Tokio Marine Holdings

To Be a Good Company

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

攻撃者をあぶり出せ！！
プロアクティブなセキュリティアプローチ

2019年11月27日

東京海上ホールディングス株式会社
IT企画部　リスク管理グループ
石川 朝久, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP

D2-3 組織を更に強くする「攻めの」サイバー攻撃対策

1）攻撃者をあぶり出せ！！プロアクティブなセキュリティアプローチ

- 時間：16:15 ~ 17:05
- 講演者：石川　朝久（東京海上ホールディングス株式会社）

⇒ **最近のプロアクティブなセキュリティ戦略について、国内外の動向を紹介する。**

2）攻撃者の脅威となりうるThreat Huntingのアプローチとは

- 時間：17:05 ~ 17:40
- 講演者：加藤 義登 氏（SecureWorks Japan 株式会社）

⇒ **プロアクティブ・アプローチの代表格である、Threat Huntingを掘り下げる。**

3）攻撃と防御の協力で態勢強化(Purple Teaming)

- 時間：17:45 ~ 18:45
- 講演者：大塚氏、猪野氏、洲崎氏、上野氏、北原氏、河村氏

⇒ **各組織のBlue Teamは、Red Teamをどう活用していくか、聞く。**

はじめに：

今日のテーマとお話したいこと

- **テーマ：**セキュリティアプローチの“新陳代謝”
  - プロアクティブに攻撃者に対処する、２つのセキュリティ・アプローチが存在し、今後重要になってくると考えられる。
  - 本講演では、当該アプローチを紹介するとともに、具体的な技術・プロセスについて、国内外の事例をもとに紹介する。

- **アジェンダ：**
  - 1. “Active Defense” アプローチ
    - 1-1：Threat Hunting
    - 1-2：TLPT
  - 2. “Think in Graph” アプローチ
  - 3. まとめ

はじめに：講演者紹介

石川　朝久（ISHIKAWA, Tomohisa）

- **所属　：東京海上ホールディングス株式会社　IT企画部　リスク管理グループ**
- **専門　：不正アクセス技術・インシデント対応・グローバルセキュリティ戦略 etc.**
- **資格　：**博士（工学）, CISSP, CSSLP, CISA, CISM, CFE, PMP
  GIACs（GSEC, GSNA, GPEN, GWAPT, GXPN, GREM, GCIH, GCFA, GWEB）
- **経歴　：**
  - 2009.04 – 2019.03　：某セキュリティ企業
    - 侵入テスト・インシデント対応・脆弱性管理・セキュア開発、セキュリティ教育 etc.
    - １年間、米国金融機関セキュリティチームに所属した経験あり
  - 2019.04 – 現在　　：東京海上ホールディングス株式会社
    - 国内外グループ企業のセキュリティ支援、CSIRT運用、グローバルセキュリティ戦略 etc.
- **対外活動（抜粋）：**
  - DEFCON 24 SE Village Speaker (2016)
  - Internet Week 2018 (2018)
  - IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）
  - オライリー社『インテリジェンス駆動型インシデントレスポンス』翻訳・監訳
    ⇒現在も、別の本を翻訳中！こうご期待！

はじめに：

注意：

- 本プレゼンテーションの内容は、全て講演者個人の見解であり、所属企業、部門の見解を代表するものではありません。

- 講演の内容については、講演者の研究、グループ会社などの取り組みなどを参考にしながら作成しています。

- 製品名・ベンダー名などが登場しますが、講演者にて実効性・有効性を評価したり、推奨しているわけではありません。利用については各組織にて判断をお願いします。

1. “Active Defense”アプローチ

現状の分析

- 検知/対応が、難しい時代になっている。
  - **理由１）正規ビジネスでも使われるプログラム・サービスの悪用**
    - 例）PowerShell・Domain Fronting …
  - **理由２）開発され続けるEvasion Technique**
    - 例）Veil-Evasion（Veil Framework）、Invoke-Obfustication
  - **理由３）環境の多様化 + 守りづらい環境**
    - **今：クラウド・外部APIの活用など、環境の多様化**
      - ペリメータモデルが通用しない世界へ。

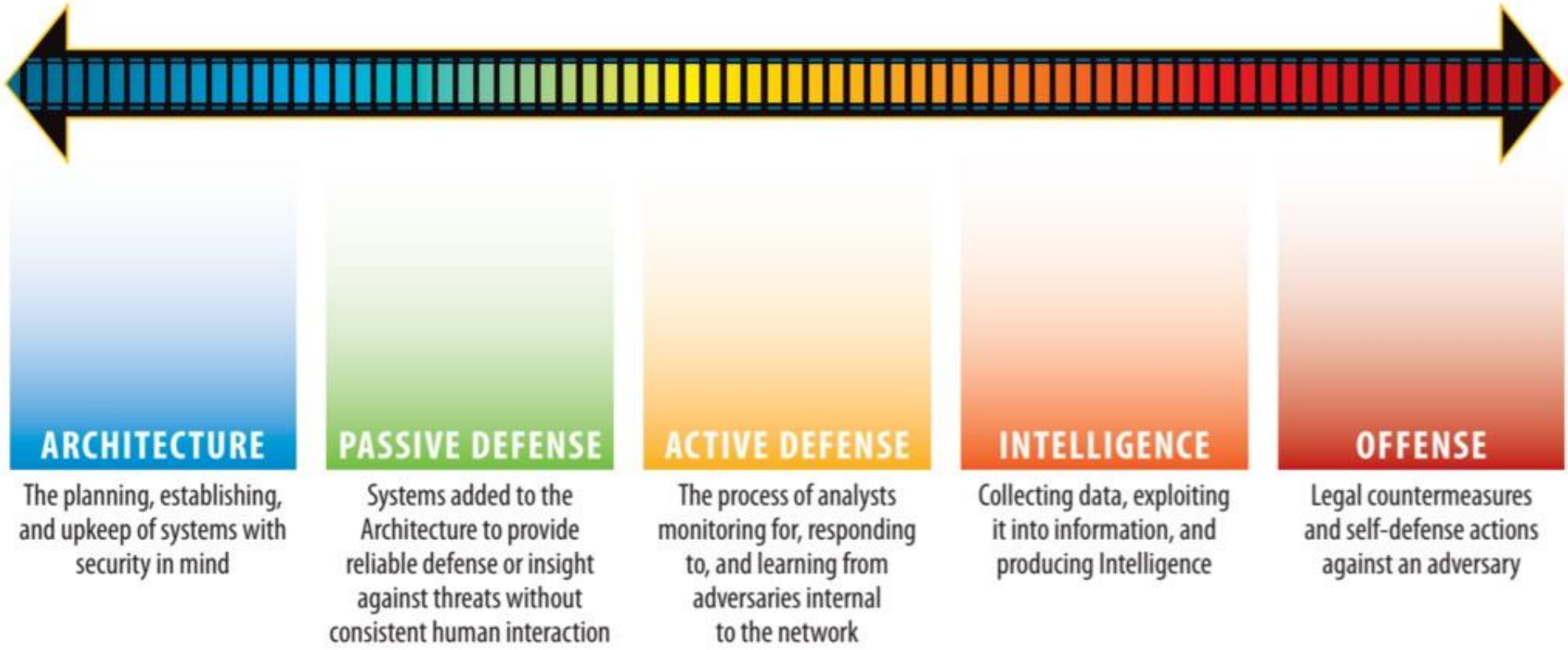
⇒ 攻撃の検知を（シグニチャなど）ゼロ・イチ判定に頼れない状況になりつつある。

⇒ 常に「不確実性のある検知」に対応する必要がある。

⇒ 脅威がセキュリティ製品に取り込まれるまでの期間（Zero-Day）をどう対処するかが課題！！

Sliding Scale of Cybersecurity

- **Sliding Scale of Cybersecurity：サイバーセキュリティ態勢の成熟度モデル**
  - SANS InstructorのRobert M. Leeにより、2015年に提唱されたモデル



