AXIS COMMUNICATIONS

사이버 보안

서로 협력하여
더 나은 사이버 보호 보장

AXIS COMMUNICATIONS

목차

사이버 사고 위험의 완화

사이버 위협으로부터 네트워크 제품 및 소프트웨어 서비스를 보호하는 것이 핵심이며 이를 통해 네트워크상의 데이터 및 시스템을 보호할 수 있습니다. 시스템이 손상되면, 데이터의 기밀성과 무결성이 손실되거나 필요할 때 데이터를 사용할 수 없게 되거나 액세스할 수 없게 될 수 있습니다.

책임감 있는 사이버 보안 파트너가 되기 위한 노력의 일환으로, Axis는 안전한 IP 기반 물리적 보안 제품을 조달하는 데 도움이 되는 몇 가지 고려 사항과 가이드라인을 마련했습니다. Axis는 귀사가 보호 조치를 더 쉽게 실행할 수 있도록 지원하여 귀사가 가장 안전한 방법으로 Axis 제품을 사용할 수 있도록 하고자 합니다.

이어지는 페이지들 외에도, 사이버 보안에 대한 자세한 내용과 더 나은 사이버 보호를 위해 함께 노력할 수 있는 방법을 https://www.axis.com/ko-kr/cybersecurity에서 확인할 수 있습니다.

공동 책임

사이버 보안은 제품, 사람, 기술 및 지속적인 프로세스를 말합니다. 그리고 사이버 보안 체인의 모든 링크가 최대한 강력해지도록 하려면 우리 모두가 협력해야 한다는 것은 분명합니다. 사이버 보안은 최종 고객을 포함한 다음 이해 관계자가 협력하여 공동으로 책임져야 하는 것입니다.

장치 제조업체

여기에서 사이버 보안이 시작됩니다. 제조업체는 설계, 개발, 생산은 물론 소프트웨어 유지 관리에서 사이버 보안 모범 관행을 적용하여 제품 수명 주기 전반에 걸쳐 결함의 위험을 최소화해야 합니다. 자체 공급망을 신중하게 관리하는 것이 중요합니다. 제품에는 다양한 보안 관제를 구현할 수 있는 기능이 내장되어 있어야 합니다. 고객의 보안 프로세스 또는 정책을 지원하는 효율적인 장치 구성 및 관리를 위한 도구가 있어야 합니다. 또한 새로 발견된 취약점에 대해 파트너와 고객에게 알릴 수 있는 채널이 있어야 합니다.

유통업체

취급하는 제품을 직접 만지지 않는 유통업체의 입장에서 보면 사이버 보안은 비교적 단순합니다. 그러나 부가가치형 유통업체는 특히 제조업체에서 장비를 구입하고 다른 (또는 자체) 브랜드로 라벨을 변경할 때 통합업체 및 설치업체와 동일한 측면을 고려해야 합니다. 투명성이 핵심입니다. 장비의 출처가 명확해야 합니다.

컨설팅 업체, 통합업체 및 설치업체

최종 고객이 보안 관제를 식별, 설계 및 구현하도록 돕고 물리적 보안 장치가 고객 네트워크에서 문제가 되지 않도록 보장할 수 있습니다. 여기에는 패스워드, 원격 액세스 관리, 소프트웨어 및 연결된 장치의 유지 관리 등에 대한 전략을 개발하는 것이 포함될 수 있습니다. 여기에는 설치된 장비에 최신 업데이트가 적용되고 시스템에 대해 바이러스 검사가 이루어지는지 확인하는 것이 포함될 수 있습니다. 사이버 보안 책임이 종종 불분명한 OEM/ODM 장비 사용에 따른 문제도 사이버 보안에 대한 전반적인 논의의 일부가 되어야 합니다.

최종 고객

각 조직에는 구체적이고 고유한 사이버 보안 요구사항이 있으므로 보편적인 사이버 보안 구성이 없습니다. 대신 필요한 보안 범위를 정의하기 위해 일련의 정보 보안 정책을 실행하는 것이 중요합니다. 기본 계정 제거, 안전하게 저장되고 주기적으로 변경되는 고유한 - 강력한 - 패스워드 지정, 차별화된 권한 할당, 항상 패치 및 업데이트 설치는 취해야 하는 몇 가지 조치일 뿐입니다.

연구자

연구자는 종종 장치 취약점을 발견합니다. 취약점이 의도적이지 않은 경우 연구자는 일반적으로 제조업체에 알려, 취약점을 게시 전에 수정할 수 있는 기회를 제조업체에 제공합니다. 그러나 중요한 취약점에 의도적인 성격이 있는 경우 연구자는 사용자의 인식을 높이기 위해 종종 대중에게 접근합니다.

사이버 보안이 물리적 보안에서 배울 수 있는 것

대부분의 사람들은 물리적 보안 위험을 쉽게 이해합니다. 도어가 잠겨 있지 않으면 승인되지 않은 사람이 들어갈 위험이 높아집니다. 눈에 보이는 귀중품은 쉽게 도난 당할 수 있습니다. 실수와 사고는 사람, 재산 및 물건에 해를 끼칠 수 있습니다. 물리적 보안과 사이버 보안은 일반적으로 동일한 방식으로 다루어집니다.

조직의 물리적 보안을 담당하든 사이버 보안을 담당하든 동일한 원칙을 적용해야 합니다.

> 자산 및 리소스를 식별 및 분류 (무엇을 보호할 것인가)

> 발생 가능한 위협을 식별 (누구로부터 무엇을 보호할 것인가)

> 위협이 악용할 수 있는 취약점을 파악(가능성)

> 나쁜 일이 발생할 경우 예상되는 비용을 파악(결과). 위험은 종종 위협의 확률에 유해한 결과를 곱한 것으로 정의됩니다. 이것을 결정한 후에는 부정적인 영향을 방지하기 위해 무엇을 하려 하는지 자문해야 합니다.

사이버 보안이란?
사이버 보안은 사이버 위협으로부터 컴퓨터 시스템과 서비스를 보호하는 것입니다. 사이버 보안 관행에는 기밀성, 무결성, 가용성, 안전성, 진정성 및 부인 방지를 보장하기 위해 컴퓨터, 전자 통신 시스템 및 서비스, 유선 및 전자 통신, 저장된 정보의 손상을 방지하고 복원하는 프로세스가 포함됩니다.

어떤 위협에 주의해야 할까요?

IT(정보 기술) 또는 OT(운영 기술) 시스템에서 보호해야 할 핵심 요소는 기밀성, 무결성, 가용성 및 안전성입니다. 그 중 어느 하나에든 부정적인 영향을 미치는 어떤 것도 사이버 보안 사고입니다.

이제 사이버 보안에 대한 가장 일반적인 위협과 이러한 위협이 악용하는 취약점을 살펴보겠습니다. IP 기반 물리적 보안 시스템에 가장 많이 발생하는 네 가지 사이버 위협은 다음과 같습니다.

1. **의도하지 않은 인간의 순진함과 오류**
2. **시스템의 고의적인 오용**
3. **물리적 변조 및 방해 행위**
4. **소프트웨어 취약점 악용**

1 의도하지 않은 인간의 순진함과 오류

네트워크를 보호하기 위해 아무리 훌륭한 기술을 사용하더라도 인적 요소는 여전히 보안 침해의 주요 요인으로 남아 있습니다.

사이버 공격을 받도록 빈틈을 만드는 인간의 오류 유형은 다음과 같습니다.

> **사회 공학**
사용자가 심리적 조작으로 속아 보안 실수를 하거나 민감한 정보를 제공하는 경우. 피싱과 스케어웨어는 사회 공학의 예입니다.

> **패스워드 오용**
강력한 패스워드를 사용하지 않거나 패스워드를 적절하게 보호 및/또는 업데이트하지 않은 경우 등이 이에 해당합니다.

> **주요 구성 요소의 잘못된 관리**
시스템에 액세스할 수 있도록 하는 것을 분실하거나 잘못 놓아둔 경우. 이에 해당하는 예로는 액세스 카드, 전화, 노트북 및 설명서 등이 있습니다.

> **시스템 관리 불량**
시스템 업데이트 및 보안 패치를 설치하지 않은 경우.

> **성공적이지 못한 개선**
개인이 문제를 수정하려 했는데 이로 인해 시스템 성능이 저하된 경우.

취약점과 인간의 오류
인간의 오류로 인해 발생하는 가장 일반적인 취약점 중 일부는 사이버 인식 부족과 위험 관리를 위한 정책 및 장기적 프로세스의 부족입니다. 인간의 오류의 위험을 완화하려면, 조직의 모든 구성원이 사이버 보안 모범 사례에 대해 교육을 받아야 합니다. 이외에도, 영상 관리 시스템(VMS) 또는 장치 관리자를 통해 네트워크에 연결된 장치에 대한 액세스를 신뢰할 수 있는 소수의 개인으로 제한해야 합니다.

2 시스템의 고의적인 오용

너무 흔한 또 다른 사이버 위협은 정당한 액세스 권한을 가진 사람들이 시스템을 고의적으로 오용하는 것입니다.

의도적인 오용의 유형은 다음과 같습니다.

시스템 서비스 및 리소스의 조작

데이터 훔치기

시스템에 고의적인 해를 끼치기

취약점 및 의도적인 오용

취약점을 관리하고 의도적인 시스템 오용의 위협을 완화하는 데 도움이 되는 정책과 장기적인 프로세스를 구현하는 것이 중요합니다. 민감한 데이터에 대한 액세스를 허용하는 권한을 가진 개인을 적절하게 조사하는 것은 그러한 권한을 가진 개인의 수를 제한하는 것과 마찬가지로 중요합니다.

카메라와 같이 네트워크에 연결된 물리적 보안 장치를 관리하는 데 사용되는 소프트웨어는 자체 자격 증명이 있는 관리자 계정을 사용해야 합니다. 이 계정은 공유할 수 없는 고유한 계정이어야 합니다. 그런 다음 사이트 운영자는 관리 소프트웨어에 개별 계정을 보유해야 합니다. 그리고 어떤 개인도 물리적 보안 장치에 직접 액세스할 수 없어야 합니다. 직접 액세스를 허용해야 하는 이유가 있는 경우, 이 액세스는 일시적이어야 합니다.

