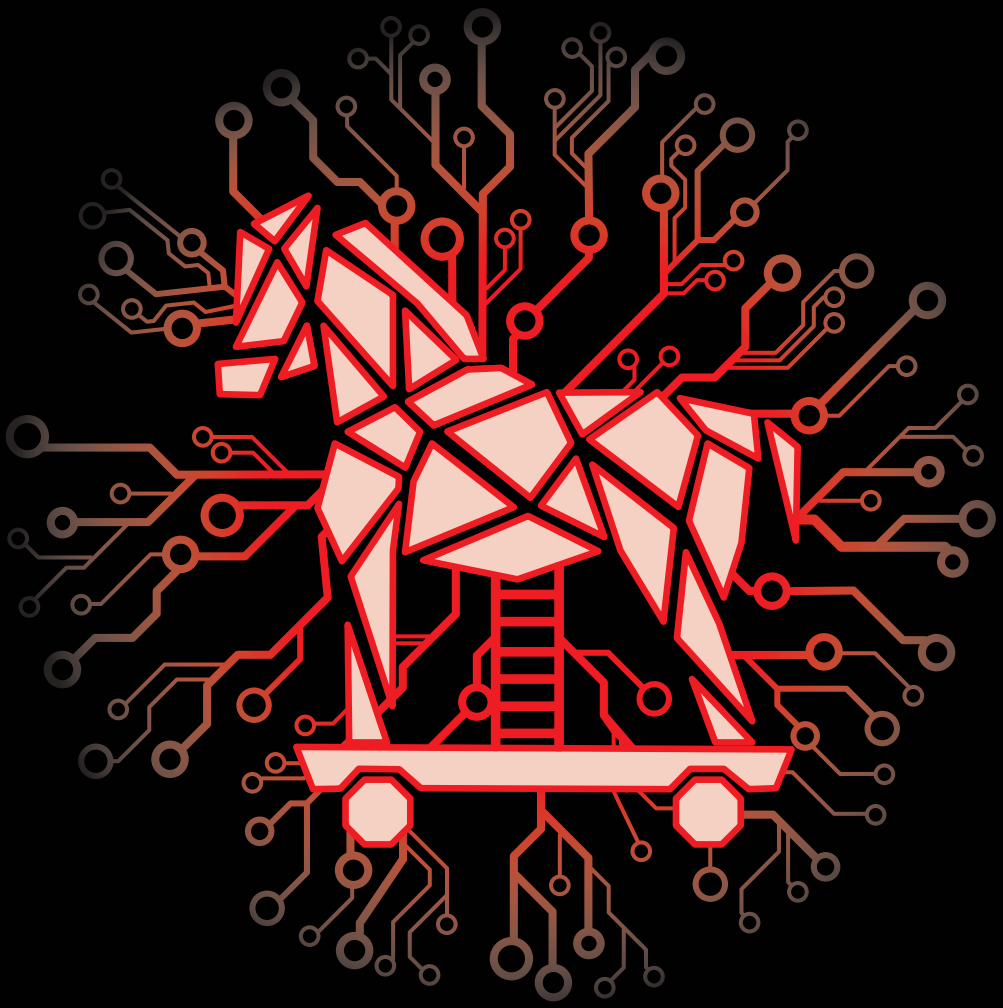
Deloitte.
デロイト トーマツ



Red Team Operations

組織レジリエンスの向上

デロイト トーマツ サイバー合同会社

はじめに

Red Teamとは、高度な攻撃に対する組織のレジリエンスを継続的に高めることを使命とするグループです。敵対者の立場で行動することによりRed Teamは組織内に存在するデジタル、物理的、および社会的な脆弱性を探り、リアルな状況下で経営陣や従業員の対応力を試します。このアプローチは、組織が効果的なセキュリティ対策を構築および実装するうえで大きな効果を発揮します。Red Teaming Operationsを通じて、組織は脅威を評価し、重要な資産を保護し、実際の攻撃に対処する能力を強化できます。

高官たちにとって懸念材料となるこれまでにない新たな情報を提供して欲しい。

George Tenet
米中央情報局（CIA）元長官

Red Teaming の歴史

Red Teamingは、数世紀にわたって発展してきた防御のためのアプローチです。その基本的なコンセプトは、攻撃側の立場に身を置くことで、敵についての理解を深め、新たな観点から効果的な対策を講じようというものです。 こうした手法をとることで、組織の弱点が明らかになり、また運用環境についての理解も深まります。この当初の目的は、とりわけ今日のサイバー分野において、今なお受け継がれています。