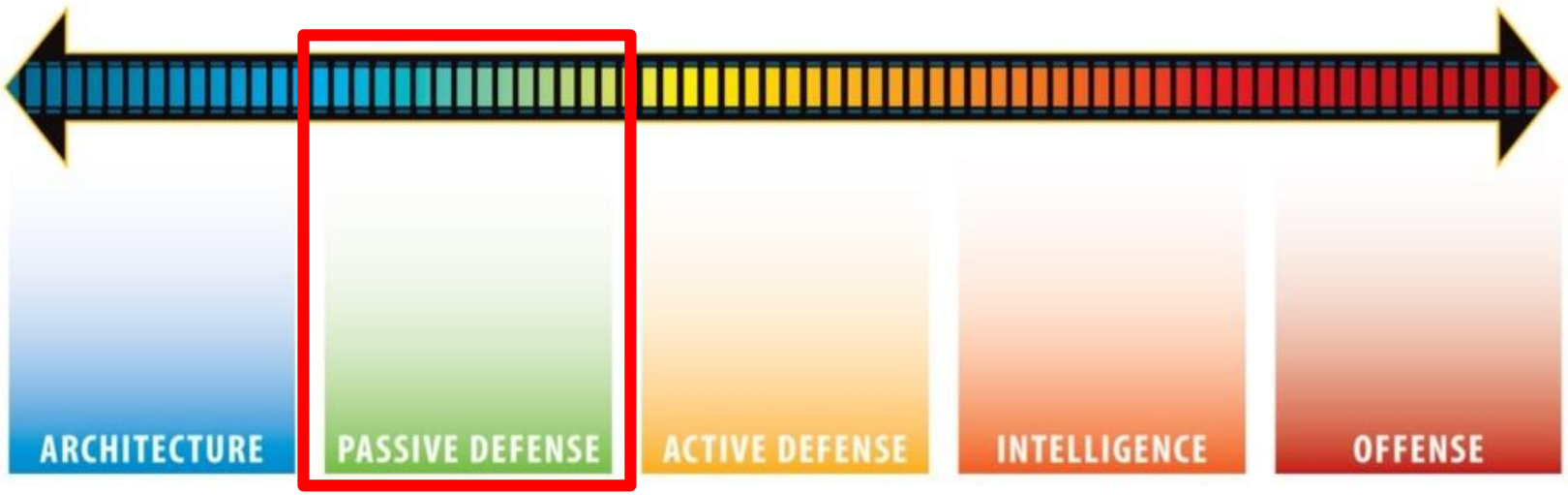
The Sliding Scale of Cyber Security (SANS) : https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Sliding Scale of Cybersecurity

- **Sliding Scale of Cybersecurity：サイバーセキュリティ態勢の成熟度モデル**
  - **Architecture**
    - セキュリティを念頭にシステム計画・構築・維持を行う態勢があること

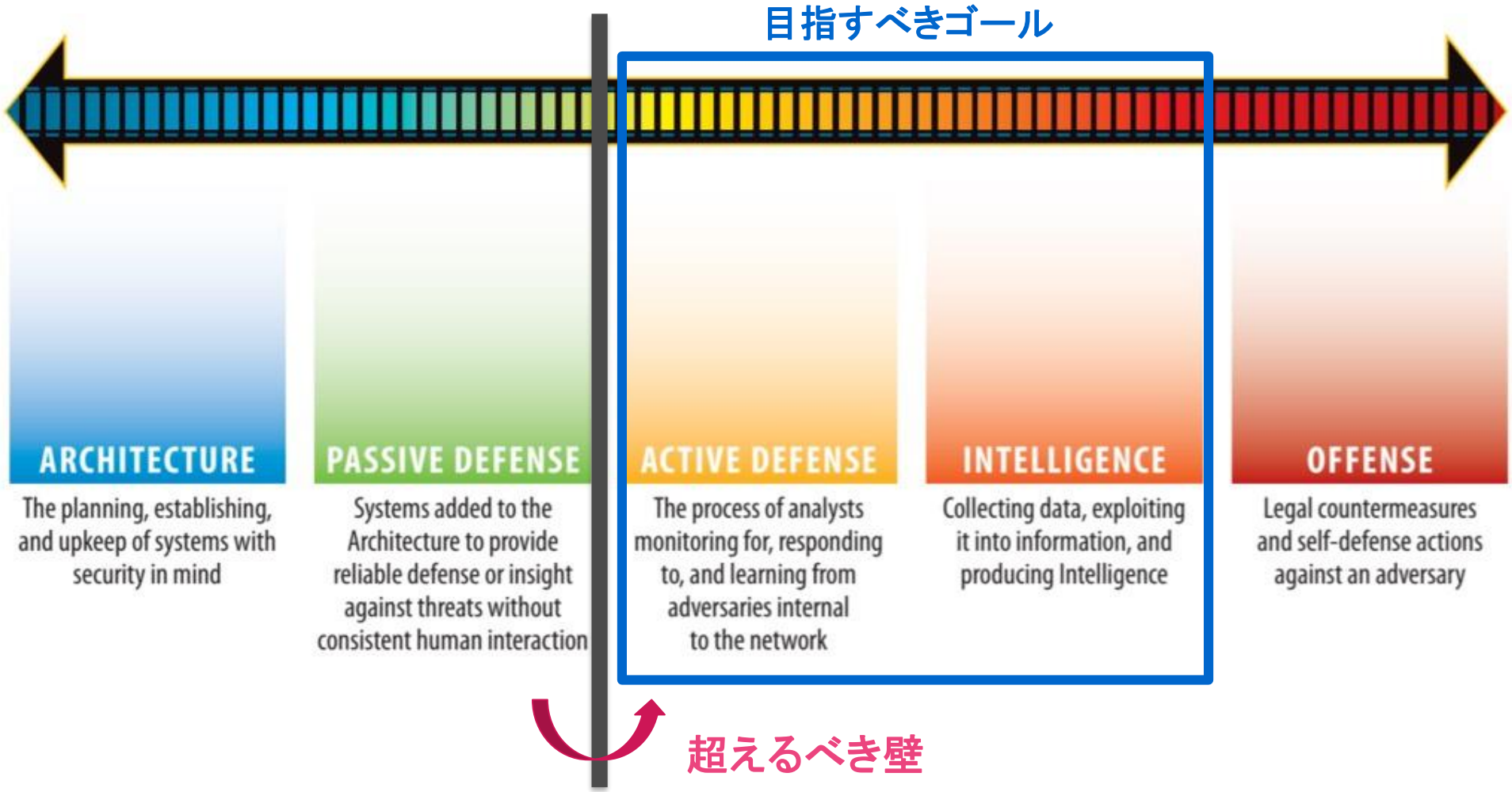
    ⇒ Cyber Hygiene（サイバー公衆衛生）
  - **Passive Defense**
    - 人が継続的に関与せず、一貫性のある防御メカニズムを有している状態

    ⇒ シグニチャベース（+一部の振る舞い検知）の検知・対応



Sliding Scale of Cybersecurity

- **Sliding Scale of Cybersecurity：サイバーセキュリティ態勢の成熟度モデル**
  - SANS InstructorのRobert M. Leeにより、2015年に提唱されたモデル

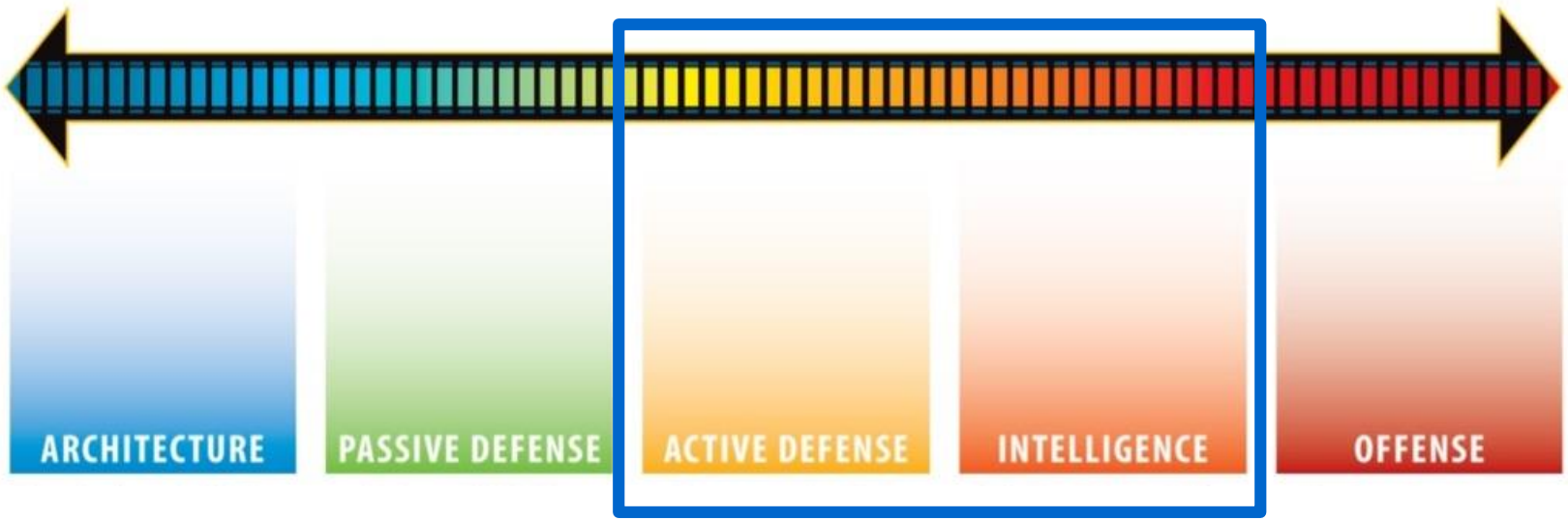


Sliding Scale of Cybersecurity – Active Defense

- **Sliding Scale of Cybersecurity：サイバーセキュリティ態勢の成熟度モデル**
  - **Active Defense**
    - 防御側が、ネットワーク内部に潜む**脅威**を監視・対応し、同時に、**攻撃者**から学び、自分の知識を応用するプロセス

