한국자동차공학회
The Korean Society of Automotive Engineers

자동차 사이버보안연구회
TI 뉴스레터

Published by FESCARO
in collaboration with AUTO-ISAC

- 2026년 2호 -

사보연 TI 뉴스레터 2호에서는 확산되는 **사이버 위협 환경 속에서 요구되는 대응 체계의 전환**을 조명합니다. AI 기반 공격이 가속화되는 상황에서 기술 중심 대응을 넘어 조직과 거버넌스 관점의 체계적 대응 전략을 다루며, 2026년을 준비하기 위한 **사이버보안 리포트와 인사이트 총 10종**을 소개합니다.

1. 사이버 보안 보고서 2026
2. 2026년 사이버 보안 예측: AI 군비 경쟁과 악성코드 자율화
3. 공격 방식의 진화: 2026년 기업을 보호하는 3가지 방법
4. 랜섬웨어 고도화 시대의 CISO 전략
5. 2025 교훈: 시스템 보안을 넘어 의사결정 보안으로
6. 취약점 관리 대응력 향상
7. 자동화와 AI 시대의 위협 탐지
8. AI가 사이버 방어의 주도권을 쥐게 해서는 안 되는 이유
9. TARA는 추적 가능한가요? 품목 정의부터 ALM까지의 핵심 평가
10. 사이버 보안 개념(ISO/SAE 21434)이 차량에만 국한될 수 없는 이유: 사이버 보안 관리자를 위한 고려 사항

1. 사이버보안 보고서 2026

by CHECK POINT

체크포인트 리서치는 전 세계 네트워크 및 환경에서 실제 공격, 취약점, 공격자 인프라 및 새로운 기술을 지속적으로 조사합니다. 2026년 사이버 보안 보고서는 2025년 한 해 동안 진행된 연구 결과를 종합하여 현재의 위협 환경과 2026년의 전망에 대한 명확하고 데이터 기반의 분석을 제공합니다. 이 보고서는 **오늘날 위협 환경을 형성하는 가장 중요한 변화**들을 강조합니다.

💬 애널리스트 코멘트 : 2025년에는 사이버 공격이 지정학적 갈등과 더욱 밀접하게 연관될 것으로 예상 되며, 공격자들은 물리적 세계의 사건들과 함께 사이버 스파이 활동, 혼란 조성 캠페인, 영향력 행사 작전을 조율할 것입니다.

자세히 보기

---

2. 2026년 사이버 보안 예측: AI 군비 경쟁과 악성코드 자율화

by DARKREADING

2026년에는 AI 기반 사이버 보안 군비 경쟁이 더욱 치열해질 것입니다. 공격자들은 자율형 악성코드와 고도화된 AI 기술을 활용하여 방어자들을 앞지르려 할 것이고, 보안팀은 업계의 벤더 통합과 플랫폼화가 가속화되는 가운데 진화하는 위협에 대응하기 위해 더욱 정교한 AI 도구를 도입할 것입니다. 사이버 보안 전문가들이 한데 모여 다음 해에 무슨 일이 일어날지 예측하는 시기가 돌아왔습니다. 하지만 대부분의 예 측은 기껏해야 약간 빗나가거나 최악의 경우 완전히 틀릴 가능성이 높습니다. 그럼에도 불구하고, 예리한 독자라면 여러 전문가들의 의견에서 공통적으로 나타나는 경향을 살펴보는 것이 좋습니다. 이러한 경향은 전반적인 방향을 정확하게 예측할 가능성이 높기 때문입니다.

💬 애널리스트 코멘트 : 공격자들은 고도화된 AI를 활용하여 피싱, 딥페이크 제작, 취약점 악용 등을 대 규모로 자동화하고 있으며, 방어자들은 위협 탐지 및 자동 대응을 위해 AI 기반 보안 도구를 배포하고 있습니다.

