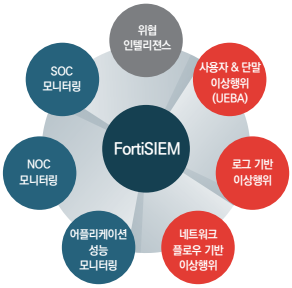
Fortinet SOC Solutions – FortiSIEM, FortiSOAR

포티넷 통합이상행위 관제 솔루션
지능형 SOC 업무 가속화 플랫폼

FortiSIEM – 통합이상행위 관제 솔루션

✓ 통합이상행위 관제 시스템

- SOC / NOC 통합
- 엔드포인트 / 네트워크 / 로그 모두 대응
- 시스템 자산 관리
- 위협 자동 대응
- 위협 인텔리전스 활용
- 머신러닝 기반 비정상 행위 탐지



✓ Security Fabric 시너지

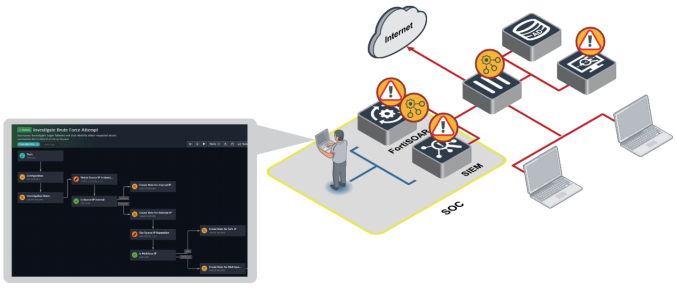
- SSL Inspection
- 광범위한 사이버공격 침입 경로 방어

✓ Endpoint Agent 특징

- 가벼운 초소형 에이전트
- 호스트 수준 행위 로그 수집
  * File Activity – Create, Delete, read…
  * File Upload / Download
  * Drive(USB) mount / unmount
  * Log on / off…
  * UEBA 관점 이상행위 탐지

Model	FortiSIEM-500F "Collector"	FortiSIEM-2000F "Supervisor"	FortiSIEM-3500G "Supervisor"
AIO License Capacity	N/A	Up to 500	Up to 2,000
EPS Capacity	5,000 ingestion	Up to 5,000 ingestion	Up to 40,000 ingestion
Form Factor	1 RU	2 RU	4 RU
CPU	Intel Xeon E3-1225V3 4C4T 3.20 GHz	Intel Xeon E5-2620V3 6C12T 2.40 GHz	2 x Intel Xeon Gold 5118 12C24T 2.30 GHz
Total Interfaces	4 x 1 GbE (RJ45)	4 x 1 GbE (RJ45)	2 x GbE RJ45 ports, 2 x GbE SFP ports, 2 x 25 GbE SFP28
Storage Capacity	3 TB (1 x 3 TB) Max. 4 x HDD	36 TB (12 x 3 TB) Max. 12 x HDD	96 TB (4 TB x 24) Max. 24 x HDD
Memory	DDR3 16 GB (2 x 8 GB)	DDR4 32 GB	DDR4 128 GB (16 GB x 8 ECC REG Memory)
Rack Units	1	2	4
AC Power Supply	1	2	2

FortiSOAR – 지능형 SOC 업무 가속화 플랫폼



Specification	Recommended	Minimum
CPU	8	8
Memory	32 GB	22 GB
Disk	1 TB (SSD)	500 GB (SSD)
NIC	1EA	1EA
비고	※ 설치 환경에 따른 권장사양 협의	

✓ SOC 업무 프로세스 통합

- 경고 / 인시던트 / 업무 프로세스 통합
- 보안팀 대응능력 상향평준화
- 이기종 다양한 운영 시스템 중앙 제어
- ROI / MTTD / MTTR 향상
- 사용자 에러 방지(Human Error)
- 사용자를 위한 강력한 커스터마이징 (UI&Report)

✓ 오케스트레이션 & 자동화(Playbook)

- 업무 프로세스 자동화
- 병렬 처리 / 큐 처리로 빠른 보안 위협대응
- 300+개 연동모듈
- 3,000+개 사용가능 플레이북 액션
- 단순 반복 작업 자동화
- SOC 사이버 피로도 감소
- 1,000+개 제조사 플레이북

엔드포인트에서 클라우드까지 단일 플랫폼 가시성 확보

자동화 기반 보안업무 플랫폼을 통해 SOC 업무 가속화