한국자동차공학회
The Korean Society of Automotive Engineers

자동차 사이버보안연구회
TI 뉴스레터

Published by FESCARO
in collaboration with AUTO-ISAC

- 2026년 5호 -

사보연 TI 뉴스레터 5호에서는 AI가 보안의 속도와 규모를 바꾸는 지금, 차량 ECU부터 개발 파이프라인, AI 에이전트까지 - 현장 실무자가 직면한 10가지 핵심 이슈를 다룹니다.

BYD Atto3 ECU 취약점(CVE-2025-61081)은 차량 보안 위협이 이미 현실임을 보여주는 사례 중 하나입니다. 침투 테스트와 OT 평가가 현장에서 제대로 작동하지 못하는 구조적 이유도 함께 살펴봅니다. AI가 오래된 소프트웨어 결함을 대규모로 발굴하기 시작하면서 패치 관리의 부담은 커지고, AI 생성 코드와 에이전트는 개발과 신원 인증의 경계를 흐리고 있습니다. 본 뉴스레터는 그 간극을 들여다봅니다.

1) CISO가 사이버 위협 인텔리전스(CTI)에 기대하는 것

by INTEL471

CISO는 더 많은 위협 인텔리전스를 원하는 것이 아닙니다. 그들이 필요로 하는 것은 자사의 환경에 맞춰 이미 검증되었고, 현재 공격자들이 실제로 수행하고 있는 활동을 기준으로 우선순위가 정해져 있으며, 조직의 비즈니스 환경에 최적화된 인텔리전스입니다. 향후 12개월 동안 CISO들이 가장 필요하다고 응답한 항목은 다음과 같습니다.

- 79% : 공격자들이 실제로 악용하고 있는 취약점에 대한 정보
- 77% : 특정 공격자의 전술·기술·절차(TTPs, Tactics, Techniques and Procedures)
- 78% : 사고 대응 이후 작성된 사고 분석 보고서를 가장 유용한 CTI 산출물 중 하나로 평가
- 89% : 위협 환경 보고서가 상황 인식에 유용하다고 평가

이러한 결과는 분명한 시사점을 보여줍니다. CISO들이 가장 필요로 하는 것은 더 많은 원시 데이터(raw feed)나 광범위한 정보 수집이 아닙니다. 오히려 수많은 정보 가운데 중요한 신호(signal)와 불필요한 잡음(noise)을 구분하는 분석 과정을 이미 거친, 실행 가능한 인텔리전스를 원하고 있습니다.

💬 애널리스트 코멘트 **:** 설문조사에 참여한 CISO 중 비즈니스 중심 인텔리전스를 가치 있다고 평가한 비율은 41%에 불과했습니다. 보고서는 이러한 결과의 원인을 관심 부족이 아니라, 해당 유형의 인텔리전스에 대한 이해와 활용 경험이 충분하지 않기 때문으로 분석했습니다.

자세히 보기

---

2) AI 시대 자동차 사이버 보안 취약점 관리의 필수 조건

by VicOne

이 블로그의 핵심 내용

- AI는 방어자의 효율성을 높이는 동시에 공격자의 익스플로잇 개발 비용을 낮추기 시작했습니다.
- 이러한 변화는 특히 수정에 시간이 오래 걸리는 자동차 산업에 상당한 영향을 미칩니다.
- 미래의 취약점 관리는 심각도뿐만 아니라 "얼마나 빨리 공격으로 이어질 수 있는지"에 대한 관점도 포함해야 합니다.

💬 애널리스트 코멘트 : 이 글은 차량 패치에 시간이 걸리기 때문에 취약점이 공개된 후 노출 기간이 더 길어질 가능성이 높다고 주장합니다. 또한 PSIRT와 개발/설계 팀 간의 협업 강화를 권장합니다.

자세히 보기

---

3) 차량 테스트 보안: 자동차 침투 테스트를 더욱 진지하게 고려해야 하는 이유

by CYEQT

불편한 진실은 SOP 이전 침투 테스트에서 발견된 많은 취약점이 테스트 과정에서 새롭게 발견된 것이 아니라는 점입니다. 이러한 취약점은 훨씬 이전에 이미 알려져 있어야 했습니다. 그 근원은 몇 달, 심지어 몇 년 전의 개념 설계 단계, 하드웨어 선정 단계, 네트워크 아키텍처 정의 단계에 있습니다. 이러한 경우 침투 테스트는 새로운 문제를 발견하는 것보다 기존의 결정을 확인하는 데 더 중점을 두게 됩니다.

