Training Roadmap

Development Paths

SANSが提供する包括的なコースカリキュラムは、
セキュリティの各分野で実践的な技術スキルを習得することができます。また、ソフトウェア開発者やICSエンジニア、経営層や法務担当者、監査人などの方々を対象としたコースもラインナップしています。

Baseline Skills

New to Cyber Security — Concepts, Terms, & Skills

Cyber Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISF

You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques — Prevent, Defend, Maintain

Every Security Professional Should Know

Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH

実践的なサイバーセキュリティ業務を担当する皆さんは、攻撃の仕組みを理解し、多層防御の考え方に基づいてシステムを保護し、インシデントが発生した場合にそのインシデントを管理できるようにする共通のスキルセットを保有するようにトレーニングする必要があります。セキュリティを確保するには、セキュリティ業務を担当する組織のスキルのベースラインを高い水準を設定する必要があります。

Security Management — Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials	MGT512 **Security Leadership Essentials for Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

多様化するセキュリティ業務プロセスとセキュリティチームを適切に管理するリーダーが必要です。それらを管理するマネ ージャは、必ずしもテクニカルな作業を行うわけではありませんが、セキュリティ戦略の策定や適切なポリシーの開発、熟練した技術者とのやり取り、成果の測定などを行う上でその基盤となるテクノロジーとフレームワークについて十分に知 っている必要があります。

Focus Job Roles

You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection — Intrusion Detection, Monitoring Over Time

Scan Packets & Networks

Intrusion Detection	SEC503 **Intrusion Detection In-Depth** | GCIA
Monitoring & Operations	SEC511 **Continuous Monitoring and Security Operations** | GMON

自組織の環境で発生していることを検知するには、高度なスキルと能力のセットが必要です。セキュリティの異常を特定するには、監視ツールを展開して検知し、その出力を分析・解釈するためのスキルを深める必要があります。

Penetration Testing — Vulnerability Analysis, Ethical Hacking

Every Pen Tester Should Know

Networks	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
Web Apps	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

弱点を見つけることができる専門家は、防御を構築することに専念している専門家とは異なるスキルセットが必要です。レッドチーム/ブルーチーム展開の基本原則は、脆弱性を見つけるには防御とは異なる考え方と異なるツールが必要で、それらは防衛の専門家が防御を改善するために不可欠であるということです。

Incident Response & Threat Hunting — Host & Network Forensics

Every Forensics and IR Professional Should Know

Endpoint Forensics	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
Network Forensics	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

ホストやネットワークシステムに関する証拠保全を行う場合や、同様の手法を使用してスレットハンティングを行う場合には、攻撃を詳細に分析し、適切な修復・復旧計画を策定・実行できる、インシデントハンドリングの初動対応の域をはるかに越えて活動できる特別なプロフェッショナルが必要です。

CISSP® Training	MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations — Harden Specific Defenses

Specialized Defensive Area

Blue Team	SEC450 **Blue Team Fundamentals: Security Operations and Analysis**
OSINT	SEC487 **Open-Source Intelligence (OSINT) Gathering and Analysis**
Advanced Generalist	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
Cloud Security	SEC545 **Cloud Security Architecture and Operations**
Windows/Powershell	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Linux/ Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA

Other Advanced Defense Courses

Security Architecture	SEC530 **Defensible Security Architecture and Engineering** | GDSA
Adversary Emulation	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT

Specialized Penetration Testing — Focused Techniques & Areas

In-Depth Coverage

Vulnerability Assessment	SEC460 **Enterprise Threat and Vulnerability Assessment** | GEVA
Networks	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers**
Web Apps	SEC642 **Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques**
Mobile	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
Wireless	SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Python Coding	SEC573 **Automating Information Security with Python** | GPYC

Digital Forensics, Malware Analysis, & Threat Intel — Specialized Investigative Skills

Malware Analysis

Malware Analysis	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM

Threat Intelligence

Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI

Digital Forensics & Media Exploitation

Battlefield Forensics & Data Acquisition	FOR498 **Battlefield Forensics & Data Acquisition**
Smartphones	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
Memory Forensics	FOR526 **Advanced Memory Forensics & Threat Detection**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

Advanced Management — Advanced Leadership, Audit, Legal

Management Skills

Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
Managing Vulnerabilities	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
Project Management	MGT525 **IT Project Management, Effective Communication, and PMP® Exam Prep** | GCPM

Audit & Legal

Audit & Monitor	AUD507 **Auditing & Monitoring Networks, Perimeters, and Systems** | GSNA
Law & Investigations	LEG523 **Law of Data Security and Investigations** | GLEG

Industrial Controls

Every ICS Security Professionals Should Know

Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID
ICS Security In-Depth	ICS612 **ICS Cyber Security In-Depth**

NERC Protection

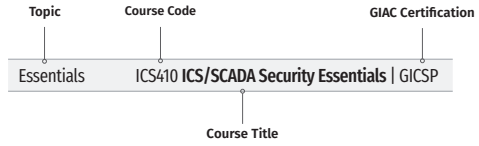
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

DevSecOps

Every Developer Should Know

Secure Web Apps	DEV522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation** | GCSA

COURSE LISTING KEY:



65+ hands-on courses

To learn more about additional SANS courses, go to: **sans.org/courses**

See in-depth course descriptions and the digital version of this roadmap at: **sans.org/roadmap**

SANS The most trusted source for cybersecurity training, certifications, degrees, and research