「工場セキュリティガイドライン啓発・連続セミナ」

セキュリティ対策に対する始めの一歩を提供する

サイバーコマンド株式会社 代表取締役
株式会社フーバー・クロステクノロジーズ 取締役
一般社団法人情報処理安全確保支援士会 理事
一般社団法人国際サイバーセキュリティ協会 理事

浦中　究

自己紹介

浦中 究(Uranaka Kiwamu)

【経歴】

富士通グループ、日本オラクル株式会社等にて、プロジェクトマネージャ、サービスマネージャとしての実績と、サーバインフラ、ネットワーク、データベース、クラウド、サイバーセキュリティのエンジニアとして経験を積み、ベンチャー企業にてCISOを務めた後にサイバーコマンド株式会社 代表取締役に就任。

その他、株式会社フーバー・クロステクノロジーズの取締役、一般社団法人の「情報処理安全確保支援士会」「国際サイバーセキュリティ協会」の理事を務める。

また、一般社団法人PMI日本支関西ブランチにて、定量的なプロジェクトマネジメントを研究テーマして活動。PMIフォーラムにて研究発表を行った実績を持つなど研究者としての側面も持つ。

登録番号：006197号

Company Introduction

サイバー空間の脅威から人々を守るプロフェッショナル集団

CYBER COMMAND

Mission Statement

増え続ける脅威から人々を守るため
サイバー攻撃と戦う

Vision Statement

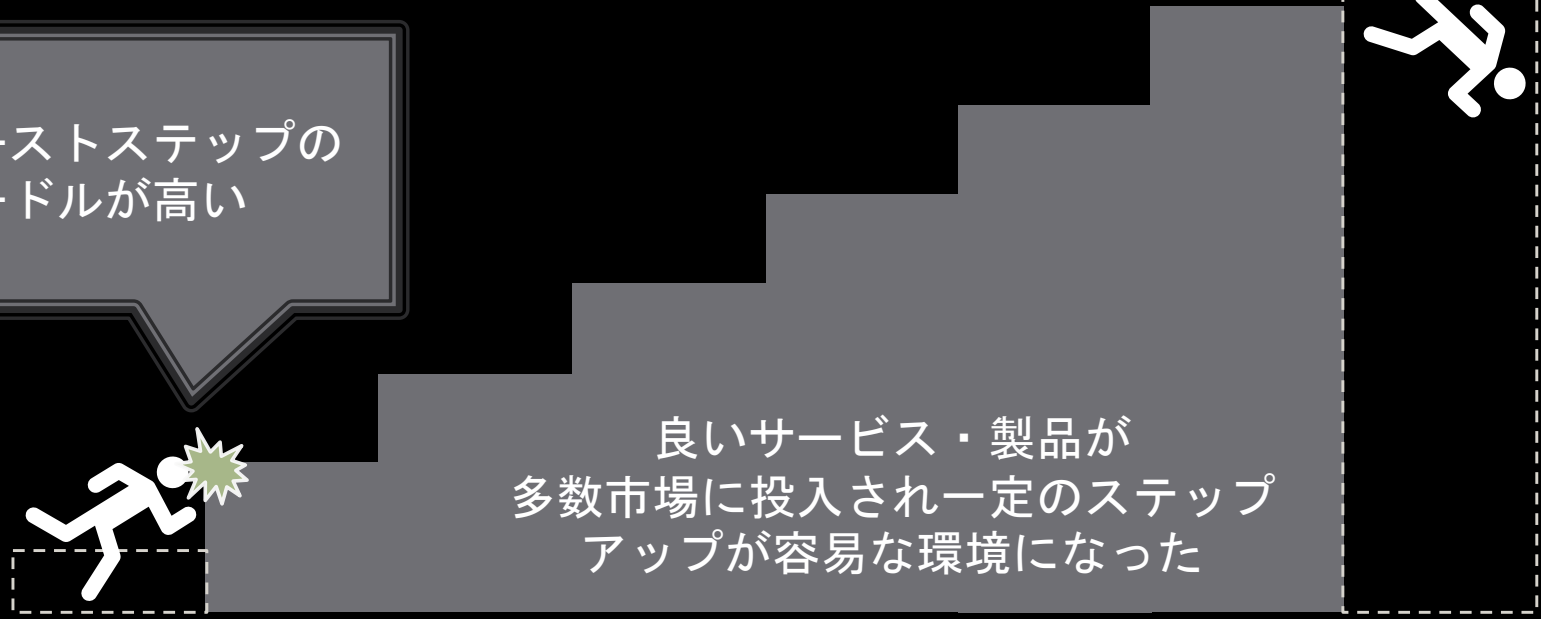
理論と実戦力を兼ね備えた専門家を
提供、育成し続ける

