FORTINET

FortiSOAR™

Top Security Orchestration and Response (SOAR) Software

보안 관제 센터 효율 제고 및 인시던트 대응 시간 단축

eROP

이롭은 보안 오케스트레이션 및 자동화
대응을 전문적으로 지원하는 포티넷 파트너입니다.
이롭과 함께 기업의 보안 경쟁력 혁신을 경험해 보십시오.

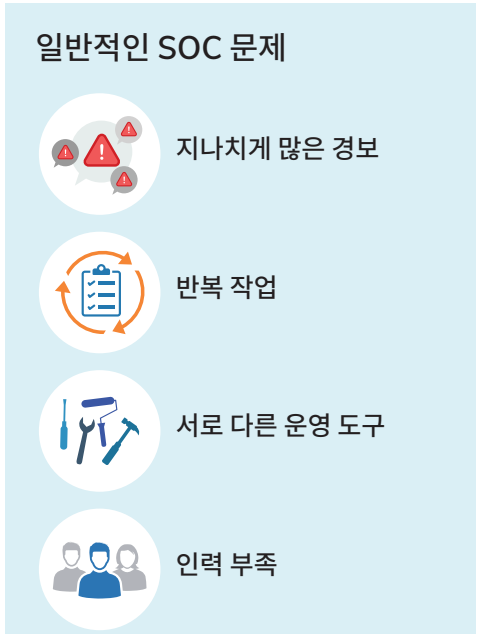
데이터 시트

FortiSOAR™

설치 지원 플랫폼

FortiSOAR는 SOC팀이 계속해서 유입이 증가하는 경보, 반복적인 수동 프로세스 및 리소스 부족에 효율적으로 대응할 수 있도록 설계된 종합적인 보안 오케스트레이션, 자동화 및 대응 워크벤치입니다. 이 특허 출원된 맞춤형 보안 관제 플랫폼은 자동화된 플레이북과 인시던트 분류, 실시간 복구 업데이트를 통해 기업에서 공격을 식별, 방어, 대응하도록 지원합니다.

FortiSOAR는 350개 이상의 보안 플랫폼과 3000개 이상의 작업을 원활하게 통합하여 SOC 팀 생산성을 최적화합니다. 이 솔루션을 적용하면 더 빠르게 대응하고, 절차가 간소화되어 완화 시간이 몇 시간에서 몇 분으로 단축됩니다.



하이라이트

- 간소하고 사용이 간편한 GUI를 통해 보안 경보, 인시던트, 지표, 자산 및 태스크 관리
- 오탐을 없애고 중요한 경보에만 집중해 SOC 팀의 생산성 강화
- 사용자 정의 가능한 보고서와 대시보드를 통해 ROI, MTTD, MTTR 추적
- 350여 개의 보안 플랫폼 통합과 자동 워크플로 및 커넥터 작업 3,000여 건을 포함한 비주얼 플레이북 디자이너 내에서 자동화 수행
- 명확하고 감사 가능한 플레이북과 사용자 지정 모듈을 사용해 끊임없이 바뀌는 조사 요구 사항을 처리하므로 작업자의 실수가 발생할 가능성 최소화
- 단일, 협업형 콘솔에서 진정한 멀티테넌트 분산형 아키텍처를 사용해 네트워크 보안 솔루션 확장
- 자동 오탐 필터링을 사용해 진짜 위협을 식별하고 Forti-SOAR의 ML 기반 추천 엔진을 사용해 유사한 위협과 공격 캠페인 예측
- 자동화, 인시던트 상관관계, 위협 인텔리전스, 취약점 데이터를통해 반복적인 태스크 배제
- 기본 내장 인시던트 워룸(War Room)을 활용해 위기 관리와 협업형 P1 인시던트 조사 간소화
- 보안 인시던트 검색 시간을 몇 시간에서 몇 초로 단축
- FortiSOAR 모바일 애플리케이션을 활용해 중요한 의사 결정을 내리고 이동 중에도 최신 정보 입수
- 커넥터 빌더 마법사를 사용해 제품 사용자 인터페이스 내에 손쉽게 커넥터 빌드 및 편집
- 유연한 배포 옵션 - VM, 호스팅 또는 클라우드, Forti-Cloud, AWS, Azure에서 이용 가능하며 FAZ/FMG에서 관리 확장 프로그램으로도 이용 가능

