2023/7/29 Ver.2.0

●情報システムペンテスター

			定義
ジョブディスクリプション			**ITシステムのセキュリティ検証を実施** ・対象の情報システムにおける脅威シナリオの作成 ・発見した脆弱性を使用した脅威の実現可否確認 ・脅威の実現可否に基づくセキュリティ耐性の評価 ・セキュリティ耐性評価を基にした対策の提言
エントリー	業務遂行能力	管理	上位のサポートにより以下を部分的に実施できる： **④報告書案の作成** -報告書作成能力（エグゼクティブサマリー、検証結果の詳細報告） **⑤顧客との調整** -ペネトレーション実施における顧客との調整（ゴールの共有、報告内容の取扱い、対策記載レベルの合意など）
		技術	上位のサポートにより以下を部分的に実施できる： **③ペネトレーションテストの実施** -下記のような様々な攻撃手法※を用いたペネトレーションテストの実施 （策定された脅威シナリオに基づいた脅威の顕在化） - Reconnaissance（偵察）：作戦を計画するために使用できる情報の収集 - Resource Development（資源開発）：作戦を支援するために使用できるリソースの確立 - Initial Access（初期アクセス）：ネットワークへの侵入 - Execution（実行）：悪意のあるコードの実行 - Persistence（永続性）：確立したアクセスやリソースの維持 - Privilege Escalation（特権の昇格）：より高いレベルの権限の取得 - Defense Evasion（防衛回避）：検出からの回避 - Credential Access（ID情報へのアクセス）:アカウント名とパスワードの窃取 - Discovery（発見）：環境の掌握 - Lateral Movement（横方向の動き）：ターゲット内部での移動 - Collection（コレクション）：関連するデータの収集 - Command and Control（コマンドと制御）：C&Cサーバーとの通信による制御 - Exfiltration（抽出）：データの窃取 - Impact（影響）：システムとデータの操作、中断、または破壊 ※攻撃手法参照元：MITRE ATT&CK エンタープライズ向け戦術 **④報告書案の作成** -検証結果の上位層への報告、報告書案の作成
	知識	管理	
		技術	**①最新の攻撃の手口に関する知識** -サイバー攻撃の戦略・戦術・手順に関する知識（例：MITRE ATT&CK エンタープライズ向け戦術） -検証対象の関連サービスに対して想定される脅威に関する知識 **②ハードニング技術に関する知識** -機器やアプリケーションのハードニング技術に関する知識

アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）