02 급진적 변화의 시점에서

2. 급진적 변화의 시점에서

2.1 2025년 사이버보안 업계의 주요 화두

2.1.1 AI와 머신러닝의 양면성

2025년 사이버 보안의 가장 중요한 화두 중 하나는 인공지능과 머신러닝의 양면성입니다. AI는 위협 탐지와 보안 자동화에 크게 기여하고 있지만, 동시에 공격자들 또한 AI를 무기화하여 새로운 수준의 위협을 만들어내고 있습니다. 딥페이크 기술은 CEO 사기나 음성 피싱에 활용되고 있으며, AI가 생성한 피싱 이메일은 정교함과 대규모 확산력을 동시에 확보하였습니다. 또한 챗봇을 이용한 자동화된 사회공학적 기법과 AI 기반의 패스워드 크래킹은 계정 탈취 공격의 장벽을 점점 낮추고 있습니다. 이와 같이, AI는 더 이상 방어만의 도구가 아니라 공격자에게도 동일하게 활용되는 양날의 검으로, 보안 체계 전반의 재정립을 요구하는 핵심 변수로 부상하였습니다.

2025년사이버보안업계의주요화두

급진적변화의시점에서

AI와 머신러닝의 양면성

⚔️ **AI를 활용한 공격의 진화**
하지만 공격자들도 AI를 적극 활용하고 있어 새로운 위협이 등장

AI 기반 공격 기법들:
- **딥페이크 기술:** CEO 사기, 음성 피싱 등에 활용
- **AI 생성 피싱 이메일:** 문법적으로 완벽하고 개인화된 피싱 메일 대량 생성
- **자동화된 소셜 엔지니어링:** 챗봇을 이용한 대화형 사기
- **AI 기반 패스워드 크래킹:** 딥러닝을 활용한 효율적인 비밀번호 추측

크리덴셜 스터핑의 낮아지는 장벽

SKT Enterprise 20

※ AI 공격 기법

- 딥페이크 (Deepfake)

o 인공지능을 이용해서 실제와 구분하기 어려운 가짜 영상이나 음성을 만드는 기술입니다. 유명인의 얼굴을 다른 사람의 몸에 합성하거나, 실제로 하지 않은 말을 하는 것처럼 만들 수 있습니다. 처음에는 엔터테인먼트 목적으로 시작되었지만, 현재는 정치적 조작이나 사기 범죄에 악용되고 있습니다. 특히 CEO나 임원을 사칭한 보이스 피싱이 급증하고 있습니다.

- 소셜 엔지니어링

o 기술적 해킹보다는 사람의 심리를 이용해서 정보를 빼내거나 시스템에 침입하는 기법입니다. 예를 들어 IT 직원을 사칭해서 전화를 걸어 비밀번호를 물어보거나, 긴급상황을 연출해서 보안 절차를 우회하도록 유도합니다. 아무리 기술적 보안이 완벽해도 사람이 속으면 무용지물이 되므로, 직원 교육이 매우 중요합니다.

- 크리덴셜 스터핑

o 한 사이트에서 유출된 아이디와 비밀번호를 다른 사이트에서도 자동으로 시도해보는 공격입니다. 많은 사람들이 여러 사이트에서 같은 비밀번호를 사용하는 습관을 악용한 것입니다. AI를 이용하면 성공 확률이 높은 조합을 우선적으로 시도해서 효율을 높일 수 있습니다. 이를 방지하려면 사이트마다 다른 비밀번호를 사용하거나 2단계 인증을 설정해야 합니다.

- AI 생성 피싱 이메일

o ChatGPT 같은 대화형 AI를 이용해서 매우 자연스럽고 설득력 있는 피싱 이메일을 대량으로 생성하는 기법입니다. 과거의 피싱 이메일은 문법 오류나 어색한 표현 때문에 쉽게 구분할 수 있었지만, AI가 만든 이메일은 진짜와 구분하기 매우 어렵습니다. 개인 정보를 수집해서 맞춤형 피싱 이메일을 만드는 것도 가능해졌습니다.

