DATA SHEET

FortiSOAR™

SOC 팀과 엔터프라이즈를 위한 적응적 보안

FortiSOAR™는 전체적인 보안 오케스트레이션, 자동화 및 대응 워크벤치로써, SOC 팀에서 끊임없이 수신되는 알림, 반복적 수동 프로세스, 리소스 부족 문제에 효율적으로 대응할 수 있도록 설계되었습니다. 사용자 정의가 가능하고 특허를 가지고 있는 이 보안 운영 플랫폼은 기업에 자동화된 대응책, 사고 분류, 실시간 복구 업데이트를 제공하여 공격을 식별, 방어하고 조치를 취할 수 있도록 지원합니다. FortiSOAR™은 300개 이상의 보안 플랫폼 및 3,000개 이상의 작업을 매끄럽게 통합하여 SOC 팀의 생산성을 최적화합니다. 따라서 대응 속도가 빨라지며, 손쉽게 공격을 억제하고, 보안 조치의 시간을 몇 시간에서 몇 초로 단축합니다.

일반적인 SOC 문제

너무 많은 알림

반복적인 작업

서로 분리된
각종 프로그램들

인력 부족

하이라이트

FortiSOAR는 SOC 팀이 다음과 같은 대응을 신속하고 안전하게 실행하도록 지원합니다.

- 간편하고 손쉬운 GUI를 통해 보안 알림, 사고, 지표, 자산, 작업 관리
- 오탐지를 제거하고 중요한 알림에만 집중시켜 SOC 팀의 생산성 향상
- 사용자 정의가 가능한 보고서와 대시보드를 통해 ROI, MTTD, MTTR 추적
- Visual Playbook Designer 내 자동화, 300개 이상의 보안 플랫폼 통합 및 자동화된 워크플로와 커넥터를 위한 3,000개 이상의 작업
- 명확하고 확인 가능한 대응책과 사용자 정의 모듈을 적용해 끊임없이 변화하는 요구 사항을 처리함으로써 인적 오류 최소화
- 단일한 협업 콘솔에서 진정한 멀티 테넌트 분산 아키텍처로 네트워크 보안 솔루션 확장
- 자동화된 오탐지 필터링으로 실제 위협을 파악하고, FortiSOAR의 권고 엔진으로 유사한 위협과 이벤트 예측
- 자동화, 사고 상관관계, 위협 정보, 취약성 데이터를 통해 반복적 작업 제거
- FortiSOAR의 자동화 템플릿을 수정 적용하여 시간과 리소스를 절약함으로써 SOC 프로세스의 효율성과 효과 개선
- 보안 사고 발견 시간을 몇 시간에서 몇 초로 단축

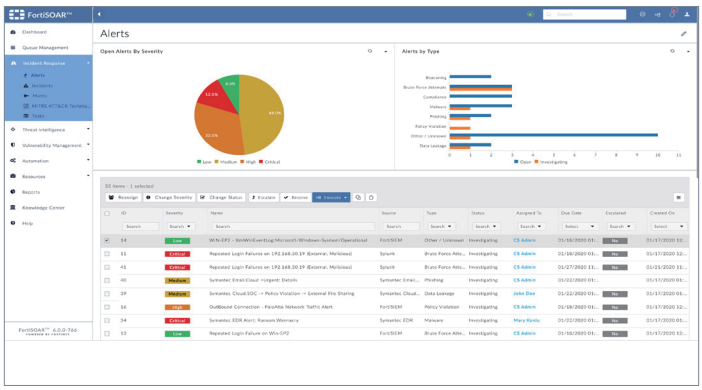
주요 기능

역할 기반 사고 관리

FortiSOAR™의 엔터프라이즈 역할 기반 사고 관리 솔루션은 SOC 정책과 가이드라인에 따라 민감한 데이터를 관리할 수 있는 안정적 필드 수준 역할 기반 액세스 제어 기능을 기업에 제공합니다.

자동화된 필터링이 적용되고 사용자 정의가 가능한 필터 그리드 뷰에서 알림과 사고를 쉽게 관리할 수 있어 분석 전문가들이 실제 위협에 집중할 수 있습니다. 알림과 사고에 동적인 조치와 대응책을 적용하고, 직관적인 사용자 인터페이스에서 상관관계가 있는 위협 데이터를 분석합니다.

FortiSOAR의 권고 사항 엔진은 이전에 식별한 사례를 바탕으로 심각도, 자산, 사용자 등의 여러 가지 필드를 예측하고, SOC 분석 전문가들이 이러한 필드를 그룹화하고 연결하여 유사한 알림, 일반적인 위협, 개체와 관련된 중복과 이벤트를 찾아내도록 돕습니다.



