BAS（Breach & Attack Simulation）

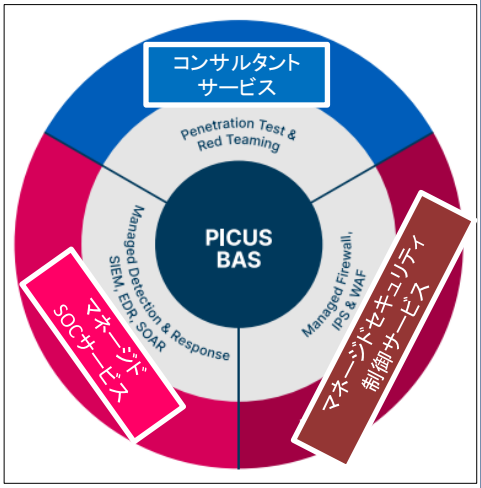
Picus「サイバー防御検証プラットフォーム」

MSSP向け使用事例
Picusによるソリューション概要

近年、マネージドセキュリティサービスプロバイダ(MSSP: Managed Security Services Provider)は、新しい顧客要件についていくために且つ競合他社から抜きん出るために、自社が提供する内容を拡大しています。

調査会社フォレスター(Forrester)は、「マネージド侵入検出/防止システム及びマネージドファイアウォールなどの実証済みのサービスは今では下降傾向にあり、その代わりに、マネージド検出・対応(MDR: managed detection and response)、セキュリティオーケストレーション自動化・対応(MSOAR: security orchestration automation and response)、及びマネージドセキュリティアナリティクス(MSA: managed security analytics)などの最新サービスが急速に成長している」とレポートしています。

又、フォレスターは、「顧客は、プロバイダは消極的であり、コンテキスト的でアクション志向の修復を提供できていない、と感じている。代わりに、ベンダがクライアントにとっての『アラートファクトリー(alert factories)』として機能している」と強調しています。MDR、MSOAR、及び他の新しいSOCサービスは、この欠点に対処できる可能性がありますが、比較的高価であり、予算的に問題です。



侵害・攻撃シミュレーション(BAS: Breach and Attack Simulation)プラットフォームは、MSSPが考慮すべき新しい視点を提供します。脅威中心の検証を自動化された機能として提供するBASプラットフォームは、

・コストを低減し、既存のマネージドサービスの品質を改善します。
・新しい収益機会を開きます。

Picus SecurityのBASプラットフォームは、MSSP運用をより競争力のある構造の方へ変換すること、新しいサービス提供を生み出すこと、及び年間経常収益(ARR: annual recurring revenue)を増加させることを支援するように設計されています。

Picus BASは、主要な防止テクノロジー、SIEM、EDR及びSOARなどの検出テクノロジー、サービスデスクプラットフォーム、脆弱性管理ソリューション、並びにレポートツール及びプロビジョニングツールとシームレスに統合します。これにより、潜在的なリスクの識別、対応及び軽減の各プロセスに対する自動化機能を強化し、コンサルタントサービス、マネージドSOCサービス、及びマネージドセキュリティ制御サービスの価値を付加します。

●柔軟なライセンスモデルによって経常収益を増加させる

MSSPは、説得力のあるセキュリティサービスを提供する必要があるだけではなく、柔軟な価格モデルでそれを提供する必要があります。**Picusの都度前払いのトランザクションライセンス及びバルクライセンスのオプションにより、確実にMSSPパートナーは最も適切な価格を顧客に提供することができます。**

このソリューション概要では、以下のBAS使用事例について詳述 します。

1） コンサルタントサービス
2） マネージドSOCサービス
3） マネージドセキュリティ制御サービス

侵害・攻撃シミュレーション(BAS)テクノロジー及び継続的なセキュリティ検証(CSV: Continuous Security Validation)テクノロジーの成長は、
マネージドセキュリティサービスプロバイダがクライアントのためのセキュリティ成果を高めるとともに、新しい経常収益源、販売機会を生み出し、
コスト構造を最適化する機会を提供します!

