사이버 보안

장치 수명 주기 관리

사이버 보안 위험은 생산에서 폐기에 이르는 네트워크 장비 수명 주기의 모든 단계에 존재합니다. 이러한 위험을 간과하면 운영 중단과 데이터의 기밀성, 무결성 및 가용성 손실로 이어질 수 있습니다. 따라서 공급업체부터 최종 고객에 이르기까지 모든 이해관계자가 위험 관리를 책임지는 것이 중요합니다.

따라서 장치 보안 수명 주기에 대한 고려 사항은 조달에서 중요합니다. 제조업체는 제품이 고객에게 전달되기 전, 제품이 사용되는 동안, 그리고 제품이 폐기될 때 사이버 보안 위험을 줄이기 위한 조치를 취해야 합니다.

이어지는 페이지들에서는 Axis가 Axis 장치의 수명 주기 동안 위험을 완화하기 위해 지원하는 접근 방식과 프로세스뿐만 아니라 기술, 도구 및 지침을 한눈에 살펴볼 수 있습니다.

보안의 기반: Axis Edge Vault, AXIS OS, Axis 보안 개발 모델


생산


유통


구현


운영 중


폐기

보안의 기반 – 하드웨어, 소프트웨어 및 접근 방법

처음부터 제품 무결성 보호 및 취약성 위험 감소

Axis Edge Vault 사이버 보안 플랫폼
이 하드웨어 기반 플랫폼은 장치 ID와 무결성을 무단 액세스로부터 보호하는 기능을 지원하므로 장치를 안전하게 부팅하고 통합하며, 키와 같은 민감한 데이터를 보호할 수 있습니다.

운영 체제, AXIS OS
AXIS OS는 다양한 Axis 장치를 구동합니다. 취약성 관리의 업계 모범 관행을 통합한 AXIS OS는 수많은 제품에 걸쳐 소프트웨어 보안 기능 및 패치를 빠르고 효율적으로 배포할 수 있는 플랫폼을 제공합니다.

Axis 보안 개발 모델(ASDM)
소프트웨어 취약점이 있는 제품을 출시할 위험을 줄이기 위해 Axis에서 적용하는 방법론입니다. ASDM은 보안 고려 사항이 소프트웨어 개발의 필수적인 부분이 되도록 하며, 무엇보다도 위험 평가, 위협 모델링, 코드 분석, 침투 테스트, 버그 바운티 프로그램, 취약점 스캔 및 관리 등을 포함합니다.

투명성
투명성은 신뢰를 구축하기 위한 Axis의 업무 방식에서 중요한 부분입니다. Axis는 공통 취약점 및 노출(CVE) 번호 부여 기관(Common Vulnerability and Exposures (CVE) Numbering Authority)입니다. Axis는 취약점을 게시하고 이해 관계자에게 알려 고객이 적절한 조치를 취할 수 있도록 합니다. Axis는 AXIS OS용 소프트웨어 자재 명세서(SBOM)도 게시합니다.

생산 및 유통

구성부품의 손상 위험 감소

> **공급망:** 주요 구성부품은 전략적 공급업체에서 직접 조달합니다. Axis는 제조 파트너와 긴밀하게 협력합니다. 생산 공정을 모니터링하고 데이터를 연중무휴로 공유하여 실시간 분석 및 투명성을 확보합니다.

> **Axis Edge Vault:** 생산 중에 Axis 장치에 설치되는 Axis Edge Vault에는 다음과 같은 특장점이 포함됩니다.
>> **보안 키 저장소**: 키의 변조 방지 저장을 위한 암호화 컴퓨팅 모듈(예: SE(Secure Element), TPM(Trusted Platform Module), TEE(Trusted Execution Environment)을 포함
>> **Signed Firmware**: 설치된 AXIS OS가 Axis의 정품임을 보장. 이 기능은 장치에 다운로드하여 설치할 새 펌웨어도 Axis에서 서명하도록 보장합니다.
>> **Secure Boot**: 장치가 펌웨어에 Axis 서명이 있는지 확인할 수 있도록 합니다. 펌웨어가 승인되지 않았거나 변경된 경우, 부팅 프로세스가 중단되고 장치 작동이 중지됩니다. Signed Firmware, Secure Boot 및 공장 출하 시 기본값 설정의 조합을 통해 장치 배송 중에 장치가 악의적으로 변경되는 것을 방지합니다.
>> **Axis 장치 ID**: Axis 장치의 진위 여부를 증명할 수 있는 해당 키가 포함된 장치 고유 인증서입니다. IEEE 802.1AR을 기반으로 하는 Axis 장치 ID를 사용하면 네트워크에서 장치를 안전하게 식별하고 온보딩할 수 있습니다.
>> **암호화된 파일 시스템**: 장치가 시스템 통합업체에서 최종 고객에게 배송 중인 기간과 같이, 장치를 사용하지 않는 동안에 파일 시스템에 저장된 고객별 구성 및 정보가 추출되거나 변조되는 것을 방지합니다.

구현

손상되거나 보안이 부적절하게 강화되어 무단 액세스, 민감한 데이터 추출, 네트워크 엔드포인트 간 전송 중인 데이터의 변경으로 이어질 수 있는 제품을 네트워크에 배치할 경우 발생할 수 있는 위험 해결

> **공장 출하 시 기본값:** 장치를 구성하기 전에 장치에서 공장 출하 시 기본값 설정을 수행합니다. 이렇게 하면 원치 않는 소프트웨어나 구성이 장치에서 완전히 제거되므로 AXIS OS와 기본 설정만 남게 됩니다.

