SANS

The most trusted source for information security training, certification, and research.

INFORMATION SECURITY TRAINING

JAPAN

2020年（2020年8月～2021年3月）

コースカタログ

90+
Certified instructors

200+
Live events globally, plus multiple online options

"Best training I've attended. Great material that you can apply immediately."
- Nik Whitis, AFG

Curricula

- Cyber Defence
- Detection & Monitoring
- Penetration Testing
- Incident Response
- Cyber Threat Intelligence
- Ethical Hacking
- Security Management
- Audit | Legal
- Secure Development
- ICS/SCADA Security

REGISTER AT
www.sans.org

CONTACT US AT
Japan@sans.org
JAPAN **+81 3 3242 6276**

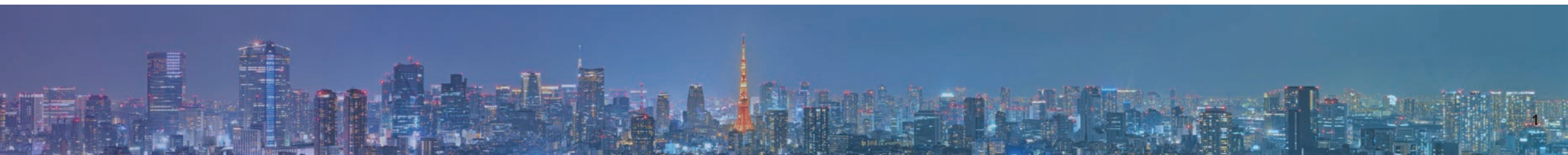
Ver. 201912

SANS 2020 Event Schedule（2020年8月～2021年3月）

（2020年10月8日現在）

Courses	Japan Bi-Lingual Live Online 2020 Aug31-Sep5	Tokyo Autumn 2020 Oct5-17	Tokyo Nov 2020 Nov9-14	Tokyo Dec 2020 Nov30-Dec5	Tokyo Jan 2021 Jan 18-23	Secure Japan 2021 Mar 1-20
SEC401: Security Essentials Bootcamp Style			SEC401			SEC401 (w1)
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis		SEC487				
SEC501: Advanced Security Essentials – Enterprise Defender			SEC501			
SEC540: Cloud Security and DevOps Automation					SEC540	
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling		SEC504		SEC504		SEC504 (w1)
SEC511: Continuous Monitoring and Security Operations		SEC511				SEC511 (w2)
SEC530: Defensible Security Architecture						
SEC542: Web App Penetration Testing and Ethical Hacking			SEC542			SEC542 (w1)
SEC545: Cloud Security Architecture and Operations		SEC545				SEC545 (w2)
SEC555: SIEM with Tactical Analytics						
SEC560: Network Penetration Testing and Ethical Hacking	SEC560			SEC560		SEC560 (w2)
SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses			SEC599			
SEC642: Advanced Web App PenTesting, Ethical Hacking & Exploitation Techniques						
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking		SEC660				
SEC760: Advanced Exploit Development for Penetration Testers						SEC760 (w2)
FOR500: Windows Forensic Analysis		FOR500			FOR500	
FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics	FOR508			FOR508		FOR508 (w1)
FOR572: Advanced Network Forensics: threat Hunting, Analysis, and Incident Response					FOR572	
FOR578: Cyber Threat Intelligence				FOR578		
SEC588: Cloud Penetration Testing						SEC588 (w3)
FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques		FOR610				FOR610 (w1)
ICS410: ICS/SCADA Security Essentials					ICS410	
SANS NetWars Cyber Ranges						

※実施コースは変更される可能性があります。最新の情報はWebサイトにてご確認ください。
※赤文字のSEC401、SEC504は、日本語/日本語テキストによる講義。黒文字は同時通訳による講義。
※20201年3月末までは「ライブオンライン」による開催となります。
※Secure Japan 2021の(w1)は第1週目、(w2)は第2週目、(w3)は第3週目の実施を表します。



Training Roadmap

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

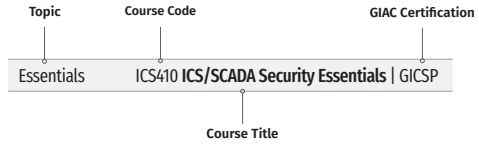
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

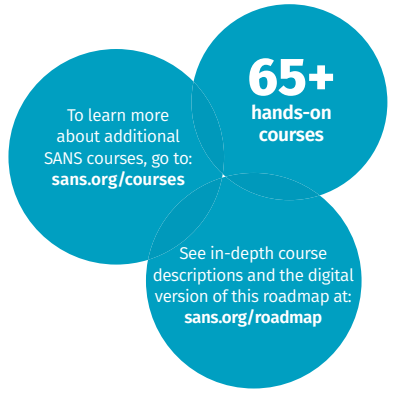
DevSecOps

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:





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

SANS トレーニングフォーマット

SANS Institute は、ライブコース、OnDemand コースなどの形態にかかわらず、トレーニングで得られる知識・スキル・経験が皆さんの期待値を上回るよう全力で努力しています。

ライブコース インストラクション

プレミアムトレーニングイベント

SANS のトップインストラクターが担当するライブイベントが、私たちが最も推奨するトレーニングフォーマットです。

- 集合研修型で集中的に行われる講義
- SANS 認定インストラクターと直接コンタクトできる環境
- 他の受講生との具体的なディスカッション
- NetWars トーナメントや Community Night などのボーナスセッションなど、研修以外のプログラムが併設

