NFLabs.

Your Security Partner

学生の頃と社会に出てからのセキュリティ業務のギャップ

株式会社エヌ・エフ・ラボラトリーズ
事業推進部 研究開発担当
保要　隆明

このセッションでは

- 講演者が学生の頃思っていたセキュリティ業務と実際に社会に出て感じたセキュリティ業務にまつわるギャップを3つ紹介

- 粒度が粗いものから細かいものまで様々。
- あくまで講演者の経験範囲内で感じたギャップです

- （学生のみなさん）研究の方向性を決める一助となれば幸いです
- （社会人のみなさん）他にもこんなギャップがあった、みたいなものがあれば#mws2020-pre でお願いします！

講演者の経歴

学生時代 (2010～2016)	• ネットワークセキュリティ研究室に所属 • ボットネット対策、無線LAN攻撃対策の技術の研究 • （課外活動として）CTF参加、勉強会登壇、ハニポ、サーバ運用、書籍執筆 など
NTTCom （2016～2019）	• 社内のCSIRTに所属（途中、SOCにてOJT） • 社内のセキュリティ監視 および インシデントハンドリング • ユーザヒアリング、ログ分析、マルウェア解析、フォレンジック など
NFLabs. （2019～2022）	• 研究開発担当所属 • 研修コンテンツ開発、講師、研修PF開発、ペンテスト、教育サービス開発 • 資料作成、ペンテスト、コーディング、アジャイル開発 など

ギャップ1

セキュリティ業務は技術だけではない

ギャップ1

- 学生の頃: セキュリティ業務は技術で解決できる問題が多いと思っていた

- 現実: セキュリティ業務は技術、だけで解決できない問題が多い
- 例えば…
  - 不審メールを不審と思わず開いてしまう（ユーザリテラシー）
  - 業務プロセスに不備があり誤操作が起きて、インシデントが発生する
  - セキュリティ運用に決まった手順がなく、品質がバラバラ
  - そもそも、セキュリティ運用者の知識・スキルが足りない

- 技術、人、プロセスなど複数の観点で業務の課題を解決する必要がある

ギャップ2

通信ログの情報量が少ない

ギャップ2

- 学生の頃: 通信ログはpcapのフォーマットで保存されていると思っていた

- 現実: pcapで保存されてることは少ない。プロキシログやFWログなど情報量が落ちた形で保存されていることが多い
- 理由：
  - 企業のトラフィックは膨大なため、pcapで保存するとストレージが溢れる
  - 攻撃検知やインシデント調査に通信のすべてのデータが必要とは限らない
    - 近年は、エンドポイントのログも活用した検知・調査も増えている

- なるべく少ない情報量で検知・調査ができると理想

ギャップ3

Windowsサーバが多い

ギャップ3

- 学生の頃: サーバはLinuxが多いと思っていた

- 現実: Linuxサーバもあるが、Windowsサーバも多い
- 理由:
  - クライアントがWindowsを使っていると、環境に統合しやすい
    - 特に、Active DirectoryはWindows環境を統合管理するのにとても便利
  - GUIの方が操作しやすいため

- Windows環境のセキュリティの課題やそれを狙った脅威もまだまだ現実は多い

さいごに

- 講演者が学生の頃思っていたセキュリティ業務と実際に社会に出て感じたセキュリティ業務にまつわるギャップを3つ紹介。
- 学生から見える課題と現実のセキュリティの課題は、大きく異ることがある

- 研究の方向性に困ったら、実業務で課題になっていることに目を向けて見るのも良いかもしれない
  - MWSのコミュニティには “産” の有識者もたくさんいるので、その人に課題を相談しても良い
  - 企業のインターンシップを活用して、世の中の課題を直に感じるのも良い