次世代「オンライン/e-ラーニング」サイバーセキュリティ教材「CYRIN(サイリン)」のご案内

ランサムウェアやエモテット、フィッシング詐欺攻撃などサイバー脅威による被害が、業種や組織規模問わず急増しており、機密情報の流出など大きな損失を被っています。これらの被害を防ぐためにもサイバーセキュリティについて、グローバルで且つ常に新しい知識を持つ「セキュリティ技術者」を育てることが必要不可欠です！

今回ご紹介させて頂く「CYRIN」は Architecture Technology Corporation 社(ATCorp，米国ミネアポリス)が米国連邦政府や米軍向けに開発した次世代の「オンライン/e ラーニングサイバーセキュリテイ教育・トレーニングツール」で、北米やヨーロッパの先進国をはじめ、国内では既に国立大学、テレコムキャリア、大手メーカー、陸上自衛隊、CATV 事業者など、多数の実績があり、無償トライアルを御試しになる御客様が増えております！

CYRIN の主な特長

1） 北米や先進国の教育機関や企業で認められた、他に類のない「グローバルなサイバーセキュリティ人材育成教材」です！

「ハッカーやサイバー脅威には国境がありません！」 これからのセキュリティ教材は、国内実績のみでは不十分で世界の主要国で鍛え上げられたグローバルな利用実績が必要です。

2） 従来の教材とは異なり、IT/OT の両分野を含めた世界の最新ニーズを取り込んだ「演習シナリオ」を日本語、又は英語でいつ何処からでも学習できます！(業界初！)

国境のないサイバー脅威に立ち向かうためには、当然英語力のレベルアップも必要です。

「CYRIN」は、学習中でも、即日本語又は英語に切り替えることができます。学習者は必要に応じてそれを繰り返すことでセキュリティ専門用語(英語)の理解や習得も同時に可能になりますので、学習シナリオのレベルが上がるにつれて、自然に先端企業や世界で通用するグローバルなサイバーセキュリティ技術者に育っていきます。

3） 学習者のパフォーマンス(成績)管理がリモートから可能です！

学習者個人、及び教官用のダッシュボードを用いて個人やチーム(クラス)のパフォーマンス(成績)管理がリモートから可能です。

4） シナリオの独自開発が可能です！

「エクササイズ・ビルダー」(オプション)により、学校及び組織の目的やテーマに合わせた独自の演習シナリオ開発が可能です。

※無償トライアルや教育機関向け特別アカデミック割引プラン(一般価格の 30～40%OFF)もございます。

是非一度，御電話(下記)又は Email(sales@cornet-solutions.co.jp) にて御問い合わせ下さいませ。

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

CYRIN®（サイリン）
“オンライン・サイバーセキュリティ教育ツール”

「日本語と英語」での学習が可能です！

「国境のないサイバー脅威」対策には、
既に世界の先進国に実績を有する「教材」を用いた教育が必要です!

米軍やアメリカ連邦政府向けに開発された「CYRIN®」は業界で初めて「日本語と英語」での学習を可能にした
「ハンズオン形式で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」です!

特長（I）

● **既に米軍や世界の先進国で実績を有するグローバルな教材で学習可能！**

CYRIN®は他の教材とは異なり、2009年に**米軍やアメリカ連邦政府向けに開発**されて以来、**既に先進国や海外の教育機関に数多くの実績を有し、グローバルな教材として実証済み。「国内外のサイバー脅威」対策には最適です！**

● **次世代のグローバルな教材を日本語と英語で学習できるハイブリッドな教材！**

CYRIN®は日本語又は英語で学習できる国内初のハイブリッドな**「オンライン/ e-ラーニング教材」**です。
(※いつでもボタン一つで「日本語⇔英語」の切り替えができるので、グローバルなサイバーセキュリティ技術の習得過程にに必要な「英語による表現力」も同時に向上していきます)。

● **実践的ハンズオントレーニング！**

・CYRIN®では実際に手を動かして学習や演習を行うことで技術力を高められます。**Redチーム(攻撃側)とBlueチーム(防御側)の対抗戦や、Webプロキシの設定、アクティブスキャン、サーバーの脆弱性発見など、実践的な経験を積むことができます。**
CYRINの「eラーニング」の中核は、個人的に実施されるかチームの一員として実施されるかに関わらずハンズオンラボ演習に基づいており、教育者、情報セキュリティ管理者及び受講者に多くのメリットを提供します。

