한국자동차공학회
The Korean Society of Automotive Engineers

사이버보안연구회
TI 뉴스레터

Published by FESCARO
in collaboration with AUTO-ISAC

사보연 TI(Threat Intelligence) 뉴스레터에서는 모빌리티의 신뢰성을 높이기 위한 **사이버보안 리포트와 인사이트 총 10종**을 소개합니다. **2026년 전망부터 올해의 주요 동향**을 살펴보고, **글로벌 업계가 주목하는 이슈를 중심으로 향후 대응에 필요한 시사점**을 확인해보세요.

---

1. Cybersecurity Forecast 2026: 다가올 위협에 대비하기

by Google Cloud

앞으로의 사이버보안은 **적대자와 방어자 양측의 급속한 진화와 정교화**로 특징지어질 것입니다. 점점 더 정교한 사이버 범죄 활동, 네트워크에 장기간 잠복한 채 첩보 활동을 벌이는 국가 차원의 공격자들, 그리고 공격의 규모와 속도를 높이기 위해 AI를 활용하는 적대 세력들이 있습니다. 사이버보안 방어자들은 인공지능과 에이전틱 AI를 활용하여 이 적대 세력으로부터 조직을 보호할 것입니다.

애널리스트 코멘트 : 본 보고서는 실제 트렌드와 전문가 분석을 기반으로 작성되었습니다.

자세히 보기

---

2. 2026년 사이버 위험 동향: 방어뿐 아니라 회복력 구축

by SECURITYWEEK

지난 한 해에서 얻을 수 있는 가장 중요한 교훈은 바로 '**모든 공격을 막으려 애쓰는 것만으로는 적을 앞지를 수 없다는 것**'입니다. 오히려 눈에 띄게 회복력을 강화함으로써 적보다 오래 살아남을 수 있습니다. 최근 2026년 신흥 위협에 대한 강연에서 저는 사이버 공격이 이전보다 훨씬 더 복잡하고, 지속적이며, 지능적이고, 자동화될 것이라고 주장했습니다. 이는 **완벽한 예방이 점점 어려워진다는 것**을 의미합니다. 따라서 가장 중요한 것은 **회복력**, 즉 **공격을 견뎌내고, 즉각적으로 적응하며, 최소한의 피해로 신속하게 복구할 수 있는 능력**입니다. 회복력은 단순히 기술을 구매하는 것으로 해결되는 문제가 아닙니다. **조직 전체의 역량**입니다. 그리고 회복력은 진정으로 총체적인 접근 방식을 취할 때 비로소 효과를 발휘합니다. 즉, 명확하고 체계적인 거버넌스, 가정이 아닌 실제 테스트를 거친 운영 준비 태세, 탐지뿐 아니라 복구까지 고려하여 설계된 기술, 그리고 자신의 역할을 이해하고 압박 속에서도 행동할 수 있는 인력이 필요합니다. 문화, 소통, 그리고 책임감은 단순한 자산이 아니라, 그 효과를 증폭시키는 핵심 요소입니다.

애널리스트 코멘트 : 인공지능(AI) 기반 공격자들은 이미 자동화를 활용하여 정찰 활동을 확장하고, 고도로 맞춤화된 소셜 엔지니어링 공격을 대규모로 수행하고 있습니다. 본 기사는 AI 활용 사례에 대한 데이터 분류 요건을 포함한 안전장치를 마련할 것을 권고합니다.

자세히 보기

---

3. 2026년의 SBOM : 찬반 양론

by DARK READING

소프트웨어 구성 요소 명세서(SBOM)는 소프트웨어 공급망 보안 문제를 해결하는 데 중요한 도구로 주목받고 있지만, 빠르게 변화하는 소프트웨어 생태계와 검증된 엔드투엔드 코드 체인 구축의 복잡성으로 인해 **광범위한 도입이 지연**되고 있습니다. 예를 들어 Docker는 자사의 보안 강화 이미지(Docker Hardened Images)에 소프트웨어 구성 요소 목록을 적극적으로 도입했습니다. 이 이미지는 불필요한 소프트웨어 구성 요소(아티팩트)를 최소화하도록 처음부터 설계되었으며, 완전한 SBOM과 함께 소프트웨어 아티팩트 공급망 레벨(SLSA) 3단계 검증을 통해 출처 증명을 제공합니다. SLSA는 빌드 무결성을 디지털 방식으로 보장하고 소프트웨어 소스 검증을 제공하는 방식입니다.

