O’Reilly Security Conference 2017 参加報告

山本哲生

今日はできるだけ
インタラクティブな形式に
します

アジェンダ

- セキュリティには教育が大事
- Zero Trust Networkingについて
- その他各セッションを紹介

Zero Trust Networksについて

Zero Trust Networks

- Firewallの内側の端末も信用しない
- リソースへのアクセスはすべてProxyを通す
- Proxyでリクエスト元の物理位置、使用者、端末、端末の状態など複数の情報に基づいてアクセス制御

メリット

- Firewall内部に侵入されても即甚大な被害とはならない
- 端末でマルウェアが検出されたら即アクセス遮断できる
- VPNが不要になる
- BYOD (Bring Your Own Device) が可能になる

OTHER RESOURCES

- O'Reilly Media *Zero Trust Networks*, by Doug Barth and Evan Gilman
- Google BeyondCorp
  https://cloud.google.com/beyondcorp/
- Netflix LISA
  Location Independent Security Approach
- Edgewise Networks
  https://www.edgewise.net

その他キーノートや
セッションを紹介

Why cloud-native enterprise security matters

Three R

- Rotate: 認証情報（鍵ファイルなど）を数時間ごとに更新する
- Repave: サーバーやアプリケーションの状態を数時間ごとにあるべき状態に戻す
- Repair: 脆弱性が公開されたら直ちにパッチをあてる

Inside the bad actor's studio

- オンラインサービスへの攻撃の検出には教師なし学習が今後重要になる
  （日々新しい手法が出てくるため教師データがない）

- 生存期間が長いアカウントは信頼できる、といった過去有効だった特徴を悪用してくることも

Securing existing AWS infrastructure

- セキュリティ監査ツールはいくつかあるので使おう
  evident.io, scout2, s3scan

- IAMの作成にはterraformを使おう

- アクセスキーやシークレットキーはアプリに含めずインスタンスロールから権限を取得しよう

- IAMのパスワードポリシーを厳しくしてMFAを有効にしよう

Securely Moving Data to the Cloud with Confidence and Customer Focus

- Zoning: インシデント発生時の影響範囲を限定する
- Logging & Monitoring: ログを取る、リアルタイムにログ監視する
- Authentication: 常にMFAを使う
- Encryption: 常に暗号化する、鍵はローテートする

おしまい