CYRIN®（サイリン）

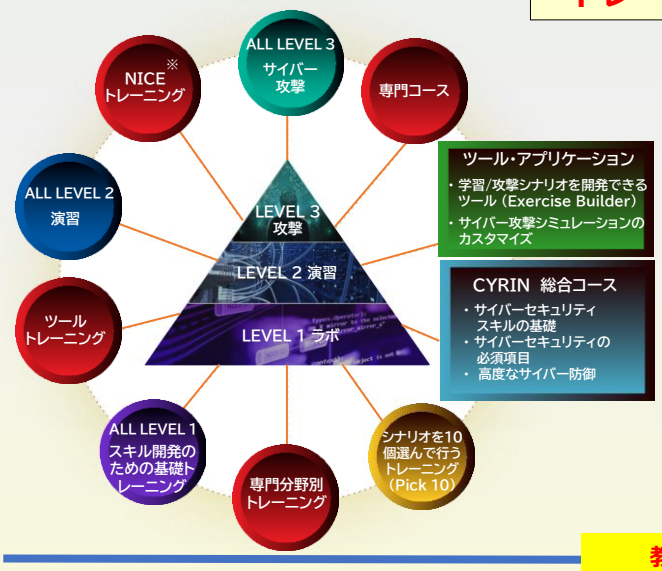
ハンズオン形式で「日本語でも英語でも」初歩から学べる グローバルな次世代のオンラインサイバーセキュリティ教育システム！

「国境のないサイバー脅威」対策と人材育成には、
既に世界の先進国で実績を有する「教材」を用いた教育が必須です!

主な特長

- Cloud（Azure）ベースにより、PCとインターネット環境さえあれば、**いつでもどこでも**受講可能（オンプレモデルも有り）。
- CYRIN®は他の教材とは異なり、2009年に**アメリカ連邦政府のプロジェクト向けに開発されて以来、**米軍を始め、政府機関、大学、更には英国の教育市場で80％のシェアを占める大手教育機関など既に世界で多くの導入実績をベースに教材を開発。
- SSCP（Systems Security Certified Practitioner）やCISSP（Certified Information Systems Security Professional）の資格維持に必要なCPE（Continuing Professional Educations）クレジットが取得可能。
- NIST（アメリカ国立標準技術研究所）が策定したNICE（National Initiative for Cybersecurity Education）フレームワークをベースとしたパッケージプラン。
- IT/OT（Operational Technology: 発電所や工場などの制御システム）、両分野のサイバーセキュリティ技術者を教育。
- 新しいシナリオは、自社又は**米国の大学等と協力して定期的にアップデート。**
- インストラクターが各受講者やグループの学習進捗及び評価をリアルタイムに行える**学習パフォーマンス管理機能。**
  ※シナリオ演習結果（演習回数、所要時間、成績等）や、それらを表示する"リーダーボード"によりグループ及び個人評価。（受講者は自身の学習進捗・評価のみ閲覧可）
- 演習シナリオの変更や独自開発は、**「エクササイズ・ビルダー」（オプション機能）により**自由に。

トレーニング体系



※大半のCYRINコースを修了するのに要する時間は、**平均で2時間以内です**。

※受講者は、**レベル1のスキル開発ラボから始めてサイバー演習レベルに進んでから、最後にインシデント攻撃シナリオに進むことが推奨されます。**

（これは、上級レベルのCYRINコースの多くは「予備知識」を必要とするためです。スキル開発ラボには詳細な指示が含まれていますが、**受講者が上級レベルの演習及や攻撃を履修するにつれて、指示及びヒントが少なくなります。**）

※NICEトレーニング
NIST（アメリカ国立標準技術研究所）が策定したNICE（National Initiative for Cybersecurity Education）フレームワークをベースとしたパッケージプランです。