・受講者がラボを修了しているか完全コースを修了しているかに関わらず、全てのCYRIN学習は一時停止することができ、受講者が停止した箇所をプラットフォームが記憶しているので、受講者は都合の良いときに続行することができます。

特長（II）

●**米軍や(ISC)²**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に既に世界で多くの導入実績をベースに教材を開発。
●**CISSP（Certified Information Systems Security Professional）**の資格維持に必要な**CPE（Continuing Professional Educations）クレジット**を取得。
●**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。
●学習内容や演習シナリオの変更や開発が自由に行える**「エクササイズ・ビルダー」。**
●各受講者やグループの学習進捗や評価が行える**パフォーマンス管理機能。**
●**IT/OT（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。**
●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。

“CYRIN”はBusiness Intelligence Group（米国）が運営するFortress Cybersecurity AwardのTraining部門（2022）で受賞しました！

“Fortress Cybersecurity Award”
Business Intelligence Group（米国）によって2018年に新設された
Cyber Security Awardsプログラムです。
急増するサイバー脅威に対して、データや電子資産を安全に保つために
取り組む、世界をリードする企業に賞が与えられます。

受講認定証

国内導入実績

既にテレコムキャリア、大手メーカー、陸上自衛隊、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

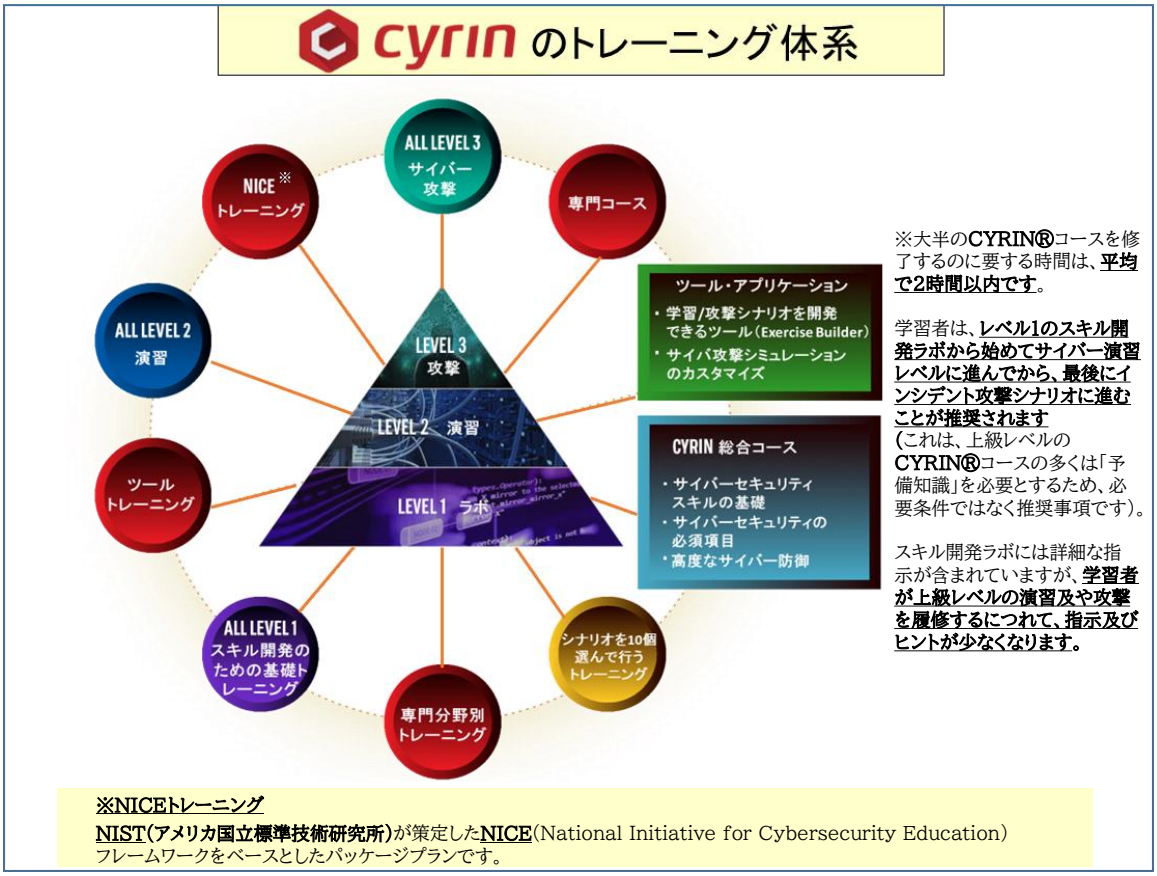
CYRIN®プラットフォーム

CYRIN®は、実際のツール、現実の攻撃やシナリオを特徴とする次世代サイバーレンジプラットフォームです。
受講者、管理者及び教育者が現実的な実践シナリオにおいて使用できるハンズオントレーニング及び経験を提供します。

CYRIN®は、サイバーセキュリティについて学習し始めの受講者から、新しい方法で自分を試したいと思っている経験豊富なサイバー防衛専門家まで、日本国内だけではなく世界中の受講者をトレーニングするために使用されています。

CYRIN®は、受講者がどのように学習し、それをどのようにモニターすべきかについて15年を超える研究開発を行ってきた他に類のないグローバルな教材です。
Microsoft Azureクラウドにおいて動作し、仮想マシン及びインテリジェントエージェント技術を使用します。
CYRIN®が提供する「オンライントレーニング（e-ラーニング）」は、個人的に実施されるかチームの一員として実施されるかに関わらずハンズオンラボ演習に基づいています。CYRIN®プラットフォームは、教育者、情報セキュリティ管理者及び受講者に多数のメリットを提供します。