주요 기능

간소화된 역할 기반 인시던트 관리

FortiSOAR의 엔터프라이즈 역할 기반 인시던트 관리 솔루션은 조직에 강력한 필드 수준 역할 기반 액세스 제어 권한을 제공하여 SOC 정책 및 지침에 따라 민감한 데이터를 관리할 수 있도록 합니다.

사용자 정의가 가능한 필터 그리드 보기에서 자동화된 필터링 기능을 사용하여 경보와 인시던트를 쉽게 관리하여 분석가가 실제 위협에 집중할 수 있습니다. 경보 및 인시던트에 대해 동적 작업 및 플레이북을 실행하고 직관적인 사용자 인터페이스에서 상호 연관된 위협 데이터를 분석합니다. FortiSOAR의 ML 기반 추천 엔진은 이전에 식별한 사례를 기반으로 심각도, 자산, 사용자 등과 같은 다양한 필드를 예측하여, SOC 분석가가 이러한 필드를 함께 그룹화 및 연결하여 유사한 경보, 공통 위협 및 엔티티를 포함한 중복 항목 및 캠페인을 식별하도록 지원합니다.

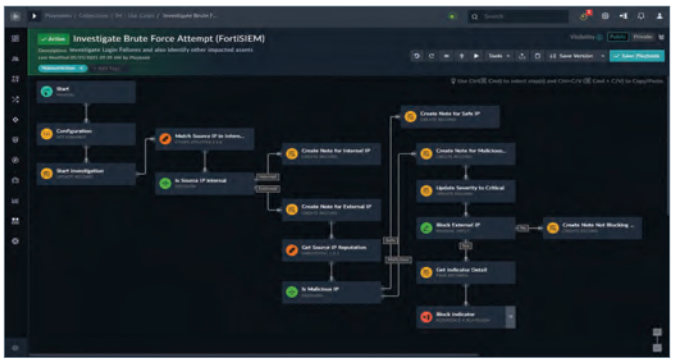
FortiSOAR 모바일 앱은 인시던트 관리에 새로운 차원을 추가하고 사용자가 경보 대기열 모니터링, 중요한 플레이북 트리거, 이동 중 중요한 승인 제공 등과 같은 조치를 취할 수 있도록 합니다.

진정한 멀티테넌트

FortiSOAR는 회복력이 뛰어나고 안전하며 확장이 가능한 분산형 아키텍처를 통해 진정한 분산형 멀티테넌트 제품 서비스를 제공하여 MSSP가 MDR과 같은 서비스를 제공하면서 동시에, 지역단위 및 전 세계 단위의 SOC 환경에서 잘 운영되도록 지원하도록 합니다.

특정 테넌트에 대해 자동화 워크플로를 원격으로 실행하는 기능, 테넌트 플레이북, 모듈, 보기를 원격으로 관리하는 기능으로 고유한 고객 환경 및 제품 다양성 취급이 간소화되었습니다. 또한 FortiSOAR는 마스터 노드로의 데이터 흐름 제어라는 승인 요구 사항이 있는 경우에도 테넌트를 포함합니다.

다른 테넌트 기능에는 테넌트별 경보, 인시던트 보기, 보고서 및 대시보드, 필터 보기 작성이 있습니다. 서비스 제공업체 및 고객은 완벽한 격리 및 관리를 위한 전담 SOAR 테넌트 노드와 고객의 온프레미스 통합을 활용하는 데 사용할 수 있는 경량 FortiSOAR 에이전트 중에 선택할 수 있습니다. 다양한 시나리오에 잘 맞출 수 있는 뛰어난 유연성을 제공하는 하이브리드 모델도 가능합니다.



