デロイトのRed Team Operationsの原則

私たちは以下のことを原則として徹底します。

テクノロジーとビジネスの融合 – サイバーセキュリティの目的は組織のビジネスの安定性・成長を確保することです。
Red Team Operationsがこの目的達成に寄与するよう、テクノロジーのみならず、組織のビジネスを理解します。

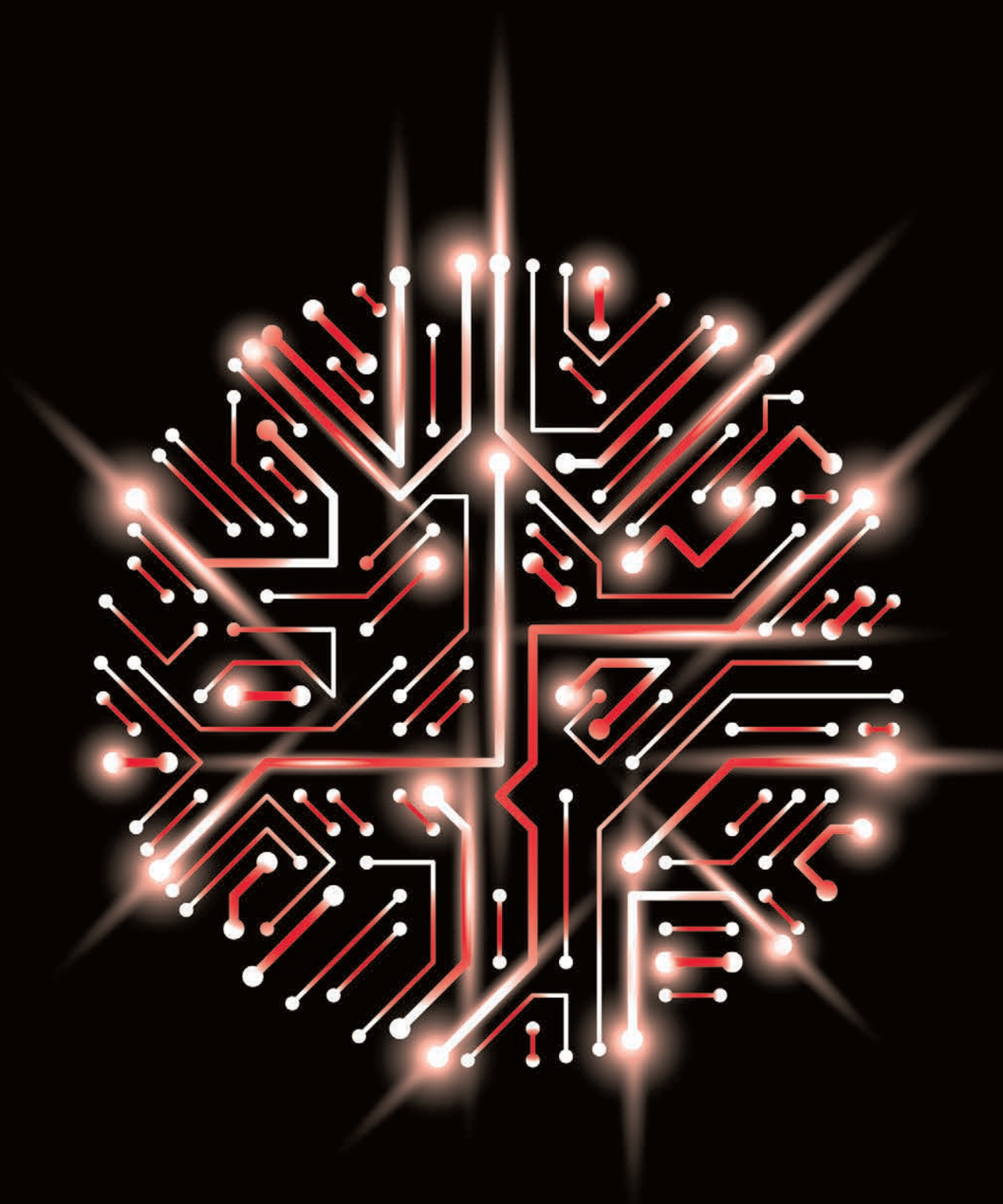
攻撃者に対する徹底的理解 – Red Team Operationsのシナリオ策定に際しては、
組織が抱える脅威、想定される攻撃者像の分析を行うことで、組織に現実に起こりうるシナリオを策定します。

効果の最大化 – 攻撃を成功させることが最終目標ではなく、
組織のサイバー攻撃対応力高度化に資することを目的とし、Red Team Operationsを計画・遂行します。

Deloitte.
デロイト トーマツ

IS 669126 / ISO 27001

BCMS 568132 / ISO 22301



Red Team Operations のご紹介

Physical, Human, or Cyber? Where are your weak links?