※ **AI** 방어 기술

- **AI/ML** 기반 위협 탐지

o 머신러닝 알고리즘을 이용해서 정상적인 네트워크 트래픽이나 사용자 행동 패턴을 학습한 후, 이상한 활동을 자동으로 탐지하는 기술입니다. 기존의 시그니처 기반 탐지는 알려진 공격만 막을 수 있었지만, AI 기반 탐지는 새로운 형태의 공격도 발견할 수 있습니다. 다만 오탐(정상을 비정상으로 판단)과 미탐(비정상을 정상으로 판단)의 균형을 맞추는 것이 어려운 과제입니다.

- 행동 분석 **(Behavioral Analytics)**

o 사용자나 시스템의 평상시 행동 패턴을 학습해서 baseline을 만든 후, 평소와 다른 행동을 하면 경고를 발생시키는 기술입니다. 예를 들어 평소 오전 9시에 출근해서 오후 6시에 퇴근하는 직원이 새벽 3시에 로그인하면 의심스러운 활동으로 판단합니다. 내부자 위협이나 계정 탈취 공격을 탐지하는 데 매우 효과적입니다.

- 자동화된 대응 **(Automated Response)**

o 위협이 탐지되면 사람의 개입 없이 자동으로 대응 조치를 실행하는 기술입니다. 예를 들어 악성코드가 발견되면 해당 PC를 네트워크에서 자동으로 격리하고, 관련 파일을 삭제하고, 담당자에게 알림을 보냅니다. 공격의 속도가 빨라지면서 사람의 반응 속도로는 대응이 어려워졌기 때문에 필수적인 기술이 되었습니다.

2.1.2 제로 트러스트 보안 모델의 확산

제로 트러스트는 "절대 신뢰하지 말고, 항상 검증하라"는 철학에 기반한 보안 모델입니다. 과거에는 기업 내부 네트워크를 안전한 영역으로 간주했지만, 내부자 위협과 APT 공격이 증가하면서 이러한 전제가 무너졌습니다. 따라서 모든 사용자와 기기를 잠재적 위험 요소로 보고, 접속과 행위마다 지속적으로 검증하는 것이 기본 원칙이 되었습니다. 특히 코로나19 이후 재택근무와 클라우드 사용이 급격히 확산되면서, 경계가 사라진

초연결 환경에서 제로 트러스트는 기존 성벽형 보안을 대체하는 현대 보안의 핵심 패러다임으로 자리잡게 되었습니다.

2025년 사이버보안업계의주요 화두

급진적변화의시점에서

제로트러스트보안모델의확산

🎯 "절대 신뢰하지 말고, 항상 검증하라"

코로나19로 인한 원격근무 확산과 클라우드 전환 가속화로 기존의 성벽 방어 (Perimeter Defense) 모델이 한계를 드러내면서 제로 트러스트가 새로운 패러다임으로 주목받고 있음.

제로 트러스트의 핵심 원칙:

- **최소 권한 원칙**: 업무에 필요한 최소한의 권한만 부여
- **지속적 검증**: 사용자와 디바이스를 지속적으로 인증하고 권한 검증
- **마이크로 세그멘테이션**: 네트워크를 세밀하게 분할하여 측면 이동 차단
- **암호화 우선**: 모든 통신과 데이터를 암호화

국내외 동향:

- 미국 정부는 2024년까지 모든 연방 기관에 제로 트러스트 아키텍처 도입 의무화
- 국내 공공기관과 대기업들도 제로 트러스트 도입을 적극 검토 중

얼마나 더 막아낼 수 있을까?