3 물리적 변조 또는 방해 행위

물리적 보호는 사이버 보안의 관점에서 매우 중요합니다.

> 물리적으로 노출된 장치는 변조될 수 있습니다.

> 물리적으로 노출된 장치는 도난당할 수 있습니다.

> 물리적으로 노출된 케이블은 분리되거나, 올바르지 않은 장비에 연결되거나, 절단될 수 있습니다.

취약점 및 물리적 위협

일반적인 취약점으로는 잠긴 장소에 배치되지 않은 서버 및 스위치, 쉽게 접근할 수 있고 보호 하우징으로 보호되지 않는 카메라, 벽 또는 도관으로 보호되지 않는 케이블 등의 네트워크 장비가 있습니다. 네트워크에 연결된 장치는 동일한 네트워크에 있는 다른 자산을 노출시킬 수도 있습니다.

부정적 영향을 인식하십시오.

비디오, 오디오 및 접근 제어 시스템은 금융 거래를 처리하거나 고객 데이터를 보유하지 않습니다. 따라서, 이러한 시스템에 대한 공격은 수익을 창출하기 어려우므로 조직적 사이버 범죄자의 입장에서 보면 가치가 제한적일 수 있습니다. 그러나 손상된 시스템은 다른 시스템에 위협이 될 수 있습니다.

따라서 이로 인해 발생하는 비용을 추정하기가 어렵습니다. 유감스럽게도, 많은 경우에, 조직은 비싼 교훈을 얻습니다. 보호는 품질과 같은 것입니다. 지불하는 비용에 비례하여 결과를 얻을 수 있습니다. 그리고 공급업체가 제품 수명 주기 동안 사이버 보안을 고려하지 않은 경우, 저렴하게 구매하면 장기적으로 훨씬 더 많은 비용이 발생할 수 있습니다.

4 소프트웨어 취약점 악용

소프트웨어 개발 시, 공격에 악용될 수 있는 보안 취약점을 초래할 수 있는 위험(가장 일반적으로 버그 또는 코딩 오류)이 수반됩니다. 제품에 존재하는 소프트웨어 취약점의 수가 많을수록 공격에 노출될 위험이 높아집니다. 제품을 출시하기 전에, 제조업체가 소프트웨어 개발의 모든 단계에서 취약점의 위험을 최소화하는 프로세스와 도구를 포함하는 소프트웨어 개발 모델을 마련하는 것이 이상적입니다.

오류가 전혀 없는 소프트웨어 릴리스를 배포하는 것은 업계에서 드문 일이지만, 보안 위험을 제기하는 버그 및 기타 부적절한 구현은 제품 제조업체가 파악하여 수정하고 고객에게 알려야 합니다. 따라서 제조업체는 새로 발견된 소프트웨어 취약점에 대해 투명하게 알리고 적시에 고객에게 해결책을 제공해야 합니다. 고객이 제품 제조업체에서 제공하는 보안 패치 및 버그 수정이 포함된 소프트웨어 업데이트를 지속적으로 실행하는 것도 중요합니다.

최종 고객이 위험을 완화하기 위해 고려해야 할 사항은 무엇인가요?

우선, 사이버 보안을 염두에 두고 물리적 보안 제품을 조달할 때 고려해야 할 몇 가지 사항이 있습니다.

먼저, 물리적 보안 공급업체의 사이버 보안 접근 방식을 검토하십시오. 공급업체가 사이버 보안을 관리하는 회사 정책을 갖고 있고 이러한 정책에 따라 지속적으로 자산을 식별 및 평가하고 해당 자산과 관련된 위험 평가를 수행하나요? 공급업체가 공급망과 어떻게 협력하는지 이해하는 것도 중요합니다. 이외에도, 공급업체의 제품이 사이버 보안 기능 및 지원이 내장된 상태로 설계 및 제조되나요?

네트워크 제품의 수명 주기 동안 사이버 보안을 지원하기 위해 어떤 조치를 제공하나요? 시스템에 대한 공격이 발생하면 어떻게 하나요? 공급업체의 제품과 관련된 사이버 보안 사고에 대응하는 데 도움이 되는 지침이 있나요?

이러한 질문은 고려해야 할 몇 가지 질문일 뿐입니다. 이어지는 페이지들에서 더 자세히 살펴보겠습니다.

귀사의 감시 공급업체 및 공급업체의 공급업체에 대해 무엇을 알아야 할까요?

보안 위협은 항상 존재합니다. 새로운 위협이 발생하고 그 성격은 언제든지 바뀔 수 있습니다. 종종 조직은 공급업체가 이러한 위험을 평가하고 대응하는 방법에만 집중합니다. 그러나 공급업체의 공급업체는 어떤가요? 공급업체는 어떻게 전체 공급망을 관리하고 유지하며 모든 제품이 부품 수준에서 완제품으로 안전하게 전환하도록 보장하나요?

귀사의 공급업체가 보안 위험 최소화에 초점을 맞춥니까?

> 공급업체가 부품 수준에서 완제품에 이르는 전체 공급망을 통제하나요?

> 공급업체가 보안을 필수적으로 고려하는 소프트웨어 개발 모델을 보유하고 있나요?

> 공급업체가 보호 기능이 내장된 제품을 설계하고 제조하나요?

> 공급업체가 보호를 갖추는 데 필요한 지식과 도구를 공유하나요?

> 공급업체가 새로 발견된 소프트웨어 취약점에 대해 신속한 대응과 무료 업그레이드를 제공하나요?

공급망 파트너

공급망 보안은 엄격한 평가 프로세스를 통해 올바른 공급망 파트너를 선택하는 것에서 시작됩니다. 평가 프로세스에는 각 기업의 품질 및 지속 가능 경영 프로세스에 대한 분석이 포함되어야 합니다. 최소한 ISO 9001 또는 IATF 16949에 따라 제3자의 인증을 받아야 합니다.

하위 공급업체 평가

공급업체는 위험 관리를 위해 하위 공급업체의 프로세스와 생산 시설 및 공정을 평가해야 합니다. 현장 방문과 후속 현장 감사를 통해 해당 시설이 승인된 공급업체 자격 요건과 표준을 충족하는지 평가해야 합니다. 잠재적인 신규 공급망 파트너 평가의 일환으로 하위 공급업체의 재무 상태와 소유 구조를 자세히 분석해야 합니다.

전략적 하위 공급업체

중요 부품의 공급업체 및 제조 파트너와 관련하여 이러한 당사자들과의 관계는 특히 밀접하고 장기적인 경향이 있습니다. 이들은 전략적 하위 공급업체로, 공급업체와 공동 프로젝트 및 개발을 추진하고, 목표를 설정하고, 장기적인 상호 계약을 체결하고 장기적인 상호 계획을 수립합니다. 공급업체 제품의 모든 중요 부품을 전략적 하위 공급업체에서 직접 조달하여 사내에 보관해야 합니다. 중요하지 않은 부품은 제조 파트너가 조달할 수 있지만, 승인된 공급업체 목록에 있는 공급업체로부터만 조달할 수 있습니다.

공급업체의 생산은 얼마나 안전하나요?

> 공급업체가 제조 공정을 정의하고 모니터링하나요?

> 공급업체가 중요한 생산 장비를 개발하고 생산하고 있나요?

> 공급업체가 생산 중에 부품, 모듈 및 제품을 테스트하기 위한 시스템을 소프트웨어, 테스트 컴퓨터 및 기타 IT 하드웨어 인프라와 함께 제공하나요?

> 공급업체가 실시간 데이터 분석을 가능하게 하고 잠재적인 보안 위험을 평가하고 위험 완화 계획을 실행하기 위해 생산 데이터를 연중무휴로 수집하나요?

공급업체가 하위 공급업체가 지정된 요구사항을 준수하도록 하는 가장 좋은 방법은 매년 또는 2년에 한 번씩 정기적 현장 감사를 수행하는 것입니다. 이러한 감사에는 프로세스 준수, 품질 관리, 추적성 기록과 같은 다양한 중요 측면이 포함되어야 합니다. 공장 내 물리적 취급, 재고 관리 및 생산 장비에 대한 검토도 포함되어야 합니다.

분기별 경영 실적 검토는 기대치 대비 성과를 추적하는 좋은 방법입니다. 전략적 하위 공급업체의 경우 이러한 검토는 최고 경영진이 수행하는 것이 좋습니다.

물리적 보안

부품 공급업체에서 유통 센터에 이르기까지 공급망 내의 모든 현장은 시설 보안에 대한 높은 요구사항을 충족해야 합니다. 예를 들어, 출입구를 지속적으로 보호하고 접근 제어 및 방문자 등록을 기록하고 보관해야 합니다. 추가적으로, 스캔 장비를 사용하여 원치 않는 물체나 물질을 감지해야 합니다. 그리고, 엄격한 보안 규정과 관리 조치를 유지하는 잘 알려진 운송업체를 통해서만 운송을 준비해야 합니다. 마지막으로, 카메라를 사용하여 입고 및 출고되는 물품을 자주 감시하고 문서화하는 것이 좋습니다.

제로 트러스트 네트워크

네트워크는 점점 더 취약해지고 있습니다. 연결된 장치가 기하급수적으로 증가함에 따라, 공격에 노출된 네트워크 엔드포인트가 생겨나고 있습니다. 사이버 공격은 더 많아졌을 뿐만 아니라 더 정교해졌습니다. 그 결과, "제로 트러스트"라는 개념이 등장했습니다.

네트워크에서 누구도 그리고 아무것도 신뢰하지 마십시오.

명칭에서 알 수 있듯이 제로 트러스트 네트워크 내의 기본 입장은 네트워크에 연결하는 엔터티 및 네트워크 내의 엔터티 - 인간이든 시스템이든 - 를 신뢰할 수 없다는 것입니다. 이는 이러한 엔터티의 위치와 연결 방식과 관계가 없습니다. 오히려 제로 트러스트 네트워크의 최우선 철학은 "절대로 신뢰하지 말고 항상 확인하라"입니다.

