

Axonius: 공개 문서

- [CAASM 기능 및 규격](#)
- [Q&A | 보안개념의 새로운 변화, 더 중요한 자산을 지켜내는 제로트러스트의 시작](#)

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	1 특정 디바이스 및 자산 키워드 검색 1 디바이스 현황 보고 1 사용자 현황 보고 1 어댑터 연결 현황 보고 1 취약점 현황 보고 1 정책 별 현황 보고
	Devices	1 사용자 검색 및 실행 쿼리 저장 1 디바이스 상세 정보 제공 (어댑터 별 수집 정보 상이) <ul style="list-style-type: none">· 방화벽 규칙· 소프트웨어 정보· 로컬 User 및 Admin 계정 정보· 네트워크 인터페이스 정보· OS 보안 패치 정보· 취약점 정보 1 디바이스의 어댑터 연동 정보 제공 1 일별 데이터 정보 검색 제공 1 CSV 데이터 추출 제공
	Users	1 사용자 검색 및 실행 쿼리 저장 1 사용자 상세 정보 제공 (어댑터 별 수집 정보 상이) <ul style="list-style-type: none">· 사용자 및 관리자 계정 정보· 암호 만료 정보· 계정 만료 정보· 암호 변경 정보 1 사용자의 어댑터 연동 정보 제공 1 일별 데이터 정보 검색 제공 1 CSV 데이터 추출 제공
	Vulnerabilities	1 발견된 취약점의 상세 정보 제공 1 취약점 검색 및 실행 쿼리 저장 1 취약점 발견 디바이스 정보 제공 1 취약 소프트웨어 및 버전 정보 제공 1 CVSS 점수 및 CVE 심각도 정보 제공
	Queries	1 간편한 쿼리 작성을 위해 쿼리 마법사 기능 제공 1 작성된 쿼리 저장 1 쿼리 실행 이력 정보 제공
	Cloud Compliance	1 Center of Internet Security(CIS) 벤치마크 지원 1 클라우드 플랫폼 별 보안 규정 정보 제공 1 보안 규정 준수 여부 확인
	Enforcement Center	1 실행한 쿼리 결과에 대한 보안 규칙 정의 <ul style="list-style-type: none">· 알림 제공· 태그 추가 및 제거· CMDB 자산 관리· 파일 배포 및 명령 실행· 엔드포인트 보안 에이전트 작업 실행· 사용자 및 사용자 그룹 관리

		<ul style="list-style-type: none">· 클라우드 서비스 관리· 하위 도메인 제거 1 보안 규칙에 대한 실행 스케줄링 지원 1 보안 규칙 실행 이력 제공
	Adapters	1 약 550여개의 어댑터 지원 <ul style="list-style-type: none">· 예) EDR/EPP, Network CMDB, Virtualization 등 1 미지원 어댑터에 대한 자산 정보 수집 방안 제공 <ul style="list-style-type: none">· CSV· JSON· SQL Server 1 어댑터 연동 및 패치 이력 제공 1 어댑터 별 상세 정책 설정
	Reports	1 대시보드 및 사용자 지정 쿼리의 보고서 제공 1 CSV 및 PDF 추출 지원 1 이메일 전송 및 예약 전송 기능 제공
	Activity Logs	1 사용자 및 시스템 활동 로그 제공 1 CSV 추출 지원
	Instances	1 중앙 코어 노드 및 코어 노드 정보 제공 1 코어 노드 연동 지원 1 시스템 종료 및 재시작 원격 제어
	Setting	1 어댑터 연동 및 패치 등 알림 메시지 제공 1 Syslog 및 HTTPS Log 연동 지원 1 LDAP 및 SAML 로그인 지원 1 계정 별 권한 및 기능 제어

Q&A | 보안개념의 새로운 변화, 더 중요한 자산을 지켜내는 제로트러스트의 시작

개요

행사 유형: 웨비나
질문자: 참가자
답변자: 황원섭 이사

질의답변

이호승

[질문] 사내 수십만대의 서버와 네트워크 장비가 있는데 담당자가 퇴사하거나 조직이 개편되면 자산담당자의 현황 현행화가 어렵고 테스트서버나 불용처리 시스템에 대한 관리가 잘 안되는데요. 자산을 상시 최신화하여 관리하는 기술이나 기능도 있는지 궁금합니다.

[답변] 이 질문에 대한 내용이 CAASM이다. 자산이 많고 복잡한 환경은 수기로 자산파악이 힘들다. 자동화와 식별을 통해 유니크한 값을 통해 각각의 자산을 찾는것이 중요하다.

윤성원

[질문] 공격표면 확장 공격이 요새 핫이슈인데 이는 재택근무의 확산으로 더 부각되는 데 이 공격을 효과적으로 막는 방법은 무엇인지 궁금합니다.