Red Team Operationsとは

実践的なアプローチによるセキュリティテスト
Red Team Operationsは、現実的なシナリオに基づいたインシデントのシミュレーションによって、サイバー攻撃への対応（予防・発見）力を評価するセキュリティテストの手法です。

Red Team Operationsは組織のあらゆる要素をスコープに入れ、シナリオに基づくアプローチを行うことから、従来の「脆弱性テスト」よりも実践的な評価が可能です。

Red Team Operationsの実施によって、組織のサイバーセキュリティの実力および課題を可視化することにより、サイバー攻撃への対応力高度化を促進します。

3つの主要エレメント

サイバー攻撃者はネットワーク経由に限らず、物理・人といった側面からも攻撃またはそのための事前準備（情報収集等）を行います。
従って、Red Team Operationsにおいても次の3要素を対象とします。

- **Physical（物理）:** データセンター、オフィス、来客用会議室などの物理空間
- **Human（人）:** 従業員、顧客、外部委託先など、サイバー空間と物理空間を接続する人々
- **Cyber（ネットワーク）:** インターネット、イントラネットなど、すべてのコンピューターネットワークを包括したサイバー空間

数字で見るDeloitteのRed Team Operations

94%

クライアントの94%が、Red Team Operationsで侵入に“成功”されています。

70%

クライアントの70%が、システムやCrown Jewel（攻撃目標）が攻撃を受けたことの発見や対応ができませんでした。

1日

偵察フェーズから、入り口となるデバイス上の権限を奪取し、クライアントのネットワークに最初にアクセスするまでの所要時間は、平均して僅か1日でした。

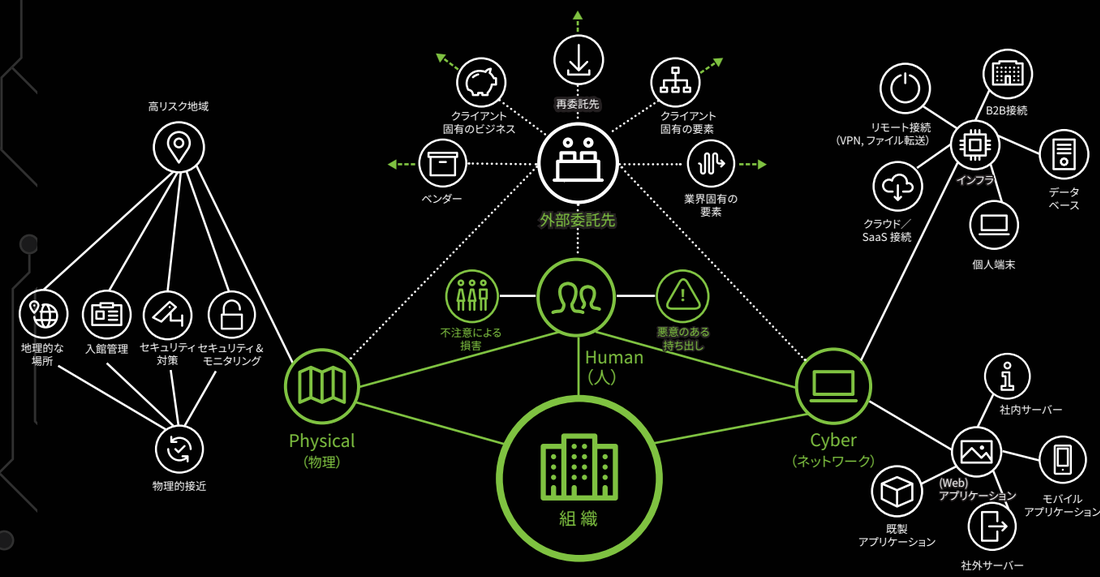
6日

偵察のフェーズを終え、Crown Jewel（攻撃目標）を攻略するまでの所要時間は、平均して6日間でした。

攻撃目標の例

- 巨額の不正送金
- 製造ラインの停止
- 研究開発情報等知的財産の窃取
- 社内システム管理者権限の奪取

攻撃対象領域



組織の状況・特性を踏まえた攻撃目標とシナリオを策定し、
サイバー攻撃への対応（予防・発見）力を評価し、
対策の改善に繋げます