💬 애널리스트 코멘트 : 최종 빌드 단계에서 생성되는 SBOM은 취약점 관리를 위한 실행 가능한 보안 정보를 제공하기보다는 규정 준수 여부만 확인하는 부정확한 매니페스트를 생성합니다.

자세히 보기

---

4. 수직적 TARA 통합! 시스템 경계를 넘어 사이버 위험 분석을 연결해야 하는 이유

by CYEQT

자동차 및 차량 산업의 전통적인 개발 프로젝트에서 TARA는 종종 컴포넌트 또는 도메인 단위로 수행됩니다. 그러나 센서 퓨전, 도메인 ECU, 커넥티비티 모듈, V2X, 백엔드 API 등을 포함하는 복잡한 아키텍처에서는, 이러한 접근 방식이 구조적으로 유발된 '**불투명한 위험 전파(opaque risk propagation)**'로 이어진다는 경험적 사례가 있습니다. 쉽게 말해, 손상 영향과 발생 가능성이 서브시스템 수준에서 상위 수준(차량/서비스)으로, 그리고 다시 하위 수준(구체적 요구사항)으로 일관되게 추적되지 못한다는 의미입니다. 결과적으로 분석 결과는 개별적으로는 일관되어 보이지만(예: 공급사 관점), 시스템 전체 관점에서는 비교가 어렵거나 심지어 불완전할 수 있습니다.

💬 애널리스트 코멘트 : 이 글은 서브시스템 분석을 상위 시스템 TARA에 체계적으로 통합할 것을 주장하며, 그 이점으로 모든 것을 두 번 평가할 필요가 없어진다고 설명합니다.

자세히 보기

---

5. Pwn2Own Automotive에서 본 시사점 : 제로데이 취약점이 드러낸 전기차 충전기(EVSE) 사이버보안 표준의 공백

by VicOne

이번 연구 결과는 EV 충전 인프라에서 증가하는 사이버보안 위험을 강조하며, 오늘날의 표준이 EV 생태계를 충분히 보호할 수 있는지에 대한 긴급한 의문을 제기합니다. 이를 검토하기 위해, 우리는 클라우즈 레벨 매핑(clause-level mapping) 작업을 수행하여 현재 주요 EVSE 사이버보안 표준이 Pwn2Own Automotive에서 드러난 **취약점 유형**을 얼마나 잘 다루고 있는지, 혹은 다루지 못하고 있는지를 분석했습니다. 참고로 ISO 21434(자동차 사이버보안 엔지니어링)는 표 1에 포함되지 않았습니다. 해당 표준은 “차량 외부 시스템(예: 백엔드 서버)도 사이버보안 목적으로 고려될 수 있다”고 언급하는 반면, **시스템이 적용범위에서 제외**된다고도 명시합니다. 8장에 있는 지속적 사이버보안 활동 모범 사례를 참고할 수 있으나, 의무 사항은 아닙니다. 반면 UN R155는 제조업체가 **부속서 5(Annex 5)의 세 부분 전체를 위험 평가에 포함하도록 요구**합니다.

