NRI SECURE

Internet Week 2019

D2-3 組織を更に強くする「攻めの」サイバー攻撃対策

攻撃と防御の協力で態勢強化（Purple Teaming）

2019年11月27日

NRIセキュアテクノロジーズ株式会社

大塚　淳平

出演者紹介

猪野 裕司（株式会社リクルートテクノロジーズ）

河村 辰也 (Sansan株式会社)

洲崎 俊(三井物産セキュアディレクション株式会社)

北原 憲(株式会社ラック)

上野 宣(株式会社トライコーダ 代表取締役)

大塚 淳平 (NRIセキュアテクノロジーズ株式会社) ※モデレータ兼前半講演

大塚　淳平（Otsuka, Jumpei）

- **所属：ＮＲＩセキュアテクノロジーズ株式会社**
- **主な経験：攻撃技術・不正アクセス技術を活かし、対応力強化支援**
  （脆弱性診断・侵入テスト、インシデント対応支援、脆弱性管理支援など）
- **プロジェクト実績：**

  金融機関向け脅威ベースのペネトレーションテスト、インフラ事業者向けペネトレーションテスト、脆弱性管理運用支援（コンサル）など
- **委員、講演など：**

  ISOG-J 脆弱性診断士WG
  IPA 情報セキュリティ10大脅威 選考委員

  FISC TLPT手引書　検討部会　委員
  東京工業大学 情報理工学院 特定准教授
  産業技術高等専門学校 客員准教授、他、講演など

テーマ

関係者限

BlueTeamの皆さまがセキュリティ態勢強化をするための一助

ペネトレーションテストの効果を最大化するためにRedTeamと連携する考え方をご紹介（Purple Teaming）

実務者の声、事例から具体的にイメージする

ペネトレーションテストで見かけた"穴"

- 穴だらけの社内システム
  （古いOS、古いアプリ、脆弱な設定、運用上の不備、など）
- 人の脆弱性
  （脆弱なパスワード、運用上の不備、メールは開いてしまう、など）
- 組織としての対応
  （一部しか攻撃が検出できない、気付けたが対応しきれない、など）

依然として“穴”は残っている

- ”穴”は残り続けている
- 対策が難しい理由は？

ご支援時に出会った例　※あくまで例です

- 対策費用が膨大で進められない
- どこから対策すべきか判断が難しい
- 報告内容が正直わからない
- 業務アプリへの影響により社内から責められる
- 運用上の都合で進められない
- 社内ネットワークへの侵入リスクの想定が甘い

せっかく明らかにしたリスクが置き去りに・・・？

- リスクは分かったけど対策は数年後
- 予算の都合で暫定対策も難しい
- 対策できていないから来年度はペネトレもやらない

※様々な例を組み合わせた後の展開を個人的に想像したものです


このような時に活用するのが
Purple Teaming

RedTeam と BlueTeam　役割の確認

 Red	 Blue
セキュリティ施策を 攻撃者目線で確認	攻撃者による影響から組織を守る 製品の品質確保、維持
セキュリティ診断 ペネトレーションテスト システム監査	CSIRT インシデントレスポンス セキュリティ監視 ネットワーク監視