ワシントンDCやラスベガスなど、数十コースが同時に進行し、1,000人以上の参加者が集う大規模なトレーニングイベントが毎年開催されています。

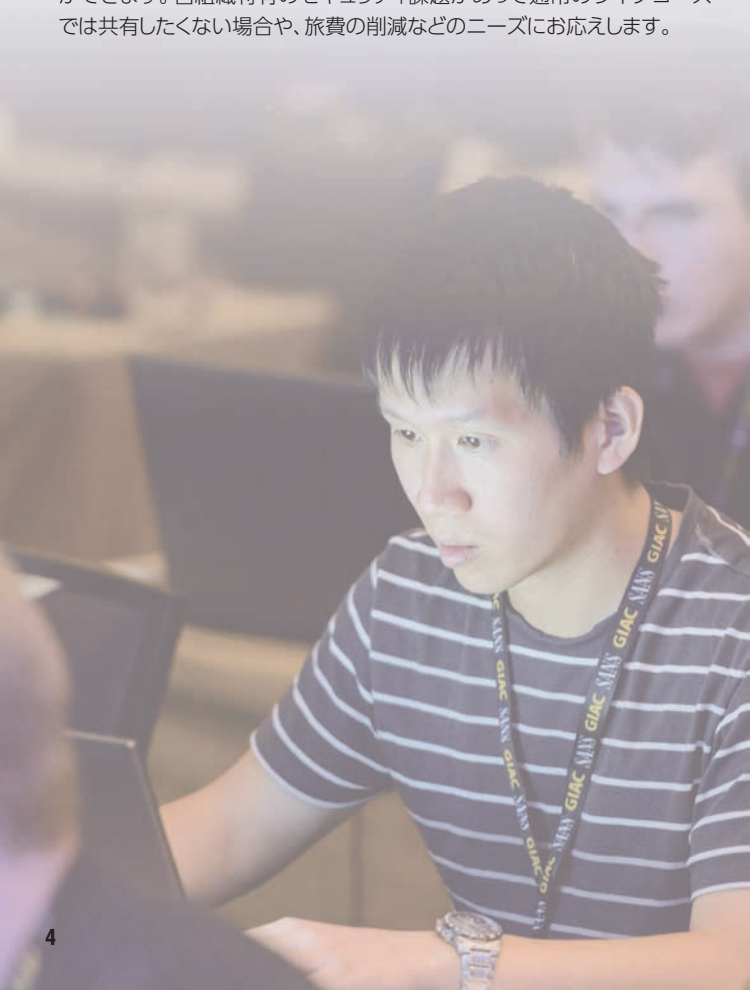
最近では、東京でも10コース程度が1つのイベントで実施され、およそ300人の受講者が集まる規模で開催しています。

Summits

Summit（サミット）と呼ばれるフォーマットは、1-2 日間で行われるコミュニティイベントです。国内外の専門家がスピーカーとして登壇し、参加者も交えて活発な意見交換を行います。

プライベートクラス

25人以上の受講者がいれば、SANS 認定インストラクターを派遣することができます。自組織特有のセキュリティ課題があって通常のライブコースでは共有したくない場合や、旅費の削減などのニーズにお応えします。



オンライントレーニング

SANS のオンライントレーニングは、ライブコースと同等の学習効果を遠隔地の受講者に提供します。

30 コース以上の選択肢をご用意し、いつでもどこでも好きなときに受講できます。遠隔地の方やライブコースの開催時にタイミングが合わなかった方など、毎年数千人の方々がオンラインコース（OnDemand）を受講し、GIAC 認定資格を取得しています。

SANS トレーニングをオンラインで受講するメリットとしては、

- **自身のペースで 4 か月以上にわたって受講できる**
- **理解するまで何度でも受講可能**
- **ライブトレーニングと同じハンズオン演習を何度でも**
- **旅費・渡航費の削減**
- **自宅や職場など都合のいい場所で効率よく学習できる**

SANS OnDemand、vLive、Simulcast、SelfStudyの各プログラムは、約100名のプロフェッショナルによるサポート体制で、ライブトレーニングとほぼ同じ品質をご提供します。

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

“広範囲にわたるセキュリティスキルを学ぶことができ、自分の不足している部分を確認することができました。”

-SEC501受講（システムインテグレータ）

SEC401

GSEC Certification
Security Essentials

www.giac.org/gsec

Security Essentials Bootcamp Style

受講日数:6日間
46 CPEs

Secure Japan 2020
3月2日～14日

Cyber Defence Japan 2020
6月29日～7月11日

Tokyo Autumn 2020
10月5日～17日

Osaka 2020
11月9日～14日

日本語教材を使用し、
日本語で講義を行います。

本コースは、SANS のトレーニングラインナップの中で最もポピュラーなコースです。このコースで、GIAC の GSEC 認定取得に必要な全カリキュラムを学習すれば、必要な学習・演習の時間を最大限に活用して、情報セキュリティ業務におけるキャリアアップを図ることができます。また、このコースで扱う最新の知識と技術は、組織とシステムのセキュリティ確保の責任を担う方々にとって、業務を効率的に遂行する上で必要不可欠なものとなるでしょう。

自組織にとってリスクとは何ですか？ ＞ そのリスクは最も優先度の高いリスクですか？ ＞ そのリスクを低減する最も効果的で安価な対策は何ですか？

セキュリティとは、正しく防衛する分野に集中することです。SEC401 では、コンピュータと情報セキュリティに関する言語と基礎理論を学びます。あなたがシステムや組織を保護する責任がある場合には、必要とされる基本的で効果的なセキュリティ知識を短期間で身に付けることができます。

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

受講日数:6日間
37 CPEs

Secure Japan 2020
3月2日～14日

Cyber Defence Japan 2020
6月29日～7月11日

Tokyo Autumn 2020
10月5日～17日

Osaka 2020
11月9日～14日

日本語教材を使用し、
日本語で講義を行います。

本コースは、悪意ある者のねらいとその手口を詳細に理解し、それを踏まえた脆弱性の発見と侵入検知の実技経験を養い、ペネトレーションテストや総合的なインシデントハンドリングが行えるようになることを目的としています。単なるハッキング攻撃技術の講義にとどまらず、アタッカーによる攻撃手法を詳細に見ていくことで攻撃に対する準備、検知、レスポンスを可能にし、段階的なプロセスを経たコンピュータインシデントハンドリング手法の習得を目指します。そして、演習を通じて、アタッカーより先にセキュリティホールを検知する訓練を行います。さらに、従業員の監視や法的措置をとる際の手順、証拠の保全といった、コンピュータアタックのレスポンスに絡む法的な問題についても取り上げます。

このコースは、特にインシデントハンドリングに携わる方の受講をお勧めします。また、一般的なセキュリティ業務、システム管理、セキュリティ構築などを担当している方にも、攻撃の阻止、検知、レスポンスを行うためのシステム設計、構築、運用の方法が理解できるという点で有益でしょう。

SEC501

Advanced Security Essentials – Enterprise Defender

GCED Certification
Enterprise Defender

www.giac.org/gced

受講日数:6日間
38 CPEs
Secure Japan 2020
3月2日～14日
Tokyo Autumn 2020
10月5日～17日
英語教材/同時通訳

本コースは、セキュリティチームが組織を守るためのコアポリシーとプラクティスの全てが学べるよう設計されています。従来から「予防は理想、検知は必須」というコンセプトがあります。しかし、ただ検知するだけではほとんど価値がありません。ネットワークセキュリティは、可能な限り多くの攻撃を防ぎ、発生したインシデントを迅速に検出して適切に対応するという「PREVENT - DETECT – RESPONSE」戦略を実現するために、絶え間なく改善する必要があります。
もちろん、攻撃を防ぎ、重要なデータを保護するための最善の努力にもかかわらず、いくつかの攻撃は成功してしまうでしょう。したがって、組織は適時に攻撃を検知できる必要があります。これは、ネットワーク上を流れるトラフィックを理解し、攻撃の兆候を探し、侵入前に問題や問題を特定するためのペネトレーションテストと脆弱性分析を組織に実施することで実現します。次に、攻撃が検知された時点で迅速かつ適切に対応し、必要なフォレンジックを実行する必要があります。攻撃者がどのように侵入したかを理解することによって得られた知識は、証拠保全や再発防止対策にフィードバックされ、セキュリティライフサイクルを完了することができます。
本コースでは、組織の情報セキュリティを堅牢化する全ての要素が習得できます。

