セキュリティ組織強化トレーニング上級

ー サイバーセキュリティトレーニング ー

サイバー攻撃が高度化・多様化し、サイバーレジリエンスの重要性が高まる中、多くの企業・組織で、有事を想定したインシデント対応の実践的な検証の必要性が高まっています。
「サイバーセキュリティ実践演習」を実施することで、自組織の対応力や課題を可視化し、セキュリティ対策の優先順位付けや体制整備につなげることが可能です。

セキュリティ対策の実効性を検証したい企業・組織におすすめ

弱点の可視化
セキュリティ対策の抜け漏れや弱点を客観的に特定したい

対応力の強化
ログ分析や端末調査を通じて、実践的なインシデント対応力の向上に取り組みたい

セキュリティ組織強化トレーニング上級の特長

本演習は、国立研究開発法人情報通信研究機構（NICT（エヌアイシーティー））主催の実践的サイバー防御演習「CYDER」や実践サイバー演習「RPCI」における豊富な講師実績を持つ専門家や、セキュリティ専門家・ホワイトハットハッカー（CEH*保有）などの経験豊富なプロフェッショナル人材が講師を担当します。講師自らが攻撃者役となり、社内環境（Active Directory）や公開サーバー（Webサーバー）を標的とした仮想攻撃を実施します。受講者は、ログ分析やサーバー・端末の調査を通じ、攻撃の検出・防御に取り組むことで、実践的な演習を体験可能です。これにより、攻撃の手口を理解し、インシデント発生時の迅速な検出・対応力を高めるとともに、自社のセキュリティ対策の実効性向上に直結する実践力を習得できます。

* CEH：Certified Ethical Hacker（認定ホワイトハットハッカー）

セキュリティ組織強化トレーニング上級の構成

演習概要	攻撃者役の当社ホワイトハットハッカーが、社内環境（Active Directory）や公開サーバー（Webサーバー）を標的とした仮想のサイバー攻撃を行います。これに対し、ログ分析やサーバー・端末の調査を通じて攻撃の検出・防御における自組織の対応力を検証できます。

演習構成

- **演習内容、ルールの説明**
- **必要な事前知識の習得**
  （代表的なサイバー攻撃の流れと手法/ログの確認ポイント/調査で使用するツール）
- **事前準備**
  （仮想組織を狙う攻撃者や攻撃手法のシナリオ設定/仮想組織のシステム構成や運用の把握）
- **演習実施**
- **演習結果の解説・講評**

受講概要	受講料	個別見積	日程	個別相談

詳細は当社Webページをご覧ください。
スマートデバイスで二次元バーコードを読み取っていただくか、URLをブラウザーのアドレスバーに入力してアクセスしてください。
https://www.hitachi-solutions-create.co.jp/solution/security_training/

商品・サービスに関するお問い合わせ・ご相談受付

Webによる受付
www.hitachi-solutions-create.co.jp/inq.html
お問い合わせページより、商品・サービスをお選びください。

メールによる受付
hsc-contact@mlc.hitachi-solutions.com

ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

製品仕様は、改良のため予告なく変更する場合がございます。最新情報は、当社Webページをご参照ください。
本カタログの内容は、2026年7月現在のものです。

株式会社 日立ソリューションズ・クリエイト
www.hitachi-solutions-create.co.jp/

HSC202607