・法人名　：サイバーコマンド株式会社
・東京本社　：東京都渋谷区渋谷1-14-9-５F
・大阪本社　：大阪市東淀川区東中島1-17-26-4F
・事業内容　：サイバーセキュリティ専門家提供サービス
　　サイバーセキュリティトレーニング

セキュリティのご支援を行う中で感じる課題

B.ラストの
ワンマイルが足りない

A.ファーストステップの
ハードルが高い



良いサービス・製品が
多数市場に投入され一定のステップ
アップが容易な環境になった

A.ファーストステップへのアプローチ

①実戦教育(短期間)

全国に在住している「情報処理安全確保支援士(RISS)」へ活躍の場を提供するとともに、低価格路線でOTアセスメントを提供。

②実戦教育(やり切るところまで)

OT領域におけるSOC人材を実機を用いて教育。職場に戻ってすぐに始められる運用の手順・報告書の書き方などを指導。

③人材の提供

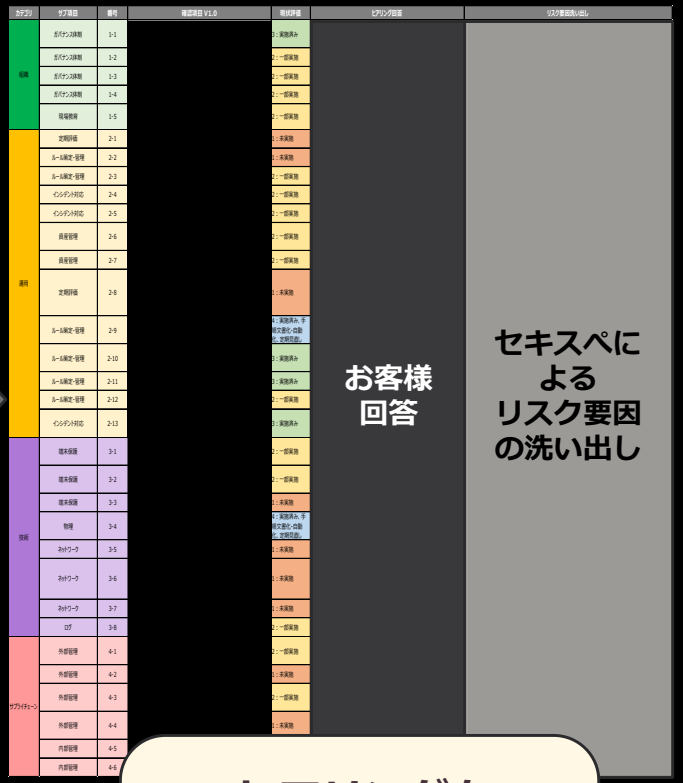
サイバーセキュリティの専門学科に、PLCの仕組みや操作を学習し、実際にハッキングするカリキュラムと講師を提供。

①簡易OTアセスメント(1/2)

Webチェックシート

まず項目ごとに
A～Eのご段階で
評価

アセスメントによるリスク要因洗い出し



ヒアリングを
しながら
問題点を洗い出し

リスクベース対策指針

アセスメントに基づき
対応の指針を提供

①簡易OTアセスメント(2/2)

情報処理安全確保支援士と
全国の案件をつなぐ
プラットフォームを検討中

PoC
2024年3月に
2社実施予定

②OT・SOC教育(1/2)