2.1.3 OT/IoT 보안의 급부상

2025년 사이버보안업계의주요 화두

급진적변화의시점에서

🏭 OT/IoT 보안의급부상

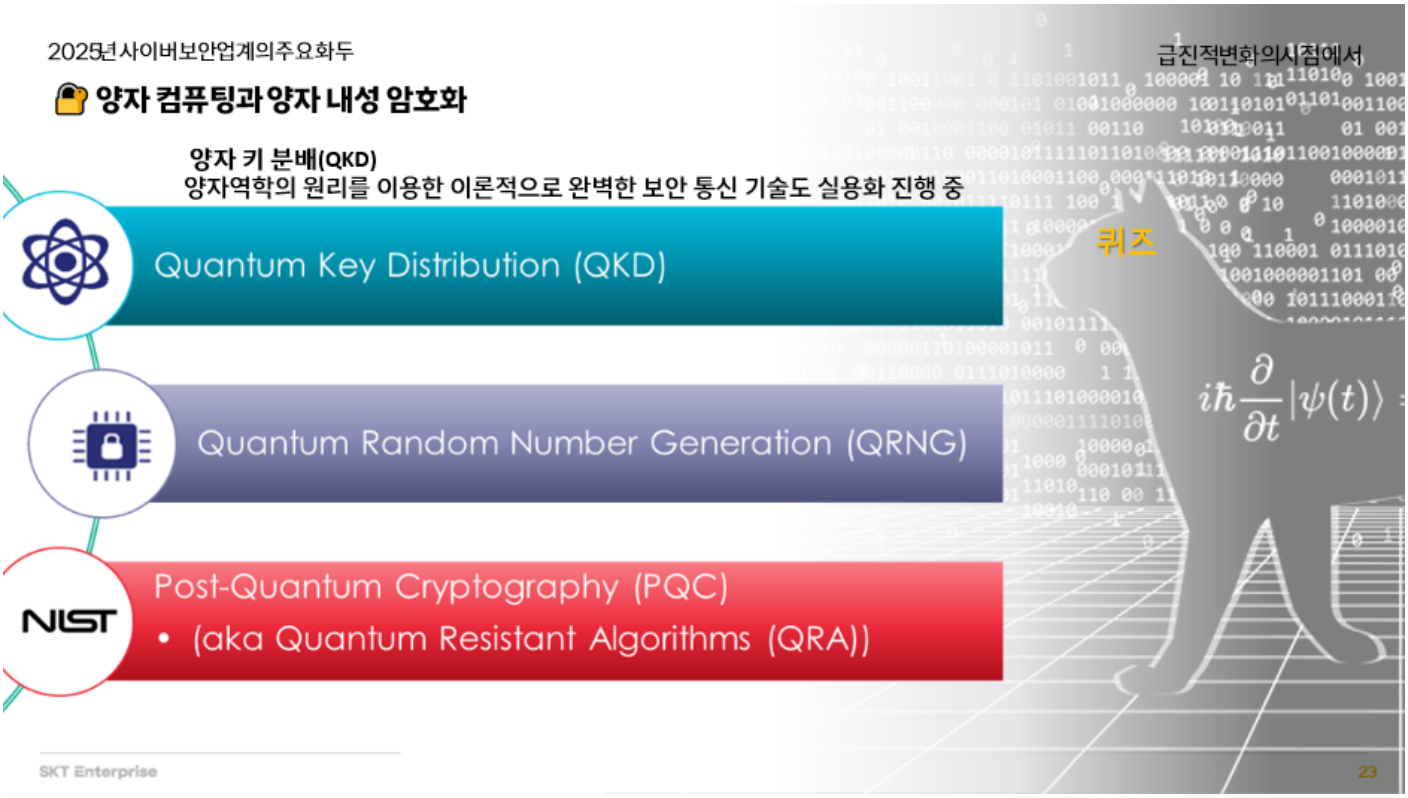
DDoS가 과거에는 매우 비싼 공격

오늘 날은 가장 값싸고 효과적인 공격 방법

DDoS(Distributed Denial of Service, 분산 서비스 거부 공격)는 여러 대의 컴퓨터나 IoT 장치들을 동시에 동원하여 특정 서버나 네트워크에 대량의 트래픽을 발생시킴으로써 정상적인 서비스 이용을 방해하는 공격 유형입니다.

과거에는 대규모 트래픽을 만들어내려면 많은 비용과 자원이 필요했기 때문에 DDoS 공격은 매우 비싼 공격 방식이었습니다. 그러나 오늘날에는 수많은 IoT 기기들이 인터넷에 연결되고, 기본 보안 설정이 취약한 상태로 방치되면서 손쉽게 봇넷(해커가 원격 조종하는 감염 기기들의 네트워크)으로 악용되고 있습니다. 그 결과 **DDoS**는 가장 저렴하고 효과적인 공격 수단으로 자리잡게 되었습니다.