필요한 최소한의 액세스를 고수하십시오.

이를 위해서는 네트워크 내의 동작 및 액세스되는 특정 데이터의 민감도를 기반으로, 액세스하거나 네트워크 내에 있는 모든 엔터티의 정체를 여러 차례 다른 방법으로 확인해야 합니다. 본질적으로 엔터티에는 작업을 완료하는 데 필요한 최소 레벨의 액세스 권한이 부여됩니다.

제로 트러스트 네트워크 및 아키텍처

사이버 보안 강화의 필요성에 대한 고객의 인식이 높아짐에 따라, 고객은 인증된 장치의 네트워크 접속을 자동으로 허용하거나 인증되지 않은 장치를 차단할 수 있는 HTTPS 및 더 정교한 IEEE 802.1X 표준을 포함한 제로 트러스트 네트워크 및 아키텍처를 구현하고 있습니다. 네트워크 장치 제조업체가 이러한 네트워크를 지원하는 기술이나 인터페이스를 포함하여 이러한 요구 사항을 충족하는 것이 필수적인 요소로 자리잡아 가고 있습니다.

제로 트러스트 네트워크 내의 기본 입장은 네트워크에 연결하는 엔터티 및 네트워크 내의 엔터티를 신뢰할 수 없다는 것입니다.

정책 엔진 입력...

모든 제로 트러스트 네트워크의 중심에는 조직이 데이터 및 네트워크 리소스에 액세스 할 수 있는 방법에 대한 규칙을 생성, 모니터링 및 시행할 수 있도록 하는 소프트웨어인 정책 엔진이 있습니다. 정책 엔진은 네트워크 분석과 프로그래밍된 규칙의 조합을 사용하여 여러 요인에 따라 역할 기반 권한을 부여합니다.

모든 요청을 수용 또는 거부

간단히 말해서, 정책 엔진은 네트워크 액세스에 대한 모든 요청을 정책과 비교하고, 요청이 허용되는지 여부를 집행자에게 알립니다. 제로 트러스트 네트워크에서 정책 엔진은 호스팅 모델, 위치, 사용자 및 장치 전반에 걸쳐 데이터 보안 및 액세스 정책을 정의하고 시행합니다.

규칙의 정의 및 적용

정책 엔진이 작동하려면 조직은 차세대 방화벽(NGFW), 이메일 및 클라우드 보안 게이트웨이, 데이터 소실 방지(DLP) 소프트웨어와 같은 주요 보안 관리 수단 내에서 규칙과 정책을 신중하게 정의해야 합니다. 이러한 통제 수단은 함께 결합되어 호스팅 모델 및 위치를 넘어 네트워크 마이크로 세분화를 시행합니다.

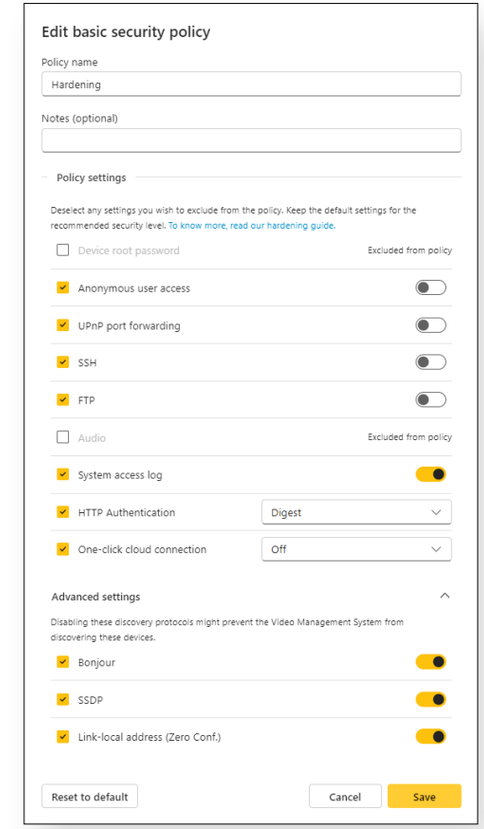
데이터 및 네트워크 리소스에 어떻게 액세스할 수 있나요?

정책 엔진을 사용하면 다음을 수행할 수 있습니다.

> 규칙 생성
> 규칙 모니터링
> 규칙 실행

현재와 미래의 정책 엔진

현재, 각 솔루션의 관리 콘솔에서 정책을 설정해야 할 수도 있지만 점점 더 통합되는 콘솔이 제품 전반에 걸쳐 정책을 자동으로 정의하고 업데이트할 수 있습니다. ID 및 액세스 관리(IAM), 다요소 인증, 푸시 알림, 파일 권한, 암호화 및 보안 오케스트레이션은 모두 제로 트러스트 네트워크 아키텍처 설계에서 일정한 역할을 합니다.



정책 엔진 설정.

효과적인 수명 주기 관리를 구현하는 것이 중요한 이유

위협의 트렌드에 뒤떨어지지 않아야 합니다.

효과적인 수명 주기 관리는 조직이 비즈니스를 안전하게 보호하고 미래에 더 잘 대비할 수 있도록 도와줍니다. 이를 위해 위험이 어디에 있는지 알고 악용될 수 있는 영역에 대한 최신 정보를 유지해야 합니다. 이것은 보안 시스템에 특히 중요합니다. 네트워크 감시 카메라가 작동 중지되면 심각한 결과가 발생할 수 있기 때문입니다.

네트워크에 연결된 장치는 업데이트 필요

네트워크에 연결된 모든 장치(네트워크 카메라에서 VMS에 이르기까지)는 어느 시점에서는 공격자가 알려진 취약점을 악용하고 기존 보호 기능을 약화시키는 것을 방지하도록 업데이트 및 패치해야 합니다.

제조업체는 취약점을 해결하고 버그를 수정하며 기타 성능 문제를 해결하는 장치 소프트웨어용 업데이트 및 보안 패치를 정기적으로 배포하여 안정적이고 안전한 시스템을 유지하는 데 도움이 되도록 합니다. 그러나, 조직은 종종 하드웨어가 실행되는 펌웨어나 운영 체제를 업데이트하지 않습니다.

이는 일반적으로 네트워크의 모든 장치에 대한 전체적인 파악이 부족하기 때문입니다. 오버뷰가 있더라도, 모든 장치를 업데이트하는 것은 번거롭고 시간이 많이 걸릴 수 있습니다.

장치 소프트웨어를 업데이트하지 않으면 장치가 사이버 공격에 취약해질 수 있으며, 운영 손실부터 규정 미준수로 인한 규제 기관의 거액의 벌금에 이르는 다양한 문제를 초래할 수 있습니다.

네트워크는 연결된 장치만큼만 안전하다는 말이 있듯이, 네트워크에 연결된 물리적 자산의 수명 주기를 효과적으로 관리하는 것이 중요합니다.

하나의 장치 – 두 가지 수명

소프트웨어 기반 장치와 관련된 두 가지 유형의 수명 주기가 있습니다:

1) 장치의 기능적 수명 - 또는 장치가 현실적으로 작동하고 기능할 수 있는 기간. 예를 들어 네트워크 카메라의 기능적 수명은 일반적으로 10-15년입니다.

2) 장치의 경제적 수명 주기 - 또는 장치가 새롭고 더 효율적인 기술을 채택하는 비용보다 유지관리 비용이 더 많이 들기 시작할 때까지 얼마나 오래 걸리나요? IP 카메라는 15년 동안 기능할 수 있지만, 사이버 보안 환경의 급격한 변화로 인해 IP 카메라의 실제 수명은 더 짧아질 것입니다.

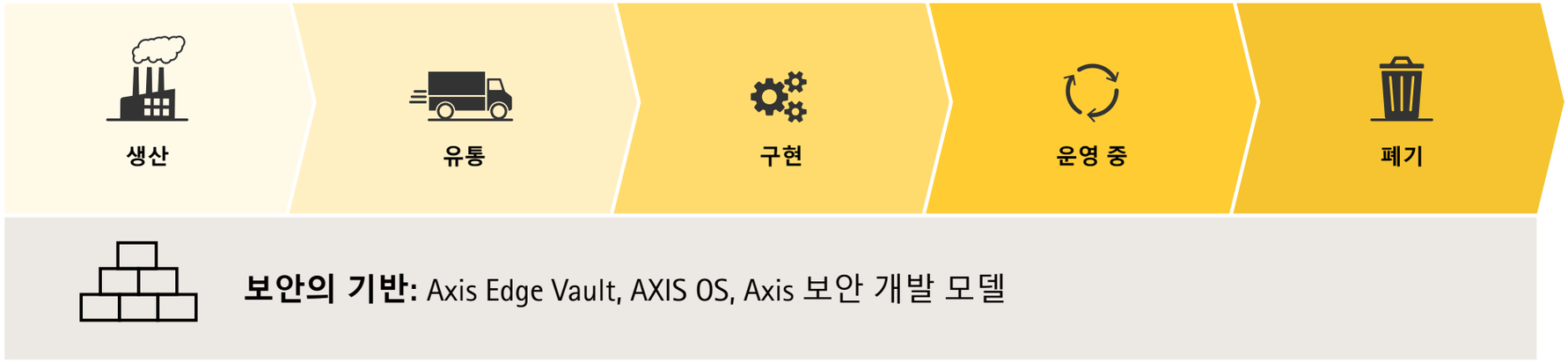
자산을 사전 대응 방식으로 관리하십시오.

수명 주기 관리는 물리적 자산의 기능적 및 경제적 수명 주기를 효과적으로 관리하는 것입니다. 조직은 네트워크에 배포된 모든 장치에 대한 명확한 오버뷰를 파악하여 위협으로부터 안전을 확보해야 합니다.