～セキュリティ対策基礎～

前半では、サイバー攻撃の背景や国内の事例から製造表のセキュリティ対策の必要性を学習します。

後半では、セキュリティ対策を進める上で重要なSOC対応について学習します。

IT・セキュリティの知識がない方にも、対策の必要性を理解して頂き興味を持って頂くことを目的とします。

■OTとは何か？
- OTの定義
- OTのシステム
- ITとOTの融合
- ITとOTの違い
- セキュリティ対策の必要性
  - ①工場目標とセキュリティ
  - ②QCDSとCIAの関係
  - ③OT環境でCIAを脅かす行動

■サイバー攻撃概論
- サイバー攻撃の背景
- 事例紹介
  - ①小島プレス工業
  - ②名古屋港コンテナターミナル
- 攻撃手法の解説
  - ①境界防御の限界
  - ②多層防御
  - ③標的型攻撃モデル
  - ④サイバーキルチェーン

■OT SOC概論
- SOCの役割
- IT端末とOT端末の特徴
- ITでのSOC対応
- OTでのSOC対応
  - ①脆弱なNW構成
  - ②侵入を検知・追跡できない構成
  - ③OT端末の何を監視するか？
- パデューモデル階層構造
- 事例から学ぶ攻撃手法
  - ①TSMC WannaCry感染事例
  - ②米フロリダ水道局　TeamViewer悪用
- イスラエル電力公社のサイバーセキュリテイ

■工場のセキュリティ対策の進め方
- フィジカルガイドラインの解説
- セキュリティ対策を進めるためには
  - ①管理すべきアセット数
  - ②SOC対応ための監視機能
  - ③資産管理を継続するコスト
- 対策に有効なNozomiの機能

②OT・SOC教育(2/2)

～Nozomiトレーニング～

ソリューション紹介では、Guardianの機能・機器の選定・構成などを中心に学習します。導入実績で、導入に至ったポイントや導入後の声を紹介します。

ハンズオンでは、実際にNozomiの画面を見て操作してを行います。資産管理・脆弱性管理・ネットワーク可視化・アラートなど　セキュリティ対策・SOC対応に重要な機能を体験して頂きます。

■Nozomiソリューション紹介
- 製品紹介 Guardian
- SaaSプラットフォーム Vantage
- Nozomi 3 つの勘所
- Guardian導入イメージ
- Guardianの強み
  ①グローバルユーザの声
  ②国内ユーザの声
- お客様から喜ばるポイント
- お客様で採用されるポイント
- 導入実績
- 製造業お客様共通の課題
- とある企業における導入ケース

■Nozomiハンズオン
- 製品概要
- インストール
- 各種画面の説明
- ダッシュボード
- 環境
  ①アセットビュー
  ②ネットワークビュー
  ③プロセスビュー
- 分析
  ①クエリ
  ②レポート
  ③タイムマシン
  ④脆弱性
- 学習
- アラート
- 管理

③専門学校教育(1/2)

TECH.C. OSAKA

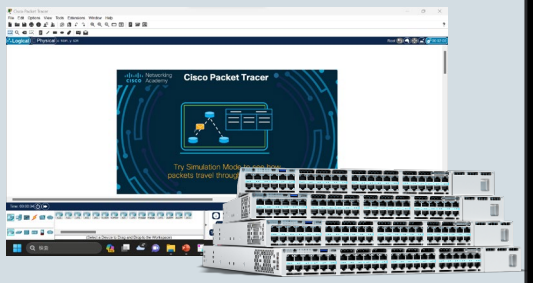
CYBER COMMAND

OSAKA

CYBER COMMAND

学校法人 コミュニケーションアート
OCA大阪デザイン&テクノロジー専門学校

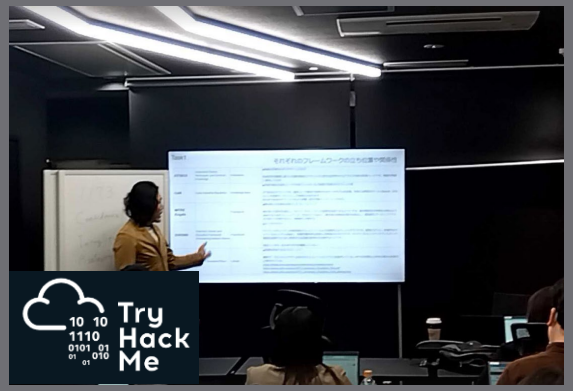
③専門学校教育(2/2)

