データシート

EclecticIQアカデミー

CTIの基礎

EclecticIQアカデミーCTI基礎コースでチームのスキルとCTIの専門知識を次のレベルに引き上げましょう

はじめに

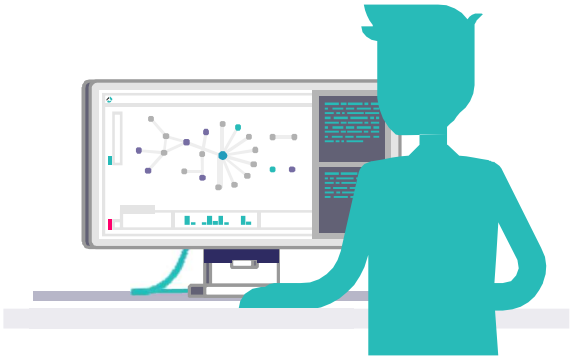
サイバースキル不足は、世界中のCISO（最高情報セキュリティ責任者）にとって心配の種です。ほぼすべての組織のSOCが人材不足です。訓練を受けたサイバースタッフはいつだって、最も望まれるところに転職してしまうからです。

この課題に対処するため、多くの組織は第三者組織による継続的な教育を実施して、サイバーチームとネットワークチームのスキルアップを図っています。

多くのセキュリティ職にとって、このタイプのトレーニングと認定はよく機能していますが、費用が高くなります。しかし、脅威インテリジェンストレーニングに関してはそうではありません。チームメンバーの知識、スキル、能力（KSA）を上げるためには、脅威アナリストはかなり専門的なトレーニング、つまり脅威インテリジェンスプラットフォーム（TIP）に関するトレーニングを受ける必要があります。

EclecticIQは、EclecticIQプラットフォームの専用の個人用インスタンスを使い、社内CTIエキスパートを通じて、CTIアナリストが必要とする専門トレーニングを提供しています。トレーニングでは以下のことを学習できます。

- CTIチームの能力を向上させるための、幅広い実践的スキル
- 既存のSOC/ネットワークチームメンバーのスキルを向上させる詳細な知識
- 予算にやさしい料金設定の、コスト効率に優れたトレーニング



主なメリット

サイバースキル不足に対処

EclecticIQプラットフォームのCTIアナリストになれるように、現在のSOCとネットワークチームメンバーのスキルを高めます。スキルアップによって、CTIアナリスト不足の影響を軽減しながら、既存の人員のキャリアの道が開けます。

世界クラスの脅威インテリジェンスのエキスパートから学ぶ

弊社の経験豊かなトレーナーが、Fusion Center、およびEclecticIQプラットフォームを日常的に使用している社内CTIアナリストチームからの先進的なフレームワークとベストプラクティスを利用して、分析的思考方法を徹底的に教えます。たとえば、受講者はMITRE ATT&CKのような先進的なフレームワーク、侵入分析のダイヤモンドモデルのような従来のフレームワークの利用方法を学びます。

TIPによる価値創出までの期間を短縮

受講者はEclecticIQプラットフォームについて個人的なイメージで学習するので、学習したことを即座に活用できます。この実践的で現実世界に即したアプローチは、TIPの価値を素早く実証し、組織のCTI投資での価値創出の期間を短縮します。

EclecticIQ

EclecticIQアカデミー CTI基礎のユースケース

SOCチームメンバーのスキルアップ

課題:

- 第三者によるCTIトレーニングは費用が高く、実践よりも理論の比率が多い
- 受講者がトレーニングをTIPに応用する方法を見つけるまで数時間もかかる

ソリューション:

- EclecticIQは、基本的な分析CTIフレームワークをEclecticIQプラットフォームに応用する方法を教えることで、理論を実践に結び付けます
- プロのCTIインストラクターが実践的な対面形式のトレーニングをオンラインまたはオンサイトで提供します

メリット:

- 社内スタッフのスキルアップは、CTIスキルの不足に対処する上で効果的
- EclecticIQのトレーニングは費用対効果が高く、限られたトレーニング予算に対応

CTIの効果を強化

課題:

- CTIチームには、様々な能力のメンバーが存在し、分析フレームワークとプラクティスが共有されていない
- そのため、協働の機会が減り、一貫性のない不正確なコミュニケーションが生じる

ソリューション:

- CTI基礎を利用すると、チーム全体をトレーニングして、基本的、実用的なサイバー脅威インテリジェンスを生成できます
- EclecticIQプラットフォームの個人用インスタンスを使用することで、CTIアナリストはベストプラクティスを素早く応用する方法を学びます

メリット:

- TIPを効果的に運用することで、より的確な脅威の検知、優先順位付け、分析を推進
- TIP運用を最適化することで、全体的なセキュリティに対する姿勢を強化

EclecticIQアカデミーのCTI基礎コースについて

インストラクターがCTI基礎5日間コースをEclecticIQ学習管理システム（LMS）で実施します。お客様の要件に応じて、クラスはオンラインまたはオンサイトになります。

EclecticIQは、外部のCTIエキスパートと協力してCTI基礎を開発しました。Fusion Centerからのベストプラクティス、EclecticIQプラットフォームを日常的に使用している弊社のCTIアナリストの社内チームのベストプラクティスを組み入れています。

