Cybersecurity reference guide

사용자 설명서

목차

Cybersecurity reference guide

소개

소개

이 가이드의 목적은 공통 기준을 제공하고 Axis에서 제작한 사이버 보안 관련 자료에 대한 참조 자료 역할을 하는 것입니다. 이는 NIST, SANS, ISO 및 RSA 컨퍼런스와 사이버 보안 커뮤니티 내 다양한 조직의 자료를 기반으로 한 단순화된 설명, 모델 및 구조입니다.

Axis의 다른 자료에 대한 링크:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

사이버 보안의 정의

부분적으로 NIST의 정의를 기반으로 합니다.

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

조직 유형

조직마다 자산, 리소스, 노출 및 사이버 성숙도가 다릅니다. 권장 사항을 따를 때, *CIS 통제(이전의 중요 보안 통제)* 세 가지 조직 프로파일을 정의합니다.

- **SANS 구현 그룹 1(IG1)**

  대부분의 경우 IG1 기업은 일반적으로 IT 자산과 직원을 보호하는 데 전념할 IT 및 사이버 보안 전문 지식이 제한적인 중소기업입니다.

- **SANS 구현 그룹 2(IG2)**

  IG2 기업은 IT 인프라 관리 및 보호를 담당하는 개인을 고용합니다. 이러한 기업은 일반적으로 직무와 임무에 따라 서로 다른 위험 프로파일을 가진 여러 부서를 지원합니다. 소규모 기업 단위에는 규정 준수 부담이 있을 수 있습니다.

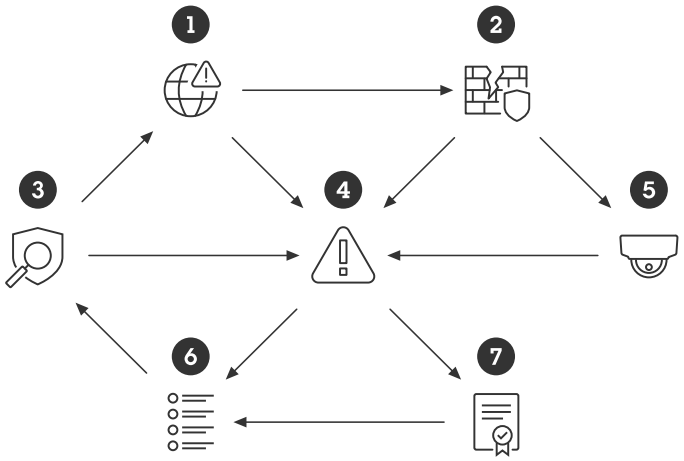
- **SANS 구현 그룹 3(IG3)**

  IG3 기업은 일반적으로 사이버 보안의 다양한 측면(예: 위험 관리, 침투 테스트, 애플리케이션 보안)을 전문으로 하는 보안 전문가를 고용합니다. IG3 자산 및 데이터에는 규제 및 규정 준수 감독의 대상이 되는 민감한 정보 또는 기능이 포함되어 있습니다.

용어

용어

용어 맵은 이 문서에서 논의되는 특정 사이버 보안 핵심 용어의 관계를 보여줍니다.



- **(1) 위협** 악용**(2) 취약점** 노출**(5) 자산** 및 증가**(4) 위험**
- **(4) 위험** 영향 **(7) 방침** 및 나타내기 **(6) 요구 사항**
- **(6) 요건** 에서 다루어진다 **(3) 보안 통제**, 끊임없이 직면하는 **(1) 위협** 완화하는 동안 **(4) 위험**

위험

사이버 보안은 시간이 지남에 따라 위험을 관리하는 것입니다. 위험은 결코 제거할 수 없으며 완화될 뿐입니다. 때때로 사람들은 용어를 혼동합니다. 위험, 자산, 위협, 취약성 또는 부정적인 영향

RFC 4949 Internet Security Glossary에 정의된 사이버 보안 위험은 특정 위협이 특정한 유해 결과로 특정 취약점을 악용할 가능성으로 표현되는 예상 손실입니다.

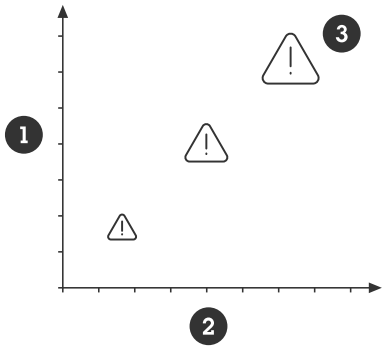
일반적으로 사용되는 단축 버전은 **위험=확률x영향**과 같습니다.

