課題解決OPS

ワンポイントソリューション

ae-001

予期しないログオン要求が

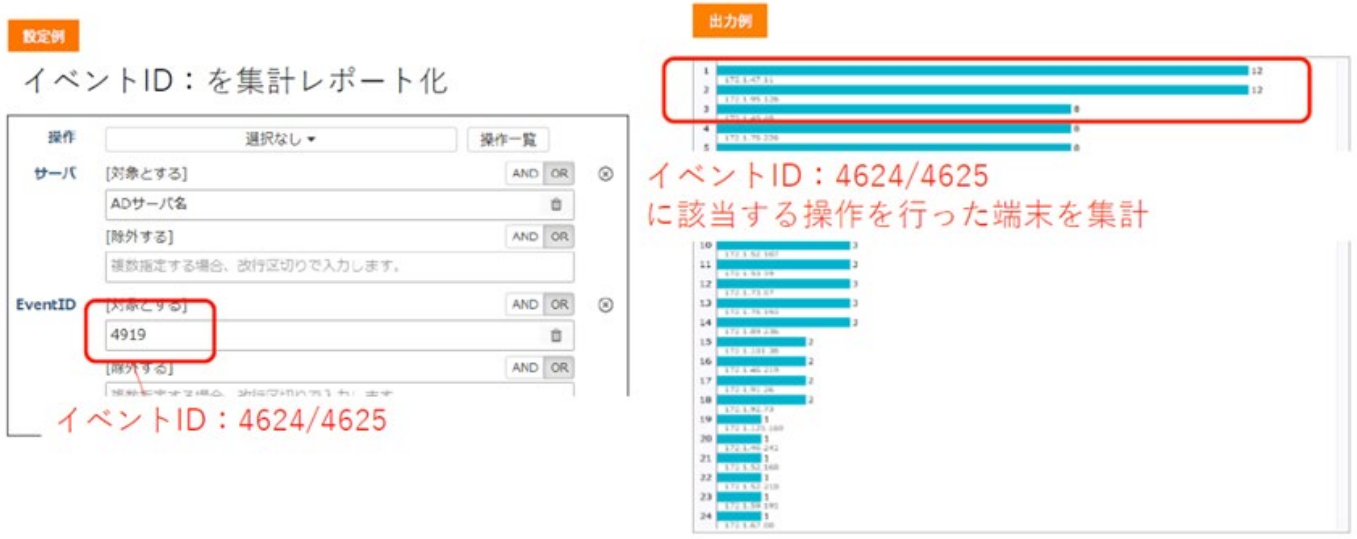
大量に発生していないか確認したい

課　　題

外部から認証要求リクエストが大量に発生している場合、サイバー攻撃を受けている可能性があるので、どの程度大量のログオンの失敗が起きているのか実態を把握したい。

解決方法

Active Directoryのログを基に、短時間に大量のログオン失敗をしていないか、また、認証要求を行うはずがない端末から認証要求が行われていないか、特定端末から複数のアカウントに対して認証要求が行われていないか、などについて、イベントID:4625のログを集計して調べることができます。



運用で意図しない利用が確認された場合には、該当するアカウント、端末がマルウェアに感染していないか等を調査すべきです。

Point!

ALog EVAのサイバー攻撃自動検知パックを利用すれば、ログオン失敗のレポートをグラフで分かり易く出力できます。

Product / Service

ALog EVA サイバー攻撃自動検知パック

[区　分]　セキュリティ
[環　境]　Windows
[タ　グ]　サイバー攻撃, 不正アクセス, ログ解析

https://ceccs.site/ops/

CCS 株式会社シーイーシーカスタマサービス
プロダクトサービス事業部