SANS | GIAC CERTIFICATIONS

世界トップクラスの組織環境 IRチーム構築のためのロードマップ

大規模環境におけるサイバー防衛 体制のための実践ガイド

大規模な環境における効果的なブルーチーム構築

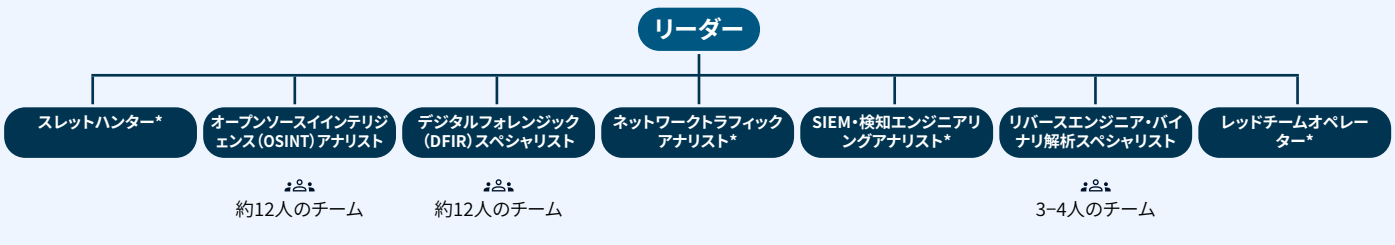
このビジュアルブループリントは高度で大規模な脅威に直面するグローバル組織向けに設計された現代のエンタープライズ環境におけるインシデントレスポンス（IR）チームの核心的な役割を概説しています。これらのチームは高度な脅威を検知、追跡し、対応する必要があります。以下の各役割には、

以下の内容が含まれます：

- インシデントレスポンスのライフサイクルにおける役割
- 日常の運用業務
- 主要なスキル
- 基礎から上級まで段階的なSANSトレーニングコース

エンタープライズ インシデントレスポンスチームの構成

アクティブサイバーディフェンスの役割



*組織の規模に比例したチーム規模

以下は大規模なグローバル組織向けに、高度な脅威をエンタープライズレベルで検知、追跡、対応するための実践的な「ブルーチーム構成」です。以下の各役割には、以下の要素が含まれます：

(1) インシデント対応ライフサイクルにおける通常の位置付け、

(2) 日常業務、

(3) 主要なスキル、および

(4) 段階的なSANSトレーニングパス（初心者 → 中級者 → 上級者）。

コースの選択は、組織の現在の成熟度と人員規模に応じて行われます。

スレットハンター

ミッション：自動化されたコントロールを回避する攻撃者の行動を積極的に探知し、攻撃者がそれらを悪用する前に検知のギャップを埋める。

積極的な調査

タスク

- スレットインテリジェンスとATT&CKから仮説を構築する
- EDR/NDR/SIEMの膨大な情報から情報を精査する
- 環境寄生型（Living Off The Land）攻撃を追跡する

主要なスキル

- MITRE ATT&CKマッピング
- ログからの情報検索
- 仮説駆動型調査
- スクリプティング・自動化（Python, PowerShell）

SANSのトレーニング体系

SEC504: Hacker Tools, Techniques, and Incident Handling

FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics –ハイブリッド・エステートを横断するマルチレイヤー・ハント

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

FOR608: Enterprise-Class Incident Response & Threat Hunting

オープンソースインテリジェンス（OSINT）アナリスト

ミッション：公開されている情報を収集、検証し、統合することで、内部調査および戦略的スレットインテリジェンス製品を強化する。

強化とアトリビューション

タスク

- ソーシャルメディア、WHOIS、ダークウェブ、および漏洩データを横断的に分析
- インシデントに地理的/時間的背景を提供
- ブランド保護と経営陣保護を支援

主要なスキル

- OPSEC
- データマイニング
- ジオロケーション
- APIのスクリプティング
- レポートの作成

SANSのトレーニング体系

SEC497: Practical Open-Source Intelligence (OSINT) –安全な収集の基本

SEC587: Advanced OSINT Gathering and Analysis –深い技術的ピボットと自動化

FOR589: Cybercrime Investigations

デジタルフォレンジックスペシャリスト

ミッション：インシデントが確認された際の、封じ込め、根絶、およびフォレンジックの再構築を主導する。

証拠収集と是正措置

タスク

- 対象のトリアージと揮発性データの収集
- ディスク、メモリ、およびアーティファクト分析（Windows、*nix、クラウド）
- 根本原因とタイムライン分析：法的報告書の草案作成

