AXIS COMMUNICATIONS CYBERSECURITY MAGAZINE

보호에 함께 하는 파트너

사이버 보안의 세계가 주는
통찰 및 영감

들어가기 >

AXIS COMMUNICATIONS

서론

보호를 위한 강력한 프레임워크

알다시피, 사이버 보안 문제에 대한 단일 해결책은 없으며 어떤 제품에든 내장되는 강력한 사이버 보안 같은 것은 없습니다. 오히려 사이버 보안은 하위 공급업체에서 제조업체까지, 설치업체 및 통합업체에서 최종 사용자까지, 모두가 각자 중요한 역할을 수행하는 신뢰할 수 있는 파트너십의 문제입니다. 사이버 보안은 일회성 결과 달성보다는 지속적인 과정의 문제이기도 합니다.

책임 있는 사이버 보안 파트너가 되는 것의 일환으로, Axis는 이 매거진에 기사, 팁 및 영감을 모아 놓았습니다. 여기에서 소개하는 내용이 최신 정보를 입수하고 자신을 보호하려는 귀사의 노력에 도움이 될 것이라고 생각하며 귀사가 이러한 내용을 유용하게 사용하기를 희망합니다.

그러나 페이지를 넘기기 전에 잠시 시간을 내어 미국 국립 표준 기술 연구소 (National Institute of Standards and Technology: NIST)의 위험 관리 프레임워크에 대해 소개하고자 합니다. 사이버 보안은 본질적으로 위험 관리의 문제이므로, 좋은 출발점은 비즈니스 또는 조직에 대한 잠재적 위험을 위험 관리 프레임워크(많은 프레임워크가 있습니다)를 사용하여 위험의 확률과 잠재적인 해로움의 수준의 관점에서 평가하는 것입니다.

Axis는 사이버 보안 접근 방식을 NIST 프레임워크에 맞추는 것을 선택했습니다. NIST 지침은 전 세계적으로 사용되며 대기업 및 조직뿐만 아니라 중소기업에도 적합합니다. 조직에서 다른 프레임워크를 사용해도, 그것은 NIST 프레임워크와 호환될 수 있습니다.

NIST 프레임워크는 식별, 보호, 감지, 대응, 복구와 같은 5개 요소를 중심으로 하는 접근 방법입니다. Axis 웹사이트에서 각 요소, 귀사의 사이버 보안 파트너로서 Axis의 역할 및 귀사 자신의 역할에 대해 자세히 알아볼 수 있습니다. www.axis.com/ko-kr/cybersecurity.

매거진의 내용을 읽는 시간이 즐거운 시간이 되기를 바랍니다!

목차

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 자원을 식별 및 분류(무엇을 보호할 것인가)
- 발생 가능한 위협을 식별(누구로부터 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.

자산과 자원에 유의하십시오.

비디오 시스템과 관련하여, 보호가 필요한 분명한 자원은 카메라의 비디오 피드입니다. 자산은 영상 관리 시스템(VMS)의 영상 녹화물입니다. 접근은 일반적으로 사용자 권한에 따라 제어됩니다. 고려해야 할 기타 자산은 사용자 계정 및 패스워드, 구성, 운영 체제, 펌웨어 및 소프트웨어, 네트워크 연결형 장치입니다.

상세 정보 >

주의해야 할 위협은 무엇입니까?

사이버 위협으로부터 자신을 보호하기 위한 첫 번째 단계는 직면한 위협이 무엇인지 아는 것입니다. 기밀성, 무결성 및 가용성은 IT 시스템에서 보호해야 하는 핵심 요소로 간주됩니다. 그 중 어느 하나에든 부정적인 영향을 미치는 어떤 것도 사이버 보안 사고입니다. 이제 사이버 보안에 대한 가장 일반적인 위협과 이러한 위협이 악용하는 취약점을 살펴보겠습니다.

상세 정보 >

1

의도하지 않은 인간의 순진함과 오류

네트워크를 보호하기 위해 추가하는 기술이 아무리 뛰어나도, 공격자가 한 사람이라도 이메일의 엉뚱한 링크를 클릭하도록 하면, 공격자가 침투할 수 있게 됩니다. 따라서 사이버 범죄자에게는 이것이 가장 쉽고 선호하는 공격 수단입니다. 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 암호를 사용하지 않거나 암호를 적절하게 보호 및/또는 업데이트하지 못하는 경우를 포함합니다.
- **중요 구성 요소의 잘못된 관리:** 시스템에 액세스하는 것을 허용할 수 있는 항목을 분실하거나 잘못 배치한 경우. 이에 해당하는 예로는 액세스 카드, 전화, 노트북 및 설명서 등이 있습니다.
- **시스템 관리 불량:** 시스템 업데이트 및 보안 패치를 설치하지 않는 경우.
- **개선 실패:** 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. 또한 영상에 대한 액세스를 제한하고 중요한 권한을 VMS를 통해 신뢰할 수 있는 소수의 개인으로 제한해야 합니다.

상세 정보 >

시스템의 고의적인 오용

너무 흔한 또 다른 사이버 위협은 정당한 액세스 권한을 가진 사람들이 영상 시스템을 고의적으로 오용하는 것입니다. 의도적인 오용의 유형은 다음과 같습니다.

2

- 시스템 서비스 및 리소스에 대한 무단 액세스 및 조작
- 데이터 훔치기
- 시스템에 고의적인 해를 끼치기

취약점 및 의도적인 오용

취약점을 관리하고 시스템의 의도적 오용의 위협을 완화하는 데 도움이 되는 정책 및 장기적 프로세스를 시행하는 것이 중요합니다. 민감한 데이터에 대한 액세스를 허용하는 권한을 가진 개인을 적절하게 조사하는 것은 그러한 권한을 가진 개인의 수를 제한하는 것과 마찬가지로 중요합니다. 장치는 관리(어드민) 및 일상 운영 클라이언트(VMS)를 위한 별도의 계정이 있어야 하며 유지관리 및 장애 처리용으로는 임시 계정을 사용해야 합니다. 이 세 계정이 모두 동일한 계정을 공유하는 경우 암호가 조직 내에서 쉽게 알려져 고의적이거나 우발적인 오용의 기회가 만들어질 수 있습니다.

상세 정보 >

3

물리적 변조 또는 방해 행위

IT 시스템에 대한 물리적 보호는 사이버 보안의 관점에서 매우 중요합니다.

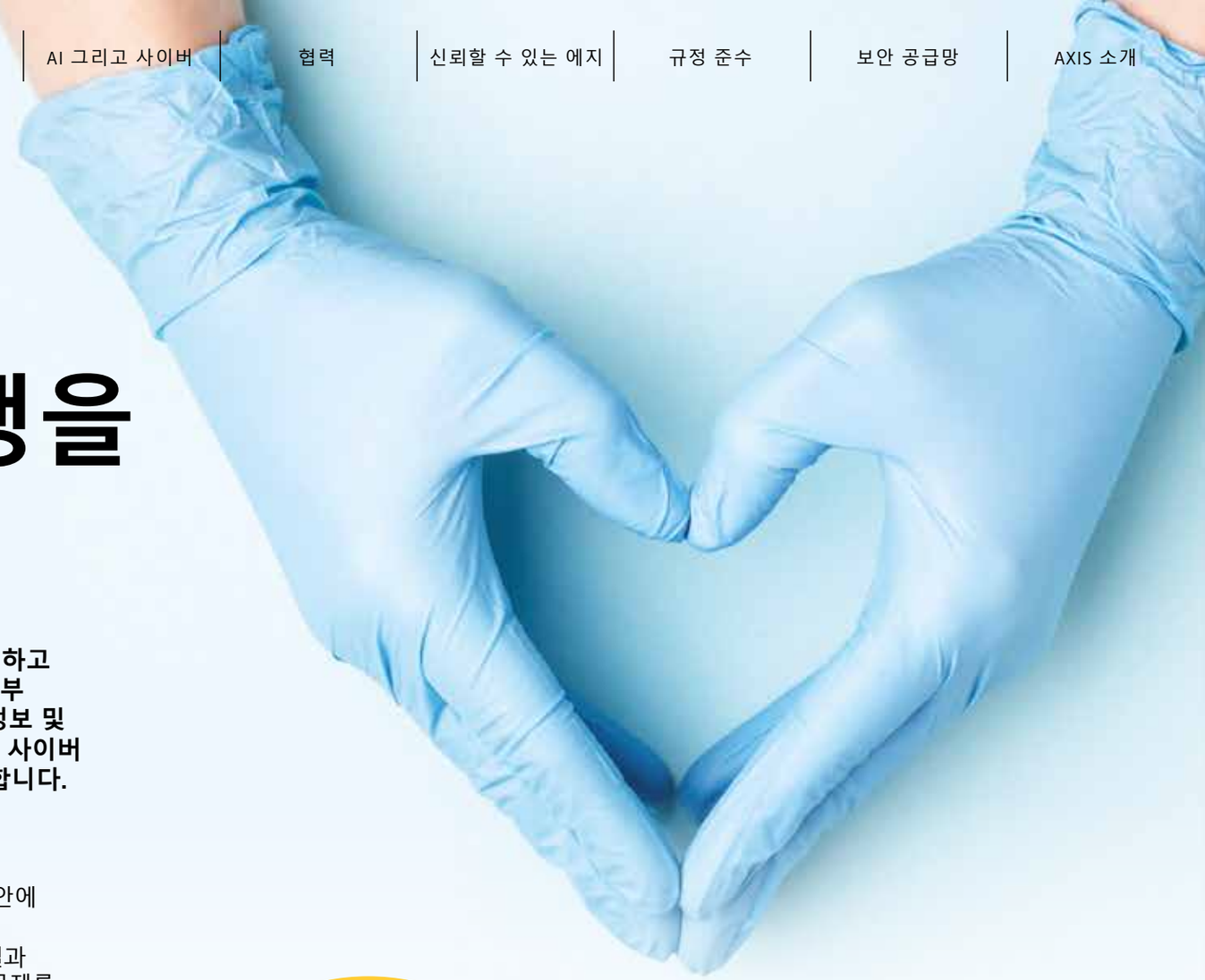
- 물리적으로 노출된 장치는 변조될 수 있습니다.
- 물리적으로 노출된 장치는 도난당할 수 있습니다.
- 물리적으로 노출된 케이블은 분리되거나, 올바르지 않은 장비에 연결되거나, 절단될 수 있습니다.

취약점 및 물리적 위협

카메라 자체가 탬퍼링 행위(부당 조작)에만 취약한 것은 아닙니다. 카메라가 네트워크 케이블을 노출시킬 수도 있습니다. 이는 네트워크에 침입할 기회를 제공할 수 있습니다. 악용될 수 있는 위협이 발생할 기회를 제공할 수 있는 다른 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.

부정적 영향을 인식하십시오.

영상 시스템은 금융 거래를 처리하거나 고객 데이터를 보관하지 않습니다. 즉, 영상 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 저가의 시스템 보호 수단을 구입하면 장기적으로 훨씬 더 많은 비용이 들 수 있습니다.



우수한 사이버 위생을 유지하십시오

우수한 사이버 위생이란 시스템 및 장치 사용자가 시스템 성능 상태를 유지하고 온라인 보안을 개선하기 위해 이용하는 관행과 절차를 의미합니다. 전체 내부 프로세스의 일부인 우수한 사이버 위생은 도난 또는 손상될 수 있는 신원 정보 및 기타 정보의 안전을 보장하는 데 도움이 됩니다. 물리적 위생과 마찬가지로 사이버 위생도 정기적으로 수행하여 자연적인 악화와 일반적인 위협을 제거해야 합니다.