    ⇒ **「脅威ベースのアプローチ」へのシフト**

  - **Intelligence**
    - **Active Defense** + 脅威インテリジェンスの活用・生成



Active Defenseを実現する方法

- 防御側がActive Defenseを実現する方法：３種類に分類される。
    - **振る舞い検知・脅威インテリジェンス・脅威ハンティング**

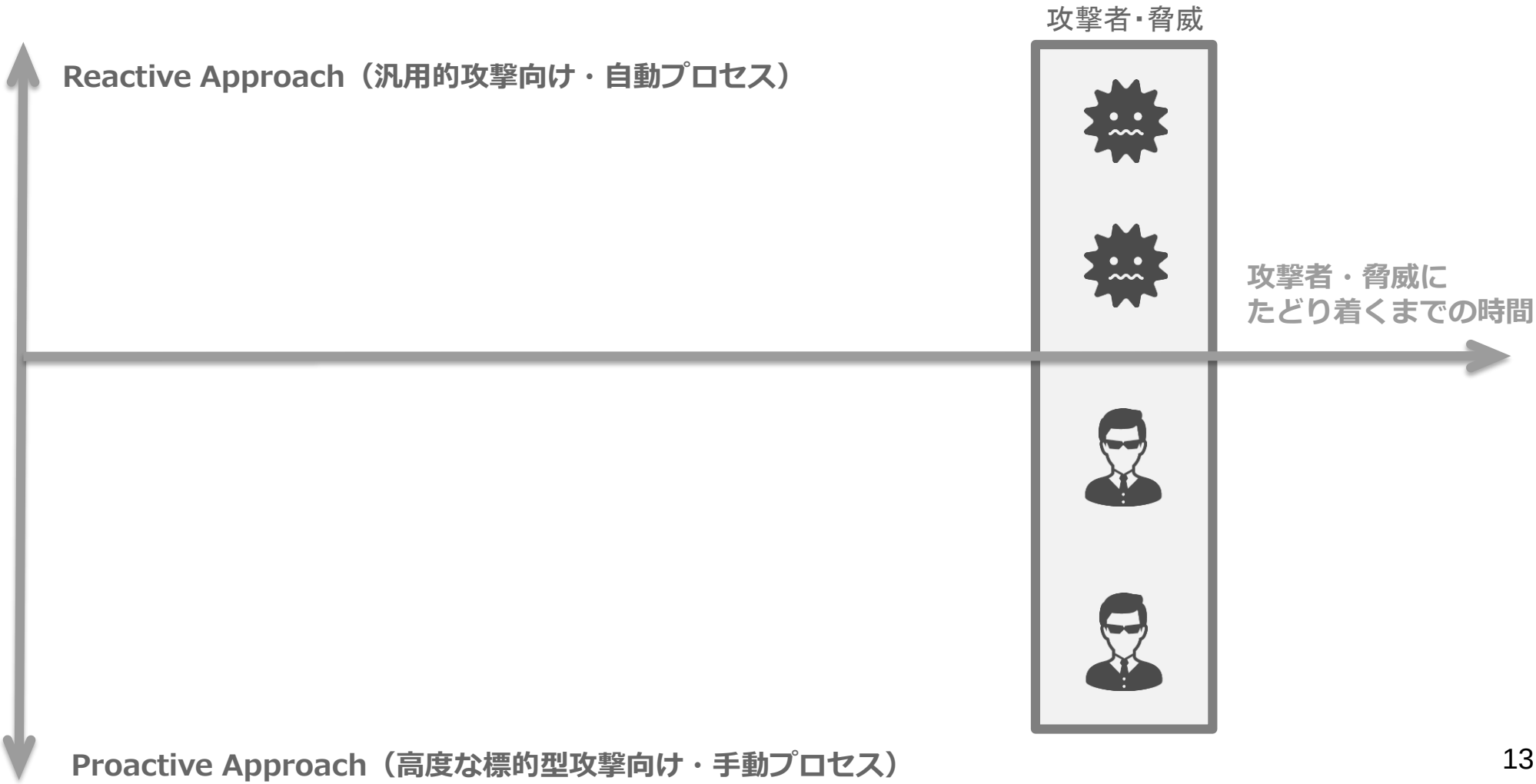
＜登場する重要キーワード＞

- **IOC（Indicator of Compromise・侵害指標）**
    - 既知の脅威・攻撃手法を特定するための技術的特性情報
    - 例）ハッシュ値、IPアドレス、ドメイン名、ホスト上に残る痕跡

- **脅威インテリジェンス**
    - 攻撃者・脅威の防止・検知に利用できる情報の総称

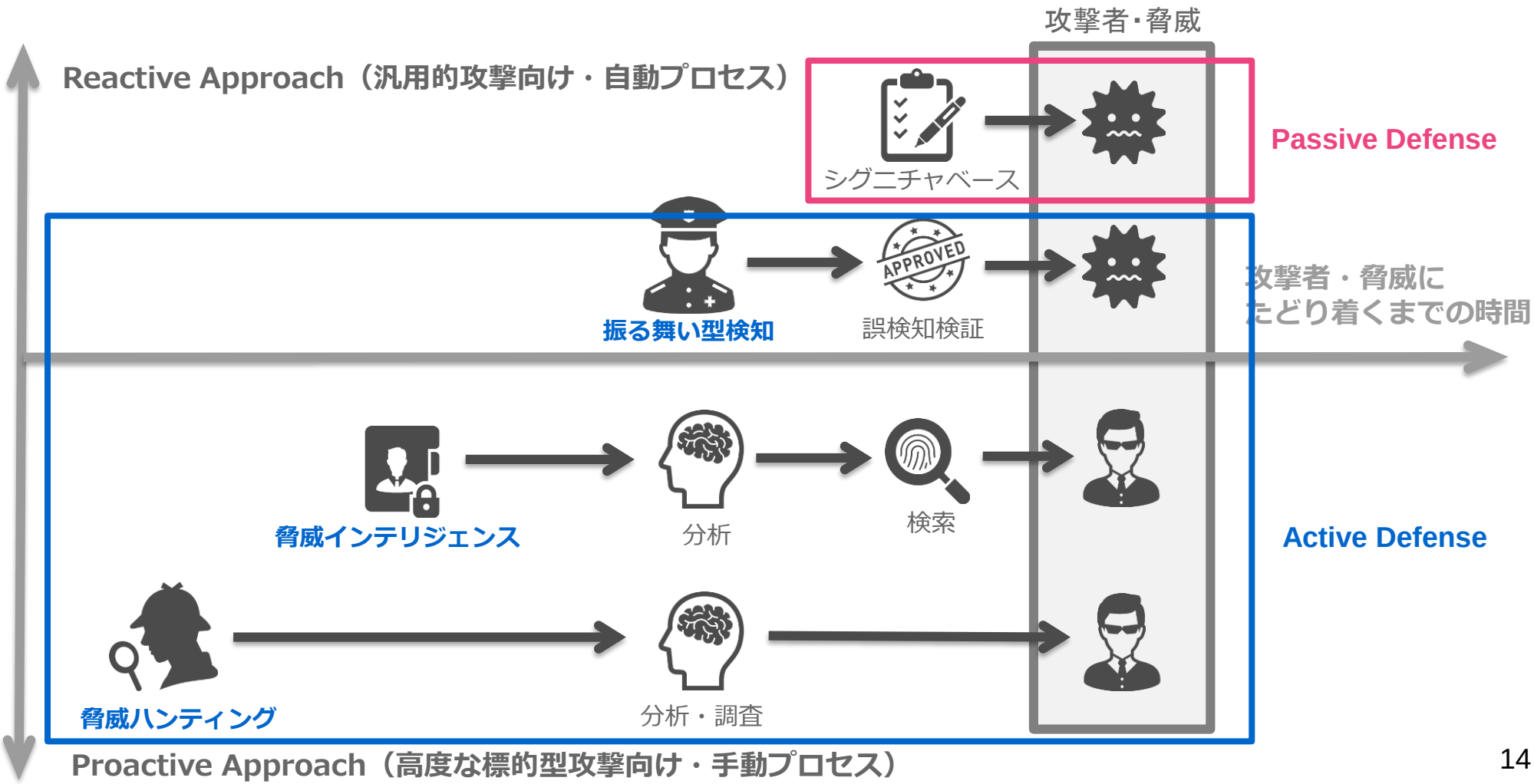
Active Defenseを実現する方法

- 防御側がActive Defenseを実現する方法：３種類に分類される。
  - 振る舞い検知・脅威インテリジェンス・脅威ハンティング



Active Defenseを実現する方法

- 防御側がActive Defenseを実現する方法：３種類に分類される。
  - 振る舞い検知・脅威インテリジェンス・脅威ハンティング



Active Defenseの成熟度を高めるアプローチ

成熟度の高いActive Defenseを実現するアプローチ２つをご紹介！

- **脅威ハンティング（Threat Hunting）　⇒ Blue Team**
  - 脅威インテリジェンスや各種情報を活用しながら、未知の攻撃者・脅威を見つけ出す手法