이 공식은 위험의 우선순위를 정하는 데 사용됩니다. RFC 정의에는 위협, 취약성 및 유해한 결과에 대한 '특정'이라는 용어가 포함되어 있습니다. 각 위협은 가장 그럴듯하고 부정적인 영향이 가장 큰 위협부터 시작하여 개별적으로 살펴봐야 합니다.

위험을 논의할 때 어려운 점은 확률 요인입니다. 일이 일어날 수도 있고 일어나지 않을 수도 있습니다. 공격자가 취약점을 악용할 확률은 취약점이 얼마나 쉽게 악용(노출)되는지와 공격자가 이를 악용할 수 있는 잠재적 이점에 따라 결정되는 경우가 많습니다.

다음 두 가지 차원으로 위험을 표시할 수 있습니다. 위험이 발생할 확률을 한 축으로 사용하고 위험이 발생할 경우 위험의 영향을 다른 축으로 사용합니다. 이를 통해 각 위험에 부여해야 하는 잠재적인 영향과 우선순위를 명확하게 볼 수 있습니다.

용어



*1 낮은 확률에서 높은 확률까지의 **확률***
*2 낮은 영향부터 높은 영향까지의 **부정적인 영향***
*3 낮은 수준부터 높은 수준까지의 **위험 수준***

공격가치=공격 혜택–공격비용

보호 기능을 추가하면 공격 비용이 증가하여 확률이 감소합니다. 공격 비용은 공격이 성공하는 데 얼마나 많은 시간, 리소스, 기술 및 정교함이 필요한지와 관련됩니다. 잡힐 위험이나 기타 부정적인 결과도 공격 비용의 일부입니다.

사이버 공간의 위험을 분석하는 프로세스인 위험 평가는 물리적 보호와 동일합니다. 고려해야 할 질문은 다음과 같습니다.

1. 무엇을 보호하고 싶습니까?
2. 누구로부터 그것을 보호하고 싶습니까?
3. 부정적인 영향을 미칠 가능성은 얼마나 됩니까?
4. 실패하면 결과는 얼마나 심각할 것 같습니까?
5. 위험을 완화하려면 어떤 전략을 구현해야 합니까?

모든 유형의 보호 또는 보안 제어 조치를 구현하면 일정 유형의 비용이 발생합니다. 모든 조직에는 제한된 재정 자원이 있습니다. 위험이 무엇인지 모르면 보호를 위한 예산을 추정하기가 어렵습니다. 항상 위험을 감수해야 하지만 그 결정은 의도적인 위험 기반 결정이어야 합니다.

각 자산 유형에 대한 잠재적인 부정적인 영향을 추정하는 것은 어렵고 복잡합니다. 많은 경우 추정치는 주관적이며 영향 분석은 과소평가되는 경우가 많습니다. ISO 27000 영향 모델 및 지정 유형(예: 제한적, 심각한, 극심한 또는 재난적)을 사용하면 우선순위를 지정하는 데 도움이 되는 빠른 오버뷰를 얻을 수 있습니다. 이는 부정적인 영향을 복구하는 데 걸리는 시간을 기준으로 추정하여 보다 정확한 값을 설정하는 간단한 방법을 제공합니다. 즉, 다음과 같습니다.

- **제한된**=몇 시간~며칠
- **심각한**=며칠~몇 주
- **극심한**=몇 주~몇 달
- **재난적**=몇 달~몇 년까지(전체적인 경우)

자산

물리적 보호는 사람과 물리적 개체를 보호하는 데 중점을 두는 반면, 사이버 보안 보호는 데이터 자산과 컴퓨터 리소스를 보호하는 데 중점을 둡니다. 세 가지 주요 영역:

- **기밀성**: 정보 또는 자원 공개
- **무결성**: 정보 또는 자원의 파괴 또는 변경

용어

- **Availability(가용성)**: 정보와 자원에 대한 접근성

이러한 영역을 CIA 트라이어드라고도 합니다. 운영 기술(OT)은 유용성을 우선시하는 반면, 정보 기술(IT) 작업은 보안을 우선시하는 경우가 많습니다. 기밀성, 무결성, 가용성 간의 적절한 균형을 찾는 것이 어려운 경우가 많습니다.