Red Teamingの技法は、19世紀のドイツで「War Gaming（戦争ゲーム）」の実践から派生したものです。War Gamingでは、時間的制約が厳しいなかで、事前に選択されたシナリオの分析を求められます。これは軍事紛争下での不測の事態（軍事衝突）に際して、より的確な指令を下せるようになることを目的とします。天候、地形、情報の欠落または誤り、兵站、配置された部隊の移動や効力など、さまざまな要因が当初の計画の成功に多大な影響を及ぼします。戦争ゲームの当初のセットアップはボードゲームで、リアルな地形ピースとゲームトークンを使用して、詳細なルールのもとで戦闘シーンのシミュレーションが行われていました。この当初の手法は、今日では一般的に「War Gaming」と呼ばれています。

その後「Red Teaming」という用語は、主に冷戦時代の米軍により、広く一般に知られるようになりました。米軍では「アグレッサー」と呼ばれる部隊が、ソ連軍の軍事作戦や行動をシミュレートするよう訓練されました。これはソ連軍にとってはごく当たり前の、しかしながら米軍にとっては不慣れな戦術、作戦行動、武器、さらには地形などに対する心構えを米軍兵士にさせることを目的とするものです。
さらに最近では、9月11日の同時多発テロ事件の翌日、当時のCIA長官であったGeorge Tenet氏が、「Red Cell」と呼ばれるCIA部隊の創設を指示する簡潔かつ異例の命令を出しました。このチームに与えられた使命は、意思決定者にとって懸念材料となる、これまでにない新たな情報を提供することです。この命令が異例と言われるのは、Tenet氏自身が、国家安全保障に関わる情報を入手して評価することを主な任務とする機関をすでに率いていたためです。衝撃的な事案の発生を受けて、Tenet氏は、型にはまった従来の考え方を抜本的かつ体系的にゆさぶり、予想外のテロ攻撃のリスクを最小限に抑える役割を担う新たなチームが必要であると考えました。

2011年に、英国のサイバーセキュリティセンター（GCHQ/MI5の一部）が英国サイバーセキュリティ戦略のためのガイドラインを発行しました。その後2013年にイングランド銀行が、このガイドラインに沿って、英国の金融機関のレジリエンスをテストするためRed Teams（CIAのレッドセルに相当）の構築を目的とするCBESTプログラムを立ち上げました。またオランダ中央銀行に牽引される形で、欧州中央銀行（ECB）も欧州の金融機関のレジリエンスをテストするためのTIBER（Threat Intelligence Based Ethical Red Teaming）を策定しました。さらにその後、中東およびアジアにおいても多くの当局で同様の取り組みが進んでいます。

これまでの歴史を通してRed Teamingは常に2つの目的で行われてきました。1つ目は攻撃者に利用される恐れがある新たな技法やアプローチの発見、そしてもう1つが、こうした攻撃の視覚化や対応能力の強化を目的とする防衛チームのトレーニングです。その最終目標は全体的なレジリエンスの向上であり、これはあらゆる時代、国家、およびビジネス環境にわたって共通のニーズです。

組織レジリエンスの向上

攻撃への備えがどれほど強固な組織であっても、脆弱性を完全に排除することはできません。セキュリティは永続的な状態ではなく、攻撃が成功するリスクは常に存在しています。そのため予防的な保護対策に加えて、組織レジリエンス、すなわち攻撃による影響が発生した場合にも、ビジネスプロセスを維持または復旧する能力が、企業のITおよびITセキュリティには強く求められます。

組織レジリエンスを向上させるためには、脅威を予測し、可能性の高い攻撃に備え、攻撃による影響から可能な限り迅速に回復して事業活動を再開し、さらに必要に応じて独自のセキュリティ対策を講じる能力が必要です。レジリエンスを高めるために、組織は以下のことを求められます。

- 既存の脅威に関する情報を適切な情報源から入手する。
- 入手した情報から正しい結論を導き出す。
- 意思決定の認知的側面および社会的側面の影響に留意する。
- 適切な技術的および組織的なセキュリティ対策を講じ、その長期的な有効性を確保する。