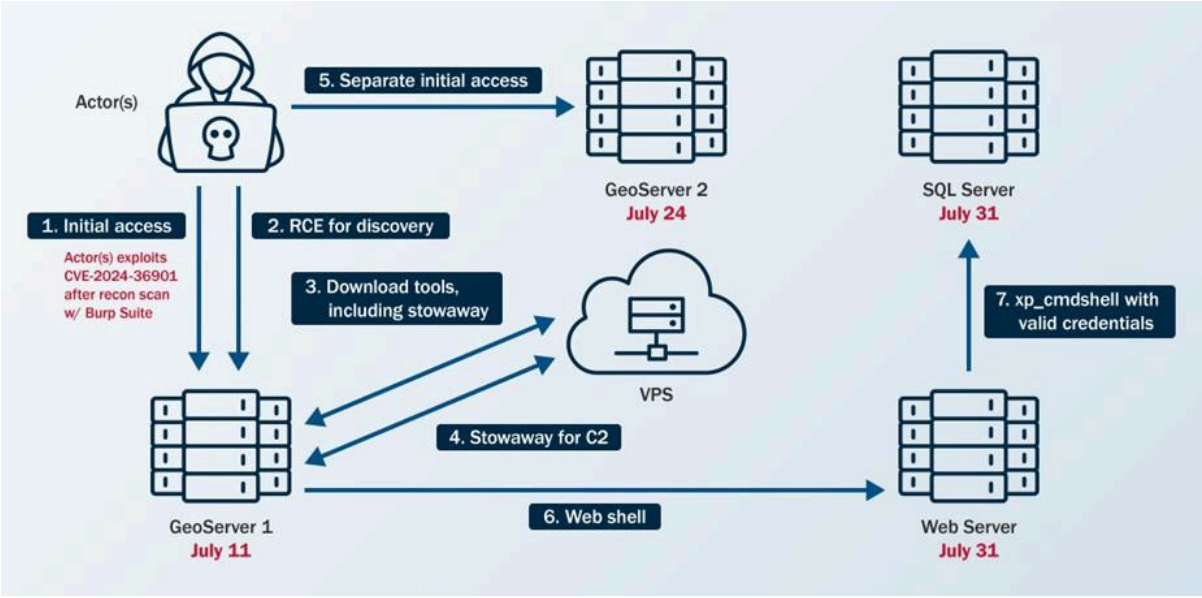
애널리스트 코멘트 **:** Phoenix Contact CHARX SEC-3100 EV의 취약점을 검토함으로써, 다양한 EVSE 표준에서 드러난 허점을 본 기사에서 상세히 다뤄졌습니다.

자세히 보기

---

6. 사고 대응 참여에서 얻은 교훈을 공유하다

by CISA



CISA는 미국 연방 민간 행정부 기관(FCEB) 중 한 곳에서 해당 기관의 엔드포인트 탐지 및 대응(EDR) 도구가 생성한 보안 경고를 통해, 잠재적인 악성 활동이 탐지된 사고 대응을 개시했습니다. CISA는 이번 대응 과정을 통해 **효과적인 위험 완화, 사고 대비, 사고 발생 시 대응하는 방법** 등을 보여주며 다음의 세 가지를 지적했습니다:

- 취약점이 신속하게 수정되지 않음
- 기관이 사고 대응 계획을 테스트하거나 훈련하지 않음
- EDR 경고가 지속적으로 검토되지 않음

💬 애널리스트 코멘트 : 이번 공지는 즉시 활용 가능한 IOC와 ATT&CK 매핑을 제공하여, 보안팀이 이를 곧바로 탐지 규칙으로 전환할 수 있도록 지원합니다.

자세히 보기

---

7. API 보안이 실패하면 이동성이 멈춘다 : 2025년 사이버 사고에서 얻은 교훈

by Upstream

지금까지 **발생한 사고들은 다음의 공통된 패턴**을 따라갑니다.

- 인증이 우회되었거나 누락됨
- 키가 노출되었거나 적절히 관리되지 않음
- 엔드포인트가 의도한 것보다 더 많은 데이터를 반환함

각각의 실패는 통합 지점을 곧바로 공격 표면으로 전환시켰습니다.

💬 애널리스트 코멘트 : 이 글은 최소한의 개선만으로도 자동차 사이버 생태계 전체의 복원력을 크게 강화할 수 있음을 시사합니다.