[답변] 현재는 자산이 흩어져있기 때문에 검증하는 제로트러스트 방식을 사용하는것, 자산의 사용 용도에 따라 적용방식이 다를거 같다.

지정호

[질문] 자산의 가치의 위험을 줄이기 위한 중요한 방안은 무엇인지요? 기업 자산 분류 기준과 가치 평가는 어떻게 이루어지는지요?

[답변] 본 질문은 제 전문 분야가 아니므로 답변을 아끼도록 하겠습니다.^^ 너그러운 이해를 부탁드립니다.

문주웅

[질문] Multi-layered Security를 구축한 기업에서 여전히 보안 사고가 발생하는 경우 이에 대해서 체계적으로 대응할 수 있는 방법에 대해서 질문드립니다

[답변] 최근 트렌드는 관리되지 않는 자산(device)에서 보안 사고가 많이 발생되고 있습니다. 웨비나에서 소개해 드린데로 기존에 보안 위험을 모니터링하고 자산의 취약점을 대응하는 방식과 더불어 내부 자산을 자동으로 식별하는 CA-ASM 솔루션으로 체계적으로 대응할 수 있습니다.

지정호

[질문] 제로트러스트에서 MFA 다중 인증 적용과 보안 강화와 취약점에 대한 가시성 확보의 중요 사항과 관련하여 Axonius는 타 솔루션과 차별성은 무엇이며, 지원 방안은 어떻게 되는지요?

[답변] 본 웨비나에서 자산의 가시성 확보가 조직의 위험 관리 측면에서 매우 중요하다고 강조하였습니다. 저희 Axonius 솔루션은 자산 식별을 사람의 관여없이 이미 보유하신 다양한 IT/보안 솔루션과 연동하여 자산(IT device) 데이터를 수집하여 상관분석엔진을 통해서 자동으로 unique device를 식별하고 수집한 다양한 정보들을 통합하여 검색 및 대시보드, 자동화 액션 기능을 제공합니다. 솔루션 소개 시간을 허락해 주시면 찾아 뵙고 소개 및 데모로 설명드리겠습니다.

서보영

[질문] CEO 입장에서 장비들 들어가고 유지보수 인력문제로 없어지고 있는데 어떻게 생각하는지 궁금합니다

[답변] 제 생각에는 이제 기업이 살아남기 위해서 보안은 필수라고 생각합니다. 적은 인원으로 보안과 위험 대응을 효과적으로 할 수 있는 방법은, 내부 자산 가시성과 취약성을 관리할 수 있는 CAASM과 같은 솔루션이 반드시 필요하다고 생각합니다.

이민수

[질문] 잠재적 위험을 효과적으로 절감하려는 경우 총자산가치, 취약성의 심각도, 위협의 심각도를 최적으로 관리하는 방안은 무엇인가요?

[답변] 저는 사실 위험관리 전문가가 아닙니다. 저도 공부하고 있습니다. ^^ 다만, 본 웨비나에서 위험(Risk)를 언급한 이유는 보안에 있어서 자산 식별의 중요성을 강조하기 위해서 입니다.

이호승

[질문] 계열사 및 그룹사 보안관리와 관계를 하고 있는데 위탁서비스는 자산정보를 제공할수 없다는게 일반적이고 자산과 상관없이 모든 위협을 식별하고 처리해달라고 하고 보안서비스 제공자의 현실은 호락호락 하지 않거든요.CAASM 은 자체보안을 하는 기업만 도입을 하거나 제안되고 있는지 보안서비스용으로 구축해서 사용하거나 제공하는 사례가 있는지 궁금합니다.

[답변] CAASM은 기업 내부의 자산 정보를 다루기 때문에 서비스 보다는 Enterprise용 솔루션 이라고 볼 수 있습니다. 다만, 최근에는 보안서비스 용으로도 검토하고 있습니다. 저희 Axonius CAASM 솔루션은 SIEM처럼 여러 IT/보안솔루션에서 자산 데이터를 수집하여 상관분석하는 플랫폼 임으로, 보안 서비스용도로 활용할 수 있습니다.

윤성원

[질문] IT 자산관리는 사실은 it에서 하는 것보다 회계시스템을 관리하는 ERP 팀이 하는 것이 더 현실적인데 왜냐하면 IT팀은 자산만 시스템에 입력하고 그 유지관리만 하는것이 현실이라 IT 자산하면 IT팀, 보안팀, ERP팀, 3개팀이 모두 관여되는데 이렇게 되면 권한이 분산되어 결과적으로 서로 책임 떠넘기기만 하는데 3개팀중 어느팀이 독자적으로 관리하는 것이 가장 효과적일지 궁금하고 해외는 어떻게 관리하는지요?