2.1.4 양자 컴퓨팅과 양자 내성 암호화


2025년 사이버보안업계의 주요화두

급진적변화의시점에서

양자 컴퓨팅과 양자 내성 암호화

양자 키 분배(QKD)
양자역학의 원리를 이용한 이론적으로 완벽한 보안 통신 기술도 실용화 진행 중

Quantum Key Distribution (QKD)

Quantum Random Number Generation (QRNG)

Post-Quantum Cryptography (PQC)
- (aka Quantum Resistant Algorithms (QRA))

- **QKD (**양자 키 분배**)**

o 양자역학의 원리를 이용해서 절대적으로 안전한 암호화 키를 전달하는 기술입니다. 만약 누군가 중간에서 키를 엿보려고 하면 양자 상태가 변화해서 즉시 발각됩니다. 현재는 실험실 수준이지만, 상용화되면 완벽한 보안 통신이 가능해집니다. 다만 거리 제한과 높은 비용이 해결해야 할 과제입니다.

- **PQC (**양자 내성 암호**)**

o 미래에 양자컴퓨터가 상용화되면 현재의 RSA, ECC 등 암호화 기술이 모두 뚫릴 수 있습니다. 이에 대비해서 양자컴퓨터로도 뚫기 어려운 새로운 암호화 알고리즘을 개발하는 것이 PQC입니다. 미국 NIST에서 표준화를 진행하고 있으며, 양자컴퓨터 시대에 대비한 필수 기술입니다.

- **QRNG (양자 난수 생성)**

o 양자역학의 불확정성 원리를 이용해서 완전한 난수를 생성하는 기술입니다. 기존의 컴퓨터 난수는 사실 규칙에 따라 만들어지는 '가짜 난수'이지만, QRNG는 물리적으로 예측 불가능한 진짜 난수를 만들 수 있습니다. 암호화에서 난수의 품질은 보안 강도와 직결되므로 매우 중요한 기술입니다.

2.1.5 랜섬웨어의 진화와 대응

2025년사이버보안업계의주요화두

급진적변화의시점에서

랜섬웨어의 진화와 대응

랜섬웨어-as-a-Service (RaaS)
랜섬웨어가 하나의 비즈니스 모델로 정착하면서 기술이 없는 범죄자들도 쉽게 랜섬웨어 공격을 수행.

RaaS의 특징:
- **프랜차이즈 모델**: 랜섬웨어 개발자가 공격자에게 도구와 인프라 제공
- **고객 서비스**: 피해자 상담, 복호화 지원 등 '서비스' 제공
- **수익 분배**: 몸값의 일정 비율을 개발자와 공격자가 분배

이중 갈취(Double Extortion)
단순히 파일을 암호화하는 것에서 벗어나 데이터를 유출한 후 공개하겠다고 협박하는

랜섬웨어 대응 전략:
- **백업의 중요성**: 3-2-1 백업 규칙 (3개 복사본, 2개 매체, 1개 오프라인)
- **사고 대응 계획**: 평상시 랜섬웨어 대응 절차 수립 및 훈련
- **사이버 보험**: 랜섬웨어 피해 복구 비용 보장

랜섬웨어 감염 관련 신고 40% 내외

SKT Enterprise

24

오늘날 랜섬웨어는 단순한 공격 수단을 넘어서, 서비스화된 비즈니스 모델로 발전하고 있습니다. 이를 통해 기술력이 없는 범죄자들도 손쉽게 공격을 수행할 수 있게 되었습니다. 또한 단순히 파일을 암호화하는 것에 그치지 않고, 데이터를 유출해 공개하겠다고 협박하는 이중 갈취 수법도 등장하였습니다.

이에 대응하기 위한 기업들의 전략으로는 3-2-1 원칙에 따른 백업, 평상시 랜섬웨어 대응 절차 점검과 훈련, 그리고 사이버 보험이 제시되고 있습니다. 실제로 국내 보안 사고 신고의 40%가 랜섬웨어 감염과 관련된 만큼, 지금은 랜섬웨어에 대한 경각심과 사전 대비가 중요한 시점입니다.

※ 랜섬웨어 생태계

- **RaaS (서비스형 랜섬웨어)**

o 랜섬웨어를 마치 일반 소프트웨어 서비스처럼 제공하는 비즈니스 모델입니다. 랜섬웨어 개발자가 기술을 제공하고, 실제 공격은 다른 범죄자들이 수행한 후 수익을 나눠 갖습니다. 이로 인해 기술적 지식이 부족한 범죄자들도 쉽게 랜섬웨어 공격을 할 수 있게 되었습니다. 사이버 범죄의 '산업화'를 보여주는 대표적 사례입니다.