적절한 보호 수준을 결정하려면 자산과 자원을 분류해야 합니다. 부정적인 영향 측면에서 모든 데이터 자산과 컴퓨터 리소스가 동일한 것은 아닙니다. 그들은 종종 다음과 같이 분류됩니다:

- **공개**: 자산이 일반 소비자를 대상으로 합니다. 또는 대중에게 공개되면 부정적인 영향이 제한됩니다.
- **비공개**: 자산이 특정/선택된 그룹에 대한 권한을 갖습니다. 일반적으로 부정적인 영향은 회사나 가족과 같은 특정 조직 내로 제한됩니다.
- **제한된**: 자산은 조직 내에서 선택된 개인에게 특권이 있습니다.

비디오 시스템의 라이브 비디오는 공개로 분류될 수 있으며, 이는 일반 대중과 조직 내 대중을 모두 의미합니다. 그러나 대부분의 경우 실시간 영상은 비공개로 분류됩니다. 즉, 특정 조직 단위에서만 액세스할 수 있습니다. 한편, 녹화된 영상은 매우 민감한 장면이 있을 수 있어 제한된 영상으로 분류되는 경우가 대부분입니다. 자격 증명 및 구성도 제한된 것으로 분류되어야 하는 데이터입니다.

위협

위협은 자산이나 리소스를 손상시키거나 해를 입힐 수 있는 모든 것으로 정의할 수 있습니다. 일반적으로 사람들은 사이버 위협을 악의적인 해커 및 맬웨어와 연관시키는 경향이 있습니다. 실제로 사고, 의도하지 않은 오용 또는 하드웨어 오류로 인해 부정적인 영향이 자주 발생합니다.

공격은 갑자기 발생하지 않습니다. 시스템과 자산을 손상시키려는 동기는 항상 존재합니다. 공격은 기회주의적 공격 또는 표적 공격으로 분류할 수 있습니다. 사이버 보안에서 공격자는 악의적인 의도를 가지고 있을 수 있는 적이라고도 합니다.

오늘날 대부분의 공격은 기회주의적입니다. 기회의 창이 있기 때문에 발생하는 공격. 외부 기회주의적 공격자는 피해자가 누구인지조차 모르는 경우가 많습니다. 이 공격자는 피싱 및 프로빙과 같은 저비용 공격 벡터를 사용합니다. 이러한 경우에는 실패한 공격에 시간과 자원을 소비할 의지가 없습니다. 그들은 빠르게 다음 시도로 이동합니다. 표준 보호 수준을 적용하면 기회주의적 공격과 관련된 대부분의 위험을 완화합니다. 특정 목표를 가지고 특정 시스템을 표적으로 삼는 공격자, 즉 표적 공격으로부터 보호하는 것이 더 어렵습니다. 표적 공격은 기회주의적 공격자와 동일한 저비용 공격 벡터를 사용합니다. 그러나 초기 공격이 실패하면 목표를 달성하기 위해 보다 정교한 방법을 사용하기 위해 보다 단호하고 시간과 리소스를 기꺼이 사용합니다. 그들에게 중요한 것은 얼마나 많은 가치가 걸려 있는지에 관한 것입니다.

일반적인 적(위협 행위자)

- **가까운 친한 사람**: 당신의 사생활을 엿보고 싶어하는 사람들
- **직원들**: 또는 우연히 또는 고의적인 오용으로 인해 시스템에 합법적으로 액세스한 사람
- **장난치는 사람들**: 컴퓨터 시스템을 방해하는 것을 즐거운 도전으로 생각하는 사람들
- **핵티비스트**: 정치적, 이념적 동기로 조직을 공격하려는 사람
- **사이버 범죄자**: 사기나 귀중한 정보 판매를 통해 돈을 버는 데 관심이 있는 사람들
- **산업 경쟁자**: 자신의 회사나 조직을 위해 경제적 이익을 얻는 데 관심이 있는 단체
- **사이버 테러리스트**: 종종 이데올로기적 또는 정치적 이유로 경각심이나 공황을 일으키기 위해 고안된 공격을 수행하는 사람 또는 단체
- **국민 국가**: 경제적, 정치적 마일리지를 획득하거나 중요한 정보 시스템에 피해를 입히기 위해 행동하는 외국 정보 기관 요원
- **개인**: 동기가 위에 나열된 것과 다를 수 있는 특정 개인 또는 그룹이 스스로 행동하는 경우. 이는 조사 기자, 화이트 해커 또는 이와 유사한 사람일 수 있습니다. 결함을 수정하기보다 숨기는 데 우선순위를 둔다면 화이트 햇 해커(일명 윤리적 해커)가 위협이 될 수 있습니다.