자세히 보기

---

3. 공격 방식의 진화: 2026년 기업을 보호하는 3가지 방법

by THE HACKER NEWS

사이버 범죄자들은 매년 기업으로부터 돈과 데이터를 훔치는 새로운 수법을 찾아냅니다. 기업 네트워크 에 침입하여 민감한 데이터를 추출하고 다크 웹에서 판매하는 것은 이제 손쉬운 수익원이 되었습니다. 하지만 2025년에는 중소기업(SMB)을 대상으로 한 데이터 유출 사고가 잇따르면서 사이버 범죄자들이 어떤 유형의 기업을 표적으로 삼는지에 대한 기존의 인식이 흔들리고 있습니다. 이 글에서는 **2025년 주요 데이터 유출 사고에서 얻은 교훈과 더불어 중소기업이 내년에 스스로를 보호할 수 있는 가장 효과적인 방법**을 제시합니다.
2025년 이전에는 풍부한 자원을 보유한 대기업이 해커들의 주요 공격 대상이었습니다. 중소기업은 공격 가치가 낮기 때문에 사이버 공격에 취약하지 않다고 여겨졌습니다. 그러나 데이터 유출 관측소(Data Breach Observatory)의 새로운 보안 연구에 따르면 이러한 상황이 바뀌고 있습니다. 이제 중소기업이 사이버 공격의 주요 표적이 될 가능성이 높아지고 있습니다. 이러한 전술 변화는 대기업들이 사이버 보안 에 투자하고 몸값 지불을 거부하는 데서 비롯되었습니다. 사이버 범죄자들은 대기업을 공격해서는 가치있는 정보를 얻어낼 가능성이 낮다고 판단하여, 대신 중소기업을 공격 대상으로 삼고 있습니다.

💬 애널리스트 코멘트 : 사이버 범죄자들이 사이버 보안에 투자하는 대기업에서 방어 자원이 부족한 중 소기업으로 공격 대상을 옮기면서, 2025년에는 중소기업이 전체 데이터 유출 사고의 70.5%를 차지할 것 으로 예상됩니다.

자세히 보기

---

4. 랜섬웨어 고도화 시대의 CISO 전략

by DARKREADING

2025년 초, 랜섬웨어와의 전쟁에서 전환점을 맞이한 듯 보였습니다. 블록체인 분석 결과, 랜섬웨어에 대한 암호화폐 지불액이 크게 감소하여 2022년 이후 처음으로 수익이 줄어든 것으로 나타났습니다. 하지만 안타깝게도 이러한 낙관적인 전망은 오래가지 못했습니다. 위협 행위자들은 적응력이 뛰어나며, 궁지에 몰리면 더욱 위험해질 수 있습니다. 최근 Semperis의 연구에 따르면 조사 기간 동안 발생한 랜섬웨어 공격의 2/5에서 공격자가 임원에게 신체적 위해를 가하겠다고 위협했습니다. 또한 성공적으로 침해당한 기업의 2/3 이상이 결국 협박범에게 몸값을 지불했습니다. 이러한 **기업 보안 악몽에서 벗어날 수 있는 유일한 길은 사이버 복원력을 강화하는 것**입니다.

💬 애널리스트 코멘트 : Active Directory, Entra ID, Okta를 포함한 ID 관리 시스템이 조사 대상 랜섬 웨어 공격의 83%에서 침해당했습니다. 공격자는 탈취한 자격 증명을 사용하여 네트워크를 이동하고, 접 근 권한을 높이고, 장기간 접근을 유지합니다.

자세히 보기

---

5. 2025 교훈: 시스템 보안을 넘어 의사결정 보안으로

by DARKREADING

2026년이 시작되면서 2025년에 대한 불편한 깨달음이 계속 떠오릅니다. 우리는 공격자를 잘못 이해한 것이 아닙니다. 우리는 실패를 잘못 이해했습니다. **작년의 피해 대부분은 정교한 기술이나 예상치 못한 적에게서 비롯된 것이 아닙니다.** 평범한 시스템이 조용히 무너지면서 사람들의 의사결정 방식이 바뀌었기 때문입니다. 시스템은 계속 작동했고, 대시보드는 녹색으로 표시되었습니다. 하지만 신뢰는 무너졌고, 판단력은 흐려졌으며, 사람들은 믿을 만한 정보 없이 행동해야 했습니다. 진정한 피해는 바로 그 지점에서 발생했습니다. Change Healthcare에 대한 랜섬웨어 공격은 미국 의료 시스템 전반의 청구 처리 시스템을 마비시켰습니다. 시스템은 결국 복구되었지만, 병원과 의료 제공자들은 불완전한 데이터, 지연된 진료비 지급, 그리고 수동적인 해결책을 사용하며 몇 주를 보내야 했습니다.