Axis 사이버 보안 접근 방법

Axis는 높은 수준의 사이버 보안을 지원하기 위해 최선을 다하고 있습니다. Axis는 제품과 사이버 보안 프로세스를 개선하기 위해 지속적으로 노력하고 있습니다. Axis는 Axis의 운영 및 공급망을 보호하는 방법, 취약점 위험을 줄이는 소프트웨어 개발을 처리하는 방법, 새로 발견된 취약점을 관리하는 방법, Axis 제품에 보안을 구축하고 제품 수명 주기 동안 사이버 보안을 지원하는 방법에 대해 투명하게 공개하는 것이 중요하다고 믿습니다.

이어지는 페이지들에서는 Axis의 보안 기초로서 Axis가 취하는 조치를 자세히 설명합니다. 이와 더불어, 생산부터 구현, 운영 중, 폐기에 이르기까지 제품 수명 주기의 다양한 단계에서 위험을 완화하고 귀사가 Axis 제품의 보안을 유지하도록 돕기 위해 Axis가 어떤 작업을 수행하고 무엇을 제공하는지 자세히 설명합니다.



보안 기초

내부 보안에 대한 구조적이고 체계적인 접근 방식

Axis는 보안에 대한 협업적 접근 방식을 장려하며, 이에 따라 모든 직원이 내부 보안의 지속적인 개선을 추진하도록 도울 것을 권장합니다. Axis의 ISO 27001 인증 정보 보안 관리 시스템(ISMS)은 사이버 보안 프레임워크의 기초입니다. Axis는 ISMS의 일부로 사이버 보안 관제를 구현하여 소프트웨어와 커넥티드 서비스를 위한 IT 인프라 및 개발 플랫폼을 관리할 때 모범 관행을 따르도록 하고 있습니다.

Axis는 구조화되고 체계적인 접근 방식을 따름으로써 자산의 기밀성, 무결성 및 가용성을 보호합니다. Axis는 AXIS OS 장치 포트폴리오에 대한 사이버 보안 표준인 ETSI EN 303 645를 포함하여 다양한 규제 요구 사항과 전략적으로 선택된 프레임워크 및 표준도 준수합니다. 그렇지만 규정과 인증에만 의존하지 않으며, 수많은 인증이 반드시 더 나은 사이버 보안을 의미하지는 않습니다.

Axis 규정 준수에 대해 자세히 알아보기

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

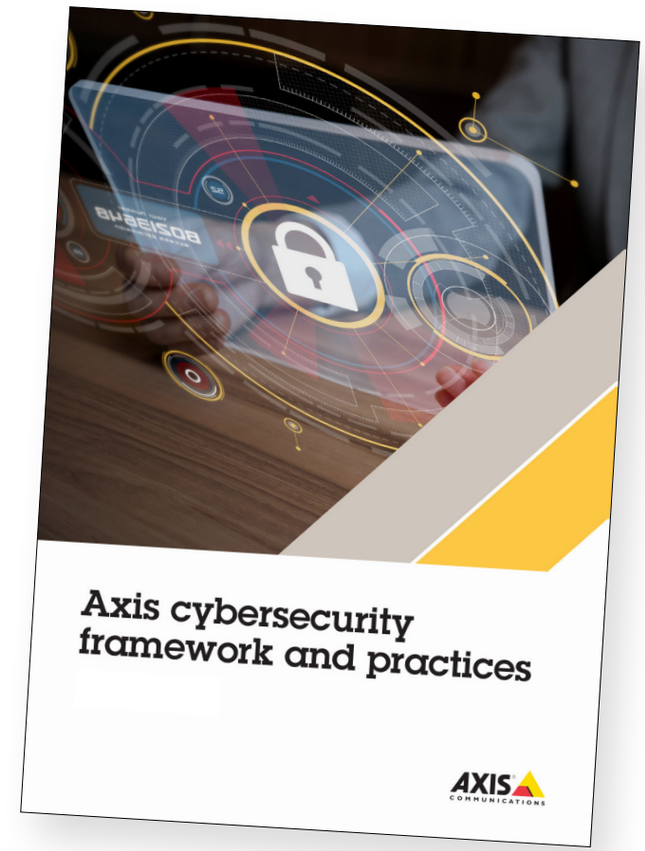
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 | | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(1)



제품 무결성 보호 및 소프트웨어의 취약점 위험 감소

내부 보안에서 제품 보안으로 넘어가면, 다음 조치가 Axis 하드웨어 및 소프트웨어의 보안 기초를 형성하며, 투명성이라는 Axis의 기본 원칙을 반영합니다.

Axis Edge Vault 사이버 보안 플랫폼

Axis 장치에 내장된 이 하드웨어 기반 플랫폼에는 Axis 장치의 무결성을 보호하는 기능이 포함되어 있어 장치를 안전하게 부팅하고 통합하며 암호화 키와 같은 민감한 데이터를 무단 액세스로부터 보호할 수 있습니다.

Axis Edge Vault에 대해 자세히 알아보기

Axis 보안 개발 모델(ASDM)

ASDM은 소프트웨어 취약점이 있는 제품을 출시할 위험을 줄이기 위해 Axis에서 적용하는 개발 방법론입니다. 이 방법은 보안 고려 사항이 소프트웨어 개발의 필수적인 부분이 되도록 보장하며, 위험 평가, 위협 모델링, 코드 분석, 침투 테스트, 버그 바운티 프로그램, 취약점 스캔 및 관리와 같은 영역을 다룹니다. ASDM은 개발의 모든 단계에서 문제를 신속하게 감지하고 해결함으로써 Axis 고객의 보안 관련 위험을 줄이는 데 도움을 줍니다.

상세 정보 읽기 ASDM

AXIS OS

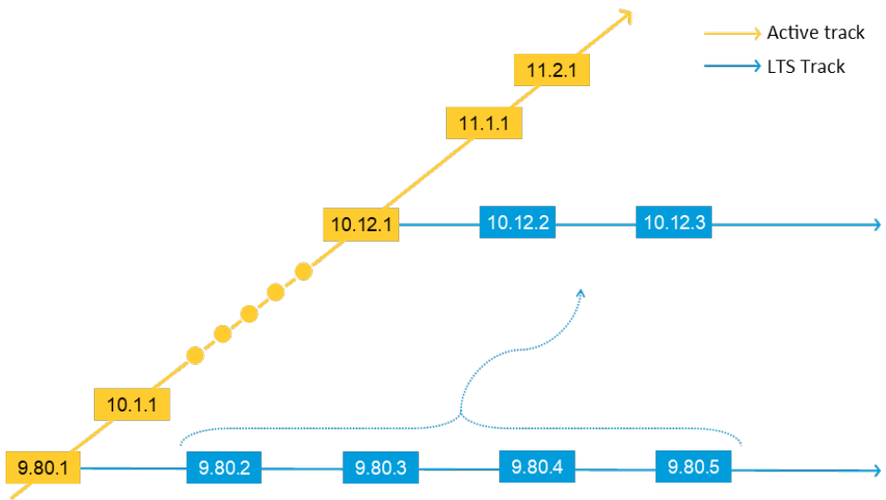
AXIS OS는 에지 장치를 위한 Linux 기반 운영 체제입니다. 개방성, 투명성 및 사이버 보안을 중심으로 구축된 이 강력한 운영 체제는 Axis 장치를 위한 다양한 OS 트랙을 갖추고 있어, Axis가 수많은 제품에 걸쳐 소프트웨어 보안 기능 및 패치를 신속하게 배포할 수 있도록 합니다. 이 운영 체제는 위험을 완화하고 Axis 제품과 서비스를 최신 상태로 유지하고 보호하는 것을 돕도록 고안되었습니다. 많은 제품의 지원 종료 날짜가 Axis 웹사이트에 표시되므로, 적시에 제품의 폐기 및 교체를 계획할 수 있습니다.

AXIS OS에 대해 자세히 알아보기

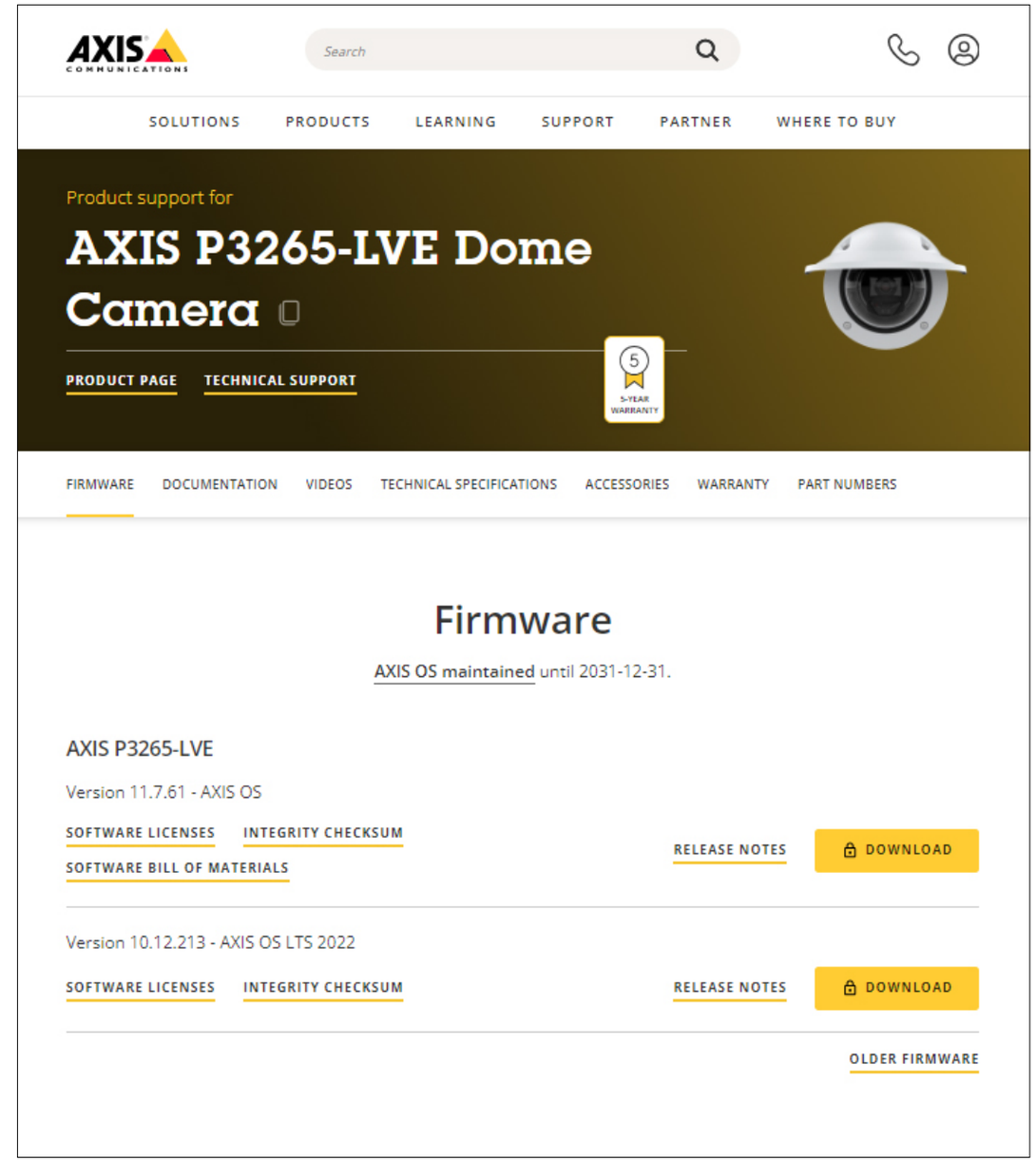
소프트웨어 구성품 명세서(SBOM)