자세히 보기

---

8. 보안 운영센터에서 최고 경영진까지 : 위협 인텔리전스가 이사회 차원의 최우선 과제가 된 이유

by Recorded Future

위협 인텔리전스는 그 기능의 폭과 활용 방식에서 근본적인 변화를 겪고 있습니다. 과거에는 위협 인텔리전스가 보안팀이 침해 지표(IOC)를 수집하고 위험에 기반한 결정을 내리는 방어적 수단으로 사용되었던 반면에, 이제는 선제적이고 전략적인 도구로 진화하고 있습니다. 점점 더 많은 기업이 위협 인텔리전스를 이용해 투자 방향을 결정하고, 어떤 보안 도구를 도입할지, 어떤 공급망 또는 서드파티 업체와 협력할지, 그리고 직원 교육을 어떻게 진행할지를 판단하고 있습니다. 따라서, 조직들은 더 이상 위협 인텔리전스를 보안팀에만 국한된 정기 보고 자료로 보지 않고, 더 넓은 비즈니스 의사결정에 기여하는 중요한 가치로 인식하기 시작했습니다. 오늘날 **위협 인텔리전스는 기업 전반에 걸쳐 활용되며, 이사회와 임원진의 결정부터 일상적인 보안 운영에 이르기까지 다양한 의사결정을 지원**하고 있습니다.

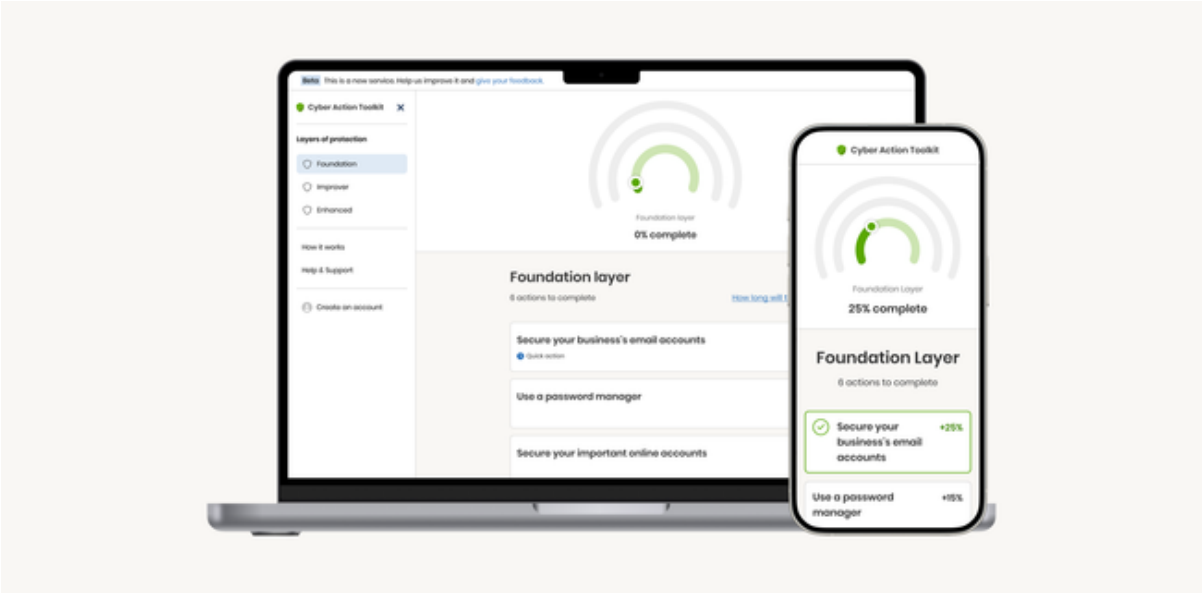
💬 애널리스트 코멘트 : 위협 인텔리전스는 IOC 기반의 전술적 방어 도구에서 벗어나, 이제 전체 조직이 투자·도구 선정·공급망 검증·직원 교육 등 핵심 의사결정을 내리는 데 활용하는 전략적 프레임워크로 진화했으며, 현재 83%의 기업이 전담 TI 팀을 운영해 일상적인 보안 및 경영 판단을 지원하고 있습니다.

