DATA SHEET

FortiSOAR

SOC チーム向けセキュリティインシデントレスポンスシステム

FortiSOAR は、SOC チーム向けに設計された、セキュリティのオーケストレーション、自動化（オートメーション）、レスポンス（SOAR）の包括的なワークベンチとして、増え続ける大量のアラート、手作業での反復的プロセス、リソース不足への効率的な対応を可能にします。特許取得済のカスタマイズ可能なこのセキュリティオペレーションプラットフォームによって、プレイブックとインシデントのトリアージの自動化、そして攻撃の識別、防御、対抗によるリアルタイムの減災が可能になります。FortiSOAR は、300 以上のセキュリティプラットフォームと 3,000 以上のアクションとのシームレスな統合により、SOC チームの生産性を最適化します。その結果、迅速なレスポンスと無駄のない隔離が可能になり、減災の時間が数時間から数秒へと短縮されます。

SOCの一般的な課題

過剰なアラート

反復的タスク

ツールの混在

担当者の不足

ハイライト

FortiSOAR によって、SOC チームは以下の作業を迅速かつ安全に進められるようになります。

- シンプルで使いやすい GUI を利用して、セキュリティアラート、インシデント、指標、資産、タスクを管理
- 誤検知を回避し、重要なアラートだけに集中できるようにすることで、SOC チームの生産性を向上
- カスタマイズ可能なレポートとダッシュボードを利用して、ROI、MTTD、MTTR を追跡
- ビジュアルプレイブックデザイナーにおいて 300 以上のセキュリティプラットフォーム、3,000 以上のアクションと統合し、ワークフローやコネクタを自動化
- わかりやすく監査も可能なプレイブックとカスタムモジュールを採用して常に変化する調査要件を処理することで、人為的なミスを最小限に抑制
- 協調的な単一コンソールから、真のマルチテナント対応分散型アーキテクチャで構築されたネットワークセキュリティソリューションを拡張
- 自動化された誤検知フィルタリングで実際の脅威を特定し、類似する脅威やキャンペーンを FortiSOAR の推奨エンジンで予測
- 自動化、インシデントの関連付け、脅威インテリジェンスや脆弱性データを活用して反復的タスクを回避
- FortiSOAR の自動化テンプレートをカスタマイズして活用することで時間とリソースを節約し、SOC プロセスの効率性と有効性を向上
- セキュリティインシデントの発見に要する時間を数時間から数秒へと大幅に短縮

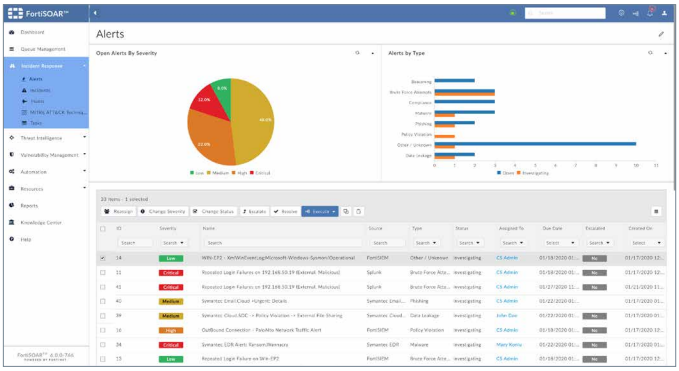
主な機能と特長

ロールベースのインシデント管理

エンタープライズ向けのロールベースのインシデント管理ソリューションである FortiSOAR は、フィールドレベルでのロールベースの堅牢なアクセス制御機能を提供し、SOC のポリシーやガイドラインに基づく機密データの管理を可能にします。

自動フィルタリング機能を備え、カスタマイズも可能なフィルターグリッドビューでアラートやインシデントを容易に管理できるため、実際の脅威の分析に注力できるようになります。アラートやインシデントの発生時には、直感的なユーザーインターフェースを活用してダイナミックなアクションやプレイブックを実行すると同時に、関連する脅威データを分析できます。

FortiSOAR の推奨エンジンは、過去に特定されたケースに基づいて脅威の深刻度、資産、ユーザーなどのさまざまなフィールドを予測します。SOC アナリストは、ケースのグループ化やリンク付けに利用して類似するアラートや共通する脅威あるいは犯罪者を発見し、関連するキャンペーンを特定できます。



ロールベースのダッシュボードとレポート

SOC チームは、ロールベースのダッシュボードとレポートが提供する定量化可能な測定基準を使用して、調査や SOC パフォーマンスをきめ細かく測定、追跡、分析できます。

FortiSOAR には、業界標準のペルソナ重視型ダッシュボードテンプレート、直観的なドラッグアンドドロップ対応ビジュアルレイアウトビルダーなど、すぐに利用できるツールライブラリが付属しているため、SOC チームは最適なツールを利用して時間やリソースを最大限に有効活用できます。包括的なチャート、リスト、カウンター、パフォーマンス指標は、詳細なビューや有用なデータモデルの作成に役立ちます。FortiSOAR は、インシデントの解決、インシデントの概要、週単位のアラートやインシデントの進捗、IOC の概要などの業界標準レポートも提供します。さらに、NIST によって定義された幅広いインシデントフェーズにおける MTTR や MTTD、アナリストの負荷、エスカレーション率、自動化の ROI、その他の SOC パフォーマンス指標などの測定基準を追跡します。

マルチテナント環境のサポート

FortiSOAR は、拡張性、耐障害性、セキュリティを兼ね備えた分散型アーキテクチャによる真の分散型マルチテナント対応製品で、MDR などのサービスを提供しながら地域やグローバルの SOC 環境を運用する MSSP を支援します。

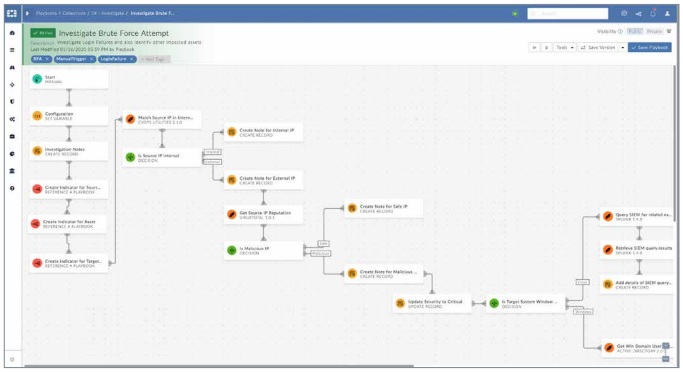
自動化されたワークフローをリモートから特定のテナントに対して実行できるため、顧客特有の環境への対応や製品の多様性への対応が合理化されます。また、マスターノードへのデータフローの制御に対する要求の承認にテナントを関与させることもできます。テナント毎に、専用のアラート、インシデントのビュー、レポート / ダッシュボード、フィルタービューを作成することも可能です。

ビジュアルプレイブックビルダー

FortiSOAR のビジュアルプレイブックデザイナーを使用すると、SOC チームは最も効率的な方法でプレイブックの設計、開発、デバッグ、制御、そして活用が可能になります。

300 以上の OOB ワークフローの統合、3,000 以上の自動化されたアクション、開発を容易にする包括的な表現ライブラリ、プレイブックのシミュレーションと参照、Python などのコードをワークフローで実行する機能、バージョン管理、プライバシー制御、クラッシュ時の復旧、ループなどの高度なステップ制御、エラー処理、通知などの機能を使用し、直感的なデザインのドラッグアンドドロップ対応インターフェースから複数のステップを結び付けることができます。

拡張可能な FortiSOAR のプラットフォームでは、フィールド、ビュー、権限をカスタマイズして新しいモジュールを定義し、自動化されたワークフローやプレイブックをその上位に作成することができます。これにより、アナリストは脆弱性や脅威の管理、さらに法規制やコンプライアンスに対応するソリューションを容易に利用可能になります。