主要なスキル

- 管理の連鎖と正確なフォレンジックイメージの管理
- タイムラインとログの相関分析、マルウェアのトリアージ
- クラウドアーティファクトの取得

SANSのトレーニング体系

FOR498: Digital Acquisition & Rapid Triage
-トリアージを実施し、収集する

FOR500: Windows Forensic Analysis
– ホスト上の深い調査と証拠収集

FOR508: Advanced Incident Response, Threat Hunting & Digital Forensics
–エンタープライズ規模の調査とメモリー・フォレンジック

FOR608: Enterprise-Class Incident Response & Threat Hunting

ネットワークトラフィックアナリスト

ミッション：パケットキャプチャ、フロー分析、プロトコル解析を活用し、攻撃者の活動を検出、検証、および範囲を特定する。

パッケージとフロー

タスク

- 継続的なpcap/Zeek/Surricataのレビュー
- IDSシグネチャの構築/維持
- 証拠のためのセッションの再構築

主要なスキル

- TCP/IPおよびアプリケーションプロトコルに関する深い知識
- IDSのチューニング統計的アノマリ検知
- スレットハンティングワークフロー

SANSのトレーニング体系

SEC401: Security Essentials – Network, Endpoint, and Cloud
–TCP/IPの基礎とSOCの基礎について理解する。

SEC503: Network Monitoring and Threat Detection In-Depth

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
– NetFlow、pcap、ログを統合し、驚異の検出とレスポンスに活用する。

SIEM・検知エンジニアリングアナリスト

ミッション：様々なログを相関分析し、スレットハンターとIR関係者が即時かつ高精度にセキュリティイベントを検知できるようにする。

検知とチューニング

タスク

- ログの正規化と拡張
- 検出ルール、ダッシュボード、アラートの作成/テスト
- ATT&CKへのマッピング:偽陽性の削減

主要なスキル

- ログ解析とデータエンジニアリング
- クエリ言語（KQL、SPL）、SOAR自動化
- MITREカバレッジマッピング、KPIとレポート作成

SANSのトレーニング体系

SEC450: SOC Analyst Training – Applied Skills for Cyber Defense Operations – SOCアナリスト“スターターキット”

SEC555: Detection Engineering and SIEM Analytics –検知ラボの構築、SIEMの最適化、ルールの作成

SEC511: Cybersecurity Engineering: Advanced Threat Detection & Monitoring – NDR/EDR/SIEMフュージョン→の連携、ハイブリッドクラウドの可視化、GMON認証

リバースエンジニアバイナリ分析スペシャリスト

ミッション：不審な実行ファイル、ファームウェア、およびメモリイメージを解析し、その動作原理や機能、検出方法、および対策方法を理解する。

マルウェア&脆弱性リサーチ

タスク

- Ghidra/IDAを使用して、難読化されたバイナリを解除し、静的解析を実施
- サンドボックス環境でマルウェアの動的解析を実施（Windows/Linux/ARM）
- タイムラインを構築し、IoCを作成、YARA/SIGMAへのルール化
- パッチとファジングの結果を分析し、0-/1-day脆弱性を発見

主要なスキル

- x86-64/ARM アセンブリ言語 PE/ELF 形式の理解
- OS とコンパイラの内部構造、動的バイナリ計装（WinDbg、GDB、Frida）
- スクリプト言語（Python）環境内の運用セキュリティ（OPSEC）
- エクスプロイト緩和策のバイパス、脆弱性の深堀り、カーネル/ヒープエクスプロイト