추가적으로, Axis는 고객, 보안 연구자 및 당국을 위해 사이버 보안에 더욱 중점을 두고 투명성을 개선한 AXIS OS용 소프트웨어 구성품 명세서(SBOM)를 게시합니다. SBOM은 Axis 장치용 운영 체제를 구성하는 데 사용되는 구성 요소의 광범위하고 상세한 목록을 제공합니다. 이 목록은 공급업체가 적용한 사이버 보안 모범 관행에 대한 인사이트를 제공하며, 취약점 평가, 위협 분석 및 수정 계획을 전문으로 하는 제삼자를 위한 귀중한 정보를 포함합니다.

소프트웨어 구성품 명세서에 대해 자세히 알아보기



AXIS OS 트랙.



새로 발견된 취약점 관리

공통 취약점 및 노출(CVE) 번호 지정 기관(CNA)의 회원사로서 Axis는 고객이 적절하고 시기적절한 조치를 취할 수 있도록 취약점에 대한 정보를 게시하고 이해 관계자에게 알립니다. Axis는 외부 연구자와 협력하여 투명하고 책임감 있고 조율된 프로세스를 통해 취약점과 노출을 공개합니다. Axis는 해당 장치, 소프트웨어 또는 서비스에 패치를 제공하고 필요한 모든 정보를 **Axis 웹사이트**와 공개적으로 이용 가능한 CVE 프로그램 취약점 데이터베이스를 통해 게시합니다. 이외에도, Axis는 귀사가 가입하여 취약점 및 기타 보안 관련 문제에 대한 정보를 받을 수 있도록 보안 알림 서비스를 제공합니다. Axis는 설치된 제품의 운영 체제를 최신 상태로 유지하여 최신 보안 패치가 적용될 수 있도록 하는 것의 중요성을 강조합니다.

Axis 취약점 관리 정책에 대해 자세히 알아보기

버그 바운티 프로그램

Axis는 투명한 취약점 관리 전략의 일환으로 버그 바운티 프로그램을 운영합니다. 이 프로그램은 크라우드 소싱 사이버 보안의 선두주자인 Bugcrowd와 협력하여 진행됩니다. Axis는 외부 보안 연구자 및 윤리적 해커와 전문적인 관계를 구축하기 위해 최선을 다하고 있습니다. 이 프로그램의 일환으로, AXIS OS 기반 제품의 취약점을 발견한 연구자는 "바운티" 현금 보상을 받을 수 있습니다. 그런 다음 Axis는 발견된 취약점 등을 외부에 투명하게 공개하고 영향을 받는 제품에 패치를 제공합니다.

생산

유통

손상된 하드웨어 및 소프트웨어 구성 요소의 위험 감소

공급망 보안

모든 제품과 마찬가지로 물리적 보안 제품은 무결성을 유지하면서 설계의 목적에 맞게 그리고 의도한 대로 작동해야 합니다. 이는 제품이 공급망을 통과하는 동안 제품의 하드웨어 및 운영 체제가 무단 변경 또는 조작으로부터 성공적으로 보호되는 경우 달성할 수 있습니다.

품질 관리

Axis는 공급업체 및 제조 파트너와 함께 제품의 무결성을 유지하고 보호하기 위해 다양한 품질 관리를 적용합니다. 부품은 항상 Axis 규격에 명시된 BOM에 따라 승인된 공급업체 목록에 있는 공급업체로부터 공급됩니다. 공급업체는 Axis의 허가 없이 규격, 작업 지침 또는 품질 검사 문서를 변경할 수 없습니다. 승인된 변경사항은 모두 문서화하고 기록해야 합니다.

추적성

자재 취급 프로세스는 항상 자재 상태를 유지하여 품질을 손상시킬 수 있는 편차를 모두 드러냅니다. 공급업체와 제조 파트너는 입고 자재에서 완성된 부품에 이르는 생산품을 추적할 수 있도록 추적 시스템을 유지해야 합니다. 생산 중에 물리적 부품은 여러 테스트를 거쳐 적합성을 확인하고 편차를 드러냅니다.

위조 부품 탐지

자동 광학 검사(AOI)로 위조 부품이 장착되지 않았는지 확인할 수 있습니다. Axis에서는 중요한 생산 장비는 물론 생산 과정에서 부품, 모듈 및 제품을 다양한 단계에서 테스트하기 위한 시스템을 개발하고 생산합니다. 이 프로세스는 변조 위험을 제한합니다. 추가적인 보안 관리 조치로서, 모든 테스트 데이터를 Axis와 연중 무휴로 공유하여 무단 수정을 즉시 발견할 수 있도록 합니다.

Axis 공급망 보안에 대해 자세히 알아보기

배포 중 위협에 대응하기

Axis 장치에 내장된 사이버 보안 기능은 공장 출하 시 장치에 기본값으로 설정되어 있어, 배송 중 무단 소프트웨어 수정으로부터 보호합니다. Axis Edge Vault에서 지원하는 기능(다음 페이지에서 자세히 설명)은 장치의 민감한 정보를 보호하고 장치에서 정품 Axis 운영 체제만 실행되도록 합니다.

공급업체가 조직에 가해지는 위험을 완화할 수 있는 조치를 실행하고 있는지 확인하기 위해 공급업체 위험 평가를 수행할 때, 공급망 보안을 이해해야 합니다.

내장형 사이버 보안 기능

Axis 장치에는 안전한 부팅과 간편한 온보딩을 가능하게 할 수 있고 민감한 정보가 보호되도록 할 수 있는 보안 기능이 내장되어 있습니다.

Axis Edge Vault 사이버 보안 플랫폼
Axis의 하드웨어 기반 사이버 보안 플랫폼은 Axis 장치가 네트워크의 신뢰할 수 있고 안정적인 요소가 될 수 있도록 견고한 기반을 제공합니다. Axis Edge Vault에는 다음과 같은 기능*이 내장되어 있습니다.

> **보안 키 저장소**. 여기에는 암호화 키를 안전하게 저장하는 암호화 컴퓨팅 모듈이 포함되며, 장치가 손상된 경우에도 장치의 ID 및 기타 민감한 정보를 무단 액세스로부터 보호합니다. 암호화 컴퓨팅 모듈은 Axis 시스템 온 칩(SoC)에 내장된 신뢰할 수 있는 실행 환경(Trusted Execution Environment)일 수 있습니다. 마더보드의 별도 칩인 보안 요소 또는 신뢰할 수 있는 플랫폼 모듈(Trusted Platform Module)일 수도 있습니다. Axis 장치는 이 세 가지 모듈 중 하나 또는 그 조합을 사용하여 구축됩니다.

> **Signed firmware** 및 **Secure boot**. 장치가 정품 Axis 운영 체제(AXIS OS)만 다운로드하고 실행하도록 합니다.

