コースコード：GX-SVMP
税込価格：132,000円 (税抜価格：120,000円)
日数：1日間

ここに注目!!

本講座は、各種一次資料に基づいて構成されており、それらを業種を問わず利用できるように一般化した内容となっています。
受講者が自社に学習成果を持ち帰り、根拠をもって上司や決裁権者に説明できるよう、講座資料にも根拠となる一次資料の出典を明記しています。

講座の骨格：
・金融庁 / 日本銀行「フロンティアAIによる脅威変化を踏まえた短期的な対応」の9項目の準拠
・短期応急（1ヶ月）と中長期（自動化への移行）の2軸で全体を構造化
判断の枠組み:
・Gather CTEMの5フェーズ、ISOG-J手引きの2段階設計、CISA SSVC / KEV

受講対象者

このトレーニングはこのような方におすすめです。

・実務経験2～3年以上のITエンジニア

前提条件/前提知識

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

システムの開発経験もしくはネットワークの構築経験

目的

このコースを修了すると次のことができるようになります。

本講座は、フロンティアAI時代に求められる「対応すべき脆弱性を見極め、優先順位を判断できるエンジニア」を育成することを目的としています。

アウトライン

資産から自動化まで、脆弱性管理の全工程を一続きで設計します
各章のワークが、そのまま持ち帰りの成果物になるよう設計されています。

前提と守る対象（1～2章）
・脅威変化を数値で押さえ、経営に上げる報告観点を言語化する
・ASMとSBOMで「公表当日に該当有無を返せる」状態を作る

判断（3～5章）
・保守契約とリソースの空白を洗い出す

・CVSS / KEV / EPSS / SSVCの使い分けと、多軸トリアージの組み立て
・90分の机上演習で、8件の脆弱性を一人で並べ替える

直せない前提の設計（6〜7章）
・仮想パッチ / 分離・監視と、リスク受容手続をセットで設計する
・能動的サービス停止の判断基準と、脆弱性対応の自動化への移行

〜1日の流れ〜
午前で脅威と守る対象を押さえ、午後の90分演習で判断を体で覚えられます。
演習では、8件の脆弱性が同時に発生したという例で行います。
記入様式はISOG-
Jの手引きに準拠しているので、そのまま自社の文書の骨格としてもご使用いただけます。

10:00〜10:50 第1章 フロンティアAIで脅威は何が変わったのか
10:50〜12:00 第2章 守る対象を知る：資産特定と技術負債の解消
13:00〜13:40 第3章 リソースと契約：有事に動ける体制か
13:40〜14:30 第4章 リスクベーストリアージの理論
14:40〜16:10 第5章 机上演習：脆弱性トリアージ
16:20〜17:10 第6章 パッチが当てられない時：補完防御への設計
17:10〜17:50 第7章 止める勇気と、つながる力、そして自動化へ
17:50〜18:00 クロージング：明日から着手する1項目