> **장치의 최신 펌웨어 확인:** 생산과 구현 사이에 약간의 시간이 지났을 수 있으므로, 특정 장치에 대한 최신 버그 수정이 포함되어 있을 수 있는 최신 펌웨어를 Axis 웹 사이트에서 확인하는 것이 좋습니다.

> **Axis 장치 ID:** 네트워크에서 정품 Axis 장치만 구현되도록 하기 위해, Axis 장치 ID를 IEEE 802.1X 인증을 사용해서, 또는 HTTPS 프로토콜을 통해 보안 네트워크 연결을 설정할 때 확인할 수 있습니다. IEEE 802.1X 네트워크에서, Axis 장치 ID를 활용하여 보안을 강화하고 배포 시간을 단축할 수 있습니다.

> **보안 키 저장소:** 암호화 컴퓨팅 모듈이 포함된 보안 키 저장소는 Axis 장치 ID 및 고객이 로드한 키와 같은 민감한 정보를 보관하여 장치가 손상된 경우에도 무단 액세스 및 민감한 정보의 악의적인 추출을 방지합니다.

> **암호화된 파일 시스템:** 장치를 사용하지 않을 때 파일 시스템에 저장된 데이터를 추출하거나 변조할 수 없도록 합니다.

> **보안 강화 가이드:** Axis 웹 사이트의 AXIS OS 포털에서 제공되는 AXIS OS 보안 강화 가이드는 일반적인 위협을 해결하기 위한 기본 구성을 설정하고 모범 관행과 기술적 조언을 제공합니다. 영상 관리 소프트웨어인 AXIS Camera Station과 Axis 네트워크 스위치에 대한 보안 강화 가이드도 있습니다.

> **AXIS OS 보안 스캐너 가이드:** Axis는 Axis 장치가 취약점이나 취약한 구성의 영향을 받는지 확인하기 위해 Axis 장치에 대한 보안 스캔을 실행할 것을 권장합니다. AXIS OS 보안 스캐너 가이드는 스캐너의 특정 지적 사항을 해결하는 방법에 대한 권장 사항을 제공하고 일반적인 "잘못된 경보"에 대해 간략하게 설명합니다.

> **AXIS Device Manager:** 로컬에서 Axis 장치를 효율적으로 구성하고 관리할 수 있도록 지원하는 도구입니다. 이 도구를 사용하면 장치 자격 증명 관리, 인증서 배포, 사용하지 않는 서비스 비활성화, AXIS OS 업그레이드와 같은 설치 및 보안 작업을 일괄 처리할 수 있습니다.


생산


유통


구현


운영 중


폐기

운영 중

알려진 취약점이 있는 펌웨어를 실행하거나, 인증되지 않은 펌웨어로 장치를 업데이트하거나 보안 구성이 만료된 상태로 방치할 경우 발생할 수 있는 위험 해결

> **펌웨어 업그레이드:** AXIS OS 활성 트랙 또는 LTS(장기 지원) 트랙을 사용하여 펌웨어를 최신 상태로 유지함으로써 Axis 장치의 사이버 보안을 유지하는 것이 중요합니다. 두 트랙을 사용한 펌웨어 업데이트는 무료로 제공되며 보안 패치가 포함됩니다. Signed Firmware는 정품 Axis 펌웨어만 설치할 수 있도록 보장합니다.

> **AXIS Device Manager Extend:** AXIS Device Manager를 보완하는 도구이며, Axis 장치를 원격으로 관리하고 장치의 펌웨어 업그레이드와 같은 유지 관리 작업의 확장을 간소화할 수 있습니다.

> **취약성 관리:** Axis는 취약점 및 기타 보안 관련 문제에 대한 정보를 얻기 위해 가입할 수 있는 보안 알림 서비스를 제공합니다.

> **AXIS OS 포렌식 가이드:** Axis 장치가 설치된 주변 네트워크 및 IT 인프라에 대한 사이버 보안 공격이 발생할 경우, Axis 장치에 대한 포렌식 분석을 수행하는 모든 사람을 위한 기술적 조언을 제공합니다.

> **Signed Video:** 지원되는 카메라에서 이 기능을 활성화하면 비디오 스트림이 장치를 떠나기 전에 암호화 서명이 추가되어, 보는 사람이 비디오의 변조 여부를 확인할 수 있습니다. 이는 수사 시 또는 기소 시 특히 중요합니다.

폐기

더 이상 지원되지 않고 패치되지 않은 알려진 취약점이 있는 장치의 위험과, 폐기 후 장치에 남아 있는 민감한 데이터의 위험 해결

> **펌웨어 지원 종료일:** Axis.com의 많은 제품에 대한 지원 웹 페이지에는 특정 제품의 펌웨어에 대한 지원 종료일이 게시되어 있어 고객이 적시에 제품의 폐기 및 교체를 계획할 수 있습니다.

> **AXIS Device Manager Extend:** 제품 단종 및 지원 종료 정보를 포함하여 시스템 내 모든 장치의 보증 상태를 쉽게 추적할 수 있도록 지원합니다. 이 정보를 통해 장치를 폐기할 준비를 하고 지원되지 않는 장치로 인해 발생할 수 있는 위험을 제거할 수 있습니다.

> **안내:** Axis 웹 사이트의 AXIS OS 포털은 Axis 장치 폐기에 대한 안내를 제공합니다. 장치를 공장 기본값으로 설정하면 모든 구성과 데이터가 지워집니다.

상세 내용 참조 사이트: **www.axis.com/ko-kr/about-axis/cybersecurity**