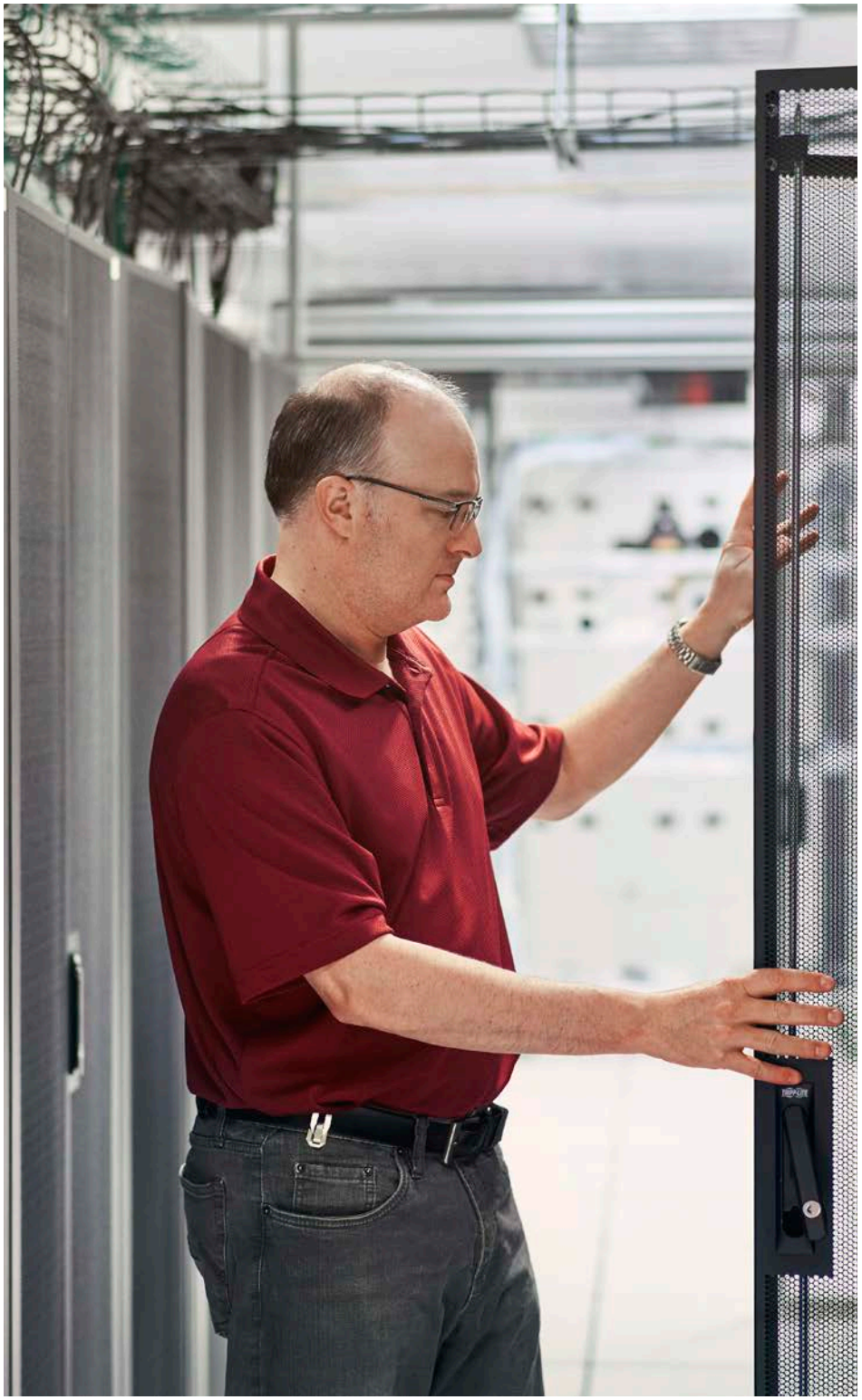
# 물리 보안 분야에서의 사이버 보안

오늘날의 사이버 위협에 대한 방어 및
물리 보안 시스템 내 기밀 정보 보호에 대한 가이드

Genetec™



# 목차


사이버 범죄가 사상 최고 수준에 달하고 있습니다.
충분히 대응하고 계십니까? 3

사이버 위협 현황의 이해 4

데이터 보호 조치의 강화 9

강력한 사이버 보안 전략의 유지 17

5분을 투자할 가치가 있는
사이버 보안 동향에 관한 영상들 23

Genetec과 함께하는 데이터 보호 전략의 구축 24

# 사이버 범죄가 사상 최고 수준에 달하고 있습니다. 충분히 대응하고 계십니까?

사이버 범죄는 그 어느 때보다 빠르게 증가하고 있습니다. 사이버시큐리티 벤처스(Cybersecurity Ventures)의 보고서는 사이버 범죄로 인한 전 세계적 비용이 연간 10조 5,000억 달러에 이를 것으로 보고 있습니다. 이 비용이 연간 15%씩 증가하면서 사상 최대 규모의 경제적 부의 이동이 예측되고 있습니다.

이로 인해 기업들은 변화하는 위협에 대한 민첩하고 신속한 대응력을 유지할 수 있기를 원합니다. 몇 가지 보호 계층을 보안 생태계에 구축하는 것은 바람직한 첫걸음이지만 충분하지 않을 수 있습니다.

오늘날 사이버 공격에 대한 진정한 대응력을 갖추기 위해서는 보다 공격적인 사이버 보안 전략이 필요합니다. 또한 자동화된 도구를 제공하는 신뢰할 수 있는 파트너를 선택하여 위협을 한층 효과적으로 경감시킬 수 있어야 합니다.

본 전자책을 통해 사이버 보안 판도의 수준을 높이고 기업을 보호하는 데 필요한 모든 것을 확인하실 수 있습니다.