우수한 사이버 위생의 이점

장치 및 소프트웨어에 대한 일상적인 사이버 위생 절차를 수행하면 유지관리 및 보안에 도움이 됩니다.

- 유지관리는 장치와 소프트웨어가 최고의 효율로 실행되도록 합니다. 조각난 파일과 오래된 프로그램은 취약점 발생 위험을 증가시킵니다. 유지관리 절차는 이러한 문제를 조기에 식별하는 데 도움이 되며 심각한 문제 발생을 방지할 수 있습니다. 제대로 유지관리된 시스템은 사이버 보안 위험에 취약하지 않을 수 있습니다.
- 해커와 신원 도용자부터 바이러스 및 지능형 맬웨어에 이르기까지 조직은 끊임없이 위험에 처해 있습니다. 위협을 예측하고 우수한 사이버 위생 관행을 구현함으로써, 조기 감지를 촉진하고 위험이 현실화되는 것을 대비하거나 예방할 수 있습니다.

물리적 위생과 마찬가지로 사이버 위생도 정기적으로 수행되어야 합니다.

상세 정보 >

강력하고 고유한 암호를 사용하십시오.

당연하게 들릴 수 있지만 사이버 범죄자가 시스템에 무단으로 액세스하는 가장 일반적인 방법은 취약한 패스워드 사용을 이용하는 것입니다. 대부분의 IP 기반 장치는 기본 패스워드 및 설정과 함께 제공됩니다. 따라서 IT 또는 회사 정책에 따라 기본 패스워드 및 설정을 즉시 변경하는 것이 중요합니다. 조직은 강력하고 고유한 패스워드(8자 이상)를 사용하여 올바른 패스워드 관리를 보장해야 하고, 주기적으로 변경해야 하며, 사이트 간에 패스워드를 공유해서는 안 됩니다. 패스워드 정책은 컴퓨터 시스템에서 시행할 수 없습니다. 조직은 직원을 교육하고 조직의 패스워드 모범 사례를 직원에게 이해시켜야 합니다. 또한 인증서를 사용하여 패스워드와 사용자 이름을 암호화하는 것이 좋습니다.

단 하나의 일반적인 단어나 이름을 암호로 사용할 경우, 해당 암호는 길이에 관계 없이 몇 초 내에 크래킹될 수 있습니다.

IT 또는 보안 네트워크 정책에 따라 장치를 배치 및 설치하십시오.

장치를 배치할 때 사용하지 않는 서비스를 활성화된 상태로 두면 안 됩니다. 이렇게 하면 사이버 범죄자가 손쉽게 공격하고 악성 애플리케이션을 설치할 수 있습니다. 사용하지 않는 서비스를 비활성화하고 신뢰할 수 있는 애플리케이션만 설치하면 잠재적 공격자가 시스템 취약성을 악용할 가능성이 줄어듭니다. 또한 장치가 적절한 물리적 설치를 따르고 네트워크 포트와 SD 카드 포트가 일반인이 액세스할 수 없도록 하는 것도 중요합니다.

상세 정보 >

명확한 역할 및 소유권을 정의하십시오.

직원이 자신의 책임 영역에 대해 올바른 액세스 권한을 갖도록 하려면 명확한 규칙과 절차를 수립해야 합니다. 조직은 "최소 권한 계정"의 원칙을 따라야 합니다. 즉, 사용자는 작업 수행에 필요한 리소스에만 액세스할 수 있습니다. 기본(디폴트) 계정은 절대로 사용해서는 안 됩니다. 유지관리 목적으로 임시 계정을 사용하는 경우, 작업이 완료되면 임시 계정을 제거해야 합니다.

장치의 기본 설정, 특히 기본 암호에 절대로 의존해서는 안 됩니다. 일반 기기의 기본 관리 계정 ID와 암호는 간단한 Google 검색을 통해 쉽게 찾을 수 있으므로 해커가 쉽게 침투할 수 있습니다. 장치 보호 서비스를 활성화 및 구성하고, 기본 설정을 데모 전용으로 사용하십시오.

61%
의 작업자가 장치에서 개인 작업과 업무 작업을 혼용

80%
의 직원이 업무에서 승인되지 않은 SaaS 애플리케이션을 사용한다고 인정

75%
의 네트워크 침입이 취약하거나 도난당한 자격 증명을 악용

상세 정보 >

적용 가능한 최신 펌웨어를 사용하십시오.

장치가 사용 가능한 최신 펌웨어로 업데이트되었습니까? 시스템 및 장치의 버그 또는 결함은 조직을 공격에 취약하게 만들고 해커가 서버 개인 키 또는 사용자 암호를 훔치도록 할 수 있습니다. 잘 문서화된 소프트웨어/펌웨어 업데이트 관리 계획을 구비하고, 항상 네트워크 장치가 최신 펌웨어 및 보안 업데이트로 업데이트되도록 하는 것이 중요합니다.

위험 분석을 수행하십시오.

조직이 자산 보호에 얼마를 지출해야 할까요? 잠재적인 내부 및 외부 위협과 주요 자산이 손상되거나 소실될 경우의 영향을 분석하여, 자산 보호를 위한 노력의 우선순위를 정할 수 있습니다. 또한 NIST(National Institute of Standards and Technology) 사이버 보안 프레임워크와 같은 위험 관리 프레임워크가 있습니다. 이러한 위험 관리 프레임워크는 위험 관리를 위한 프로세스 및 지침을 제공하는 데 도움이 될 수 있습니다.

기록된 침해 건수는 2019년에 크게 증가했습니다. 드러난 침해 건수는 2018년 대비 3배 이상인

85억건 이상

이었습니다.*

*IBM X-Force Threat Intelligence Index 2020 시스템 보호 및 가능한 위협에 대한 지식 확보

상세 정보 >

귀사의 공급망은 얼마나 안전합니까?

전체 공급망과 긴밀히 협력하면 네트워크 및 연결된 장치 모두에 발생할 수 있는 위협을 더 잘 이해할 수 있습니다. 오늘날 많은 IT 제조업체는 안전한 공급망 문서를 제공할 뿐만 아니라, 네트워크에 연결된 장치의 보안을 강화하기 위한 문서화된 모범 사례 또는 가이드를 제공합니다. 이것이 제공되지 않는 경우, 제조업체와 대화를 시작하거나 다른 사용자 생성 문서를 입수하는 것이 중요합니다. 장치는 개별 장치로서 또한 시스템 전체로서 IT 정책을 준수해야 합니다.

항상 암호화된 연결을 사용하십시오.

어떤 산업군이든 관계 없이, 모든 데이터에는 안전한 암호화가 필요합니다. 암호화된 연결은 모든 네트워크, 심지어 로컬 또는 '내부' 네트워크에서도 사용해야 합니다. 인증 프로토콜은 정보가 네트워크를 통해 전송되기 전에 암호화되도록 보장하고 악성 코드가 암호화되지 않은 전송을 "포착"하는 경우의 공격 가능성을 효과적으로 줄입니다.

보안 프로토콜

- HTTP Digest(액세스) 인증은 웹 서버가 자격 증명 및 사용자 이름 또는 암호와 같은 사용자 신원을 확인하는 데 사용할 수 있는 합의된 방법 중 하나입니다.
- HTTPS(HyperText Transfer Protocol Secure)는 가장 일반적인 데이터 암호화 프로토콜입니다. HTTPS는 전송된 데이터가 SSL(Secure Sockets Layer) 또는 TLS(Transport Layer Security)를 사용하여 추가로 암호화된다는 점을 제외하면 HTTP와 동일합니다.
- SRTP(Secure Real-Time Transport Protocol)는 비디오 자체에 대한 추가 보호를 위해 비디오 스트림을 암호화합니다. 영상의 로컬 저장을 위해 VMS 또는 SD 카드를 사용하는 경우, VMS 또는 SD 카드도 암호화되어 있는지 확인하십시오.

상세 정보 >

잘 유지관리된 시스템은 전체 시스템 성능 상태에 중요합니다.

네트워크 경계를 보호하십시오.

방화벽과 필터를 이해하고 있습니까? 네트워크를 백본으로부터 보호함으로써 사이버 보안 모범 사례를 구현하기 위한 다른 노력을 더 잘 지원할 수 있습니다. 물리적 보안 장치에서 VLAN(가상 근거리 통신망)과 같은 네트워크 분할을 사용하면 민감한 정보의 스누핑 및 개별 서버와 네트워크 장치에 대한 공격의 위험을 줄이는 데 도움이 됩니다. 또한 ACL(Access Control Lists)은 네트워크 상의 악의적인 움직임을 제어하는 데 도움이 될 수 있습니다. 새 장치에 투자하기 전에 공급업체에 네트워크 포트 목록을 요청하여 솔루션이 전체 네트워크에 걸쳐 작동하는지 확인하십시오.

시스템 및 프로세스를 유지관리하십시오.

잘 유지관리된 시스템은 전체 시스템 성능 상태에 중요합니다. 무단 액세스 시도를 감지하려면 장치 및 시스템 로그를 주기적으로 모니터링해야 합니다. 오늘날과 같이 빠르게 변화하는 기술 세계에서는 새로운 업데이트, 기능 및 모범 사례가 항상 생성되므로, 유지관리 절차를 문서화하여 누구나 프로세스를 이해할 수 있도록 해야 합니다.

AXIS Device Manager와 같은 장치 관리 소프트웨어를 사용하면 조직이 네트워크에 연결된 모든 장치 및 소프트웨어의 전체 실시간 인벤토리를 신속하게 수집하는 데 도움이 될 수 있습니다. 장치 관리 소프트웨어는 전체 네트워크를 검사하고 모델 번호, IP 및 MAC 주소, 펌웨어 버전 및 인증서 상태를 포함한 모든 주요 정보를 수집합니다.

효과적인 수명주기 관리를 구현하는 것이 중요한 이유

사람들이 하는 말처럼, 네트워크는 네트워크에 연결된 장치 만큼만 안전합니다. 또한 조직은 네트워크를 보호하기 위해 계층화된 보호 방법을 구현하는 데 적극적인 동시에 물리적 자산의 수명주기를 효과적으로 관리할 수 있는 방법도 필요합니다. 그러나 조직에서는 새 펌웨어를 즉시 사용할 수 있는 경우에도 소프트웨어 업데이트를 무시하는 경우가 많습니다. 이는 일반적으로 네트워크의 모든 기술에 대한 전체적인 파악이 부족하기 때문입니다.

하나의 장치 – 두 가지 수명

소프트웨어 기반 장치와 관련된 두 가지 유형의 수명주기가 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 수명주기 - 장치가 새롭고 더 효율적인 기술을 채택하는 비용보다 유지관리 비용이 더 많이 들기 시작할 때까지 얼마나 오래 걸립니까? IP 카메라는 15년 동안 기능할 수도 있지만, 사이버 보안 환경의 급격한 변화로 인해 IP 카메라의 실제 수명이 더 짧을 것이기 때문입니다.

자산을 사전 대응 방식으로 관리하십시오.