자세히 보기

---

9. 회복력 향상을 위한 사이버 액션 툴킷

by National Cyber Security Center



NCSC의 자체 조사에 따르면, 많은 소규모 조직은 NCSC에서 제공하는 다양한 사이버보안 자료와 안내 때문에 압도당하는 느낌을 받고 있습니다. 이러한 이유로 **NCSC는 사이버 액션 툴킷을 제작**했습니다. 이 툴킷은 **소규모 기업이 쉽게 참여할 수 있는 방식으로 조언을 제공**하며, 무엇보다도 실제 행동으로 이어지도록 장려합니다. 따라 하기 쉬우며, 사이버보안 경험이 전혀 없어도 시작과 동시에 즉각적인 보호를 모두 무료로 제공합니다.

이 보고서는 사이버 액션 툴킷의 배경과 제작 의도, 그리고 NCSC가 이 형식을 선택한 이유를 다음과 같이 설명합니다. “단순화되고 시각적으로 흥미를 유발하며 보상 기반으로 구성된 사이버보안 메시지는 소규모 조직이 직면한 장벽을 효과적으로 해결하며, 산업 전반에 확장 가능한 모델을 제공한다.”

애널리스트 코멘트 : 이 툴킷은 영국 국가사이버보안센터(NCSC)가 제작한 것으로, 기업의 자산과 평판을 사이버 범죄로부터 보호하기 위한 명확하고 이해하기 쉬운 실천 지침을 제공합니다.

자세히 보기

---

10. Auto-ISAC과 Google, 자동차 산업 사이버보안 강화를 위한 파트너십 체결

by Google Cloud

Google Cloud는 자동차 정보 공유 및 분석 센터(Auto-ISAC)의 혁신 파트너로 합류하게 되어 매우 기쁩니다. 이번 파트너십을 통해 Google은 자동차 및 운송 산업에 대한 지원을 더욱 강화할 수 있게 되었습니다. Auto-ISAC은 차량 사이버보안 위험에 대응하기 위해 설립된 글로벌 커뮤니티입니다. Google은 IT, OT, 공급망 물류, 제품 보안 등 다양한 분야의 전문 지식을 바탕으로 **소프트웨어 정의 차량(SDV) 및 인더스트리 4.0의 복잡성을 효과적으로 해결**할 수 있도록 지원할 것입니다. 이번 파트너십은 Google이 해당 산업의 **디지털 전환**을 지원하고 인프라의 안전성을 보장하기 위해 최선을 다하고 있음을 보여줍니다. 글로벌 보안 인텔리전스와 Auto-ISAC의 공동 방어 모델을 결합하여, 회원사들이 점점 더 복잡해지는 사이버보안 환경 속에서 경계를 늦추지 않고, 위협을 예측 및 완화하며, 위기를 효과적으로 관리하고, 운영 연속성을 보장하는 데 필요한 지식과 지원을 제공하고자 합니다.

애널리스트 코멘트 : Auto-ISAC은 차량에 대한 새로운 사이버보안 위험에 대한 정보를 공유하고 분석하며, 경·중형 차량 OEM, 공급업체, 상용차 부문을 포함한 전 세계 자동차 산업 전반에 걸쳐 차량 사이버보안 역량을 공동으로 강화하기 위한 업계 주도 커뮤니티입니다.

자세히 보기

사보연은 수집한 위협 인텔리전스를 사보연 위협인텔리전스 데이터베이스에 저장하고 있습니다. 누구나 접속할 수 있습니다. ISO21434 사이버 보안 관리 체계(CSMS. Cyber Security Management System)를 갖추시는데 도움이 된다면 사보연의 보람입니다.

📌 사보연 TI 뉴스레터 1월 호는 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