【責任者向けプログラム】

サイバー危機対応机上演習（CyberCREST）ご案内資料

サイバークレスト

2022年10月

独立行政法人情報処理推進機構

産業サイバーセキュリティセンター

開催概要（1）

目まぐるしく変化する社会情勢の中で、
高度なサイバー脅威から制御システムを有する企業・団体を守る
ために必要なサイバーセキュリティ対策を学ぶ3日間

サイバー危機対応机上演習※1,2では、制御システムを有する企業・団体のサイバーセキュリティ責任者を対象に、組織を守る為に必要なスキルとメソッドをご紹介します。

近年、ウクライナ情勢に関連してサイバー脅威が高まっており、重要インフラ企業に対するサイバー攻撃が発生しています。国家や、国家の支援を受けた攻撃者など、潤沢なリソースを持つ脅威主体による攻撃が主流となっており、個々の企業だけでは自組織を守ることが難しくなっています。

本演習では、米国サイバー軍出身の専門家やCISO、セキュリティアーキテクトの専門家らが講師を担当します。各講師が自身の経験を共有するとともに、ロールプレイング演習を交えながら、複雑な脅威に対し、企業がどのような対策を行えばよいのかをご紹介します。

※1 サイバー危機対応机上演習(CyberCREST: Cyber Crisis RESponse Table top exercise)
※2 米国IronNet Cybersecurity社のナレッジ・ノウハウをベースに、産業サイバーセキュリティセンター提供プログラムとして、IronNet Cybersecurity社とIPAが日本における社会インフラ、産業基盤をもつ企業様向けにオーダーメイドで演習開発をしております。

開催概要(2)

対象者

- 制御システムを有する企業・団体のサイバーセキュリティ対策を統括されている責任者やサイバーセキュリティ対策部門の管理職

本演習で得られること

- 制御システムを有する企業に対して行われる攻撃デモやケーススタディを通して、攻撃者はどのように準備をし、攻撃を実行するのかを分析し、攻撃者は攻撃をどのように考えているのかが理解できます。
- サイバー軍出身の講師陣による、地政学的なサイバー脅威への対策を理解できます。
- コレクティブ・ディフェンスを理解し、どのようなアクションを取るべきかが分かります。
- 受講者の方々や海外セキュリティ専門家とのコミュニティやリレーションを構築できます。

開催概要(3)

日程/開催形態

日程:　2023年1月25日(水)～1月27日(金) 3日間

開催場所:　文京グリーンコートセンターオフィス13階
情報処理推進機構　会議室
※新型コロナウイルスの状況によりオンライン開催へ変更する可能性があります

定員

- 30名

受講料

- 30万円(税込)

言語サポート

- 本演習は英語ベースで行いますが、日本語テキスト、通訳の提供(日英)を予定しております。

コレクティブ・ディフェンス

コレクティブ・ディフェンスとは

- サイバー脅威は日々複雑性を増しており、個々の企業だけでは自組織を守ることが難しくなっています。国家や、国家の支援を受けた攻撃者など、潤沢なリソースを持つ脅威主体に対して、企業側が政府や同業他社と情報共有を図り、協働して立ち向かう戦略**「コレクティブ・ディフェンス」**が重要となっています。
- 米国サイバースペースソラリウム委員会（CSC: The Cyberspace Solarium Commission）における報告書※1では、これまでのサイバー脅威に対抗する戦略を再構築し、サイバー抑止力を高めるための方法として、コレクティブ・ディフェンスの必要性を説いています。

※1 The Cyberspace Solarium Commission (2020). “Cyberspace Solarium Commission Report”

本演習3つの特徴

特徴①

「米国の先進的なサイバーセキュリティ戦略“コレクティブ・ディフェンス”」

- Red Team(攻撃者側)とBlue Team(防御側)の視点で、攻撃手法や攻撃パターンについて学ぶとともに、これらのリスクを軽減させ、自社をどのように守っていくべきかを学習いただけます。
- 実践的な演習を通じて、コレクティブ・ディフェンスがご自身の企業へどのような利益をもたらすのか、導入方法も含めて学んでいただけます。

特徴②

「CISOとして成長するための個別フィードバック」

- 担当講師より、演習全体を通して受講者へフィードバックを行います。CISOとして成長するための助言をいたします。

特徴③

「米国重要インフラ分野の有識者による特別講演」

- 米国重要インフラ分野の有識者が、自身のコレクティブ・ディフェンスに関連するこれまでの経験談などをお話いただく予定です。

講師陣

ジョージ・ラモント氏（George Lamont）

IronNet Cybersecurity, Inc.
最高情報責任者（CIO）

米サイバーコマンドの大佐として、初の合同サイバートレーニング、認証基準およびサイバーフラッグ演習を始めた第一人者。
これまで、様々な国で通信ネットワークを構築し、世界中でチームを率いた経歴がある。ニューハンプシャー大学で数学と電気工学の理学士号を、オクラホマシティ大学でMBAを取得。CISSP保有。

フェルナンド・マイミ博士（Fernando Maymí, Ph.D.）

IronNet Cybersecurity, Inc.
最高情報セキュリティ責任者（CISO）

米陸軍のシンクタンクであるArmy Cyber Instituteの所長代理を歴任し、産官学のパートナーシップ活動に従事。また、サイバー空間の問題に関する議会のリーダーや企業の重役を務めた。
CISSP All-in-one Exam GuideおよびCompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guideの著者。