역할 기반 대시보드 및 보고

역할 기반 대시보드와 보고는 SOC 팀이 측정 가능한 지표로 조사 결과와 SOC 성과를 측정, 추적 및 분석할 수 있는 기능을 제공합니다.

FortiSOAR's™에 구축된 업계 표준 라이브러리, 방법 중심적인 대시보드 템플릿, 직관적인 드래그 앤 드랍 방식의 시각적 레이아웃 빌더는 SOC 팀이 시간과 리소스를 최적화할 수 있는 최고의 도구가 될 것입니다. 종합적인 도표, 목록, 카운터, 성과 지표가 자세한 뷰와 유익한 데이터 모델을 개발하도록 도와줍니다. 또한, FortiSOAR는 사고 마감, 사고 요약, 주간 알림, 사고 진행 상황, IOC 요약 등에 대한 업계 표준 보고서를 제공합니다. MTTR, 여러 NIST 승인 사고 단계에 대한 MTTD, 분석 전문가 로드, 보고 비율, 자동화 ROI, 기타 SOC 성과 지표 등의 지표를 추적합니다.

멀티 테넌시

FortiSOAR™는 엄밀하게 분산된 멀티 테넌트(Multi-Tenant) 제품을 제공하며, 회복력과 안전성을 갖춘 분산된 확장형 아키텍처를 사용합니다. 따라서 MSSP는 MDR과 유사한 서비스를 제공하면서도 지역 및 글로벌 SOC 환경에서 운영을 지원할 수 있습니다.

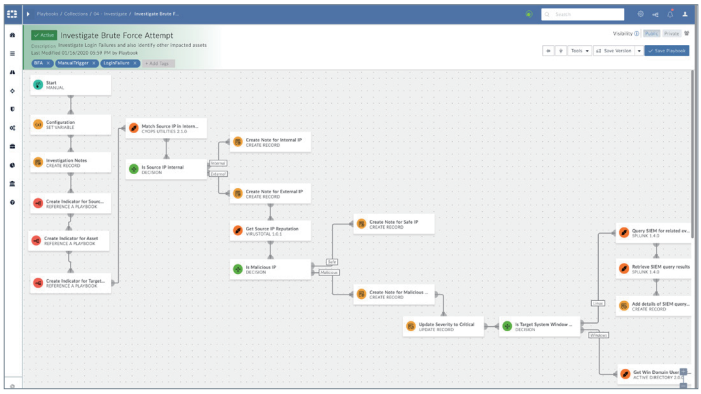
특정 테넌트에 대한 자동화 워크플로를 원격으로 실행하는 기능을 사용하면 고유한 고객 환경 및 제품을 간단하게 처리할 수 있습니다. 또한, FortiSOAR는 마스터 노드에 대한 데이터 흐름을 제어하기 위한 승인 요구 사항에 테넌트를 사용합니다. 그 외에 다른 테넌트 기능에는 테넌트별 알림, 사고 뷰, 보고서 및 대시보드, 필터 뷰를 생성하는 기능 등이 포함됩니다.

시각적 대응책 구성

FortiSOAR™의 Visual Playbook Designer를 사용하는 SOC 팀은 가장 효율적으로 대응책을 설계하여 디버깅하고, 관리, 사용할 수 있습니다.

직관적인 디자인에는 여러 단계를 연결해주는 드래그 앤 드롭 방식 인터페이스가 포함되며, 300개 이상의 OOB 워크플로 통합, 3,000개 이상의 자동화된 작업, 간편한 개발을 위한 종합적 수식 라이브러리, 대응책 시뮬레이션 및 참조, 워크플로에서 Python과 같은 코드 실행 기능, 버전 관리, 개인정보 관리, 충돌 복구, 지능적 단계 관리(예: 루핑), 오류 처리, 알림 등을 사용합니다.

FortiSOAR의 확장 가능한 플랫폼은 새 모듈을 정의하는 기능을 제공합니다. 필드, 뷰, 권한을 사용자 정의하고 그 위에 스마트 자동화 워크플로와 대응책을 생성하여 분석 전문가가 취약성 및 위기 관리, 규제, 규정 준수를 위해 솔루션을 지원하는 기능을 단순화합니다.



FortiSOAR로 ROI 최대화

단계	수동	FortiSOAR
아티팩트를 강화하여 IOC 식별	45~60분	3분
SIEM에서 이벤트 분류	20분	1분
Zip을 데토네이션 엔진에 제출	1~6시간	1분
영향을 받은 기기 격리	10분	1분
사고 분석, 생성 및 주석 첨부	60분	5분
방화벽(예: FortiGate)에서 IOC 차단	45분~2시간	2분
복구 업데이트 및 사고 대응	60분~6시간	5분
사고 요약 보고서 작성 및 발송	2~3시간	2분
합계	**4.5~15시간**	**20분**

커넥터 및 통합

FortiSOAR 타사 커넥트 및 통합은 데스크톱 보안 소프트웨어, 디렉터리, 네트워크 인프라, 기타 타사 보안 시스템을 포함한 수백 개의 제품에 무제한 액세스를 제공하여 ROI를 최대화하고, 보안 오케스트레이션, 자동화 및 대응(SOAR)을 통해 네트워크 전체에 독보적인 가시성과 제어 기능을 제공합니다. FortiSOAR는 다른 공급업체 및 기술과 매끄럽게 통합됩니다. 다음은 FortiSOAR가 통합되는 커넥트 샘플입니다.