SANSのトレーニング体系

FOR610: Reverse-Engineering Malware: Malware Analysis Tools & Techniques –ラボ中心の静的・動的解析入門

SEC760: Advanced Exploit Development for Penetration Testers –パッチ拡散、高度な悪用、最新の緩和策

リバースエンジニアリングの適用領域

- トリアージ段階において、アナリストは疑わしいサンプルをリバースエンジニアリング（RE）チームに送付し、迅速な機能プロファイリングを実施します。
- 封じ込めと根絶の段階では、REの分析結果がカスタムYARA/SIGMAシグネチャやホスト/ネットワークブロックルールを策定する基盤となります。
- 事後対応では、REが根本原因の洞察（例：悪用されたCVE、ローダーチェーン）を提供し、検出技術、スレットハンティング、レッドチームシミュレーションに反映され、継続的な改善を通じてサイクルを閉じています。

レッドチームオペレーター

ミッション：既知の攻撃者の戦術、技術、手順（TTPs）を模倣しサイバーセキュリティプログラムの有効性と性と運用上のレジリエンスを評価する。

攻撃者エミュレーション

タスク

- 現実世界の攻撃者を模倣した攻撃キャンペーンの計画、開発、実行
- ターゲット環境、サービス、アプリケーションに対する脆弱性の特定と悪用
- 攻撃キャンペーンを支援するためのカスタムエクスプロイトとC2ツールの開発と適応

主要なスキル

- 技術的侵害（列挙、権限昇格、横展開、持続性）
- スクリプト作成と開発（C、C++、Python、PowerShell）
- 攻撃用ツール（Cobalt Strike、Empire、BloodHound）、OPSEC考慮事項

SANSのトレーニング体系

SEC504: Hacker Tools, Techniques, and Incident Handling

SEC560: Enterprise Penetration Testing

SEC565: Red Team Operations and Adversary Emulation

SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control

ピースがどのように組み合わさるか

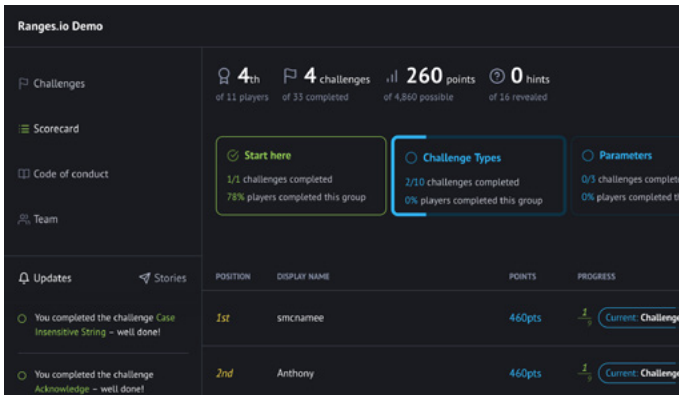
1. **収集と可視化 —** ネットワークトラフィックアナリストとSIEMエンジニアは、テレメトリが完全かつ適切に解析されていることを確認します。
2. **検出とハンティング —** スレットハンターは仮説を基にテレメトリを分析し、SIEMエンジニアは成功した検知技術を永続的なルールとして定義します。
3. **フォレンジックとIR —** DFIR専門家は影響を検証し、脅威を封じ込め詳細なフォレンジックを実施し、OSINTアナリストはは外部コンテキストで調査結果を補完します。
4. **継続的改善 —** 教訓を検知技術者とハンティングプレイブックにフィードバックし、戦術が進化する中で各役割が鋭さを保つためのトレーニングロードマップを確立します。