FortiSOAR による ROI の最大化

ステップ	手作業	FortiSOAR
情報を拡充して IOC を識別	45 ～ 60 分	3 分
SIEM からイベントのトリアージを実行	20 分	1 分
ZIP をデトネーションエンジンに送信	1 ～ 6 時間	1 分
影響を受けたデバイスの隔離	10 分	1 分
インシデントの分析、作成、注釈付け	60 分	5 分
IOC をファイアウォール（FortiGate など）でブロック	45 分～ 2 時間	2 分
減災とインシデントレスポンス	60 分～ 6 時間	5 分
インシデント概要レポートを準備して送信	2 ～ 3 時間	2 分
所要時間総計	**4.5 ～ 15 時間**	**20 分**

コネクタと統合

FortiSOAR のサードパーティ製コネクタおよび統合機能により、デスクトップセキュリティソフトウェア、ディレクトリ、ネットワークインフラストラクチャ、そしてその他のサードパーティ製セキュリティシステムなどの何百もの製品への無制限アクセスが可能となり、ROI の最大化、セキュリティのオーケストレーション、自動化（オートメーション）、そしてレスポンス（SOAR）によるネットワークの比類ない可視性と制御が実現します。FortiSOAR は、他のベンダーやテクノロジーとのシームレスな統合が可能です。FortiSOAR との統合を可能にするコネクタの一部を以下に記載します。

ネットワークとファイアウォール	FortiOS、Cisco Meraki MX VPNファイアウォール、Infoblox DDI、CISCO Umbrella Enforcement、Empire、CISCO Firepower、ForeScout、Zscaler、Imperva Incapsula、NetSkope、RSA Netwitness Logs and Packets、PaloAltoファイアウォール、CISCO ASA、SOPHOS UTM-9、FortiGateファイアウォール、Arbor APS、F5 Big-IP、Proofpoint TAP、Check Pointファイアウォール、CISCO Catalyst、Citrix NetScaler WAF、Sophos XG、Cisco Stealthwatch、Pfsense、Symantec Messaging Gateway
脆弱性管理	Rapid7 Nexpose、Kenna、Qualys、Tripwire IP360、Symantec CCSVM、Tenable IO、ThreadFix、Tenable Security Center
サポートチケット管理	ConnectWise Manage、Foresight、Zendesk、ServiceAide、Manage Engine Service Desk Plus、Salesforce、BMC Remedy AR System、OTRS、Request Tracker、JIRA、Pagerduty、RSA Archer、Cherwell、ServiceNow
DevOps	AWS Athena、AWS S3、Twilio、IBM BigFix、AWS EC2
エンドポイントセキュリティ	Endgame、Trend Micro Control Manager、CrowdStrike Falcon、FireEye HX、Carbon Black Defense、Malwarebytes、McAfee EPO、Symantec EDR Cloud、Microsoft WMI、TrendMicro Deep Security、Symantec EPM、Symantec DLP、WINRM、NetBIOS、Microsoft SCCM、Microsoft SCOM、CISCO AMP、Carbon Black Protection Bit9、CYLANCE Protect、SentinelOne、Carbon Black Response、TANIUM
脅威インテリジェンス	EmailRep、AlienVault USM Central、Trend Micro SMS、Malware Domain List、Infocyte、Attivo BOTsink、FireEye ISIGHT、Vectra、Phishing Initiative、Threatcrowd、ThreatConnect、CRITS、McAfee Threat Intelligence Exchange、Facebook ThreatExchange、Intel 471、Soltra Edge、Anomali STAXX、Recorded Future、AlienVault OTX、MISP、DARKTRACE、IBM X-Force、ANOMALI THREATSTREAM、BluVector、ThreatQuotient
分析	FortiSIEM、RSA Netwitness SIEM、Sophos Central、Rapid7 InsightIDR、LogPoint、Micro Focus ArcSight Logger、Alienvault USM Anywhere、xMatters、Sumo Logic、LogRhythm、Syslog、Elasticsearch、McAfee ESM、IBM QRadar、ArcSight、Splunk
Fortinet Connectors	FortiMail、FortiEDR、FortiAnalyzer、FortiGate、FortiSandbox、FortiGuard Webfilter Lookup、FortiOS

* FortiSOARは、上記リストに記載されていないベンダーおよびテクノロジーとの統合も可能です。

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