Roteiro de Treinamento em Cibersegurança

Tópico	Código do curso	Título do curso	Certificação GIAC
Fundamento	ICS410	**ICS/SCADA Security Essentials**	GICSP

Habilidades Básicas

NOVO EM CIBERSEGURANÇA | COMPUTADORES, TECNOLOGIA E SEGURANÇA

FUNDAMENTAIS EM COMPUTAÇÃO E TI	SEC275 **Foundations: Computers, Technology & Security**	GFACT
FUNDAMENTAIS EM CIBERSEGURANÇA	SEC301 **Introduction to Cyber Security**	GISF

Este curso de nível básico abrange um amplo espectro de tópicos de segurança e traz uma grande variedade de exemplos da vida real. Uma mistura equilibrada de assuntos técnicos e gerenciais tornam este curso atraente aos participantes que precisam entender as facetas evidentes dos conceitos básicos de segurança da informação e os fundamentos da gestão de riscos.

TÉCNICAS PRINCIPAIS | PREVENÇÃO, DEFESA E MANUTENÇÃO

Todo profissional de segurança deve saber

ESSENCIAIS EM SEGURANÇA	SEC401 **Security Essentials: Network, Endpoint, and Cloud**	GSEC

Se você é novo em segurança da informação ou um profissional experiente com foco especializado, o SEC401 fornecerá as habilidades e técnicas básicas de segurança da informação que você precisa para proteger e assegurar suas informações críticas e ativos de tecnologia, seja no local ou em nuvem.

BLUE TEAM	SEC450 **Blue Team Fundamentals: Security Operations and Analysis**	GSOC
TÉCNICAS DE ATACANTES	SEC504 **Hacker Tools, Techniques, and Incident Handling**	GCIH

Todos os profissionais encarregados do trabalho prático de cibersegurança devem ser treinados para possuir um conjunto comum de habilidades que lhes permita proteger sistemas, praticar a defesa com profundidade, entender como funcionam os ataques e gerenciar incidentes quando eles ocorrem. Para estar seguro, é preciso definir um nível alto para o conjunto de habilidades básicas em sua organização de segurança.

ESSENCIAIS DE ANÁLISE FORENSE DIGITAL

Todo profissional de análise forense e resposta a incidentes deve saber

ESSENCIAL EM ANÁLISE FORENSE DIGITAL	FOR308 **Digital Forensics Essentials**	
ANÁLISE FORENSE EM CAMPO DE BATALHA E AQUISIÇÃO DE DADOS	FOR498 **Battlefield Forensics & Data Acquisition**	GBFA

SEGURANÇA DE SISTEMAS DE CONTROLE INDUSTRIAL

Todo profissional de segurança de ICS deve saber

ESSENCIAIS	ICS410 **ICS/SCADA Security Essentials**	GICSP

SEGURANÇA DE SISTEMAS DE CONTROLE INDUSTRIAL

Todo gerente de segurança de ICS deve saber

ESSENCIAIS	ICS418 **ICS Security Essentials for Managers**	

ESSENCIAIS EM SEGURANÇA EM NUVEM

Todo profissional de segurança em nuvem deve saber

ESSENCIAIS	SEC488 **Cloud Security Essentials**	GCLD

Se você é novo em cibersegurança ou está procurando se aprimorar, os treinamentos essenciais de segurança em nuvem são um requisito para as organizações de hoje. Esses cursos fornecem conhecimento básico necessário para apresentar aos alunos o setor de segurança em nuvem, bem como práticas aprofundadas e práticas em laboratórios.

FUNDAMENTAIS EM NUVEM

Criado para profissionais que precisam estar familiarizados com os conceitos, princípios e termos básicos de segurança em nuvem, mas que não precisam de detalhes muito profundos.

INTRODUÇÃO	SEC388 **Intro to Cloud Computing and Security**

FUNDAMENTAIS EM LIDERANÇA

Todo gerente de cibersegurança deve saber

TREINAMENTO CISSP®	MGT414 **SANS Training Program for CISSP® Certification**	GISP
GESTÃO DE RISCOS	MGT415 **A Practical Introduction to Cyber Security Risk Management**	
CONSCIENTIZAÇÃO DE SEGURANÇA	MGT433 **Managing Human Risk**	SSAP
CONTROLES CIS	SEC440 **CIS Critical Controls: A Practical Introduction**	

Com um número crescente de tecnólogos talentosos, as organizações exigem líderes eficazes para gerenciar suas equipes e processos. Esses líderes não necessariamente realizarão trabalho prático, mas devem saber o suficiente sobre as tecnologias e estruturas subjacentes para ajudar a definir a estratégia, desenvolver políticas apropriadas, interagir com profissionais qualificados e medir os resultados.

CYBER RANGES

CTF E CURIOSIDADES	Bootup CTF
TESTE DE HABILIDADES E APLICAÇÃO PRÁTICA	Netwars Core

Essas ofertas de alcance cibernético cobrem a mais ampla gama de tópicos e são destinadas a todos os profissionais de segurança da informação em todos os níveis.