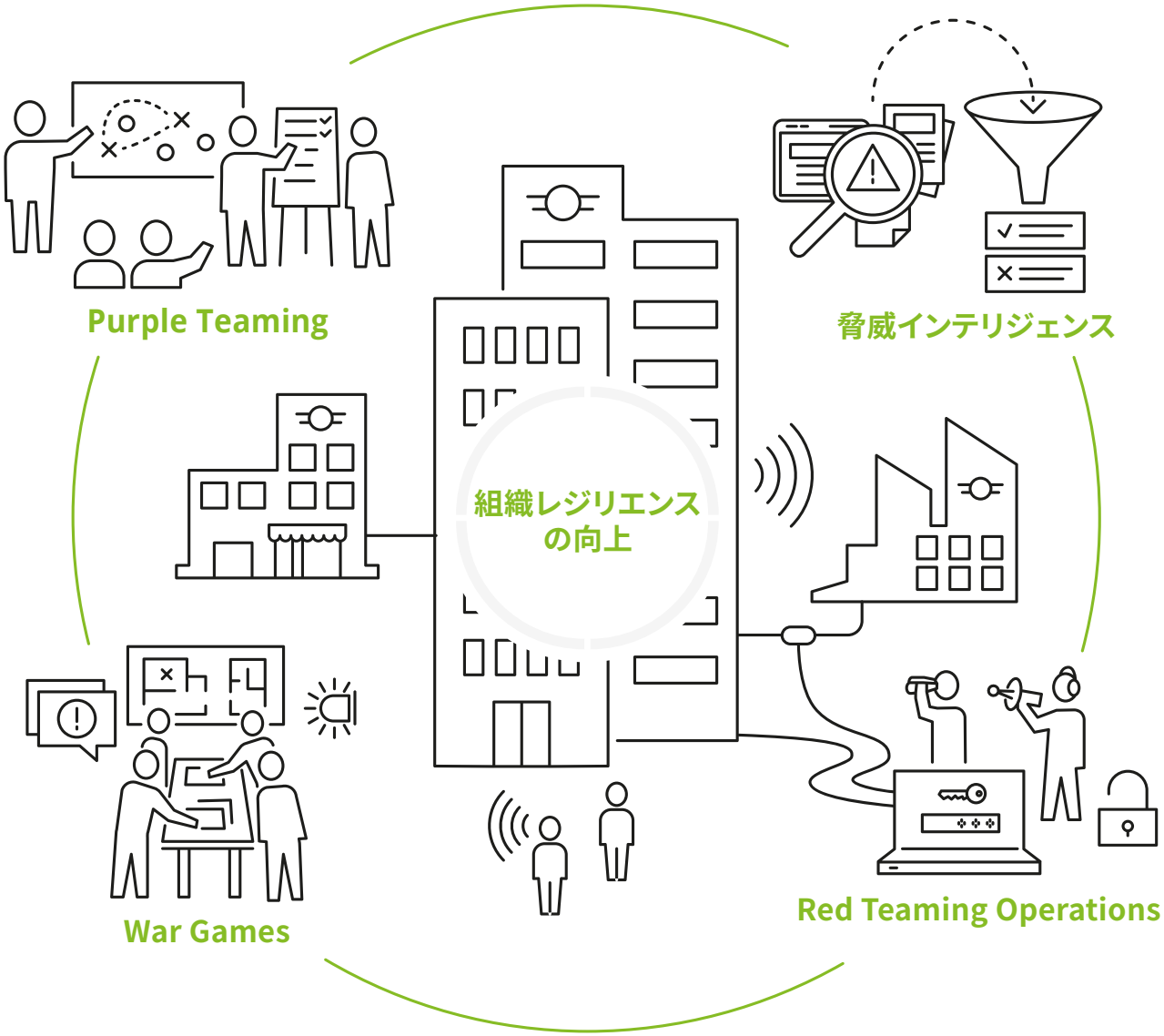
DeloitteはRed Teaming Operationsを通じて、組織によるこうした取り組みを支援しています。組織レジリエンスの現状についての共同アセスメントをはじめとして、Deloitteは以下のようなサービスの組み合わせを、組織のニーズに応じて提供可能です。

- リスクおよび想定される脅威に関する情報を継続的に提供。
- サイバー攻撃に対する組織レジリエンスを検証し、潜在的なリスクを評価するために、リアルなテストおよびシミュレーションを実行。
- 組織固有のニーズに応じて調整された改善プログラムを策定およびサポート。

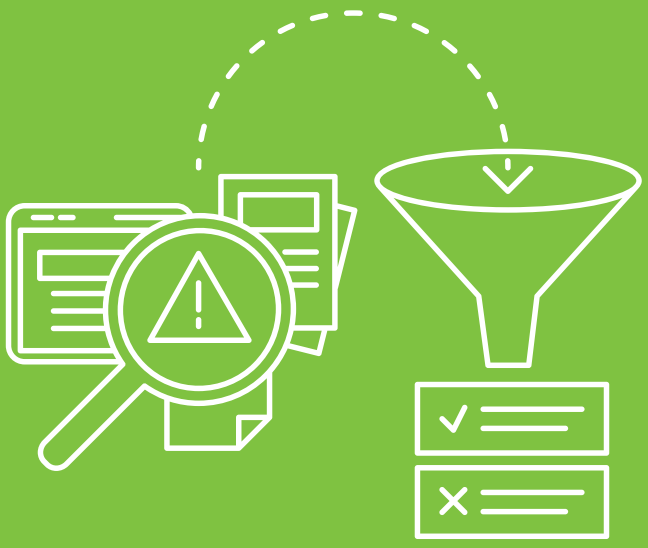
Deloitteは、敵対者の立場から組織の安全性を考察するという手法により、世界中のさまざまな組織のレジリエンスを向上させてきた実績を有します。デジタル時代を勝ち抜くために、今日の組織は高品質のサービスと将来を見据えた一貫性のあるアプローチを必要としています。