1장

# 사이버 위협 현황의 이해

"사이버 보안은 업계는 물론 모든 사람들의 관심사입니다. Genetec은 우리가 속한 지역사회와 공동체에 큰 책임감을 느끼고 있으며 이러한 신념에 따라 개인정보보호와 사이버 보안을 강조해 왔습니다. 우리는 보안과 개인정보보호는 공존할 수 있으며, 분리할 때보다 통합할 때 더 유리하다고 믿습니다. 또한 이러한 가치를 공유하는 기관들이 있기에 당사가 지속적으로 성공할 수 있다고 생각합니다. 앞으로도 계속해서 각 분야의 기관과 신뢰를 구축하기 위해 노력할 것입니다."

**–피에르 라즈(Pierre Racz)**
Genetec CEO

# 위협의 근원

보안 시스템을 해킹하는 일은 어떤 형태로든 이루어질 수 있습니다.
오늘날 가장 일반적인 공격 전략 중 일부는 다음과 같습니다.

**스파이웨어**

공격 대상자의 컴퓨터에 악성 소프트웨어를 설치하거나 모방 웹사이트를 만들어 신용카드 정보나 암호를 입력하도록 속이는 수단

**랜섬웨어**

필수 데이터 또는 시스템에 대한 공격 대상자의 접근권한을 차단하여 접근권한을 돌려받기 위한 비용을 공격자에게 지불하도록 하는 악성 소프트웨어를 설치

**서비스 거부(DDoS) 공격**

사용자가 접근할 수 없도록 대상 시스템 또는 네트워크로 대량의 트래픽 또는 충돌을 유발하는 정보를 전송

**무차별 대입 공격**

암호를 추측하거나 간단한 알고리즘을 사용하여 암호를 해독함으로써 시스템 또는 네트워크에 무단으로 접근

**중간자 공격**

패킷 스니퍼를 사용하여 네트워크상에서 전송 중인 사용자 이름, 암호 또는 영상 자료와 같은 기타 데이터 등의 정보를 캡처

**피싱 공격**

사람을 속여 중요한 정보를 노출시키거나 악성 소프트웨어를 설치하도록 설계되어, 신뢰할 수 있는 출처에서 온 것처럼 보이는 사기성 메시지를 전송

**이와 같은 위협을 방어하기를 원하시나요? 다음 자료들을 확인하시기 바랍니다.**

하이라이트
일반적인 사이버 보안 아키텍처

블로그
사이버 보안 대응 능력을 강화하는 10가지 단계

영상
사이버 보안 영상 자료

# 사이버 공격이 기업에 미치는 재정적 영향

유출 사고로 인한 피해를 복구하기 위해 법, 규제, 기술 측면의 비용을 기업이 부담

소프트웨어, 네트워크 또는 웹사이트가 다운된 후 업무 중단으로 인한 조직의 생산성 저하

손상된 장치를 복원 또는 교체하거나 유출된 웹사이트의 코드를 수정하기 위한 비용 지출

고객 데이터 유출로 인한 기업에 대한 고객의 신뢰도 상실 및 직원의 이직률 증가

공격으로 인한 상장기업의 주식 실적 타격

## 수치로 보는 사이버 유출 사고

### 전체 유출 사고의 19%
자격 증명의 도난 또는 손상으로 인해 발생
자료 출처

### 142만 달러
신뢰도 상실로 인한 평균 사업 손실액
자료 출처

### 30.8%의 하락폭
사이버 유출 사고 이후 3년 동안 하락한 주가의 폭
자료 출처

### 435만 달러
2022년에 사상 최고치를 기록한 데이터 유출로 인한 평균 비용
자료 출처

### 전체 CEO의 75%
2024년에는 사이버 보안 사고에 대해 개인적 책임을 지게 됩니다.
자료 출처

### 전체 소기업의 60%
사이버 공격 후 6개월 이상 사업 지속 불가
자료 출처

### 전체 유출 사고의 16%
피싱 공격으로 인해 발생
자료 출처

# 사이버 보안 방어 능력을 확인하기 위한 5가지 질문

기존 방식의 보안 기술은 오늘날의 위협을 방어하도록 설계되지 않았습니다. 따라서 데이터 기밀성, 무결성 및 가용성을 보장하는 사이버 보안 및 개인정보보호를 위한 기본 사항을 지원하지 못합니다.

다음 질문을 통해 귀사의 구세대 장치가 사이버 보안 대응을 저해하지 않는지 확인하시기 바랍니다.

1. 수백 대의 카메라 중 한 대를 보호하지 못해서 해당 장치가 고객 정보의 유출 경로가 될 경우, 이러한 상황이 초래할 재무상 및 운영상 결과를 알고 계십니까?
2. 다양한 소프트웨어 및 펌웨어를 업데이트하고 시스템상 사이버 보안 조치를 관리하는 데 팀이 얼마나 많은 시간을 소비하는지 알고 계십니까?
3. 강력한 암호 정책을 구축 및 유지하고 데이터에 대한 접근권한을 효과적으로 제한할 수 있습니까? 여러 단계의 인증을 통해 통합 인증(single sign-on) 기능을 제공할 수 있습니까?
4. 구세대 시스템에 최신 암호화 기법 또는 사이버 보안 기능을 채택하여 변화하는 위협에 선행적으로 대응할 수 있습니까?
5. 고객 또는 경찰관이 귀하의 조직이 수집한 영상 자료를 확인하겠다는 요청를 받았을 때 해당 영상 내의 다른 개인의 신원을 보호하면서 안전하게 공유할 수 있습니까?

