configuração mínima de 8GB de RAM, 40GB de espaço livre em disco, porta USB e placa
- de rede (RJ45 ou *wireless*) para acesso à Internet
- Capacidade de executar, pelo menos, uma Máquina Virtual (VM)
- Software de Virtualização: VMWare, versão mais atualizada, de preferência Workstation
- (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS)

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno, o GoHacking Academy
- Acesso às gravações das sessões ao vivo do treinamento
- Apostila do curso no formato PDF
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

GoHacking

(GHSOC)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- **Ter uma visão geral do funcionamento de um SOC**
- **Definir o escopo de serviços do um SOC**
- **Entender as diferenças e a relação entre SOC, NOC, MSS, MDR, CSIRT e as tecnologias associadas (SIEM,**
- **EDR, NDR, XDR, SOAR, Data Lakes)**
- **Realizar o planejamento estratégico de montagem de um SOC**
- **Entender as capacidades de um SOC**
- **Avaliar o orçamento e custeio de um SOC**
- **Entender as principais funções e processos existentes dentro de um serviço de MDR**
- **Compreender os papéis e responsabilidades das funções de um MDR**
- **Apresentar uma visão holística das ferramentas necessárias para gestão de um serviço de MDR**
- **Avaliar modelos de gestão de capacidade e qualificação para MDR e SOC**
- **Dominar importantes aspectos de Governança de um SOC**

GoHacking

CYBER SECURITY TRAININGS