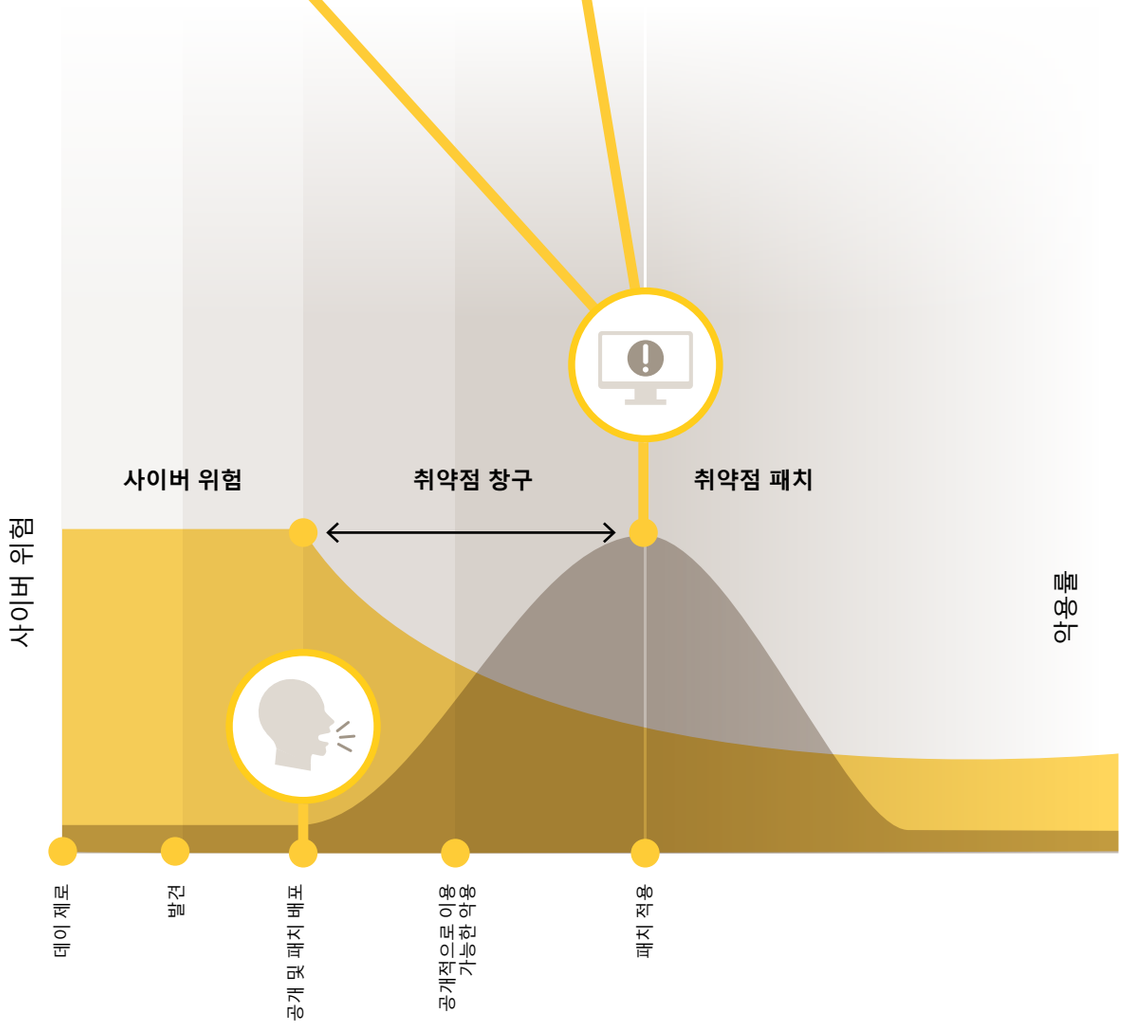
수명주기 관리는 물리적 자산의 기능적 및 경제적 수명주기를 효과적으로 관리하는 것입니다. 조직은 네트워크에 배포된 모든 기술을 명확히 파악하여 네트워크와 중요 데이터를 면밀히 주시하고 위협과 취약점으로부터 안전하게 보호해야 합니다.

영국 정보위원회(Information Commissioner's Office: ICO)에 따르면

"침입의 60%는 이용 가능한 패치가 있지만 이를 적용하지 않아 생긴 취약점과 관련되어 있습니다."

상세 정보 >

희망은 계획이 아닙니다.



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

업데이트 및 패치는 사이버 보안을 개선하는 가장 좋은 방법이지만 이전 기술에 항상 사용할 수 있는 것은 아닙니다. 이는 제조업체에서 더 이상 지원하지 않을 수 있기 때문입니다. 그리고 사이버 보안의 관점에서 보면, 패치가 적용되지 않은 더 오래된 기술이 가장 큰 위험을 초래합니다. 조직이 진행 중인 위협을 파악하고 항상 최신 사이버 보안 모범 사례를 따르도록 하는 것이 중요합니다. 간과된 장치는 쉽게 공격자의 진입 지점이 될 수 있습니다.

위협에 뒤떨어지지 않아야 합니다.

효과적인 수명주기 관리는 조직이 비즈니스의 보안을 유지하는 데 도움이 됩니다. 그리고 미래를 더 잘 준비하는 데 도움이 됩니다. 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 결과가 끔찍할 수 있기 때문입니다.

물리적 장치도 업데이트가 필요합니다.

제조업체는 취약점을 해결하고 버그를 수정하며 기타 성능 문제를 해결하는 펌웨어 업데이트 및 보안 패치를 정기적으로 배포하여 안정적이고 안전한 시스템을 유지하는 데 도움이 되도록 합니다. 조직은 운영 체제 및 애플리케이션 패치의 중요성을 이해하고 있지만 하드웨어가 실행되는 펌웨어를 업데이트하지 못하는 경우가 많습니다. 이로 인해 이러한 장치는 사이버 공격에 취약해지며 귀중한 고객 데이터의 소실에서 규정 위반에 대한 규제 기관의 거액의 벌금에 이르기까지 모든 결과를 초래할 수 있습니다.

상세 정보 >

간소화된 수명주기 관리

구조화된 수명주기 관리 프로그램은 조직이 미래를 적절히 계획하는 데 도움이 됩니다. 또한, 보안 위협 및 취약성을 최소화하기 위해 가장 적절한 고급 기술을 사용합니다. AXIS Device Manager와 같은 장치 관리 소프트웨어는 조직이 이러한 작업을 자동화하여 자산을 효과적으로 관리할 수 있도록 할 수 있습니다.

작동 방식?

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 검사할 수 있고, 새 장치 또는 업데이트된 장치가 발견되면 모델 번호, IP 및 MAC 주소, 펌웨어 버전 및 인증서 상태를 포함한 모든 주요 정보를 수집합니다.

전체 파악

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

시간과 노력을 절약하십시오.

장치 관리 소프트웨어는 조직이 사이버 보안 위험을 관리할 때 많은 시간과 스트레스를 줄이는 데 도움이 됩니다. 이러한 유형의 소프트웨어를 사용하면 다음을 수행하여 시스템을 유지관리할 수 있습니다.

- 시스템 변경, 펌웨어 업데이트 및 새 인증서를 모든 해당 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 펌웨어 버전을 실행하고 있는지 확인합니다.
- 네트워크에 걸쳐 사용자 권한 수준을 관리하고 수정 사항을 구성합니다.

상세 정보 >

실시간 통찰력을 확보하십시오.

장치 관리 도구는 조직의 생태계 상태에 대한 실시간 통찰을 조직에 제공합니다. 예를 들어, 어떤 장치가 최신 패치, 펌웨어 업데이트 및 인증서로 업데이트된 상태인지 알 수 있습니다. 또한 제조업체에서 더 이상 지원하지 않는 경우 장치가 제거 대상으로 지정되었는지 알 수 있습니다. 이 귀중한 정보는 맬웨어가 장치를 잠재적으로 감염시킬 수 있는지 확인하는 데 도움이 될 수 있습니다. 다량의 다른 취약성 문제가 네트워크를 손상시키기 전에 해당 취약성 문제를 해결하는 데 필요한 모든 정보에 액세스 할 수 있습니다.

사전 예방적 생태계 보안

장치 관리 프로세스를 자동화하면 위협과 취약점으로부터 네트워크를 보호하는 데 도움이 됩니다. 그러나 조직은 의미 있는 사이버 보안 정책과 모범 사례를 따라야 합니다. 예를 들어 조직에 패스워드 안전성에 대한 정책이 있습니까? 사용자가 암호를 얼마나 자주 변경해야 합니까? 잠재적인 공격에 대한 노출 영역을 줄이기 위해 사용하지 않는 서비스를 비활성화하는 것이 모범 사례입니까? 장치가 취약점을 얼마나 자주 검사합니까? 제조업체가 알려진 공격을 게시할 때 위험 수준에 액세스하기 위한 절차가 마련되어 있습니까? 이런 것들이 네트워크 생태계를 사전 예방적으로 보호하기 위한 조치를 식별하고 구현할 수 있도록 하기 위한 몇 가지 질문입니다.

자동화된 수명 주기의 5가지 이점

1. 자사 환경의 핵심 기술에 집중
2. 기술의 수명이 종료될 시기를 미리 파악
3. 주요 시스템 구성 요소를 갑자기 교체할 필요를 제거
4. 장치 교체를 위한 적절한 계획을 수립
5. 매년 예측 가능한 장치 비율에 대한 예산을 수립

제로 트러스트 네트워크란 무엇입니까?

네트워크는 점점 더 취약해지고 있습니다. 네트워크는 점점 더 정교해지고 점점 더 증가하는 사이버 공격 및 연결된 장치의 기하급수적 성장으로 위협을 받고 있습니다. 연결된 장치 각각은 공격에 개방된 또 다른 네트워크 엔드포인트를 생성합니다. 그 결과 "제로 트러스트"라는 개념 그리고 이와 더불어 제로 트러스트 네트워크 및 아키텍처가 등장했습니다. Axis를 포함한 하드웨어 제조업체의 경우 제로 트러스트 미래를 준비하는 것이 필수적입니다. 제로 트러스트 미래는 우리가 생각하는 것보다 더 빨리 올 것입니다.

네트워크에서 누구도 그리고 아무것도 신뢰하지 마십시오.

명칭에서 알 수 있듯이 제로 트러스트 네트워크 내의 기본 입장은 네트워크에 연결하는 엔터티 및 네트워크 내의 엔터티 - 겉보기에 인간이든 시스템이든 - 를 신뢰할 수 없다는 것입니다. 이것은 엔터티가 어디에 있든 어떻게 연결되어 있든 상관 없습니다. 오히려 제로 트러스트 네트워크의 최우선 철학은 "절대로 신뢰하지 말고 항상 확인하라"입니다.

필요한 최소한의 액세스를 고수하십시오.

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

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

상세 정보 >

방화벽 만으로 충분하지 않은 3가지 이유

역사적으로 조직은 회사 방화벽이 최대한 견고해지도록 하는 데 의존해 왔지만 이러한 접근 방식은 여러 가지 이유로 점점 더 문제가 되고 있습니다.

1 손상 가능성이 높습니다.

방화벽에 의존하는 것은 네트워크 액세스에 대한 보안을 보장하는 것처럼 보이지만, 방화벽을 침입할 수 있는 사람이라면 누구나 네트워크 내에서 대단히 자유롭게 이동할 수 있습니다.

2 방화벽으로는 더 이상 충분하지 않습니다.

네트워크에 연결된 장치 수가 너무 많기 때문에 단일 솔루션으로 네트워크 경계를 보호하는 것이 더 이상 불가능합니다.

3 더 "투과성 있는" 네트워크는 이점을 제공합니다.

네트워크를 넘어서 클라우드 기반 서비스의 사용과 원활하게 연결된 고객 및 공급업체의 시스템의 이점은 네트워크 보안의 본질을 변화시켰습니다.