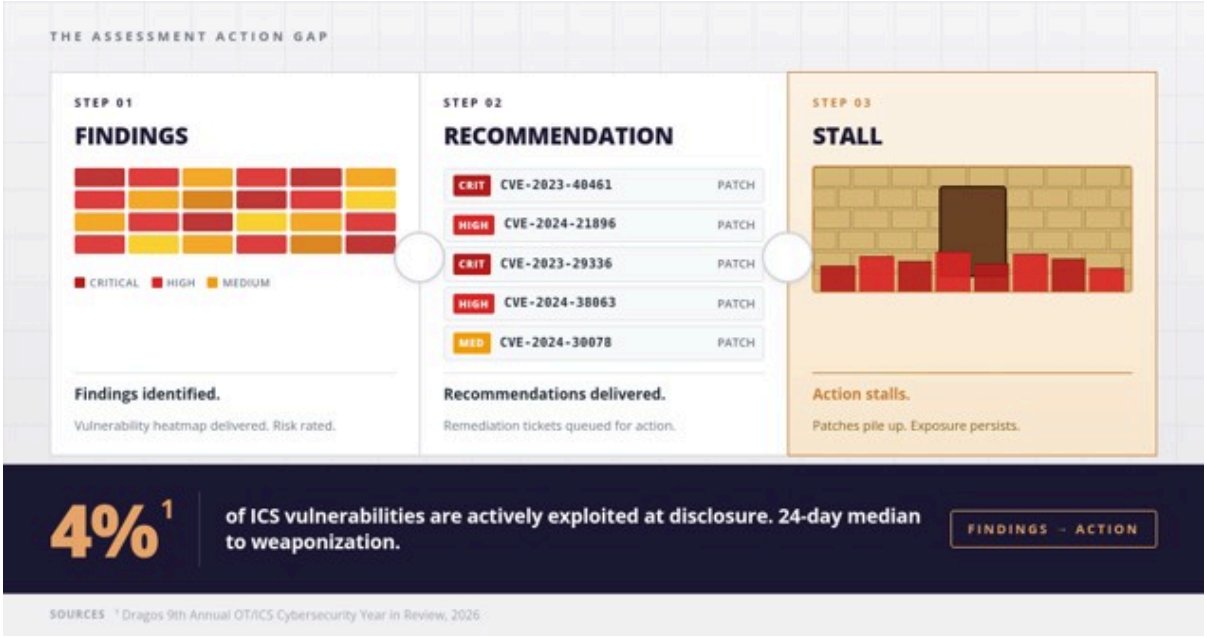
💬 애널리스트 코멘트 : 이 글은 보안이 개념 설계 단계부터 시작되어야 하며, 안전과 보안이 함께 고려되어야 하고, SOP 이전 한 번의 침투 테스트 대신 개발 단계에서 반복적인 침투 테스트를 실시해야 한다고 주장합니다. 또한 규정 준수가 안전한 제품 설계와 동의어는 아니라는 점을 지적합니다.

자세히 보기

---

4) OT 평가가 시작하기도 전에 중단되는 이유

by txOne



이는 흔히 발생하는 문제입니다. ICS 취약점 중 실제로 악용되는 경우는 공개 시점에 4%에 불과하며, 공개 후 실제 악용까지 걸리는 평균 기간은 24일입니다. 일반적인 평가 보고서에는 "취약점 X가 자산 Y에 영향을 미칩니다. 권장 조치는 패치 Z를 적용하는 것입니다."와 같은 내용이 포함됩니다. 하지만 보고서에는 해당 자산에 의존하는 생산 프로세스가 무엇인지, 패치 적용 중 해당 프로세스에 어떤 변화가 발생하는지, 장애 발생 시간은 얼마나 되는지, 패치가 해당 장치에서 실행되는 특정 펌웨어에 대해 검증되었는지, 그리고 문제가 발생할 경우 누가 책임을 져야 하는지에 대한 내용은 나와 있지 않습니다.

💬 애널리스트 코멘트 : 이 기사는 OT 평가의 문제점이 기술적 문제보다는 프로세스 자체에 있다고 분석합니다.

