제품 사양 문서

Contoso CipherGuard Sentinel X7

1. 제품 개요

1.1 소개

복원력이 우수한 고급 보안 제품인 Contoso CipherGuard Sentinel X7은 컴퓨터 네트워크 인프라를 강화하여 다양한 위협과 취약성을 방지할 수 있도록 세심하게 제작되었습니다. 이 문서에서는 Contoso CipherGuard Sentinel X7의 기술 사양, 특징 및 기능을 자세히 소개합니다.

1.2 주요 특징

- **방화벽 보호:** Contoso CipherGuard Sentinel X7은 상태 저장 검사 방화벽을 활용해 DPI(Deep Packet Inspection) 기술을 적용합니다. 그리고 애플리케이션 레이어에서 네트워크 패킷을 검사 및 분석하여 데이터 흐름을 세부적으로 제어합니다. 지속적으로 개선되는 네트워크 환경을 토대로 하여 방화벽의 규칙 집합이 동적으로 조정되므로 애플리케이션 레이어 공격 관련 위험을 완화할 수 있습니다.

- **IDPS(Intrusion Detection and Prevention System):** 기계 학습 알고리즘을 기반으로 구동되는 Contoso의 IDPS는 네트워크 트래픽 패턴과 변칙을 지속적으로 모니터링합니다. 그리고 서명 기반 검색, 변칙 검색 및 휴리스틱 분석을 활용하여 발생 가능한 위협을 식별한 후 차단합니다. 이 시스템은 위협 인텔리전스 피드를 활용합니다. 해당 피드에는 마지막으로 알려진 공격 패턴이 계속 추가되므로 시스템이 항상 업데이트된 상태로 유지됩니다.

- **VPN(가상 사설망) 지원:** Contoso CipherGuard Sentinel X7은 IPSec, OpenVPN 등의 업계 표준 VPN 프로토콜을 지원합니다. 그리고 전송 중인 데이터를 암호화하여 공용 네트워크의 원활한 보안 통신을 지원합니다. VPN 모듈에는 AES-256 등의 고급 암호화 알고리즘이 적용되므로 원격 사용자와 지점용으로 안정적이면서도 안전한 통신 채널이 제공됩니다.

- **엔드포인트 보안:** 다계층 방어 방식이 적용되어 있는 Contoso의 엔드포인트 보안 모듈에는 바이러스 백신, 맬웨어 방지 프로그램, 호스트 기반 침입 방지 기능이 통합되어 있습니다. 이 모듈은 실시간 행동 분석과 휴리스틱 검사를 수행하여 악의적인 활동을 사전에 검색 및 차단합니다. 새롭게 등장하는 위협에 신속하게 대응하기 위해 이 모듈을 위협 인텔리전스 플랫폼에 통합할 수도 있습니다.

- **로깅 및 모니터링:** 로깅 및 모니터링 하위 시스템은 네트워크 활동에 대한 포괄적인 데이터를 캡처합니다. 이러한 데이터에는 트래픽 패턴, 사용자 인증 이벤트 및 보안 정책 위반 관련 세부 로그가 포함됩니다. SIEM(보안 정보 및 이벤트 관리)과 통합되어 있는 이 기능을 활용하면 중앙 집중식 모니터링과 분석을 원활하게 진행할 수 있습니다. 따라서 보안 관리자가 발생 가능한 보안 인시던트에 신속하게 대응할 수 있습니다.

- **사용자 인증 및 액세스 제어**: Contoso CipherGuard Sentinel X7은 생체 인식 인증, 스마트 카드 통합 등의 MFA(다단계 인증) 메커니즘을 지원합니다. 또한 통합형 LDAP 및 Active Directory를 활용하는 사용자 역할 기반 액세스 제어 정책도 적용됩니다. 이러한 정책은 동적으로 적용되므로 권한 있는 사용자만 중요한 리소스에 액세스할 수 있습니다.

2. 기술 사양

2.1 하드웨어 요구 사항

- **프로세서:** 쿼드 코어 2.5GHz 이상(하드웨어 가속 지원)
- **RAM:** 최소 16GB, ECC(Error-Correcting Code) RAM 권장
- **스토리지:** 최소 200GB(SDD 사용 시 최적 성능 제공)
- **NIC(네트워크 인터페이스 카드):** 듀얼 기가비트 이더넷(점보 프레임 지원)

2.2 소프트웨어 요구 사항

- **운영 체제:** Windows Server 2019 이상/CentOS 8 또는 동급 운영 체제와 호환됨
- **데이터베이스:** 고성능 인덱싱용으로 최적화된 데이터 스토리지용 PostgreSQL 13
- **보안 업데이트:** 위협 인텔리전스 피드 자동 업데이트 및 정기 보안 패치

2.3 네트워크 호환성

- **프로토콜:** TCP/IP, UDP, ICMP, IPv6 지원
- **통합:** BGP 및 OSPF 라우팅 프로토콜과 원활하게 통합 가능
- **호환성:** Cisco, Juniper 및 기타 유명 네트워킹 공급업체 제품과 상호 운용 가능

3. 구현 계획

3.1 배포 단계

1. **배포 전 평가:** 침투 테스트와 위험 분석을 비롯하여 포괄적인 네트워크 취약성 평가를 수행합니다.

2. **설치:** 하드웨어를 가장 효율적으로 활용하고 최적의 리소스를 할당할 수 있도록 전용 서버나 가상 머신에 Contoso CipherGuard Sentinel X7을 배포합니다.

3. **구성:** 조직의 요구 사항에 따라 보안 정책, 액세스 제어 및 방화벽 규칙을 사용자 지정합니다. 검색 정확도를 최대한 높일 수 있도록 침입 검색 매개 변수를 미세 조정합니다.

4. **테스트:** 시뮬레이션형 공격 시나리오와 부하 테스트를 포함하여 철저한 테스트 계획을 실행해 솔루션의 효율성과 성능을 검증합니다.

5. **학습:** IT 담당자를 대상으로 심층 학습 세션을 제공합니다. 해당 학습에서는 일상적인 작업 방식, 인시던트 대응 절차, 유지 관리 작업 등의 내용을 다룰 수 있습니다.

3.2 유지 관리 및 지원

- **정기 업데이트:** Contoso는 최신 위협 인텔리전스와 향상된 보안 기능을 통합하는 방식으로 제품을 지속적으로 업데이트합니다.

- **기술 지원:** Contoso의 연중무휴 전담 지원 팀이 Contoso CipherGuard Sentinel X7 관련 기술 문제나 문의 사항을 즉시 지원해 드립니다.