**업그레이드할 때가 됐다고 생각하시나요? 다음 자료들을 확인하시기 바랍니다.**

솔루션
Security Center 개요 살펴보기

영상
Security Center의 사이버 보안 기능 활성화

블로그
사이버 위협을 방어하기 위한 5가지 단계

# Lee Health

## 보건의료 현장 전반에 걸친 중요 정보의 보호

Lee Health는 미국 플로리다주에서 100개 이상의 의료 거점을 보유한 최대 규모의 공중보건 시스템을 운영하고 있습니다. 최근 Lee Health의 보건의료팀은 Genetec Security Center를 사용하여 20여 곳의 현장 운영을 표준화했습니다. 보건의료팀은 이제 하나의 직관적 솔루션을 통해 다양한 시스템을 모니터링하고 있습니다.

보안팀이 물리적 위협으로부터 기업을 보호하느라 분주한 가운데 지원군 Security Center는 보건의료팀에 사이버 위험에 대해 알립니다. 시스템 유지관리와 관련해서는 건강 모니터링 기능이 보안팀에 큰 도움이 되고 있습니다.

Lee Health의 보안 기술 및 비급성 환자치료 부문 이사인 션(Sean)은 말합니다. "기존 시스템에서는 시스템을 개선하기 위한 문제나 기회를 전혀 파악하지 못했습니다. 그러나 Security Center는 시스템 각 수준에 적합한 세부 정보를 제공합니다. 이로써 어떤 장치에 문제가 있는지 즉시 확인하고 건강 기록 보고서를 실행하여 어떤 상황에서든 대처할 수 있습니다."

Lee Health는 앞으로 Genetec 플랫폼을 통해 모든 현장을 운영하는 방향으로 보안 전략을 추진하고 있습니다. 현재 700대 이상의 카메라와 325개의 문이 Security Center와 연결되어 있으며, 이 수치는 내년 중 두 배로 늘어날 것입니다.

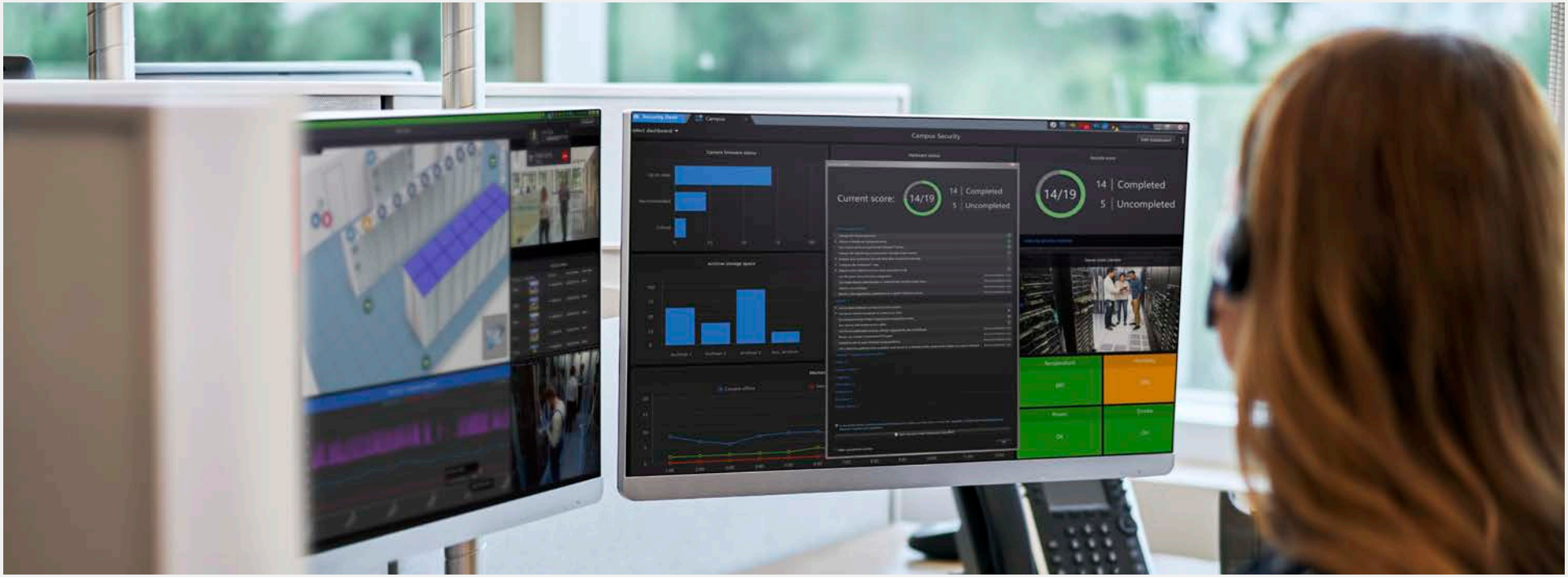
"사이버 보안을 강화해 온 오랜 경력을 가진 Security Center는 특히 Lee Health의 정보시스템 팀에게 매력적인 솔루션이었습니다. 일부 구세대 장비에 대해 우리가 갖고 있던 불만은 최신 사이버 보안 표준에 미달된다는 것이었습니다. Security Center를 사용함으로써 이러한 간극을 좁히고 IS 파트너들의 요구사항을 충족시킬 수 있었습니다."

**–션 오웬스(Sean Owens)**
Lee Health 보안 기술 및 비급성 환자치료 부문 이사

# 데이터 보호 조치의 강화

"사이버 보안은 Genetec의 핵심 업무입니다.
Genetec은 설계에서 도입에 이르기까지 IT 보안 우수 관행을 물리
보안 제품을 개발하는 데 적용하기 위해 노력하고 있습니다."

**–마티외 슈발리에(Mathieu Chevalier)**
Genetec 수석 보안 설계자



# 시행해야 할 가장 중요한 3가지 사이버 보안 대책

요즘에는 물리 보안을 구축하면서 사이버 보안 대응 능력을 갖추기 위해 많은 작업을 해야 합니다. 더 많은 계층의 대응 능력을 구현할수록 사업을 더 강력하게 보호할 수 있습니다. 지금부터 가장 중요한 사이버 보안 도구들을 살펴보겠습니다.