弊社のトレーニングを利用すると、自社CTIチームのスキルを向上させて、EclecticIQプラットフォームへの投資から価値を最大限に引き出すことができます。

EclecticIQ

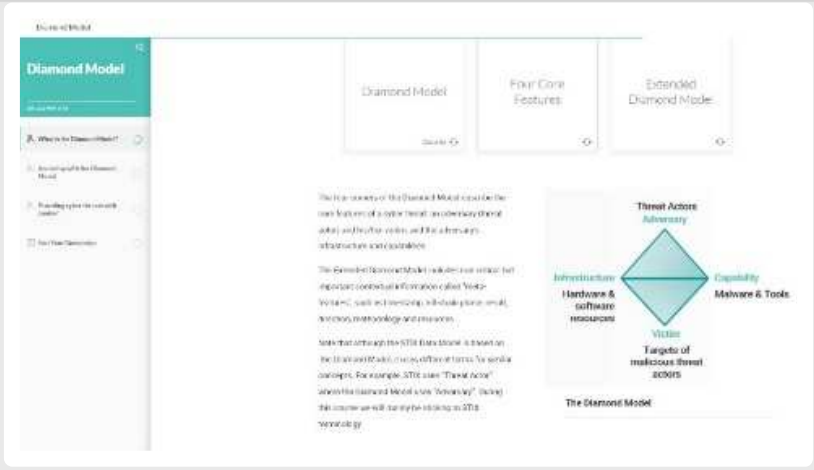
EclecticIQ
CTI基礎の概要

1日目

- インターネットの歴史
- サイバー脅威分析VS脅威インテリジェンス
- データをインテリジェンスに変換
- STIX 1.2データモデル
- プラットフォーム演習

2日目

- サイバー戦場のインテリジェンス準備
- インテリジェンスのライフサイクル
- 優先するインテリジェンス要件の定義
- サイバーキルチェーン
- ダイヤモンドモデリング



3日目

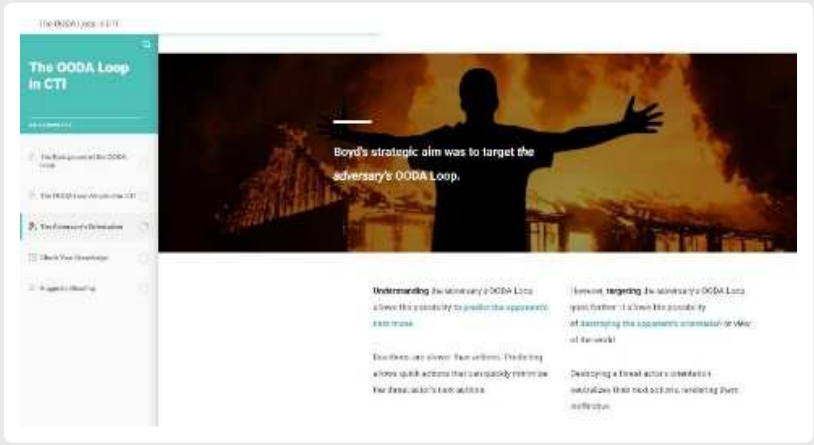
- 攻撃に関する状況の定義
- MITRE ATT&CK®の概要とプロファイリング
- 脅威モデリング
- 脅威インテリジェンスにおける脆弱性データの使用
- 脅威プロファイリング
- プラットフォーム演習

EclecticIQ

EclecticIQ
CTI基礎の概要

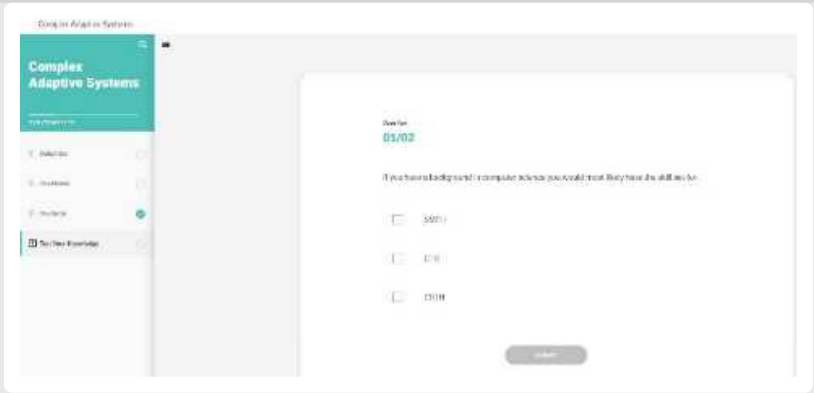
4日目

- 認識の偏り
- OODAループ
- 矛盾する仮説の分析
- プラットフォーム演習



5日目

- 組織構造へのサイバー脅威インテリジェンスの統合
- 複雑な適応システム
- プラットフォーム演習
- 脅威エージェントライブラリー
- プラットフォーム演習



EclecticIQについて

EclecticIQは、行政機関と一般企業を対象に、インテリジェンスで強化したサイバーセキュリティを実現します。お客様のサイバーセキュリティの焦点を脅威の現実に合わせる、アナリストを中心に考えた製品とサービスを開発しています。その結果、インテリジェンス主導型セキュリティ、検知と予防の向上、コスト効率に優れたセキュリティ投資が実現します。

EclecticIQアカデミーの詳細：**www.eclecticiq.com**
EclecticIQへのお問い合わせ：**info@eclecticiq.com** または**+31 (0) 20 737 1063**

EclecticIQ