- 各受講者又はチームイベントは、サイバーレンジの各自の個人インスタンスを取得し、各自のスケジュールで演習にアクセスできます。
  演習は一時停止することができ、後で再開するために状態が完全保存されます。
- 全てのアクセスは標準ウェブブラウザを経由するので、特別なソフトウェアは不要です。
- 受講者は、仮想環境内の自身のアクションに基づいた、進捗のリアルタイム評価を確認できます。
- 状況に依存した指示やヒントは受講者を導き、行き詰っている可能性がある受講者を助けます。
- 「**パフォーマンス管理ツール**」により、指導者及びセキュリティ管理者は、個々の受講者の学習状況、受講者群におけるメトリックを確認できます。
  これらのメトリックは、受講者が苦労している箇所又は更なる練習が必要とされる箇所に指導者及び管理者を導くのに役立ちます。
- チームベースのシナリオにより、受講者は指導者によって設定された課題において協力したり、直接対決することができます。
- **CYRIN®**のLMS(Learning Management System)
  学習管理システムは、オープン標準に基づいており、LTI(Learning Tool Interoperability：学習ツールの相互運用性)を使用して既存のLMSシステムと統合できます。



※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**。

学習者は、**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、必要条件ではなく推奨事項です）。

スキル開発ラボには詳細な指示が含まれていますが、**学習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。

シナリオやトレーニングコンテンツの開発に！
"Exercise Builder"

CYRIN®上で各自のコンテンツを「**オーサリング(Authoring)**」したい受講者が利用できるCYRINソフトウェアモジュールです（オプション）。
24時間365日ブラウザベースのクラウドアクセスが可能なため各自のトレーニングコンテンツをCYRINプラットフォームにポートすることができ，既存のCYRIN学習コンテンツを変更して、組織の特定の要件及び独自の要件に合わせてトレーニングをカスタマイズすることができます。

受講者は、各自の運用ネットワークをミラーリングするCYRIN上で各自の攻撃シミュレーションを作成し、CYRIN上で実行されているミラーリングされたネットワークトポロジーに対して攻撃シミュレーションを実行することもできます。更に、各自のラボ、演習及びインシデント攻撃シナリオをゼロから作成することも可能です。

Exercise Builderは、特許を取得したドラッグアンドドロップ方法を使用して、事前構成された又はカスタマイズ可能な仮想マシンを有するカスタムネットワークを構築します。
又、インテリジェントエージェント技術を使用して、それぞれのコースの修了のあらゆる段階で受講者の進捗をモニターします。

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

トレーニングレベル

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
4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までです。