자세히 보기

---

5) 앤트로픽의 미토스(Mythos)는 기업 보안을 얼마나 바꿀 수 있을까?

by INTEL471

앤트로픽이 2026년 4월 7일 클로드 미토스(Claude Mythos) 프리뷰를 공개한 이후, CISO(최고정보보안책임자)들 사이에서 최첨단 인공지능(AI) 모델이 공격 및 방어 목적으로 활용될 가능성에 대한 관심이 크게 높아졌습니다. 보안 업계의 반응은 엇갈리고 있습니다. 우리가 알고 있는 소프트웨어 보안의 시대는 끝난 것일까요? 아니면 단순한 AI 과대광고일까요? 보안 실무자 및 리더들과의 논의에서, 이러한 모델이 얼마나 빠른 속도와 규모로 무기화될 수 있는지, 그리고 이것이 오늘날의 보안 프로그램에 어떤 의미를 갖는지에 대한 우려가 집중적으로 제기되었습니다. 이 블로그에서는 앤트로픽의 미토스 취약점 발견 및 익스플로잇 생성 기능에 대한 분석가들의 평가, AI 기반 취약점 연구 및 공격자의 활용 사례, 그리고 업계의 숨겨진 시각을 공유합니다.

💬 애널리스트 코멘트 : 미토스 프리뷰는 일반 Claude API가 아니라 Glasswing 컨소시엄(AWS·애플·구글·MS 등 약 50개 검증 조직)에만 제한적으로 게이팅되어 있어, 일반 계정 탈취만으로는 접근할 수 없습니다. 따라서 현실적 위협 벡터는 'Glasswing 파트너사의 자격증명·운영 환경 침해'로 좁혀집니다. INTEL471은 지하 조직이 이미 이 제한된 접근권을 노린 비공식 획득 시도를 정황으로 포착하고 있다고 전합니다. 자동차 업계로 보면, 1차 공급업체나 보안 벤더가 Glasswing 파트너일 경우 해당 조직의 토큰·계정 관리가 곧 공급망 리스크로 직결됩니다.

자세히 보기

---

6) 대규모 패치 시대가 도래할 것입니다

by Talos BLOG

AI는 소프트웨어 품질 향상의 큰 희망입니다. AI의 버그 탐지 능력은 지속적으로 개선되어 새 버전이 출시될 때마다 이전 버전보다 더 나은 성능을 보여줍니다. 이제 AI는 숙련된 취약점 연구원만큼은 아니지만, 인간의 분석으로는 따라잡을 수 없는 규모와 속도로 코드를 스캔하여 오류를 찾아낼 수 있는 단계에 이르렀습니다. AI를 잘 활용하면 잠재적인 취약점이 실제 운영 환경에 배포되기 전에 식별할 수 있습니다. 장기적으로 이는 매우 긍정적인 소식입니다. 자동화된 소프트웨어 검토 및 분석이 향상되면 코드 품질이 개선될 것입니다.

그러나 단기적으로는 수십 년 동안 누적된 기술 부채와 잠재적인 오류가 드러나게 될 것이며, 이를 해결해야 할 필요성이 커질 것입니다. 더욱 복잡한 문제는 공격자들이 이러한 도구를 이용하여 악용 가능한 취약점을 찾아 악용할 수 있다는 점입니다. 결과적으로 패치 요구량이 급증할 가능성이 높습니다. 취약점이 더 많이 발견될수록 더 많은 수정 패치가 배포되어 이미 과부하 상태인 운영팀에 추가적인 부담을 가중시킵니다. 이러한 패치 중 상당수는 시급히 배포되어야 하며, 일부는 현재 활발히 악용되고 있는 취약점을 해결해야 합니다. 적절한 계획이 없다면 수정 패치의 양이 조직의 배포 역량을 초과할 수 있습니다. 패치가 쏟아지기 시작하는 시점은 아직 오지 않았지만, 그 조짐은 이미 나타나고 있습니다.

지금이야말로 패치 우선순위 설정, 대규모 패치 적용, 그리고 신속하게 또는 아예 패치를 적용할 수 없는 시스템 관리 방안을 고려하기에 최적의 시기입니다. 이러한 질문들을 미리 생각해보고 프로세스를 개선할 수도 있지만, 패치가 쏟아져 나올 때 허둥댈 수도 있습니다. 준비가 되었든 안 되었든, 대규모 패치가 필요한 시기는 반드시 올 것입니다.

