2024 年 7 月 2 日
S & J 株式会社
代表取締役社長　三輪　信雄
東証グロース：5599

S&J、『Active Directory 監視サービス』は Operation Blotless 攻撃キャンペーンの検知が可能 独自開発エージェントによる調査レポート無償トライアル開始

S & J 株式会社（本社：東京都港区、代表取締役社長：三輪　信雄、証券コード：5599、https://www.sandj.co.jp/、以下、S&J）は、独自開発 SOC サービス「Active Directory 監視サービス」により、Operation Blotless 攻撃キャンペーンの検知が可能なことをお知らせします。
併せて、2024 年 7 月 8 日（月）より、お客様のセキュリティ環境の安全性を独自開発エージェントにて調査・報告する調査レポート無償トライアルを開始することもお知らせします。

2024 年 6 月 25 日（火）、JPCERT コーディネーションセンターから Operation Blotless 攻撃キャンペーンに関する注意喚起が公表されました。同センターでは、脅威グループ「Volt Typhoon」による同種の攻撃を例に、短期および中長期の対策を提示しています。

Volt Typhoon の侵害検知は困難

「Volt Typhoon」は、政府機関や重要インフラ企業への侵入経路を確保することを目的としていると見られています。

- Active Directory の各種ログが少ない
- 初期侵入経路となった機器の各種ログが少ない
- 侵害箇所が限定的

このグループは、固有のマルウェアをほとんど使用せず、環境寄生型の戦術を徹底しているため、被害現場にはインジケーター・オブ・コンプロマイズ（IoC）となる情報をほとんど残しません。

また、一回あたりの侵害期間が短く、侵害範囲も限定的であるため、被害現場に残るアーティファクトの量が少ないことが特徴です。これにより、IoC 情報を作出する機会とその量が大きく減り、検知が非常に困難になります。

『Active Directory 監視サービス』で Operation Blotless 攻撃キャンペーンの検知が可能に

S&J で蓄積されたインシデントレスポンスのノウハウを元に開発された本サービスは、上記の特徴を持つ Operation Blotless 攻撃キャンペーンを現バージョンでも検知することができます。
また、2024 年 7 月 8 日（月）には本攻撃に特化した検知ロジックのリリースを予定しており、より安全かつ安定したビジネス環境の実現を支援いたします。

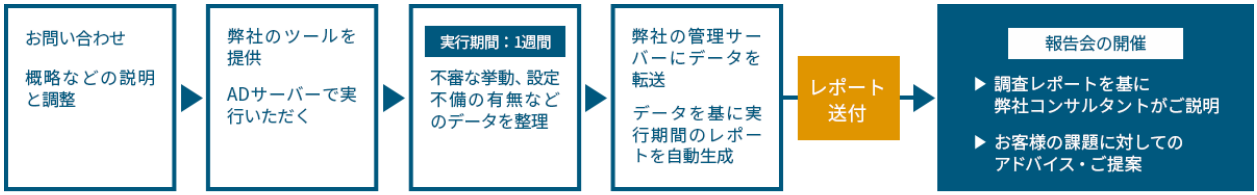
"Operation Blotless 攻撃キャンペーン"が検知可能『Active Directory 監視サービス』
▼https://www.sandj.co.jp/operation_blotless/

『Active Directory 監視サービス』の特徴

- S&J が独自開発したエージェント（AD Agent）とクラウドでの独自ロジックの組み合わせにより、SIEM では検知できない脅威を検出することができます。
- S&J がこれまでに対応してきたランサムウェアや APT 攻撃などのインシデントレスポンス（IR）の経験をノウハウとして検知ロジックを組み込んでいます。
- AD 特有の脅威（DCShadow、DCSync、Pass the Hash、Golden Ticket、BloodHound など）を検知することができます。
- AD 固有の重要なパッチ（Zerologon、SIGRed、PrintNightmare など）の適用チェックを行います。
- DC（Domain Controller）だけでなく、ファイルサーバーや仮想基盤などの Windows Server を監視することで、より早く脅威を検知することが可能になります。
- 脅威を検知することで攻撃に対する対処をいち早く実施することができます。
- 24 時間 365 日体制で監視を行います。
- 検知した情報のみを送信するため、SIEM よりも転送するログ量が格段に少なくなります。
- 不審な動作をしたアカウントは、リモートでアカウントの無効化を行います（別途オプション）。
- 過検知を AI エイジング機能で大幅に削減しています。

AD Agent 調査レポート無償トライアル

本トライアルでは、S&J が独自開発したエージェント（AD Agent）の調査レポートを使用して対策の助言を無償で実施いただけます。



トライアル期間 2024年7月8日(月)～8月31日(土)

2024 年 7 月 8 日～8 月 31 日

『Active Directory 監視サービス』AD Agent 調査レポート無償トライアル

▼https://www.sandj.co.jp/operation_blotless/

大量ログオン失敗やパッチの未適用、監査ログの出力設定や CPU 使用率などを抽出し、お客様の環境に対して弊社コンサルタントがアドバイスをさせていただくことにより、より安全かつ安定したビジネス環境の実現を支援いたします。

S & J 株式会社について

URL	https://www.sandj.co.jp/
本社	〒105-0003 東京都港区西新橋 2-4-12 西新橋 PR-EX8 階
設立日	2008 年 11 月 7 日
資本金	4 億 4,162 万円
上場取引所	東京証券取引所グロース市場（証券コード：5599）
代表者	代表取締役 三輪 信雄（みわ のぶお）
事業内容	サイバー攻撃対策システムの開発及び運用、サイバー攻撃監視やセキュリティ診断、コンサルティング、インシデント対応などのサービス提供。S&J は、自社開発の運用システム「SOC Engine®」により、効率的・効果的なセキュリティ運用サービスを提供しています。

本件に関するお問い合わせについて
https://www.sandj.co.jp/contact/
S & J 株式会社 広報担当
TEL： 03-6205-8500（代表）
MAIL：pr@sandj.co.jp