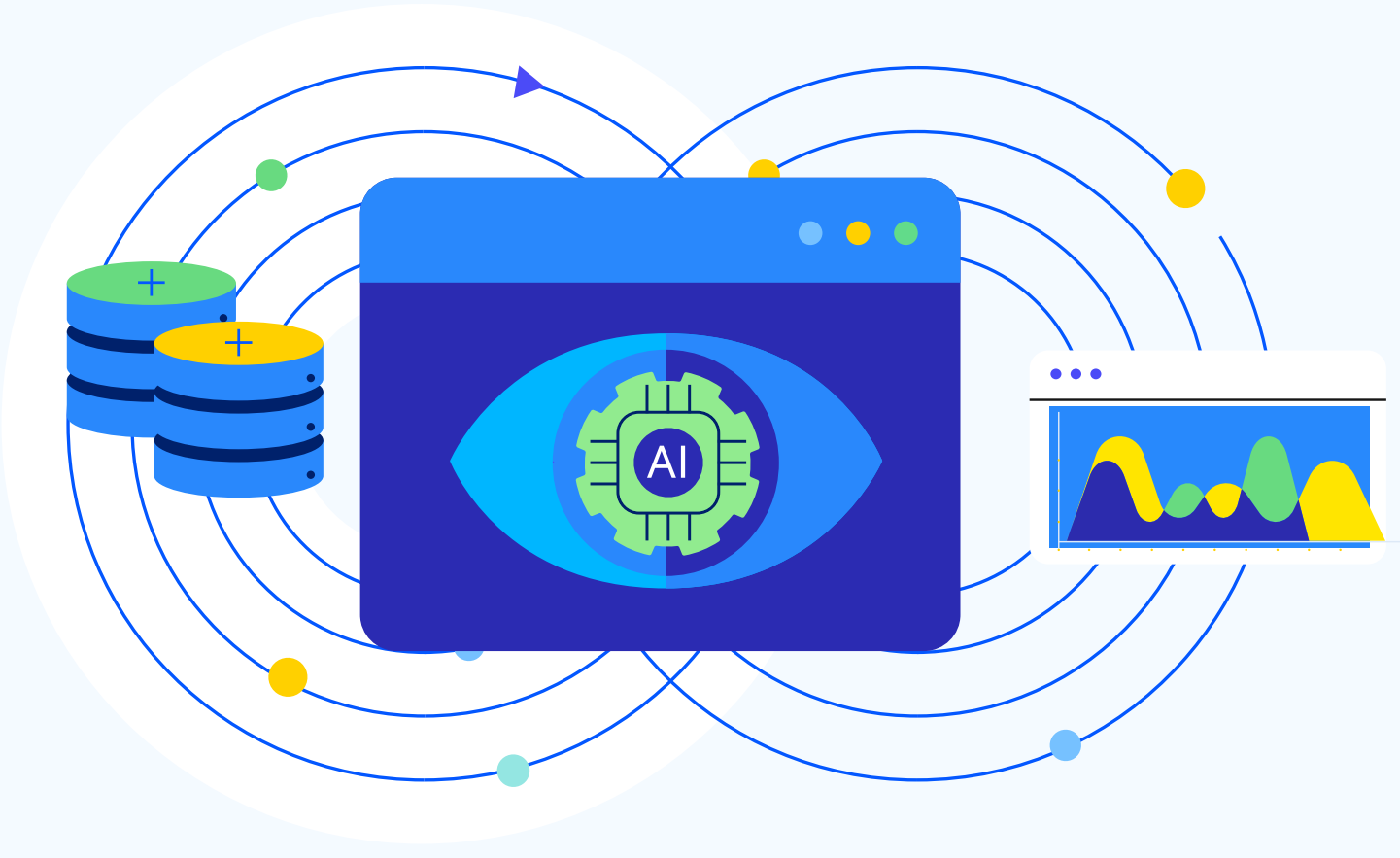
Progress Flowmon

Flowmon ADS

AI を実装した Flowmon 異常検出システム

脅威の検出：
リアルタイムで攻撃を検出

データシート



データ侵害の特定と修復に費やす時間 – IBM の調査

データ侵害の特定:	**190日以上**
問題の修復:	**さらに60日以上**

上記 IBM の調査結果が示すように、データ侵害の特定と修復には長い時間がかかっています。堅牢なセキュリティソリューションを導入して明確なプロセスを定義できれば、このような問題に効果的に対処でき、検出と対応に要する時間を短縮して、経済的および社会的な損害を最小限に抑えることができます。

Flowmon を使用しているある政府機関は、データ侵害の被害に遭いました。DMZ 内のサーバーが侵害され、攻撃者がデバイスをコントロールできるようになりました。

何が起こったか、分単位でチェックしてみましょう。

何が起こったのかを時間軸で検証

0分経過 – アドレス解決プロトコル (ARP) スキャン

攻撃者は最初に、同じ /24 ネットワークサブネット内で電源がオンになっていて、ARP 要求に応答するデバイスをリストアップしました。Flowmon は、252台のデバイスに対する ARP スキャンが行われたというアクテビティを検出しました。応答したデバイスは1台もありませんでした。

3分経過 – インターネット制御メッセージプロトコル (ICMP) スキャン

次に、攻撃者は、ICMP プロトコルを使用してネットワーク内のデバイスのリストアップを実行しました。10万台を超えるデバイスに対して接続が試みられ、ネットワークにかなりのノイズが発生しました。Flowmon は、このアクティビティを、ICMP ping フラッドと ICMP スキャンの両方として検出し、ネットワークトラフィックに400万件を超える ICMP 要求が隠されている証拠を示しました。

31分経過 – セキュアシェル (SSH) 攻撃