> **"일단 네트워크 내부에 있으면, 잠재적으로 복구 불가능한 피해를 유발하는 데이터 소실이 실제로 발생할 위험이 있습니다. 악의적인 행위자가 적발되기 전까지 (적발된다 하더라도) 몇 주 또는 몇 달 동안 활발하게 돌아다니면서요.**
>
> Wayne Dorris, Axis Communications 지역 아키텍처 및 엔지니어링 매니저

상세 정보 >

제로 트러스트의 작동 원리

제로 트러스트는 세분화된 네트워크 경계 보안 및 네트워크 마이크로 세분화와 같은 기술을 사용합니다. 전자는 사용자와 장치를 기반으로 합니다. 사용자 및 장치의 물리적 위치와 기타 식별 데이터를 사용해 해당 자격 증명의 신뢰성을 판정하고 네트워크 접근 허용 여부를 결정합니다. 후자는 더 중요한 데이터가 있는 네트워크의 특정 부분에 다양한 수준의 보안을 적용하는 것을 포함합니다.

추가적 보안 계층

개인에게 자신의 역할을 수행하는 데 필요한 네트워크 부분 및 데이터에만 액세스할 수 있는 권한을 부여하는 것은 보안의 측면에서 분명한 이점을 제공합니다. 그러나 이러한 ID와 관련된 비정상적인 동작을 표시하면 보안 수준이 더 높아집니다. 예를 들어, 네트워크 관리자는 R&D 또는 재무 서버의 유지관리를 위해 광범위한 네트워크 액세스 권한을 가질 수 있습니다.

보안 위험 신호

동일한 네트워크 관리자의 자격 증명이 한밤중에 특정 중요 파일이나 데이터를 다운로드하여 네트워크 외부로 전송하는 데 사용된 경우 보안 위험 신호가 됩니다. 제로 트러스트 네트워크에서는 추가 인증을 사용할 수 있거나, 비정상적인 활동을 실시간으로 표시하고 조사를 위해 보안 운영 센터의 주의를 끌 수 있습니다.

비정상적인 동작은 보안 자격 증명을 도난당했거나 불만을 품은 직원 또는 기업 스파이 활동을 통해 이득을 얻으려는 사람을 가리킬 수 있습니다.

상세 정보 >

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 요청과 해당 컨텍스트를 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

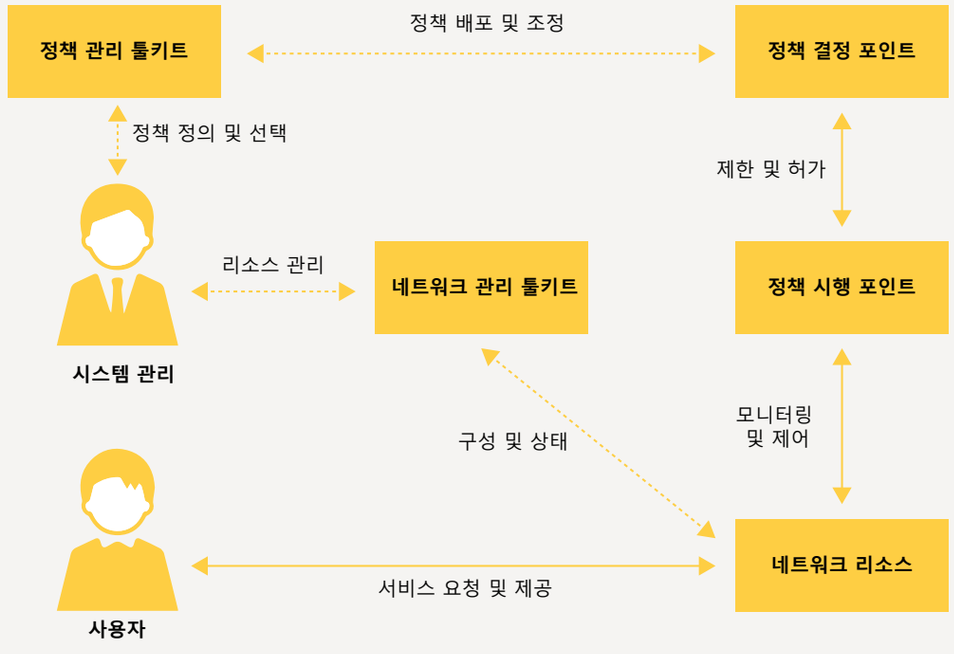
정책 엔진이 작동하려면 조직은 차세대 방화벽(NGFW), 이메일 및 클라우드 보안 게이트웨이, 데이터 소실 방지(DLP) 소프트웨어와 같은 주요 보안 관리 수단 내에서 규칙과 정책을 신중하게 정의해야 합니다. 이러한 통제 수단은 함께 결합되어 호스팅 모델 및 위치를 넘어 네트워크 마이크로 세분화를 시행합니다.

데이터 및 네트워크 리소스에 어떻게 액세스할 수 있습니까?

정책 엔진을 사용하면 다음을 수행할 수 있습니다.

- 규칙 생성
- 규칙 모니터링
- 규칙 시행

정책 엔진 – 개요



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.

상세 정보 >

제로 트러스트 네트워크와 영상 감시

물론 네트워크에 연결하는 엔터티에는 사람이 포함되지만 오늘날 가장 많은 네트워크 연결은 장치에서 발생합니다. 여기에는 네트워크 감시 카메라 및 관련 네트워크 연결 장치가 포함됩니다. 조직이 제로 트러스트 네트워크 아키텍처로 이동함에 따라 네트워크 장치는 "절대로 신뢰하지 말고 항상 확인하라"는 원칙을 준수해야 합니다.

정말 아이러니합니다!

조직을 물리적으로 안전하게 유지하도록 고안된 감시 카메라가 사이버 보안 취약점을 유발한다면 아이러니하지 않겠습니까? 다시 말하지만, 전통적인 형태의 장치 보안으로는 더 이상 충분하지 않습니다. 악의적인 사용자는 직원의 액세스 자격 증명을 훔칠 수 있는 방식과 동일한 방식으로 장치의 보안 인증서도 손상시킬 수 있습니다. 제로 트러스트 네트워크에서는 장치가 네트워크에 대한 신뢰성을 입증하기 위한 새로운 접근 방식이 필요합니다.

다소 놀라운 해결책

연결된 하드웨어 장치에 불변의 신뢰점을 제공할 수 있는 기술 중 하나는 블록체인 기술입니다. 많은 사람들에게 블록체인은 패스워드 화폐와 관련되어 있어서 블록체인의 평판이 약간 나빠졌습니다. 그러나 그 자체로 블록체인은 두 당사자 간의 거래를 효율적이고 검증 가능하고 영구적인 방식으로 기록할 수 있는 개방형 분산 원장입니다. 조직은 하드웨어 신뢰점을 사용하기 위해 사적 블록체인을 사용할 수 있고 이를 통해 장치 내에 불변의 신뢰 키를 마련할 수 있습니다.

예측에 따르면
2025년에 IoT 장치가

750
억 개
를 넘을 것입니다.

블록체인 기술이 효과가 있는 이유

블록체인의 구성으로 인해, 체인의 데이터 트랜잭션은 모두 암호로 연결된 모든 선행 트랜잭션의 합의 노드로부터 동의 없이 변경될 수 없습니다. 따라서 하드웨어 장치의 식별 가능한 부분에 대한 신뢰 키가 블록체인에 내장되어 있으면 장치 자체에 대한 불변의 자격 증명이 생성됩니다.

사이버 공간에서 AI 군비 경쟁이 진행 중입니다.

기술이 발전하면 악의적인 행위자가 자신의 범죄 목표를 지원할 수 있는 가능성을 빠르게 조사하게 될 것입니다. 사이버 범죄자가 랜섬웨어 공격 또는 금융 정보 도용을 계획할 때 - 또는 국가가 적의 핵심 인프라를 파괴하려고 할 때(더 나쁘게는 아니더라도) - 새로운 기술은 그들의 잠재적인 무기가 될 수 있습니다.

이러한 조직은 여느 합법적인 비즈니스와 마찬가지로 많은 자금을 지원 받습니다. 이러한 조직은 인공 지능(AI), 머신 러닝(ML), 딥 러닝(DL)과 같은 새로운 기술의 사용을 혁신할 수 있습니다. 또한 국가 또는 국제 규정이나 법률, 도덕 또는 윤리 규범에 구애받지 않습니다.

그들은 단지 이러한 기술이 범죄 목표를 달성할 수 있는 기회를 제공하는지를 살펴 볼 것입니다.

AI를 포함하는 새로운 기술은 항상 범죄자들의 손에 들어가게 됩니다. **다행히도, 신기술은 표적이 되는 조직에서 방어 수단으로 사용할 수도 있습니다.**

상세 정보 >

눈에 잘 띄지 않는 곳에 숨어 있습니다

점점 더 많은 네트워크 침입자가 인공 지능을 사용하여 공격의 정교함을 개선하고 있습니다. 대규모 DDoS(Distributed Denial of Service) 공격이 종종 헤드라인을 장식합니다. 유명 웹사이트와 온라인 서비스를 비활성화하기 때문입니다. 이러한 공격이 어떻게 가능할까요?

대부분의 사이버 범죄자들의 주요 목표는 최대한 오랫동안 탐지되지 않은 상태를 유지하는 것입니다. 그들은 본질적으로 집 강도처럼 행동합니다. 방에서 방으로 이동하면서 카메라와 경보를 조심스럽게 작동 중지시키고 귀중품을 찾은 다음, 들어올 때와 마찬가지로 은밀하게 떠납니다. 동일한 방식으로, 사이버 범죄자들은 탐지되지 않고 네트워크에 침투하여 네트워크 내부에서 돌아다닌 후 빠져나가려고 합니다.

1

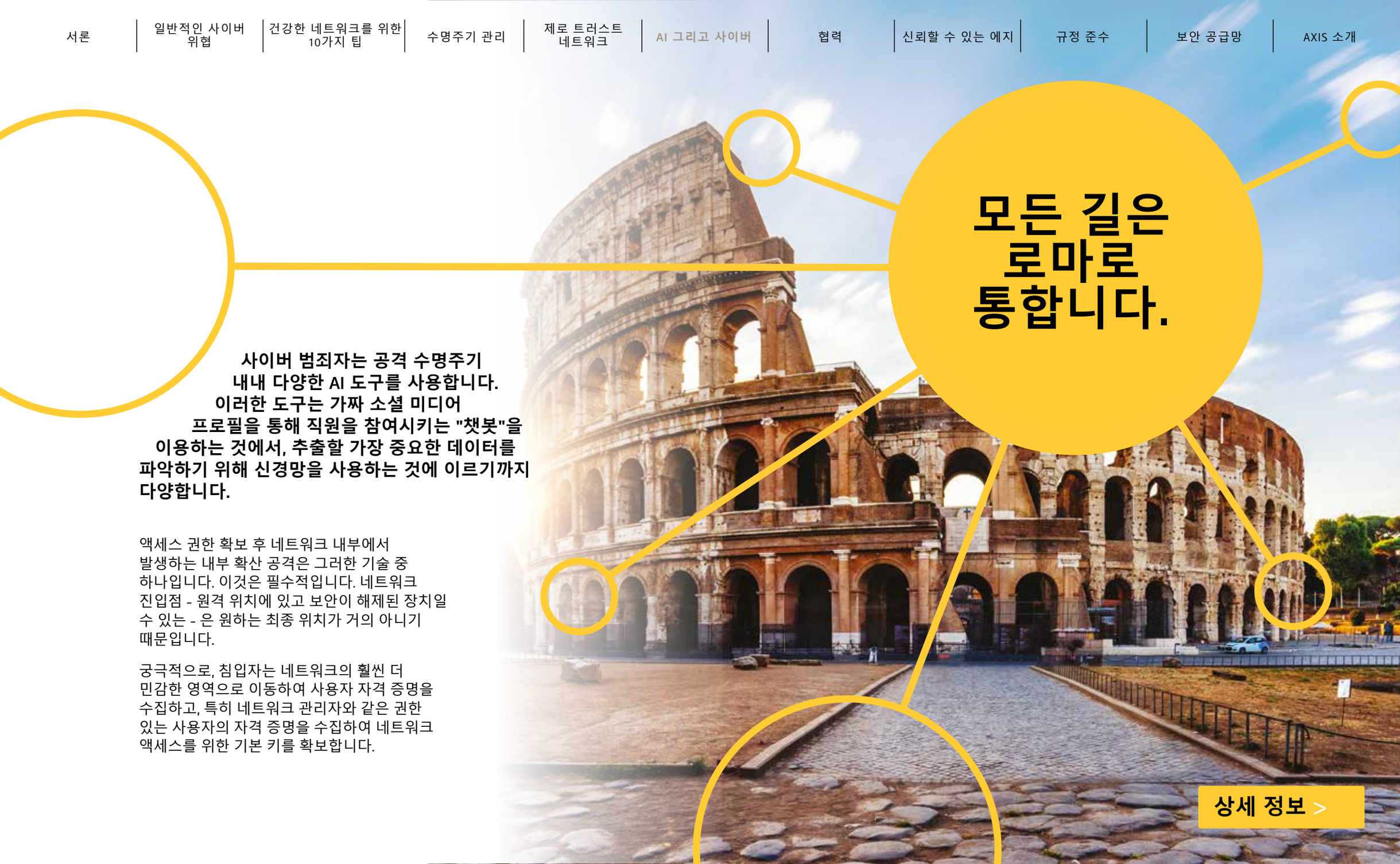
이를 위한 한 가지 방법은 사람이든 장치이든 최대한 네트워크의 합법적 사용자처럼 보이는 것입니다. 그리고 이것이 AI와 ML이 귀중한 새로운 무기가 되는 지점입니다. 이를 통해 사이버 범죄자는 사람과 장치의 네트워크 동작을 학습하고 새로운 맬웨어 및 피싱 전략을 신속하게 개발하고 이를 대규모로 배포할 수 있습니다.