Red vs Blue

RedTeam と BlueTeam　役割の確認

Red

Blue

どちらも
組織のサイバーレジリエンスを向上するために活動

セキュリティ診断
ペネトレーションテスト
システム監査

CSIRT
インシデントレスポンス
セキュリティ監視
ネットワーク監視

Purple Teaming とは？

- RedとBlueを協力させるためのコンセプト

Purple Teaming とは？

RedとBlueを協力させるためのコンセプト

必ずしも「チーム」ではない
（チーム化してもよい）

実現するためには

相手の立場に立って考える（橋渡しするチームがいてもよい）

・対策、レスポンスへの理解
・対象組織についての理解
（業務上の制限、意思決定プロセスなど）
・攻撃観点や情報をBlueと共有

・攻撃者が使うテクニックの理解（TTPs）
・テストへの協力（改善活動として）
・対策、改善内容をRedと共有

対策推進時のためにRed（攻撃）を理解する

攻撃者が使うテクニックの理解（TTPs）

- ✓ 攻撃手法を駆使して攻略されるケースを読み解く
- ✓ ログ等の痕跡から攻撃を検知できるようになる
- ✓ 新しい攻撃をシグネチャ化する能力の向上

テスト（診断、ペネトレ）への協力

- ✓ どこを攻撃されたらまずいのかは、Blue Teamが詳しい
- ✓ より効果的な対象（よりやばい対象）をターゲットにする等

対策、改善内容をRedと共有

- ✓ Redから見て困る対策＝有効な対策

Redは外部委託しているので・・・

Redをより自分たちに近づける

・情報共有は対象や禁止事項の指定など必要最小限
・実施後に結果を受領、報告会などで活動完了

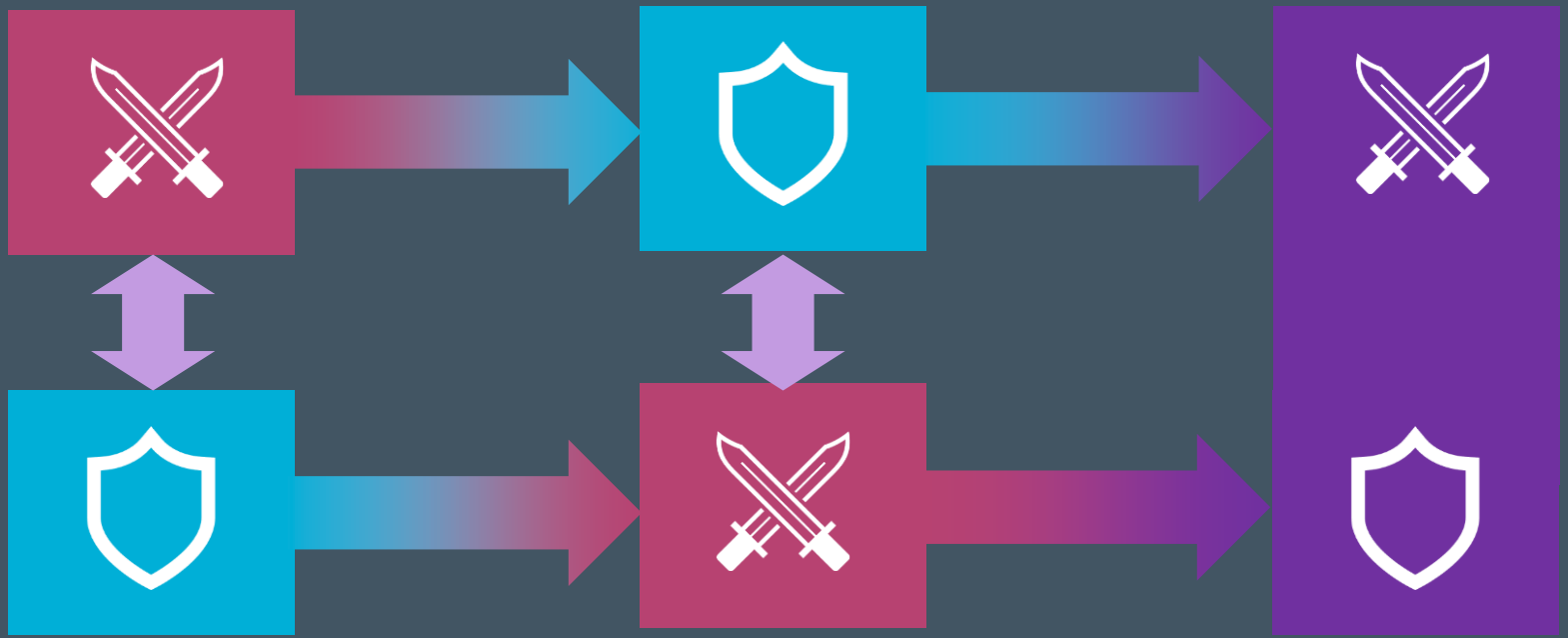
効果　第三者評価としてのセキュリティレベルチェック

・セキュリティ対策状況などを踏まえ実施内容を相談
・実施後の対策を共有し、今後の取り組み内容を相談

効果　セキュリティレベル向上を目的としたテストの実施

実現するために

弊社事例（人的交流）



トレーニングからのアプローチ

- Attack & Difenseの観点・技術を学ぶ
- SANS SEC599
  Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses

  https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses

実際にこのような考え方は使えるものなのか
それぞれの実務者から聞いてみましょう

パネリスト紹介

猪野 裕司（株式会社リクルートテクノロジーズ）

河村 辰也 (Sansan株式会社)

洲崎 俊(三井物産セキュアディレクション株式会社)

北原 憲(株式会社ラック)

上野 宣(株式会社トライコーダ 代表取締役)

大塚 淳平 (NRIセキュアテクノロジーズ株式会社）※モデレータ兼

関係者限

テーマ

- 参加いただいた皆様が、Purple Teamingの考え方を活かすための一助として、以下のテーマで対談

ペネトレーションテストでの
Red、Blueの協力とは？

Purple Teamingを進めるときに
困ったこと、対策例

会場の皆様から募集　※随時

ペネトレーションテストで
Red、Blueが協力した効果は？

- 数年間、1つのペネトレーションテスト提供企業と協力しながら、テストとセキュリティ対策を進めたことで効果を実感
  - ペネトレーションテストは、前回（前年）の結果を踏まえて、前提条件（一定のアカウントを掌握しているなど）、実施範囲や目標を決定
  - RedとBlueで協力し、視点を変えながらペネトレーションテストに取り組めたことによって、検知能力向上など効果が出た実感があった
  - ペネトレーションテスト提供企業の選定は、内部の重要情報を知られる可能性があるのでNDAで縛るのはもちろん、経営層への安心材料として、テストで取得できてしまった重要情報を漏洩させることが割に合わない人（情報漏洩させるメリットよりもデメリットの方が大きい人）を選定した（最初の選定時）。
- Blueは日常業務に加え、社内調整などが必要で大変だが、Redと協力してなるべく円滑に
  - ペネトレーションテストの受け入れ側（Blue）に、Redのことを理解した方がいたので調整が円滑に進んだ（社内に必要な準備や想定影響、対応方法の説明ができた）
  - Redの活動を理解いただくために、テスト実施時にどのように攻撃するかなどを解説しながら実行するケースもある
- BlueからRedに過去のペネトレーションテストの取り組みや気になる点（自社の弱点と思わしき点）を共有することで、効果的なテストを実現
- REDは攻撃が成功したら嬉しい（成功）と思われがちではあるが、対策が十分に施され、攻略できなかった（攻撃が成功しなかった）場合でも安全な企業と出会えて嬉しい（良い対策事例に出会えた）

Purple Teamingを進めるときに困ったこと、対策例

- 既に認知されている問題（脆弱性）がRedから報告されてきていた
  - 制約上対策ができない問題のみに注目されてしまうと、想定していた効果が得られない
  - 問題が存在していることの確認と問題を利用して何ができるのかは分けて考えた方が良い
  - 既に認知されている問題がある場合は、Redへ共有し、攻撃者によって問題を悪用された際の影響リスクも調査対象とすることでペンテストの効果を高めることができる
- スコープが固まり（狭まり）すぎていて、テスト中に攻撃条件が成立しないケースがある（実施後に想定を置いてリスクを想定する必要がある）
  - あまりに厳しい条件では、実施に時間を要することも（限られた期間で実施するため十分なテストにならない可能性）
- テスト中にテストであるのか、本当の攻撃や不審者であるのか、判断しづらいことがあった、テスト時には告知してもよいが、本当の攻撃・不審者への対応も考慮する必要がある
- 経営層にセキュリティ対策の必要性を理解いただくため、クライシスコミュニケーション研修（記者会見などを体験する研修）を実施