最初に侵害されたホストからアクセスできる複数のサーバー上の SSH サービスに対して、パスワードスプレー攻撃が開始されました。Flowmon は、21台の異なるサーバーで実行されている SSH サービスに対する失敗した攻撃を検出し、約3,000回のログイン試行の証拠を提供しました。

45分経過 – AI を活用したイベント分析

Flowmon の AI 搭載イベント分析エンジンは、単一のデバイスによって実行されたすべての悪意あるアクティビティを関連づけました。点と点がつながったことにより、侵害されたデバイスの脅威スコアが 49 (最大値は100) に上昇し、ネットワーク内で最大の懸念事項と認定され、人間の介入が必要なレベルであるとのフラグ付きで報告されました。

発生後1時間以内 – イベント修復

フラグが立った状況の報告を見て、セキュリティオペレーションセンターは、侵害されたデバイスをすぐにネットワークから切断しました。そして、国のサイバーセキュリティ当局にインシデントを報告するのに必要な証拠を収集しました。攻撃を早い段階で阻止できたため、組織の環境への影響はありませんでした。

まとめ

このように、Flowmon はリアルタイムで攻撃を検出することに成功し、脅威を緩和するための貴重な詳細情報を提供しました。Flowmon の AI 搭載エンジンは、複雑なネットワーク内で侵害されたデバイスを正確に特定しました。この政府機関は、Flowmon からの詳細な情報を使って迅速に侵害からの修復を達成でき、検出できなかった場合に要したであろう莫大なコストの発生を防ぐことができました。

強力なネットワーク監視ソリューションである Flowmon は、データ侵害の脅威を迅速に検出し、詳細なイベント分析情報も提供するので、脅威に対して速やかな対応が可能になります。

情報提供：
プログレスインフラストラクチャ担当
プリンシパルエンジニア
Jirka Krejčíř

プログレス・ソフトウェア・ジャパン株式会社
〒106-0047 東京都港区南麻布 4-11-22 南麻布 T&F ビル
www.progress.com/jp/flowmon
sales_japan@progress.com

Progress