CAASM 기능 및 규격

Axonius CAM 기능 및 규격 - r1 - 우승민 - 20221101.docx

규격의 명칭 정의

구분	명칭	환경	비고
Server	Cybersecurity Asset Management	Cloud	-
		On-premises	-

기능 및 규격

구분	분류	상세 규격
Web Console	**Dashboard**	I 특정 디바이스 및 자산 키워드 검색 I 디바이스 현황 보고 I 사용자 현황 보고 I 어댑터 연결 현황 보고 I 취약점 현황 보고 I 정책 별 현황 보고
	Devices	I 사용자 검색 및 실행 쿼리 저장 I 디바이스 상세 정보 제공 (어댑터 별 수집 정보 상이) · 방화벽 규칙 · 소프트웨어 정보 · 로컬 User 및 Admin 계정 정보 · 네트워크 인터페이스 정보 · OS 보안 패치 정보 · 취약점 정보 I 디바이스의 어댑터 연동 정보 제공 I 일별 데이터 정보 검색 제공 I CSV 데이터 추출 제공

Users	l 사용자 검색 및 실행 쿼리 저장 l 사용자 상세 정보 제공 (어댑터 별 수집 정보 상이) · 사용자 및 관리자 계정 정보 · 암호 만료 정보 · 계정 만료 정보 · 암호 변경 정보 l 사용자의 어댑터 연동 정보 제공 l 일별 데이터 정보 검색 제공 l CSV 데이터 추출 제공
Vulnerabilities	l 발견된 취약점의 상세 정보 제공 l 취약점 검색 및 실행 쿼리 저장 l 취약점 발견 디바이스 정보 제공 l 취약 소프트웨어 및 버전 정보 제공 l CVSS 점수 및 CVE 심각도 정보 제공
Queries	l 간편한 쿼리 작성을 위해 쿼리 마법사 기능 제공 l 작성된 쿼리 저장 l 쿼리 실행 이력 정보 제공
Cloud Compliance	l Center of Internet Security(CIS) 벤치마크 지원 l 클라우드 플랫폼 별 보안 규정 정보 제공 l 보안 규정 준수 여부 확인
Enforcement Center	l 실행한 쿼리 결과에 대한 보안 규칙 정의 · 알림 제공 · 태그 추가 및 제거 · CMDB 자산 관리 · 파일 배포 및 명령 실행 · 엔드포인트 보안 에이전트 작업 실행 · 사용자 및 사용자 그룹 관리 · 클라우드 서비스 관리 · 하위 도메인 제거 l 보안 규칙에 대한 실행 스케줄링 지원 l 보안 규칙 실행 이력 제공
Adapters	l 약 550여개의 어댑터 지원 · 예) EDR/EPP, Network CMDB, Virtualization 등 l 미지원 어댑터에 대한 자산 정보 수집 방안 제공 · CSV · JSON · SQL Server l 어댑터 연동 및 패치 이력 제공 l 어댑터 별 상세 정책 설정

	Reports	l 대시보드 및 사용자 지정 쿼리의 보고서 제공 l CSV 및 PDF 추출 지원 l 이메일 전송 및 예약 전송 기능 제공
	Activity Logs	l 사용자 및 시스템 활동 로그 제공 l CSV 추출 지원
	Instances	l 중앙 코어 노드 및 코어 노드 정보 제공 l 코어 노드 연동 지원 l 시스템 종료 및 재시작 원격 제어
	Setting	l 어댑터 연동 및 패치 등 알림 메시지 제공 l Syslog 및 HTTPS Log연동 지원 l LDAP 및 SAML 로그인 지원 l 계정 별 권한 및 기능 제어

Revision #8
★Created 2022-11-02 08:54:12 KST
Updated 2025-04-19 02:06:16 KST