  ⇒ この講演は理論編。具体的事例は２番目のセッションで！

- **TLPT（Threat-Lead Penetration Test）　⇒ Red Team**
  - Active Defenseの有効性を検証を行う手法

  ⇒（この会場に多くいると思われる）防御側の担当者が、どのようにRed TeamやTLPTを活用するかについては３番目のセッションで！

1-1：脅威ハンティング（Threat Hunting）

脅威ハンティング（Threat Hunting）

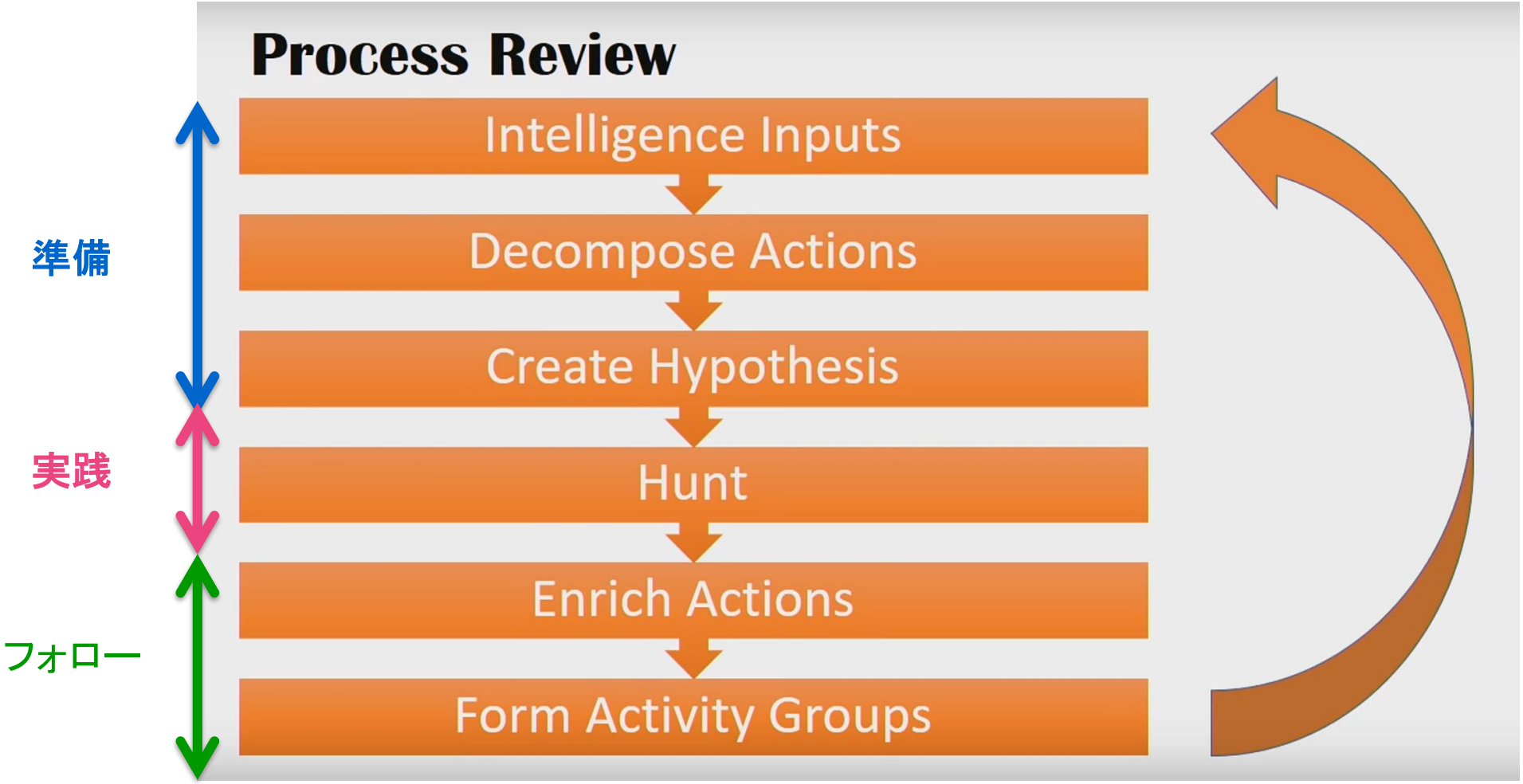
Sqrrl社による定義（現在：Amazonにより買収）

- 既存のセキュリティ対策を回避する**高度な脅威を検知・隔離**するため、（Blue Teamが）**能動的・再帰的にネットワーク内を探索するプロセス**

- **プロセスモデル：どのように脅威ハンティングを実施するか？**
  - Sqrrl社 : Hunting Loop
  - Carbon Black社 : The Carbon Black Hunt Chain
  - CyberReason社 : Threat Hunting 8 Steps
  - SANS Institute : SANS Threat Hunting Model
  - **SANS Institute : Intelligence Driven Threat Hunting**

Intelligence Driven Threat Hunting

- **Proposed in SANS CTI Summit 2018 by Keith Gilbert**



Intelligent Hunting: Using Threat Intelligence to Guide Your Hunts : https://www.youtube.com/watch?v=-QlaOX5w8G8

Intelligence Driven Threat Hunting（準備）

Step 1：Intelligence Input (脅威インテリジェンスの入手)

⇒ 脅威インテリジェンス（攻撃者・脅威の防止・検知に利用できる情報）を入手し、脅威ハンティングのネタ・手がかりを入手

- **外部ソース（Open）**
  - （無償の）ベンダーレポートやブログ
  - （無償の）脅威インテリジェンス情報
- **外部ソース（Closed）**
  - （有償の）脅威インテリジェンスベンダー
  - 情報コミュニティ（ISAC・InfraGard …）
- **内部ソース**
  - 各種アラート
  - ベースラインとの差異
  - ユーザからの通報

