SANSトレーニングロードマップ

トピック / コース番号 / 対応するGIAC
Essentials — ICS410 **ICS/SCADA Security Essentials** | GICSP
コース名

全般的な基礎スキル

新しくセキュリティに関わる方 | コンピュータ、技術、セキュリティ

コンピュータITの基礎	SEC275 **Foundations: Computers, Technology & Security** | GFACT
サイバーセキュリティの基礎	SEC301 **Introduction to Cyber Security** | GISF

この入門コースでは、セキュリティに関する幅広いトピックを取り上げ、実際の事例をふんだんに盛り込んでいます。技術的な問題と経営的な問題をバランスよく取り入れたこのコースは、情報セキュリティの基礎とリスクマネジメントの基本を理解する必要がある受講者にとって魅力的なコースです。

要素技術 | 攻撃、保護、防御、運用

セキュリティに関わる全ての方が知っておくべき知識

セキュリティの基礎	SEC401 **Security Essentials: Network, Endpoint, and Cloud** | GSEC
防御するためのスキル	SEC450 **Blue Team Fundamentals: Security Operations and Analysis** | GSOC
攻撃者のテクニック	SEC504 **Hacker Tools, Techniques, and Incident Handling** | GCIH

SEC401は、情報セキュリティの初心者から、専門分野に特化したベテラン技術者まで、オンプレミスまたはクラウドに関わらず、重要な情報や技術資産を保護しセキュリティを高めるために必要な情報セキュリティスキルと技術を習得することができます。

サイバーセキュリティの業務に携わるすべての技術者は、システムの安全確保、防御、攻撃の仕組みの理解、およびインシデント発生時の対応をするための基本的なスキルを身につけるためにトレーニングを受ける必要があります。セキュリティを確保するためには、組織内で要求されるスキル以上の基礎知識を習得しておく必要があります。

SANS SECURITY AWARENESSの技術トレーニング

IT管理者のためのセキュリティ基礎

最新の脅威から組織を守るためには、それらの脅威の一歩先を行くために継続的なスキルアップが必要です。短いCBTを受講することで、技術チームのスキルセットに適した学習スピードで、進化するセキュリティのコンセプトの理解を深めることができます。

フォレンジックの基礎

フォレンジックとインシデントレスポンス担当者が知っておくべき知識

フォレンジックの基礎	FOR308 **Digital Forensics Essentials**
有事の際のフォレンジック技術とデータ抽出	FOR498 **Battlefield Forensics & Data Acquisition** | GBFA

クラウドセキュリティの基礎

クラウドセキュリティ担当者が知っておくべき知識

クラウドセキュリティの基礎	SEC488 **Cloud Security Essentials** | GCLD

サイバーセキュリティに初めて携わる方やスキルアップを目指す方にとって、クラウドセキュリティについての知識は現在多くの組織で必要とされています。これらのコースでは、クラウドセキュリティのために必要な基礎知識を学び、実践的な演習を通じて理解を深めます。

クラウドセキュリティの基礎

クラウドセキュリティの基本的な概念、原則、用語の知識は必要だけど、実践的なクラウド業務には携わらない方向けのコースです。

クラウドセキュリティ入門	SEC388 **Intro to Cloud Computing and Security**

SANS SECURITY AWARENESSの技術トレーニング

開発者のためのセキュアコーディング

開発者はもちろんのこと、ソフトウェア開発プロセスに携わる、アーキテクト、管理者、ビジネスオーナー、パートナーを含む様々な業務に応じたトレーニングを行い、開発段階からセキュリティレベルの高いアプリケーションを構築できるようにします。

産業制御システム(ICS)セキュリティ

ICS管理責任者が知っておくべき知識

ICSセキュリティ管理の基礎	ICS410 **ICS/SCADA Security Essentials** | GICSP

産業制御システム(ICS)セキュリティ

ICS担当者が知っておくべき知識

ICSセキュリティ管理の基礎	ICS418 **ICS Security Essentials for Managers**

基本的なリーダーシップ

全てのサイバーセキュリティマネージャーが知っておくべき知識

CISSP®トレーニング	MGT414 **SANS Training Program for CISSP® Certification** | GISP
リスクマネジメント	MGT415 **A Practical Introduction to Cyber Security Risk Management**
セキュリティ意識	MGT433 **Managing Human Risk** | SSAP

有能な技術者の数が増えているため、組織はチームとプロセスを管理するために効果的なリーダーを必要としています。これらのリーダーは必ずしも実践的な作業を行うとは限りませんが、戦略の設定、適切なポリシーの策定、熟練した実務家との対話、および結果の測定に役立つ基礎となるテクノロジ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。