**첫 번째 계층 – 암호화**

간단히 말해서 암호화를 사용하면 비디오 카메라, 출입통제 리더기 및 기타 IoT 센서와 같은 보안 장치에서 서버 및 클라이언트 워크스테이션과 전송되는 모든 물리 보안 데이터를 보호할 수 있습니다. 암호화는 정보를 인코딩하거나 권한이 없는 사용자들로부터 정보를 숨기고 보호하기 위해 텍스트를 읽을 수 없도록 뒤섞는 것입니다.

**팁!** 특히 VMS 암호화의 경우, 전송 중인 데이터와 저장된 데이터 모두에 강력한 암호화 방법을 사용하는 것이 필수입니다. 일반적으로 전송 중인 데이터가 더 취약하다고 여겨지지만 공격자는 항상 가장 취약한 진입점을 대상으로 공격합니다.

### 2번째 계층 - 인증

인증은 보호된 리소스에 대한 액세스를 승인하기 전에 전에 사용자, 서버 또는 클라이언트 응용 프로그램의 신원을 검증하는 프로세스입니다. 클라이언트 쪽에는 사용자 이름과 비밀번호, 보안 토큰 등의 다양한 기법이 인증으로 포함될 수 있습니다. 서버 쪽에는 일반적으로 신뢰할 수 있는 써드파티 확인이 디지털 증명서를 통해 이뤄집니다.

**팁!** 여러 형태의 인증을 도입하는 것은 보호 수단을 추가적으로 갖추는 과정입니다. 사용자 이름과 비밀번호 외에도 전화 인증 앱, 생체 인증, YubiKey, 또는 스마트 카드와 같은 하드웨어 보안 토큰을 사용하여 공격자를 추가적으로 방어하는 조치 역시 고려해야 합니다.

### 3번째 계층 - 권한 부여

권한 부여는 응용 프로그램에 접근하여 확인할 수 있거나 수행할 수 있는 작업을 추가적으로 제한하기 위해 특정 사용자 권한을 정의하는 프로세스입니다. 보안 시스템 내에서의 권한 부여에는 내부 또는 외부로 공유 가능한 정보의 유형 및 공유 시기, 데이터의 보관 기간이 포함될 수 있습니다.

**팁!** 보안 시스템과 Microsoft Active Directory를 통합하여 이처럼 세분화된 권한의 프로비저닝을 자동화할 수 있습니다. 이를 통해 권한 부여 설정을 간소화할 수 있을 뿐만 아니라 직원이 퇴사할 때 시스템 권한이 회수되도록 할 수 있습니다.

# 사이버 보안에 대한 Genetec의 접근법

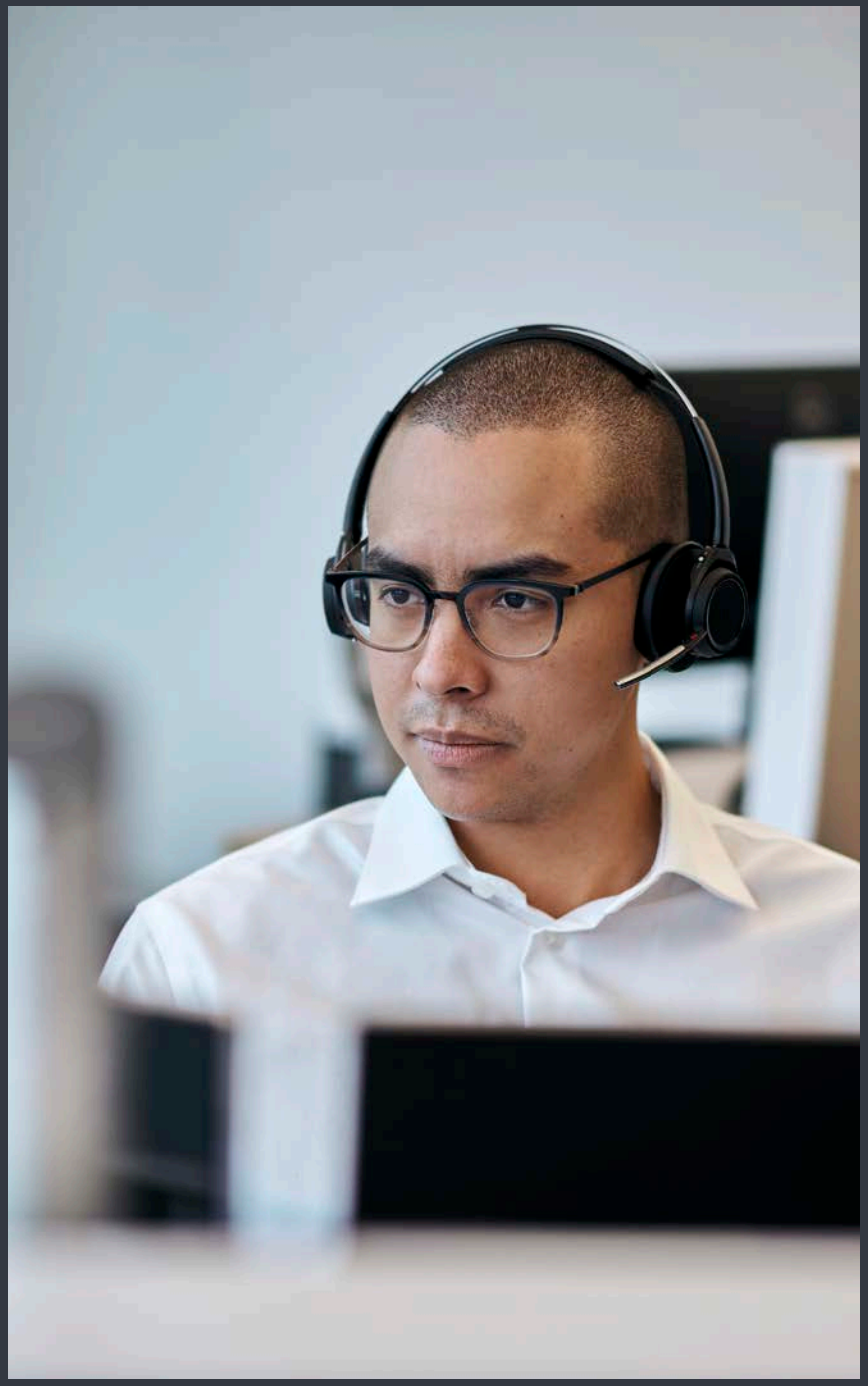
Genetec은 사이버 방어 기능을 내장한 제품을 제공합니다. Genetec의 제품을 사용한다는 것은 중요한 정보를 엿보는 행위로부터 데이터를 보호하는 데 필요한 수단을 갖고 있다는 의미입니다. 아래에서 자세히 살펴보겠습니다.