💬 애널리스트 코멘트 : 이 기사는 AI가 인간 연구원이 따라잡을 수 없는 규모와 속도로 취약점 발견을 가속화하여 단기적으로 패치 물량을 급증시키고, 이미 과부하 상태인 운영팀에 더 큰 부담을 줄 수 있음을 보여줍니다.

자세히 보기

---

7) AI 생성 코드가 SDLC(소프트웨어 개발 수명주기)에 넘쳐나면서 애플리케이션 보안 전략이 변화하고 있습니다.

by HACKREAD

AI 코딩 도구는 실험 단계를 넘어 일상적인 개발 지원 도구로 자리 잡았으며, 소프트웨어 팀이 함수 초안을 작성하고, 익숙하지 않은 코드를 설명하고, 테스트를 생성하고, 반복적인 변경 작업을 더 빠르게 처리할 수 있도록 돕고 있습니다. 하지만 보안 팀에게 더 어려운 문제는 AI로 생성된 코드가 얼마나 많이 풀 리퀘스트에 반영되기 전에 안전성 검증이 이루어지는가 하는 것입니다. 최근 Stack Overflow 설문조사에 따르면 개발자의 46%가 AI 도구 출력의 정확성을 불신하는 반면, 33%는 신뢰하는 것으로 나타났습니다. 이러한 우려는 정기적인 보안 검토 과정에서 드러납니다. 예를 들어, 생성된 API 핸들러는 컴파일 및 단위 테스트를 통과하지만 객체 수준 권한이 누락될 수 있습니다. 또한, 제안된 종속성이 합법적으로 보이지만 실제로는 버려졌거나, 취약하거나, 이름이 의심스러울 수 있습니다. 대규모 언어 모델(LLM) 애플리케이션에 대한 OWASP Top 10은 공급망 노출을 LLM 지원 시스템과 관련된 주요 위험 요소 중 하나로 간주합니다. 이 목록에는 프롬프트 주입, 안전하지 않은 출력 처리, 민감 정보 유출, 과도한 권한 위임, 공급망 취약성이 포함됩니다. 오늘날 이러한 위험은 개발 환경, 코드 어시스턴트, 파이프라인 자동화 및 AI 기반 애플리케이션에 점점 더 만연하고 있습니다.

💬 애널리스트 코멘트 : 소프트웨어 개발 팀은 컴파일되고 단위 테스트를 통과하며 프로덕션 환경에 배포할 준비가 된 것처럼 보이는 AI 생성 코드를 점점 더 많이 만들어내고 있지만, 이러한 코드에는 권한 허점, 취약한 입력 유효성 검사 또는 일상적인 검토를 우회하는 안전하지 않은 종속성 선택이 숨어 있을 수 있습니다.

자세히 보기

---

8) 인공지능용 소프트웨어 명세서(SBOM) - 최소 구성 요소

by BSI

본 문서는 공공 및 민간 부문 이해관계자들이 인공지능(AI)용 소프트웨어 명세서(SBOM)에 포함되어야 할 합리적인 요건에 대한 실질적인 지침을 제공하고, AI 공급망 전반의 투명성과 사이버 보안을 강화하는 데 기여하고자 합니다. 2025년 6월 G7 사이버 보안 워킹 그룹이 발표한 AI용 SBOM에 대한 공동 비전을 기반으로, AI용 SBOM에 포함되어야 할 최소 구성 요소에 대한 유용한 실질적인 권고안을 제시합니다. 이러한 최소 구성 요소는 의무 사항이 아니며, 새로운 요건, 표준 또는 법률을 제정하는 것도 아닙니다. 또한, G7 회원국의 기술 발전 및 법률·정책 프레임워크의 변화에 발맞춰 향후 수정 및 보완될 수 있습니다. 일부 관할 지역에서는 본 문서에서 제안하는 특정 요소들이 이미 법적 요건 및 의무, 또는 기존 및 향후 표준을 통해 다뤄지고 있거나 다뤄질 것으로 예상될 수 있습니다.

💬 애널리스트 코멘트 : 인공지능(AI) 시스템 관련 SBOM(소프트웨어 구성 명세서)의 일부 항목은 일부 관할 지역에서 의무화될 가능성이 있으므로, 전 세계적으로 AI 시스템을 개발하는 자동차 기업들은 개발 및 구현 단계에서 이를 고려해야 할 수 있습니다.