セキュリティは成果ではなく過程である。

Bruce Schneier



組織レジリエンスの向上に必要な 4 つの要素



脅威インテリジェンス

Red Teaming Operations

War Games

Purple Teaming

脅威インテリジェンス

既存の脅威について確実に理解することは、あらゆる組織におけるレジリエンスと適応性の向上の基礎となります。

「インテリジェンス」という用語は、軍事および情報サービス分野にその起源があり、特定の目的を達成するためのデータの収集、処理、および発信を意味します。

Deloitteでは、サイバー脅威インテリジェンスサービスとして、悪意のある行為者の意図、機会、能力などに関する情報を提供しています。ニーズに合わせて調整されたインテリジェンスは、組織がこうした脅威に対抗するうえで大きな効果を発揮します。サイバー脅威インテリジェンスで焦点となるのが、個々の組織に対する具体的なサイバー脅威の特定です。

インテリジェンス成果物は、組織のビジネス目標にマッピングされて、それらのインテリジェンスが組織に付加価値をもたらしているかどうかが判断されます。この分野における複雑かつ急速な進化についての正確な知識は、レジリエンスに重点を置いたあらゆる活動の基礎となります。Deloitteは、既存の脅威ランドスケープを全方位から考察し、効果的なアセスメントをクライアントに提供しています。目標となるのは、ニーズに合ったタイムリーかつ実用的なインテリジェンスを提供することにより組織が、より確かな意思決定を下し、リスクの軽減につなげることです。

サイバー脅威インテリジェンスサービスにおいては、2つの要素が重要になります。第1に基礎となる情報の品質と多様性、そして第2に（実際のインテリジェンスを生み出すための）継続的な情報かつ専門的な評価です。

そのためDeloitteでは非常に広範かつ多様な情報調達を行っています。このプロセスの中心となるのがオープンソースインテリジェンスで、その主な手法はインターネット上での適切な情報の探索です。自動検索エンジンを使用したアナリスト主導の高度な検索（検索範囲には、オープンWeb、ディープWeb、およびダークWebが明示的に包含されます）に加えて、Deloitteでは、とりわけ重要な点に関しては人のアナリストを使用しています。このようにDeloitteでは、各種のソフトウェアやツールを開発および使用し、機械学習アルゴリズムなどの革新的な技法を駆使することで、無数の一次情報源から関連性の高い情報を取得し、これを分類しています。

サイバー脅威インテリジェンスはクライアントの関与を常に必要とします。標準化されたセルフ アセスメントを社内開発したり、グローバルな脅威ランドスケープを把握したりすることに加えて、クライアントは、Deloitteのアナリストとのワークショップにおいて、想定される攻撃シナリオの計画および設計に参加します。攻撃シナリオは、クライアントの目標に照らして検証された統計分析に基づいて作成され、現在および将来の脅威ランドスケープの予測が反映されます。

Red Teaming Operations

Red Teaming作戦において、Deloitteは組織に対するリアルな攻撃をシミュレートして脆弱性の特定とその利用を試み、ビジネスクリティカルな資産にどのような悪影響を及ぼせるかを実証します。Red Teaming作戦の目的は組織のレジリエンスの検証です。

Red Teaming作戦は、脅威ランドスケープに関する事前の分析に基づき作成された攻撃シナリオに沿って実施されます。このシナリオに欠かせないのが、想定される攻撃者グループ、および各グループ固有の意図、専門知識、能力などに関する詳細な記述です。また攻撃シナリオには、攻撃が成功した場合に組織が被る悪影響を含めて、攻撃の目的が明記されます。