용어

취약점

모든 시스템에는 취약점이 있습니다. 취약점은 공격자가 시스템을 공격하거나 시스템에 액세스할 수 있는 기회를 제공합니다. 결함, 노출, 기능 또는 인적 오류로 인해 발생할 수 있습니다. 악의적인 공격자는 알려진 취약점을 악용하려고 할 수 있으며 종종 하나 이상을 결합합니다. 성공적인 위반 사례의 대부분은 인적 오류, 잘못 구성된 시스템 또는 제대로 유지 관리되지 않은 시스템으로 인해 발생합니다. 종종 적절한 정책 부족, 정의되지 않은 책임 및 낮은 조직 인식으로 인해 발생합니다.

소프트웨어 취약점

장치 API(Application Programming Interface) 및 소프트웨어 서비스에는 공격에 악용될 수 있는 결함이나 기능이 있을 수 있습니다. 어떤 공급업체도 제품에 결함이 없다고 보장할 수 없습니다. 결함이 알려진 경우 보안 제어 조치를 보완하여 위험을 완화할 수 있습니다 반면, 공격자가 알려지지 않은 새로운 결함을 발견하면 피해자가 시스템을 보호할 시간이 없기 때문에 제로데이 공격이 성공할 위험이 높아집니다.

Common Vulnerability Scoring System(CVSS)은 소프트웨어 취약성의 심각도를 분류하는 한 가지 방법입니다. 악용이 얼마나 쉬운지, 부정적인 영향이 무엇인지 살펴보는 공식입니다. 점수는 0~10 사이의 값이며 10이 가장 큰 심각도를 나타냅니다. 게시된 CVE(Common Vulnerability and Exposures) 보고서에서 CVSS 번호를 자주 찾을 수 있습니다.

Axis는 CVSS를 소프트웨어/제품에서 식별된 취약성이 얼마나 중요한지 결정하는 측정 방법 중 하나로 사용합니다.

정책

장기적으로 적절한 위험 감소를 달성하려면 명확한 시스템 정책과 프로세스를 정의하는 것이 중요합니다. 권장되는 접근 방식은 ISO 27001, NIST 또는 이와 유사한 것과 같이 잘 정의된 IT 보호 프레임워크에 따라 작업하는 것입니다. 소규모 조직에는 이 작업이 부담스러울 수 있지만, 최소한의 정책 및 프로세스 문서를 작성하기만 해도 아무 것도 하지 않는 것보다 훨씬 도움이 될 것입니다.

보안 제어

보안 제어는 물리적 재산, 정보, 컴퓨터 시스템 또는 그 밖의 자산에 대한 보안 위험을 피하거나 감지하거나 대처하거나 최소화하기 위해 사용되는 보호 수단 또는 대책입니다. 보안 제어를 배포하는 프로세스를 흔히 강화라고 합니다.

보상 보안 통제는 선호하는 보안 통제를 적용하는 것이 불가능하거나 선호하는 통제를 사용할 수 없거나 비용이 너무 많이 드는 경우 사용할 수 있는 대체 안전 장치입니다.

시간이 지나면서 위협, 가치, 취약성 및 노출이 변하므로 보안 제어를 지속적으로 모니터링하고 업데이트해야 합니다. 이를 위해서는 정책과 프로세스를 정의하고 준수해야 합니다.

SANS 연구소는 *CIS 제어 목록*을 발간하였으며 이는 우선순위가 지정된 사이버 방어 모범 사례의 권장 세트입니다. 보안 제어의 다양성을 보여주기 위해 전체 목록은 다음과 같습니다.

- CIS 제어 1번: 엔터프라이즈 자산의 재고 및 제어
- CIS 제어 2번: 소프트웨어 자산의 재고 및 제어
- CIS 제어 3번: 데이터 보호
- CIS 제어 4번: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
- CIS 제어 5번: 계정 관리
- CIS 제어 6번: 접근 제어 관리
- CIS 제어 7번: 지속적인 취약점 관리
- CIS 제어 8번: 감사 로그 관리
- CIS 제어 9번: 이메일 및 웹 브라우저 보호
- CIS 제어 10번: 맬웨어 방어

용어

- CIS 제어 11번: 데이터 복구
- CIS 제어 12번: 네트워크 인프라 관리
- CIS 제어 13번: 네트워크 모니터링 및 방어
- CIS 제어 14번: 보안 인식 및 기술 교육
- CIS 제어 15번: 서비스 제공업체 관리
- CIS 제어 16번: 애플리케이션 소프트웨어 보안
- CIS 제어 17번: 사고 대응 관리
- CIS 제어 18번: 침투 테스트

*AXIS OS Hardening Guide(AXIS OS 강화 가이드)*는 CIS를 기반으로 합니다.