### 접근 불가능한 방식으로 정보 보관

고급 암호화, 권한 부여 및 권한 부여 방법을 사용하여 데이터를 보호하고 데이터가 악용되지 않도록 방지할 수 있습니다. 영상 녹화에 워터마크 및 디지털 서명 기능을 추가하여 데이터의 변조를 막을 수 있습니다.

### 데이터 가용성을 유지

재해 복구를 수행하고 사이버 보안 태세를 실시간으로 추적하며 권장사항에 따라 사이버 보안 대응 능력을 강화할 수 있습니다. 이 모든 기능을 통해 데이터 가용성을 항상 유지하고 시스템의 모든 구성 요소가 정상 작동하도록 할 수 있습니다.



### 소프트웨어 및 장치의 유지관리

내장된 장치 모니터링 및 업데이트 서비스를 통해 시스템을 최상의 성능으로 가동시킬 수 있습니다. 또한 소프트웨어 및 펌웨어 업데이트를 일원화하고 예약할 수 있으며 비밀번호 암호가 자동으로 교체되도록 하여 잠재적 취약점을 신속하게 해결할 수 있습니다.

### 시스템 감사를 통한 사용자 활동 추적

내장된 감사 로그 및 사용자 활동 보고서를 통해 관리 영속성을 완벽하게 유지할 수 있습니다. ID 관리를 간소화하고 사용자 및 역할에 대한 액세스 검토를 예약하여 감사 요구사항 및 기업 정책을 준수합니다.

### 검증되고 규정을 준수하는 솔루션의 사용

Genetec의 개발 표준 및 솔루션의 무결성은 신뢰할 수 있습니다. Genetec은 최신 사이버 보안 우수 관행를 준수하기 위해 국제 협회와 협력하고 있습니다. Genetec은 자체 제품에도 침투 테스트 및 감사를 수행합니다.

**사이버 보안에 대한 Genetec의 접근법을 살펴보길 원하시나요? 이 자료들부터 살펴보시기 바랍니다.**

솔루션
사이버 범죄 활동으로부터의 보호

하이라이트
Genetec의 사이버 보안 인증서

영상
3분으로 살펴보는 사이버 보안 우수 관행

# 융합이 데이터 보호에 보다 쉽고 효과적인 이유

많은 조직들이 해커를 차단하고 사업을 보호하고자 단일 데이터와 전역 데이터 보호 및 개인정보보호 전략의 도입을 검토하고 있습니다. Security Center는 모든 물리 보안 시스템에서 사이버 보안 대책을 표준화할 수 있도록 도입 프로세스를 간소화합니다. 아래에서 자세히 살펴보겠습니다.

### 데이터 보호의 일원화

통합 플랫폼을 사용하면 사이버 보안을 확보하거나 시스템 상태를 추적하기 위해 여러 솔루션을 살펴보느라 시간을 낭비할 필요가 없으며, 단 하나의 인터페이스로 모든 시스템의 데이터를 관리할 수 있습니다.

### 다양한 방어 기능 내장

통합된 도구와 서비스가 잠재적인 취약점에 대해 알려주며 업데이트를 간소화하는 데 도움을 줍니다. 이 밖에도 시스템 액세스 및 사용자 권한을 제한하고 보안 점수를 표시하는 기능은 시스템의 사이버 보안 대응 능력을 갖추는 데 도움을 줍니다.

### 한 번의 로그인으로 위험 경감

통합된 플랫폼에서 사용자에게 필요한 것은 하나의 ID와 비밀번호뿐입니다. 이를 통해 여러 개의 비밀번호가 도난되거나 해킹될 가능성과 잠재적 침해 가능성을 최소화할 수 있습니다. 또한 모든 현장에 걸쳐 데이터 보존 정책이 현지 법률에 부합하도록 사용자 정의할 수 있습니다.

**Genetec의 내장된 사이버 보안 기능에 관심이 있으십니까? 다음 자료들을 살펴보시기 바랍니다.**

경험
Genetec 업데이트 서비스

팟캐스트
위험한 사업 – 1부

영상
장치 보안을 위한 내장 기능

# 기술 공급업체의 사이버 보안 접근법을 평가하기 위한 10가지 질문

위험 경감을 위한 가장 좋은 방법 중 하나는 신뢰할 수 있는 공급업체와 협력하는 것입니다. 모든 공급업체가 사이버 보안을 홍보하고 있는 요즘, 다음 질문들을 통해 기존 공급망 또는 신규 공급업체의 신뢰성을 평가할 수 있습니다.

1. 공급업체는 새로운 위협의 등장과 그 위협이 운영, 데이터 및 인력에 미치는 잠재적 영향을 선행적으로 모니터링하고 있습니까?
2. 공급업체는 보안 격차와 취약점을 해소하기 위한 포괄적인 전략을 갖고 있습니까?
3. 공급업체는 사이버 보안과 관련하여 어떤 정책을 시행하고 있습니까?
4. 공급업체가 개발한 솔루션에는 고급 인증 및 암호화 기술과 같은 여러 보안 계층이 적용되어 있습니까?
5. 공급업체는 조직의 데이터 및 고객의 개인정보를 어떻게 보호하고 있습니까?
6. 공급업체는 보안은 물론 데이터 보호 또한 고려하고 있는 파트너와 협력하고 있습니까? 공급업체는 최고 수준의 사이버 보안 및 규정 준수를 보장하기 위해 파트너를 신중하게 검토하고 선정하고 있습니까?
7. 공급업체는 사이버 보안 우수 관행에 대한 정보를 고객에게 알리고 지원하기 위해 어떤 조치를 취하고 있습니까?
8. 공급업체는 알려진 취약점에 대해 설명하고 신속한 해결을 위한 전략과 수정사항을 공유하고 있습니까?
9. 공급업체는 ISO 27001과 같은 정보 보안 표준을 준수합니까? 공급업체는 다른 규제 기관 및 국제 협회의 인증을 받았습니까?
10. 공급업체는 보안 격차를 확인하고 해결하기 위해 써드파티 감사자를 고용하고 침투 테스트를 수행하고 있습니까?

**Genetec의 신뢰할 수 있는 파트너 네트워크에 대해 알고 싶으신가요? 여기서 자세히 살펴보세요.**

영상
사이버 보안을 위한 견고한 파트너 제휴

경험
Genetec의 세계적 파트너 네트워크

블로그
Genetec의 사이버 보안 인증서 살펴보기

# Cytiva

## 생명공학 분야에서의 사이버 보안 우수 관행의 강화

40여 개 국가에 100개 이상의 거점을 두고 있는 Cytiva는 치료제 개발과 제조를 고도화하고 가속화하는 기술 및 서비스를 제공하고 있습니다.

현재 Cytiva 팀은 주요한 연구 및 제조 현장에서 Security Center SaaS 에디션 버전을 사용하여 출입통제 및 VMS를 관리합니다.

Cytiva의 관련 제품 책임자 앨런(Allen)은 말합니다. "예전에는 취약점을 패치하고 소프트웨어를 업데이트할 뿐이었고 이런 환경을 관리하는 것만으로도 벅찼습니다. Genetec Security Center SaaS 에디션 버전을 도입한 후 소프트웨어 수명주기 관리를 최소화할 수 있었습니다.

공급업체가 대부분의 일을 처리하면 우리는 시간을 절약할 수 있고 공급업체에 대한 신뢰성도 높아집니다."

Cytiva는 전 세계 모든 지역에서 다양한 의무를 준수하는 동시에 높은 수준의 보안을 유지하기 위해 노력하고 있습니다. 그 일환으로 사이버 보안 우수 관행을 유지해야 합니다.

앨런은 이렇게 설명합니다. "과거에는 액세스 요청을 처리하기 위해 더 많은 인원들이 물리 보안 시스템에 접근할 수 있도록 해야 했습니다. 프로비저닝 워크플로우는 모두 Genetec ClearID™ 내에서 자동화되므로 이제는 응용 프로그램 자체에 대한 액세스를 극히 제한된 시스템 사용자 그룹을 대상으로 한정할 수 있게 됐습니다. 그래서 보안 운영의 보안성과 대응 능력이 크게 향상되었습니다."

"보안 기업들은 사이버 보안 분야에서 별다른 가시적인 성과가 없거나 성과를 거뒀다 하더라도 필요한 정보를 갖추지 못한 경우가 많습니다. Genetec은 우리의 평가와 요청에 상당한 분량의 자료를 준비해 대응했고 아주 짧은 시간 안에 모든 일을 처리했습니다. 그때 Genetec이 준비되어 있을 뿐만 아니라 사이버 보안의 모든 측면에 대해 잘 알고 있다는 것을 확인할 수 있었습니다."

**–래리 앨런(Larry Allen)**
Cytiva 설비 • 보안 • 위기 관리용 기술 제품 책임자

# 강력한 사이버 보안 전략의 유지

"최고의 사이버 보안 우수 관행 가운데 최우선 순위에 두어야 할 것은 언제나 '인식'입니다. 사람들은 무엇이 좋고 나쁜 행동인지, 그리고 그에 대해 취해야 할 조치와 해서는 안 되는 조치를 알고 적절한 조치를 취하지 못했을 때 어떤 일이 초래될지에 대한 위험성을 인지해야 합니다. 또한 기업은 확실한 사고 대응 계획을 갖춰야 합니다. 아무리 방어 능력이 뛰어나도 사고는 발생할 수 있기 때문입니다. 피해를 경감시키고 조직의 데이터와 자산을 최대한 신속하게 보호할 수 있도록 적절한 대응 계획을 수립해야 합니다."

**–마티외 슈발리에(Mathieu Chevalier)**
Genetec 수석 보안 설계자

# 클라우드 및 하이브리드 클라우드를 활용한 사이버 보안 강화

물리 보안 시스템의 보안성을 강화하는 동시에 사이버 보안 우수 관행을 유지하기 위해서는 온프라미스 시스템에서 많은 추가 작업을 해야 합니다. 전 세계에 수백 개의 거점을 보유하고 있다면 복잡도는 급증합니다. 클라우드 서비스는 IT팀과 보안팀의 지속적인 유지관리 부담을 덜어주기 때문에 사이버 보안 대응 능력을 갖추기 위한 간편한 방법을 제시해 줍니다. 아래에서 자세히 살펴보겠습니다.

### 최신 사이버 보안 기능으로의 접근

클라우드 기반 물리 보안 솔루션을 사용하면 전송 중 상태와 저장 상태에서 암호화된 통신, 세분화된 개인정보보호 관리, 강력한 사용자 권한 부여 및 다양한 상태 모니터링 도구 등 내장된 최신 사이버 보안 기능에 언제든지 접근할 수 있습니다.

