Threat Insights（脅威インサイト）

日々、世界各地で新たなセキュリティ脆弱性が報告されています。そして、これらの脆弱性を悪用する新たな攻撃が定期的に発生しています。連日世界中で何千もの新しいマルウェアの亜種がリリースされています。

課題

DDoS 攻撃といった既知の脅威からの保護など簡単です。**しかし今日では、ネットワークやノード/エンドポイントを保護するのではなく、重要でかつ貴重なデータを保護することが重要です。これは、ユーザ、アクセスに使用するデバイス、そしてゼロトラスト セキュリティを確立するステップであるコンテキストと状況認識の検証で実現されます。** 従来のファイアウォールや IDS/IPS は、このアプローチ向けに設計されていません。可観測性は、ユーザとエンティティの行動分析、および効果的な脅威インテリジェンスとセキュリティ態勢管理ソリューションにとって必要です。さらに、ITOps と SecOps の分離したアプローチにより、構成やアクセス ポリシーが変更され、知らないうちにパフォーマンスに影響を与えたり、ユーザへのアプリケーション アクセスが完全にシャットダウンされたりする可能性があります。

セキュリティのために、アプリケーション/ネットワークのパフォーマンスを犠牲にする必要もありません。**どのネットワークでも、包括的なハイブリッド クラウド セキュリティ監視は、複数のベンダーと複数のドメインのコラボレーションによって実現され、それぞれがセキュリティの保証と保護を提供するためにそれぞれの役割を果たします。**

ソリューション

Ennetix の目標は、ネットワーク上のすべてのパケットとコンピュータ上で実行されるすべてのアプリケーションの出所の全体を見つけ出し、記録することです。パケットについては、パケットを生成したデバイス、パケットを送信したデバイス上のアプリケーション、そのパケットの開始方法、アプリケーションをコンパイルした組織、アプリケーションを実行したユーザ、ユーザのログイン元、およびユーザがどのように自分自身を認証したかを知る必要があります。

Ennelix xVisor の可観測性と検出は、ユーザとアプリケーションの関係を基礎と出発点とし、“Trust Nothing” という新しいパラダイムで成功するために不可欠な継続的な**ユーザエンティティビヘイビア分析 (UEBA)** を提供します。xVisor は、ネットワーク トラフィック (南北と東西の両方) とエンドポイント データをサードパーティの脅威インテリジェンス データとシームレスに組み合わせて、ユーザとアプリケーションの関係の完全なエンドツーエンドの可視性を提供します。xVisor は、多くの攻撃に共通する動作とキル チェーンの検出に重点を置いています。これにより、我々は常に先手を打つことができます。

xVisor の革新的な分析技術には、プロセスとエンティティの動作の分類と予測、アプリケーション/プロセス/プロバイダーの起源、新しい攻撃キルチェーンの特定などが含まれます。xVisor は、アクセス拒否、セキュリティ ポリシーの変更などによるパフォーマンスの低下を相関させることができます。さらに、xVisor は、サードパーティのアプリケーションコードベース分析、開発者チームの整合性と起源の保証などを使用した DevSecOps 統合を通じて、ソフトウェア サプライ チェーンのセキュリティ管理も可能にします。

おわりに

AIOps は、脅威に関する Insight（洞察）と、セキュリティ体制の変更による潜在的なパフォーマンスへの影響や低下の事前検証がなければ不完全です。Ennetix は、ネットワークとエンドポイントのデータ、およびサードパーティの脅威インテリジェンス ソースを包括的に統合することで、ネットワークのセキュリティを確保するために尽力しています。

NewGras

国内でのお問い合わせ先：NewGras,Inc.

https://www.newgras.com