일반적인 위협에 대한 보호 조치

일반적인 위협에 대한 보호 조치

일반적인 위협을 이해하고 대응함으로써 대부분의 위험을 완화할 수 있습니다.

의도적이거나 우발적인 시스템 오용

시스템의 유용성과 보안 사이의 균형은 어렵습니다. 많은 시스템은 보안이 아닌 편의성 측면에서 강화됩니다. 이는 고의적이거나 우발적인 오용의 기회를 제공합니다. 시스템에 합법적으로 액세스할 수 있는 사람은 모든 시스템에 대한 가장 일반적인 위협입니다.

일반적인 위협의 예:

- 개인은 승인되지 않은 서비스(예: 실시간 또는 녹화된 비디오)에 액세스할 수 있습니다.
- 개인은 실수를 합니다.
- 개인은 시스템 성능을 저하시키는 문제를 해결하려고 할 수 있습니다.
- 불만을 품은 개인이 시스템에 고의적으로 피해를 입힐 수 있습니다.
- 개인은 사회 공학에 취약합니다.
- 개인은 도둑질을 합니다.
- 개인은 중요한 구성 요소(출입 카드, 전화, 노트북, 문서 등)를 분실하거나 다른 곳으로 옮길 수 있습니다.
- 사람들의 컴퓨터가 손상되어 의도치 않게 맬웨어로 시스템을 감염시킬 수 있습니다.

일반적으로 권장되는 보호 조치:

- 정의된 사용자 계정 정책 및 프로세스
- 충분한 접근 인증 방식
- 시간 경과에 따른 사용자 계정 및 권한을 관리하는 도구
- 노출을 줄입니다.
- 사이버 인식 교육

Axis가 이 위협에 대응하는 데 도움을 주는 방법:

- *AXIS OS 강화 가이드*는 장치의 일반적인 위협에 대한 일반적인 보안 제어를 설명합니다.
- *AXIS Camera Station 강화 가이드*는 비디오 시스템에 대한 일반적인 보안 제어를 설명합니다.
- *AXIS Device Manager* 및 *AXIS Device Manager Extend*는 일반적인 보안 제어를 관리하도록 지원합니다.

물리적 변조 및 파괴

IT 시스템의 물리적 보호는 사이버 보안 관점에서 매우 중요합니다.

일반적인 위협의 예:

- 물리적으로 노출된 장비는 임의로 조작될 수 있습니다.
- 도난당할 수 있는 물리적으로 노출된 장비
- 물리적으로 노출된 케이블은 연결이 끊기거나 방향이 바뀌거나 절단될 수 있습니다.

일반적으로 권장되는 보호 조치:

- 잠긴 구역에 네트워크 장비(예: 서버 및 스위치) 배치
- 접근하기 어렵게 카메라를 장착하십시오.
- 물리적으로 노출된 경우 보호 케이스를 사용합니다.
- 벽이나 도관의 케이블을 보호합니다.

Axis가 이 위협에 대응하는 데 도움을 주는 방법:

- 승인되지 않은 사용자가 SD 카드를 꺼낼 수 있는 경우 비디오 재생을 방지하기 위해 암호화된 SD 카드
- 카메라 뷰 탬퍼링 감지
- 케이스 열림 감지

알려진 소프트웨어 취약점 악용

모든 소프트웨어 기반 제품에는 악용될 수 있는 취약점이 있습니다. 이는 알려진 것과 알려지지 않은 것으로 분류될 수 있습니다. 알려지지 않은 모든 취약점은 결국 알려지게 됩니다. 그것은 단지 시간 문제일 뿐입니다. 대부분의 취약점은 위험이 낮습니다. 즉, 악용하기가 매우 어렵거나 부정적인 영향이 제한적입니다. 때때로 악용될 수 있고 상당한 부정적인 영향을 초래할 수 있는 취약점이 발견됩니다. MITRE는 다른 사람들이 위험을 완화할 수 있도록 돕기 위해 CVE(Common Vulnerabilities and Exposures)의 대규모 데이터베이스를 호스팅합니다.