- **レベル1（全ての教育ラボ）**
  最新シナリオの「Docker、Docker Compose、およびDocker Networkingの入門」を含む48のスキル開発ラボを提供しています。
  これらのラボの多くは、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を提供しています。
- **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ネットワークおよびOT（ICS：Industrial Control System（産業用制御システム/SCADA））に対する5個の攻撃シナリオ（ICS/OTアプリケーションレベルのDoS攻撃や中間者攻撃（マンインザミドル攻撃など））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いただきます。）

（御参考）レベル4（レベル1～3の演習を利用した総合コース）
CYRIN®のレベル4は、修了するのに平均で40時間かかる総合サイバーセキュリティトレーニングコースを提供しています。
これらの詳細なコースは、全米で認められたサイバーセキュリティトレーナーであるケヴィン・カードウェル(Kevin Cardwell)氏が主催しています。
※本コースも「オンライン」形式で行われますが、**現在は英語版のみ可能です。**

シナリオのご紹介

Level 1（No. 1～48）

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. LAMPスタックのデプロイ
6. Active Directoryのインストールと設定
7. Docker、Docker Compose、および Docker Networkingの入門
8. WindowsとLinuxのコマンドラインの調査
9. 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

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

セキュアなネットワークのセットアップ

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

脆弱性スキャン

40. Metasploit入門
41. OpenVASを使用した脆弱性スキャン
42. SPARTAによるセキュリティ分析の自動化
43. SQLインジェクションの脆弱性の検出と悪用
44. 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
45. Vegaを使用したWebアプリケーションのセキュリティ分析
46. Niktoを使用したWebアプリケーションのセキュリティ分析
47. 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
48. Webサイトの偵察

Level 2（No. 49～56）

攻撃、防御及びシステム管理

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

Level 3（No. 57～61）

攻撃シナリオ（IT＆OT）

57. マルウェアベース攻撃の検出・無力化
58. ICS OT 中間者攻撃（マンインザミドル攻撃）
59. ICS IT/OT フィッシング攻撃
60. ICS OT アプリケーションレベルのDoS攻撃
61. ICS OT ネットワークレベルのDoS攻撃

＊ICS: Industrial Control System（産業用制御システム/SCADA）

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）

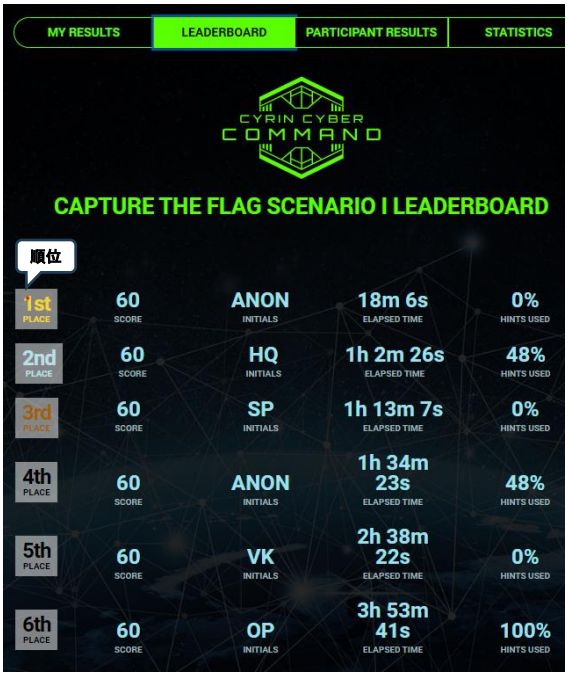
詳細は、https://www.cornet-solutions.co.jp/cyrin_contact/までお問い合わせ下さい。

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

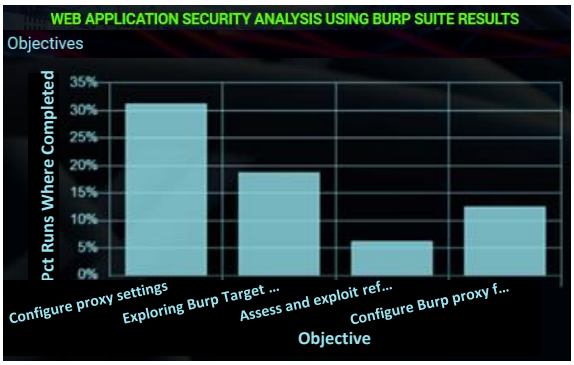
●リーダー(Leader)ボード(インストラクタ用ダッシュボード)表示例

・**CYRIN®**は、指導者及びトレーニング管理者がそれぞれの受講者の進捗を「リアルタイム」で見ることができる、このパワフルな受講者評価モジュールを提供します。Performance Managerにより、指導者及び管理者はラボ、演習、攻撃又はコースが修了した後に受講者のパフォーマンスを測定することもできます。