教材例

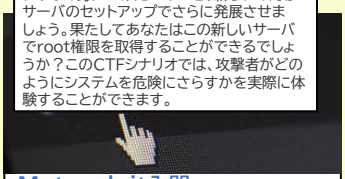
DoS攻撃と防御
本シナリオでは、3種類のDoS（サービス拒否）攻撃と、それを軽減するためのテクニックを学びます。

キャプチャー・ザ・フラッグ シナリオ2
最初のCTF（キャプチャー・ザ・フラッグ）シナリオで身につけたスキルを、新しいWebサーバのセットアップでさらに発展させましょう。果たしてあなたはこの新しいサーバでroot権限を取得することができるでしょうか？このCTFシナリオでは、攻撃者がどのようにシステムを危険にさらすかを実際に体験することができます。

未知のネットワーク上で稼働しているマシンやサービスを識別
受講者は、nmap、unicornscan、fping などのツールを使用して、Unix と Windows の両方のターゲットを含むローカルネットワーク上のシステムを識別します。また、これらのシステムが実行しているオペレーティングシステムと、それらが提供しているネットワークサービスの種類を識別します。

Splunkを使用したログ分析
本シナリオでは、Splunk Enterprise のセキュリティ情報収集および分析プラットフォームを設定し、安全に実行する方法を学習します。本シナリオの目的は、デプロイメントサーバを介して複数の Splunk データフォワーダのインスタンスを展開し、サーバから受信したログを分析することです。

Active Directoryを使用したドメインユーザアカウントの管理
受講者は、Windows Active Directoryサービスを使用して、ドメインユーザアカウントを作成・管理する方法を学習します。また、セキュリティポリシーを設定し、そのセキュリティポリシーをユーザやorganizational units（OU：組織単位）に割り当てることを学習します。



Metasploit入門
受講者は、広く使われているオープンソースのMetasploit®フレームワークと、脆弱なソフトウェアや安全でないシステム設定をエクスプロイト（脆弱性に対する攻撃）するための関連ツールの使用経験を積むことができます。本演習では、ネットワークのスキャンからリモートシェルの取得、機密情報へのアクセスに至るまで、すべてのプロセスを学習します。

Elastic Stackを使用したログ分析
Elastic Stackは、あらゆる種類のソースから、あらゆる種類のフォーマットでデータを取得し、そのデータをリアルタイムで検索、分析、可視化するために設計されたサービス群です。

OWASP-ZAPを使用したWebアプリケーションのセキュリティ分析
OWASPプログラムのZAPツール群をKali Linuxから使用し、複数のWebサービスをスキャンして脆弱性を検証します。受講者は、潜在的な攻撃者がデータベースのテーブル全体を利用できる脆弱性を持つWebサイトで、ZAPの動作を確認することができます。

国内実績
既に防衛大学校、陸上自衛隊システム通信・サイバー学校、テレコムキャリア、大手メーカー、国立大学、CATV事業者等、多数導入実績がございます！

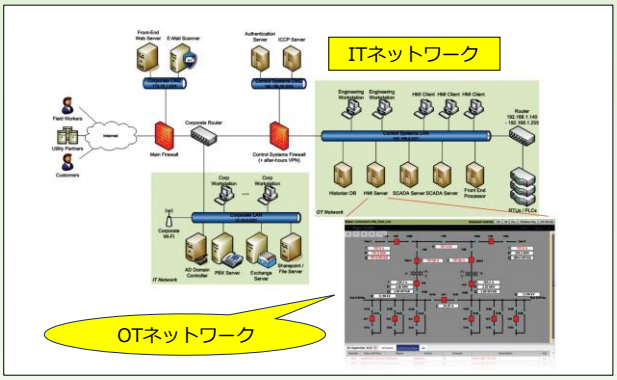
日本総代理店
コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

トレーニングレベル

cyrin

CYRIN®には、受講者が上達するにつれて難易度を上げるように設計された**3つの異なるトレーニングレベルがあります。**
※標準メニューはレベル1のみ、レベル1～2、もしくはレベル1～3です。