- **Affiliate Model (제휴 모델)**

o 랜섬웨어 조직이 직접 공격하지 않고 다른 해커 그룹에게 도구와 인프라를 제공한 후 수익을 분배하는 방식입니다. 개발자는 기술에 집중하고, 공격자는 침투에 집중하는 전문화된 분업 구조입니다. 이런 모델로 인해 랜섬웨어 공격의 효율성과 성공률이 크게 높아졌습니다.

2.1.6 사이버보안 인력 부족 문제

2025년사이버보안업계의주요화두

급진적변화의시점에서

👥 사이버보안 인력 부족 문제

📊 심각한 인력 난
전 세계적으로 사이버보안 전문가가 350만 명 부족한 상황이며,
국내도 마찬가지로 심각한 인력 부족에 직면해 있습니다.

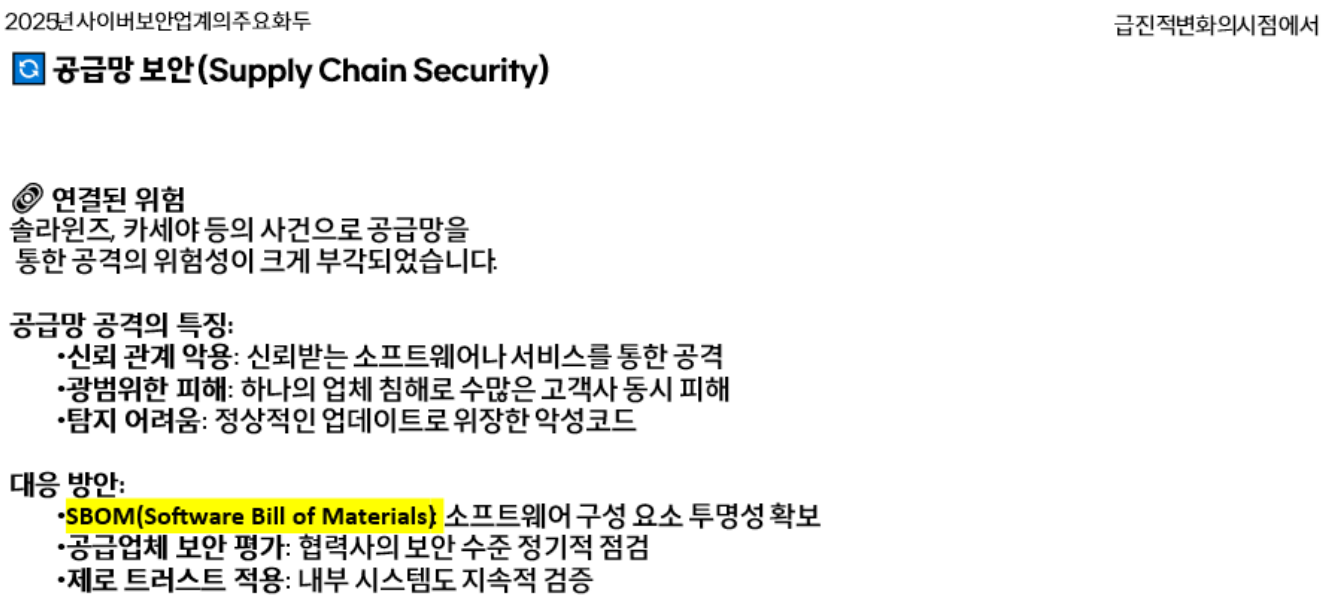
인력 부족의 원인:
- **높은 수준의 보안 인력은 Computer Science 인력 중 최고 등급**

해결 방안:
- **없음**

1 VS 100의 방어 구조

SKT Enterprise

사이버보안 인력 부족의 근본 원인은 단순합니다. 보안은 IT 기술 중에서도 가장 높은 수준의 전문성을 필요로 하는 분야이며, 이로 인해 숙련된 전문가를 충분히 확보하기가 매우 어려운 실정입니다.



2.1.7 공급망 보안

2025년 사이버보안 업계의 주요 화두

급진적 변화의 시점에서

🔄 공급망 보안(Supply Chain Security)

🔗 연결된 위험
솔라윈즈, 카세야 등의 사건으로 공급망을
통한 공격의 위험성이 크게 부각되었습니다.

