SANS | GIAC CERTIFICATIONS

Cyber Mission Force (CMF)向けのシニアレベルのオペレーター職向けプログラム

SANSの8つのコースで構成されるプログラム

この資料では、シニアレベルのCMFオペレーターを対象としたSANSの8つのコースで構成されるプログラムを紹介します。本プログラムは、GIAC認定資格に準拠した6か月間のミッション対応型トレーニングで構成されており、サイバー専門家が攻撃戦術、インシデント対応、攻撃者エミュレーションに重点を置いた高度な役職に備え、必要なスキルを習得できるよう設計されています。

Cyber Mission Force (CMF)のシニアレベルのオペレーター職向けプログラム

SANSの8つのコースで構成されるプログラム

CMFオペレーターは、米国軍隊のサイバー作戦枠組みにおいて専門的で任務上重要な役割を担っており、通常は米国サイバーコマンド（USCYBERCOM）の下で活動しています。

Cyber Protection Teamsサイバー保護チーム（CPT）、Cyber National Mission Team（NMT）、またはCyber Combat Mission Teams（CMT）において、技術専門家、リーダー、ミッションプランナーとして活躍するこれらの専門家は、攻撃的または防御的なサイバー作戦の計画と実行を担当しています。

CMFオペレーター候補者は、6ヶ月間にわたり8つのコースを受講し、各コース終了後2週間かけて関連するGIAC認定試験の準備を行います。

- **SEC560:** Enterprise Penetration Testing™ (GPEN)
- **SEC580:** Metasploit for Enterprise Penetration Testing™
- **SEC542:** Web App Penetration Testing and Ethical Hacking™ (GWAPT)
- **SEC565:** Red Team Operations and Adversary Emulation™ (GRTP)
- **FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics™ (GCFA)
- **SEC599:** Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™ (GDAT)
- **SEC660:** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ (GXPN)
- **SEC699:** Advanced Purple Teaming – Adversary Emulation & Detection Engineering™

Stephen Sims Curriculum Lead, SANS Offensive Operations

SEC560: Enterprise Penetration Testing™ (GPEN)

ネットワークペネトレーションテストとエシカルハッキングを実施するための高度な手法を解説し、現実の環境における脆弱性の発見と悪用に関する実践的なテクニックを紹介します。

SEC580: Metasploit for Enterprise Penetration Testing™

エンタープライズ環境のペネトレーションテストにおける自動化とカスタマイズに焦点を当て、Metasploitの機能を活用する手法を解説します。特にスクリプト作成やエクスプロイト後の侵入、偵察や横展開に重点を置いています。

SEC542: Web App Penetration Testing and Ethical Hacking™ (GWAPT)

技術者が最新のツールと技術を活用し、一般的なウェブアプリケーションの脆弱性を特定し、攻撃するためのスキルを習得します。
攻撃者のツールと手法、およびウェブアプリケーションのペネトレーションテストにおけるベストプラクティスについて紹介します。

SEC565: Red Team Operations and Adversary Emulation™ (GRTP)

レッドチームキャンペーンの計画と実行に関する専門知識を習得し、現実の攻撃者を模倣したサイバー
スレットインテリジェンス、レッドチームの技術、およびエンゲージメント計画を習得します。

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics™ (GCFA)

高度な脅威の検出、インシデントレスポンス、フォレンジックに関する詳細なトレーニングを提供し、様々な環境における実践的なフォレンジック分析とスレットハンティングを紹介します。

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™ (GDAT)

このコースでは、MITRE ATT&CKやCyber Kill Chainなどの業界のスタンダードなフレームワークを活用し、現実の攻撃分析、攻撃者のエミュレーション、防御戦略の実装を組み合わせた内容となっています。

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ (GXPN)

30以上の実践的なラボを通じて、高度な攻撃手法をシミュレートし、重要なビジネスリスクを特定し、実証する、影響力の大きい攻撃ベクトルに関する深い専門知識の習得を目的としたコースになっています。

SEC699: Advanced Purple Teaming – Adversary Emulation & Detection Engineering™

SANS の高度なパープル チーム サービス。データ侵害の防止と検出のための敵対者エミュレーションに重点を置いています。

www.sans.org

Japan@sans.org

「これまでのところ、素晴らしい経験です。方法論や目標を念頭に置いて資料を順を追って学ぶことで、情報がどのように役立つか、現実の世界での応用可能性について、より広い視点を得ることができます。」

—Venus G., アメリカ空軍 (USAF)

「これらのコースは、私がインシデント対応を任された際に、どこから手をつけていいか、異常をどのように特定するかを学ぶのに役立ちました。また、処理しなければならない膨大なデータに圧倒されないようにする方法も教えてくれました。」

—Sharwin S., 情報通信メディア開発庁 (IMDA)

SANS | GIAC CERTIFICATIONS