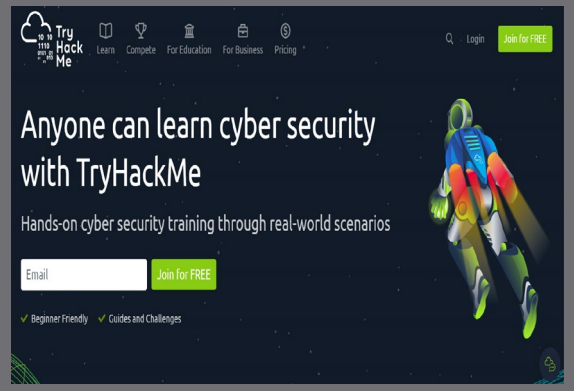
1年生	2年生	3年生	4年生
ITインフラ基礎	ITインフラ応用	ITセキュリティ	OTセキュリティ
		KALI	
専門講師の座学 PacketTracerによる インフラ構築演習	ルータ、スイッチの実機 を使用した構築演習	サーバOSの要塞化 フォレンジック演習 バイナリ解析等の演習	ツールとPLC実機による プログラミング演習 OTサイバー攻撃演習
※画像引用：オーム社HPより	※画像引用：シスコ社HPより	※画像引用：Kali Linux HPより	※画像引用：三菱電機社HP、アドウィン社HPより

学生の段階からITとOTの垣根を取り払う

B.ラストワンマイルへのアプローチ

①実戦教育(やり切るところまで)





SOC、フォレンジック、脆弱性診断等、100～140時間の実戦を提供。具体的な報告書の書き方などを現役エンジニアが採点・指導。

②実戦型人材の供給

現場で手を動かすエンジニアを採用・育成・提供するスキームを構築。

①実戦教育

受講者が一人でできる状態になるまで指導

▼2,3日のトレーニングでは、現場に戻っていきなりやってくださいと言っても実際は難しいというのが実態。サイバーコマンドでは受講者の方が現場に戻って一人でアウトプットができるところまで指導。複数の事例や例題を実機を通じて学習。報告書の妥当性までチェックします。

短期間の研修は
知識は得られるけど
できるわけじゃない

仕事でお金をもらう
前提で長時間指導
現場で一人でできる

②実戦型人材の供給(1/2)

[システム運用＋SOC対応オペレーター供給キャンペーン]

▼2024年2月よりSOCオペレーターが可能な人材の提供拡大を行っています。全体で20名～30名のキャパシティをご用意しており、業務リソース不足の解消、セキュリティ関連ビジネスの拡大をアシスト。