공급망 공격의 특징:
- **신뢰 관계 악용**: 신뢰받는 소프트웨어나 서비스를 통한 공격
- **광범위한 피해**: 하나의 업체 침해로 수많은 고객사 동시 피해
- **탐지 어려움**: 정상적인 업데이트로 위장한 악성코드

대응 방안:
- **SBOM(Software Bill of Materials)**: 소프트웨어 구성 요소 투명성 확보
- **공급업체 보안 평가**: 협력사의 보안 수준 정기적 점검
- **제로 트러스트 적용**: 내부 시스템도 지속적 검증

SKT Enterprise

26

공급망 공격은 한 번의 침투로 수많은 고객사와 파트너사에 동시에 피해를 줄 수 있는 가장 파급력 있는 사이버 위협 중 하나입니다. 공격자는 신뢰받는 소프트웨어 업데이트나 협력사의 서비스를 악용하기 때문에 피해 기업은 정상적인 행위로 오인하기 쉽고, 이로 인해 피해 범위가 기하급수적으로 확대됩니다.

따라서 단일 기업의 보안 노력만으로는 충분하지 않으며, 생태계 전체의 투명성과 신뢰성 확보가 핵심 과제로 떠올랐습니다. 이를 위해 SBOM을 통한 소프트웨어 구성 요소의 가시성 확보, 협력사 보안 수준에 대한 정기적 검증, 그리고 제로 트러스트 원칙에 기반한 지속적 모니터링이 필수적입니다.

※ SBOM (소프트웨어 부품 명세서)

- 소프트웨어에 어떤 구성 요소들이 포함되어 있는지 투명하게 공개하는 것입니다. 현대 소프트웨어는 수많은 오픈소스 라이브러리를 조합해서 만들어지는데, 이 중 하나라도 취약점이 있으면 전체가 위험해집니다. SBOM을 통해 어떤 부품을 사용했는지 알면 취약점 발견 시 빠르게 대응할 수 있습니다. 미국 정부에서 의무화를 추진하고 있습니다.

2.1.7.1 용어집 #7

① OT/IoT 보안

o 운영기술 (OT)과 사물인터넷 (IoT)의 디지털화로 급부상한 보안 영역

o 제조업, 에너지, 교통 등 핵심 인프라를 보호하기 위한 대응 분야

o 물리 세계와 사이버 세계가 융합되는 새로운 보안 과제

② RaaS (Ransomware-as-a-Service)

o 서비스 형태로 제공되는 랜섬웨어 기반 사이버 범죄 모델

o 개발자와 실행자가 분업 구조로 수익을 나누는 비즈니스 형태

o 기술력이 없는 범죄자도 쉽게 공격을 수행할 수 있는 체계

③ SBOM (Software Bill of Materials)

o 소프트웨어 구성 요소를 투명하게 공개하는 형식서

o 공급망 공격 대응을 위해 필수적으로 요구되는 정보 체계

o 취약점 진단과 패치 시 빠른 대응을 가능하게 하는 핵심 자료

④ QKD (Quantum Key Distribution)

o 양자 얽힘 원리에 기반한 절대 보안 통신 기술

o 양자컴퓨터 시대에도 유지 가능한 보안 체계

o 기존 암호화 방식의 한계를 극복할 차세대 열쇠

⑤ PQC (Post-Quantum Cryptography)

o 양자컴퓨터 연산 능력에도 안전성을 유지하는 암호 기술

o 현존하는 RSA, ECC 암호 체계를 대체할 차세대 후보군

o NIST에서 진행 중인 표준화 절차

⑥ QRNG (Quantum Random Number)

o 양자의 불확정성을 활용한 난수 생성 방식

o 예측 불가능하고 완전한 무작위성을 보장하는 기술

o 암호화 보안의 기반이 되는 핵심 요소

※ 양자 보안 기술

- QKD를 통한 양자 키 분배
- PQC를 통한 양자 내성 암호
- QRNG를 통한 양자 난수 생성

2.2 Gartner 2025

2.2.1 2025년 사이버보안 9대 트렌드

Gartner 2025

Top 9 Trends in Cybersecurity for 2025

변화 가능화
(Enabling transformation)

회복력 내재화
(Embedding resilience)

변화 가능화 및 회복력 내재화
(Enabling transformation and embedding resilience)