顧客例

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

BAS（Breach & Attack Simulation）

1） コンサルタントサービス

● ペネトレーションテスト及びレッドチームサービスを提供するまでの時間を短縮する

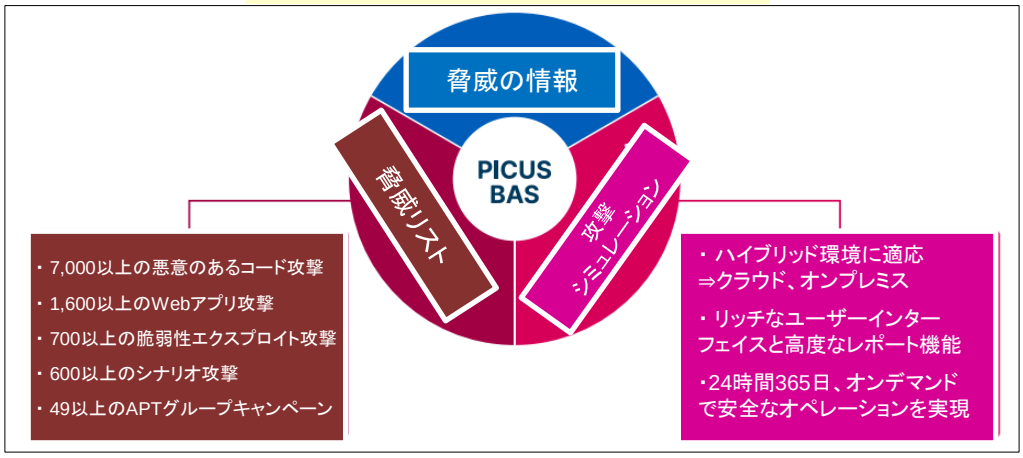
様々な範囲におけるペネトレーションテスト(ペンテスト)及びレッドチームなどの攻撃的セキュリティプラクティスは、敵対者エミュレーションを伴います。敵対者エミュレーションは、侵入的であり、殆どの場合、脅威サンプリング及びプラットフォーム関連の要件のために長時間にわたる手作業を必要とすることがあります。

Picusは、数クリック以内で展開することができ、必要な脅威ペイロード、アトミック技術、及び既製又は特注の高度なシナリオをネットワークセグメント及びエンドポイントにわたってわずか数分で結集させることができる、ロバストなエミュレーションエンジンを提供します。

ペンテスト及びレッドチーム演習においてPicusを使用すると、セキュリティプラクティショナーは以下を容易に行うことができます。

・範囲内の攻撃に対する防止レイヤ、ロギングレイヤ、及び検出レイヤにおけるレディネスステータスを特定する
・関連するCVE、CWE、OWASP、MITRE ATT&CK及びキルチェーンのリファレンス、深刻度レベル、及び脅威プロファイルに関するインサイトを得る
・軽減推奨事項を入手する

Picus「サイバー防御検証プラットフォーム」



Picus BASで強化されたペンテスト及びレッドチームは、以下の利点を提供します。
・工数の削減
・敵対者エミュレーション範囲の拡大

● BASで強化されたセキュリティポスチャ評価サービス

Picus BASプラットフォームを使用すると、MSSPは、クライアントの全体的なセキュリティポスチャ及びそれぞれの異なる防御コンポーネントがどのようにセキュリティポスチャに寄与しているかについてレポートするセキュリティポスチャ評価サービスを提供することができます。

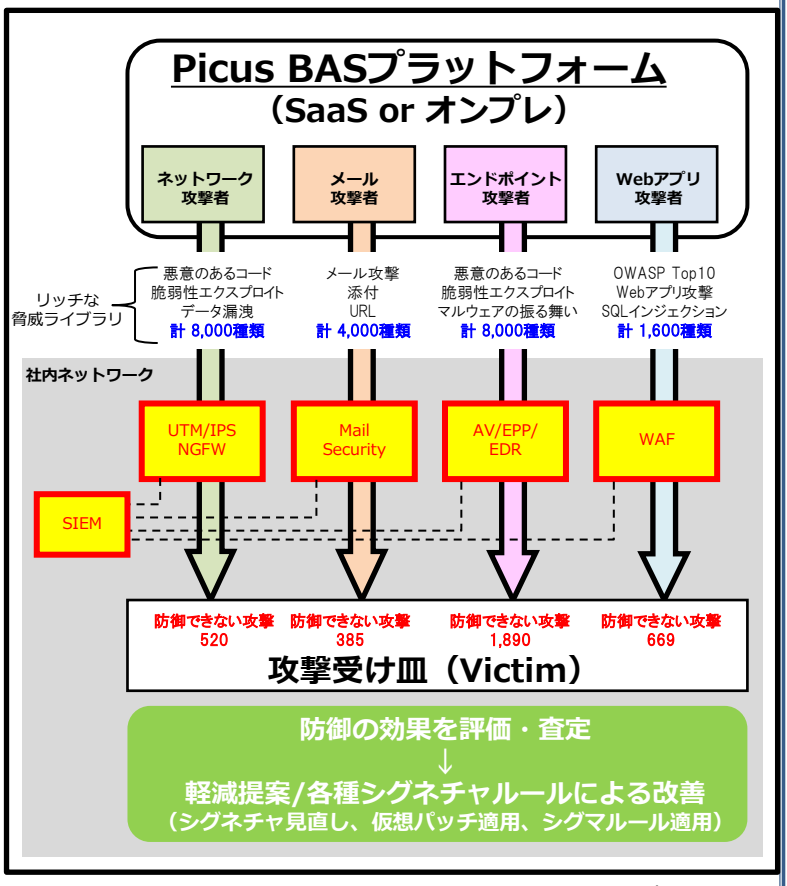
Picus BASプラットフォームには、リッチな脅威ライブラリが搭載されています。1万以上のマルウェア、ウェブアプリ攻撃及びエクスプロイトのサンプルに加え、数百の高度な攻撃シナリオを大規模ネットワークにわたって同時に数時間又は数日実行することができます。