リアルなシナリオ

SANSのラボでは、コースのコンセプトや学習目標を強化するための実践的な経験を積むことができます。日々の業務で実際に遭遇する課題に基づきラボを設計し、既存のスレットアクターを活用し、複雑な現実的なシナリオを再現しています。SANSのインタラクティブなレンジとスレットベースの攻撃データは、毎週攻撃を受けている組織やエンティティを模倣して一から構築されています。これらの環境は非常に再現度が高いため、SANSのインストラクターは、受講生に教えるための「本物の」攻撃データを使用する許可をどのようにして得たのかとよく尋ねられます。

自己添削型ハンズオン学習

SANSのラボは複雑なラボを順を追って学習できるオンライン・ワークブックによる自己添削できる手順が含まれます。動画によるヒントやシステムで、各ステップを詳細に解説します。必要に応じて受講生はコマンドを非表示にしたり、ツールを活用して問題を解くことができます。



スキルの評価と実践的なスキルの応用

SANS Cyber Rangesは実践的なスキルの応用とスキル評価に重点を置き、自身や自身のチームが得意とするスキルや、よりトレーニングが必要なスキルのインサイトを提供します。Cyber Rangeの受講者はストーリー仕立てのインタラクティブな演習を通じて問題解決し、実際の業務にすぐに活用できるスキルを向上させます。SANSのサイバーレンジは、初級者から上級者まで、幅広い分野とあらゆる難易度を網羅しています。

SANS
CYBER RANGES

CYBER RANGE
SANS SKILLS QUEST
BY NETWARS

sans.org/cyber-ranges

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

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。

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

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：業務別トレーニング

IT管理者のためのセキュリティ基礎

PCI DSS準拠トレーニング

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。各業務に基づいた短いモジュールに分割されているトレーニングを選択して受講し、業務に応じて必要となるセキュリティの概念について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

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本要素

基本的なクラウドセキュリティの概念や原則、用語などについて理解する必要はあるものの、実際にクラウド技術で手を動かすことはない方のためのコースです

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

SANS SECURITY AWARENESS：業務別トレーニング

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、ソフトウェア開発工程に携わる、アーキテクトやテスター、管理者やビジネスオーナー、そしてパートナーを含む様々な業務に応じたトレーニングを活用し、上流工程からセキュリティを意識したアプリケーションを開発できるようにします。

産業用制御システム（ICS）セキュリティ

ICS・OT（Operational Technology）に携わるすべての方が知っておくべき知識

ICSセキュリティの基礎	ICS410 ICS/SCADA Security Essentials™ | GICSP

管理者のためのICS・OTセキュリティ

ICSセキュリティの基礎	ICS418 ICS Security Essentials for Leaders™

セキュリティリーダーシップの基礎知識

すべてのサイバーセキュリティに関する管理職が知っておくべき知識

CISSP®トレーニング	LDR414 SANS Training Program for CISSP® Certification™ | GISP
セキュリティ意識	LDR433 Managing Human Risk™ | SSAP
RISK ASSESSMENT	LDR419 Performing a Cybersecurity Risk Assessment™

優秀なセキュリティ技術者が増える中、それぞれの組織ではチームや業務を管理するためのリーダーが必要とされています。管理職は必ずしもセキュリティの実務を行うわけではありませんが、ポリシーや業務戦略の策定、技術担当者とのコミュニケーションや業績評価のために、基礎的な技術やフレームワークについて理解しておく必要があります。

SANS SECURITY AWARENESS：業務別トレーニング

全役職員のためのセキュリティ意識向上トレーニング

SANS SECURITY AWARENESSオンライントレーニングでは、全役職員にとって必要となる、緊急性の高いリスクやコンプライアンスに関するモジュールも提供しています。各役職員のセキュリティ行動を促し、組織全体のセキュリティ向上に繋がります。
※モジュールごとで多言語対応というのはこだけでなくSecurity Awarenessの一般的な話なので省いてあります。

サイバーレンジ

全てのセキュリティ担当者のための実践演習

スキルの確認と実践演習	BootUp CTF Core NetWars Core NetWars Continuous

SANSのサイバーレンジでは幅広いトピックをカバーするインタラクティブな実践演習を通じ、それぞれのスキルの確認と定着を促します。

人工知能（AI）

AIセキュリティの基礎

AI	AIS247 AI Security Essentials for Business Leaders™

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 Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ | 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