SKT Enterprise

Enabling transformation

급진적변화의시점에서

1 GenAI driving data security programs

2 Collaborative cyber-risk management

3 Managing machine identities

Embedding resilience

4 Transitioning to cyber resilience

5 Cybersecurity technology optimization

6 CISO and security team well-being

Enabling transformation and embedding resilience

7 Tactical AI

8 Extending the value of security behavior and culture programs

9 Managing third-party cybersecurity risks

변화 가능화 (Enabling transformation)

① GenAI가 데이터 보안 프로그램을 주도

o 제 3자 서비스, 비즈니스 애플리케이션 또는 맞춤형 아키텍처를 통한 GenAI에 대한 수요가 조직들이 AI 기반 가치를 추구하면서 증가하고 있습니다. 그러나 데이터 정확성, 개인정보보호, 컴플라이언스에 대한 우려가 채택을 저해하고 있습니다.

② 협력적 사이버 위험 관리

o 비즈니스 기술자들이 독립적으로 기술 투자 결정을 내리면서, 전통적인 중앙집중식 사이버 위험 관리는 확장에 어려움을 겪고 있으며, 이로 인해 마찰이 발생하고 민첩성이 감소하고 있습니다. GenAI와 같은 혁신적 기술의 비즈니스 채택은 사이버 위험 환경을 급속히 발전시키고 있습니다.

③ 머신 아이덴티티 관리

o 클라우드 서비스, 자동화, DevOps, AI의 증가로 인해 물리적 디바이스와 소프트웨어 워크로드를 위한 머신 계정과 자격 증명 사용이 확대되면서, 머신의 비인간 아이덴티티와 액세스 관리가 점점 더 중요해지고 있습니다.

회복력 내재화 (Embedding resilience)

④ 사이버 회복력으로의 전환

o 보안 및 위험 관리 (SRM) 리더들은 예방 중심 사고방식에서 사이버 회복력에 집중하는 방향으로 전환하고 있습니다. 이는 "만약이 아닌 언제"라는 사고방식을 채택하고 사건이 불가피하다는 것을 수용함으로써 영향을 최소화하고 적응력을 향상시키는 데 중점을 둡니다.

⑤ 사이버보안 기술 최적화

o 사이버보안 기술 옵션이 확대되는 가운데 대형 벤더들이 광범위한 플랫폼으로의 통합을 추진하면서 SRM 리더들은 긴장에 직면하고 있습니다. 이러한 플랫폼들은 복잡성을 줄이고 더 많은 위협을 다루는 것을 목표로 하지만, 종종 포인트 솔루션과 중복되어 잠재적 비효율성과 공백을 메우기 위한 추가 도구의 필요성을 야기합니다.

⑥ CISO 및 보안팀 웰빙

o 스킬 부족 산업에서 SRM 리더와 보안팀의 번아웃은 주요 우려사항입니다. 미래 지향적인 SRM 리더들은 정신 건강을 강조하며, 자신의 스트레스 관리를 우선시하고 회복력 향상을 위해 팀 웰빙 이니셔티브에 투자하고 있습니다.

변화 가능화 및 회복력 내재화 **(Enabling transformation and embedding resilience)**

⑦ 전술적 AI

o SRM 리더들은 처음에 GenAI 과대광고로 인해 AI에 실망했지만, 이후 더 좁고 측정 가능한 사용 사례에 집중하는 방향으로 전환했습니다. 이러한 더 전술적인 구현은 AI 도구를 기존 메트릭 및 이니셔티브와 일치시켜 가시성을 향상시키고 AI 투자의 실제 가치를 입증합니다.

⑧ 보안 행동 및 문화 프로그램의 가치 확장

o 보안 행동 및 문화 프로그램 (SBCP)은 현재 조직에게 중추적입니다. SRM 리더들은 사이버보안 향상을 위해 이러한 프로그램을 가치 있게 여기며, 인간 수준의 위험 이해와 소유권에 집중하여 보안을 조직 문화에 내재화하는 전략적 전환을 이끌고 있습니다.

⑨ 제 3자 사이버보안 위험 관리

o GenAI 도구를 사용하는 제 3자에 대한 의존도 증가는 강력한 대응 및 복구 전략의 필요성을 부각시킵니다. 진보적인 SRM 리더들은 제 3자 관계를 중단하거나 종료하는 정책에 집중하고 비즈니스 스폰서와 협력하여 위험을 관리하고 통제 구현을 안내합니다.

Revision #2
Created 27 September 2025 04:22:13 by 최주용
Updated 27 September 2025 04:53:24 by 최주용