Picusは、防止機能、ロギング機能、及び検出機能にわたって、それぞれのセキュリティ制御テクノロジー(SIEM、EDR、AV、EPP、NGFW、IPS、WAF、DLP、CASBなど)の寄与及び定義されたネットワーク経路又はエンドポイント上での効果の複合スコアを明らかにすることができます。

Picusは、エグゼクティブユーザ及び運用ユーザに合わせたリッチなレポートによって評価所見を提示します。

Picusは、その所見をベストプラクティスガイダンスの形での一般的な軽減提案及びベンダ固有の軽減提案、ログソース提案、IPS/WAFシグネチャ、シグマルール、ベンダ固有のEDRルール、及びベンダ固有のSIEM検出ルールで補完します。

セキュリティポスチャ評価は、**1回限りのサービス又は定期サービスとして提供することができ、新しいサービスエンゲージメントをもたらし、経常収益を増加させることができます。**



コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

2） マネージドSOCサービス

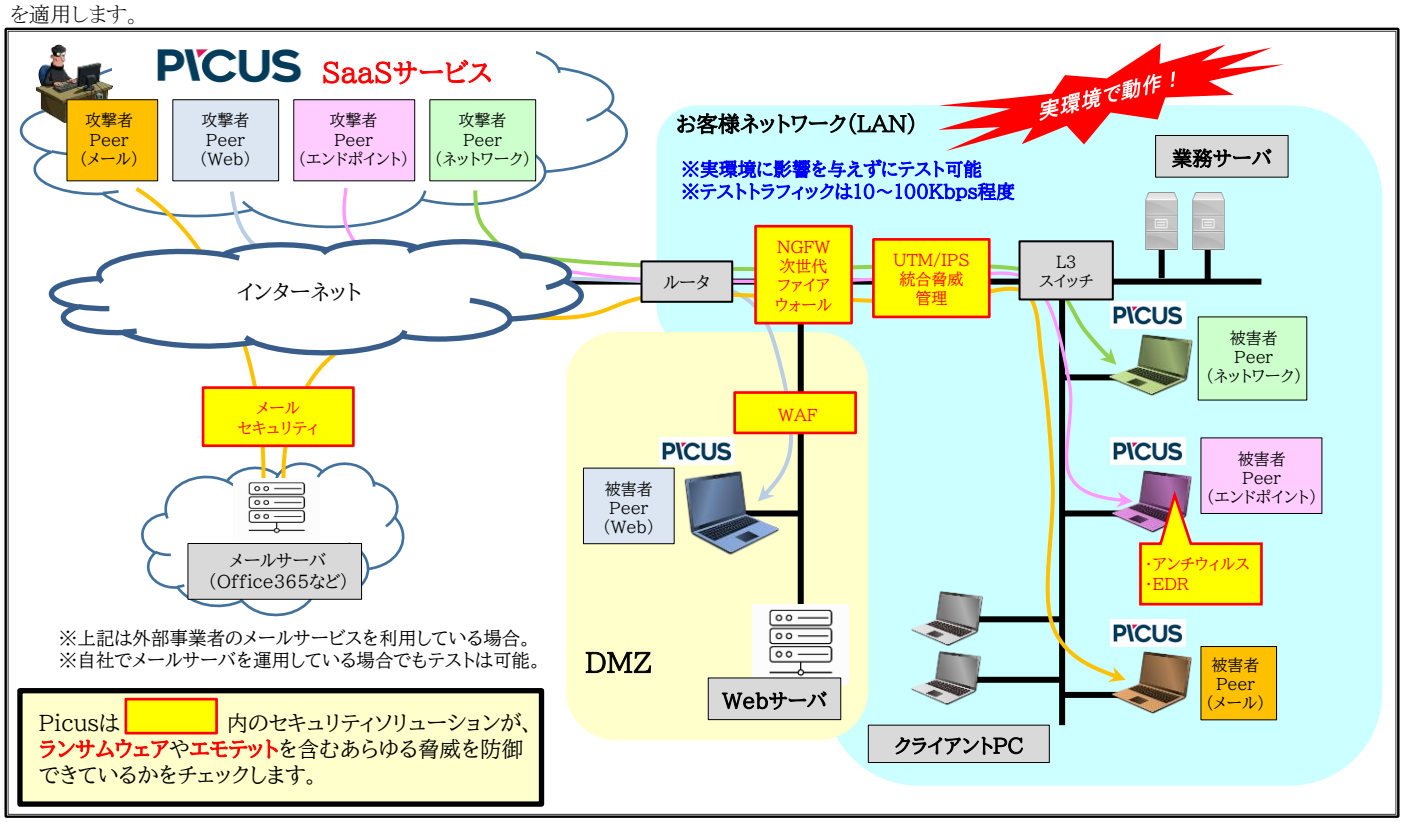
● 既存のSOCサービスを最適化する

検出・対応、SIEM、EDR、SOAR、及びセキュリティアナリティクスなどのマネージドSOCサービスは、セキュリティ成熟に向けた即時の進歩を顧客にもたらします。その一方で、MSSPは顧客環境を理解するとともに、コストを増加させてサービス品質を損なう可能性がある問題に対処する必要があります。

Picus BAS プラットフォームをツールボックスに追加すると、以下のような大きな利点があり ます。

・詳細な初期顧客評価により、現実的なスコーピング及び資産配分が可能になる
・セキュリティ制御、SIEM/EDRロギング、及び検出の継続的な検証は、顧客のセキュリティポスチャを改善し、インシデントの数を低減することにより コストを低減する
・Picusは、数千のベンダ固有の防止シグネチャ、ベンダ固有のSIEMルール及びEDRルール、並びにシグマルールを提供して、軽減及び インシデント対応を加速させる
・敵対者エミュレーションに基づくセキュリティアナリティクス及びMITREカバレッジに関連するメトリックは、QoSトランスペアレンシーをもたらし、 顧客の信頼を高める