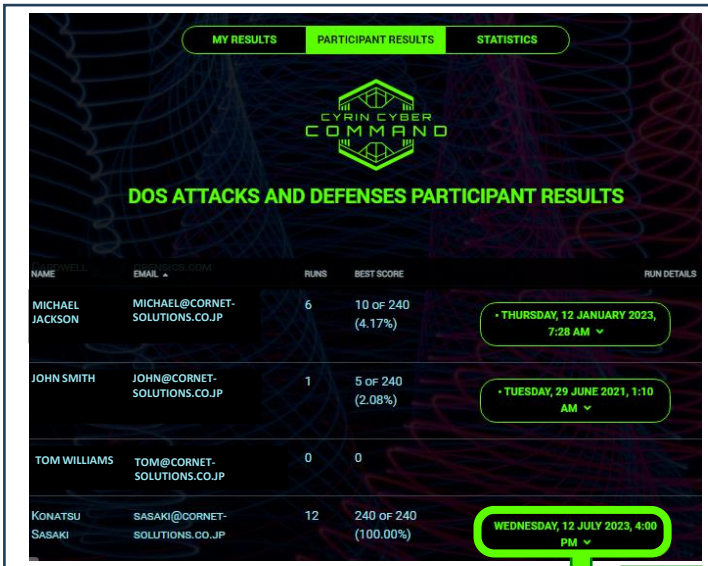
・CYRIN®は、**50を超える**スキル開発用の対話型/没入型ラボ、個人演習及びチーム演習、並びにインシデント攻撃シナリオを受講者に提供します。
通常、ラボは個々の受講者によって修了します。演習は個人又は個々の受講者のチームによって修了することができ、攻撃シナリオは個人、又はグループで修了することができます。



SCORE: 受講者がシナリオ内で獲得した得点を示します。
INITIALS:受講者のイニシャルを示します。匿名(ANON)にすることも可能です。
ELAPSED TIME: シナリオを終了するまでに要した時間を表示します。
HINTS USED: シナリオ内にあるヒントを使用した割合を示します。
*本画面についてはキャプチャーザ・フラッグ等、点数を競うシナリオにおいて採用されています。
ヒント(HINTS) については、Level 2以降のシナリオにおいて、表示されます。

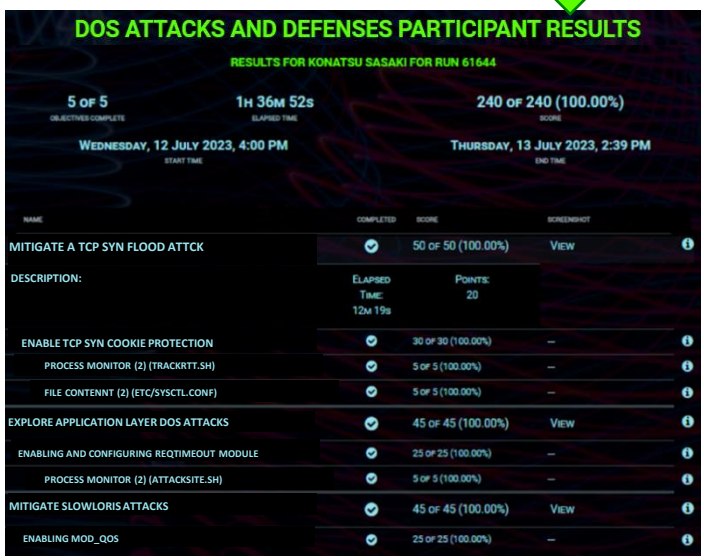


Pct Runs Where completed:
シナリオ内にある各目標に対して、受講者がどの位の割合(%)で完了したかを示します。
Objective:
シナリオに設定されている各目標の名前が記載されています。
*本画面については全シナリオで使用できます。