### 즉시 제공되는 수정사항 및 업데이트

Genetec 클라우드 서비스에서는 최신 버전과 수정사항이 사용 가능한 상태가 되면 즉시 접근할 수 있습니다. 이로써 물리 보안 시스템을 항상 최신 상태로 유지하고 취약점으로부터 보호할 수 있습니다.

### 데이터 중복성의 개선

Genetec 하이브리드 클라우드를 도입하면, 영상을 클라우드에 보관하면서 사내에 보안 시스템을 갖출 수 있습니다. 3개의 영상 파일 사본을 클라우드에 저장할 수 있기 때문에 더 높은 수준의 중복성과 가용성을 확보할 수 있는 것입니다.

**클라우드로의 확장을 고려하고 계신가요? 다음 자료들을 살펴보시기 바랍니다.**

솔루션
Genetec Stratocast™ Cloud VMS

하이라이트
클라우드 퍼스트: 패널 토론

백서
클라우드의 보안성

# 사이버 보안 전략을 효과적으로 유지하는 방법

물리 보안에서 사이버 보안을 유지한다는 것은 그저 공격을 방어하는 것에 그치는 것이 아니라, 고객 및 파트너와의 신뢰 관계를 확립하여 향후 몇 년에 걸쳐 성공적인 사업을 보장한다는 것을 의미합니다. 그러기 위해서는 데이터 보호 및 개인정보보호 대책을 지속적으로 분석하고 거듭 평가하며 갱신해야 합니다.
아래에서 자세히 살펴보겠습니다.

**위협 현황에 대한 인지**

사이버 위협 보호에 대한 정보를 파악하기 위해 IT 또는 보안 전문가에게만 의존해서는 안 됩니다. 변화하는 위험과 완화 전략에 뒤처지지 않도록 최선을 다해야 합니다. 즉, 직원들 역시 공통된 인식을 공유할 수 있도록, 해야 할 일과 해서는 안 되는 일에 대한 행동요령을 교육받아야 합니다.

**위험 평가 및 자산 재고조사의 수행**

적합한 사이버 보안 메커니즘을 마련할 수 있도록 환경의 구석구석을 파악해야 합니다. 컴퓨터, IoT 장치, 사용자, 데이터 유형 등의 목록을 작성하면 사이버 보안에 대한 보호를 보다 높은 수준으로 유지할 수 있습니다.

### 시스템 업데이트 및 패치를 최신 상태로 유지

패치를 적용함으로써 특히 보안 취약점을 해결하고 잠재적으로 큰 위험을 완화시킬 수 있습니다. 소프트웨어 또는 펌웨어 업데이트를 알리는 자동화된 도구를 고려하여 물리 보안 시스템을 견고하게 유지할 수 있는 기회를 놓치지 않도록 해야 합니다.

### 다중 인증의 시행

비밀번호는 쉽게 도난 또는 공유될 수 있기 때문에 비밀번호에만 의존해서는 안 됩니다. 최근의 사이버 위협을 제대로 방어하기 위해서는 다양한 인증 방식이 필요합니다. 비밀번호를 사용하는 경우 정기적으로 변경해야 합니다.

### 유출 사고 복구를 위한 계획 수립

기업의 목표는 이행하는 모든 업무에 사이버 위협에 대한 100%의 보호를 달성하는 것이지만 그것만으로는 공격자를 원천 차단하기에는 충분하지 않을 수 있습니다. 유출 사고 가능성을 감지하는 물리 보안 시스템을 갖추는 것은 필수지만 사이버 보안 사고 대응 계획을 수립하는 것 역시 중요합니다.

**더 많은 사이버 보안 자료가 필요하신가요? 다음 자료들을 확인하시기 바랍니다.**

영상
Security Center 우수 관행 수립

보고서
물리 보안 현황

하이라이트
Genetec 시스템 가용성 모니터링

# 사이버 보안 판도의 수준을 높일 수 있는 3가지 강화 도구

모든 물리 보안 시스템의 보호 수준이 동등하게 구축되지는 않습니다. 물론 일부 공급업체는 기본적인 정보를 제공하기도 하지만 오늘날의 위협 상황에 대처하려면 더 많은 정보가 필요합니다. Genetec은 기업이 사이버 보안 대응 능력을 마련할 수 있도록 지원하는 독자적인 강화 도구를 제공하기 위해 새로운 관점에서 생각합니다. 아래에서 자세히 살펴보겠습니다.

### 자동화된 규정 준수 기록 관리

귀사의 보안 시스템 상태를 간단히 확인할 수 있는 개요가 필요하신가요? 방법은 간단합니다. Genetec은 시스템의 보안성을 실시간으로 확인하는 동적 강화 도구인 Security Score 위젯을 제공합니다. 이 위젯은 가이드라인을 만들어 시스템의 다양한 요소들이 규정을 준수하는지 모니터링합니다. 이어서 규정 준수를 점수화하고 개선을 위한 권장사항을 제안합니다.

### 향상된 업데이트 예약

제품 업데이트는 종종 새로 발견된 취약점에 대한 중요한 수정사항을 제공합니다. 그러나 여전히 많은 기업들이 주요 업데이트가 어떻게 사이버 보안 대응 능력을 유지하고 있는지를 간과하고 있습니다. Genetec의 Firmware Vault는 새로운 IP 카메라 펌웨어가 배포될 때마다 알려주는 도구입니다. 클릭 몇 번만으로 업데이트를 다운로드받고 시스템에 배포하여 최신 방어 기능을 확보할 수 있습니다.

### 효율적인 비밀번호 관리

비밀번호 관리 정책은 장치의 보안성을 확보하는 데 필수입니다. Security Center에서 내장된 비밀번호 관리자를 통해 사용 중인 장치 제조업체의 규칙을 준수하는 강력하고 무작위적인 장치 비밀번호를 자동으로 생성할 수 있습니다. 또한 일정에 따라 또는 일괄적으로 카메라 암호를 자동으로 업데이트하도록 시스템을 구성할 수도 있습니다.