Intelligence Driven Threat Hunting（準備）

Step 2 : Decompose Action（アクションの分解）

⇒ 脅威インテリジェンスを読み解き、検証可能な単位に分解するフェーズ

- 例）どんな攻撃手法・ツールを利用するのか？
- 例）どんなIOCが提供されているのか？

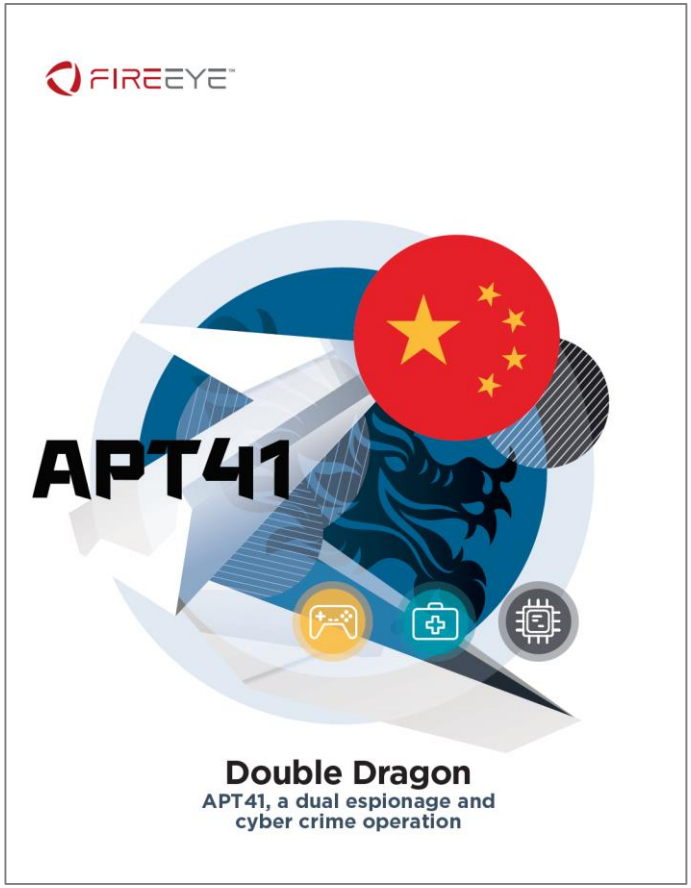
Step 3 : Create Hypothesis（仮説構築）

⇒ 闇雲に探すのではなく **（検証可能な）仮説 → 検証** の流れが重要！！

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis

⇒ 例）ベンダーレポートを脅威インテリジェンスのインプットとする場合



TECHNICAL ANNEX

APT41 IOCs

Table 16. CRACKSHOT

File MD5	File SHA1	File SHA256
04fb0ccf3ef309b1cd587f609ab0e81e	44260a1dfd92922a621124640015160e621f32d5	993d14d00b1463519fea78ca65d8529663f487cd76b67b3fd35440bcdf7a8e31
0b2e07205245697a749e422238f9f785	dde82093decde6371eb852a5e9a1aa4acf3b56ba	049a2d4d54c511b16f8bc33dae670736bf938c3542f2342192ad877ab38a7b5d
272537bbd2a8e2a2c3938dc31f0d2461	a045939f53c5ad2c0f7368b082aa7b0bd7b116da	d00b3edc3fe688fa035f1b919ef6e8f451a9c2197ef83d9bac3fa3af5e752243
dd792f9185860e1464b4346254b2101b	a260dcf193e747cee49ae83568eea6c04bf93cb3	7096f1fdefa15065283a0b7928d1ab97923688c7974f98a33c94de214c675567
fcfab508663d9ce519b51f767e902806	8272c1f41f7c223316c0d78bd3bd5744e25c2e9f	c667c9b2b9741247a56fcf0deebb4dc52b9ab4c0da6d9cdaba5461a5e2c86e0c

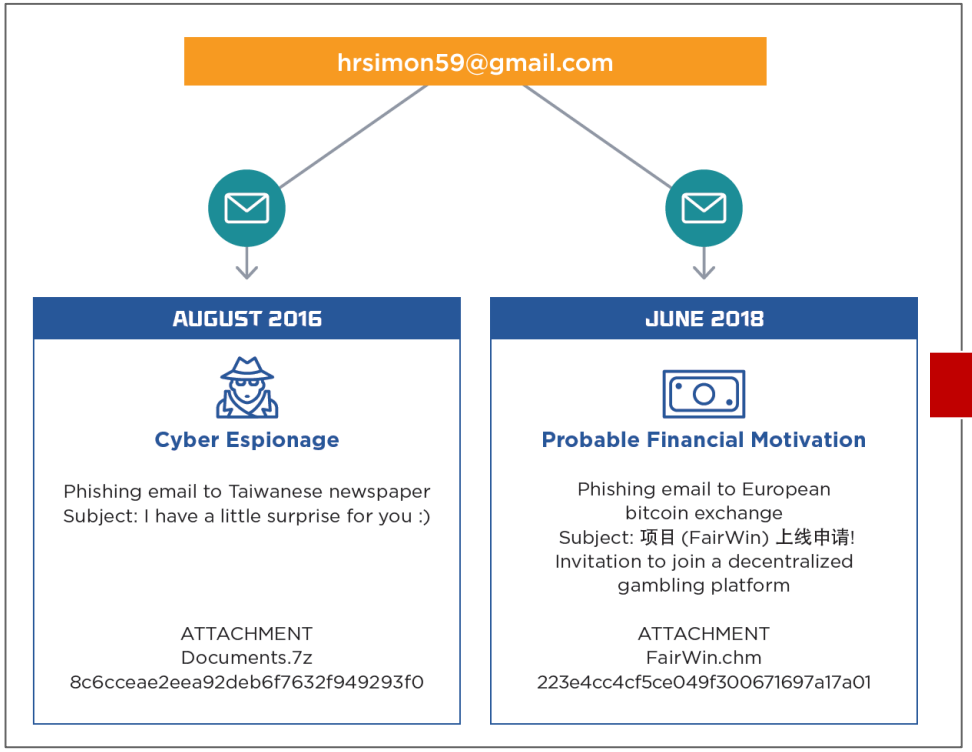
Table 17. GEARSHIFT

File MD5	File SHA1	File SHA256
5b26f5c7c367d5e976aaba320965cc7f	c2fb50c9ef7ae776a42409bce8ef1be464654a4e	7e0c95fc64357f12e837112987333cdaf8c1208ef8c100649eba71f1ea90c1db
f8c89ccd8937f2b760e6706738210744	f3c222606f890573e6128fbeb389f37bd6f6bda3	4aa6970cac04ace4a930de67d4c18106cf4004ba66670cfcdaa77a4c4821a213

FireEye APT 41 : https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis



＜仮説＞
APT41に攻撃されているのであれば…？

APT41 frequently uses the publicly available utility WMIEXEC to move laterally across an environment. WMIEXEC is a tool that allows for the execution of WMI commands on remote machines. Examples of commands executed by the utility include:

```
cmd.exe /c whoami > C:\wmi.dll 2>&1
cmd.exe /c del C:\wmi.dll /F > nul 2>&1
cmd.exe /c a.bat > C:\wmi.dll 2>&1
```

＜仮説＞
APT41に攻撃されているのであれば…？

FireEye APT 41 : https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis

＜具体的な分解 + 仮説構築手法＞

- **ビギナー向け ：（ベンダーレポート等の）IOCを利用して仮説構築する**
  - 但し、IOCは過去の攻撃に関する情報であり、古い。
  - セキュリティ製品が、シグニチャとして反映済と想定される。

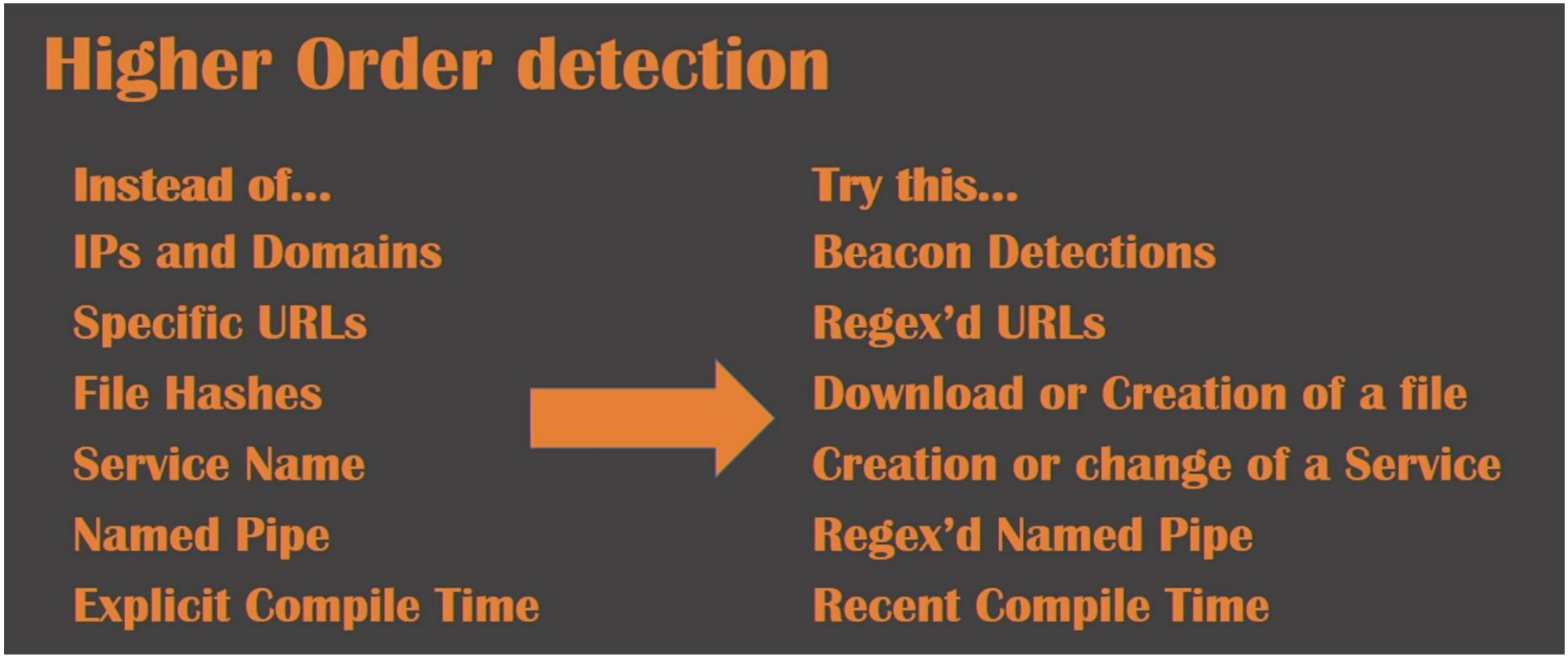
- **中級者向け　：攻撃手法（IoA・TTPs）などに着目する**
  - MITRE社 ATT&CKの活用
  - テクニック：IOCの一般化（IOC Generalization）