Red Teamingは、企業の資産を狙った攻撃に利用される恐れがある未知の脆弱性と攻撃ベクトルを特定し、それらを使用してプロセスの停止や機密データの不正入手を試みます。攻撃シナリオの作成および実行にあたり、DeloitteのRed Teamは、ファシリティ、ネットワーク、およびアプリケーションの物理的セキュリティの評価に加えて、人間を標的とする攻撃（ソーシャルエンジニアリングなど）の機会についての評価も行います。攻撃シナリオは、物理的な侵入戦術、ソーシャルエンジニアリング、ハッキング技法などで構成され、設定された目的をRed Teamが達成できるような形に、これらの要素が組み合わされます。とりわけ重要な手法を以下に示します。

- 従業員をだまして機密情報の開示や不適切なアクションを行わせて、彼らが意図せずにRed Teamの攻撃を支援するように仕向ける。
- 社屋を偵察し、立入禁止区域への侵入を可能にする、物理的セキュリティ境界またはプロセス内に存在する脆弱性を特定する。
- 適切なツールおよび技法を駆使してネットワークやアプリケーションに侵入し、その後標的となる資産に向かってラテラルムーブメントを開始する。

このようにRed Teaming作戦を通じて、シミュレートされたサイバー攻撃に対する組織の防御、検知、対応、および回復能力が評価され、またコントロールとプロセスが効果的に適用されているかどうかが検証されます。

Red Teaming作戦の開始前および最中に、Deloitteのコンサルタントが、クライアントとの入念な打ち合わせに基づき、個々のテストに適用すべき制限/制約事項を特定し、これを遵守します。

Deloitteが作成するテストレポートには、シミュレートされたサイバー攻撃の手法および攻撃経路についての説明が記載されます。またレジリエンスの向上に役立つ、人員（People）、プロセス（Process）、テクノロジー（Technology）についての観察結果および推奨事項に加えて、Red Teaming作戦によるビジネスインパクトの概要も示されます。

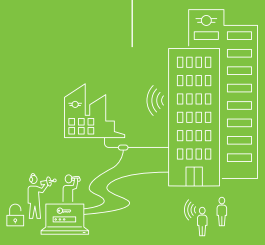
脅威インテリジェンス

Red Teaming Operations

War Games

Purple Teaming

脅威インテリジェンス



Red Teaming Operations

War Games

Purple Teaming

War Games

War Gamesは、組織の応答性を試すことを目的とするシナリオベースのシミュレーションです。この演習において、企業の危機管理チームのメンバーは、シミュレートされたリアルな危機的状況のもと、自身の戦略、計画、スキルなどを実地に応用し、結果を検証する機会を与えられます。

企業危機は破壊的かつ多面的な影響を及ぼす事象であり、あらゆる組織を不意打ちします。過去の事例から明らかなとおり、的を絞った迅速な行動をとることで、危機の持続時間および影響を大幅に軽減することが可能です。十分にリハーサルを積んだ、効率的で自信に満ちた危機管理チームは、レジリエントな組織の基盤となります。適切な対応能力を育成および維持するためには、必要なプロセスや手順を事前に設計および文書化することに加えて、関係者の定期的な訓練が欠かせません。

DeloitteのWar Gamesのフレームワークを使用することで、危機管理チームは安全な学習環境内で、危機的状況に備えた訓練を積むことができます。演習の範囲とシナリオは、クライアントのニーズと能力に合わせて、最適な成果が得られるように設計されます。

適切なシナリオを選択する際に重要な判断基準となるのが、Deloitteのインテリジェンスサービスによって決定される各シナリオの発生確率です。このような方法を採ることで、組織はニーズに最適なシナリオのもと、ガイダンスに従って内部コンピテンシーを向上させることが可能になります。すなわち組織は、発生する可能性が高い危機への対応力をシミュレーションを通じて強化できます。

企業危機は予測が難しく、その内容も多岐にわたるため、War Gamesでは特定のケースを事前にテストすることよりも、危機的状況に効果的に対処するために必要なフレームワークと前提条件を提供することに重点が置かれています。

緊迫した状況下でとるべき行動パターンを確立するには、事前のリハーサルが必要であり、それに最適なのがWar Gamesです。危機管理チームによる反応は、DeloitteのRed Teaming側の新たな反応を引き起こし、このようにして2つのチーム間で戦いのシミュレーションが繰り広げられます。

アクティブな参加者があらゆる状況に対応できるかどうかは、組織のレジリエンスの直接的な指標となります。

Purple Teaming

Purple Teamingでは、探知側（Blue Team）と攻撃側（Red Team）双方の能力強化に重点が置かれます。Blue Teamは、Red Teamの活動を探知しようとし、それに対してRed Teamは可能な限り秘かに行動することを目指します。

People（人）、Process（プロセス）、Technology（テクノロジー）に関するセキュリティコントロールの全体的な有効性を評価するには、Red Teaming作戦を実施するのが最も効果的です。検証すべき重要なポイントの1つが、組織のセキュリティオペレーションセンター（SOC）の有効性で、SOCアナリストが、Red Teamを検知できるかどうかが評価されます。敵の検知という結果にはさまざまな要因が影響するため、その評価は簡単ではありません。

SOCは人間の免疫システムになぞらえることができ、似たような状況を以前に経験していれば、サイバー攻撃を速やかに検知できます。その反対に、SOCアナリストにとって未知の攻撃者であったり、同種の攻撃を以前に分析したことがなかったりする場合は、攻撃の検知はほぼ不可能です。Purple Teamingは、3つのフェーズを通じて、このギャップを解消できるように設計されています。

あらゆる演習には準備が欠かせませんが、Purple Teamingも例外ではありません。この演習では、Deloitteのチームがクライアントのインフラストラクチャ内で、可能であればSOCチームに通知することなくRed Teaming作戦を実施し、必要な侵害指標（IOC）を取得します。
このフェーズの目標は、悪意のある行為者に利用される恐れがある攻撃経路の発見です。Red Teamは実行したすべてのステップを詳細に記録し、これらの記録は第2フェーズで使用されます。

SOCは第2フェーズから参加し、この時点で、実行されたRed Teaming作戦の内容と使用された攻撃経路を知らされます。これを受けてSOCはRed Teamが使用した攻撃手法を自身が検知できた（または検知できなかった）理由を探るための取り組みを開始します。
またDeloitteのBlue Teamingスペシャリストが、攻撃手法を検知する方法について、追加のコンテキストを提供します。データソースが存在し、保持されているデータ量が十分な場合は、Deloitteのスペシャリストがクライアントによる IOCの発見をサポートするとともに、概要レベルのユースケースの設計を支援し、広い視野に立ってIOCを特定できるようにアドバイスを提供します。

第3フェーズでは、同じ経路と手法による攻撃がRed Teamによって再び実行されます。このシナリオは最初に実行されたシナリオとよく似ていますが、最も有益な結果が得られるように、第2フェーズで得られた成果に基づき特定の制限要素を迂回して実施されます。
言うまでもなく、SOCはこの攻撃が行われることを承知していますが、インシデントへの対応が可能な限り自然なものとなるように、攻撃が発生する正確なタイミングは知らされません。この演習により、SOCの検知能力がどの程度向上したかについて追加の情報が得られます。このフェーズでは検知された内容に加えて、あらゆる改善点が評価されます。また検知できた可能性がありながら見逃されたすべての攻撃手法が調査され、改善策が提示されます。必要な調整が小規模の場合は、現行のRed Teamingメンバーが攻撃を再び実行し、結果の検証に必要な新たなデータを生成します。

脅威インテリジェンス

Red Teaming Operations

War Games

Purple Teaming

脅威インテリジェンス主導の Red Teaming

急速に拡大しているセキュリティ問題は、個々の企業だけでなく、各国政府、欧州連合、およびその他の国際機関にとっても重大な関心事となっています。

2013年に、英国の金融政策委員会が財務省に対して、財務省および規制当局が英国の主要な金融システムおよびインフラストラクチャプロバイダーと協力して、高度なサイバー攻撃に対するレジリエンスをテストするためのフレームワーク（CBEST）を構築するよう勧告しました。同委員会によるこの勧告は、継続的な警戒や運用レジリエンスを強化するための投資によって攻撃に対抗する責務があることを、金融機関やインフラストラクチャプロバイダーの経営幹部に認識させることを目的とします。これ以降、他の国際当局も同様のアプローチを採用しており、例えばECBではTIBER-EUフレームワークが採用されています。

脅威インテリジェンス主導のRed Team Operationsは、通常、同様のアプローチで行われます。

一般的脅威ランドスケープフェーズ
（オプションの）一般的脅威ランドスケープ（GLT）フェーズでは、国内金融セクターの脅威ランドスケープについてのアセスメントが実施されます。このフェーズには、関連性が高い攻撃主体を、その主体固有の手法、戦術、および手順（TTP: Techniques, Tactics and Procedures）とともに特定する作業も含まれます。この情報は、後続のステージで攻撃シナリオを作成する際のベースとなります。新たな攻撃主体やTTPが登場して、組織にリスクをもたらす可能性があるため、一般的脅威ランドスケープは通常、継続的に更新されます。

準備フェーズ
このフェーズでは、インテリジェンス主導のテスト計画が正式に始動し、テストの管理責任を負うチームが設立されます。またテストの範囲が組織の取締役会によって決定、承認、および保証され、関係当局によって検証されます。最後にテストを実施するために、脅威インテリジェンスおよびRed Teamのプロバイダーが調達されます。