비주얼 플레이북 빌더

FortiSOAR의 비주얼 플레이북 디자이너를 통해 SOC 팀은 가장 효율적인 방법으로 플레이북을 설계, 개발, 디버그, 제어 및 사용할 수 있습니다.

여러 단계를 한 번에 묶은 드래그 앤 드롭 인터페이스, 350개 이상의 OOB 워크플로 통합, 3,000개 이상의 자동 작업, 간편하게 개발할 수 있는 종합적 표현식 라이브러리, 플레이북 시뮬레이션 및 참조, 파이썬 등과 같이 워크플로에서 코드를 실행하는 기능, 버전 관리, 개인정보 관리, 충돌 복구, 고급 단계 관리(예: 루핑, 오류처리, 알림, 실행 취소/다시 실행) 등과 같이 직관적인 설계를 제공합니다. 플레이북 우선순위 지정, 공개/비공개 표시 여부, 시뮬레이션 엔진 등과 같은 고급 기능이 잘 오케스트레이션된 솔루션을 설계하는 데 더욱 뛰어난 수준의 제어를 제공합니다.

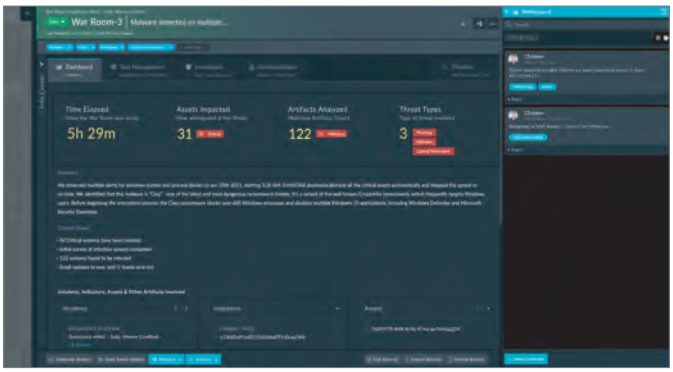
FortiSOAR의 확장 가능한 플랫폼은 필드, 보기 및 권한의 맞춤화를 통해 새 모듈을 정의하는 기능과 무엇보다 자동화된 스마트 워크플로 및 플레이북 생성 기능을 제공하여 취약점 및 위협 관리와 규제 및 규정 준수를 위한 솔루션을 지원하는 분석가의 업무를 간소화합니다.

주요 기능

인시던트 War Room을 통해 위기 관리

FortiSOAR는 공동 P1 인시던트 조사 간소화에 사용할 수 있는 전용 위기 관리 프레임워크인 인시던트 War Room을 제공합니다. 중대한 인시던트는 주위에서 War Room을 가동해 조직 전체에서 팀원을 신속하게 소집하는 트리거가 될 수 있습니다. MS Teams, Slack, Zoom 등과 같은 외부 협업 도구와 협력하여 작동할 수 있는 조사 전담 협업 자원을 할당, 모니터링 및 구성하기 위한 작업 관리를 위해 구성원마다 열람 가능한 항목을 제어하는 액세스 제어 기능이 기본 제공됩니다.

위기 관리를 위해 특별히 개발되어 알림 게시판 및 전용 보고 섹션 등과 같은 기타 중요한 요소를 관리합니다.

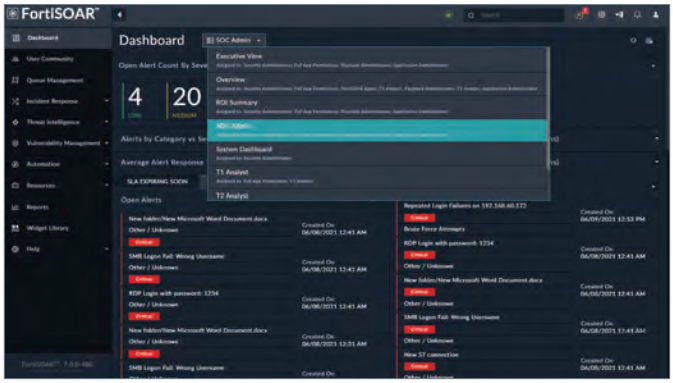


역할 기반 대시보드 및 보고

역할 기반 대시보드 및 보고 기능은 SOC 팀이 정량화할 수 있는 메트릭을 사용하여 조사 및 SOC 성능을 세부적으로 측정, 추적 및 분석할 수 있도록 합니다.