Funções de Trabalho em Foco

PROJETO, DETECÇÃO E CONTROLES DEFENSIVOS

Habilidades focadas em Defesa Cibernética

GENERALISTA AVANÇADO	SEC501 **Advanced Security Essentials – Enterprise Defender**	GCED
MONITORAMENTO E OPERAÇÕES	SEC511 **Continuous Monitoring and Security Operations**	GMON
ARQUITETURA EM SEGURANÇA	SEC530 **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**	GDSA

A detecção do que acontece em seu ambiente requer um conjunto cada vez mais sofisticado de habilidades e recursos. A identificação de anomalias de segurança requer maior profundidade de compreensão para implantar ferramentas de detecção e monitoramento e interpretar sua saída.

Inteligência em código aberto

OSINT	SEC497 **Practical Open-Source Intelligence (OSINT)**	GOSI

OPERAÇÕES OFENSIVAS | ANÁLISE DE VULNERABILIDADE, TESTE DE INVASÃO

Todo profissional de operações ofensivas deve saber

TESTE DE INVASÃO DE REDE	SEC560 **Enterprise Penetration Testing**	GPEN
APLICATIVOS DA WEB	SEC542 **Web App Penetration Testing and Ethical Hacking**	GWAPT
AVALIAÇÃO DE VULNERABILIDADE	SEC460 **Enterprise and Cloud | Threat and Vulnerability Assessment**	GEVA

O profissional que consegue encontrar fraquezas geralmente é de uma área diferente daquela focada exclusivamente na construção de defesas. Um princípio básico das implantações de Red/Blue Team é que encontrar vulnerabilidades requer diferentes formas de pensar e diferentes ferramentas. As habilidades em operações ofensivas são essenciais para que os profissionais de cibersegurança melhorem suas defesas.

RESPOSTA A INCIDENTES E CAÇA A AMEAÇAS | HOST E ANÁLISE FORENSE DE REDE

Todo profissional de análise forense e resposta a incidentes deve saber

ANÁLISE FORENSE DE ENDPOINT	FOR500 **Windows Forensic Analysis** FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** FOR532 **Enterprise Memory Forensics In-Depth** FOR608 **Enterprise-Class Incident Response & Threat Hunting**	GCFE GCFA
ANÁLISE FORENSE DE REDE	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**	GNFA

Esteja você procurando manter um caminho de evidências em sistemas host ou de rede ou procurando ameaças usando técnicas semelhantes, organizações maiores precisam de profissionais especializados que possam ir além do tratamento de incidentes de primeira resposta para analisar um ataque e desenvolver um plano apropriado de remediação e recuperação.

SEGURANÇA DE SISTEMAS DE CONTROLE INDUSTRIAL

Todo profissional de segurança de ICS deve saber

DEFESA E RESPOSTA DO ICS	ICS515 **ICS Visibility, Detection, and Response**	GRID
SEGURANÇA AVANÇADA EM ICS	ICS612 **ICS Cybersecurity In-Depth**	

Proteção NERC

ESSENCIAIS EM SEGURANÇA NERC	ICS456 **Essentials for NERC Critical Infrastructure Protection**	GCIP

PRINCIPAIS EM SEGURANÇA EM NUVEM

Preparação para funções de trabalho mais focadas

NUVEM PÚBLICA	SEC510 **Public Cloud Security: AWS, Azure, and GCP**	GPCS
AUTOMAÇÃO E DEVSECOPS	SEC540 **Cloud Security and DevSecOps Automation**	GCSA
MONITORAMENTO E DETECÇÃO	SEC541 **Cloud Security Attacker Techniques, Monitoring & Threat Detection**	GCTD
ARQUITETURA	SEC549 **Enterprise Cloud Security Architecture**	

PRINCIPAIS EM LIDERANÇA

Líder tansformacional de cibersegurança

LIDERANÇA TECNOLÓGICA	MGT512 **Security Leadership Essentials for Managers**	GSLC
ESTRATÉGIA DE SEGURANÇA	MGT514 **Security Strategic Planning, Policy, and Leadership**	GSTRT
CULTURA DE SEGURANÇA	MGT521 **Leading Cybersecurity Change: Building a Security-Based Culture**	

Executivo operacional de cibersegurança

GESTÃO DE VULNERABILIDADE	MGT516 **Building and Leading Vulnerability Management Programs**	
SOC	MGT551 **Building and Leading Security Operations Centers**	GSOM
FRAMEWORKS E CONTROLES	SEC566 **Implementing and Auditing Security Frameworks & Controls**	GCCC

CYBER RANGES

DEFESA CIBERNÉTICA	Netwars Cyber Defense
ANÁLISE FORENSE DIGITAL E RESPOSTA A INCIDENTES	Netwars DFIR
SISTEMAS DE CONTROLE INDUSTRIAL	Netwars ICS
GERAÇÃO E DISTRIBUIÇÃO DE ENERGIA	Netwars GRID
LIDERANÇA E GESTÃO DE NEGÓCIOS	Cyber42

O SANS oferece versões especializadas do Netwars para funções de trabalho mais específicas. Esses Cyber Ranges se aprofundam nos respectivos tópicos e ajudam a avançar em sua carreira com desafios e cenários baseados em situações e eventos da vida real.