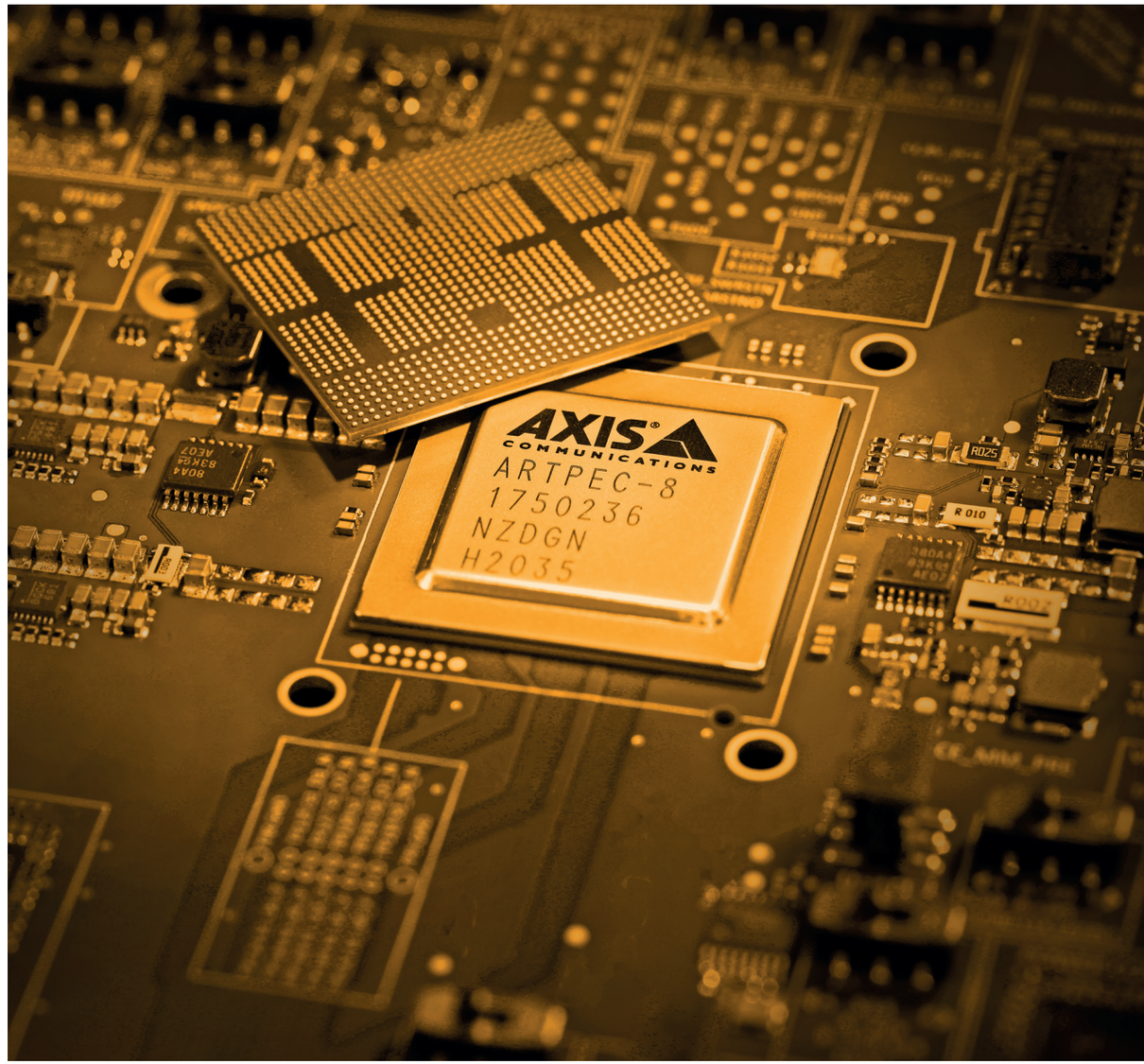
> **Axis 장치 ID**. IEEE 802.1AR을 준수하며 안전한 장치 식별 및 네트워크 온보딩에 사용됩니다.

> **암호화된 파일 시스템**. 시스템 통합업체에서 최종 고객으로 전송되는 경우와 같이 장치를 사용하지 않는 동안 파일 시스템의 데이터가 추출되거나 변조되지 않도록 보호합니다.

> **Signed video**. 사용자가 캡처한 영상의 진위 여부를 확인하고 영상이 변조되지 않았는지 확인할 수 있도록 합니다.

참고: 모든 장치 모델이 모든 Axis Edge Vault 기능을 지원하는 것은 아닙니다. 제품에서 지원되는 기능을 확인하려면 데이터시트 또는 Axis 제품 선택기를 확인하십시오.

상세 정보 Axis Edge Vault



기본값 설정

제품 보안 기능 외에도, Axis 장치는 사전 정의된 기본 보호 설정과 함께 제공됩니다.

자격 증명 및 네트워크 프로토콜

사용자 이름과 패스워드가 포함된 계정을 설정할 때까지 Axis 장치가 작동하지 않습니다. 설정 후에는 해당 자격 증명을 사용할 때만 관리자 기능 및/또는 비디오 스트림에 액세스할 수 있습니다.

이외에도, 장치 인터페이스에 액세스하기 위한 HTTP 및 HTTPS, 비디오 및 오디오 스트리밍을 위한 RTSP 및 RTP, 제삼자 애플리케이션에서 Axis 장치를 검색하기 위한 UPnP 및 Bonjour와 같은 일부 프로토콜 등 최소 수의 네트워크 프로토콜 및 서비스만 기본적으로 Axis 장치에서 활성화됩니다.

고객의 제로 트러스트 네트워크 요구 사항 충족

Axis는 고유한 Axis 장치 ID를 갖고 있고 HTTPS 프로토콜 및 IEEE 802.1X 표준, 장치 인증을 위한 IEEE 802.1AR 및 자동 데이터 암호화를 위한 IEEE 802.1AE MACsec을 지원하는 제품을 생산하여 제로 트러스트 요구 사항에 대응하고 있습니다.

HTTPS가 기본적으로 활성화되어 있어, 장치의 패스워드를 안전하게 설정할 수 있습니다. 이외에도, HTTPS를 사용하는 영상 관리 소프트웨어가 최신 제품의 Axis 장치 ID에서 지원하는 신뢰할 수 있는 CA 서명 SSL 인증서를 확인할 수 있도록 합니다.

Axis 제품에서 기본적으로 활성화되는 IEEE 802.1X, IEEE 802.1AR 및 IEEE 802.1AE를 지원하여 자동화된 장치 온보딩, 인증 및 엔드 투 엔드 암호화를 가능하게 합니다. 이를 통해 IEEE 802.1X를 지원하여 Axis 장치를 기업 네트워크에 효율적이고 안전하게 통합할 수 있는 표준 메커니즘을 IT 전문가에게 제공합니다. Aruba 네트워크에서 Axis 장치를 사용하는 고객은 Axis 장치의 안전한 온보딩 및 관리를 위한 모범 관행 구성을 설명하는 통합 가이드를 다운로드할 수 있습니다.

엔터프라이즈 IT용 Axis 솔루션에 대해 자세히 알아보기

구현

구현 중의 사이버 보안

Axis 장치는 랩톱, 데스크톱 컴퓨터 또는 모바일 장치와 같은 다른 장치와 마찬가지로 네트워크 엔드포인트입니다. 그러나 노트북 컴퓨터와 달리, Axis 장치는 사용자가 잠재적으로 유해한 웹사이트를 방문하거나 악성 이메일 첨부 파일을 열거나 신뢰할 수 없는 애플리케이션을 설치하도록 하지 않습니다. 그럼에도 불구하고 네트워크 비디오, 오디오 또는 접근 제어 제품은 연결된 시스템에 위험을 노출시킬 수 있는 인터페이스가 있는 장치입니다.

Axis 제품에 제공되는 보안 강화 가이드는 사이버 위험에 대한 노출을 줄이는 방법에 대한 권장 사항을 제공합니다. 다음은 몇 가지 기본 권장 사항입니다. 예를 들어, 장치를 구성하기 전에 공장 기본 설정을 수행하여 원치 않는 소프트웨어나 구성이 없도록 하는 것이 좋습니다.

이외에도, 장치가 특정 장치에 대한 최신 보안 패치 및 버그 수정이 포함될 최신 AXIS OS에서 실행되는지 확인합니다.

강력한 패스워드를 설정하고, 장치의 웹 인터페이스에 대한 직접 액세스를 제한하고, HTTPS(클라이언트와 장치 간의 데이터 트래픽을 암호화하는)만 사용하도록 장치를 구성하고, 사용하지 않는 서비스 및 기능을 비활성화하여 불필요한 위험을 줄여야 합니다. 장치에서 날짜와 시간을 올바르게 설정하여 정확한 시스템 로그를 기록하고 HTTPS 및 IEEE 802.1X와 같은 서비스가 의존하는 디지털 인증서가 유효성이 검사되고 사용될 수 있도록 하는 것도 중요합니다.

로컬에서 Axis 장치를 효율적으로 구성하고 관리할 수 있도록 하는 Axis 도구는 AXIS Device Manager입니다. 이 도구를 사용하면 장치 자격 증명 관리, 디지털 인증서 배포, 사용하지 않는 서비스 비활성화, AXIS OS 업그레이드와 같은 설치 및 보안 작업을 일괄 처리할 수 있습니다. 장치 관리 소프트웨어에 대한 자세한 내용은 다음 페이지를 참조하십시오.

AXIS OS 기반 장치에 대한 전체 및 확장 보안 강화 권장 사항은 AXIS OS 보안 강화 가이드를 참조하십시오. Axis 영상 관리 소프트웨어 및 네트워크 스위치에 대한 보안 강화 가이드에 액세스하려면, 사이버 보안 리소스 페이지로 이동하십시오. Axis 장치를 엔터프라이즈 IT 인프라 및 네트워크에 원활하게 통합할 수 있는 방법에 대한 자세한 내용은 엔터프라이즈 IT용 Axis 솔루션을 참조하십시오.

Axis는 위험을 완화하고 Axis 제품 및 서비스를 최신 상태로 유지하고 보호하는 데 도움이 되는 도구, 설명서 및 교육을 제공합니다. **Axis 사이버 보안 리소스**를 참조하십시오.

운영 중

운영 중인 장치의 사이버 보안

장치 운영 중에, 장치의 사이버 보안을 유지하는 가장 중요한 방법 중 하나는 펌웨어 또는 운영 체제인 AXIS OS가 최신 상태로 유지되는지 확인하는 것입니다. 이를 통해 장치에 최신 보안 패치와 버그 수정이 통합되도록 합니다. Axis 장치의 기능, Signed firmware 및 Secure boot는 정품 AXIS OS만 설치 및 작동할 수 있도록 합니다. 무료로 제공되는 AXIS OS 버전은 활성 트랙 또는 장기 지원(LTS) 트랙에 속합니다. 활성 트랙에 속한 AXIS OS 버전은 새로운 기능을 지원하지만, LTS 트랙에 속한 버전은 호환성 문제의 위험을 최소화하기 위해 새로운 기능을 지원하지 않습니다. 그러나 두 트랙 모두 보안 패치와 버그 수정이 포함되어 있습니다. 새로 발견된 취약점을 계속 확인하는 방법은 Axis 보안 알림 서비스에 등록하는 것입니다. 게시된 취약점에는 해당 제품을 새 장치 소프트웨어로 수정하는 방법에 대한 지침이 포함될 것입니다.

많은 수의 장치에 대한 운영 체제를 더 쉽고 더 효율적으로 업데이트할 수 있도록, Axis는 AXIS Device Manager 및 AXIS Device Manager Extend와 같은 장치 관리 소프트웨어를 제공합니다.

장치 관리 소프트웨어는 어떻게 작동하나요?