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ス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 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
LINUXフォレンジック	FOR577 LINUX Incident Response and Threat Hunting™

WindowsやLinuxなどの各ホストやサーバー、またはネットワーク上でのフォレンジックを行い証跡をまとめたり、こうしたスキルを用いてスレットハンティングを行ったりするために、攻撃の分析や初動対応、本格的なインシデントレスポンスやシステム回復のための専門的な知識が必要です。

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 Cloud Security Controls and Mitigations™ | GPCS
自動化とDevSecOps	SEC540 Cloud Security and DevSecOps Automation™ | GCSA
監視と検出	SEC541 Cloud Security Threat Detection™ | GCTD
アーキテクチャ	SEC549 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。

産業用制御システム（ICS）セキュリティ

ICS・OT（Operational Technology）に携わるすべての方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™

産業用制御システムによって現実世界は動かされており、ICSを守るセキュリティ担当者は極めて重要な役割と言えます。OTや国家安全保障、そして人命を守るために、重要インフラを守るスキルを身につけましょう。

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	LDR512 Security Leadership Essentials for Managers™ | GSLC
セキュリティ戦略	LDR514 Security Strategic Planning, Policy, and Leadership™ | GSTRT
セキュリティ文化	LDR521 Security Culture for Leaders™

運用周りのセキュリティリーダー

脆弱性管理	LDR516 Building and Leading Vulnerability Management Programs™
SOC	LDR551 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 CIS Controls™ | GCCC

サイバーレンジ

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

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

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
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™ | GMLE

Open-Source Intelligence

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

攻撃者の高度技術 | 専門的な技術と分野

ネットワーク、Web、クラウド

Exploit開発	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ | GXPN 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

レッドチーム	SEC565 Red Team Operations and Adversary Emulation™ | GRTP 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 Product Security Penetration Testing – Safeguarding Supply Chains and Managing Third-Party Risk™
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 Advanced Purple Teaming – Adversary Emulation & Detection Engineering™

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 and Cyber Extortion™
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 and Threat Hunting™

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	LDR520 Cloud Security for Leaders™

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：業務別トレーニング

ICS技術者のためのトレーニング

産業用制御システム（ICS）をはじめとするOT（Operational Technology）技術者や運用担当者、その他OT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身につけることができます。

高度なセキュリティリーダーシップ

サイバーセキュリティに関する多様な専門業務を管理するための知識

設計と実装	LDR520 Cloud Security for Leaders™
プロジェクトマネジメント	LDR525 Managing Cybersecurity Initiatives & Effective Communication™ | GCPM
インシデントレスポンス	LDR553 Cyber Incident Management™

SANS SECURITY AWARENESS：業務別トレーニング

リーダー・管理者のためのセキュリティの基礎

リーダーシップに焦点を当てた各種モジュールでは、管理職堂の方がチーム・部署を運用するために必要不可欠な、安全なデジタル環境を効率的に構築・運用・維持するためのノウハウを得られます。

www.sans.org

Japan@sans.org

「コース全体では多くのトピックが取り上げられており、特にクラウドIRとクラウドインフラストラクチャに対する攻撃者の手法が取り上げられています。講師は知識が豊富で、プレゼンテーションも的確で、学習体験全体を向上させることができました。」

—Joshua Wright, アメリカ陸軍

「このコースは、提供されるコンテンツがよく構成されており、実践的な演習が組み込まれているため、素晴らしいコースです。」

—Malay P., 米国連邦政府

「優れた教材と指導内容です。このコースを最大限に活用するためには、インストラクターの専門知識と同じコースを受講している生徒の経験から得られるメリットを享受するため、対面での受講がおすすめです。」

—Nicholas A., 連邦捜査局（FBI）

SANS | GIAC CERTIFICATIONS