산업 표준, 개인 중심 대시보드 템플릿, 직관적인 드래그 앤 드롭 시각적 레이아웃 빌더로 구성된 FortiSOAR의 미리 작성된 라이브러리를 통해 SOC 팀은 시간과 리소스를 최적화하기 위한 최고의 도구를 갖춘 셈입니다. 포괄적인 차트, 목록, 카운터, 성능 메트릭은 다채로운 보기 및 유용한 데이터 모델을 작성하는 데 도움이 됩니다. 또한 FortiSOAR는 인시던트 종결, 인시던트 요약, 주별 알림 및 인시던트 진행 상황, IOC 요약 등에 대한 산업 표준 보고서를 제공합니다.

이것은 SOC 팀이 MTTR 및 승인된 다양한 NIST 인시던트 단계, 업무 부하, 에스컬레이션 비율, 자동화 ROI 및 기타 SOC 성능 메트릭 등 여러 메트릭을 추적할 수 있게 합니다.



위협 인텔리전스 관리

FortiSOAR는 향상된 위협 인텔리전스 관리 지원을 제공하여 FortiGuard와의 긴밀한 통합을 활용해 지표 평가, 위협 범주 및 위협 백과사전 액세스 권한을 무제한 조회하도록 합니다. 정형 및 비정형 피드의 수집은 CSV/STIX 파일에서 지표를 가져와 STIX형식으로 내보내는 기능으로 지원됩니다.

또한 분석가는 지표 공유, 지표 만료 및 제외 목록을 위해 TLP(Traffic Light Protocol)를 사용하여 지표를 훨씬 간단하게 관리할 수도 있습니다. 또한 FortiSOAR에는 표준 SIEM 및 UEBA 제품과 지표 공유를 위한 바로 사용 가능한 플레이북 여러 개가 포함되어 있습니다.

FortiSOAR 모바일 애플리케이션

FortiSOAR 웹 인터페이스의 확장인 FortiSOAR 모바일 애플리케이션은 즉각적인 승인, 알림 및 위협 모니터링과 같은 중요하고 긴급한 조치를 신속하게 이행해 SOC 팀과 경영진이 민첩하게 조치하고 이동 중에 중요한 정보를 제공할 수 있도록 합니다.

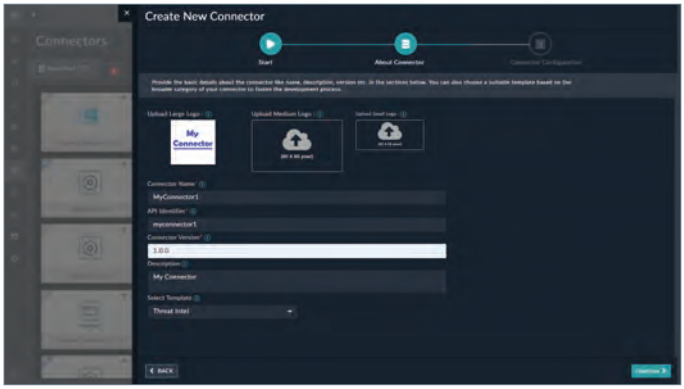
분석가는 애플리케이션의 풍부한 사용자 경험을 통해 FortiSOAR를 쉽게 탐색하여 레코드 보기 및 재할당, 승인 제공, 중요한 플레이북 트리거 및 경보 대기열 모니터링 등과 같은 작업을 실행할 수 있습니다.