NAME: 受講者の名前です。
EMAIL: 受講者のメールアドレスです。
RUNS: シナリオを何回実行したかを示します。
BEST SCORE: シナリオを複数回実行した場合、そのベストスコアが表示されます。(実行が1回のみの場合は、そのスコア)
RUN DETAILS: 各実行の結果を確認することができます。
*本画面については全シナリオで使用できます。

クリックすると、シナリオの実行結果の詳細をみることができます。



NAME: シナリオに設定されている各目標の名前が記載されています。
COMPLETED: 各目標が完了しているかを確認することができます。
(チェックが入っていれば、完了です。)
SCORE: 各目標で獲得した得点が記載されています。
SCREENSHOT: 各目標で使用されている仮想マシンの画面(スクリーンショット)を確認することができます。
*本画面については全シナリオで使用できます。

●Architecture Technology Corporation(ATC)について

Architecture Technology Corporation (ATCorp、米国ミネアポリス) は、Sperry UnivacやHoneywellなどの業界をリードする企業のメンバーによって1981年に設立されました。以来、分散コンピューティング、次世代ネットワーキング、情報保証、情報管理、インテリジェントシステム、データモデリング、機械学習に関する研究開発を行っています。

2009年に米軍や米国連邦政府向けにCYRIN®を開発し、いつでもどこでもオンラインのサイバーセキュリティ トレーニングを可能にしました。現在、このクラウドベースのプラットフォームには、50を超えるセルフペースのスキル開発トレーニングラボ、個人およびチームベースの演習、サイバーセキュリティインシデント攻撃シナリオがあります。
ATCorpは、米国および海外の大学や教育機関、先進国の企業など、多数の顧客と受講者をトレーニングしてきました。開発以来13年にわたり、既に15,000人を超えるユーザーがCYRIN®で約100,000回の実習を完了しています。

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

英国で初めてQA社がチームベースのサイバーレンジ“CYRIN”を提供！

Architecture Technology Corporation (ATCorp)が、英国の「QA社(https://www.qa.com/)」との戦略的企業提携に合意！

*(CYRIN*は、受講者が協力してサイバー脅威を克服することを必要とするチームベースのインシデント攻撃シナリオを使用してサイバー防衛スキルを磨く、次世代サイバーレンジです)

QA社は、英国のトレーニング市場の80%以上を占める英国最大のコマーシャルトレーニング会社です。この提携により、ATCorpは英国における貴重な販売パートナーを獲得することになり、QA社のサイバーセキュリティトレーニングポートフォリオに大きな貢献をするでしょう。

QA社は、CYRIN の導入により、同社のサイバーセキュリティポートフォリオを拡大しました。

QA社のサイバーセキュリティトレーニングポートフォリオに追加された最新の製品により、セキュリティ運用チームは、攻撃ベースのシナリオに基づいたスキル開発と自社内のサイバートレーニング資料を組み合わせて、大規模に、共に学習及び実践することが可能になります。

QA社と米国を拠点とするメーカーArchitecture Technology Corporation (ATCorp)の提携により、QA社はCYRINを提供する英国初のトレーニングプロバイダになります!

QA社のサイバーセキュリティ担当ディレクター のリチャード・ベック(Richard Beck)氏は、

「サイバー攻撃の現実は、脅威が検出された瞬間からセキュリティ運用チームが効果的に協力することを必要とするものです。各個人が一緒に実践したことがなければ、彼らが深刻なサイバー攻撃に直面した際に効果的に協力することは不可能です」と説明しています。

更に、「CYRINサイバーレンジは、スキル開発ラボ、個人演習及びチーム演習を提供し、受講者がサイバーセキュリティインシデント攻撃の性質及び発生源、並びにその攻撃を軽減して無力化する方法を特定することを必要とします。このアプローチは、サイバーセキュリティスキルを磨き、常に協力しているわけではないグループがプレッシャーのかかる中で共同で問題解決を実践するのを支援するので、サイバー攻撃が発生した場合にチームが迅速に且つうまく対処することができるという安心感をビジネスリーダーに与えます。」と述べています。