ご参加いただいた方からのご質問

Question	Answer
Red Teamとして活動する時に有用な攻撃情報収集先やフリーツールがあれば教えてください。（現在グループ内の会社向けに1人RedTeamとして活動しています。）	MITRE ATT&CKを参考にシナリオを作成し、カバー範囲を広げていくのがいいのではないでしょうか。
ペネトレーションテストの内製化を検討されたことがありますか？	回答A：ペネトレーションテストの内製化（Red Teamの構築）は検討しています。費用の関係で、長期間テストするというのがなかなか難しいのと、Redの技術を持った人間が社内にいれば、インシデント対応能力（Blueの能力）も向上すると考えているからです。
	回答B：内製Red Teamよりも、シフトレフトをおすすめします。セキュリティエンジニアがシステム開発チームへ合流、もしくはシステム開発チームをセキュリティチームへ受け入れることにより、製品企画、システム開発段階において脆弱性を作り込まない体制を構築することで永続的な効果が得ることができます。 また、ペンテストは知識があるだけで実施できる簡単なものではありません。知識があるだけのペンテストで検出できるものはそもそも委託する必要ないです。品質面を考慮すると外部に委託するほうがよいと考えています。
BLUEから見たペネトレーションテストの理想的な実施頻度を教えてください（コスト、体制は考慮せず理想的な頻度が知りたいです。）	回答A：組織の拡大や業務内容の変化によって理想的な実施頻度は変わると思いますが、3ヶ月～半年に1回程度実施できるとよいと思っています。
	回答B：テストの実施頻度をあげるよりも、テスト結果をしっかりと咀嚼して、セキュリティレベルをあげることが重要だと考えています。対策せずに毎年同じ問題が発見されている状態では、定期的にペンテストを実施してもリスクを低減するという本来の目的を達成できないため、頻度を上げても効果が得られません。

※パネルメンバーで分担して回答しています。各個人の見解です。

ご参加いただいた方からのご質問

Question	Answer
ペネトレーションテストの実施調整時にシステム運用部門とBLUEチーム間では、打ち合わせなどでどの程度のコミュニケーションをとるのでしょうか？	ペンテストは自社のシステムのリスクを軽減することが目的です。 何度もペンテストを実施している状況において最適なテストを行うためには、業務やシステムを理解しているBlue Teamがテスト計画を策定することをおすすめします。 コミュニケーションについては、 計画策定では、ベンダーと会話しながら期間、対象、目的などを企画し、それらを運用チームに対して説明して承認をとります。 実施の承認が得られた後は、円滑なテスト実施にむけ、ベンダーのリクエストに応じて環境の準備を調整します。 その中では、下記のような打合せを実施することになります。 ・ステークホルダー打ち合わせ （承認関連：単発、運用チーム：計画説明、実施内容合意など要所） ・ベンダー打ち合わせ （テスト計画、準備、テスト内容のフィージビリティ確認など、ペンテストを円滑に実施するため打合せ、頻度高め） なお、計画（スコープ、レギュレーション、目的）、準備（人員手配、場所手配）、実行（周知、テスト進捗管理など）に加え、一般的なプロジェクト管理のタスクもBlue Teamにて実施しています。テスト実施の際も、実施対象の運用チームに連絡し、どのようなログが出力されるのか、影響を受ける可能性があるシステムがどこなのかを周知するようにしています。