- **レベル1（全ての教育ラボ）**
  最新シナリオの「暗号技術の基礎」を含む**52のスキル開発ラボ**を提供します。これらの多くは、ネットワーク管理と防御で一般的に使用されるツールに関するトレーニングになります。
- **レベル2（レベル1＋個人及びチーム演習）**
  レッドチーム（攻撃側）/ブルーチーム（防御側）の演習、CTF（キャプチャー・ザ・フラッグ）や個人及びチームでの演習に使われる8つのシナリオが用意されています。
- **レベル3（レベル2＋攻撃シナリオ）**
  ITネットワークや**OT（産業用制御システム/SCADA）に対する7個の攻撃シナリオ（ICS/OTアプリケーションレベルDoS攻撃やMITM（Man-In-The-Middle攻撃など）**が提供されます。



※お薦めプランはCYRINラボ、演習、又は攻撃シナリオをレベル1～3の中から最大10個選択できる「Pick 10プログラム」です。
（御客様の希望する学習目的を伺った上で、推奨シナリオをご提案させて頂きます。
レベル3は最大1つまで選択可）

シナリオの御紹介

Level 1（No. 1～52）

IT及びDevOps

1. CYRIN入門
2. シェルスクリプトの入門
3. MariaDBとMySQLの入門
4. Jenkins CI/CD パイプラインの入門
5. Active Directoryのインストールと設定
6. Docker、Docker Compose、およびDocker Networkingの入門
7. WindowsとLinuxのコマンドラインの調査
8. システム管理者のためのWindowsオペレーティングシステムの基礎
9. システム管理者のためのLinuxオペレーティングシステムの基礎

サイバーフォレンジック

10. ファイルシステムフォレンジックの入門
11. GRRを使用したライブフォレンジック
12. Windowsフォレンジックアーティファクト
13. Volatilityを使用したメモリ分析の入門
14. Rekallを使用したメモリ分析の入門
15. P2P フォレンジックの入門
16. 高度なP2Pフォレンジック
17. eMule P2Pフォレンジック

インシデントレスポンス

18. DoS攻撃と防御
19. プロトコル分析1：Wiresharkの基本
20. プロトコル分析2：ネットワークトラフィックからのデータ抽出
21. 潜在的なマルウェアの分析

ネットワーク監視及び偵察

22. 未知のネットワーク上で稼働しているデバイスやサービスを識別
23. サービス識別 1
24. サービス識別 2
25. RSYSLOGを使用したログ分析
26. Splunkを使用したログ分析
27. Elastic Stackを使用したログ分析

セキュアなWebアプリケーションの設定

28. Apache Webサーバの安全な設定
29. Apacheにおける安全なSSL設定
30. LAMPスタックのデプロイ

セキュアなネットワーク・システムの設定

31. pfSenseを使用したファイアウォールの設定
32. OpenVPNを使用したVPNサーバの設定
33. BINDを使用したスプリット ホライズン DNS設定
34. IPtablesを使用したファイアウォールの設定
35. Snortを使用した不正侵入検知システム（IDS）設定の入門
36. VyOSを使用したファイアウォールの設定
37. Zeek（旧Bro）を使用した不正侵入検知
38. SSHサーバの設定
39. Active Directoryを使用したドメインユーザアカウントの管理
40. OSSECを使用したホスト型IDSのセットアップ

脆弱性スキャン

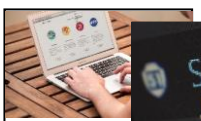
41. Metasploit入門
42. OpenVASを使用した脆弱性スキャン
43. SPARTAによるセキュリティ分析の自動化

Webアプリケーションのセキュリティ分析

44. SQLインジェクションの脆弱性の検出と悪用
45. Burp Suiteを使用したWebアプリケーションのセキュリティ分析
46. Vegaを使用したWebアプリケーションのセキュリティ分析
47. Niktoを使用したWebアプリケーションのセキュリティ分析
48. OWASP-ZAPを使用したWebアプリケーションのセキュリティ分析
49. Webサイトの偵察