💬 애널리스트 코멘트 **:** 2025년에 발생한 여러 사이버 사고에서 공통적인 패턴이 발견되었습니다. 관리 자 자격 증명 공유, 만료되지 않는 비상 접근 권한, 그리고 보안 제어를 우회하는 서비스 계정 등이 그 예 입니다.

자세히 보기

---

6. 취약점 관리 대응력 향상

by National Cyber Security Centre

얼마 전 NCSC(미국 국가보안센터)는 **'용납 가능한' 취약점과 '용납 불가능한' 취약점을 평가하는 방법을 설명하는 연구 보고서**를 발표했습니다. 당시에도 언급했듯이 모든 시스템에는 취약점이 존재하며, 많은 취약점은 복잡하고 피하기 어렵습니다. 동시에 조직은 '쉽게'(따라서 기대되는) 구현이 가능한 최상위 수 준의 완화 조치를 통해 이러한 취약점을 제거하기 위해 노력해야 합니다. 이러한 완화 조치가 발견되면 개발자(벤더, SaaS 제공업체, 오픈 소스 관리자 또는 기여자, 오픈 소스 프로젝트에 대한 취약점 공개, 팀 또는 개별 개발자 포함)는 동일한 근본 원인을 공유하는 다른 취약점을 찾아 수정할 수 있도록 프로세스 와 작업 방식을 조정하는 데 집중해야 합니다.

애널리스트 코멘트 : 영국 국가사이버보안센터(NCSC)는 연구 논문을 강조하는 것 외에도 취약점 관리 접근 방식 개선에 중점을 두고 있으며, 취약점 연구원, 개발자 및 조직 전반에 대한 지침을 제공합니다.

자세히 보기

---

7. 자동화와 AI 시대의 위협 탐지

by SECURITYWEEK

수백 명의 전문가와 인터뷰를 통해 그들의 전문적인 의견을 수렴했습니다. 이 글에서는 **공격자들이 자동 화와 AI를 도입함에 따라 위협 탐지가 어떻게 변화하고 있으며, 보안 팀은 어떻게 이에 적응하고 있는지** 살펴봅니다. 위협 탐지는 끊임없이 변화하고 있습니다. 주로 사후 대응 기술이었던 위협 탐지는 사전 예방 적 대응으로 발전했고, 이제는 자동화 단계로 나아가고 있습니다. 위협 탐지는 시스템 내부의 위협을 찾아 내는 활동입니다. 이는 외부 공격 표면 관리(EASM)와 보안 운영 센터(SOC) 사이에 위치합니다. EASM은 네트워크와 인터넷 사이의 인터페이스를 보호하여 공격을 차단하는 것을 목표로 합니다. 만약 EASM이 실패하고 공격자가 시스템에 침입한다면, 위협 탐지는 공격자가 남긴 흔적을 찾아 모니터링하여 피해가 발생하기 전에 공격을 무력화하는 역할을 합니다. SOC 엔지니어는 위협 탐지를 통해 얻은 새로운 데이터를 바탕으로 SIEM(보안 정보 및 이벤트 관리) 시스템에 적용할 새로운 탐지 규칙을 구축합니다.

애널리스트 코멘트 : 이 기사는 위협 탐지가 사후 대응적인 지표 기반 탐지에서 머신 러닝 기반 데이터, 사이버 위협 인텔리전스(CTI), 그리고 이미 침해가 발생했다는 가정 하에 가설 기반 조사를 활용하는 사전 예방적인 행동 이상 분석으로 진화하고 있음을 설명합니다.

