Security Intelligence

개요

용도: 소프트웨어 정의 네트워크 보안 서비스 플랫폼

사양: NSX 제공 오버레이 네트워크 기반의 Virtual Machine

대상

상태	대상	범주
미검수	브로드컴 파트너	포스트세일즈

내용

기능

Security Services Platform Installer

범주	내용
기능	HTML5 웹 유저인터페이스를 제공하여 OS 무관 동일환 제어 경험 기능
	보안 서비스 플랫폼의 관리 네트워크 및 도메인을 정의하는 기능
	가상화 데이터 센터 접속하여 준비사항을 수집하는 기능

보안 서비스 플랫폼의 평가 토폴로지 배포 기능	
보안 서비스 플랫폼의 고급 토폴로지 배포 기능	
보안 서비스 플랫폼 배포를 위한 사전 체크 기능	
보안 서비스 플랫폼을 컨테이너 기반한 격리 에코 시스템으로 구성하는 기능	
성능	보안 서비스 플랫폼 전체의 정상 상태를 확인하고 점수를 표시
	보안 서비스 플랫폼의 기술지원을 위한 로그를 수집하고 번들 파일을 작성
관리	보안 서비스 플래폼의 수명주기를 관리
	보안 서비스 플랫폼 설치자의 백업 및 복원을 관리
	보안 서비스 플랫폼 설치자의 업그레이드를 관리
	보안 서비스 플랫폼 설치자의 신뢰 접속 경로 제공을 위한 SSL 인증서를 관리
	보안 서비스 플랫폼 설치자의 기본 계정 암호를 관리

Security Services Platform

범주	내용
기능	지난 30일 요약 기능
	보안 서비스 별 위협 요약 기능
	플랫폼 시스템 대시보드 기능
	지정한 기간 내 위협 평가 보고서를 작성하는 기능
성능	보안 서비스 별 정상 상태를 확인하고 자원량을 표시
관리	보안 서비스 별 활성화/비활성화 관리
	소프트웨어 정의 네트워크 관리자 연결을 관리

보안 서비스 플랫폼의 백업 및 복원을 관리
보안 서비스 플랫폼의 업그레이드를 관리
보안 인식 제어를 위한 사설 IP 범위 관리
인터넷 접속을 위한 프록시 연결을 관리
로그 전달을 위한 SIEM 연결을 관리
로그 전달을 위한 시스로그 연결을 관리
보안 서비스 플랫폼의 신뢰 접속 경로 제공을 위한 SSL 인증서를 관리
보안 서비스 플랫폼의 기본 계정 암호를 관리
RBAC 위한 LDAP 연결 및 역할 할당

Security Intelligence

범주	내용
기능	집계한 흐름의 보안 정보를 시각화하고 상호작용하며 검토하는 기능
	집계한 흐름 속 워크로드/시간 별 범위를 검토하여 보안 정책을 추천하는 기능
	추천한 보안 정책을 소프트웨어 정의 네트워크 관리자의 보안 구성에 즉시 적용하는 기능
	집계한 흐름 메트릭에서 객체를 파악하여 워크로드를 분류하는 기능
성능	보안 서비스 별 정상 상태를 확인하고 자원량을 표시
관리	소프트웨어 정의 네트워크 내 흐름을 수집할 대상을 관리
	소프트웨어 정의 네트워크 내 MITRE ATT&CK Framework 탐지할 유형을 관리
	보안 인식 제어를 위한 사설 IP 범위 관리

Network Detection and Response

- VM-to-VM Traffic Flow Analysis
- Firewall Visibility
- Automated Security Policy
- Rule and Group Recommendation Analytics

Malware Prevention

범주	내용
기능	탐지한 악성 파일의 집계를 시각화하고 열거하는 기능
	별도로 검사한 유니크 파일을 검사하고 열거하는 기능
	탐지 후 별도로 허용한 파일을 열거하는 기능
	의심스러운 트래픽 흐름의 집계를 시각화하는 기능

고지사항

Revision #1
Created 2025-10-30 21:16:40 KST by 오예빈
Updated 2025-11-03 19:57:49 KST by 오예빈