2

그러나 네트워크에 액세스하는 가장 간단한 방법은 여전히 합법적인 사용자가 링크를 클릭하고 문을 열게 만드는 것입니다. 그리고 상사의 가짜 이메일 - 진짜 이메일과 거의 구분할 수 없는 어조와 어투로 되어 있는 - 이 종종 가장 효과적인 열쇠가 될 수 있습니다.

인공 지능(AI)은 컴퓨터가 작업 결과를 저장하고 분석할 수 있도록 하는 일련의 알고리즘입니다. 따라서 다음에 유사한 요청이 발생할 때 그에 따라 해당 작업을 조정할 수 있습니다. 수백 또는 수천 개의 그러한 요청이 이루어지는 동안, AI는 자체 응답 및 조치를 점진적으로 최적화합니다.

상세 정보 >



모든 길은 로마로 통합니다.

사이버 범죄자는 공격 수명주기 내내 다양한 AI 도구를 사용합니다. 이러한 도구는 가짜 소셜 미디어 프로필을 통해 직원을 참여시키는 "챗봇"을 이용하는 것에서, 추출할 가장 중요한 데이터를 파악하기 위해 신경망을 사용하는 것에 이르기까지 다양합니다.

액세스 권한 확보 후 네트워크 내부에서 발생하는 내부 확산 공격은 그러한 기술 중 하나입니다. 이것은 필수적입니다. 네트워크 진입점 - 원격 위치에 있고 보안이 해제된 장치일 수 있는 - 은 원하는 최종 위치가 거의 아니기 때문입니다.

궁극적으로, 침입자는 네트워크의 훨씬 더 민감한 영역으로 이동하여 사용자 자격 증명을 수집하고, 특히 네트워크 관리자와 같은 권한 있는 사용자의 자격 증명을 수집하여 네트워크 액세스를 위한 기본 키를 확보합니다.

상세 정보 >

IT와 OT 사이의 위험한 연결 고리

연결된 장치와 소위 사물 인터넷(IoT)이 전 세계에서 폭발적으로 증가함에 따라 위험이 빠르게 증가합니다. IT(정보 기술) 네트워크가 OT(운영 기술) 환경과 더욱 긴밀하게 통합되기 때문입니다.

간단히 말해서 IT 네트워크는 디지털 정보의 흐름을 관리합니다. 이와는 대조적으로, OT는 비즈니스 또는 특정 위치의 물리적 프로세스, 기계 및 물리적 자산의 운영을 관리합니다. 도난보다는 혼란과 파괴를 목표로 하는 악의적인 행위자들에게는 OT 액세스가 필수적입니다. 발전소, 정유 공장 또는 병원 내의 기계에 대한 접근을 통해 발생할 수 있는 잠재적인 피해를 이해하는 데는 전혀 상상이 필요하지 않습니다.

상세 정보 >

조사하기

사이버 범죄자들이 AI를 사용할 가능성이 있다는 사실은 상당히 오싹한 일입니다. 그러나 네트워크의 침투를 보호하려는 사람들도 AI를 사용할 수 있습니다. 그리고 많은 면에서 방어자가 공격자 대비 우위를 갖습니다.

많은 면에서 방어자가 공격자 대비 우위를 갖습니다.

DARKTRACE

Darktrace는 사이버 보안 분야에서 AI에 중점을 두는 선도적인 글로벌 기업 중 하나로 인정 받고 있습니다. 예상하듯이, Darktrace는 범죄 조직에서 AI 사용이 증가하는 것을 이해하는 데 전문성을 갖고 있습니다. Darktrace는 범죄자보다 한발 앞서기 위해 AI와 ML을 지속적으로 혁신하고 있습니다.

상세 정보 >

AI - 공격 뿐만 아니라 방어를 위한 도구

다음 몇 페이지에 걸쳐 Darktrace의 수석 부사장인 Jeff Cornelius와 이야기를 나누면서 그의 회사가 어떻게 AI와 ML을 사용하여 사이버 범죄자보다 앞서 나가는지 자세히 알아봅니다.

Darktrace의 Jeff Cornelius와의 인터뷰

상황이 얼마나 나쁩니까?

"무엇보다도, 인공지능과 머신러닝을 개발하는 것은, 미디어를 통해 접할 수 있는 느낌과는 다르게 쉬운 일이 아닙니다! 그리고 우리는 사이버 공격을 계속하려는 범죄 조직과 국가에 강력한 적을 가지고 있지만 우리에게 유리한 여러 측면이 있습니다.

"가장 중요한 것은, 고객이 우리에게 제공하는 액세스 권한을 고려할 때, 우리는 모든 기기와 사용자의 행동을 이해하는 데 필요한 전체 네트워크 활동을 볼 수 있다는 것입니다. 반대로, 악당들은 활동의 제한된 부분만 볼 수 있습니다. 그들이 처음 발을 디딜 때 취하는 모든 행동은 얼마간은 이러한 짐작에 의존한 것입니다. 그들과 달리 우리는 환경을 전부 이해하고 있구요.

"궁극적으로 이들의 목표에는 회사/조직이 일반적으로 수행하지 않는 활동들이 포함됩니다. 우리의 주요 목표는 이러한 네트워크 동작의 이상 징후를 식별하고 해결하는 것입니다. 이는 적이 언제 어디서 나타날지, 어떤 새로운 방법을 사용할지, 목표가 무엇인지 알 수 없기 때문에, 그 범위는 매우 광범위합니다."

상세 정보 >

흥미로운 비유

Darktrace의 Jeff Cornelius와의 인터뷰

?

명확히 설명해 주시겠습니까?

"비유를 들자면, 제가 집 밖에서 하는 매일의 움직임을 연구했던 사람은 제 습관에 대한 상당히 상세한 것들을 파악할 수 있을 것입니다. 제가 보통 매일 집을 나가는 시간, 출근하는 경로, 점심 식사하는 장소 같은 것들 말입니다. 아마도 그들은 제 삶의 그런 부분들을 제대로 흉내낼 수 있을 것입니다.

"그러나 그들이 집 안을 보지 않은 채로, 내 아침 식사 취향을 모방하려고 한다면, 가까운 가족 구성원이 이상하다고 쉽게 알아차릴 수 있는 실수를 저지를 것이 거의 확실합니다. 일반적으로 인터넷에는 영리한 스피어 피싱 이메일로 개인을 표적으로 삼을 수 있는 괜찮은 정보가 있지만, 일단 내부에 들어오면 사이버 범죄자는 우리 식탁에 앉아 있게 됩니다."

상세 정보 >

감독된 머신 러닝...

Darktrace의 Jeff Cornelius와의 인터뷰

?

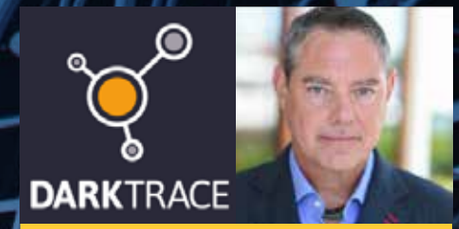
머신 러닝에 대해 자세히 알려주십시오.

"감독된 머신러닝 (ML)과 감독되지 않은 머신러닝(ML) 사이에는 중요한 차이가 있습니다. 전자에서는 컴퓨터가 일련의 알려진 데이터에 대해 훈련되고, 컴퓨터는 기록된 결과가 예상된 결과인지 확인하기 위해 이러한 데이터를 지속적으로 다시 참조합니다.

"사이버 보안의 관점에서, 학습 모델은 알려진 맬웨어에 기반해 있습니다. 범죄자와 사이버 보안 사이의 진정한 경쟁은 바로 여기에서 이루어집니다. 악의적인 행위자는 ML을 사용하여 새로운 버전의 맬웨어를 만들고 있습니다. 그리고 맬웨어는 기하급수적으로 증가하고 있습니다. 그리고 사이버 보안 회사는 감독된 ML 방어를 위한 새로운 모델을 작성하여 맬웨어의 증가 속도를 따라잡기 위해서 노력하고 있습니다. 그것은 새로운 단어와 심지어 언어가 매일 만들어지는 세상을 따라잡으려 노력하는 맞춤법 검사기와 비슷합니다. 그리고 따라잡는 것이 불가능하지는 않더라도 점점 더 어려워지고 있습니다.

상세 정보 >

...vs. 감독되지 않은 머신 러닝'



Darktrace의 Jeff Cornelius와의 인터뷰

?

그러나 다른 방법이 있습니까?

"예. 이와는 대조적으로, 감독되지 않은 ML 알고리즘은 과거의 위협에 대한 지식에 의존하는 대신 독립적으로 데이터를 분류하고 주목해야 하는 패턴을 감지합니다. 네트워크 데이터를 대규모로 분석하고 파악한 증거에만 기반하여 수십억 개의 확률 기반 계산을 합니다. 이를 통해 특정 네트워크에 걸쳐 장치, 사용자 또는 어느 한 엔터티의 그룹과 관련된 '정상적인' 동작에 대한 이해를 형성합니다. 그런 다음 진화하는 위협을 가리킬 수 있는 이러한 진화하는 '삶의 패턴'에서 벗어난 것을 감지할 수 있습니다. 이 조기 경고 시스템을 통해 우리는 사이버 범죄자와 악의적 행위자보다 한발 앞서 나갈 수 있습니다."