일반적으로 권장되는 보호 조치:

- 지속적인 패치 프로세스는 시스템의 알려진 취약점 수를 최소화하는 데 도움이 됩니다.
- 네트워크 노출을 최소화하여 알려진 취약점을 조사하고 악용하기 어렵게 만듭니다.
- 결함을 최소화하고, 패치를 제공하고, 심각한 취약점이 발견되면 공개하는 프로세스를 갖춘 정책 및 프로세스에 따라 작업하는 신뢰할 수 있는 하위 공급업체와 협력하십시오.

Axis가 지원하는 방법:

- *Axis 보안 개발 모델*은 소프트웨어 취약성이 있는 제품을 출시할 위험을 줄이기 위해 Axis가 사용하는 프로세스와 도구를 정의하는 프레임워크입니다.
- *Axis 취약점 관리 정책*은 적절한 조치를 취하기 위해 고객이 알아야 할 취약점을 식별, 해결 및 공개하는 작업이 포함됩니다. 2021년 4월부터 Axis는 Axis 제품에 대한 CVE(Common Vulnerability and Exposures) 번호 부여 기관(CNA)으로 승인되어 당사 프로세스를 MITRE Corporation의 업계 표준 프로세스에 맞게 조정할 수 있습니다. 이는 결과적으로 고객을 더 나은 방식으로 지원하는 데 도움이 됩니다.
- *AXIS OS 강화 가이드*와 같은 *Axis 강화 가이드* 소프트웨어 결함 악용 위험을 줄이기 위해 노출을 줄이고 보상 제어를 추가하는 방법에 대한 권장 사항을 제공합니다.
- LTS(장기 지원) 펌웨어 버전을 사용하면 고객은 타사 영상 관리 시스템과의 비호환성 문제로 인한 위험을 최소화하면서 Axis 장치의 운영 체제에 패치를 적용할 수 있습니다.

공급망 공격

공급망 공격은 공급망에서 덜 안전한 요소를 대상으로 조직을 손상시키려는 사이버 공격입니다. 이는 높은 수준의 시스템 보호로 인해 다른 공격 벡터(예: 사회 공학, 피싱 공격 및 인터페이스 프로빙)가 실패할 때 주로 사용됩니다. 공격은 소프트웨어/펌웨어/제품을 손상시키고 관리자가 이를 시스템에 설치하도록 유인하여 이루어집니다. 시스템 소유자에게 배송하는 동안 제품이 손상될 수 있습니다. 공급망 공격을 성공적으로 수행하려면 기술, 시간 및 리소스가 필요합니다.

일반적으로 권장되는 보호 조치:

- 신뢰할 수 있고 검증된 소스의 소프트웨어만 설치하는 정책을 가지고 있습니다.

일반적인 위협에 대한 보호 조치

- 설치 전에 소프트웨어 체크섬(다이제스트)을 공급업체의 체크섬과 비교하여 소프트웨어 무결성을 확인하십시오.
- 배송 시 패키지나 제품에 훼손 흔적이 있는지 확인하십시오.

Axis가 이 위협에 대응하는 데 도움을 주는 방법:

- Axis 소프트웨어는 체크섬과 함께 게시되므로 관리자는 소프트웨어를 설치하기 전에 소프트웨어의 무결성을 확인할 수 있습니다.
- Axis 장치의 서명된 펌웨어는 설치된 AXIS OS가 Axis에서 만든 정품인지, 장치에 다운로드하여 설치할 모든 새 펌웨어도 Axis에서 서명했는지 확인합니다.
- Axis 장치의 보안 부팅을 사용하면 장치에서 펌웨어에 Axis 서명이 있는지 확인할 수 있습니다. 펌웨어가 인증되지 않았거나 변경된 경우 부팅 프로세스가 중단됩니다.
- IEEE 802.1AR 호환 Axis 장치 ID는 케이스 내부의 하드웨어가 Axis에서 제공되었는지 시스템이 확인할 수 있는 방법을 제공하는 장치 고유의 Axis 공급업체 인증서입니다.
- SD 카드 암호화 및 파일 시스템 암호화는 카드나 장치 도난 시 저장된 데이터의 추출을 방지합니다.

사용자 설명서
Cybersecurity reference guide

Ver. M3.2
날짜: 11월 2023
부품 번호 T10201166