サイバーレンジ

CTFとトリビア	Bootup CTF
スキルの確認と実践応用	NetWars Core

サイバーレンジでは幅広いトピックをカバーし、どのようなレベルの方にもお楽しみいただけます。

業務に応じたスキル

システム設計、侵入検知、防御技術

サイバー攻撃からシステムを守るためのスキル

サイバーセキュリティ全般について応用技術	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
監視と運用	SEC511 **Continuous Monitoring and Security Operations** | GMON
セキュリティアーキテクチャ	SEC530 **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise** | GDSA

ネットワーク内で何が起きているかを検知するためには、高度なスキルと能力が要求されます。通常ではない挙動を特定するためには、検知・監視ツールの導入や、それらからの出力を分析・利用するためのノウハウが必要となります。

Open-Source Intelligence

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

攻撃者の技術 | 脆弱性の分析、ペネトレーションテスト

攻撃技術に携わる担当者が知っておくべき知識

ネットワークペネトレーションテスト	SEC560 **Enterprise Penetration Testing** | GPEN
Webアプリケーションテスト	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT
脆弱性診断	SEC460 **Enterprise and Cloud | Threat and Vulnerability Assessment** | GEVA

セキュリティ上の問題点を検出するプロフェッショナルは、システムの防御を担当する専門家とは異なるスキルやノウハウが必要となります。REDチーム(攻撃技術の専門家)とBLUEチーム(防御技術の専門家)にはそれぞれ必要となる知識があり、脆弱性を検出するには、攻撃者側の知識やツールが必要となります。攻撃技術を知ることによって、防御の能力も向上させることができます。

インシデントレスポンスとすレットハンティング | ホストベースのネットワークベースのフォレンジック

フォレンジックとインシデントレスポンス担当者が知っておくべき知識

エンドポイントフォレンジック	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA FOR532 **Enterprise Memory Forensics In-Depth** FOR577: **LINUX Incident Response & Analysis** FOR608 **Enterprise-Class Incident Response & Threat Hunting**
ネットワークフォレンジック	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

セキュリティ上の問題点を検出するプロフェッショナルは、システムの防御を担当する専門家とは異なるスキルやノウハウが必要となります。REDチーム(攻撃技術の専門家)とBLUEチーム(防御技術の専門家)にはそれぞれ必要となる知識があり、脆弱性を検出するには、攻撃者側の知識やツールが必要となります。攻撃技術を知ることによって、防御の能力も向上させることができます。

クラウドセキュリティの要素技術

業務に応じた各要素分析

パブリッククラウド	SEC510 **Public Cloud Security: AWS, Azure, and GCP** | GPCS
自動化とDevSecOps	SEC540 **Cloud Security and DevSecOps Automation** | GCSA
監視と検出	SEC541 **Cloud Security Attacker Techniques, Monitoring & Threat Detection** | GCTD
アーキテクチャ	SEC549 **Enterprise Cloud Security Architecture**

世界的なクラウドへの大規模な移行に伴い、パブリッククラウドの利用に伴うセキュリティリスクやメリット、マルチクラウド環境の導入や活用方法、DevOpsの開発プロジェクトにセキュリティを組み込む方法などを理解しているプロフェッショナルが求められています。

産業制御システム(ICS)セキュリティ

ICS担当者が知っておくべき知識

ICS防御とインシデントレスポンス	ICS515 **ICS Visibility, Detection, and Response** | GRID
ICSセキュリティ応用技術	ICS612 **ICS Cybersecurity In-Depth**

リーダーシップの要素技術

変革するサイバーセキュリティリーダー

テクノロジーリーダーシップ	MGT512 **Security Leadership Essentials for Managers** | GSLC
セキュリティ戦略	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
セキュリティ文化	MGT521 **Leading Cybersecurity Change: Building a Security-Based Culture**

運用周りのセキュリティリーダー

脆弱性管理	MGT516 **Building and Leading Vulnerability Management Programs**
SOC	MGT551 **Building and Leading Security Operations Centers** | GSOM
フレームワークとコントロール	SEC566 **Implementing and Auditing Security Frameworks & Controls** | GCCC

サイバーレンジ

サイバーディフェンス	NetWars Cyber Defense
デジタルフォレンジックとインシデントレスポンス(DFIR)	NetWars DFIR
産業制御システム(ICS)	NetWars ICS
発電・送電システム(ICS/SCADA)	NetWars GRID