힘을 합쳐 사이버 보안 위협을 완화

회사, 조직, 중요 인프라 및 도시를 보호하는 것은 혼자서 할 수 있는 일이 아닙니다. 사이버 보안에 대한 특효약이나 단일 해결책은 없습니다. 오히려 수용 가능한 수준의 사이버 보안을 성공적으로 유지하는 것은 분명히 최종 사용자를 포함하여 다수의 헌신적인 이해 관계자들 간의 협력 노력입니다.

사이버 보안을 위한 문화 구축

여기에서도 모두 힘을 합치는 것과 관련되어 있습니다. 조직의 모든 개인을 사이버 보안 팀의 구성원으로 보아야 합니다. 고려사항:

- 직원 사이버 보안 교육에 투자
- 신입 직원 입사 시 교육
- 고위 관리자가 사이버 보안 정책을 시행하도록 장려
- 사이버 위협이 출현함에 따라 지속적으로 사이버 위협에 대한 학습 및 커뮤니케이션
- 새 네트워크 장비를 선택할 때 사이버 보안을 요구사항으로 검토
- BYOD(Bring-Your-Own-Device) 정책 실행
- 보안 사고 대응 전략의 생성 및 적용

전체 조직이 사이버 보안 계획에 참여하게 되면, 네트워크 및 장치의 보안을 보장할 수 있는 훨씬 더 나은 위치에 있게 됩니다.

상세 정보 >

공동 책임

사이버 보안은 제품, 사람, 기술 및 지속적인 프로세스에 관한 것입니다. 그리고 사이버 보안 체인의 모든 링크가 최대한 강력해지도록 하려면 협력해야 한다는 것은 분명합니다. 사이버 보안은 최종 사용자를 포함한 다음 이해 관계자가 협력하여 공동으로 책임져야 하는 것입니다.

통합업체 및 설치업체

통합업체 및 설치업체는 모든 장비가 최신 업데이트로 패치되고 정교한 바이러스 스캐너를 실행하도록 해야 합니다. 또한 시간이 지남에 따라 패스워드, 원격 액세스 관리, 소프트웨어 및 연결된 장치의 유지관리를 위한 견고한 전략을 실행하도록 하는 것은 이해 관계자와의 공동 노력입니다.

판매업체

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

컨설턴트

컨설턴트는 시스템의 규격을 지정하는 데 도움을 주고, 적절한 수명 유지관리의 규격을 지정하는 데도 도움을 주며 잠재적 관련 비용에 대해 투명해야 합니다. 사이버 보안 책임이 종종 불분명한 OEM/ODM 장비 사용에 따른 문제도 사이버 보안에 대한 전반적인 논의의 일부가 되어야 합니다.

장치 제조업체

여기에서 사이버 보안이 시작됩니다. 제조업체는 결함의 위험을 최소화하기 위해 설계, 개발 및 테스트 부문의 사이버 보안 모범 사례를 적용해야 합니다. 내장된 보안 기능, 자체 개발 칩, 자체 공급망에 대한 세심한 관리도 중요합니다. 저렴하고 자동화된 장치 관리를 위한 도구를 제공하고 채널과 파트너에게 알려진 취약점에 대해 알리는 것도 중요합니다.

연구업체

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

최종 사용자

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.

상세 정보 >

보호에 함께 하는 파트너

협력을 통해서만 지속적으로 진화하는 사이버 보안 위협에 대처할 준비를 더 잘할 수 있고 위협이 구체화될 경우에도 빠르게 대응할 수 있습니다. 모든 이해 관계자는 사이버 보안 솔루션 구현의 모든 측면(장치 제조, 시스템 설계 및 설치에서 유지관리 및 장치 관리에 이르는)이 올바르게 수행되도록 보장하는 역할을 합니다. 우리는 바로 이러한 방식으로 경계합니다.

사이버 보안이 에지에서 신뢰를 높이는 방법

에지의 세계

2021년으로 접어 들면서, 네트워크 "에지"의 컴퓨팅을 향한 모멘텀이 증가하고 있습니다. 수십억 개의 소위 **IoT** 장치가 이미 네트워크에 연결되어 있고, 이 숫자가 **급속하게 증가하고** 있다는 것은 그 자체로는 뉴스가 아닙니다. 그러나 이러한 장치의 특성과 요구사항은 사이버 보안에 심각한 영향을 미칩니다.

IoT

사물 인터넷(IoT)은 인터넷에 연결되고 서로 "통신"할 수 있는 장치의 네트워크를 말합니다. 여기에는 스마트폰 및 웨어러블 장치와 같은 기술 장치, 스마트 계량기와 같은 스마트 홈 장치, 스마트 기계와 같은 산업용 장치가 포함됩니다. IoT 장치는 센서와 프로세서를 사용하여 그 환경에서 수집한 데이터를 수집 및 분석하고 그에 따라 작업을 생성합니다.

급속한 증가

2025년에는, 예측에 따르면 750억 개 이상의 연결된 사물 인터넷(IoT) 장치가 사용될 것으로 예상됩니다. 이는 2019년의 IoT 설치 기반에서 거의 3배 정도 증가하는 것입니다.

상세 정보 >

에지의 세계

> ❝ 카메라 자체 내에서 더 많은 데이터 처리 및 분석이 이루어지는 추세입니다.

간단히 말해서, 네트워크에 연결되는 "사물" 중 더 많은 사물이 무슨 일이 일어나고 있는지 즉시 감지하고, 무엇을 할지 결정하고, 조치를 취할 수 있는 능력을 필요로 하거나 그러한 능력으로부터 이점을 얻을 것입니다.

자율 주행차는 이에 대한 분명한 예입니다.

외부 환경과의 통신(예: 교통 신호와의 통신) 또는 위험 감지 센서를 통한 통신(예: 차량 전방에 갑자기 나타나는 물체)을 통해 결정을 순식간에 처리해야 합니다. 취할 조치를 결정하기 전에 데이터 센터에서 처리 및 분석하기 위해 네트워크에 걸쳐 차량에서 전송되는 데이터의 지연 시간은 용납할 수 없을 정도로 오래 걸립니다.

영상 감시도 마찬가지입니다.

사후 대응이 아닌 사전 대응으로 전환하려면, 즉 상황 발생 후의 대응보다 사고 예방으로 전환하려면 더 많은 데이터 처리 및 분석이 카메라 자체 내에서 이루어져야 합니다. 그러나 에지의 장치 수가 증가하고 이러한 장치가 안전 및 보안에서 더 중요한 역할을 수행함에 따라 여러 결과가 발생합니다. 이러한 결과는 이어지는 페이지들에서 살펴볼 것입니다.

상세 정보 >

전용 장치의 고유한 능력

전용 및 최적화된 하드웨어 및 소프트웨어 – 특정 애플리케이션을 위해 고안된 – 는 더 높은 수준의 에지 컴퓨팅으로 전환하는 데 필수적입니다. 연결된 장치는 향상된 컴퓨팅 능력을 필요로 하며 처음부터 사이버 보안을 염두에 두고 목적에 맞게 설계 및 제조해야 합니다.

바로 이것이 고유한 통합 처리 칩이 중요해지는 영역입니다. 예를 들어, Axis의 장치는 "백도어"를 생성하는 승인되지 않은 악의적 "펌웨어" 업그레이드와 같은 사이버 공격으로부터 장치를 보호하는 자체 설계 "시스템 온 칩"을 사용합니다. 최신 버전에서 ARTPEC-7 프로세서는 보안에 우선순위를 두고 현재와 미래의 영상 감시 요구사항을 위해 특별히 고안되었습니다.

영상 감시 전용으로 고안된 Axis ARTPEC-7 칩의 최신 버전은 초기 칩보다 50배 이상의 높은 성능을 제공합니다. 칩을 자체적으로 설계하고 제조함으로써, Axis는 사이버 보안 위협과 같은 외적 요소의 진화에 대응하면서 고객의 필요에 최상으로 최적화된 제품을 생산할 수 있습니다.

> **"ARTPEC-7은 네트워크 카메라에 매우 높은 이미지 품질을 제공할 뿐만 아니라 고성능, 우수한 대역폭 효율 및 에지에서 분석을 실행할 수 있는 능력을 제공할 수 있습니다.**
>
> Stefan Lundberg, Axis Communications 전문 엔지니어

상세 정보 >

신뢰할 수 있는 에지를 향하여

신뢰는 다양한 형태를 취합니다.

- **조직이 책임감 있게 데이터를 수집하고 사용할 것이라는 신뢰**
- **장치와 데이터가 사이버 범죄자로부터 안전하다는 신뢰**
- **데이터 자체가 정확하고 기술 자체가 의도대로 작동할 것이라는 신뢰**

에지는 이 신뢰가 생성되거나 파괴되는 지점입니다.

전체 공급망에 걸쳐 신뢰가 중요합니다. 하드웨어 자체에 스파이 칩을 내장하는 것은 실현 가능성이 떨어지지만, 제조 시점보다 후속 펌웨어 업그레이드를 통해 스파이 "백도어"를 장치에 설치하는 것이 비교적 쉽습니다.

상세 정보 >

신뢰할 수 있는 에지를 향하여

개인 정보 보호에 관한 문제는 전 세계에서 계속 논의될 것입니다. 동적 익명화 및 마스킹과 같은 기술을 에지에서 사용하여 개인 정보를 보호할 수 있지만, 태도와 규정은 지역 및 국가에 걸쳐서 일관되지 않습니다. 감시 부문의 기업은 국제 법률 기준을 계속 탐색해야 할 것입니다.

사이버 보안은 그 어느 때보다 더 중요합니다.

장치 자체에서 더 많은 데이터 처리 및 분석이 이루어짐에 따라, 사이버 보안은 훨씬 더 중요해질 것입니다. 점점 더 복잡하고 정교한 사이버 공격에 직면해 있는데도, 많은 조직이 여전히 가장 기본적인 펌웨어 업그레이드를 수행하지 못하고 있습니다. 보안 시스템의 기본은 명확한 하드웨어 정책, 소프트웨어 정책 및 사용자 정책을 통해 개별 장치 관리와 전체 감시 솔루션의 포괄적 수명주기 관리가 모두 필요하다는 것입니다.

규정 위반의 위협

최근 몇 년 동안 British Airways 및 Marriott International과 같은 조직은 규정을 준수하지 않아 막대한 벌금이 부과되었습니다. 벌칙의 위협은 비즈니스 커뮤니티에 충격을 주었으며, 이제 조직이 사이버 보안 예산을 사용하는 방식에 영향을 미치고 있습니다.

조직도 랜섬웨어, 악성 소프트웨어 및 피싱과 같은 다른 표적 공격의 위협에 노출되어 있습니다. 이로 인해 시스템 종료, 데이터 소실, 운영 중단, 부정적 대외 이미지, 고객 상실 및 매출 감소가 발생할 수 있습니다.

규정 준수란 무엇입니까?

종종 규정 준수는 정부 규정 및 국제 표준을 준수하는 것을 가리키는 것으로 간주됩니다. 그러나 이것은 이야기의 일부일 뿐입니다. 또한 조직은 내부 통제 및 모범 사례를 구현하고 따라야 하는 동시에 거래하는 파트너도 규정을 준수하도록 해야 합니다.

이제 조직은 고객 데이터를 적절하게 보호할 책임이 있습니다.

고려해야 할 세 가지 영역이 있습니다.

1. **규정 준수**
   GDPR과 같은 정부 규정 및 ISO 또는 NIST와 같은 기준 및 국제 표준
2. **내부 규정 준수**
   내부 회사 정책 및 모범 사례
3. **외부 규정 준수**
   공급망 내의 규정 준수

상세 정보 >

법률을 준수해야 할 우리의 의무

EU 일반 개인정보 보호법(GDPR)과 같은 데이터 보호법은 조직, 기업 또는 정부에서 소비자의 개인 정보를 사용하는 방식을 통제하기 위해 고안되었습니다. 사이버 보안과 관련하여 이러한 법률은 종종 조직이 사용하는 보안 솔루션과 밀접한 관련이 있습니다.