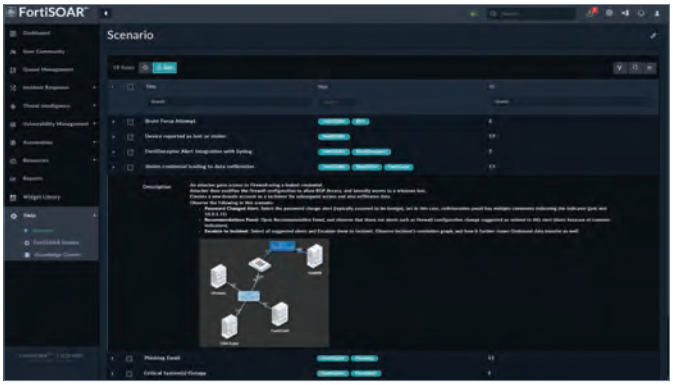
주요 기능

커넥터 및 위젯 생성 스튜디오

기본 제공 커넥터 마법사를 통해 분석가는 다양한 타사 제품의 데이터를 보내고 검색하기 위한 사용자 지정 커넥터를 쉽게 만들고 기존 커넥터를 쉽게 편집할 수 있습니다. 손쉽게 사용할 수 있는 인터페이스는 기본 제공 테스트 프레임워크를 제공하고 단계별 마법사 프레임워크를 사용하여 제품 UI에서 직접 간단하게 커넥터를 빌드할 수 있도록 합니다. 분석가는 기본 제공되는 여러 템플릿 중에서 선택해 커넥터를 쉽게 개발할 수 있어 모범 사례를 따르기 쉽습니다.

마찬가지로 위젯 생성 마법사를 사용하면 UI 내에서 새로운 사용자 정의 위젯을 구축해 사용자가 필요에 따라 데이터를 표현하는 방식에 제한을 받지 않도록 합니다.





인시던트 대응 콘텐츠 팩

FortiSOAR 인시던트 대응 콘텐츠 팩을 사용하면 분석가와 사용자가 FortiSOAR 인시던트 대응의 이점을 경험할 수 있습니다. 모듈식 아키텍처를 사용하여 빌드된 인시던트 대응 콘텐츠 팩은 효율적인 보안 오케이스트레이션, 자동화, 대응 솔루션을 최적의 방법으로 구성 및 구현하기 위한 모범 사례를 구현한 것입니다.

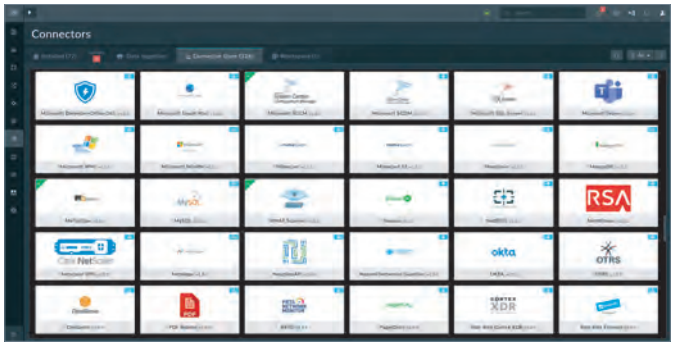
콘텐츠 팩은 다양한 기본 모듈, 종합적인 유틸리티 및 사용 사례 플레이북 모음, 산업 표준 대시보드 및 역할과 SOC 팀이 FortiSOAR 의 이점을 경험하고 유리하게 시작할 수 있도록 지원하는 많은 샘플, 시뮬레이션 및 교육 데이터로 구성되어 있습니다.