자세히 보기

---

9) 자동차를 보호하다: 미시간 자동차 업계 CISO들

by Security Boulevard

오늘날의 자동차는 하나의 네트워크 플랫폼이며, 제조 현장은 IT와 OT(운영기술)가 융합된 환경입니다. 공급망은 수십 개 국가와 수천 개의 공급업체로 구성되어 있습니다. 또한 디지털화, 전동화, 연결성 확대에 대한 경쟁 압박은 공격 표면을 최소화하고 통제하려는 보안의 기본 원칙과 끊임없이 충돌합니다. 글로벌 자동차 산업을 대표하는 기업들의 보안 리더와 전략을 소개합니다.

💬 애널리스트 코멘트 : 이번 기사에 소개된 리더들은 정적인 위험 환경을 관리하는 것이 아닙니다. 이들은 공격 표면이 지속적으로 확대되고, 공급망이 점점 소프트웨어 중심으로 변화하며, 대규모 보안 사고의 영향이 공장 운영을 넘어 차량 안전까지 확대되는 환경 속에서 조직을 보호하고 있습니다. 이는 향후 자동차 산업의 사이버보안 경쟁력을 좌우하는 중요한 요소가 될 것입니다.

자세히 보기

---

10) 모두가 AI 에이전트를 개발하고 있지만, 그들이 개인 정보를 어떻게 알아낼지는 아무도 예측할 수 없습니다.

by CYBERSCOOP

앤트로픽이 가장 강력한 AI 모델 미토스(Mythos)를 공개하지 않기로 한 결정은, 단 하나의 AI 에이전트가 수백 명의 해커보다 빠르게 취약점을 스캔할 수 있는 시대가 왔음을 보여줍니다. 그러나 그 에이전트들이 뚫으려는 시스템 대부분은 여전히 "키보드 뒤에 사람이 있다"는 전제 위에 설계돼 있습니다. AI 에이전트는 이 전제를 양방향에서 무너뜨립니다. 정당한 에이전트(Operator, Gemini, Visa 등)도 사람을 대신해 행동하려면 사용자의 신원·자격증명이 필요하고, 공격자는 "침입하지 않고 로그인한다." 탈취한 자격증명으로 인간을 대규모 위장하는 것입니다. 이제 핵심 과제는 로그인 시점의 인증이 아니라 "이미 들여보낸 것이 누구·무엇인지 아는 것"이며, 저자는 문 앞에서뿐 아니라 모든 행위·모든 행위자(사람·기계)에 대해 신원을 지속적으로 검증할 수 있는 조직만이 우위를 갖는다고 결론짓습니다.

💬 애널리스트 코멘트 : 핵심은 단일 운영자가 실직원 한 명의 인건비로 수십~수백 개의 정상 페르소나를 동시에 가동할 수 있다는 점입니다. 공격의 병목이 '기술·인력'에서 '강력한 모델 + 탈취된 자격증명'으로 옮겨간 만큼, 방어의 무게중심도 로그인 시점의 1회성 인증에서 모든 행위·모든 행위자(사람·기계)에 대한 지속적 신원 검증으로 이동해야 합니다. 이는 자동차·모빌리티 영역에도 그대로 적용됩니다. 차량 내 AI 에이전트, OTA, V2X 환경에서 머신 ID(machine identity) 관리와 행동 기준선 기반 이상탐지(behavioral IDS)가 더 이상 선택이 아닌 전제 조건이 되고 있습니다.

자세히 보기

📌사보연 TI 뉴스레터 5호는 아래 구성원들의 기여를 바탕으로 제작되었습니다.

전문가 의견

- 전상훈 교수 (국민대학교)
- 이해승 상무 (피아이코드)

추진 및 편집

- 엄선현 부장 (페스카로)
- 남현경 연구원 (현대모비스)
- 김호진 상무 (오토노머스A2Z)
- 박상범 책임연구원 (현대모비스)
- 우사무엘 교수 (단국대학교)
- 이태관 책임매니저 (현대자동차)
- 황이슬 과장 (페스카로)

한국자동차공학회 사이버보안연구회

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

사보연 위협인텔리전스 데이터베이스 → CSMS Audit 대응에 활용하십시오.