GDPR은 유럽 법률이지만 대부분의 글로벌 조직은 어떤 방식으로든 이에 대응해야 합니다. 예를 들어, EU에 데이터를 저장하는 미국 기업은 GDPR을 준수해야 합니다. 마찬가지로 조직이 데이터 처리를 사용하는 제3자와 계약을 체결한 경우, 이들 당사자도 GDPR을 준수해야 합니다. 미국의 50개 주 모두에는 데이터 보호에 대한 별도의 규정이 있어서 주 간 작업을 관리하기 어렵고 시간이 많이 걸립니다.

내부 거버넌스는 더 많은 비용이 듭니다.

해커는 표준을 해킹하지 않습니다. 회사를 살펴보고 특정 취약점이 무엇인지, 어디에 취약점이 노출되어 있는지 확인합니다. 조직은 전체 예산을 사이버 보안에 쉽게 사용할 수 있습니다. 그러나 목표는 충분한 보호를 제공하지만 혁신을 방해하지 않는 것이어야 합니다. 이것은 균형이며 위험에 대한 조직의 욕구에 달려 있습니다. 일부 조직은 법률에서 정한 것보다 훨씬 더 강력한 통제를 구현합니다. 사이버 보안 침해가 발생한 경우 조직이 비즈니스를 보호하기 위해 적절한 조치를 취했음을 입증해야 하기 때문입니다.

공급망 내의 규정 준수

공급망이 복잡한 조직에는 다른 규정 준수 요구사항도 있습니다. 예를 들어, 미국 정부와 비즈니스를 수행하는 유럽 기반 조직은 사이버 보안 절차의 내부 관리에 기반한 감사 인증을 요구하는 사이버 보안 성숙도 모델 인증(Cybersecurity Maturity Model Certification)과 같은 표준을 준수해야 합니다. 최악의 경우, 제3자(공급자와 같은)도 규정 위반에 대해 부분적으로 책임이 있을 수 있고, 따라서 벌금의 일정 비율을 부담할 수 있습니다.

외부 의무는 중요하지만, 이러한 규정을 넘어서는 조직의 내부 정책을 갖추는 것이 권장됩니다. 결국, 규정 준수를 보장하고 모든 위반으로부터 데이터가 보호되도록 보장하는 것은 조직의 책임이기 때문입니다.

상세 정보 >

어떤 규정이 귀사에 적용됩니까?

규정 준수를 지속하려면 지속적인 노력이 필요합니다. 조직에 적용되는 사이버 보안 및 데이터 관리 규정은 일반적으로 해당 산업에 따라 다릅니다. 그러나 여러 산업 및 국가에 적용되는 여러 규정이 있습니다.

조직은 법률에 반영될 수 있는 향후 지침과 변경 사항을 지속적으로 검토해야 합니다. 현재의 위협과 공격을 조사하고 어떤 규정 준수 법률과 규정이 적용되고 있는지 이해함으로써 조직은 새로운 규정 준수 검사를 통과하기 위해 무엇을 변경해야 하는지 결정할 수 있습니다.

사이버 보안 감사

조직이 준수해야 하는 규정을 확인한 후에는, 전체 규정 준수 상태를 확인해야 합니다. 내부 사이버 보안 감사를 수행하여 조직의 IT 보안 거버넌스 프로세스를 평가할 수 있습니다. 일반적으로 조직은 매년 사이버 보안 감사를 수행해야 합니다. 그러나 모든 관리 조치를 지속적으로 모니터링하여 관리 조치의 빈틈을 적시에 보완할 수 있도록 하는 것이 좋습니다. 또한 조직은 보안 관리 조치에 대한 이러한 지속적인 평가를 정기적으로 문서화하는 것이 좋습니다. 그런 다음 이를 향후 감사에 사용할 수 있습니다.

사이버 보안 감사 중에 고려해야 할 몇 가지 사항:

- **위험 관리:** 조직에서 어떤 프로세스를 사용하여 규정 준수와 관련된 위험을 파악하고 관리합니까? 예를 들어, 위험을 어떻게 전달하고 어떤 프로세스를 사용하여 위험을 평가합니까?
- **내부 감사 프로세스:** 조직은 규정 준수를 지속적으로 모니터링하기 위해 내부 감사 프로세스를 수립해야 합니다. 예를 들어, 사이버 보안 관행에 대한 변경사항을 파악, 평가 및 관리하기 위해 어떤 프로세스를 갖추고 있습니까?
- **보안 및 개인 정보 보호 교육:** 직원이 권한이 부여되어 있고 IT 보안 요구사항의 빈틈을 파악하는 데 필요한 교육을 받았습니까? 예를 들어, 이메일 피싱 처리 방법에 대한 교육 프로그램이 있습니까? 그러한 교육 프로그램을 갖는 것은 이야기의 일부일 뿐입니다. 내부 관리 조치가 교육의 효과를 결정할 것입니다. 조직의 특정 영역이 고위험 영역인 경우, 매년이 아닌 분기별로 점검을 수행할 수 있습니다.

상세 정보 >

규정 준수 모니터링

내부 감사의 결과는 규정 준수 모니터링 계획을 만드는 데 사용할 수 있습니다. 이 계획은 조직의 전반적인 규정 준수 노력을 지속적으로 평가하고 감사 중에 파악된 모든 위험에 대응하는 데 사용할 수 있습니다. 조직에 가장 큰 위협이 되는 위험에 우선 순위를 두어야 합니다. 조직에서 시행하는 규정 준수 관리 조치를 평가하여 사이버 보안 관리 조치 내의 모든 규제 틈새를 파악할 수 있습니다.

사이버 보안 위험을 모니터링할 책임이 있는 사람을 결정할 때는 반드시 필요한 전문 지식에 기반하여 역할을 배정해야 합니다. 어떤 직원이 필요한 기량을 보유하고 있고 어떤 위험 모니터링 활동을 결합할 수 있는지 자문하여 역할 배정을 최적화할 수 있습니다.

최신 상태입니까?

제조업체는 일반적으로 취약점을 해결하기 위해 그리고 새로운 법률이 채택될 때마다 정기적인 펌웨어 업데이트를 보냅니다. 그러나 제품이 더 이상 지원되지 않을 때를 항상 대비할 수 있도록 모든 장치 및 장치 수명주기 상태를 명확하게 파악하는 것도 중요합니다. AXIS Device Manager와 같은 장치 관리 도구는 제품이 업데이트되고 규정을 준수하도록 하는 데 도움이 됩니다. 이러한 도구는 라이선스 구독 갱신, 유지관리 시간 또는 승인에 대한 알림을 전송하여 조직이 규정 준수 요구사항을 충족하고 항상 최신 상태를 유지하도록 하는 데 도움이 됩니다. 또한 감사에 필요한 경우, 이러한 도구는 필요한 문서를 제공할 수도 있습니다.

규정 준수를 보여주십시오.

고객은 종종 장치 제조업체에 사이버 보안 수준에 대한 설문 조사를 완료할 것을 요청합니다. 조직은 연속성 계획, 인증 구현 방법 및 네트워크에서 데이터를 보호하는 방법에 대한 질문에 답해야 합니다. 이러한 모든 정보를 공유할 준비가 되도록 함으로써 조직은 실사를 수행한 방법을 신속하게 보여주어 고객의 마음을 편안하게 할 수 있습니다.

> **“ 규정 위반의 대가는 큽니다. 규정 준수 비용이 비싸다고 생각되면 규정 위반을 시도하십시오.**
>
> 전 미국 법무 차관 Paul McNulty https://youattest.com/

상세 정보 >

문서, 문서, 문서

문서화는 규정 준수를 보여줄 수 있도록 하는 데 중요합니다. 내부 정책에는 다음과 같은 설명이 포함될 수 있습니다.

- 왜 그리고 무엇을 기록하고 있습니까?
- 대중에게 그들이 모니터링되고 있음을 알리는 문구를 표시합니까?
- 감시 영상에서 개인을 보여줍니까? 이는 대중의 개인 정보에 영향을 미치므로 고려하고 문서화해야 합니다. 누가 영상에 액세스할 수 있습니까?
- 데이터를 어떻게 그리고 얼마나 오래 보관합니까? 데이터 스토리지가 물리적으로 그리고 사이버 보안 관점에서 모두 안전합니까? 어떤 방법으로 이전 영상이 삭제되도록 합니까?

특정 시나리오에 대한 문서화도 포함해야 합니다. 예를 들어 침입자가 있는 경우 어떻게 처리해야 합니까? 누가 데이터를 관리할 책임이 있고 어떤 프로세스가 사용됩니까? 또한 내부 감사 중에 확인된 모든 결함과 조직이 빈틈을 없애기 위해 취하고 있는 노력에 대해 규제 위원회에 지속적으로 알리는 것이 좋습니다.

규정 준수는 움직이는 목표물과도 같은 것입니다.

법률과 규정은 지속적으로 발전하고 있으며, 가장 엄격한 규정 준수 모니터링 계획조차도 규제 벌금으로부터 귀사를 완전히 보호하지는 못한다는 점을 인식하는 것이 중요합니다. 조직은 지속적으로 준수를 모니터링하고 준수를 자신있게 보여줄 수 있어야 합니다.

바로 지금이 행동할 시기입니다.

규정 준수가 사이버 보안의 핵심 구성 요소라는 것은 의심의 여지가 없으며 규정 준수 문제는 항상 존재합니다. 조직과 소비자는 똑바로 앉아서 위협에 주의하고 있고, 신속하게 행동하지 않을 경우 자신의 시스템과 데이터가 공격에 취약하다는 것을 깨닫고 있습니다. 조직은 확신을 가지고 혁신과 성장을 추구하기를 원하지만 사이버 범죄로 인한 위험도 최소화해야 합니다. 반면에 소비자는 자신들의 데이터가 안전하게 유지되기를 원하며, 자신들과 거래하는 조직이 이를 수행하는 방법을 알아내기를 기대합니다. 정부 규제는 공급업체, 제조업체 및 최종 사용자가 모두 사이버 보안 효과에 대해 책임을 지는 협업적 접근 방식으로만 해결할 수 있는 문제입니다. 궁극적으로는, 이를 통해 피해 유발 침해의 위험을 최소화할 수 있습니다.

규정 준수가 사이버 보안의 핵심 구성 요소라는 것은 의심의 여지가 없으며 규정 준수 문제는 항상 존재합니다.

