유형: 사이버 공격 대상: 전체	정리/요약 시트 **랜섬웨어 – 대량의 워크스테이션 사용 불가**	

1. 경고

하지 말아야 할 것	해야 할 것
삭제 금지: 모든 정보는 조사 증거로 사용됩니다.	보안운영센터(SOC) 및 정보 시스템 보안 책임자 대상 경고
암호화된 파일이나 애플리케이션을 열지 말 것: 감염을 중단시켜야 합니다.	SOC와 모든 정보 공유: 공격 규모 및 비상 대응 우선 순위 평가 목적
	SOC의 지시를 따를 것

2. 비상 조치

1. 중요한 시스템 격리:
   - 모든 네트워크 연결 해제
   - 컴퓨터에서 네트워크 케이블 분리
   - Wi-Fi 연결 해제
2. 모든 주변 장치 분리
3. 침해 범위 평가 및 증거 수집

3. 연속성 솔루션

모든 워크스테이션을 통해 활동 중요도 순에 따라 인터넷으로 액세스할 수 있는 가상화된 작업 환경 제공

4. 비즈니스 연속성 계획 활성화 기준

PCA 활동에 대한 최종 결정을 내리는 부서는 의사결정 위기 부서입니다.
기준 1: 워크스테이션의 5%를 사용할 수 없음
기준 2: 다른 사이트/법인/애플리케이션에 랜섬웨어를 퍼뜨릴 위험