- **独自のシナリオ開発を可能にする「Exercise Builder機能」**

受講者は、CYRIN独自の「Exercise Builder機能」を使用して、自社のトレーニング資料及び攻撃シミュレーションをトレーニングセッションに組み込むことができます。QAのカリキュラムスペシャリストは、自社内のカリキュラムチームと連携して、既存のトレーニング資料を最大限に活用するシナリオベースのチームトレーニング演習を作成します。自社内のコンテンツ及びツールをCYRINラボ、演習及びインシデント攻撃シナリオと組み合わせることができることにより、パワフルで且つ統合された仮想トレーニングプラットフォームを実現します。

- **受講者用「リアルタイム評価」機能や、指導者用「パフォーマンス管理ツール」**

CYRINを用いれば、スキル開発の追跡は簡単です。受講者は自分の進捗のリアルタイム評価を見ることができ、パフォーマンス管理ツールは個人の受講者レベルとチームレベルの両方で更なる実践が必要とされる箇所を指導者や管理者に示します。

ATCorpの技術サービスVP(Vice President) のロブ・ジョイス博士(Dr Rob Joyce)は、

「初期のLANテクノロジー並びに分散コンピュータ及びソフトウェアシステムの設計及び実装における業界で尊敬されるパイオニアとして、ATCorpがサイバーレンジプラットフォームを構築することは必然的なステップでした。これにより、現実的な仮想化されたコンピュータネットワークを用いて実践することができ 、政府及び大規模な組織が高度なスキルを持つ人間による防衛を高めることが可能になりました」と説明しています。

「CYRINは、高度なITネットワークに依存している大規模な組織、特に産業制御システムに依存している組織がロバストなサイバーセキュリティ対応を整備しているという確信を持てるように支援するための理想的な教育ツールです。このアプローチは、緊急時にのみ引っ張り出される従来のサイバープレイブックよりも効果的です。ATCorpは、QAとの今回の提携を発表し、CYRINを英国市場に導入することを嬉しく思います。」

- **QA社について(https://www.qa.com/about-qa/)**

QA社は、英国の技術系人材及びトレーニング組織の大手です。同社はテクノロジーにおける専門会社 であり、個人及び企業がデジタル革命の勝者になることを支援する人材及びトレーニングサービスの包括的なスイートを提供しています。

昨年は293,000人以上がQA社のプログラムで学習しました。同社は、FTSE 250の大部分を占める5,000社以上の企業クライアントにサービスを提供しています。QA社は、アジャイル、サイバーセキュリティ、クラウドコンピューティング及びDevOps並びに多くの他のテクノロジー専門分野における実践をリードしています。QAは、人を中心としたテクノロジートランスフォーメーションを専門としており、QA社のトレーニングプログラムは、企業が既存従業員のスキル向上又は再教育を行うのを支援します。

- **Architecture Technology Corporationについて**

ATCorpは、株式非公開のテクノロジー会社です。同社は、下記の定評のある効果的なハードウェア/ソフトウェアテクノロジー開発及びアプリケーションを通じて、39年以上にわたり下記分野にて証明されたソリューションを顧客に提供しています。

・サイバーセキュリティ ・パフォーマンスエンジニアリング ・ソフトウェアパフォーマンス改善 ・システムエンジニアリング ・戦術的ネットワーク

現在、CYRINサイバーレンジは、50以上のラボ(学習講座)、演習、及びサイバー攻撃シナリオを提供しています。ラボは、サイバーフォレンジック(Cyber Forensics)及びウェブアプリケーションセキュリティ解析(Web Application Security Analysis)を含む8つの専門カテゴリーで利用可能です。

※本資料はArchitecture Technology Corporation社が2021年に公開した英文資料に基づいて、弊社が作成した資料です。
英文と和文資料に差異がある場合には、英文資料が優先されます。

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

サイバー演習システムCYRINのススメ

今、サイバーセキュリティの脅威はかつてないほどに高まっています。現代の企業組織において、サイバーセキュリティ対策は、経営者、一般社員、そしてITシステム部門、すべての社員が一丸となって取り組むべき課題です。その中でも特に、サイバー攻撃への対処を最前線で実際に行う技術者は、セキュリティ対策に関する技術的知識を学ぶことが求められます。しかしながら、セキュリティ対策に関する技術的知識は、今や非常に広範で、学習も容易ではありません。