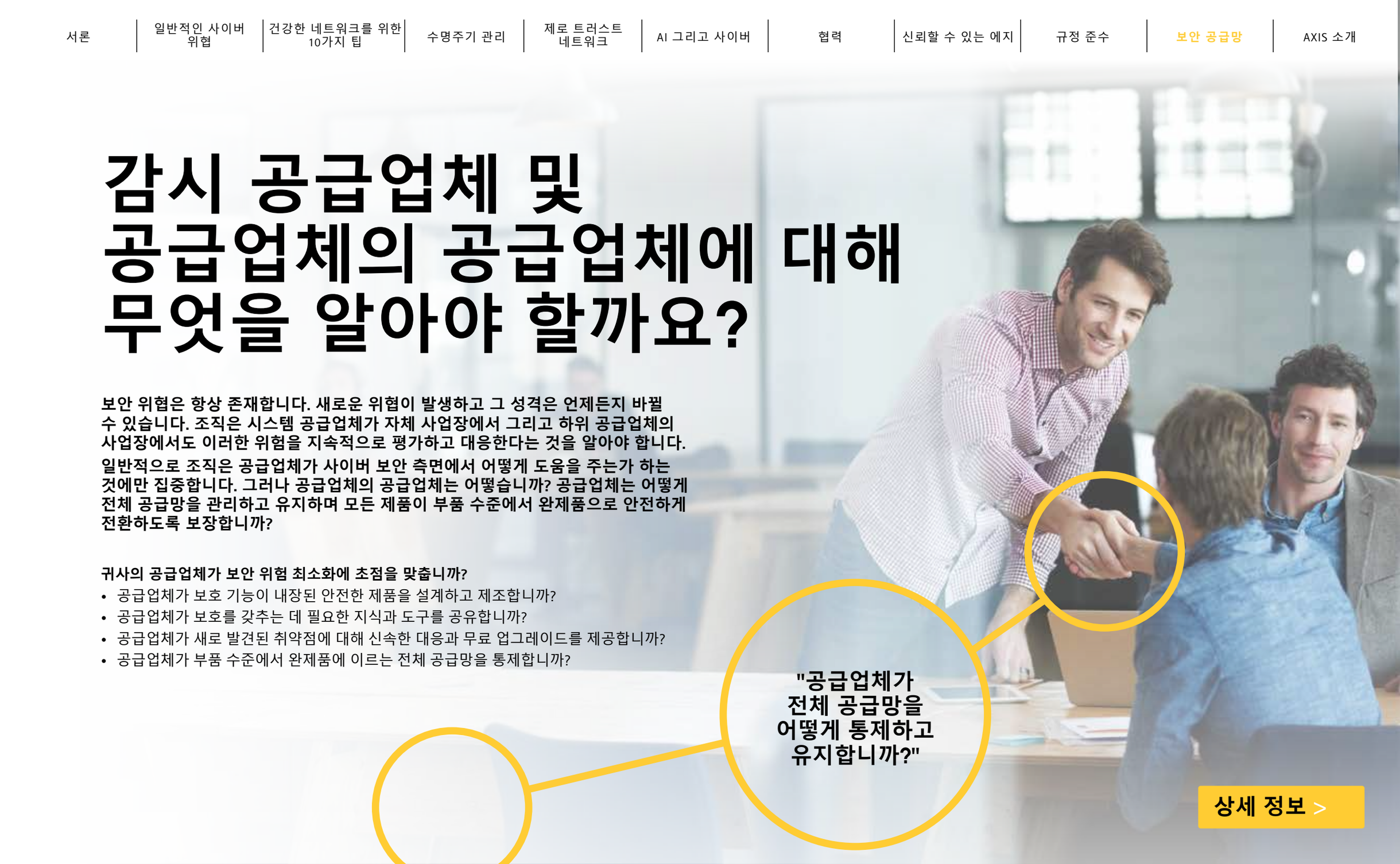
감시 공급업체 및 공급업체의 공급업체에 대해 무엇을 알아야 할까요?

보안 위협은 항상 존재합니다. 새로운 위협이 발생하고 그 성격은 언제든지 바뀔 수 있습니다. 조직은 시스템 공급업체가 자체 사업장에서 그리고 하위 공급업체의 사업장에서도 이러한 위험을 지속적으로 평가하고 대응한다는 것을 알아야 합니다.

일반적으로 조직은 공급업체가 사이버 보안 측면에서 어떻게 도움을 주는가 하는 것에만 집중합니다. 그러나 공급업체의 공급업체는 어떻습니까? 공급업체는 어떻게 전체 공급망을 관리하고 유지하며 모든 제품이 부품 수준에서 완제품으로 안전하게 전환하도록 보장합니까?

귀사의 공급업체가 보안 위험 최소화에 초점을 맞춥니까?

- 공급업체가 보호 기능이 내장된 안전한 제품을 설계하고 제조합니까?
- 공급업체가 보호를 갖추는 데 필요한 지식과 도구를 공유합니까?
- 공급업체가 새로 발견된 취약점에 대해 신속한 대응과 무료 업그레이드를 제공합니까?
- 공급업체가 부품 수준에서 완제품에 이르는 전체 공급망을 통제합니까?



상세 정보 >

적절한 파트너 찾기

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 또한 위험 관리를 위해 하위 공급업체의 프로세스와 생산 시설 및 공정을 평가해야 합니다. 해당 회사가 승인된 공급업체 자격에 대해 설정된 요구사항 및 표준을 충족하는지 평가하기 위해 현장을 방문하고 후속 조치 차원에서 현장 감사를 수행해야 합니다. 잠재적인 새로운 공급망 파트너에 대한 평가의 일환으로, 공급업체는 조직의 재무 상태 및 소유 구조에 대한 심층 분석을 수행해야 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. 따라서 공동 작업과 의사 소통이 긴밀하고 매일 이루어지며, 현장을 자주 방문합니다.

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 안전합니까?

- 공급업체가 제조 공정을 정의하고 모니터링합니까?
- 공급업체가 중요한 생산 장비를 개발하고 생산하고 있습니까?
- 공급업체가 생산 중에 부품, 모듈 및 제품을 테스트하기 위한 시스템을 소프트웨어, 테스트 컴퓨터 및 기타 IT 하드웨어 인프라와 함께 제공합니까?
- 공급업체가 실시간 데이터 분석을 가능하게 하고 잠재적인 보안 위험을 평가하고 위험 완화 계획을 실행하기 위해 생산 데이터를 연중무휴로 수집합니까?

상세 정보 >

공급업체 감사

공급업체가 하위 공급업체가 지정된 요구사항을 준수하도록 하는 가장 좋은 방법은 매년 또는 2년에 한 번씩 정기적 현장 감사를 수행하는 것입니다.

감사는 다음과 같은 중요한 측면을 다루어야 합니다.

- 문서화를 포함한 프로세스 준수
- 시설 보안
- 물리적인 공장 내 취급
- 재고 취급
- 생산 장비
- 품질 관리
- 추적성 기록

분기별 경영 실적 검토도 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.

- 입구와 출구를 지속적으로 보호해야 하고, 접근 제어 및 방문자 등록을 기록하여 저장해야 합니다. 일부 지역에서는 시설과 주변을 보호하기 위해 경비원을 두더라도 지속적인 감시가 필요할 수 있습니다.
- 스캔 장비를 사용하여 원하지 않는 물체나 물질을 감지해야 합니다.
- 엄격한 보안 규정과 관리 조치를 유지하는 잘 알려진 운송업체와 함께 운송을 준비해야 합니다. 운전 기사와 트럭은 상차 및 하차 시 안전 규정을 준수해야 합니다.
- 모든 항공화물은 X선 촬영으로 검사해야 합니다. 또한 원산지에서 각 화물을 봉인하여 탐지 없이 침입을 방지하는 것이 일반적입니다.
- 입고 및 출고 물품은 CCTV 카메라를 사용하여 감시 및 문서화됩니다.

상세 정보 >

데이터 전송 및 정보 보안

공급망 네트워크의 데이터 전송은 암호화 방법과 인증을 사용하는 보안 프로토콜로 보호해야 합니다. 하위 공급업체 및 파트너는 높은 수준의 정보 보안을 유지하여 공급망의 빈틈 발생 위험을 완화해야 합니다.

공급업체는 민감한 회사 정보를 식별하고 관리하기 위해 체계적인 접근 방식을 사용해야 합니다. 이 시스템은 사람, 프로세스, IT 시스템 및 물리적 위치를 포함해야 하며 ISO 27001 및 EU 일반 개인정보 보호법(GDPR)을 준수해야 합니다. 이것은 인식을 향상시키고 효과적인 위험 관리를 가능하게 합니다.

인적 보안

어떤 사람을 채용하는 것인지 아는 것은 교육, 역량 및 업무 경험의 관점뿐만 아니라 보안 관점에서도 중요합니다. 예를 들어 Axis에서는 채용 프로세스의 품질과 보안이 핵심이며, 접근 방식에는 신원 확인, 추천서 요청, 채용 전의 보안 배경 조사가 포함됩니다. 신입 직원과 컨설턴트는 고용 중과 퇴사 후 지적 재산 및 기타 민감한 정보를 보호하는 기밀 유지 계약(NDA)에 서명해야 합니다.

직원에게 권한을 부여하고 위험을 줄이십시오.

Axis에서는 직원이 높은 수준의 정보 보안 인식을 유지하도록 합니다. Axis는 권한이 부여된 직원은 무엇을 해야 하고 어떤 위험이 있는지 아는 데 필요한 정보를 갖고 있다고 믿습니다. 모든 Axis 직원은 진정한 보안과 신뢰에 대한 약속의 일부입니다. 모든 직원은 정보 보안 인식에 대한 교육과 훈련을 받으며, 주의를 기울이고 경계를 유지해야 합니다. 정보, 시스템 및 리소스에 대한 접근은 제한되며 업무 수행을 위해서 필요한 직원에게만 접근이 허가됩니다. 마찬가지로 공급업체 및 제조 파트너의 직원은 정보, 시스템 및 리소스를 Axis와 공유합니다.

상세 정보 >

제품 무결성

모든 제품과 마찬가지로 감시 제품은 무결성을 유지하면서 설계의 목적에 맞게 그리고 의도한 대로 작동해야 합니다. 이는 제품이 공급망을 통과하는 동안 제품의 하드웨어 및 펌웨어가 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 수준에서 테스트하기 위한 시스템을 개발하고 생산합니다. 이 프로세스는 변조 위험을 제한합니다. 추가적인 보안 관리 조치로서, 모든 테스트 데이터를 Axis와 연중무휴로 공유하여 무단 수정을 즉시 발견할 수 있도록 합니다.

Axis라야 하는 이유

더욱 스마트하고 안전한 세상을 위한 솔루션

우리가 하는 모든 일에서 품질 추구: Axis의 모든 제품은 광범위한 테스트를 거치므로 고객은 안심하고 제품을 사용할 수 있습니다.

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 인정 받고 있습니다. 예를 들어, Axis 카메라와 엔코더의 80%는 PVC를 사용하지 않습니다.

사이버 보안 추구: Axis는 위협과 결과를 지속적으로 모니터링하고 신속하고 결정적인 조치를 취합니다. 설치 후에도 업그레이드, 업데이트 및 설치를 통해 장치의 사이버 보안을 계속 강화합니다.

세계 각지 진출 및 현지 전문 인력 확보: Axis는 50개 이상의 국가에서 네트워크 비디오 제품의 세계 최대 설치 기반 및 직원을 보유하고 있습니다. 우리는 통찰력과 경험을 공유하고 최신 기술 트렌드에 대한 최신 정보를 항상 파악합니다.

파트너십의 힘: 파트너십을 위한 노력을 통해 Axis는 시장에서 가장 통합적인 카메라 브랜드가 되었습니다.

Axis Communications 에 대하여

Axis는 보안 개선과 새로운 비즈니스 수행 방식에 대한 통찰력을 제공하는 네트워크 솔루션을 개발하여 보다 스마트하고 안전한 세상을 만들 수 있도록 지원합니다. 네트워크 비디오 업계의 선도 기업인 Axis는 비디오 감시 및 분석, 접근 제어, 인터콤, 오디오 시스템 분야의 제품과 서비스를 제공합니다. 50개 이상의 국가에서 3,800명이 넘는 Axis 임직원이 파트너와 협력하여 전세계 고객에게 최적의 솔루션을 제공하고 있습니다. 1984년에 설립된 Axis는 스웨덴에 본사를 두고 있습니다.

Axis에 대한 자세한 정보는 www.axis.com에서 확인하실 수 있습니다.