SEC511

Continuous Monitoring and Security Operations

GMON Certification
Continuous Monitoring

www.giac.org/gmon

受講日数:6日間
46 CPEs
Secure Japan 2020
3月2日～14日
Tokyo Autumn 2020
10月5日～17日
英語教材/同時通訳

今まで多くの企業・組織が、多くの時間・資金・人材を投資して、サイバー上の脅威とサイバー攻撃に対して立ち向かってきました。このような多大な努力にもかかわらず、いまだに侵入被害にあっています。
セキュリティアーキテクチャ防衛戦略（アプローチ）として、ネットワークセキュリティ監視(Network Security Monitoring: NSM)、持続的な診断と緩和(Continuous Diagnostics and Mitigation: CDM)、持続的なセキュリティ監視（Continuous Security Monitoring: CSM）があります。これらの防衛戦略をこのコースで学ぶことにより、攻撃者の兆候に気付き、敵を検出し脅威を分析することが、あなたの組織や SOC（Security Operation Center）で自ら行えるようになります。このようなプロアクティブ（先駆的）なアプローチを行うことで侵入の早期検知を行うことが可能となり、攻撃者の計画をくじくことができるでしょう。
本コースは、セキュリティ監視に当たる方々にとって画期的な内容を提供します。

SEC530

Defensible Security Architecture and Engineering

GDSA Certification
Defensible Security Architecture

www.giac.org/gdsa

受講日数:6日間
36 CPEs
2021年1月～3月期に
実施予定

本コースは、真に防御できるセキュリティアーキテクチャを構築し維持するスキルを習得できるように設計されています。モバイル、クラウド、IoT の進展に伴って「境界防御はもはや無意味だ」と言われるようになっています。確かに私たちは、境界の内と外とか、「信頼できる」「信頼できない」といった概念がもはや通用しない「脱・境界」の世界に住んでいます。この変化する景観は、多くのデバイスの利用変更と同様にマインドセットの変更を必要とします。
本コースでは、最新の防御可能なセキュリティアーキテクチャの基礎を学びます。スイッチ、ルータ、ファイアウォールなどの現在のインフラを活用し、今日直面している脅威をより効果的に防御するために、それらのデバイスを再構成する方法を習得します。また、堅牢なセキュリティインフラを構築するのに有効な新しいテクノロジーも提案します。
このコースで学ぶセキュリティアーキテクチャがインシデントの予防に役立つとともに、SIEM への重要なログの提供にもつながるため、SOC における継続的なセキュリティ監視にも相乗効果が出るでしょう。

SEC540

Cloud Security and DevOps Automation

受講日数:5日間
38 CPEs
Secure Japan 2020
3月2日～3月14日
英語教材/同時通訳

本コースは、開発者と運用者、セキュリティの専門家に、DevOps とクラウドサービスを使用して安全なインフラストラクチャとソフトウェアを構築・提供する方法を学び、DevOps の原則、実践、ツールが、オンプレミスやクラウドでホストされるアプリケーションの信頼性、整合性、セキュリティをどのように改善できるかを習得します。
コース前半の 2 日間は、現在有効に機能している DevOps セキュリティプログラムからの教訓を使用して、Secure DevOps の実装を検証します。 GitLab、Puppet、Jenkins などのオープンソースツールを使用して、インフラストラクチャとアプリケーションを自動的に構築、テスト、展開できる安全な DevOps CI/CD ツールチェーンを作成します。コース後半の 3 日間では、DevOps のワークロードをクラウドに移行し、AWS を使用してソフトウェアをセキュリティで保護することを習得します。CI/CD ツールチェーンを使用して、クラウド環境にアプリケーションとマイクロサービスを展開できるクラウドインフラストラクチャを構築します。また、AWS セキュリティサービスおよびツールを使用して、クラウドインフラストラクチャおよびアプリケーションの脆弱性を分析・修正します。
本コースでは、自動構成管理（"Infrastructure as Code"）、継続的統合、継続的配信、継続的展開、コンテナ化、マイクロセグメンテーション、自動コンプライアンス（"Compliance as Code"）、継続的モニタリングなどのための様々な素材とツールを使用し、インフラストラクチャやアプリケーションを堅牢化するノウハウとテクニックを習得します。

SEC545

Cloud Security Architecture and Operations

受講日数:5日間
30 CPEs
Secure Japan 2020
3月2日～14日
Tokyo Autumn 2020
10月5日～17日
英語教材/同時通訳

多くの組織がクラウド環境に情報インフラやデータを移行するにつれて、セキュリティが重要な優先事項になっていますが、多くのクラウドプロバイダは、内部環境に関する詳細な制御情報を開示しておらず、一般的に実装されているセキュリティコントロールのほとんどがクラウド環境では適用されていない場合もあります。
本コースでは、これらの課題に一つずつ取り組みます。すべての主要なクラウドタイプ（SaaS、PaaS、および IaaS）の技術セキュリティ原則とコントロール、クラウドサービスのリスク評価と具体的に対処する必要がある技術分野、クラウドアーキテクチャとセキュリティ設計、セキュアなインスタンスやデータセキュリティ、アカウント管理など、各レイヤーとその中のコンポーネントをカバーし、脆弱性管理とペンテストも扱います。また、インシデントハンドリングやフォレンジック、イベント管理、アプリケーションセキュリティについても掘り下げます。さらに、SecDevOps と自動化についても深く触れます。動作するツールやテクニックを探求し、API とスクリプトを使ったインシデントの検出と対応のシナリオの両面でセキュリティを完全に自動化できるいくつかの最先端のユースケースを紹介します。
クラウドサービスを利用する組織の技術者の方は必須のコースです。