参考情報:
- IOA（Indicator of Attack）　：攻撃者の攻撃パターンに注目した情報
- TTPs（Tactics, Techniques and Procedures ）：攻撃者が使う攻撃手法・テクニック。IOAとほぼ同義。

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis

⇒ IOCの一般化（IOC Generalization）



Intelligent Hunting: Using Threat Intelligence to Guide Your Hunts : https://www.youtube.com/watch?v=-QlaOX5w8G8

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis

＜仮説構築時の３要素＞

仮説構築時は、３要素を組み合わせが望ましい。

- 要素１：脅威インテリジェンス
- 要素２：自社環境が置かれている状況（IT環境・業種・ビジネス動向）
- 要素３：過去の経験（自社・世間）

⇒ **要素２と要素３は、数あるIOC・仮説のうち、どこにまず注目すべきかヒントを提供してくれる。**

Intelligence Driven Threat Hunting（準備）

Step 2 & 3 : Decompose Action & Create Hypothesis

⇒ 例）注目すべきIOCに優先度をつける

	To Catch a Penetration Tester: Top SIEM Use Cases (DerbyCon 2016)	Top 15 Indicator of Compromise （by DARK Reading）
1	信頼の低いサイトへの企業アカウントを利用した認証	不審なアウトアウトバウンド通信
2	不審なサーバへのインターネット通信	特権ユーザによる異常な挙動
3	パスワード・スプレー攻撃（Password Spraying）	地理的な不規則性
4	サーバで検知されたマルウェア	ログインに関連する異常な挙動
5	Windows端末間の通信	データベース読み込みボリュームの増加
6	管理者グループ（ローカル・ドメイン）へのユーザ追加	HTMLレスポンスのサイズ
7	許可されていないサービスアカウントによるサーバログイン	同じファイルへの多数のリクエスト
8	Windowsへの新しいサービスの作成・登録	通信におけるポートとアプリケーションの不一致
9	サービスアカウントによるサービス・アカウントに異常な挙動	疑わしいレジストリ・システムファイル変更
10	閾値を超えたネットワーク通信・データのアップロード	DNSリクエストへの異常検知

To Catch a Penetration Tester: Top SIEM Use Cases : https://www.youtube.com/watch?v=9Ndv0W2Uq0U
Top 15 Indicators Of Compromise: https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647

Intelligence Driven Threat Hunting（実践）

Step 4：Hunt!!（ハンティング）

⇒ **仮説の検証！**

⇒ 前提：十分な可視化（Full-Spectrum Visibility）が確保されていること。

⇒ フリーツール・オープンソースを活用するのも一つの手段！！

Intelligence Driven Threat Hunting（実践）

Step 4：Hunt!!（ハンティング）

- **ハンティング成功の場合（＝仮説が正しく、攻撃の痕跡を確認できた場合）**
    - ハンティングプロセスを終了。Incident Responseフェーズへ移行。
- **ハンティング失敗の場合（= 仮説が誤りで、攻撃の痕跡が確認できない場合）**
    - Step 1~3へ戻る！

- ISACなどのコミュニティにフィードバックできるとベター！

Intelligence Driven Threat Hunting（フォロー）

参考情報：成熟度の高い組織は、次のステップを行う。

Diamond Modelを軸にした高度な分析手法を前提としているため、詳細説明は割愛。

- **Step 5：Enrich Actions（アクションの充実化）**
  - 収集した情報を他の情報と結び付け、充実化させる。
- **Step 6：Form Activity Group（アクティビティグループの作成）**
  - 類似したイベント・攻撃プロセスをまとめていくプロセス。

- **The Diamond Model For Intrusion Analysis: A Primer** (SANS CTI Summit 2014)
  - https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493920823.pdf
  - https://www.youtube.com/watch?v=jbeYf1lMH-A
  - http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Intelligence Driven Threat Hunting（事後対応編）

- **よりThreat Huntingを詳しく勉強したい人は…**
  - **The Threat Hunting Project**
    - https://www.threathunting.net/
  - **SANS Summit Archives** ⇒ “Cyber Threat Intelligence Summit”
    - https://www.sans.org/cyber-security-summit/archives/
  - **SANS Reading Room** ⇒ 関連するホワイトペーパーを読む
    - https://www.sans.org/reading-room/
  - **IronGeek** ⇒ 関連するカンファレンスのプレゼンテーションを見る
    - http://www.irongeek.com/
  - **各種セキュリティベンダーのブログ**

補足：専門ベンダーにやってもらうのはいいのでは？

- こうしたActive Defense（脅威インテリジェンス・脅威ハンティング）は、MSSP/MDR-SPサービスの一部として提供してくれるサービスである（はず）。
  - MSSP　：Managed Security Service Provider
  - MDR-SP　：Managed Detection & Response Service Provider

⇒ **私見：（体力のある組織は）自社でもできれば実施したほうが良い！**

⇒ **ハイブリッドモデルを推奨**

- 理由１：脅威インテリジェンスが共有できないケースも多い

  ⇒ ISACなどでは、TLP（Traffic Light Protocol）という情報共有の可能な範囲を定義しており、情報によっては自社内に閉じて検証を行わないといけないことがある。

- 理由２：「自社環境」を熟知しているのは自分達だけ！

  ⇒ 自社環境によって、「何が異常であるか？」、「どこに弱点があるか？」は異なる。

1-2 : TLPT (Threat-Lead Penetration Test)

TLPT（Threat Lead Penetration Test）

TLPT（Threat-Lead Penetration Test）：脅威ベースのペネトレーションテスト

- 高いセキュリティが要求される金融業を中心に登場したキーワード
- 実際の攻撃シナリオに基づいてペネトレーションテストを実施することで、脅威を防ぐ態勢を確認する。

金融庁：平成29事務年度　金融行政方針

大規模な金融機関については、そのサイバーセキュリティ対応能力をもう一段引き上げるため、より高度な評価手法[14]の活用を促す。また、金融機関に対し金融ISAC[15]等を通じた情報共有の一層の推進を促す。

加えて、「G7サイバーエキスパートグループ」[16]をはじめ、様々な国際会議でサイバーセキュリティの議論が行われており、各国当局とともに具体的な方針の策定に貢献していく。

---

[13] 同方針では、（ⅰ）サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、（ⅱ）金融機関同士の情報共有の枠組みの実効性向上、（ⅲ）業界横断的演習の継続的な実施、（ⅳ）金融分野のサイバーセキュリティ強化に向けた人材育成、（ⅴ）金融庁としての態勢構築、の５項目を柱としている。

[14] 例えば、金融機関（外部ベンダー等の利用を含む）による脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）。

TLPT（Threat Lead Penetration Test）

- ペネトレーションテストの詳細は、Internet Week 2018の資料を参照のこと
  - https://www.nic.ad.jp/ja/materials/iw/2018/proceedings/d2/d2-3-ishikawa.pdf

TLPT：ポイントのおさらい

- **ポイント１：脆弱性診断と何が違うのか？**
  - 脆弱性診断は、**脆弱性の「検出網羅性」**を重視！
  - ペネトレーションテストは、**脆弱性を活用し「目的達成可否」の検証**を重視！！

- **ポイント２：（ペネトレーションと比較して）TLPTの特徴的な点はなにか？**
  - （多数の違いはあるが）大きく２点の特徴がある。

- **特徴１：現実の脅威に基づくシナリオ**
  - 実際の脅威動向をもとにシナリオを策定する。

  ⇒ 脅威インテリジェンス・OSINTなどを活用した攻撃シナリオ策定が重要！

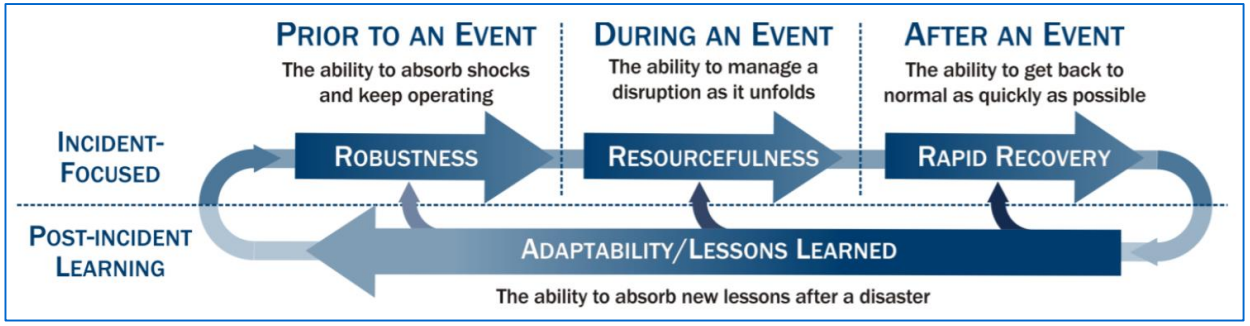
- **特徴２：サイバーレジリエンスに対する評価**
  - サイバーレジリエンスとは何か？
  - どのように評価が異なるのか？