[답변] 본 웨비나에서 보안에서 자산 식별의 중요성을 강조하였습니다. 그렇다고 현재 ERP팀이나 IT(인프라)팀에서 하고 있는 자산관리 업무가 필요없고 보안팀으로 이관해야 한다는 의미는 아닙니다.(업무 목적과 목표가 다름) 다만 보안(운영) 업무 측면에서 자산 식별이 필요하니 CAASM솔루션을 구성하여 자동으로 전체 자산을 식별한 후 해당 자산 데이터를 ERP팀이나 IT(인프라)팀에도 제공 할 수 있습니다. 해외에서도 보안팀에서 별도로 CAASM을 도입하여 활용하고 있습니다.

유재명

[질문] 생체인증, 듀얼인증을 이용한 보안인증으로 옮겨가고 있습니다. 이것 역시 한계는 있는 분명해 보입니다. 가까운 미래에는 양자를 이용한 보안방법과 제로트러스트에 대한 극복 방법도 개발중인지, 어디까지 개발되었는지 말씀해주시면 고맙겠습니다.

[답변] 본 질문은 제 전문 분야가 아니므로 답변을 아끼도록 하겠습니다.^^ 너그러운 이해를 부탁드립니다.

이민수

[질문] 기업에서 ZT, ZTA, ZTNA 모델을 선택할 때 중요하게 고려하고 점검해야 할 요소들은 각각 무엇인가요?

[답변] 저는 사실 제로트러스트 전문가가 아닙니다. 저도 공부하고 있습니다. ^^ 다만, 본 웨비나에서 제로트러스트를 언급한 이유는 보안에 있어서 자산 식별의 중요성을 강조하기 위해서 입니다.

한위원

[질문] 제로트러스트는 기존 경계보안에서의 DID심층방어와 다른 개념인지요 아님 상호 보완적인지요?

[답변] 네 제로트러스트는 기존 경계보안과 상반되는 "경계없는 보안(perimeterless security)"이라고 얘기합니다. 그러나 제 생각에는 아직까지 환경에 따라 상호 보완적으로 고려할 필요가 있다고 생각하고 있습니다.

한규권

[질문] 클라우드 네이티브 환경에서 자산관리가 가능한지요? 사례가 궁금합니다

[답변] 보안을 위한 자산 식별에 예외 영역은 없어야 한다고 생각합니다. 현재의 IT자산은 온프레미스, 클라우드(퍼블릭, 프라이빗), 가상화, 컨테이너 영역 모두에 존재합니다. Axonius 솔루션의 경우에는 Network 스위치, NAC, Host에 설치되는 Agent, AD, 클라우드와 API연동, Kubernetes 등과 연동하여 자산 정보(device의 hostname, ip, mac, os, installed software list 등)를 수집하여 상관분석엔진을 통해서 자동으로 unique device를 식별하고 수집한 다양한 정보들을 통합하여 검색 및 대시보드, 자동화 액션 기능을 제공합니다. 이미 글로벌하게 400개 이상의 고객사를 보유하고 있습니다.

문주웅

[질문] 보안 리스크를 식별할 때 $R = A * V * T$ 라는 공식에서 가장 크게 작용하는 항목은 무엇인가요?

[답변] 웨비나 시간에 이미 답변은 드렸습니지만 다시 의견 드립니다. 해당 공식만을 기준으로 본다면, 자산(Asset), 취약점(Vulnerability), 위협(Threat) 모두 중요한 항목입니다. 다만 취약점과 위협은 모두 관련된 자산이 있을때 영향도가 있기때문에, 저는 자산이 제일 크게 작용하는 항목이라고 생각합니다.

문태진

[질문] 자산들을 식별해서 DB화 시킬때, 기본적인 회사 자산들과 이동 업무성 회사자산과 개인 기기들을 업무에 사용하는 것들도 별도로 각각 카테고리를 나누어서 관리하면서 모든 디바이스 보안안정성을위한 Axonius에 특화된 솔루션은 어떤 것이 있는지요?

[답변] 저희 Axonius에서는 기업용 솔루션을 판매함으로 식별과 관리의 대상 자산(IT device)도 회사 자산만을 대상으로 합니다. 그러나 회사 내부 네트워크에서 자동으로 식별된 자산 중 개인 기기가 식별될 경우 tag를 달아서 별도로 관리할 수는 있습니다.

이민수

[질문] 기업에서 보안 리스크를 신속하게 탐지하고 식별할 수 있는 방안은 무엇인가요? 이와 관련하여 Axonius Korea에서 지원하시는 서비스에 대해서 설명 부탁드립니다

[답변] 본 웨비나 내용을 기준으로 말씀드리면, " $Risk = Asset \times Vulnerability \times Threat$ " 공식에 의해 기업의 전체 자산을 식별하고 그 자산의 취약점을 파악하여 조치하고 실시간 위협 모니터링 체계를 구성하시면 좋을 것 같습니다. 이와 관련하여 저희 Axonius에서는 기업 전체의 정확한 자산(unique device)을 자동으로 식별하고 대응 및 활용할 수 있는 CAASM 솔루션을 판매하고 있습니다.