業務内容ごとに特化されたNetwarsを提供しています。これらサイバーレンジでは、それぞれのトピックを深く掘り下げ、実際の事件・事故に基づいた課題やシナリオに挑戦することによってスキルアップできます。

専門家のための高度なスキル

システム防御に関する高度技術 | システムハードニング

プラットフォームに焦点を当てたコース

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

各トピックに焦点を当てたコース

トラフィック分析	SEC503 **Network Monitoring and Threat Detection In-Depth** | GCIA
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
POWERSHELL	SEC586 **Security Automation with PowerShell**
Pythonプログラミング	SEC573 **Automating Information Security with Python** | GPYC SEC673 **Advanced Information Security Automation with Python**
データサイエンス	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals**

Open-Source Intelligence

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

システム防御に関する高度技術 | システムハードニング

ネットワーク、Web、クラウド

Exploit開発	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC661 **ARM Exploit Development** SEC760 **Advanced Exploit Development for Penetration Testers**
クラウドペネトレーションテスト	SEC588 **Cloud Penetration Testing** | GCPN

専門的なペネトレーションテスト

ソーシャルエンジニアリング	SEC467 **Social Engineering for Security Professionals**
ブロックチェーン	SEC554 **Blockchain and Smart Contract Security**
レッドチーム	SEC565 **Red Team Operations and Adversary Emulation** SEC670 **Red Teaming Tools - Developing Windows Implants, Shellcode, Command and Control**
モバイル	SEC575 **iOS and Android Application Security Analysis and Penetration Testing** | GMOB
製品セキュリティ	SEC568 **Combating Supply Chain Attacks with Product Security Testing**
ペネトレーションテスト	SEC580 **Metasploit for Enterprise Penetration Testing**
ワイヤレス	SEC556 **IoT Penetration Testing** SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN

パープルチーム

パープルチーム戦略	SEC598 **Security Automation for Offense, Defense, and Cloud** SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT SEC699 **Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection**

フォレンジック、マルウェア分析、スレットインテリジェンス | さまざまな調査に関する専門的なスキル

特定の専門分野に関するスキル

クラウドフォレンジック	FOR509 **Enterprise Cloud Forensics & Incident Response** | GCFR
ランサムウェア	FOR528 **Ransomware for Incident Responders**
マルウェア分析	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM FOR710 **Reverse-Engineering Malware: Advanced Code Analysis**

スレットインテリジェンス

サイバースレットインテリジェンス	FOR578 **Cyber Threat Intelligence** | GCTI FOR589 **Cybercrime Intelligence**

デジタルフォレンジックとMedia Exploitation

スマートフォン	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
MACフォレンジック	FOR518 **Mac and iOS Forensic Analysis and Incident Response** | GIME
LINUXフォレンジック	FOR577 **Linux Incident Response & Analysis**

クラウドセキュリティの専門分野

特定の専門分野に関するスキル

アプリケーションセキュリティ	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
クラウドペネトレーションテスト	SEC588 **Cloud Penetration Testing** | GCPN
クラウドフォレンジック	FOR509 **Enterprise Cloud Forensics and Incident Response** | GCFR
クラウドセキュリティの設計と実装	MGT520 **Leading Cloud Security Design and Implementation**

従来のサイバーセキュリティのスキルをクラウドセキュリティに応用するための方法を学ぶことで、適切な監視、検知、テスト、および防御をすることができます。

SANS SECURITY AWARENESSの技術トレーニング

ICS技術者のためのトレーニング

エンジニア、システム運用担当者、その他ICSに携わる方が重要システムに対するサイバーインシデントの防止、検知、対応を行うために必要なスキルを強化することができます。

リーダーシップの高度知識

高度のマネジメント知識

監査と監視	AUD507 **Auditing Systems, Applications, and the Cloud** | GSNA
設計と実装	MGT520 **Leading Cloud Security Design and Implementation**
法律と調査	LEG523 **Law of Data Security and Investigations** | GLEG
プロジェクトマネジメント	MGT525 **Managing Cybersecurity Initiatives & Effective Communication** | GCPM
インシデントレスポンス	MGT553 **Cyber Incident Management**

SANS SECURITY AWARENESSの人的リスク管理

エンドユーザーのためのセキュリティ意識向上

オンラインで受講できるエンドユーザー向けのCBTでは、従業員にとって最も緊急性の高いリスクとコンプライアンスのトピックを中心に厳選して提供しています。
このトレーニングでは、多言語に対応した複数のモジュールが用意され、組織や業界に特化したプログラムを組むことによって、自身に必要となるセキュリティ意識を高めることができます。