講師陣

スティーブ・ザルースキー氏（Steve Zalewski）

Levi Strauss & Co.
副最高情報セキュリティ責任者（副CISO）

Levi Strauss & Co.社の副CISO(Chief Information Security Officer)であり、チーフセキュリティアーキテクト、サイバーセキュリティインテリジェンスやインシデント対応ディレクター。
サイバーセキュリティ戦略とインシデント対応組織のマネジメントを担当し、前職ではPacific Gas and Electric Company社でエンタープライズセキュリティアーキテクトなどの役職も経験。

ブライアン・ディクストラ氏（Brian Dykstra）

Atlantic Data Forensics社
最高経営責任者（CEO）

コンピュータフォレンジックや電子的データ探索、フォーチュン500向けのデータ漏えいのインシデント対応を行うAtlantic Data Forensics社の創立者兼CEO。
Mandiant社の共同創立者であり、CIOやプロフェッショナル教育ディレクター、FBIアカデミーでのサイバー犯罪の講師を歴任。CCFP、CISSP、CISSP-ISSAP、CIFI。

スケジュール　1日目(予定)

通訳形態：
同時通訳

1日目（1月25日 (水) 10:00～17:30）

9:00～9:50　イントロダクション

9:50～12:00　ケーススタディ

ケーススタディ1　– 攻撃者の攻撃実行計画
ケーススタディ2　- 攻撃者の攻撃実行
攻撃者は「攻撃」をどのように捉え、計画や実行を行うのか学習します。
※途中休憩あり

12:00～13:00　お昼休み

13:00～16:00　攻撃デモ

ステージ1　攻撃デモ　– ITシステムへの侵入
ステージ2　攻撃デモ　– ITからOTへの横展開
ステージ3　攻撃デモ　– OTシステムへの侵入
攻撃者側はフィッシング攻撃などからITシステムへ侵入します。侵入したマルウェアは横展開をし、OTシステムへ侵入します。

※途中休憩あり

16:00～16:30　CISOの観点

ケーススタディや攻撃デモで学習した内容を踏まえて、CISO経験のある講師による振り返りを行います。

16:30～17:30　基調講演

米国重要インフラ業界のCISOによる基調講演となります。

スケジュール　2日目(予定)

通訳形態：
同時通訳

2日目（1月26日 (木) 10:00～18:00）

10:00～11:00
オープンソースインテリジェンス（OSINT）と脅威モデリング

防御側はまず攻撃者の理解から始める必要があります。
OSINTや脅威モデリングを活用し、攻撃者が何をターゲットとしているかを学習します。

11:10～11:50　アタックサーフェスの分析

12:00～13:00　企業におけるセキュリティの構成

13:00～14:00　お昼休み

14:00～14:30　コレクティブ・ディフェンスの紹介

組織化された脅威に対して、同業他社や他業界と連携することがますます重要になっています。集団で守るコレクティブ・ディフェンスについてご紹介します。

14:30～15:30 実行可能な脅威インテリジェンス

15:40～16:40　同業他社や他業界との協調

16:50～18:00　コレクティブ・ディフェンスの開発

2日目で学習した内容を踏まえて、コレクティブ・ディフェンス実装に向けて、どのように同業他社や他業界と連携するかを学びます。

スケジュール　3日目(予定)

通訳形態：
逐次通訳

3日目（1月27日 (金) 10:00～18:00）

10:00～10:30　グループ演習イントロダクション

10:30～11:45
グループ演習1：スコーピングとギャップ分析

11:55～13:10
グループ演習2：イニシアチブの策定

13:10～14:10　お昼休み

14:10～15:25
グループ演習3：サイバー事象の集団分析

15:35～16:50
グループ演習4：複数の組織によるインシデント対応

17:00～18:00　最終アセスメントと振り返りセッション

お申し込み先・お問合せ先

受講申し込み期間

受講申込は、2022年12月28日（水）までと致します。（募集定員に到達し次第、募集を締め切りとさせて頂きますので、お早めにお申し込みください）

お申し込み方法

WEB上の受講申込書に必要事項を記入していただき、**メールにてPDFを送付ください。**
※お申込みいただきましたら、担当者よりご連絡差し上げます。

お問合せ先：　03-5978-7554（直通）（受付時間）平日9:30-18:00
coe-promotion-info@ipa.go.jp

担当者：　北村/中山

URL：　https://www.ipa.go.jp/icscoe/program/short/all_industries/2022.html

※原則として、納入後の受講料はキャンセルされる場合でも、返金は致しかねますので予めご了承ください。
※受講料請求書は押印省略で発行します。押印希望の方は、お申込み時にご連絡ください。

【個人情報の取り扱いについて】
弊機構は、本申込のためにご提出頂いた個人情報の適切な管理に努めております。ご提供頂いた個人情報は、本トレーニングを提供するために必要な範囲（事務処理および講師への当日受講者リストの配布等）で利用させて頂きます。個人情報保護についての詳細は下記のページをご参照ください。
https://www.ipa.go.jp/about/personal/index.html