※パネルメンバーで分担して回答しています。各個人の見解です。

ご参加いただいた方からのご質問

Question	Answer
ペネトレーションテストを実施すれば、脆弱性診断は必要無いのでしょうか？	ペネトレーションテストと脆弱性診断では実施目的が異なるため、どちらも実施する必要があります。
ペネトレーションテスト実施中に意図していない機密情報や不正行為を発見してしまった場合はどのように対応していますか？	不正や侵害を発見した場合には、基本的にはお客様の担当者に報告します。機密情報などに関しては、会社同士の契約に秘密保持（NDA）が含まれているのと、ペンテスターや診断士自身がプロとして倫理観を持つべきだと思います。
ペネトレーションテストにより、システムの停止や破壊など影響が出たケースはありますか？	あります。そのため、テスト実施時には、対象システムの運用部門と密にコミュニケーション（テストの実施、終了などを連絡）し、影響が発生した際にはすぐに対応できるようにしています。（そして、菓子折りを持って運用部門に謝りに行きます。）
ペネトレーションテスト実施時に「制限のある本番系へのペネトレーションテスト」と「制限の無いステージング系へのペネトレーションテスト」どちらが有効ですか？	理想論ですが、制限のない本番へのテストが有効だと考えています。これを前提として、自社環境ではどちらが有効であるかを検討されるのがよいのではないでしょうか。
クライシスコミュニケーション研修を実施するための説得方法が知りたい	検討時点で経営層のセキュリティへの意識が比較的高かったというのもあります。Blue Teamとして実施したことは、広報や法務などの他部門と連携し、複数方面から声を上げました。

※パネルメンバーで分担して回答しています。各個人の見解です。

ご参加いただいた方からのご質問

Question	Answer
セキュリティに興味がない社員に興味を持たせる方法についてアドバイスがあれば知りたい（興味を持ってくれる人を集めるのが理想であるが会社の都合もあるため…）	社内で興味を持つ人を探した方が良いです。もしマネージャの立場である場合は、会社都合を変えられるような働きかけをされるとよいのかと思います。
ペネトレーションテストを長年同じ企業に依頼する場合、気のゆるみなどにより必要なサービスが提供されない不安があるのですが・・・	自社でテスト計画を策定することで、不安を解消できるのではないでしょうか。
Blue Team、PurpleTeamの活動をする中で楽しいこと、面白いこと、やりがいなどモチベーションに繋がることについて教えてください。（”仕事なので”は除く）	セキュリティ対応支援した方々からの感謝はもちろんのこと、ネット系証券会社様から以下のようにセキュリティでSansan（法人向けサービス）を選んだと言ってくださるお客様がいることが大きなやりがいにつながっています。 https://sin.sansan.com/stories/suf17/
セキュリティホールが存在していることを認識している状態で、そのシステムに対してペネトレーションテストを行う意味はあると思われますか？	攻撃による最大の影響を見るという意味では、結果が得られるのではないでしょうか。
RedTeamを外部委託している場合に、PurpleTeamingも実施するには相応のコストがかかるのでしょうか？（高そうです。。。	Purple Teamingを実践する際には、Redを委託している中で、受け入れる側としてBlueとRedが連携するための実施内容の理解やBlueとの打ち合わせを増やしていただくことになるため、お客さん側でも対応コストが増加すると思われます。もしRedの委託先に追加の対応を依頼する場合には、相応のコストも必要です。

※パネルメンバーで分担して回答しています。各個人の見解です。

ご参加いただいた方からのご質問

Question	Answer
Red Teamを外部委託する場合に評価する基準などはありますか？	知合いへ依頼しています。敢えて評価する点を挙げると、ペンテスターが報告したCVE番号、チームメンバーの経歴（BoB卒業やDefconCTFの上位入賞）など、スキルがわかりやすい実績を確認しています。
ペネトレーションテストを海外ベンダーにお願いすることもあるのでしょうか？	海外ベンダに依頼することもあります。実力がすべてです。
海外では Bug Bounty Program が徐々に普及していますが、活用は検討されましたか？	活用を検討しました。実現するには、Blueとしても相応のコストがかかるため、少ないBlue Teamのリソースの優先順位という観点から、もう少し先にしようと判断しています。

※パネルメンバーで分担して回答しています。各個人の見解です。

最後に一言

- Redの出番は多くの企業で年に1回で外部企業から、Blueの出番は毎日
- Blueは、セキュリティの観点で事業リスクを低減する役割を担っており重要な役割
- Blueの業務は地味であるが、一歩一歩、前進させることが重要
- 経営層にリスクを的確に理解してもらい、対策を進めるためには攻撃者の視点も重要
- 診断やペネトレーションテストを実施して終わりではなく、セキュリティ対策も一緒に取り組めると効果が最大化される
- Red vs Blueではなく協力を！

Purple Teamingで
サイバーレジリエンスを更に強化