FortiSOAR로 ROI 극대화

단계	수동	FortiSOAR
아티팩트를 보강하여 IOC 식별	45~60분	3분
SIEM에서 받은 이벤트 분류 수행	20분	1분
데토네이션 엔진에 압축(Zip) 파일 제출	1~6시간	1분
영향 받는 장치 고립 시키기	10분	1분
인시던트 분석, 생성 및 주석 달기	60분	5분
방화벽(예: FortiGate)에서 IOC 차단	45분~2시간	2분
치료 및 인시던트 대응	60분~6시간	5분
인시던트 요약 보고서를 작성하여 전송	2~3시간	2분
전체 소요 시간	**4.5~15시간**	**20분**

커넥터 및 통합

FortiSOAR 타사 커넥터 및 통합은 데스크탑 보안 소프트웨어, 디렉토리, 네트워크 인프라 및 ROI를 극대화하는 기타 타사 보안 시스템을 포함한 수백 가지 제품에 대한 제한 없는 액세스를 제공하여 보안 오케스트레이션, 자동화 및 대응(SOAR)을 통해 네트워크 전반에서 따라 올 수 없는 가시성 및 제어 기능을 제공합니다.
FortiSOAR는 다른 공급업체 및 기술과 원활하게 통합되고 새로운 커넥터를 쉽게 생성하거나 기존 커넥터를 편집할 수 있도록 내장된 커넥터 빌더 마법사를 제공합니다.



다음은 현재 FortiSOAR가 제공하는 몇 가지 주요한 커넥터 통합 사항입니다.

포티넷 커넥터	FortiGate, FortiAnalyzer, FortiSIEM, FortiEDR, FortiNAC, FortiDeceptor, FortiSandbox, FortiMail, FortiGuard, FortiAI, FortiManager, FortiMonitor, FortiEMS
네트워크 및 방화벽	FortiGate, Cisco Meraki MX VPN Firewall, Infoblox DDI, CISCO Umbrella Enforcement, Cisco Meraki MX L7 Firewall, Empire, CISCO Firepower, ForeScout, Zscaler, Imperva Incapsula, NetSkope, RSA Netwitness Logs And Packets, PaloAlto Firewall, CISCO ASA, SOPHOS UTM-9, Arbor APS, F5 Big-IP, Proofpoint TAP, Check Point Firewall, CISCO Catalyst, Citrix NetScaler WAF, Sophos XG, Cisco Stealthwatch, Pfsense, Symantec Messaging Gateway, PRTG, Centreon
분석 및 SIEM	FortiSIEM, FortiAnalyzer, 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, ReversingLabs A1000
취약점 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
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 인텔리전스	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
개발 운영	AWS Athena, AWS S3, Twilio, IBM BigFix, AWS EC2
샌드박스	FortiSandbox, GitLab, ThreatSTOP, Intezer Analyze, FireEye AX, CISCO Threat Grid, URLSCAN.Io, Joe Sandbox Cloud, Koodous, Trend Micro DDAN, Symantec CAS, HYBRID-ANALYSIS, VMRAY, PaloAlto WildFire, Malwr, Lastline, SecondWrite, Cuckoo
이메일 및 이메일 보안	GSuite For GMail, Microsoft Exchange, SMTP, IMAP, Mimecast, Symantec Email Security Cloud, FireEye EX, CISCO ESA
조사	FortiAnalyzer, FortiSIEM, FortiMail, Securonix SNYPR, Symantec ICDx, Symantec Security Analytics, NMAP Scanner, Protectwise, PhishTank, CloudPassage Halo, TruSTAR, Have I Been Pwned, Farsight Security DNSDB, Cofense PhishMe, RSA Netwitness

* FortiSOAR는 여기에 나열된 것 외에도 다른 많은 공급업체 및 기술과 통합될 수 있습니다.