장치 관리 소프트웨어는 모든 카메라, 엔코더, 접근 제어, 오디오 및 네트워크에 연결된 기타 장치의 전체 실시간 인벤토리를 신속하게 수집할 수 있습니다. 장치 관리 소프트웨어는 전체 네트워크를 스캔하고, 새 장치 또는 업데이트된 장치가 발견되면 모델 번호, IP 및 MAC 주소, 장치 소프트웨어 버전 및 인증서 상태를 포함한 모든 주요 정보를 수집합니다.

전체 오버뷰

전체 네트워크 생태계를 매우 상세하게 파악하여 모든 장치에 걸쳐 일관된 수명 주기 관리 정책 및 관행을 쉽게 실행하고 모든 주요 설치, 배포, 구성, 보안 및 유지관리 작업을 안전하게 관리할 수 있습니다.

장치 관리를 위한 사이버 보안 정책과 모범 관행은 패스워드 강도 및 사용자가 패스워드를 변경해야 하는 빈도, 잠재적 공격의 표면 영역을 줄이기 위해 사용하지 않는 서비스를 비활성화해야 하는지,

장치의 취약점을 얼마나 자주 검사해야 하는지, 제조업체가 알려진 악용 사례를 게시할 때 위험 수준을 평가하는 절차를 마련해야 하는지 등의 질문을 다루어야 합니다.

시간과 노력의 절약

장치 관리 소프트웨어는 조직이 사이버 보안 위험을 관리하는 데 드는 시간과 노력을 절약하는 데 도움이 됩니다. 장치 관리 소프트웨어는 다음과 같은 용도로 사용할 수 있습니다.

> 시스템 변경, 장치 소프트웨어 업데이트 및 새 디지털 인증서를 모든 적절한 장치에 동시에 푸시합니다.

> 보안 설정을 쉽게 생성 또는 재구성하고 전체 네트워크에 적용하여 모든 장치가 최신 보안 정책 및 관행을 준수하도록 합니다.

> 모든 장치가 가장 안전한 최신 소프트웨어 버전을 실행하고 있는지 확인합니다.

> 네트워크에 걸쳐 사용자 권한 수준을 관리하고 수정 사항을 구성합니다.

실시간 인사이트를 확보하십시오.

장치 관리 도구는 조직의 생태계 상태에 대한 실시간 인사이트를 조직에 제공합니다. 예를 들어, 최신 소프트웨어 업데이트 및 인증서로 업데이트해야 하는 장치를 확인할 수 있을 뿐만 아니라 제품 단종 및 지원 종료 날짜에 대한 정보를 얻을 수 있으므로 장치를 교체해야 하는 시기를 계획할 수 있습니다.

Axis의 장치 관리 도구

Axis의 장치 관리 소프트웨어인 AXIS Device Manager 및 AXIS Device Manager Extend를 사용하면 Axis 장치를 효율적으로 관리할 수 있습니다. AXIS Device Manager와 AXIS Device Manager Extend는 서로를 보완합니다.

AXIS Device Manager

AXIS Device Manager는 새 장치를 빠르고 쉽게 설치하고 구성할 수 있도록 도와줍니다. 이 온프레미스 도구는 소프트웨어 업그레이드 및 애플리케이션 설치를 비롯한 모든 주요 설치, 보안 및 운영 작업을 지원합니다. 이 도구는 백업 및 복원 설정으로 Axis 장치를 구성할 수 있도록 하며, 따라서 사용자가 보증 상태를 확인할 수 있습니다. HTTPS 및 IEEE 802.1X 인증서와 같은 사이버 보안 관제를 적용할 수도 있습니다.

AXIS Device Manager에 대해 자세히 알아보기

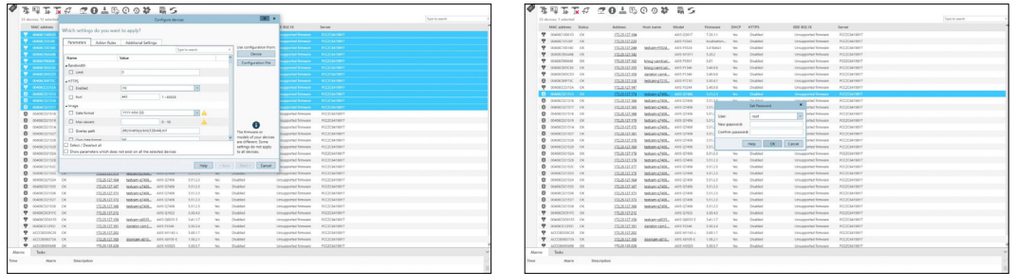
AXIS Device Manager Extend

다중 사이트 운영에 이상적인 AXIS Device Manager Extend를 사용하면 모든 사이트의 자산을 원격으로 관리할 수 있습니다. 사용하기 쉬운 이 애플리케이션은 AXIS OS 업그레이드, 보안 정책 정의, 적용 및 시행, 애플리케이션 관리와 같은 중요한 유지 관리 작업의 확장을 단순화합니다. 실시간 대시보드를 통해 오프라인 상태이거나 보증 기간이 지난 장치와 같은 시스템의 잠재적 문제에 대한 상황 인식을 제공하여 문제 해결 속도를 높입니다. 이외에도, 보안 위협을 최소화하고 취약성을 완화하는 데 도움이 되는 장치 설정에 대한 권장 사항을 제공합니다. 모든 Axis 장치에 대해 동시에 보안 정책을 정의, 적용 및 시행할 수 있습니다.

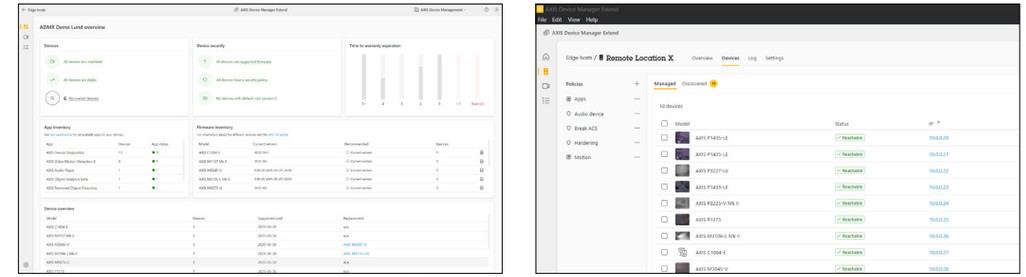
AXIS Device Manager Extend에 대해 자세히 알아보기

보안 침해가 발생한 경우

네트워크에 보안 침해가 발생한 경우, Axis는 Axis 네트워크 장치에 대한 포렌식 분석을 수행하는 데 도움이 되는 AXIS OS 포렌식 가이드를 제공합니다.



AXIS Device Manager 인터페이스 스냅샷.



AXIS Device Manager Extend 인터페이스 스냅샷.

폐기

폐기 계획

업데이트와 패치는 제품의 사이버 보안을 유지하는 가장 좋은 방법이지만, 제품이 너무 오래되어 지원을 받을 수 없는 경우 항상 사용할 수 있는 것은 아닙니다.
사이버 보안의 관점에서 볼 때, 오래되고 패치가 적용되지 않은 제품은 큰 위험을 초래할 수 있습니다. 간과된 장치는 쉽게 공격자의 진입 지점이 될 수 있습니다.

더 이상 지원되지 않고 잠재적으로 패치되지 않은 취약점이 있는 장치를 실행하는 위험을 피하려면 제품을 폐기해야 하는 시기를 계획하는 것이 중요합니다. Axis는 제품의 운영 체제에 대한 지원 종료 날짜를 표시하므로 적시에 장치를 폐기하고 교체할 준비를 할 수 있습니다. 이외에도, AXIS Device Manager Extend를 사용하면 시스템의 모든 장치에 대한 보증, 제품 단종 및 지원 종료 정보를 얻을 수 있습니다.

폐기된 장치에서 데이터를 제거하는 것도 중요합니다. 공장 출하 시 기본 설정을 수행하면 장치에서 모든 구성과 데이터를 빠르게 지울 수 있습니다. 제품 폐기에 대한 자세한 내용은 AXIS OS 포털을 참조하십시오.

규정 준수

각국 정부는 자국 내에서 활동하는 모든 기업이 준수해야 하는 사이버 보안 관련 법률과 규정을 점점 더 많이 통과시키고 있습니다. 마찬가지로, 산업과 조직에서도 제품 및 서비스 인증을 비롯한 특정 표준 준수를 점점 더 많이 의무화하고 있습니다. 법률과 규정을 준수하고 비즈니스 프로세스와 관련된 지침과 규격을 이행하는 것은 모든 이해관계자의 책임입니다.

기준으로서 사이버 보안 규정 준수

사이버 보안 규정 준수는 당국이 정의한 표준 및 규제 요건을 준수하는 것을 의미합니다. 표준과 인증이 중요하다는 것은 의심의 여지가 없지만, 이는 스토리의 일부일 뿐입니다.

표준과 인증을 준수하는 것이 '확인란 체크 표시' 연습이 되는 위험은 항상 존재합니다.

사이버 보안 규정 준수는 지속적으로 진화하고 있으며, 한때는 "있으면 좋다"고 간주되던 규정이 빠르게 의무 사항이 되고 있습니다.

그렇기 때문에 조직은 표준과 인증을 기준으로 간주해야 합니다. 즉 목표가 아닌 최소한의 요구 사항으로 간주해야 합니다. 진정한 목표는 공급업체가 가능하면 가장 안전한 방식으로 운영할 수 있는 제품과 서비스를 제공하는 것입니다. 그리고 고객에게 지속적인 사이버 보안 유지 관리의 필요성을 뒷받침하기 위해 지침과 투명성을 제공하는 것입니다.

규제

사이버 보안 규제는 조직이 조직의 시스템과 정보를 보호하고 조직이 제공하는 제품 및 서비스가 최소한의 보안 수준을 갖추도록 하는 것을 목표로 합니다. 몇 가지 중요한 규제와 그 적용 방식을 살펴보겠습니다.

2023년에 NIS2 지침이 발효되었으며, 유럽연합 회원국들은 2024년 10월까지 해당 조치를 국내법으로 전환해야 합니다. 이 지침에 따라 필수 부문에 종사하는 모든 EU 기업은 높은 수준의 공통 사이버 보안을 갖춰야 합니다. 공급업체 중 하나의 장애로 인한 것이라도 사이버 보안이 소홀한 기업은 불이익을 받을 수 있습니다.

따라서 앞으로는 공급업체 평가와 공급망 보안이 더욱 중요해질 것입니다. 이 지침은 제조업체, 수입업체 및 유통업체에 간접적으로 의무를 부과할 것이며, 이들은 제품의 수명 주기 동안 주의 의무를 다해야 합니다.

2023년 12월, EU는 디지털 요소가 포함된 하드웨어 및 소프트웨어 제품에 대한 공통 사이버 보안 표준을 정의하는 사이버 복원력법(Cyber Resilience Act)이라는 새로운 규제에 잠정적으로 합의했습니다. 여기에는 IoT 장치와 같이 다른 장치나 네트워크에 직간접적으로 연결된 제품이 포함됩니다. 이 법안은 사이버 보안 사고의 수를 줄이는 동시에 투명성을 높이고 데이터 보호 강화를 보장하는 것을 목표로 합니다. 영국은 2024년 4월에 발효되는 영국 제품 보안 및 통신 기반시설 법(UK Product Security and Telecommunications Infrastructure)이는 유사한 법률을 통과시켰습니다.

미국 정부와 비즈니스를 수행하는 조직은 사이버 보안 절차의 내부 관리에 기반한 감사 인증을 요구하는 사이버 보안 성숙도 모델 인증(Cybersecurity Maturity Model Certification)과 같은 표준을 준수해야 할 수도 있습니다.

사이버 보안을 보장하려면 지속적인 감시와 유지 관리가 필요합니다.

표준과 인증

대부분의 표준과 인증은 보안이 필수 요소가 되도록 하기 위해 기능, 대응 조치 및 프로세스에 중점을 둡니다. 이는 소프트웨어 취약점을 찾기 위한 모의 침투 테스트 및 버그 바운티 프로그램과 같은 제삼자 테스트로 보완할 수 있습니다.

제품 인증에 의존하면 고객과 정부가 어느 정도 안심할 수 있지만, 인증의 유효 기간은 일반적으로 1년이며 그 이후에는 재인증을 받아야 한다는 점에 유의해야 합니다. 새로운 기술과 기능이 지속적으로 개발되고 시장에 출시됨에 따라 인증이 뒤처질 수 있습니다.

표준이 사이버 보안 태세를 강화하는 데 도움이 될 수 있더라도 사이버 보안 사고를 방지할 수 있는 것은 아닙니다. 조직은 위협과 보안 정책을 지속적으로 검토해야 합니다.

Axis라야 하는 이유

사이버 보안 추구

사이버 보안은 Axis의 필수적인 부분입니다. 사이버 보안은 Axis의 내부 정보 보안 시스템, 공급망 관리, 제품 및 서비스 개발, 소프트웨어 취약점 관리의 기준입니다. Axis는 사이버 보안을 투명성이 핵심인 공유되고 지속적인 책임으로 간주합니다. Axis는 사용자가 Axis 제품 및 서비스를 가장 안전한 방식으로 제품을 사용할 수 있도록 하는 것을 목표로 합니다. 바로 이것이 Axis가 사이버 보안 기능과 보호 기본 설정이 내장된 제품을 설계 및 제조하고 보안 강화 가이드를 제공하는 이유입니다. Axis는 지속적으로 위협을 모니터링하고 보안을 개선하는 방법을 모색합니다. CVE 번호 지정 기관으로서 Axis는 새로 발견된 취약점을 패치하고 공개하여 고객이 적절하고 시기적절한 조치를 취할 수 있도록 대응합니다. Axis는 설치 후에도 고객이 Axis 장치의 보안을 지속적으로 강화할 수 있도록 소프트웨어 업그레이드를 제공합니다. 이외에도, AXIS Device Manager 및 AXIS Device Manager Extend와 같은 도구를 통해 Axis 장치를 더 쉽게 관리하여 장치 수명 주기 동안 사이버 보안 위험을 완화할 수 있습니다.

Axis를 선택해야 하는 다른 이유

> 모든 일에서 품질 제일 추구:

모든 Axis 제품은 고객이 안심할 수 있도록 광범위한 테스트를 거칩니다.

> 혁신적 기술:

Axis는 기술과 인간의 상상력을 결합하여 성능과 유용성을 모두 향상시킵니다. 개방형 산업 표준을 기반으로 구축되어 유연하고 확장 가능하며 통합하기 쉽습니다.

> 모든 수준에서 지속 가능성 추구:

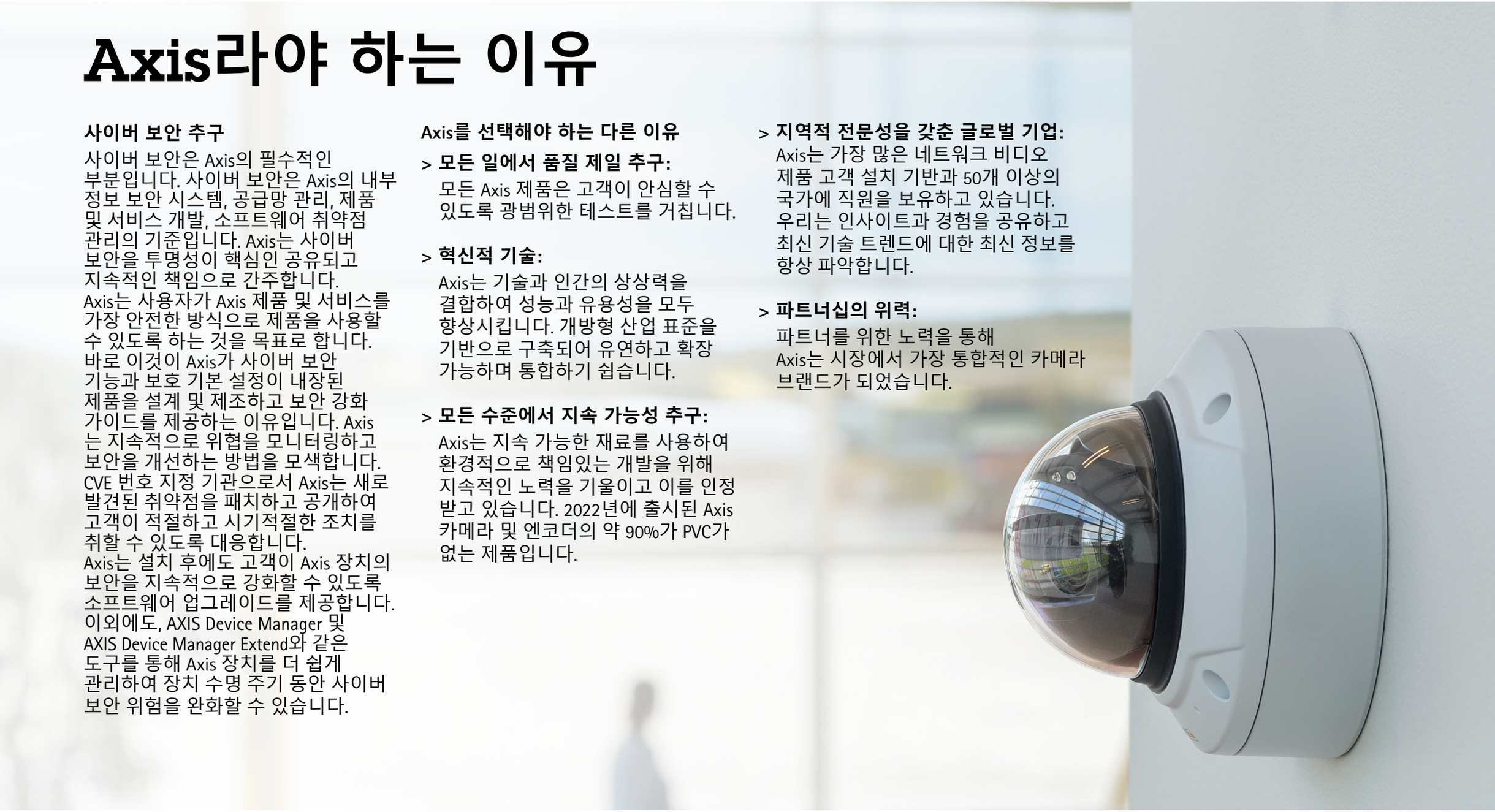
Axis는 지속 가능한 재료를 사용하여 환경적으로 책임있는 개발을 위해 지속적인 노력을 기울이고 이를 인정받고 있습니다. 2022년에 출시된 Axis 카메라 및 엔코더의 약 90%가 PVC가 없는 제품입니다.

> 지역적 전문성을 갖춘 글로벌 기업:

Axis는 가장 많은 네트워크 비디오 제품 고객 설치 기반과 50개 이상의 국가에 직원을 보유하고 있습니다. 우리는 인사이트과 경험을 공유하고 최신 기술 트렌드에 대한 최신 정보를 항상 파악합니다.

> 파트너십의 위력:

파트너를 위한 노력을 통해 Axis는 시장에서 가장 통합적인 카메라 브랜드가 되었습니다.



Axis Communications에 대하여

Axis는 보안 및 비즈니스 성과 향상을 위한 솔루션을 개발하여 더 스마트하고 더 안전한 세상을 만들 수 있도록 지원합니다. 네트워크 기술 회사이자 업계 선도 기업인 Axis는 영상 감시, 접근 제어, 인터콤 및 오디오 시스템을 위한 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 보완되고 고품질 교육을 통해 지원됩니다.

50개 이상의 국가에서 약 4,000명의 Axis 임직원이 전 세계의 기술 및 시스템 통합 파트너와 협력하여 고객에게 최적의 솔루션을 제공하고 있습니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다.