Picusプラットフォームは、SIEMプラットフォーム及びEDRプラットフォームとシームレスに統合し、敵対者エミュレーションの所見に基づいて検出アナリティクスを適用します。



● 追加のサービスを提供する

MSSPが顧客のSOCチームの付加価値サービス としての役割を果たす場合、既存のサービスパッケージの一環として、以下のサービスを有償のプレミアムサービス又は無償のプレミアム機能として提供することができます。

・定期的な運用ヘルスチェック
顧客環境において、ハードウェア障害、ソフトウェアバグ、構成 ミス、接続性問題などの問題により、気付かれることなく、セキュリティ制御が正常に機能しなくなる場合があります。Picus BASプラットフォームは、従来の監視ソリューションが検出できないそのような運用ドリフトを迅速に突き止めることができます。

・脅威ハンティング
Picusの評価インサイト、脅威中心のログ・検出ルールの可視性、及び軽減コンテンツにより、アジャイルな脅威ハンティングサービスを効率的に且つ自信を持って提供することが可能になります。

・新興の脅威に対する態勢（準備）評価
顧客が新興の脅威又はゼロデイ脅威に対する態勢についてのレポートを希望する場合、Picusライブラリによって提供される現実世界のサンプルを利用することで、MSSPチームは顧客の態勢状態を容易にレポートすることができます。

※）標準的なセキュリティデバイス設定テストソリューションでは、IPS、WAF、サンドボックスツール及びプロキシなどのアプリケーションレイヤセキュリティデバイス向けに提供されるものが限られていますが、Picusは全ての防御ソリューションに有効です。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

3） マネージドセキュリティ制御サービス

● マネージドセキュリティ制御サービスのコストを低減する

マネージドファイアウォール、IPS、WAF、及び他の制御テクノロジー管理サービスは、今ではレガシーで利益率の低い MSSPサービスであると見なされています。顧客はこの競争市場 を利用して強力な防御対策を迅速に入手することができますが、MSSPは様々なニーズを有する多数の顧客のために複雑なテクノロジーを厳しい予算で管理する必要があります。

多くのセキュリティ制御は、新興の脅威に早い段階で対処するという状況において十分に活用されていません。標準的なベンダセキュリティポリシー以上のことをするには、性能 及びフォールスポジティブに対する懸念があることから、長い工数が必要です。Picus SecurityのBASは、セキュリティプラクティショナーが運用上の課題に対処すること及びセキュリティ制御の有効性をプロアクティブに高めることを支援する、多くの革新的な機能を提供します。

軽減を重視した最大のテクノロジーアライアンス* エコシステムを有するPicusは、ベンダ固有のシグネチャ及びポリシー管理コンテンツを用いて、ベンダに依存しない評価の有効性を高めます。24時間365日の評価又はオンデマンドの評価のいずれかによるリスクフリーでトランスペアレントなPicus評価は、セキュリティギャップを突き止め、サイバー攻撃を未然に阻止します。

● Picusを使用すると、MSSPは以下を行うことができます。

・性能が改善されたトランスペアレントなサービス品質メトリックを提供する
・若手スタッフをすぐに投入する
・運用コストを最大60%低減する

● サービスの品質を改善・証明する

MSSPの主な課題の1つは、様々なチームが恩恵を受けることができる粒度で提供されるサービスの価値を証明することです。

Picus BASで強化されたマネージドセキュリティ制御サービスは、攻撃タイプ、内部ウェブトラフィック、顧客対応ウェブアプリケーション、エンドポイント、データセンタ、クラウド環境、様々なVLAN など の様々な攻撃ベクトル上で標的にされたアプリケーションに関して、どのくらいセキュリティポスチャが経時的に高められたかを示すことを可能にします。

MSSPは、サービスレベルアグリーメントの一環としてMSSPが提供するセキュリティのレベルを選ぶことができます。

※）大型のセキュリティデバイステストアプライアンスは、ラボ環境におけるセキュリティデバイスの負荷/有効性テストに重点を置いていますが、Picusは全ての防御ソリューションの評価を実環境にリスクを与えることなく「**実環境上**」で動作するように設計されています。

Picus Security社について

2013年の設立以来、Picus Securityは侵害及び攻撃シミュレーション(BAS)テクノロジーのパイオニアであり、それ以来、企業のサイバーレジリエンスの向上を支援してきました。

Picus Securityは、学術的な背景と豊富な実務経験を持つサイバーセキュリティのベテランによって設立され、エンドツーエンドの攻撃耐性の可視性と改善の為の革新的なセキュリティ検証ソリューションを開発し、すべてのサイバー防御レイヤーにわたってサイバー攻撃を未然に防ぎます。

Picusの「完全なセキュリティ検証プラットフォーム」は、運用チームとエグゼクティブチームにきめ細かく実用的な洞察を提供し、プロアクティブな機能の構築を支援し、テクノロジーの利用を最大化して、投資収益率を最適化し、侵害のリスクを一貫して低く抑えます。
Picus Security社はVodafone、INGをはじめ世界中の大手企業から信頼を得ており、MasterCardが出資するなど注目されている企業の1つです。

防衛装備庁プロジェクト（下記）に *PicusのBASが使用されました!*

防衛関連企業60社に対してセキュリティシステムの現状を査定！

● 防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業

「防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業」参加企業募集
～～ 中小企業のサイバーセキュリティ能力強化のために ～～

防衛装備庁から委託を受けた「防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業」への参加企業を募集します。
本事業は、防衛装備品の製造に携わる防衛関連中小企業のサイバーセキュリティを担う人材育成支援、防衛関連企業の情報システム等の現状の把握及び評価及びサイバーセキュリティ強化策の実証支援を行います。
本事業においては、防衛省との間で防衛装備品の調達等に係る契約の実績がある企業又は今後新たに防衛省との契約に参入することを検討している企業のうち、防衛装備品の製造、維持・整備に携わる中小企業※を対象として募集します。

引用：公益財団法人 防衛基盤整備協会 https://ssl.bsk-z.or.jp/

Network Security Partners

cisco, citrix, CHECK POINT, Forcepoint, FORTINET, paloalto NETWORKS, TREND MICRO, McAfee, modsecurity Open Source Web Application Firewall, SNORT, imperva, f5

SIEM Partners

splunk>, Microsoft Sentinel, SIGMA, CyberRes ArcSight, Elastic Security, securonix, NETWITNESS An RSA Business, LogRhythm, CRYPTOSIM, IBM Security QRadar

EDR Partners

Microsoft Defender for Endpoint, SentinelOne, CROWDSTRIKE, vmware Carbon Black.

SOAR Partners

CORTEX XSOAR BY PALO ALTO NETWORKS

※更なるパートナーシップが定期的に追加されています。最新情報はpicussecurity.com/integrationsを参照してください。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp