中島 章博
アマゾン ウェブ サービス ジャパン
ソリューションアーキテクト
2020/2/25作成

AWS INNOVATE 2020 オンラインカンファレンス

「AWS環境におけるセキュリティインシデントの調査・対応方法」のクイズおよび解答

AWS INNOVATE 2020のセッションの視聴およびアンケートにご記入頂きありがとうございます。本資料が「AWS環境におけるセキュリティインシデントの調査・対応方法」で出題されたクイズの解答になります。

AWS環境上でAmazon EC2による3層構造のWebシステムが稼働しており、Amazon GuardDutyで脅威検知とセキュリティ監視をしています。

ある日、GuardDutyで”UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration”を検出しました。検出結果のActorのIPアドレスは、自社のIPではなかったので攻撃と判断。悪用された認証情報はEC2のIAMロールの一時的な認証情報でした。即座にこの認証情報を無効化したので被害は発生しませんでした。

調査した結果、外部からOSコマンドインジェクションでこの認証情報を窃取されていたことがWebアプリケーションログから判明しました。しかし、GuardDutyではこのOSコマンドインジェクション攻撃を検出していなかったです。

なぜ検出できなかったのでしょうか？この攻撃を検出する方法はありますか？

Amazon GuardDuty の脅威検出は、VPC フローログ、AWS CloudTrail イベントログ、DNS ログを分析してアカウントの侵害、インスタンスの侵害、悪意のある偵察に関連する可能性のあるアクティビティを特定します。たとえば、GuardDuty は、異常な API コール、既知の悪質な IP アドレスへの不審なアウトバウンド通信、または DNS クエリを転送メカニズムとして使用する可能性のあるデータの窃盗を検出します。今回の攻撃、OSコマンドインジェクションは、アプリケーションドメインへの攻撃であり、GuardDuty では脅威分析をしていない攻撃になります。（スライド資料8ページ：本セッションのスコープ(2)をご参照ください）

中島 章博
アマゾン ウェブ サービス ジャパン
ソリューションアーキテクト
2020/2/25作成

Webアプリケーション層への攻撃は、AWSウェブアプリケーションファイアウォール(WAF)を導入することで、ウェブアプリケーションの保護を向上させることができます。AWS WAF では、SQL インジェクションやクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするセキュリティルールと、定義した特定のトラフィックパターンを除外するルールを作成できます。そしてWAFのログやアプリケーションログ等のセキュリティ監視・分析をすることで脅威検出が可能になります。Webサーバーなどのネットワーク層への攻撃を含めてより広範に防御とセキュリティ監視をするためには、パートナーソリューションのネットワーク型IDS/IPSおよびホスト型IDS/IPSの活用をご検討ください。

ご参考リンク

- AWS パートナーネットワーク (APN)のセキュリティ/侵入検知・防御ソリューション
  https://esp-online.com/solutions/topic/39/%E4%BE%B5%E5%85%A5%E6%A4%9C%E7%9F%A5%E3%83%BB%E9%98%B2%E5%BE%A1

- Amazon GuardDuty
  https://aws.amazon.com/jp/guardduty/

- AWS WAF – ウェブアプリケーションファイアウォール
  https://aws.amazon.com/jp/waf/