FUJITSU 人材育成・研修サービス

自組織のプロアクティブ（先回り）な防御のためにインテリジェンスの活用がお勧めです

講習会：サイバーセキュリティインテリジェンス実践

本コースでは、オープンソース（広く一般に公開されている情報）を「調べ突き合わせる」ことにより「付加価値のある情報を生成する」OSINT（Open Source Intelligence）手法を使用し、サイバー脅威インテリジェンス（CTI）を導き出しプロアクティブな防御につなげられるスキルを習得します。

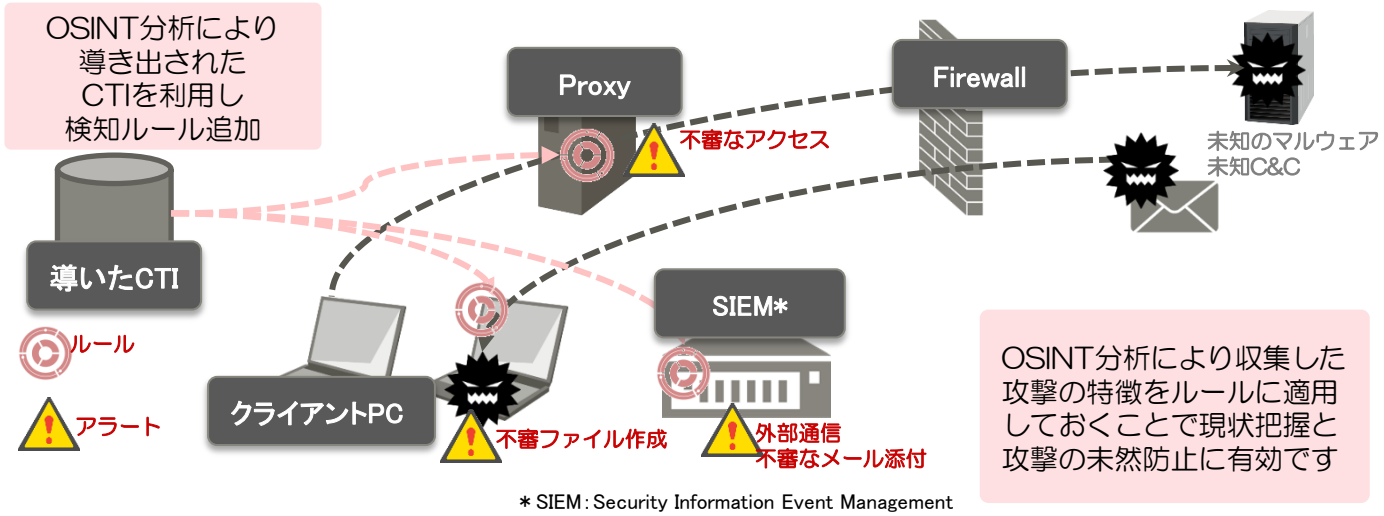
こんな課題をお持ちの方にお勧めします

■OSINT（Open Source Intelligence）分析を行いたい方
■セキュリティ情報の収集や実践的な活用方法に困っている方
■公開されている情報を活用したセキュリティ対策に興味がある方
■脅威情報の活用に興味がある方
■CSIRT業務に携わる方

参考：CTI活用のイメージ

ICT環境は今後も様々な攻撃の脅威にさらされることが予測されます。現在、各団体・組織にで構築されているCSIRT（Computer Security Incident ResponseTeam）におけるインシデントレスポンス手法は、どちらかというと侵入されてから使用される前提になっています。これをプロアクティブ（先回り）な防御に変化させるためにはサイバー脅威インテリジェンス（CTI: Cyber Threat Intelligence ）の活用が有効です。

例：導き出されたCTIを活用し攻撃の特徴を検知ルールに適用し、潜在的、将来的な攻撃を検出する



＊SIEM：Security Information Event Management

本コースおすすめのポイント！

本講座で使用するテキストは、現場でCTIやOSINT分析業務を担当している技術者により執筆されています。要点がまとまった本テキストを使用しOSINT分析を体験することで、必要なポイントを短期間で学習します。

コースの概要

サイバーセキュリティインテリジェンス実践

期間：2日間

項目	内容
型番	SV6AUSA57L
受講対象	CSIRT業務に携わる方、情報収集や実践的な活用方法に困っている方 公開されている情報を活用したセキュリティ対策に興味がある方 脅威情報の活用に興味がある方
コース概要	サイバー攻撃の対策として、多層防御だけでは防御できずに被害を受けるケースが多々報告されている。その要因の一つとして、現在おきている攻撃や近い将来に来るであろう攻撃に対する防御策を行えていない点が挙げられる。その防御策を実現するためには、攻撃の把握、防御策を導くための分析手法や防御・対策をするために組織が意思決定ができる情報（Cyber Threat Intelligence） の活用が重要になってきている。 本講座ではインターネット上にある膨大な情報から、Cyber Threat Intelligence を導き出し、自組織のプロアクティブ(先回り)な防御につなげられるスキルを習得できる。
前提知識	ネットワークやDNSなどインターネットに関する一般的な知識を有すること サイバーセキュリティに関する一般的な用語を理解していること 最近の攻撃方法や対策についての知識を有していることが望ましい
コース価格	180,000円（税別）

日程・スケジュール

時間	1日目	2日目
午前	第1章　サイバー攻撃の概要 1.1　昨今のサイバー攻撃 1.2　標的型攻撃 1.3　マルウェアについて 1.4　C&Cサーバについて	第3章　Open Source Intelligence (OSINT)分析（つづき） 3.2　検索エンジン 3.3　マルウェアデータベース 3.4　Whois 3.5　レスポンスコード分析
午後	第2章　セキュリティ情報とCyber Threat Intelligence 2.1　セキュリティ情報の重要性と分類 2.2　セキュリティ情報収集（Public Monitoring） 2.3　Cyber Threat Intelligence(CTI) 第3章　Open Source Intelligence (OSINT)分析 3.1　Open Source Intelligence (OSINT)分析	第4章　総合演習 ※OSINT分析の実践演習です。

関連コースのご案内：2018年度上期　新規開催予定のコース

項目	内容
コース名	サイバーレンジによる実践的防御訓練
受講対象	一般的なシステム開発、運用を担当するSE、CSIRTのメンバー
コース概要	システム運用の現場において、セキュリティインシデントが発生した場合、多様なOSやミドルウェア、プロダクト、ネットワーク機器やセキュリティ機器から発生する情報を収集し、セキュリティインシデントかどうかの判断が求められます。 本教育は、セキュリティインシデント発生時における初動対応を実現するために、簡易的な調査や分析が行えるかを確認します。（実践的な内容のため講義は最小限です）

※本情報は2017年10月20日現在の情報です。内容は都合により変更する可能性があります。

製品・サービスについてのお問い合わせは

お客様総合センター

0120-55-9019

受付時間 9:00～17:30（土・日・祝祭日を除く）

株式会社富士通ラーニングメディア　〒108-0075 東京都港区港南2-13-34 NSS-IIビル　http://www.knowledgewing.com/