サイバーレジリエンス（Cyber Resilience）とは？

定義：サイバー攻撃に対し、阻止・緩和・復旧を行う組織・システムの能力

⇒ NIST CSFのカテゴリー（**特定・予防・検知・対応・復旧**）の考え方と同じ！

- 参考：DHS：『A Framework for Establishing Critical Infrastructure Resilience Goals』
- **耐性（Robustness）**
  - サイバー攻撃の損害を未然に防ぎ、サービスを継続できる能力
- **臨機応変な対応（Resourcefulness）**
  - サイバー攻撃に適切に対応し、損害を最小限におさせる能力
- **早急な復旧（Rapid Recovery）**
  - サイバー攻撃前状態に早急に復旧できる能力
- **適応性（Adaptability）**
  - サイバー攻撃への対応能力を高めるため、事例・経験から学ぶ能力



https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

サイバーレジリエンスの評価

レジリエンス向上のため、技術・プロセス・人の側面から評価することが重要！

- テスト終了後に攻撃側（**Red Team**）と防御側（**Blue Team**）が議論を重ね、課題改善を行う**Purple Teaming活動**が非常に重要となる。
    - 攻撃者側の「見え方」と防御側の「見え方」は、かなり異なる。

- Red Teamの報告書は、**成績表（Report Card）**ではなく、改善を行う**インプット（Input）**ととらえるべき！！

TLPT 実施プロセス

- 詳細については、２つのドキュメントを読むことを推奨！
  - 『金融機関等におけるTLPT 実施にあたっての手引書』（FISC）
  - 『CBEST Intelligence-Led Testing CBEST Implementation Guide』

- 以下にプロセスの概略を示す。

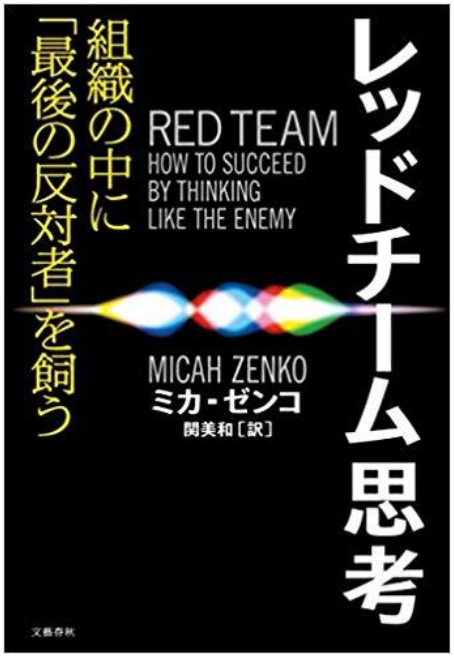
計画	シナリオ構築	テスト実施	レジリエンス評価
1-1 実施の決定	2-1 脅威インテル分析	3-1 テスト詳細計画策定	4-1 レジリエンスの評価
1-2 プロジェクト発足	2-2 攻撃シナリオ作成	3-2 テスト実施	4-2 改善計画策定・承認
1-3 スコープの決定	2-3 攻撃シナリオ検証	3-3 テスト結果レビュー	
1-4 ベンダーの選定			

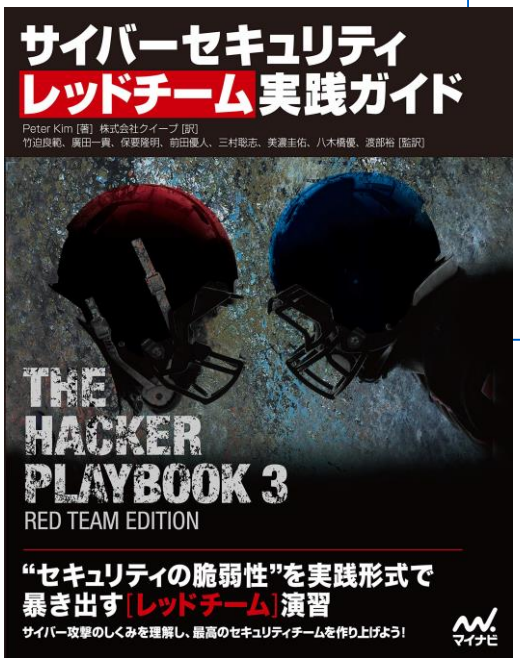
特徴1：
脅威インテリジェンスを活用した、攻撃シナリオの策定

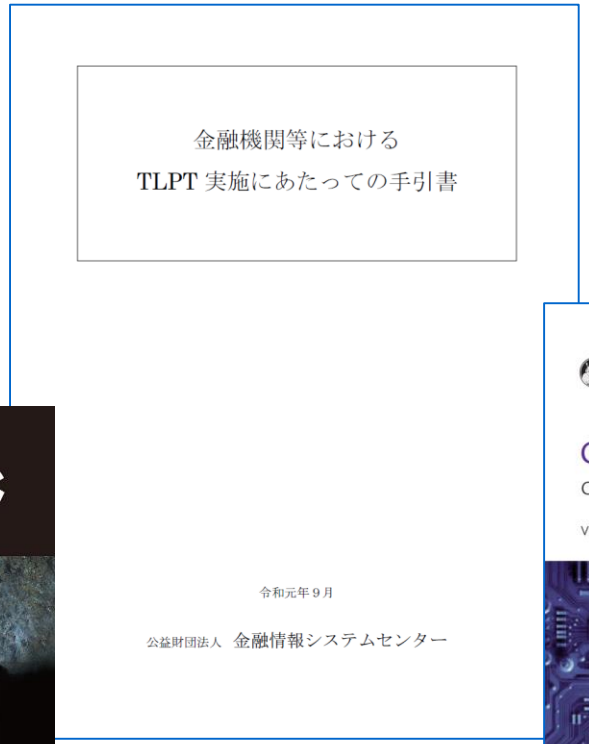
特徴2：
レジリエンス評価
Purple Teaming

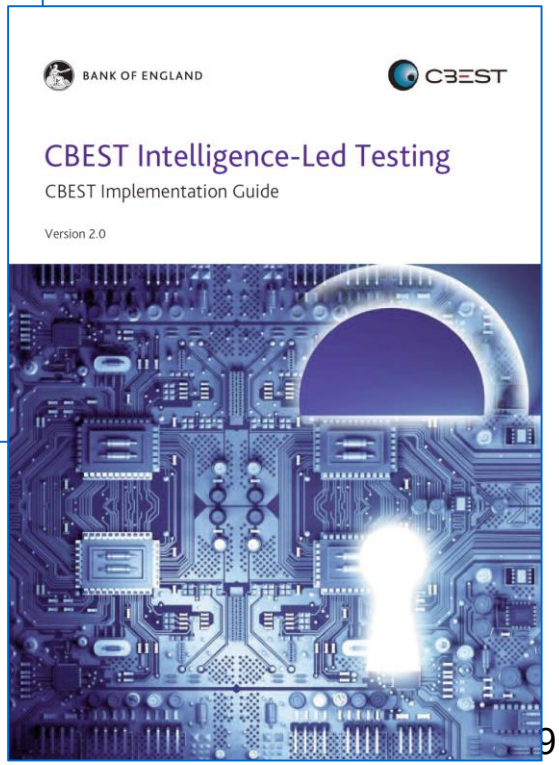
TLPT　参考資料

- TLPTを検討する場合、以下の書籍はイメージをつかむうえで有益！









2. ”Think-In-Graph” アプローチ

Attackers think in graph

Defenders think in lists. Attackers think in graphs.

As long as this is true, attackers win.

John Lambert, GM of Microsoft Threat Intelligence Center

@JohnLaTwC

（情報資産を）防御側は点（リスト）で捉える。一方、攻撃者はグラフで捉える。
これが真である限り、攻撃者は勝ち続けるだろう。

https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/

”Think-In-Graph”を攻撃者は当然活用している!