Habilidades Específicas, Funções Especializadas

DEFESA CIBERNÉTICA AVANÇADA | ENDURECIMENTO DE DEFESAS ESPECÍFICAS

Foco na plataforma

WINDOWS/ POWERSHELL	SEC505 **Securing Windows and PowerShell Automation**	GCWN

Foco no tópico

ANÁLISE DE TRÁFEGO	SEC503 **Network Monitoring and Threat Detection In-Depth**	GCIA
SIEM	SEC555 **SIEM with Tactical Analytics**	GCDA
POWERSHELL	SEC586 **Blue Team Operations: Defensive PowerShell**	
PYTHON CODING	SEC573 **Automating Information Security with Python**	GPYC
CIÊNCIA DE DADOS	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals**	

Inteligência em código aberto

OSINT	SEC587 **Advanced Open-Source Intelligence (OSINT) Gathering & Analysis**	

OPERAÇÕES OFENSIVAS ESPECIALIZADAS | TÉCNICAS E ÁREAS EM FOCO

Rede, Web e Nuvem

DESENVOLVIMENTO EM EXPLORAÇÃO	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** SEC661 **ARM Exploit Development** SEC760 **Advanced Exploit Development for Penetration Testers**	GXPN
TESTE DE INVASÃO EM NUVEM	SEC588 **Cloud Penetration Testing**	GCPN

Testes de invasão epecializados

ENGENHARIA SOCIAL	SEC467 **Social Engineering for Security Professionals**	
DEFESA ATIVA	SEC550 **Cyber Deception – Attack Detection, Disruption & Active Defense**	
BLOCKCHAIN	SEC554 **Blockchain and Smart Contract Security**	
RED TEAM	SEC565 **Red Team Operations and Adversary Emulation** SEC670 **Red Team Operations – Developing Custom Tools for Windows**	
MOBILE	SEC575 **Mobile Device Security and Ethical Hacking**	GMOB
TESTE DE INVASÃO	SEC580 **Metasploit for Enterprise Penetration Testing**	
WIRELESS	SEC556 **IoT Penetration Testing** SEC617 **Wireless Penetration Testing and Ethical Hacking**	GAWN

Purple Team

EMULAÇÃO ADVERSÁRIA	SEC598 **Security Automation for Offense, Defense, and Cloud** SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** SEC699 **Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection**	GDAT

ANÁLISE FORENSE DIGITAL, ANÁLISE DE MALWARE E INTELIGÊNCIA DE AMEAÇAS | HABILIDADES INVESTIGATIVAS ESPECIALIZADAS

Especialização

ANÁLISE FORENSE EM NUVEM	FOR509 **Enterprise Cloud Forensics & Incident Response**	GCFR
RANSOMWARE	FOR528 **Ransomware for Incident Responders**	
ANÁLISE DE MALWARE	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** FOR710 **Reverse-Engineering Malware: Advanced Code Analysis**	GREM

Inteligência em ameaças

INTELIGÊNCIA EM AMEAÇAS CIBERNÉTICAS	FOR589 **Cybercrime Intelligence**	

Análise forense digital e exploração de mídia

SMARTPHONES	FOR585 **Smartphone Forensic Analysis In-Depth**	GASF
ANÁLISE FORENSE DE MAC	FOR518 **Mac and iOS Forensic Analysis and Incident Response**	GIME

ESPECIALIZAÇÃO EM SEGURANÇA EM NUVEM

Especialização para habilidades e funções avançadas

SEGURANÇA DE APLICATIVO	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices**	GWEB
COMPLIANCE	SEC557 **Cloud Security Continuous Compliance**	
TESTE DE INVASÃO EM NUVEM	SEC588 **Cloud Penetration Testing**	GCPN
ANÁLISE FORENSE EM NUVEM	FOR509 **Enterprise Cloud Forensics and Incident Response**	GCFR

Aprender como converter as habilidades tradicionais de cibersegurança em nuances de segurança em nuvem é uma necessidade para monitoramento, detecção, teste e defesa apropriados.

LIDERANÇA E GOVERNANÇA EM CIBERSEGURANÇA EM NUVEM

Todo líder de segurança em nuvem deve saber

GESTÃO DE VULNERABILIDADE	MGT516 **Building and Leading Vulnerability Management Programs**	
DESIGN E IMPLEMENTAÇÃO	MGT520 **Leading Cloud Security Design and Implementation**	

ESPECIALIZAÇÕES EM LIDERANÇA

Liderança em cibersegurança em nuvem

GESTÃO DE VULNERABILIDADES	MGT516 **Building and Leading Vulnerability Management Programs**	
DESIGN E IMPLEMENTAÇÃO	MGT520 **Leading Cloud Security Design and Implementation**	

Especialização em gestão

AUDITORIA E MONITORAMENTO	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems**	GSNA
LEI E INVESTIGAÇÕES	LEG523 **Law of Data Security and Investigations**	GLEG
GERENCIAMENTO DE PROJETOS	MGT525 **Managing Cybersecurity Initiatives & Effective Communication**	GCPM
RESPOSTA A INCIDENTES	MGT553 **Cyber Incident Management**	