Black Hat 2024レポート: 要点とトレンド

WhoisXML APIは、2024年8月3日から8日にかけてラスベガスのマンダレイ・ベイ・コンベンション・センターで開催された「Black Hat 2024」に参加しました。Black Hatは、年に1回開催される世界有数のセキュリティカンファレンスです。今年のBlack Hatには、117カ国から2万人を超えるセキュリティ専門家が一同に会しました。

例年通り、Black Hat 2024ではセキュリティの最新動向が紹介されるとともに、今まさに出現しつつある新たな脅威が明らかにされました。本ブログでは、当社のチームが特に注目したBlack Hat 2024のハイライトをご報告します。

サードパーティリスク管理

今年のBlack Hatにおける主要テーマの一つは、サプライチェーンのセキュリティでした。サプライチェーンのセキュリティリスクには、ThreatLockerのCEO兼共同創業者であるDanny Jenkins氏をはじめ、多くのセキュリティ専門家が日々頭を悩ませています。Jenkins氏はメインステージで行われた「Understanding and Reducing Supply Chain and Software Vulnerability Risks（サプライチェーンとソフトウェアの脆弱性リスクを理解し低減する）」というセッションに登壇し、IT環境においてバックドアや予期せぬ脆弱性を特定することの重要性を強調しました。

セッションの出席者は、サードパーティーリスク管理戦略の必要性について縦横に論じ合いました。サードパーティリスク管理戦略には、ソフトウェア開発プロセスへのセキュリティの組み込み、サプライチェーンの回復力の向上、サプライチェーンにおけるセキュリティ態勢の継続的な把握などが含まれます。

サプライチェーンの回復力を強化する上で、ベンダーの徹底的なリスク評価は欠かせません。このような評価では通常、「この会社のインターネットインフラは信頼できるか」といったことが問われます。その答えを出すため、企業はベンダーのソフトウェア製品に関連したドメイン名やIPアドレスの評判をチェックすることもあります。この種のデューデリジェンスは重要な意味を持ちます。というのも、Verizonのデータ侵害調査報告書

（DBIR）によれば、データ侵害の15%にサードパーティが関与しているためです。

セキュリティとAI

人工知能（AI）は、今回のBlack Hatで大いに注目されたテーマでした。数多くのベンダーが、AIを活用したセキュリティ製品やソリューションを紹介していました。また、セキュリティにおけるAI活用のメリットやリスクを検討するセッションも複数行われました。

そのうちの一つのセッションでは、SwimlaneのCISOであるMike Lyborg氏とSecurity WeeklyのMandy Logan氏が、AIによる情報の要約、分類、優先順位付けを通じてセキュリティ運用（SecOps）をいかに効率化できるかについて議論しました。組織のセキュリティチームは、このような手法を取り入れることでより迅速かつ効果的にリスクの除去/軽減策を講じることができます。

SecOpsチームが毎日膨大な量のデータを処理していることから、セキュリティにおけるAIと自動化はゲームチェンジャーになりそうです。事実、SecOpsチームは一般に毎日平均50件のセキュリティアラートを受信しています。加えて、必要な背景情報やサイバーインテリジェンスを得るために、何十億件ものDNS、IPアドレス、ドメイン名の過去データに目を通さなければならないこともあります。そのような時にAIを活用すればデータ分析がより簡単かつ迅速になりますので、SecOpsチームは他の重要なタスクに時間を割くことができます。

サイバーセキュリティと不正行為防止の融合

当社が特に注目したもう一つのセッションは、IANS Researchで教員を務めるAllison Miller氏によるものでした。Miller氏は、サイバーセキュリティと不正行為防止との間に重なる部分が増えてきていることを論じました。同氏の研究は、同じ問題の異なる側面に対処するために、この2つの分野がますます類似したテクノロジーを使用するようになっていること

を明らかにしています。両分野のクライアントが共通のサイバーインテリジェンスソースを活用している事例を数多く見てきた当社としては、これに大いに賛同するところです。

サイバーセキュリティと不正行為防止の融合とはどのようなものでしょうか？一例を挙げましょう。サイバーセキュリティチームがボットネットの存在やブルートフォースアタックの兆候を検知するとき、不正行為防止のスペシャリストは同じ問題を、いつ起きてもおかしくないアカウント乗っ取りとして捉えます。言わば両チームは「それぞれ異なる形で同じ問題に対処している」のです。

このことは、サイバーセキュリティと不正行為防止の両方をカバーした統一的なセキュリティアプローチの必要性を浮き彫りにしています。

ユニバーサル・ゼロトラストネットワークアクセス

Black Hat 2024で再三取り上げられていたもう一つの話題は、組織のネットワークインフラのあらゆる面（クラウド環境、エンタープライズ・アプリケーション、オンプレミス・ネットワークを含む）にわたってゼロトラスト・アーキテクチャが採用されつつある、ということでした。

ユニバーサル・ゼロトラストネットワークアクセス（ZTNA）では、場所やデバイスに関わらず、認証され権限を付与されたユーザーだけが特定のアプリケーションやデータにアクセスできるようにします。これは、ハイブリッドワークモデルを採用する組織の増加傾向や、クラウドベースとオンプレミスの両方のリソースに対するセキュアなアクセスの必要性に対応しています。

ZTNAに適合したセキュリティソリューションには、即座に全てのユーザを識別し、ポリシー制御を実装し、ポリシーを更新できることが求められます。この手法では、ユーザーの身元確認や Device Postureの評価を行うために、広範囲のDNSデータを統合する必要があります。

WhoisXML APIについて

WhoisXML APIはサイバーインテリジェンスソリューションのトッププロバイダーとして、ドメイン名、IPアドレスおよびDNSのデータでAIモデルを飛躍的に強化できるサービスをご提供しています。

当社のKnow Who You're Talking To (KWYTT) Intelligenceサービスは、厳格なサードパーティー評価、正確な不正行為検知、そして継続的なサイバーリスク監視を通じ、企業のゼロトラスト戦略の実装を強力にサポートします。

当社は、ドメイン名レジストリ、レジストラ、ISP、治安当局など、世界中の主要なデータプロバイダーと綿密な協力関係を維持しており、そうした幅広いネットワークを駆使して、広範なドメイン名、IPアドレス、DNSに関する正確で最新のデータをお客様にお届けしています。

WhoisXML APIは数年前からInc.5000（米国で最も急成長中の非公開企業のリスト）に毎年掲載されており、また、Financial Timesで南北アメリカにおける急成長企業の一つに選ばれています。当社のソリューションは、フォーチュン500企業、大手セキュリティ企業をはじめ、さまざまな業界の組織を含む52,000以上のユーザーからご信頼をいただいています。