**이와 같은 독자적인 기능들을 자세히 살펴보고 싶으신가요? 다음 자료들을 확인하시기 바랍니다.**

제품
Genetec Firmware Vault 살펴보기

영상
사이버 보안 기능의 활성화

블로그
귀사의 카메라는 안전합니까?

# SYKES

## 직관적이고 자동화된 도구를 사용한 사이버 보안의 간소화

SYKES는 비즈니스 프로세스 아웃소싱 및 IT 지원 서비스를 선도하는 공급업체입니다. SYKES 팀은 전 세계적으로 Security Center 및 Genetec Streamvault™ 인프라 솔루션을 사용하여 현장 전체의 VMS 및 출입통제를 관리하고 있습니다.

글로벌 보안 책임자 슬론(Slone)은 말합니다. "우리는 Microsoft Azure 클라우드 환경 내에서 Genetec 플랫폼 전체를 운영하고 있기 때문에 우리가 처리해야 하는 물리적인 하드웨어는 없습니다. 우리가 사이버 보안 우수 관행을 충족할 수 있도록 Streamvault 어플라이언스가 이미 강화되어 있다는 점에 감사함을 느낍니다. 사무실에 설치되어 있는 기존의 DVR은 고유한 취약점을 갖고 있습니다. 우리는 Streamvault를 사용하면서 위협으로부터 보호받고 있음을 알 수 있었기에 우리 팀의 걱정거리 하나를 덜 수 있었습니다.

이제 SYKES는 보다 나은 상황에서 엄격한 감사 프로세스 및 중요 요구사항을 충족하고 다양한 규정 준수 표준을 준수할 수 있습니다. 또한 SYKES 팀은 내장된 상태 모니터링 도구를 사용하여 잠재적인 취약점이 발견되지 않을 것이라는 확신을 갖게 됐습니다.

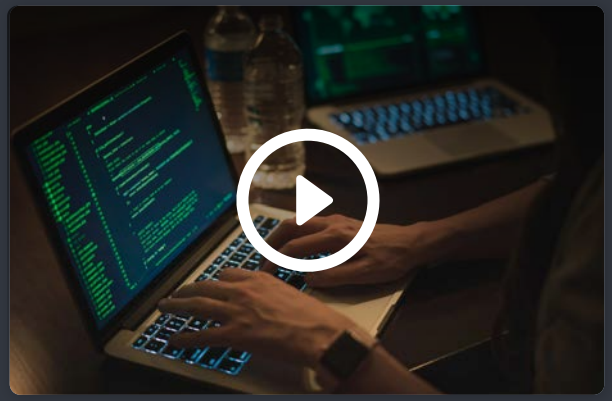
슬론은 이렇게 말합니다. "Security Center 플랫폼은 우리가 기존 시스템으로는 확인할 수 없었던 사항들을 보여줍니다. 예를 들어, 펌웨어를 업데이트해야 하는 장치의 수나 하드웨어 장애 발생 여부를 쉽게 확인할 수 있습니다. 이 덕분에 우리 팀은 능동적으로 시스템을 최신 상태로 유지하고 보안성을 갖추게 되었습니다."

"Genetec Security Center 플랫폼으로 마이그레이션한 후로 전 세계의 조직의 보안성 수준이 향상됐을 뿐만 아니라 데이터 보호 및 물리 보안에 적극적으로 접근하고 있음을 브랜드 파트너에게 보여주고 있습니다."

**–크리스토퍼 슬론(Christopher Slone)**
SYKES 글로벌 보안 사이버 운영 이사

# 5분을 투자할 가치가 있는 사이버 보안 동향에 관한 영상들

사이버 보안과 관련하여 최신 동향과 기능에 대해 학습하는 시간을 통해 큰 도움을 받을 수 있습니다. Genetec 유튜브 채널을 통해 데이터 보호 동향, 권장 도구 및 전략에 대한 최신 정보를 확인하실 수 있습니다.



사이버 위험 평가 및 경감의 중요성

사이버 공격으로부터 보안 하드웨어 보호

물리 보안 시스템의 상태 및 가용성을 유지하는 방법

# Genetec과 함께하는 데이터 보호 전략의 구축

사이버 범죄자의 공격은 갈수록 교묘해지고 있습니다. 이로 인해 업계의 조직들은 사이버 보안 대책, 표준 및 인증을 면밀히 검토해야 한다는 압박을 압박을 받고 있습니다. 이는 물리 보안 시스템을 넘어 공급망 생태계 전체로 이어집니다. 보호 전략이 작년까지는 공격자들을 효과적으로 차단했다 하더라도 미래에는 충분하지 않을 수 있기 때문입니다.

Genetec은 가장 중요한 정보를 보호할 수 있도록 규정을 준수하고 사이버 보안 대응 능력이 뛰어난 솔루션을 구축하고 있지만 여기서 그치지 않습니다. Genetec은 새로운 사이버 위협의 동향을 파악하고 파트너 및 고객과 협력하여 사이버 보안 대책을 발전시키고 있습니다. 그럼으로써 사이버 보안 태세를 항상 강력하게 유지할 수 있습니다.

데이터 보호 및 개인정보보호에 대한 Genetec의 접근법에 대해 자세히 알고 싶으신가요? Genetec Trust Center에서 확인하시기 바랍니다.

## 사이버 보안 관행을 표준화할 준비가 되셨나요?

Genetec의 융합 보안 접근법을 살펴보시기 바랍니다.

Genetec과 Genetec의 제품에 대해 자세히 알고 싶으시다면 genetec.com을 방문하세요.

**Genetec Inc.**
Genetec
info@genetec.com
@genetec

업데이트 일자: 2022-09-20