

SOC 도입으로 기업의 안전 지키기

최상의 효율을 위해서 보안 관제 센터(SOC)를 설치하거나 재구성하는 것을 고려하고 있습니까?

진화하는 물리 및 사이버 보안 위협으로부터 기업을 안전하게 지키려면 잘 설계된 SOC가 필수적입니다. SOC의 도입과 관련하여 고려해야 할 주요사항을 구성, 협업, 맥락, 명료성, 조율, 규정 준수, 사이버 보안이라는 7개 범주로 분류할 수 있습니다.

✓ 구성: 접근성과 유연성 확대

- **허브 레이아웃 최적화:** SOC를 전략적으로 배치하면 협업을 촉진하는 업무공간을 창조하고 모니터링 가시성을 최적화할 수 있습니다.
- **창문이 없는 공간 구성:** 보안을 보장하고 혼란을 최소화하려면 창문이 없고 출입이 제한되어 있어야 합니다.
- **기존 IT 인프라 점검:** 현재 어떤 유형의 IT 인프라를 보유하고 있습니까? 온프레미스, 클라우드 기반, 하이브리드 중 어느 것입니까? 기존 IT 인프라는 SOC 효율에 어떤 영향을 미칩니까?



기업들이 하이브리드 클라우드 보안으로 전환하는 이유

[알아보기](#)

✓ 협업: SOC 내부 및 외부에서 팀워크 강화

- **비디오 월 설치:** 실시간 피드를 표시할 비디오 월을 설치하여 전반적인 가시성을 향상합니다.
- **커뮤니케이션 도구에 투자:** Sipelia™와 같은 SIP 기반 커뮤니케이션 관리 도구를 사용하면, 정보를 쉽게 전송하고 원활히 소통할 수 있습니다.
- **전용 이메일 개설:** 커뮤니케이션을 향상을 위해 모든 종류의 요청을 수집하는 이메일 주소를 특정합니다.
- **디스패치 및 태스크 할당:** 미션을 효율적으로 할당하기 위해서 Mission Control™과 같은 협업 기반 의사결정 관리 시스템의 도입을 고려합니다.



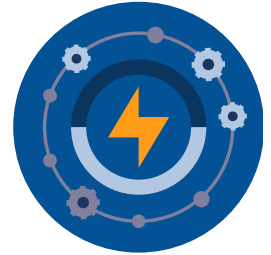
✓ 맥락: 융합형 뷰 확보

- **고급 매핑 기능 활용:** SOC의 매핑 도구를 활용하여 시설 전역의 이벤트를 쉽게 시각화하고 파악합니다.
- **IIoT 기기 연결:** 맥락에 대한 인식을 높이기 위해 IIoT 기기를 연결하고 데이터를 하나의 융합형 플랫폼에서 수집·관리합니다.
- **대시보드에 브라우저 윈도우 추가:** 뉴스 피드와 소셜 미디어 업데이트를 통합하여 외부 이벤트에 대한 인식이 용이합니다.



✓ 명료성: 정보 디지털화로 실천 가능한 인사이트 확보

- **규정 정립:** 사용자 친화적인 규정 정립으로 오경보를 없애고 오퍼레이터 간접비용을 줄입니다.
- **태스크 자동화:** 오퍼레이터가 비상시에 따를 수 있는 자동화된 워크플로를 생성하여, 규정 준수에 입각한 보안 절차에 기반해 알림이 처리되도록 합니다.
- **데이터 필터링:** 데이터를 필터링하는 자동화 도구를 실행하여 오퍼레이터가 잠재 위험을 재빨리 처리할 수 있도록 합니다.



✓ 조율: 효율적인 이벤트 확대 및 대응

- **동적 운영 절차:** Mission Control의 동적 운영 절차 도입으로 각기 다른 사건 단계에 맞춤형 대응이 가능합니다.
- **워크스테이션에서의 권한 확대:** 긴급 상황에서 더 빠르고 효율적으로 대응할 수 있도록 워크스테이션에 할당되는 권한을 확대합니다.



✓ 규정 준수: 규정 엄수 보장

- **사용자 권한 조율:** 사용자 권한을 세밀하게 조율하여 규정 준수를 보장합니다.
- **보고서 기능:** 종합적인 사건 보고서를 작성하여 포렌식 조사가 수월하게 진행되도록 합니다.



✓ 사이버 보안: 사이버 위협에 대한 대비

- **유지보수 업데이트 자동화:** 자동화된 태스크를 설정해, 기기 유지보수 업데이트와 시스템 상태에 대한 알림을 수신하고 사이버 보안을 유지합니다.
- **감사 로그:** 네이티브 포맷 내보내기과 파일 공유를 원활히 해주는 소프트웨어를 사용하되 감사 로그도 빈틈없이 유지합니다.



협업 기반 의사결정 관리 시스템으로
보안 관제 센터를 최적화하십시오.

[Mission Control 자세히 알아보기](#)