攻撃者は、一番弱いリンクを狙ってきます。防御側はすべてを満遍なく守る必要があります。CYRINは、現在のシステムに即した演習環境に基づいた広範なトピックスについて扱っており、技術者の弱い点を炙り出します。また、実践的なセキュリティ対策は知識だけでは不十分であることは多くの人が知るところです。CYRINは、実践的な演習課題を体験的に学ぶことができる演習システムです。

たとえ実践的な演習が重要であることを理解していても、CYRINと同様な演習環境を自力で作り上げることは、至難の技です。我々も自分達の研究グループにてサイバーレンジというセキュリティの演習システムを構築し、7年間にわたって理工学部の授業で利用しています。その経験からも、実践的演習によるセキュリティ技術の学習は効果が高いことを体験的に理解しており、CYRINのコンテンツの素晴らしさについて、自信を持って皆様にお薦めできます。

明治大学
サイバーセキュリティ研究所

明治大学サイバーセキュリティ研究所所長
明治大学理工学部教授
博士（工学）
齋藤孝道

明治大学サイバーセキュリティ研究所：「国内外のサイバーセキュリティに関する諸課題を解消すること」及び「そのための議論の場を創生すること」をミッションとして2020年創設。

【CYRINケーススタディ】

RIT | Global Cybersecurity Institute

RIT: Rochester Institute of Technology （ロチェスター工科大学） Global Cybersecurity Institute 152 Lomb Memorial Drive Rochester, New York 14623-5603

Kenさんへ（Architecture Technology Corporationの社長兼オーナーであるKenneth Thurber氏）

この文書は、ロチェスター工科大学のサイバーセキュリティ・ブートキャンプにおけるCYRIN**サイバーレンジテクノロジー**の使用について説明して欲しいというリクエストへお答えするものです。ロチェスター工科大学のブートキャンプに関する詳細は、https://www.rit.edu/news/rit-offers-cybersecurity-bootcamp-help-people-get-back-work-and-start-new-careersをご覧ください。
（※上記URLをクリックした際に「セキュリティ警告」が出る場合は、「許可」をクリックしてお進み下さい）

ロチェスター工科大学は利用できる様々な仮想サイバーレンジ技術やベンダーを検討した結果、ブートキャンプで使用する仮想サイバーレンジとしてCYRINを選択しました。CYRINは現在、受講者がアクセスできる約40のスキル開発ラボ、サイバーセキュリティ演習、及び多数の攻撃シナリオを持っています。攻撃シナリオはロチェスター工科大学にとって特に興味深いもので、ユーザは、産業用制御仮想ネットワーク（ICS）に対するサイバー攻撃を軽減し、ネットワークを攻撃前の状態に戻さなければならないという高度な攻撃ベクトルとなっています。

CYRINの学習階層の下位には、30以上の基本スキル開発ラボがあり、サイバーセキュリティの初心者（ブートキャンプ参加者）のトレーニングに最適です。これらのラボは約1時間で完了し、各ラボには十分なオンライン指示が組み込まれています。CYRINはまた、強力なパフォーマンス管理システムも提供しており、ロチェスター工科大学のインストラクターは個々の受講者の進捗状況を見たり、受講者全体の指標を分析したりすることができます。これにより、個々のブートキャンプの受講者や、ブートキャンプの参加者全員を見て、学習プロセスのどこに問題があるのかを把握することができます。

更に、CYRINには**「演習ビルダー機能」**があり、大学独自のラボ、演習、攻撃を「作成」することができます。ロチェスター工科大学はすでに、今後のプログラムに盛り込むため、独自のブートキャンプ用ラボの構築を進めています。CYRINシステムは、ロチェスター工科大学のグローバルサイバーセキュリティ研究所や様々な人材開発プログラムに貢献する重要な機能を備えています。

ロチェスター工科大学は、**Architecture Technology Corporation**とのパートナーシップに強く感謝しています。また、ロチェスター工科大学がCYRINをどのように実装しているかについて、具体的な追加情報が必要な場合は、ご遠慮なくお申し付けください。

Dr. Stephen Hoover (he/him/his)
Katherine Johnson Endowed Executive Director Global Cybersecurity Institute Rochester Institute of Technology

敬具

※本資料はArchitecture Technology Corporation社が公開している英文資料に基づいて、弊社が翻訳した資料です。
英文と和文資料に差異がある場合には、英文資料が優先されます。