FORTISOAR 클라우드

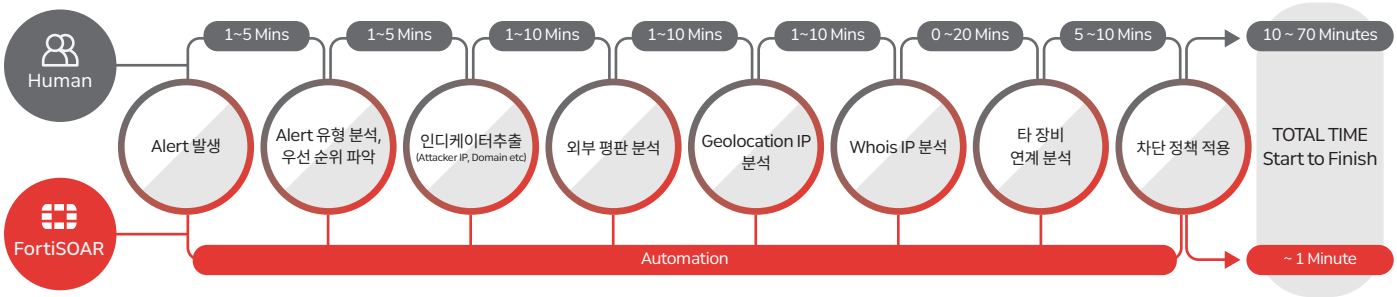
포티넷은 클라우드 기반 FortiSOAR 서비스를 통해 포티넷 관리형 FortiSOAR 플랫폼을 활용하고 싶어 하는 고객을 지원합니다.
고객과 파트너는 FortiCloud Single-Sign-On Portal에서 각자의 FortiSOAR 클라우드에 쉽게 액세스할 수 있습니다.

주문 정보

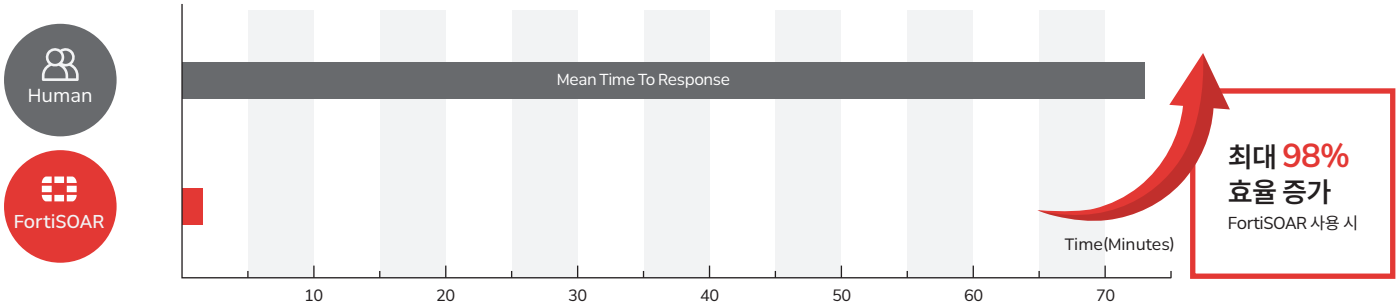
제품	SKU	설명
FortiSOAR 구독형 라이선스	FC-10-SRVMS-385-02-DD	FortiSOAR Enterprise Edition 1년 구독- 24x7 FortiCare 지원 이외에 사용자 2명 로그인 포함
	FC-10-SRVMS-386-02-DD	FortiSOAR Multi Tenant Edition 1년 구독 - 24x7 FortiCare 지원 이외에 사용자 2명 로그인 포함
	FC-10-SRVMS-387-02-DD	FortiSOAR Multi Tenant Edition - 전용 테넌트 1년 구독 - 24x7 FortiCare 지원 이외에 사용자 1명 로그인(포함)으로 제한됨
	FC-10-SRVMS-388-02-DD	FortiSOAR Multi Tenant Edition - 지역별 SOC 인스턴스 1년 구독 - 24x7 FortiCare 지원 이외에 사용자 1명 로그인 포함
	FC-10-SRVMS-384-02-DD	FortiSOAR User Seat License 1년 구독 - 24x7 FortiCare 지원 이외에 추가 사용자 1명 로그인
FortiSOAR 영구 라이선스	LIC-FSRENT-2	FortiSOAR Enterprise Edition - 사용자 2명 로그인 포함(영구 라이선스)
	LIC-FSRMTT-2	FortiSOAR Multi Tenant Edition - 사용자 2명 로그인 포함(영구 라이선스)
	LIC-FSRMTD-1	FortiSOAR Multi Tenant Edition - 전용 테넌트 - 사용자 1명 로그인으로 제한됨(포함)
	LIC-FSRMTR-2	FortiSOAR Multi Tenant Edition - 지역별 SOC 인스턴스 - 사용자 2명 로그인 포함(영구 라이선스)
	LIC-FSRAUL-1	FortiSOAR User Seat License - 추가 사용자 로그인(영구 라이선스) - 1명씩 추가
	FC1-10-SRVMP-248-02-DD	FortiSOAR Enterprise Edition을 위한 FortiCare 24x7 지원
	FC2-10-SRVMP-248-02-DD	FortiSOAR Multi Tenant Edition을 위한 FortiCare 24x7 지원
	FC3-10-SRVMP-248-02-DD	FortiSOAR Multi Tenant - 전용 테넌트를 위한 FortiCare 24x7 지원
	FC4-10-SRVMP-248-02-DD	FortiSOAR Multi Tenant - 지역별 SOC 인스턴스를 위한 FortiCare 24x7 지원
FortiSOAR 클라우드	FC-10-SRCLD-385-02-DD	FSR CLOUD Enterprise Edition 1년 구독 - 24x7 FortiCare 지원 이외에 사용자 2명 로그인 포함
	FC-10-SRCLD-386-02-DD	FSR CLOUD Multi Tenant Edition 1년 구독 - 24x7 FortiCare 지원 이외에 사용자 2명 로그인 포함
	FC-10-SRCLD-384-02-DD	FSR CLOUD User Seat License 1년 구독 - 24x7 FortiCare 지원 이외에 추가 사용자 1명 로그인

