【プレスリリース】

マカフィー株式会社
2020 年 8 月 4 日

※当資料は、米国時間 2020 年 7 月 27 日に米国で発表されたプレスリリースの抄訳です。

McAfee MVISION Cloud がクラウド脅威と MITRE ATT&CK を紐づける 最初の CASB に

クラウドネイティブな攻撃や脆弱性に対する SOC の対応を強化し、
より的確な脅威の検出と予防策を可能に

デバイスからクラウドまでを保護するサイバーセキュリティ企業である米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は、7 月 27 日（米国時間）、同社の CASB「MVISION Cloud」への MITRE ATT&CK®の導入を発表しました。クラウドサービスに対するサイバー攻撃を追跡、検出、停止するための確実な方法の提供を可能にします。これにより、セキュリティ担当者はクラウドの脅威や脆弱性が MITRE ATT&CK の「tactics（戦術）」と「techniques（技巧）」のどこに位置するかを確認することができます。マカフィーは、MITRE ATT&CK に基づきセキュリティイベントにタグ付けして視覚化する初の CASB プロバイダーとなります。

マカフィーのシニアバイスプレジデント兼クラウドセキュリティ担当ゼネラルマネージャーのラジブ・グプタ（Rajiv Gupta）は、次のように述べています。「セキュリティ担当者は MITRE ATT&CK のような反復的なプロセスやフレームワークを活用して、エンドポイントとネットワークに対する脅威を緩和し、対応しています。しかし、これまでのところ、クラウドの脅威や脆弱性は見慣れないパラダイムを示しています。セキュリティ担当者は、MVISION Cloud を利用することで、クラウドの脅威や脆弱性を MITRE ATT&CK といった共通言語に置き換え、ランブックをクラウドまで拡張し、クラウドの脆弱性を把握して先制的に対応し、企業のセキュリティを向上させることが可能になります。」

マカフィーの調査結果によると、多くの企業が自社のクラウドサービスに対して、平均月 485 回超の外部からのサイバー攻撃を受けています。MITRE ATT&CK が統合されたことにより、クラウドサービスへの攻撃に焦点が当てられ、防御面でのギャップを識別し、MVISION Cloud から直接ポリシーと設定変更を行うことが可能になります。

McAfee MVISION Cloud との MITRE ATT&CK の統合により、以下の機能を含む、クラウド攻撃や脆弱性のリスクを緩和するための新機能が提供されます。

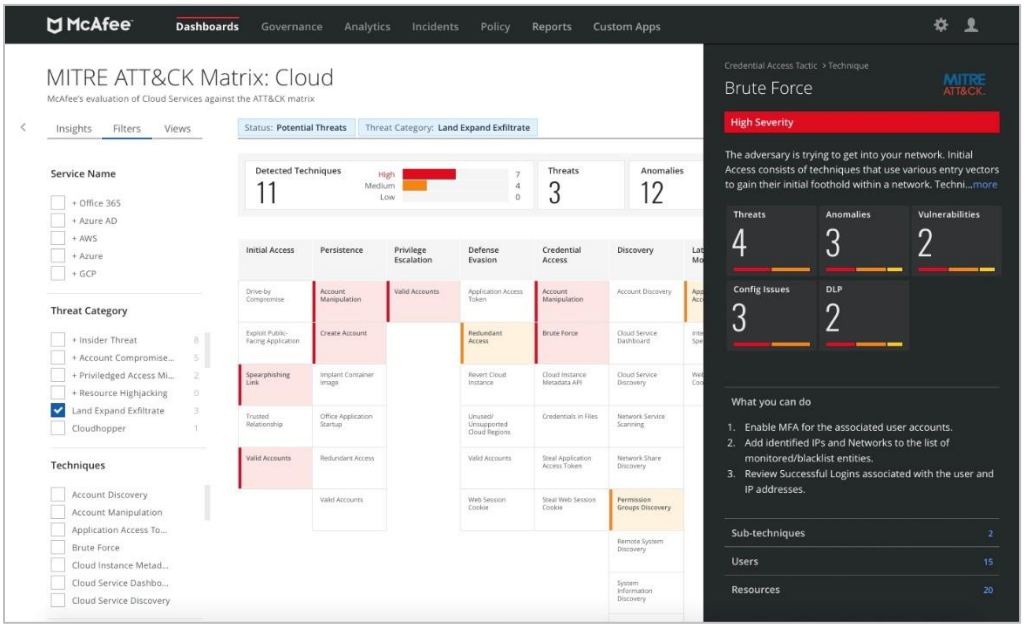
- **リアクティブからプロアクティブへの進化**：セキュリティ担当者は MITRE ATT&CK を導入した McAfee MVISION Cloud を通じて、SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）、IaaS（Infrastructure-as-a-Service）などの複数の環境に渡り阻止可能な潜在的な攻撃の視覚化が可能に
- **サイロ化を打破**：セキュリティ担当者は、フィルタリング済みのクラウドセキュリティインシデントを、API を介して SIEM や SOAR(Security Orchestration Automation and Response)プラットフォームに取り込み、デバイスやネットワークの脅威調査に使用するのと同じ MITRE ATT&CK フレームワークにマッピングが可能に

- **直接対応**：McAfee MVISION Cloud は、クラウドセキュリティポスチャ管理（CSPM）を新たなレベルへと引き上げ、セキュリティ管理者に特定の MITRE ATT&CK の敵対的戦術に対応する SaaS、PaaS、及び IaaS 環境のクラウドサービス構成の推奨事項を提示

McAfee MVISION Cloud に MITRE ATT&CK が導入されたことにより、インシデントを手動で並べ替えて MITRE ATT&CK などのフレームワークにマッピングしたり、クラウドの脅威や脆弱性のための個別のフレームワークを学習して運用したりする必要がなくなりました。特にクラウドネイティブの脅威が一段と増加する中で、こうした作業は煩雑で時間がかかる恐れがあります。MVISION Cloud を使用すれば、セキュリティ担当者はすべての脅威インシデントを自動的に MITRE ATT&CK にマッピングし、実行されたクラウド攻撃や実行に向けて進行中のクラウド攻撃のすべてを確認することが可能になります。また、インシデント、アノマリ、脅威、脆弱性を包括的に、MVISION Cloud の単一の画面で確認することも可能です。

参考情報：

- Cloud Threat Investigation 101: Hunting with MITRE ATT&CK（英語）
- Blog：MVISION Cloud への MITRE ATT & CK の統合 より精度の高い防御へ
- McAfee MVISION Cloud



MVISION Cloud のダッシュボード画面

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。詳細は https://www.mcafee.com/ja-jp/ をご覧ください。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/ja-jp/ ）
広報担当 戸田
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20 階
Tel: 070-2680-0731 Fax: 03-5428-1480
hiromi_toda@mcafee.com