




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

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド (英国の法令に基づく保証有限責任会社) のメンバーファームであるデロイト トーマツ 合同会社およびそのグループ法人 (有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザー合同会社、デロイト トーマツ 税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む) の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザー、コンサルティング、ファイナンシャルアドバイザー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト (www.deloitte.com/jp) をご覧ください。

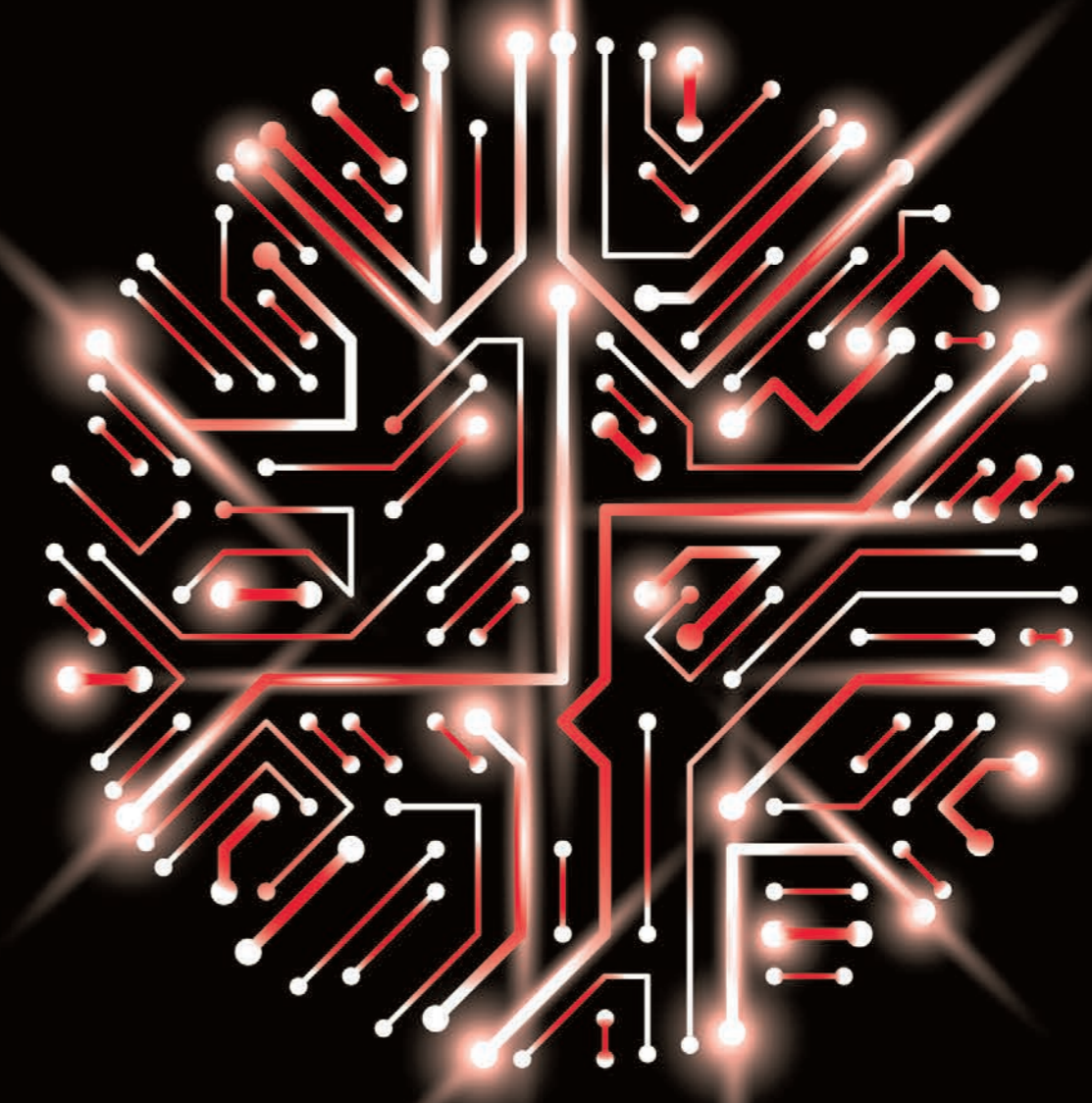
Deloitte (デロイト) は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザーサービス、リスクアドバイザー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じて、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte (デロイト) とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド (“DTTL”) ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL (または“Deloitte Global”) はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2018. For information, contact Deloitte Tohmatsu Risk Services Co., Ltd.
2018.03_0229



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

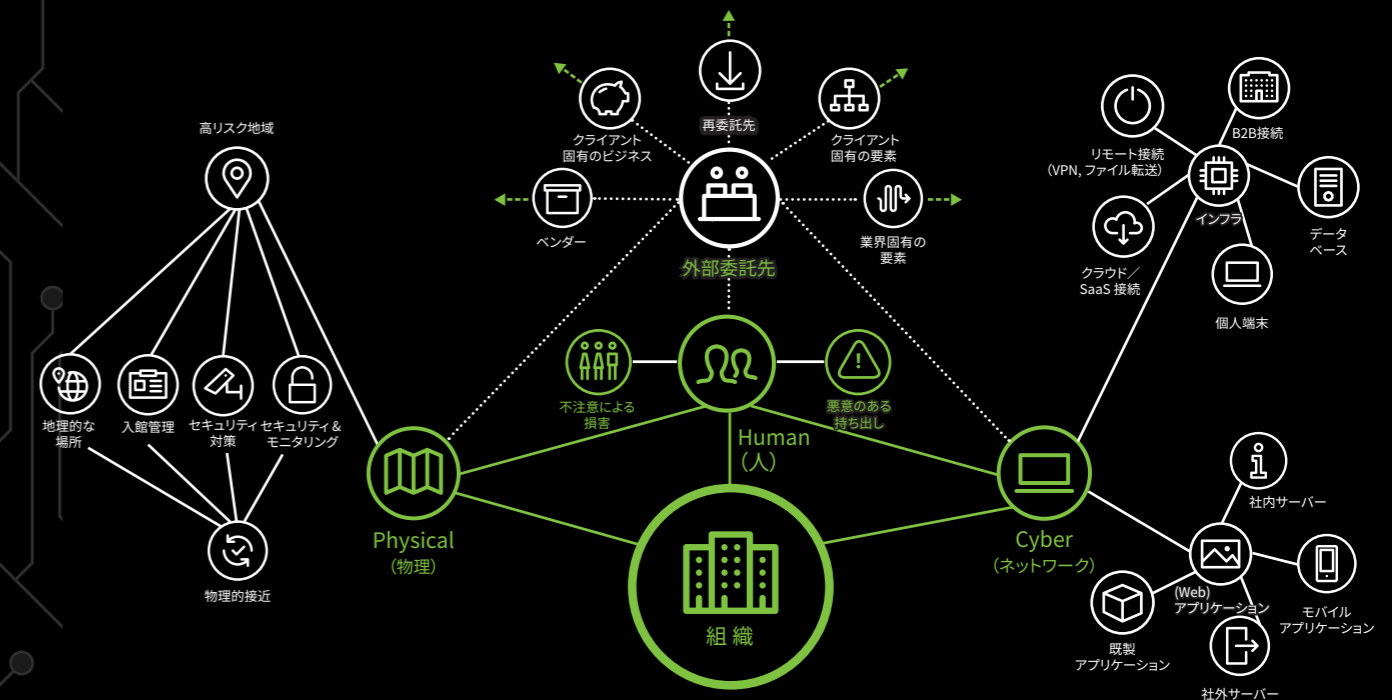
数字で見るDeloitteのRed Team Operations

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



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、対策の改善に繋がります