자세히 보기

---

8. AI가 사이버 방어의 주도권을 쥐게 해서는 안 되는 이유

by SECURITYWEEK

인공지능(AI)의 엄청난 잠재력을 낭비하는 가장 쉬운 방법은 자동화를 실제 안전으로 착각하거나, 최첨단 기술 기능을 진정한 복원력으로 오인하는 것입니다. 문제는 데이터가 처음부터 끝까지 완벽하다고 보장 할 수 있는 조직이 거의 없다는 점입니다. 공급망은 복잡하고 혼란스럽습니다. 데이터의 출처를 추적하기 어렵고, 모델은 시간이 지남에 따라 정확도가 떨어집니다. 이러한 과정에서 **인간의 감독을 배제하는 것은 더 나은 시스템을 구축하는 것이 아니라, 시스템적 실패 지점을 만들어내고 이를 첨단 기술로 위장하는 것**과 같습니다.

애널리스트 코멘트 : 이 기사는 설명 가능한 인공지능(AI) 기반의 인간 감독을 도입하고 구현하는 것 이 얼마나 중요한지 다시 한번 강조합니다.

자세히 보기

---

9. TARA는 추적 가능한가요? 품목 정의부터 ALM까지의 핵심 평가

by CYEQT

냉혹한 현실: **품목 정의, TARA, ALM 시스템, 그리고 취약점 모니터링 간의 엔드투엔드, 양방향, 그리고 의미론적으로 명확한 연결 없이는 안전한 시스템을 구축할 수 없습니다.** 오히려 안전한 것처럼 보이는 착각만 심어줄 뿐입니다. 솔직히 말해서, 다음과 같은 문제가 발생합니다.

- 감사에서는 그럴듯해 보이지만, 실제 변경 과정에서 무너지는 문서들
- 증명이 아닌 주장만 늘어놓는 검증되지 않은 클레임들
- 갑자기 생겨나 현재 위험과의 연관성을 더 이상 파악할 수 없는 요구사항들

최신 차량은 이미 무선 업데이트, 클라우드 연결, 그리고 실제 공격 표면이 릴리스 주기보다 훨씬 빠르게 변화하는 소프트웨어 정의 플랫폼입니다.

애널리스트 코멘트 : 규제 기관이 감사 과정에서 OEM 및 공급업체에 점점 더 자세한 정보를 요구함에 따라 제품의 위협 및 취약점 현황을 실시간으로 파악하는 것이 더욱 중요해지고 있습니다.

자세히 보기

---

10. 사이버 보안 개념(ISO/SAE 21434)이 차량에만 국한될 수 없는 이유: 사이버 보안 관 리자를 위한 고려 사항

by CYEQT

이 글의 핵심 메시지는 한 문장으로 요약할 수 있습니다. 기술적 조치는 차량을 보호하지만, **지속 가능한 사이버 보안을 제공하는 역량은 조직이 유지해야 합니다.** 사이버 보안 관리자는 조직의 역량을 탄탄하게 구축하고, 역할을 명확히 정의하고, 탄력적인 프로세스를 설계하고, 공급망을 체계적으로 통합함으로써 차량의 기술적 제어가 차량 인도 시점뿐만 아니라 전체 수명 주기 동안 안정적으로 작동할 수 있는 필수적인 기반을 마련할 수 있습니다. 바로 이러한 논리입니다.

💬 애널리스트 코멘트 : 이 기사는 ISO/SAE 21434의 실무 적용 및 UN R155 CSMS(사이버 보안경영시스템) 맥락에서 프로세스 및 측정, 투명성 및 증거, 통합 및 거버넌스가 핵심 성공 요인임을 강조합니다.

자세히 보기

📌사보연 TI 뉴스레터 2호는 아래 전문가 의견을 바탕으로 구성되었습니다.

- 김호진 상무 (오토노머스A2Z)
- 남현경 연구원 (현대모비스)
- 박상범 책임연구원 (현대모비스)
- 엄선현 부장 (페스카로)
- 우사무엘 교수 (단국대학교)
- 이태관 책임연구원 (현대자동차)
- 이해승 상무 (피아이코드)
- 전상훈 교수 (국민대학교)
- 최영진 책임연구원 (현대자동차)

한국자동차공학회 사이버보안연구회

E-mail : acsc.ksae@gmail.com → 사이버보안연구회 회원 가입, 사이버보안 상담

사보연 위협인텔리전스 데이터베이스 → CSMS Audit 대응에 활용하십시오.