- 攻撃者側は、価値の高い資産（High-Value Asset）への最短アクセスを探し、最短経路を模索する。（= Weakest Linkを探し出す）
- 例）Bloodhound
    - Active Directoryの信頼関係を可視化してくれるツール
        - https://github.com/BloodHoundAD

⇒ 最短の攻撃パスを明らかにして、効率的な攻撃が可能

一方、（成熟度が高い）防御側は…

- 成熟度の高い組織は、技術的対策の導入を完了し、監視も安定し始めている。
    - センサー：FW, IDS/IPS, WAF, Mail GW, AV, EDR, Web Filtering/Proxy…

⇒ こうした対策は、特定の”点”における監視が中心!（Think-In-List）

- 個々の強度は高まったが、それでも「管理の隙間」や「Weakest Link」を悪用した ”Air Pocket” を利用した攻撃は引き続き行われる。
    - クラウド・サプライチェーンなど、”Air Pocket”を生まれる隙は多々存在する。

防御側も”Think-In-Graph”を活用し始めるべき！

- **次の一手：“点”と“点”を結び、グラフで防御を考えるアプローチ**
  - 守るべき対象：“Each Asset” ⇒ “A Graph of Asset”
  - *Attackers think in graphs, but Defender also think in graph.*

- **技術的アプローチは様々：**
- **例）マイクロセグメンテーション & SDN（Software Defined Network）**
  - ネットワークを安全な単位に小分割し、セキュリティチームがリソース使用量・データにきめ細かいセキュリティポリシーを適用できる技術（Forrester社）

- **例）監視ツール：UEBA・NDR・NTA**
  - UEBA（User Entity Behavior Analysis）
  - NDR（Network Detection Analysis）
  - NTA（Network Traffic Analysis）

とはいえ、Cyber Hygieneをおろそかにしない！

- **防御側の基本原則：*”Increase Attacker Requirements”***
  - 攻撃自体を止めることは不可能（考えるだけ無駄）
  - Cyber Hygiene（サイバー公衆衛生）にて、以下を実現することが大事
    - “Weakest Link”の排除し、「**攻撃コストが高いIT環境**」を維持すること
    - 例）脆弱性管理、パッチ管理、特権管理、資産管理 …

今後、注目される（？）アプローチ

- **攻撃者のコストを挙げる技術１：Anti-OSINT**
  - OSINT （**O**pen **S**ource **INT**elligence）
  - TLPTなどを行う際に、必ずOSINTによる情報収集が行われる。
  - リスク管理の観点から、自社が公開情報がどう見えるか知っておくべき

- **攻撃者のコストを挙げる技術２：Deception**
  - SNS、ネットワーク、アプリケーションにDecoy（おとり）を仕掛け、攻撃者をそちらに誘導する。
    - メリット１：攻撃者のリソースを無駄遣いさせる
    - メリット２：Decoyに攻撃を行わせることにより時間を稼ぎ、攻撃者を研究する
    - メリット３：本来アクセスが発生しない端末・パラメータへアクセスさせ、攻撃を検知

3. まとめ

まとめ

- **“Active Defense”アプローチ**
  - “Sliding Scale of Cybersecurity” モデル
  - Active Defenseの考え方
    - ３種類のアプローチ：振る舞い検知・脅威インテリジェンス・脅威ハンティング
  - **アプローチ１：脅威ハンティング**
    - 攻撃がシグニチャ化されるまでの”Zero-Day”期間で、攻撃者をあぶりだすアプローチ
    - 実施プロセス（Intelligence Driven Threat Hunting）
  - **アプローチ２：TLPT（Threat-Lead Penetration Test）**
    - 実際の攻撃シナリオに基づきペネトレーションテストを行い、技術のみならず、人・プロセス情報の課題を明らかにして、**サイバーレジリエンス**を高める。
- **“Think-In Graph”アプローチ**
  - 攻撃者同様に、防御側も**システムを一連の”グラフ”としてとらえる**必要あり。
  - Cyber Hygieneによる「**攻撃コストが高いIT環境**」の実現。

まとめ

高度な攻撃手法に対抗するためには…

（攻撃目線を取り込んだ）プロアクティブ・アプローチが重要となる。

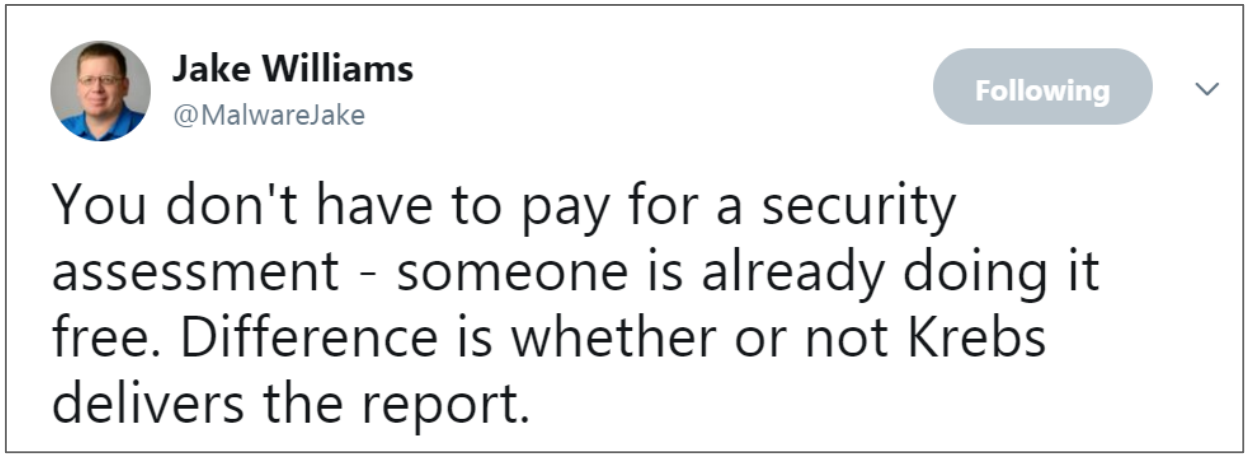
The adage is true that the security systems have to win every time, the attacker only has to win once.

The Art of Intrusion, written by Kevin Mitnick

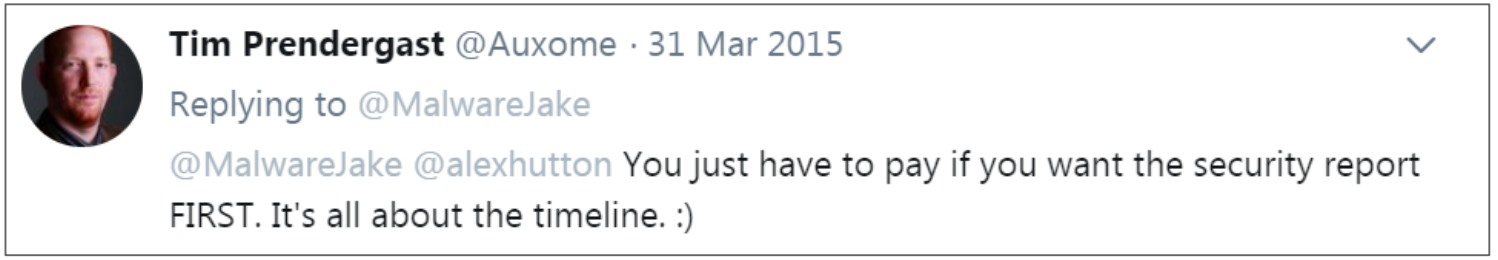
セキュリティ・システムは常勝を義務づけられ、攻撃者は一度勝つだけで良い、
という格言は的を射てる。

まとめ

対策を取らないと…



ペネトレーションテストにお金を払う必要はない。誰かが既に無料でやってくれている。
違いは、Brian Krebs氏がレポートを届けてくれるという点だけだ。



お金を払うのは、**最初に**レポートを受け取るためだ。要するに、時間軸の問題だ。

まとめ

適切に対応するためには、「サイバーレジリエンス」向上が重要！

だが考えてもみたまえ。もしシステムが完全無欠なら、それを人の手で
運用する必要すらないはずだ。（中略） いかに万全を期したシステム
であろうと、それでも不測の事態に備えた安全策は必要とされる。
万が一の柔軟な対応や、機能不全の応急措置。そうした準備まで
をも含めて、システムとは完璧なるものとして成立するのだ。

PSYCHO-PASS 第一期 #13「深淵からの招待」より

⇒ プロアクティブ・アプローチには、**技術・人・プロセス**がそろう必要あり。

まずは、できるところからやってみませんか？

ご清聴、ありがとうございました。

To Be a **Good Company**

TOKIO MARINE Tokio Marine Holdings