네트워크 & 방화벽	FortiOS, Cisco Meraki MX VPN Firewall, Infoblox DDI, CISCO Umbrella Enforcement, Empire, CISCO Firepower, ForeScout, Zscaler,Imperva Incapsula, NetSkope, RSA Netwitness Logs And Packets, PaloAlto Firewall, CISCO ASA, SOPHOS UTM-9, Fortigate Firewall, Arbor APS, F5 Big-IP, Proofpoint TAP, Check Point Firewall, CISCO Catalyst, Citrix NetScaler WAF, Sophos XG, Cisco Stealthwatch, Pfsense, Symantec Messaging Gateway
취약성 관리	Rapid7 Nexpose, Kenna, Qualys, Tripwire IP360, Symantec CCSVM, Tenable IO, ThreadFix, Tenable Security Center
티켓 관리	ConnectWise Manage, Foresight, Zendesk, ServiceAide, Manage Engine Service Desk Plus, Salesforce, BMC Remedy AR System, OTRS, Request Tracker, JIRA, Pagerduty, RSA Archer, Cherwell, ServiceNow
개발 운영	AWS Athena, AWS S3, Twilio, IBM BigFix, AWS EC2
엔드포인트 보안	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
위협 정보	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 THREAT-STREAM, BluVector, ThreatQuotient
분석	Fortinet 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 커넥터	FortiMail, FortiEDR, FortiAnalyzer, FortiGate, FortiSandbox, FortiGuard Webfilter lookup, FortiOS

* FortiSOAR는 위의 제품 외에도 다른 공급업체 및 기술과 통합될 수 있습니다.

www.fortinet.com/kr

서울특별시 강남구 영동대로 325에스타워 14 /15층 전화: 080-559-8989 Email: **kr-callcenter@fortinet.com**

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® 및 FortiGuard®와 몇몇 기타 표시는 Fortinet, Inc.의 등록 상표이며 본문에 기재된 여타 Fortinet 이름 또한 Fortinet의 등록 및/또는 일반 법적 상표일 수 있습니다. 다른 모든 제품 또는 회사명은 각각 해당하는 소유주의 등록상표일 수 있습니다. 본문에 기재된 성능 및 기타 지표는 이상적인 실험 조건 하에서 수행한 사내 연구소 테스트 결과로 획득한 것이며, 실제 성능 및 기타 결과는 다양하게 나타날 수 있습니다. 네트워크 변수, 서로 다른 네트워크 환경 및 기타 조건 등이 성능 결과에 영향을 미칠 수 있습니다. 본문의 어떤 내용도 포티넷에서 법적 구속력이 있는 약속을 한다는 의미는 아니며, 포티넷은 명시적으로나 묵시적으로나 모든 보증을 부인하는 바입니다. 다만 포티넷에서 법무 자문 위원의 서명 결재를 거친, 법적으로 유효한 서면 계약서를 체결하여 해당 계약서에 기재된 제품이 내용을 분명히 밝힌 특정 성능 지표에 따른 성능을 발휘할 것을 보증하는 경우는 예외입니다. 그러한 경우, 그와 같은 법적으로 유효한 서면 계약서에서 분명히 밝힌 특정 성능 지표만이 포티넷에 법적 구속력을 발휘합니다. 의미를 확실히 해두기 위하여, 그와 같은 보장은 포티넷의 사내 연구소 테스트를 실시한 조건과 동일한 이상적인 조건하에서의 성능에만 국한됩니다. 포티넷은 명시적으로든 묵시적으로든 본문에 따른 각종 약정, 대변 및 보장 등을 전체적으로 부인하는 바입니다. 포티넷에는 본 출판물의 내용을 변경, 수정, 전송 또는 여타의 형태로 개정할 권한이 있으며 본 출판물의 내용은 최신 버전을 적용하는 것으로 합니다. 포티넷은 명시적으로든 묵시적으로든 본문에 따른 각종 약정, 대변 및 보장 등을 전체적으로 부인하는 바입니다. 포티넷에는 본 출판물의 내용을 변경, 수정, 전송 또는 여타의 형태로 개정할 권한이 있으며 본 출판물의 내용은 최신 버전을 적용하는 것으로 합니다.