基盤技術

50. 暗号技術の基礎
51. バッファオーバーフロー攻撃と防御
52. ニューラルネットワークを使用した人工知能および機械学習入門



Webサイト偵察
Webサイト偵察とは、に関する情報を収集すす。もちろん、Webサに見せることを前提と情報があります。そしてイトで使われているソの名前やバージョン、Webアプリケーションているデータベースに報などがあります。こ

SQLインジェクションの脆弱性の検出と悪用
受講者は、SQLインジェクション脆弱性を検出し、悪用する方法を学びます。いくつかのSQLインジェクションのテクニックを使って、サーバのオペレーティングシステム、データベースの種類、テーブル名、そして最も重要な

Niktoを使用したWebアプリケーションのセキュリティ分析
受講者は、Niktoツールを使用して、ネットワーク上のWebサービスをテストし、脆弱性を文書化します。受講者は、Wiresharkなどのネットワークパケットキャプチャツールを使用して、脆弱性とテスト手順の

Level 2（No. 53～60）

攻撃、防御及びシステム管理

53. キャプチャー・ザ・フラッグ シナリオ1
54. キャプチャー・ザ・フラッグ シナリオ2
55. データ漏洩調査の実施
56. パケットキャプチャの分析と操作
57. ネットワークトラフィックを使用した侵入分析
58. 悪意のあるネットワークトラフィックの高度な分析
59. レッドチーム vs ブルーチーム
60. エンタープライズネットワークの設定

レッドチーム vs ブルーチーム
システムを攻撃しようとする攻撃者、または攻撃者による被害を防ごうとする防御者として、他の人と対戦してスキルをテストします。

ネットワークトラフィックを使用した侵入分析
実際に侵入されたパケットキャプチャを検証し、攻撃者の手口を深く理解しましょう！
Wireshark®でネットワークトラ

Level 3（No. 61～67）

攻撃シナリオ（IT&OT）

61. マルウェアベース攻撃の検出・無力化
62. ICS OT 中間者攻撃（マンインザミドル攻撃）
63. ICS IT/OT フィッシング攻撃
64. ICS OT アプリケーションレベルのDoS攻撃
65. ICS OT ネットワークレベルのDoS攻撃
66. 企業サービスに対する攻撃の調査、分析、軽減
67. HVAC SCADAシステムへの攻撃の検知と無力化

ICS OT ネットワークレベルのDoS攻撃
サービス妨害（DoS）攻撃は、企業の業務を妨害し、物理的なインフラをさらに悪化させる可能性があります。本シナリオは、まさにOTネットワークへの攻撃、つまりネットワーク層へのDoS攻撃によって、

ICS OT 中間者攻撃（マンインザミドル攻撃）
オペレーショナルテクノロジー（OT: Operational Technology）ネットワーク上のデバイスが、工場から自社に届くまでの間に侵入された場合、あなたはそれを知ることができますか？あるいは、請負

独自のシナリオやトレーニングコンテンツの開発に！ "Exercise Builder"（オプション）

"Exercise Builder"は受講者やインストラクターに下記の機能を提供します。

- 24時間365日いつでも自由に学習コンテンツの変更やカスタマイズ
- 学習や演習の目的やニーズに合った独自シナリオの新規開発
- 所属組織の要件に合わせたトレーニング内容の作成・カスタマイズ

無償トライアルのご案内

御興味のある方は是非、「CYRIN入門」「OWASP-ZAPを使用したWebアプリケーションのセキュリティ分析」の無償トライアル（30日間）をお試し下さい！（PCさえあれば時間と場所は問いません）

詳細は、https://www.cornet-solutions.co.jp/cyrin_contact/までお問い合わせ下さい。

日本総代理店
コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp