



マイターアタック(MITRE ATT&CK)を基にした
統合情報セキュリティクラウドプラットフォーム

PLURA

XDR

eXtended Detection & Response



www.plura.io



QUBITSECURITY

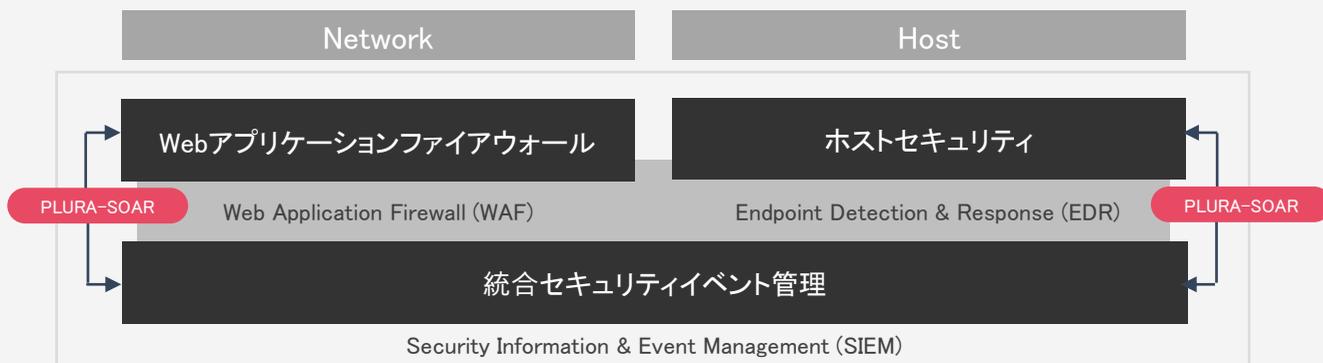
情報セキュリティは単一製品ではないプラットフォームで統合する必要があります。PLURA-XDRはWebアプリケーションファイアウォール、ホストセキュリティ、統合セキュリティイベント管理機能を統合した情報セキュリティプラットフォームです。



マイターアタックを基に実質的なセキュリティ脅威対応システムの構築



各機能を垂直に統合した革新的な情報セキュリティプラットフォーム



PLURAを選択しなければならぬ理由？

1. 統合管理のための高コストSIプロジェクトの不要
2. クラウドSECaaSでサブスクリプション型サービスとしても利用可能
3. 顧客にカスタマイズされたセキュリティポリシー機能を提供
4. リアルタイムログ分析で最も危険なAPT攻撃に対応

Unknown

Zero-Day

Application Vulnerability

情報セキュリティ及びネットワーク機器の相関分析基本機能へのエンドポイント(サーバーとPC)そして、Webのヘッダーと本文ログを分析してマイターアタックを基に、ハッキング攻撃に対応する革新製品です。



OSは監査ポリシーを設定しないと、ログは生成されません。
Webサーバーのアクセスログとともに本文ログ収集は、
ハッキング対応の出発点です。

● 主な特徴

- ✓ ゼロトラスト・アーキテクチャ (ZTA) をサポート
- ✓ 持続的標的型(APT)攻撃の検知及び対応
- ✓ アカウント乗っ取り攻撃クレデンシャルスタッフィング攻撃の検知及び対応
- ✓ Web 要求本文(Post-body)、応答本文(Resp-body) の分析
- ✓ SQLインジェクション、Webシェル、クロスサイトスクリプティング(XSS)の分析
- ✓ リアルタイム検知状況ダッシュボード、レポート及び統計サービス
- ✓ ジャンディ、テレグラム、ライン、グーグルチャットを通じて通知

運営体制(OS) ログ

Windowsサーバー： イベントログ、システムモニター(Sysmon)

Linuxサーバー： シスログ(syslog)、監査(audit) ログ

UNIXサーバー： シスログ(syslog)、監査(audit) ログ

Webサーバー ログ=アクセス+本文ログ

MS IIS、Apache HTTPD、Tomcat、NGINX、Node.js、Spring boot など

● PLURA-SIEM 連携サービス機能

- ✓ Webアプリケーションファイアウォール (PLURA-WAF)
- ✓ ホストセキュリティ (PLURA-EDR)
- ✓ 接続IPアドレス、ログイン(Login)、URL 分析サポート
- ✓ 相関分析のサポート
- ✓ 他社製品とsyslogの連携
- ✓ 検知通知Webhook及びチケットシステムとの連携
- ✓ 全体ログの収集、分析、保存サポート

OWASP TOP 10 Webハッキング攻撃を5W1Hに基づいてブロック、世界的に最も危険な攻撃であるクレデンシャルスタッフィング攻撃のブロック、個人情報・機密情報などデータ流出攻撃のブロック



Web本文分析でクレデンシャルスタッフィング攻撃とデータ流出のブロック、未知の攻撃に対応のためのSIEM連携、フルロギングサポートは必須です。

● 主な特徴

- ✓ ゼロトラスト・アーキテクチャ (ZTA) をサポート
- ✓ SQLインジェクション攻撃のブロック
- ✓ アカウント乗っ取り攻撃クレデンシャルスタッフィング攻撃のブロック
- ✓ 全体Web ログ分析で未知の攻撃に対応
- ✓ 応答本文分析でデータ漏洩攻撃に対応
- ✓ 要求及ぶ応答本文サイズ分析で異常予兆の検知
- ✓ TLS/SSL証明書管理
- ✓ 定期メンテナンスのご案内管理
- ✓ リアルタイム検知現状ダッシュボード、レポート及び統計サービス
- ✓ ジャンディ、テレグラム、ライン、グーグルチャットを通じて通知

攻撃検知は単一パケットだけでなく、
SIEM連携による相関分析を行い
Web攻撃に最適な対応を提供します。

● PLURA-SIEM 連携サービス機能

- ✓ アカウントログイン情報の収集、分析
- ✓ クレデンシャルスタッフィング攻撃・ボリュメトリック収集、分析、保存
- ✓ Webサイト改ざんの検知
- ✓ 攻撃IPアドレスの収集、分析、保存
- ✓ 攻撃URL情報の収集、分析、保存
- ✓ 全体ログ情報の収集、分析、保存



- 2018. 科学技術情報通信部、「優秀情報保護技術・製品」に選定
- 2019. 韓国発明振興院、「優秀発明品」優先購入推薦に選定
- 2020. 調達庁、「革新製品」指定認証(統合ログ管理PLURA)
- 2021. 米国・中国特許登録
- 2022. TTA、GS認証1等級獲得



CONTACT

+82-70-8802-0306
sales@qubitsec.com
www.plura.io