SEC550

Active Defense, Offensive Countermeasures and Cyber Deception *NEW!*

受講日数:5日間
30 CPEs
Tokyo Autumn 2020
10月5日～17日
英語教材/同時通訳

現在の脅威の状況は刻々と変化しています。従来の防御は有効な対策にはならず、自組織を守るための新しい戦略を開発する必要があります。さらに重要なことは、誰が攻撃しているのか、そしてその理由は何かをよりよく理解する必要があるということです。本コースで説明する防御対策は、すぐに実装できる場合もあれば、しばらく時間がかかる場合もあります。いずれにせよ、攻撃者を困らせ、攻撃者を特定し、最後に攻撃者を攻撃する必要がある場合、自由に使用できるツールのコレクションを検討しておくことが重要になるということです。
本コースは、Defense Advanced Research Projects Agency（DARPA）から資金提供を受けた Active Defense Harbinger Distribution のライブ Linux 環境に基づいて構成されています。この仮想マシンは、防御者が環境にアクティブな防御を迅速に実装できるようにゼロから構築されています。本コースには実践的な演習がふんだんに用意されています。受講者一人ひとりが自身の作業環境の構築に取り組みつつ、迅速かつ簡単に実装できるアクティブディフェンスを習得します。

SEC555

SIEM with Tactical Analytics

GCDA Certification
Detection Analyst
www.giac.org/gcda

受講日数:6日間
46 CPEs
Cyber Defence Japan 2020
6月29日～7月11日
英語教材/同時通訳

多くの組織ではログを収集する機能はありますが、分析手法が確立していないか、そのプロセスが不足しています。また、ログシステムは、適切な分析のためにソースの理解を必要とするさまざまなデータソースから膨大な量のデータを収集します。本コースでは、既存のログソリューションを強化するための手法やプロセスを習得し、ログの背後に意味を理解することができます。演習では、SANS がスポンサードする無償の SIEM ソリューションである SOF-ELK を活用し、大規模なデータ分析の経験を積んでいただくという、ヘビーでタフなコースです。
本コースでは、セキュリティ情報とイベント管理（SIEM）のアーキテクチャとプロセスを解明します。そして、SIEM を完全な SOC に統合して運用する手順を学習します。多くの異なる基盤から収集したログを相関分析するために利用可能なフォーマットにする手法、相関分析・調査手法、高度な攻撃を素早く検出する手法などに時間を割きながら、プロセスの多くを自動化して、皆さんがオフィスにもどってからこれらのタスクをすぐに実践できる方法を示します。
本コースの根本的なテーマは、最新のサイバー攻撃を利用して、継続的な監視・分析手法を積極的に適用することです。

SEC599

Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses

GDAT Certification
Defending Advanced Threats
www.giac.org/gdat

受講日数:6日間
36 CPEs
Cyber Defence Japan 2020
6月29日～7月11日
英語教材/同時通訳

本コースの目的は、今日の最新の脅威を検出して対応するために必要な知識と専門スキルを習得することです。予防のみの戦略ではもはや不十分であることを認識し、先進的な攻撃者を阻止するためのセキュリティ対策を実装することを学びます。
20 以上の演習と、最終日に行うエクササイズ “Defend-The-Flag” を通じて、受講生は実際にどのように攻撃を防ぐのかを現実世界の例を見ながら取得します。ケーススタディによる最近の攻撃の詳細分析、頻発する攻撃のタイプ、APT 攻撃サイクルから始まり、サイバー攻撃を防止、検出、対応するために効果的なセキュリティ制御をどのように実装するかを 5 日間にわたって説明します。主な内容としては、スピアフィッシングを検出するためのサンドボックスソリューションの構築、エクスプロイトの緩和テクニックとホワイトリストを利用した0—Day 攻撃の阻止、マルウェアの検出、Windows イベント監視とグループポリシーによる攻撃拡散の検知と防止、ネットワークトラフィック分析による C&C のブロックと検知、スレットインテリジェンスを活用したセキュリティ機能の改善などです。また、本コース全体で扱うツールやシステムは USB で提供され、仮想環境上ですぐに利用可能です。
本コースに参加すると、先進的な敵と戦うことになります。攻撃者は容赦なく襲いかかってきます。皆さんはさまざまな攻撃の波に対して対応できますか?

SEC487

Open-Source Intelligence (OSINT) Gathering and Analysis *NEW!*

受講日数:6日間
36 CPEs
Tokyo November 2020
11月30日～12月5日
英語教材/同時通訳

現在、計り知れない量の個人情報や潜在的に他者に損害を与え得るデータは、様々なデバイスを介して毎日アクセス・更新する Web サイト、アプリ、ソーシャルメディアプラットフォームに保存されています。これらのデータは、個人や企業、政府が金銭的なトラブルや事故・事件を解決する際に使用する証拠となり得るものです。
多くの人は、お気に入りのインターネット検索エンジンを使用すれば必要なデータを見つけるのに十分であると考えていて、インターネットのほとんどが検索エンジンによってインデックス付けされていないことに気付いていません。本コースは、インターネットからこうしたデータを発見し、収集し、分析するための合法的かつ効果的な方法を教えます。様々なツールを使用して、データを収集するに足る信頼できる場所について学習します。情報が得られたら、それが正しいことを確認する方法、収集したものを分析する方法、および調査に役立つようにする方法を示します。
受講生には、インターネットから無料のデータを収集するための基礎となるツールとテクニックを習得するために、多数のハンズオンラボが提供されます。20 以上に及ぶラボでは、ライブインターネットとダークウェブを使用しながら、真に重要な OSINT データを収集するために必要なシナリオベースの要件と OSINT テクニックのすべてを知ることができます。

SANS Intermediate and Specialised Skills

Penetration Testing & Vulnerability Analysis

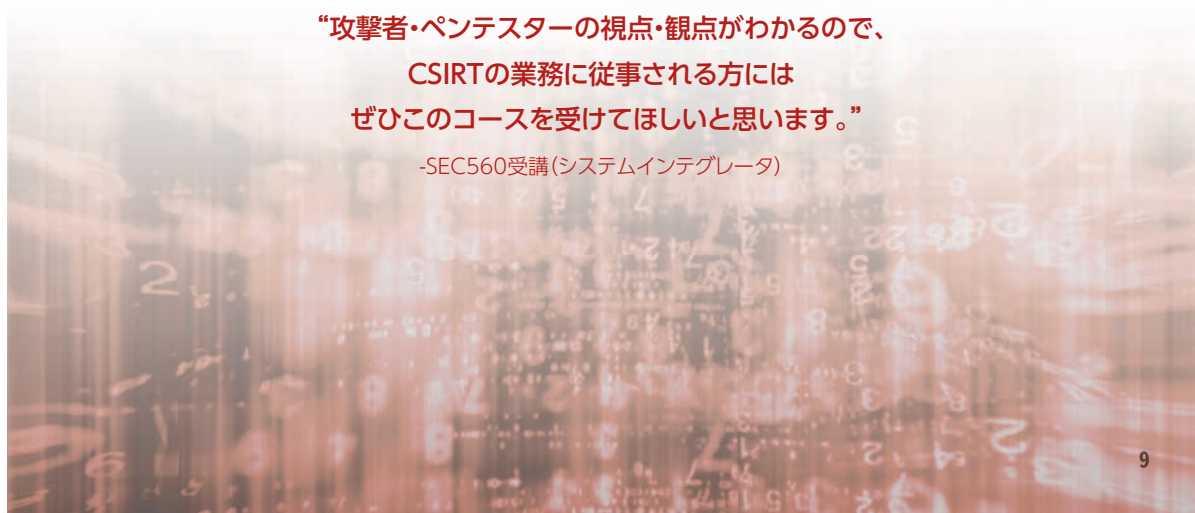
SEC560

Network Penetration Testing and Ethical Hacking

GPEN Certification
Penetration Tester
www.giac.org/gpen

受講日数:6日間
37 CPEs
Secure Japan 2020
3月2日～14日
Cyber Defence Japan 2020
6月29日～7月11日
Tokyo November 2020
11月30日～12月5日
英語教材/同時通訳

ペンテスターは、組織の情報システムの脆弱性を発見して理解するというユニークな責任を負っているサイバーセキュリティプロフェッショナルです。さらに、攻撃者が攻撃を仕掛けてくる前に、リスクを軽減するための様々な方策を講じなければなりません。SANS のペネトレーションテスト分野のフラッグシップコースである SEC560 は、この職務を全うするための強力なスキルをあなたに提供します。
本コースは、セキュリティの専門家すべてに受講いただきたいバランスのとれたコースです。適切な計画、スコープの設定や偵察といった項目から始め、その後に 30 以上の詳細な演習を通じて、スキャニング、エクスプロイト、パスワードアタック、ワイヤレス、Web アプリケーションといった詳細に進んでいきますので、侵害を受ける前に、自組織のシステムをテストする最良の方法を習得できます。本コースの受講を通じて、包括的なペンテストスキル、Ethical Hacking のノウハウを持ち帰っていただきます。



SEC542

GWAPT Certification
Web Application Penetration Tester

www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

受講日数:6日間
36 CPEs
Cyber Defence Japan 2020
6月29日～7月11日
Tokyo November 2020
11月30日～12月5日
英語教材/同時通訳

最新のサイバー防衛では、Web アプリケーションのセキュリティ上の課題を現実的かつ徹底的に理解していなければ太刀打ちできません。Web に対するいくつかのハッキング技術を手軽に学ぶことはできますが、Web アプリケーションの侵入テストではより深くかつ体系化された手法が不可欠です。SEC542 は、多くの組織を悩ませている Web アプリケーションのセキュリティ状況を正しく評価し、発見された脆弱性や欠陥の影響を実証するスキルを受講者に提供します。また、各自が所属組織に戻った後も継続してこれらのスキルが活用できるよう、フィールドテストプロセスや反復プロセスなども徹底的に学びます。ある程度の技術力を持ったいわゆる「セキュリティオタク」は、組織のリスクを業務に関連付けて説明できません。侵入テストのトレーニングの多くは、適切な対策を採用するように組織に働きかけるというよりも、攻撃者が行うのと同等の手法を習得するというリスクの側面の方が強調されがちです。SEC542 の目標は、単に高度なハッキングスキルを習得することでなく、侵入テストを正しく活用して組織をより安全にすることです。

SEC642

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

受講日数:6日間
36 CPEs
Tokyo January 2020
1月20日～25日
英語教材/同時通訳

アプリケーションの脆弱性を調査する方法や手法から始め、各種の制御と保護を迂回しシステムを悪用する高度なアイデアやスキルを身に付けます。Web アプリで利用する暗号化方式を識別し、その動作原理と悪用方法および破る方法を習得。さらに、Web アプリケーションファイアウォールやフィルタリング、他の防御技術を識別し回避する方法を学習します。また、これらを通じて安全な Web アプリケーションの開発、構築・運用も理解できます。このペンテストコースは、現代の Web アプリケーションや次世代技術のテストに必要な高度なスキルとテクニックを教授するためのコースです。コースでは、講義、現実の体験、実践的な演習を組み合わせて、エンタープライズウェブテクノロジーのセキュリティをテストするテクニック、最先端のインターネット対応アプリケーションを学びます。最終日は、現実世界の技術に基づいた楽しい環境で、過去 5 日間に取得した知識を適用するキャプチャ・ザ・フラッグ（Capture the Flag）コンテストで最高潮に達します。

SEC660

GXPN Certification
Exploit Researcher and Advanced Penetration Tester

www.giac.org/gxpn

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

受講日数:6日間
46 CPEs
Tokyo Autumn 2020
10月5日～17日
英語教材/同時通訳

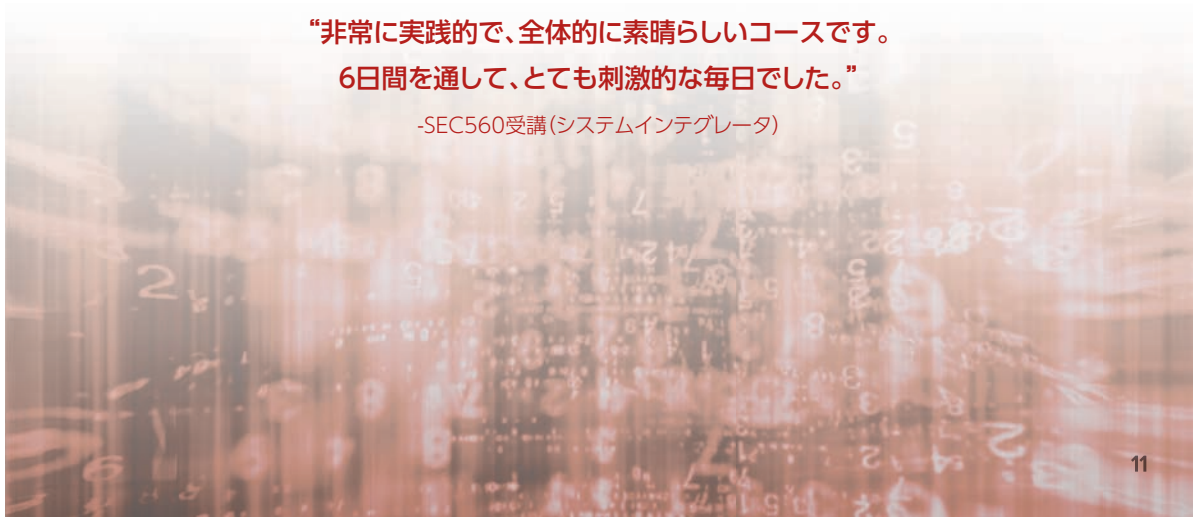
SEC660 は、「SANS SEC560:Network Penetration Testing and Ethical Hacking」コースを修了した方、または同程度のペネトレーションテストの経験を既にお持ちの方々が、さらなるステップアップをなしとげられるよう設計されたコースです。このコースの受講者は、最も経験豊富な全世界のペンテスターが実際に使用しているいくつもの攻撃方法を体験することができます。また、さらなる技術的な熟練をめざして、講義後に Bootcamp(集中ラボ演習)が含まれています。日々のコースでは、ペンテスターに必要な Python の武器化のほか、ネットワークアクセス制御（NAC）や仮想ローカル・エリア・ネットワーク（VLAN）に対する攻撃、ネットワーク機器への攻撃や、Linux および Windows の制限付き環境からの脱却、IPv6、Linux の特権昇格とエクスプロイト作成、暗号実装へのテストやファジング、また近年の OS による制御機構であるアドレス空間配置のランダム化（ASLR）やデータ実行防止（DEP）の回避、リターン指向プログラミング（ROP）、Windows エクスプロイト作成といった高度かつ広範なトピックを取り上げていきます。
本コースの最大のメリットの 1 つは、豊富なラボと追加演習時に提供される専門家レベルの実践的なガイダンスです。

SEC760

Advanced Exploit Development for Penetration Testers

受講日数:6日間
46 CPEs
Secure Japan 2020
3月2日～3月14日
英語教材/同時通訳

Microsoft Windows や Linux ディストリビューションなどの最新のオペレーティングシステムの脆弱性は、非常に複雑です。これらの脆弱性をスキルが習熟した攻撃者が悪用すると、組織の防御対策が崩壊し、深刻な被害を被る可能性が多分に存在します。
脆弱性に関する基本的な事項を理解している人は多いと思いますが、脆弱性を突くためのエクスプロイトを開発できるスキルセットを有する専門家はほとんどいないのが現状です。攻撃者はこのスキルセットを維持しています。複雑性が増せば増すほど、攻撃者優位の状況に陥ってしまうのです。
本コースでは、32bit/64bit アプリケーションのリバースエンジニアリングやリモートユーザアプリケーションの実行、カーネルエクスプロイト手法、パッチの分析による 1-day エクスプロイトの悪用手法とその対策などの高度なトピックについて学びます。最新のソフトウェアやオペレーティングシステムに対する「use-after-free アタック」などの複雑なエクスプロイトの作成手法についてもカバーします。セキュリティ開発ライフサイクル（SDL）手法を脅威モデル（Threat Modeling）とともに活用することの重要性についても理解していただきます。
様々なデバッグ手法やプラグインを効果的に活用して、脆弱性の調査に要する時間を短縮し、悪用を阻止・緩和するあらゆる手法を身につけていただけるコースです。



GIAC
The Highest Standard in Cybersecurity Certification

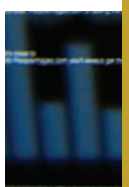
職種別、専門分野別にフォーカスした認定資格
今日のサイバー攻撃は高度に洗練されており、幅広い一般的な情報セキュリティ認定資格はもはや十分ではありません。セユリティの専門家は、複数のさまざまな脅威に対応するために必要な特定のスキルと専門知識が必要です。そのため、GIAC は 30 以上の分野の異なる認定をラインナップしています。それぞれ特定の職務に必要なスキルに重点を置いており、その分野で比類のない明確な知識とスキルがあるかどうかを判定します。

実社会で必要となる実践的な知識
理論的知識は究極のセキュリティリスクです。深刻な現実の課題を解決するための実践的な知識とハンズオンスキルは、セキュリティリスクを軽減する唯一の信頼できる手段です。この知識とスキルが習得されていることを証明するのが GIAC です。実践的なスキルを証明する認定資格という点において、GIAC に匹敵するものはありません。

最も信頼される認定資格制度
認定試験のデザインは、認定資格の質と完全性に影響します。 GIAC の試験内容と出題思想は、専門の心理学者によって設計され、各分野のセキュリティの専門家によってレビューされた厳密なプロセスを通じて開発されています。 1999 年以来、78,000 件以上の認定が発行されています。また GIAC は ANSI/ISO 17024 の認証を取得しています。

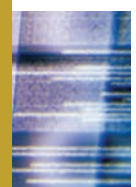
GIAC
DEEPER KNOWLEDGE. ADVANCED SECURITY.

GIAC.ORG



"I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field."

– Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)



SANS Intermediate and Specialised Skills
Incident Response and Enterprise Forensics

FOR508
Advanced Incident Response, Threat Hunting, and Digital Forensics

GCFA Certification
Forensic Analyst
www.giac.org/gcfa

受講日数:6日間
36 CPEs

Secure Japan 2020
3月2日～14日

Cyber Defence Japan 2020
6月29日～7月11日

Tokyo Autumn 2020
10月5日～17日

英語教材/同時通訳

データ侵害のうち80%以上は外部からの通知によるものであり、内部のセキュリティチームにより発見されるものではありません。そして多くの場合、攻撃者が何か月または何年も前からネットワークへ不正にアクセスしていた後で発覚すると言われています。
本コースは、以下の項目を理解することに主眼が置かれています。(1)どのように侵害されたか、(2)どのシステムに侵入されたか、(3)どのデータが持ち去られ、どのデータが改ざんされたか、(4)どのようにインシデントに対処し修正したらよいか。
本コースでは、デジタルフォレンジックアナリストやインシデントレスポンスチームが、APT を含む洗練された攻撃を行う集団や金融犯罪シンジケートに対抗して、脅威の識別、封じ込め、修正を行う手順を学習します。さらに、学習成果を高めるため、ネットワーク業界の先進的企業で実際に起きている標的型攻撃をもとに開発された、実践的な訓練にチャレンジし、課題解決を通して理解を深めていくことで、今までよりも早い段階で攻撃の存在に気付くことができるようになるでしょう。本コースを通じて、誰に何のデータが盗まれたのかを洗い出し、具体的な脅威を封じ込め、攻撃に対抗しマネジメントできる能力をもった人材として成長することができます。

**"インストラクター、教材ともに最高のレベルです。
フォレンジックに興味のある方は、
このコースで最新の深い知識を
身につけてほしいです。"**
-FOR500受講(セキュリティベンダー)

FOR500

GCFE Certification
Forensic Examiner

www.giac.org/gcfe

Windows Forensic Analysis

受講日数:6日間
36 CPEs

Tokyo January 2020
1月20日～25日

Cyber Defence Japan 2020
6月29日～7月11日

英語教材/同時通訳

FOR500(旧 FOR408)は、Windows OSに対するより深いフォレンジックスキル構築に焦点をあてたコースです。「守るものについて知らなければ、何も守ることはできない」という考え方があります。フォレンジックで出来ることやアーティファクトについて理解することは、今やサイバーセキュリティの必須事項といえるでしょう。このコースで、Windowsシステムでのデータ復旧、分析、検証方法を学んでいきましょう。ネットワーク上のユーザーの行動を詳細に追跡する方法を学習し、インシデントレスポンス、内部不正調査、民事/刑事訴訟において、見つかった証拠をどのように整理していけばよいか理解しましょう。あなたがこのコースで身に付ける新しいスキルを存分に活用し、セキュリティツールの検証、脆弱性検査の強化、インサイダーの摘発、ハッカーの追跡、セキュリティポリシーの向上に役立てましょう。Windowsは知らず知らずのうちに、想像を絶するほどの大量なデータを溜め込んでいます。FOR500は、この大量なデータから証拠を発掘する方法を教えます。
演習を行うラボでは、最新のMicrosoft製品で見つかる証拠を分析していただきます(Windows 7、Windows 8/8.1、10、OfficeおよびOffice 365、クラウドストレージ、Sharepoint、Exchange、Outlook)。

FOR572

GNFA Certification
Network Forensic Analyst

www.giac.org/gnfa

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

受講日数:6日間
36 CPEs

Tokyo January 2020
1月20日～25日

Tokyo Autumn 2020
10月5日～17日

英語教材/同時通訳

ネットワークコンポーネントを含まないフォレンジック調査を行うことは非常に稀です。エンドポイントフォレンジックはこの業界において、常にクリティカルかつ基礎的なスキルです。しかし、ネットワーク通信を見落とすことは、犯罪の防犯カメラ映像を無視するようなものです。侵入事件、データ盗難、従業員の不正、攻撃者の発見などの場合に関して、ネットワークは決定的な証明に役立ちます。エビデンスは、目的を説明する必要のある証拠を提供し、数か月以上活動している攻撃者を暴きます。そして、実際に発生した犯罪を明確に証明することに役立てられます。
FOR572は、効率的で効果的なインシデント対応調査のために必要な最もクリティカルなスキルを網羅し、システムやデバイスなどのストレージメディア上の残存データから、過去に発生または引き続き発生している一時的な通信まで、フォレンジックへの考え方を広げるための必要な知識に焦点を当てています。ネットワーク上のエビデンスの調査に取り込むために必要なツール、テクノロジー、プロセスについて、効率的かつ効果的に説明します。この一週間であなたは、豊富なツール類と職場に戻ってからすぐ利用できるスキルを身につけることができるでしょう。

FOR578

GCTI Certification
Cyber Threat Intelligence

www.giac.org/gcti

Cyber Threat Intelligence

受講日数:5日間
30 CPEs

Tokyo November 2020
11月30日～12月5日

英語教材/同時通訳

間違いなく、現在のコンピュータネットワーク防衛とインシデントレスポンスの重要な要素として、インテリジェンスとカウンターインテリジェンスが含まれます。アナリストは、自分たちのコンピュータとネットワークそして保有するデータを守るために、この要素を確実に理解し活用しなければなりません。
従来型のネットワーク防御、たとえば IDS やウィルス対策製品は脆弱性リスクに対して注力しています。また、古典的なインシデントレスポンス手法は、侵入されてから行われる前提になっています。しかし、コンピュータネットワーク侵入の手口は進化かつ洗練されてきており、近年のネットワーク化された組織が直面している脅威には不十分なアプローチであるといえるでしょう。攻撃者に関するナレッジを収集・分類・開発することを、一般にサイバースレットインテリジェンスといいますが、攻撃者が侵入を試みた情報を活用することで、攻撃が成功する可能性を減少させる知見を得ることができます。スレットインテリジェンスは、増加傾向にある洗練された APT 攻撃に対抗する上で、組織の対応能力と検知能力を飛躍的に向上させます。

FOR585

GASF Certification
Advanced Smartphone Forensics

www.giac.org/gasf

Smartphone Forensic Analysis In-Depth

受講日数:6日間
36 CPEs

デジタルフォレンジック調査でスマートフォンまたはモバイル機器がないことは稀です。多くの場合、これらのデバイスは個人の行動追跡や動機の追及に利用できる唯一の情報源となります。誰が、何を、いつ、どこで、なぜ、どのように行ったかを調査することができるでしょう。本コースでは、スマートフォンをエビデンスの取得元として焦点を当て、法廷で採用可能な（forensically sound）調査方法を解説します。そして異なる技術要素を理解し、マルウェアの発見方法や各スマートフォンのファイルシステムに深く踏み込んでフォレンジック調査を行い、結果を解析する方法を解説します。本コースを通じて実用可能な知識を習得して、内部調査や刑事／民事訴訟対策、データの解析・復元方法を身に付けます。フォレンジックアナリストやインシデントレスポンスチームのメンバー、法執行機関の関連業務に従事する方々には必須のコースです。

FOR610

GREM Certification
Reverse Engineering Malware

www.giac.org/grem

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

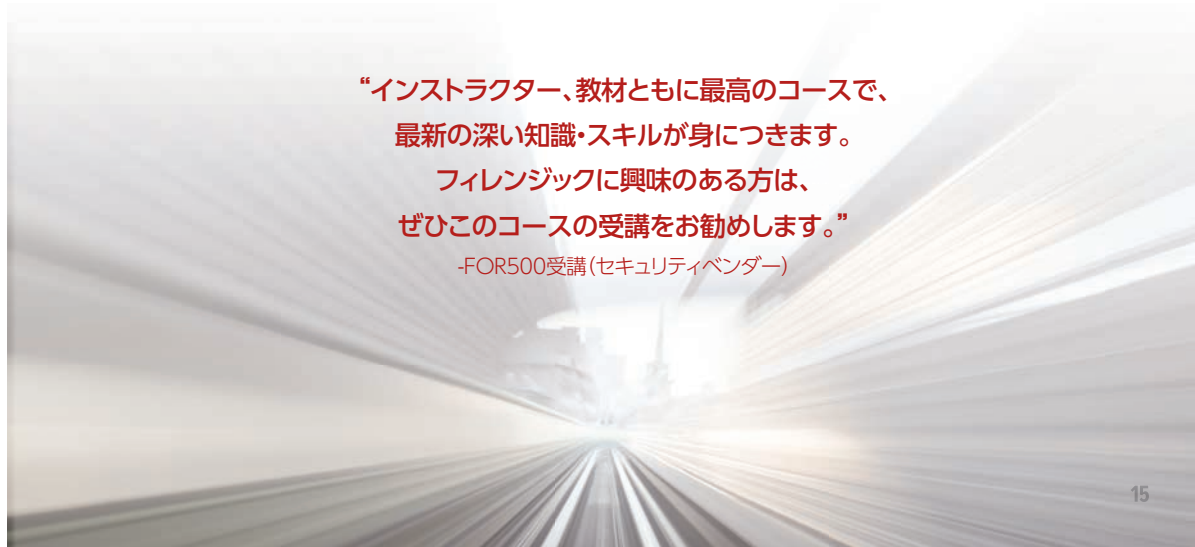
受講日数:6日間
36 CPEs

Secure Japan 2020
3月2日～14日

Tokyo Autumn 2020
10月5日～17日

英語教材/同時通訳

このコースでは、マルウェア解析ツール、手法を詳細に解説していきます。FOR610は、フォレンジック担当者、インシデントレスポンダー、セキュリティエンジニア、IT管理者にとって、感染もしくは標的となったシステム内の悪意あるプログラムを調査するための実践的なスキル獲得に役立ちます。マルウェアの機能を理解することは、組織の能力として重要なことであり、スレットインテリジェンスへの派生、インシデントレスポンス、防衛能力の強化に活用できます。本コースを通じて学習することで、マルウェアのリバースエンジニアリングに関する強固な土台となるスキルを身につけることができます。
安価かつ柔軟なラボをセットアップする方法を学び、悪意あるソフトウェアをその中で動作させ調査する方法を理解していきます。また、自己防衛型機能のあるマルウェアを扱う方法についても学んでいきます。



SANS Intermediate and Specialised Skills

Management | ICS Security | Software Security

ICS410

ICS/SCADA Security Essentials

GICSP Certification
Industrial Cyber Security Professional
www.giac.org/gicsp

受講日数:5日間
30 CPEs
Tokyo January 2020
1月20日〜25日
英語教材/同時通訳

本コースは、産業分野におけるサイバーセキュリティ専門家向けの標準的な基礎知識とスキルを身につけていただくコースです。運用している環境を安全かつセキュアに、そして既知の脅威や新しいサイバー攻撃に対抗できるように訓練することに焦点をあててカリキュラムが組み立てられています。
産業用制御システムに携わるエンジニアの特徴として、多くのエンジニアが大量の機器の機能とリスクを完全に理解しているわけではないことが挙げられます。また、通信とネットワークセキュリティを担当する IT サポート部門は、システムで使用しているドライバーとその制約条件を常に把握しているわけではありません。本コースは、従来の IT 担当者が、制御システムの設計思想と制御システムに対してどのように可用性と完全性を維持・運用すればよいかを、十分に理解できるように作られています。また、制御システムエンジニアと運用担当者の方々がサイバーセキュリティにおいて担う重要な役割を理解してもらえるようにコースを設計しています。制御システムの設計と構築についてサイバーセキュリティの考え方を取り入れることで、システムのライフサイクル全体にわたって、システムの信頼性と同じレベルでサイバーセキュリティを維持する方法を学びます。

ICS515

ICS Active Defense and Incident Response

GRID Certification
Response and Industrial Defense
www.giac.org/grid

受講日数:5日間
30 CPEs

ICS のアクティブディフェンスとインシデントレスポンスに関するこのコースでは、ネットワーク化された産業制御システムの環境を理解し、脅威を監視し、特定された侵害に対してインシデントレスポンスを行うという一連のネットワークセキュリティ強化手法を学びます。
ネットワーク内部の脅威を監視し、侵害が発生する前に対応して教訓化するこのプロセスは、アクティブディフェンス（能動的防御）と呼ばれています。この手法は、Stuxnet や Havex、BlackEnergy2 などの事例でも明らかなように、ICS をターゲットにした先進的な敵に対抗するために必要なアプローチです。受講生は、ICS 攻撃の詳細を理解し、攻撃者と戦う能力を習得して、このコースを修了することを期待できます。本コースでは、実際のマルウェアを使用した実践的なアプローチによって、ICS のサイバー攻撃を最初から最後まで掘り下げます。その過程において、効果的なスレットインテリジェンス、実効性のあるネットワークセキュリティ監視、マルウェア解析、インシデントレスポンスの活用など、アクティブディフェンスが包含する実践的かつ技術的なスキルを得ることができます。
本コースで提示される戦略と技術的スキルは、実行可能な ICS の防御対策を模索している組織の基盤となります。

SANS NETWARS CYBER RANGES

Earn up to 6 CPEs!

NEW! CYBER DEFENCE NETWARS TOURNAMENT

NetWars Defense Competition は、防御スキルに焦点を当てたCTFチャレンジです。侵害からシステムを防御するためには、妥協することなくシステム上の問題を解決する高い能力が求められます。アーキテクチャ、オペレーション、スレットハンティング、ログ分析、パケット解析、暗号などのスキルがどれくらいなのか、自己の能力を測定できる貴重な経験ができます。

参加対象者

- システム管理者
- エンタープライズディフェンダー
- アーキテクト
- ネットワークエンジニア
- セキュリティ運用技術者
- インシデントレスポンダー
- セキュリティアナリスト
- セキュリティ監査人

など

DFIR NETWARS TOURNAMENT

DFIR NetWars は、実際のインシデントに対応する際に必要なスキルを獲得するためのフォレンジックやマルウェア解析、脅威分析、インシデントレスポンスの課題が満載のインシデントシミュレータです。制限時間内に課題に対処できるかどうかチャレンジすることで、現在のスキルを試すことができます。また、不足しているスキルを特定することもできます。

参加対象者

- フォレンジックアナリスト
- マルウェアアナリスト
- インシデントレスポンダー
- サイバー犯罪捜査官
- SOC アナリスト　など

Core NETWARS EXPERIENCE

Core NetWars は、自らのコンピュータ・ネットワークセキュリティに関するスキルレベルを把握し、さらなるキャリアを積むためには何が必要か、どんな分野の知識・スキルを習得すればいいかなどを判定するために開発された CTF チャレンジです。Core NetWars Experience は他の参加者と楽しみながら、実世界のシステム・ネットワークを模した疑似環境の中で、思う存分腕試しができるというものです。勝者を決めるための競技会というよりは、自己研さん目的でデザインされた CTF チャレンジですので、問題回答、キャプチャー・ザ・フラッグ、攻防戦など、CTF のすべての要素が 1 つの環境に配置され、バランスのいい知識・スキルが求められます。

参加対象者

- セキュリティ技術者
- システム管理者
- ネットワーク管理者
- ペネトレーションテスター
- インシデントハンドラー
- セキュリティ監査人
- SOC オペレーター　など

SANS

The SANS Japan Team is ready to assist you

SANS JAPAN OFFICE

Japan@sans.org | 03-3242-6276

www.sans.org

NRIセキュアテクノロジーズ

info@sans-japan.jp | 050-3177-4699

www.sans-japan.jp

Twitter.com/SANS_JAPAN

www.facebook.com/sans.apac

www.linkedin.com/company/sans-apac