昨年12月より採用拡大	トレーニングセンターで実戦訓練	2月より順次ご提供

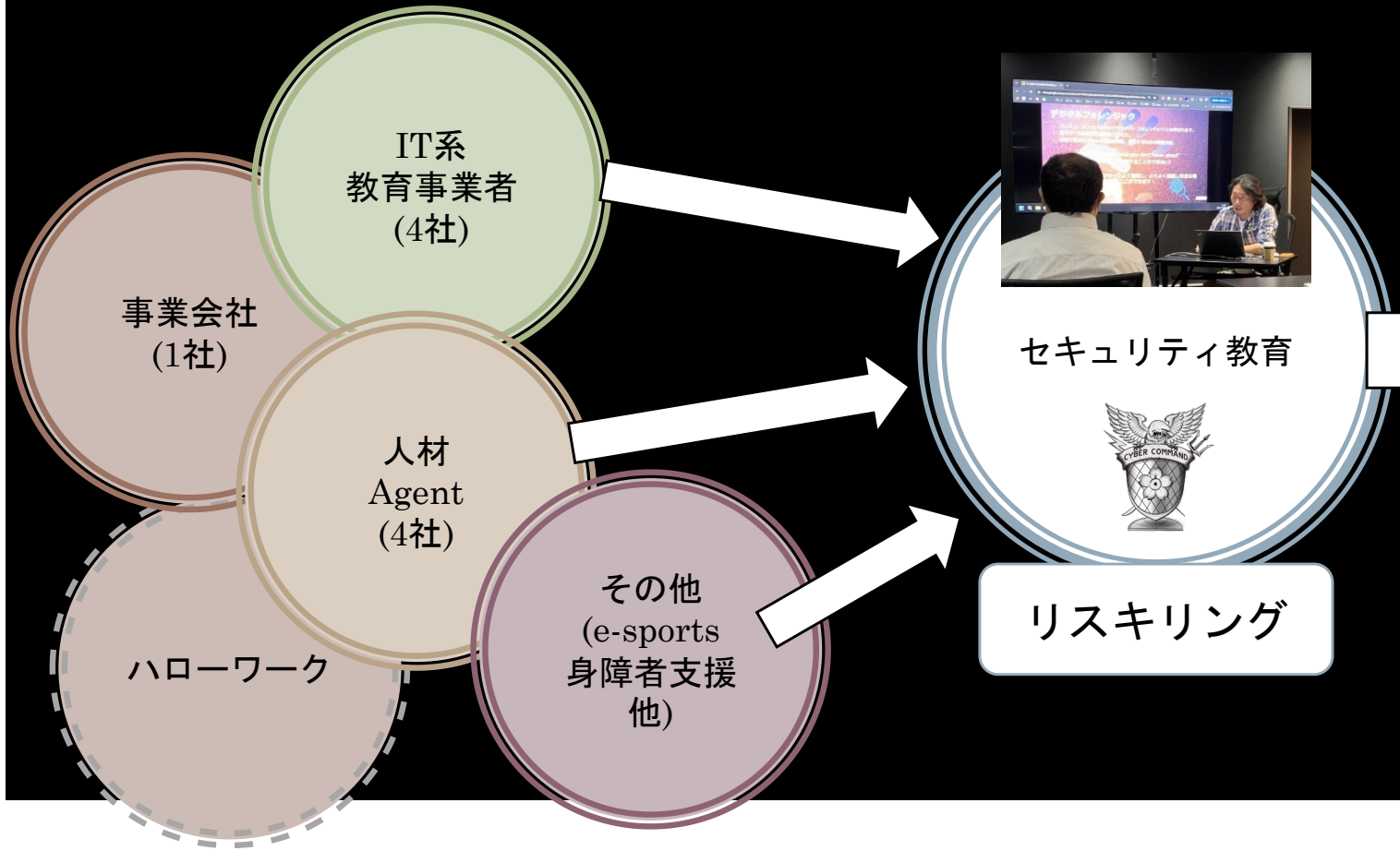
想定業務とスペック

- **想定業務**：アラートの監視と調査(24時間365日の交代勤務可)、セキュリティツールの設定と管理、IDS署名の開発と実装、必要に応じて、セキュリティ関連インシデントをアナリストおよびチームリーダーにエスカレーション。
- **スペック**：0年～2年程度のセキュリティ運用経験。ネットワーク (OSI モデル (オープン システム相互接続モデル) または TCP/IP モデル (伝送制御プロトコル/インターネット プロトコル モデル))、オペレーティング システム (Windows、Linux)、Web アプリケーションの基本的な理解。スクリプト/プログラミングのスキルを有する者もあり。
- **ツール例**：「Splunk」「Microsoft Sentinel」「Nozomi Networks Guardian」「Darktrace」「CATO SASE」「IBM Security QRadar」等

②実戦型人材の供給(2/2)

[セキュリティ業界への人材流入スキームを構築]

▼初級のITエンジニア資格(CCNA、LIPIC、LINUC等)を持った人材(40名～50名/月)を、パートナーよりご紹介いただく契約を締結し、その中から意思と素養のある方にセキュリティ教育を提供するスキームを構築しました。国内のセキュリティ人材不足解消に寄与いたします(2024年度は年間で100名以上を現場へ供給することを目標としています)。



セキュリティ教育

リスキリング

現場配属
・採用
・紹介

Thank you