テストフェーズ
テストフェーズでは、脅威インテリジェンスとRed Teamによるテストが行われます。脅威インテリジェンスプロバイダーが、組織のために的を絞った脅威インテリジェンス（TTI: Targeted Threat Intelligence）レポートを作成し、テスト用の脅威シナリオをまとめます。次にRed Teamプロバイダーが TTIレポートを使用して攻撃シナリオを作成し、指定されたクリティカルな本稼働システム、人員、およびプロセスをターゲットとする、インテリジェンス主導のRed Teaming作戦を実施します。

終了フェーズ
終了フェーズでは改善計画の作成と結果の共有が行われます。Red Teamプロバイダーが Red Teamingテストレポートのドラフト版を作成します。このレポートでは、テストで使用された手法の詳細、およびテストを通じて発見および観察された事項が報告されます。必要に応じて、レポートには技術的なコントロール、ポリシーと手順、教育と意識の向上などの観点から、改善の余地がある領域についての助言も記載されます。組織は明らかになった事項を確認し、監督機関などとも協議のうえで最終的な改善計画を策定します。

脅威インテリジェンス主導のRed Teamingがもたらすメリット:

- 確かな知識とスキルを保有し、金融サービスセクターにも精通した、有能なサイバー脅威インテリジェンスアナリストによって作成される、先進的かつ詳細なサイバー脅威インテリジェンス
- 的を絞った最新のサイバー脅威インテリジェンスに基づき、巧妙かつ先進的な攻撃をシミュレートするリアルな侵入テスト
- 技術的に難しいテスト活動を、ダメージやリスクを引き起こすことなく実行できる、熟練した侵入テスト担当者
- サイバー攻撃の検知/対応能力に関する組織の成熟度評価に役立つ標準的な主要業績評価指標（KPI）
- 金融サービス業界のその他の領域の評価に役立つベンチマーク情報（KPI）
- スペシャリスト集団によって管理される、包括的かつ強制力のある有意義な行動規範を基盤とするフレームワーク

脅威インテリジェンス主導のRed Teamingプロセス

* TI/RT: Thread Intelligence (脅威インテリジェンス)/Red Team

以下に示すようなフレームワークが、業種や地域が異なるさまざまな機関によってすでに実装されています。

CBEST

CBESTは、2013年に英国の金融当局（イングランド銀行（BoE）、英国財務省、および金融行動監視機構）によって、適切に制御およびカスタマイズされたインテリジェンス主導のサイバーセキュリティテストを提供するためのフレームワークとして導入されました。このテストでは、政府および民間のインテリジェンスプロバイダーにより、システム上重要な金融機関にとって真の脅威であると評価された攻撃主体の行動が模倣されます。CBESTは、金融サービスセクターで行われている他のセキュリティテストとは異なり、脅威インテリジェンスをベースとし、制約が少なく、クリティカルなシステムや必須のサービスに対する巧妙かつ持続的な攻撃に重点が置かれています。具体的なサイバー脅威インテリジェンスを取り込むことで、進化する脅威ランドスケープを可能な限り忠実に再現した有意義なテストが可能になります。この単一のテストによって人員、プロセス、およびテクノロジーを検証することで、金融サービスまたはインフラストラクチャプロバイダーのサイバー能力を総合的に評価できます。

GBEST

GBESTはCBESTモデルをベースとする新しいスキームで、さまざまな英国政府機関にわたって展開されています。このスキームの目的はCBESTとよく似ていますが、若干の相違点があり、例えばGBESTアセスメントに要する時間は平均的なCBESTよりも多少長めになると予想されます。
全体的なスキームは内閣府によって調整され、国家サイバーセキュリティセンター（NCSC）により脅威インテリジェンスの検証および一般的な技術アシュアランスが提供されます。個々の演習については、その演習を実施する政府部門が調達および主導し、最終的な責任を負います。

TBEST

2016年から2017年にかけて、CRESTは文化・メディア・スポーツ省（DCMS）および情報通信庁（OFCOM）と広範囲にわたって連携して、TBESTスキームを立ち上げました。このプログラムの作成にあたっては、CRESTが電気通信セクターのニーズに合わせてCBESTスキームの現実的な調整を行う役割を担いました。

iCAST

香港金融管理局（HKMA）は、香港の認可機関（AI: Authorized Institution）のサイバーレジリエンスを向上させる目的で、サイバー強化イニシアチブ（CFI）を策定しました。CFIの中核となる3つの要素が、(i) サイバーレジリエンスアセスメントフレームワーク（C-RAF）、(ii) サイバーインテリジェンス共有プラットフォーム、および (iii) プロフェッショナル育成プログラム（PDP）です。