FortiSOAR 기대효과

탐지된 침해정보 분석 업무(Network Indicator Analysis)



MTTR(Mean Time To Response) 소요 시간 비교



SOAR 제품 비교 검토 시, 필수 고려 사항

트렌드 충족을 위한 단순 도입이 아닌, 도입 효과를 볼 수 있는 SOAR 제품 선정 기준

"SOAR"
우리 조직에 최적화된, SOC 업무가속화 환경 만들기

팀협업 공간 제공 및 커스터마이징 가능 여부

SOAR + IR + VM
+ ChatOps
+ Custom Modules
+ Dashboards and Reporting

역할기반 사용자 권한분배 여부

RBAC Data Partitioning (Horizontal and Vertical), Playbook, Dashboard

손쉬운 플레이북 기능 여부, 진짜 쉬운가?

Connectors, Simulation, Debugger

유연한 아키텍쳐 지원 여부

(확장성, 멀티테넌시, 환경)

Active/Active HA, Distributed Multi-Tenancy, Enterprise, MSSP

기술지원체계

SOAR를 우리 조직에 맞추고, 성공적인 구축/운영을 가능하게 하는 인력과 체계가 준비되어 있는가?

FortiSOAR 특장점

사용자 정의 Layout 설계를 통한 분석가 UX 향상

- 분석 단계 정의 및 분석 화면 재배치/편집, 버튼 추가
- 직관적인 분석 GUI 환경
- HTML 웹 에디터 지원
- Chat Bot 형태 등 커뮤니케이션 제공

No Code 기반 모듈 및 데이터 필드 커스텀 기능

- 맞춤형 메뉴/기능 추가
- 고객사가 필요한 데이터 필드 추가
- 추가된 메뉴 및 데이터를 플레이북에서 사용 가능
- 데이터 간 Relationship 자동 구성

자동화 구현 편의성

- Drag & Drop으로 생성 가능
- 다양한 자동화 액션 지원
- 즉각적 에러 디버깅, 동작 과정 조회
- 플레이북 개발 편의성
- API Server 기능
- RESTful API 지원

eROP | FORTINET

(주)이룹 서울시 구로구 디지털로31길 38-21, 208호(구로동, E&C벤처드림타워3차) 08376
Tel. 02)3282-2303 | Email. sales@erop.co.kr | http://www.erop.co.kr