CBESTの場合と同様に、iCASTのもと、脅威インテリジェンスによって従来の侵入テストが補完されて、エンドツーエンドのテストシナリオ（攻撃の開始から事前に設定されたテスト目的の達成まで）が作成されます。これによりテスト担当者は、高度な敵対者による攻撃をよりリアルにシミュレートできるようなります。さらにiCASTアセスメントでは、こうした攻撃の検知および対応に関するAIの能力の評価に役立つKPIも提供されます。

「中級」または「上級」の成熟度を目指すAIは、「成熟度アセスメント」プロセスにおいてiCASTを実施する必要があります。

TIBER-EU

2018年5月、欧州中央銀行（ECB）は、脅威インテリジェンスベースの倫理的Red Teamingのためのフレームワーク（TIBER-EU）を採択しました。

TIBER-EUは、欧州および各国の機関、ならびに金融（およびその他の）業界に所属する組織が、Red Teamの支援のもと、既存のシステムの脆弱性をテストし、複雑なサイバー攻撃に対するレジリエンスを向上させるための共通フレームワークを提供します。このフレームワークは、制御およびカスタマイズされたインテリジェンスベースのRed Teaming Operationsに依存しています。このシミュレートされた攻撃によって、クリティカルな機能およびそれを支える基盤、すなわち人員、プロセス、およびテクノロジーの安全性が持続的に検証および強化されます。

欧州連合の各国は、国内市場でも同じフレームワークを採用するよう推奨されており、オランダではTIBER-NLが、ベルギーではTIBER-BEがすでに導入されています。

Global Red Teaming

DeloitteのメンバーファームによるGlobal Red Teamには、さまざまな領域、および世界中のあらゆる地域にわたる経験と知識を有する専門家が結集しています。

この分野横断的なチームは、サイバーセキュリティ専門家、エコノミスト、コンピューターサイエンティスト、インテリジェンスアナリスト、元武官、犯罪学者など、多方面の専門家で構成されています。Deloitteのプロフェッショナルは国や大陸を越えて活動しており、必要とされる言語や文化的コンテキストに応じて、ローカライズされたアプローチを提供可能です。

Red Teamingは、脅威インテリジェンスの領域における卓越した分析/調査スキル、War Gamingにおける軍と市民のシミュレーションに必要な広範囲にわたる実践的な戦略と戦術的経験など、Red Teamingの中核となる4つの要素に欠かせない特性をすべて備えています。また創造性や先見性に優れており、Red Teamingテストに関する経験も豊富で、さらに検知やインシデント対応機能の実装に必要な業界固有の知識に加えて、Purple Teamingに関する広範なスキルも保有しています。

Red Teamの活動は、サイバーインテリジェンスセンター（CIC）のグローバルネットワークが提供する確かなテクノロジーとコンピテンシーによって支えられています。そのため包括的な観点から、想定される脅威シナリオやレジリエンス戦略について考察することが可能です。

Red Teamは活動を継続的に最適化するために、全世界のプロフェッショナルで構成される広範なDeloitteネットワークを活用しています。このグローバルなコラボレーションにより、Deloitteはクリエイティブなソリューションを全世界のお客様に迅速に提供することが可能です。

Deloitteはお客様に最適なサポートを提供可能です。DeloitteではRed Team Operationsを通じて組織レジリエンスの向上を体系的にサポートするため、以下の3つの手順を実施します。

1

対面形式のミーティングで、Deloitteのプロフェッショナルが Red Team Operationsサービスの詳細をお客様に直接説明します。さらに構造化されたインタビューを通じて組織の現状が調査され、現在のセキュリティコンセプト、プロセス、およびテクノロジーが、セキュリティリスク、セキュリティトレーニングの状況、教育手段などと併せて分析されます。

2

手順1で得られた情報に基づき、改善機会についての協議が行われます。また特定された活動分野に対処するためのカスタマイズされた提案が作成されます。

3

組織レジリエンスを向上させるために、Deloitteの脅威インテリジェンス、Red Team Operations, War Gaming, Purple Teaming サービスが、お客様のニーズに合わせて継続的に展開されます。

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 アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（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リー合同会社、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、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に1万名以上の専門家を擁し、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）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバル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れらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

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リー、リスクアドバイザリー、税務およびこれらに関連する第一級のサービスを全世界で行っています。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Fortune Global 500®の8割の企業に対してサービス提供をしています。“Making an impact that matters”を自らの使命とするデロイトの約286,000名の専門家については、（www.deloitte.com）をご覧ください。

2019.12