한국자동차공학회
The Korean Society of Automotive Engineers

자동차 사이버보안연구회
TI 뉴스레터

Published by 자동차 사이버보안연구회
Prepared by FESCARO
in collaboration with AUTO-ISAC

- 6호 -

디지털 생태계의 안전을 위해 제정된 사이버복원력법(CRA, Cyber Resilience Act) 적용을 앞두고 있습니다. 유럽연합(EU)은 취약점 및 중대한 사고 발생에 대한 통지 의무는 2026년 9월부터, 그 밖의 의무사항은 2027년 12월부터 시행되도록 규정하고 있습니다. <TI 뉴스레터 6호>에서는 다가오는 CRA와 NIS2(Network and Information system 2)가 자동차 사이버보안에 미치는 영향을 확인할 수 있는 콘텐츠를 선정했습니다.

---

1. NIS2와 사이버 복원력법(CRA): 자동차 사이버 보안에 미치는 영향과 모빌리티 이해관계자들이 알아야 할 사항

by CYEQT

NIS2와 사이버복원력법(CRA)은 자동차 사이버보안 조직이 지금까지 다뤄온 규정과는 구조적으로 다르다. 이들은 제품 개발 또는 엔지니어링 표준이 아니라, 정부 기관의 감독, 이사회 책임, 벌금, 명확한 보고 체계를 포함하는 공법(Public Law) 기반의 규제입니다. 이러한 특성으로 인해 기존 자동차 사이버보안 규정보다 더 높은 수준의 추상성을 가진다. 기존의 자동차 분야 프레임워크는 상당한 해석의 여지가 있더라도 비교적 구체적인 요구사항을 제시하는 반면, NIS2와 CRA는 제조업체가 **무엇을 수행해야 하는지**는 제시하지만 **어떻게 수행해야 하는지**는 명확히 규정하지 않는 경우가 많습니다. 예를 들어, "제조업체는 적절한 주의의무(Due Diligence)를 이행해야 한다"는 식의 요구사항을 제시합니다.

여기에 더해 문서의 작성 방식도 다릅니다. ISO 표준이나 UN 규정과 달리, NIS2와 CRA는 법적 효력을 갖추기 위해 작성된 규정입니다. 따라서 이를 처음 접하는 엔지니어들은 익숙하지 않은 문체를 경험하게 될 것입니다. 이러한 차이는 조직 내 책임 주체, 요구되는 문서, 그리고 규정을 준수하지 않았을 때의 결과까지 모두 변화시킵니다.

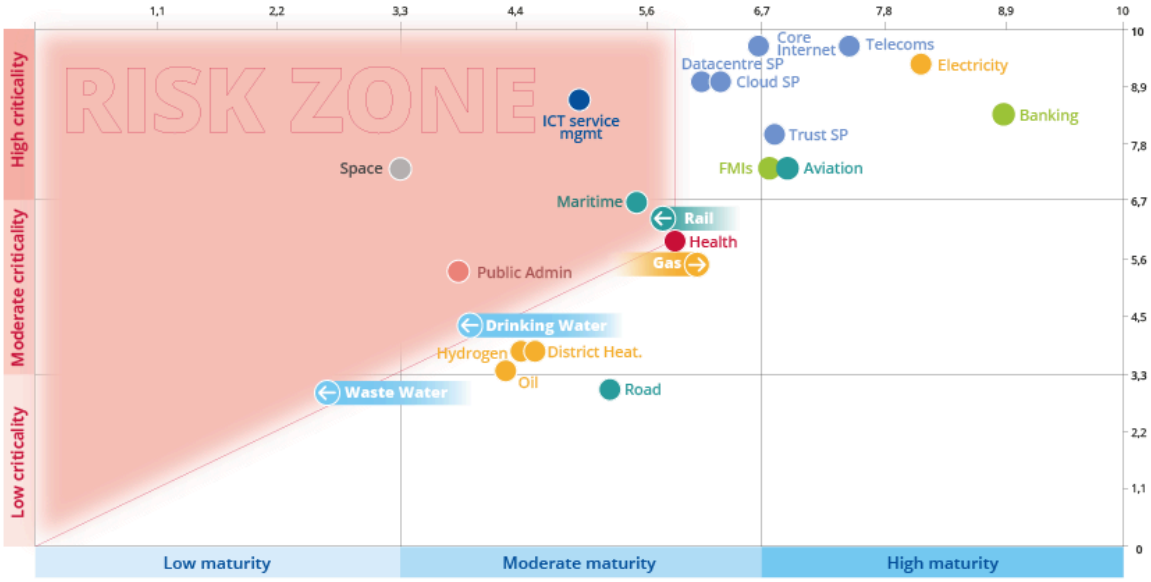
💬 애널리스트 코멘트 : 이 블로그는 NIS2가 이사회 차원의 거버넌스, 조직의 보고 의무, 그리고 IT, OT, 생산시설 및 백엔드 시스템의 복원력을 다룬다고 설명합니다. 또한 자동차 제품이 EU 형식승인(Type Approval) 체계에 따라 CRA 적용 대상에서 제외되는지, 또는 사이버복원력법(CRA)상 디지털 요소를 포함한 별도 제품(Products with Digital Elements, PDE)으로 분류되는지에 대해서도 살펴봅니다.

자세히 보기

---

2. NIS360: NIS 주요 분야의 성숙도 및 중요성에 대한 종합 분석

by enisa



이번 NIS360 보고서의 결과는 긍정적으로 평가할 만한 근거를 제공합니다. EU의 포괄적인 사이버보안 규제 체계, 특히 NIS2의 시행으로 상당한 개선이 이루어졌습니다. 올해 보고서에서는 은행, 전력, 항공, 우주, 그리고 통신·클라우드·데이터센터를 포함한 디지털 기반 서비스(Digital-by-default services)가 가장 중요한 분야로 계속 평가되었습니다. 이전 보고서 발간 이후, EU 주요 분야의 사이버보안 성숙도는 조직들이 변화하는 정책 요구사항과 직면한 사이버 위협에 대응함에 따라 꾸준히 향상되고 있는 것으로 나타났습니다.

💬 애널리스트 코멘트 : 분석 대상 분야 전반에서 확인된 사이버보안 수준의 향상은 ① 사이버보안 입법의 발전, ② 정치적 관심 증대, ③ 평가 항목(성숙도 차원) 전반의 진전이라는 복합 요인에 기인한 것으로 분석됩니다.

자세히 보기

---

3. EU, 미국·중국 공급업체 의존도 줄이기 위한 기술 주권 패키지 발표

by The Record

유럽연합(EU) 집행위원회는 오랫동안 지속되어 온 해외 기술 의존이 안보 취약성으로 이어질 수 있다는 우려 속에서, 유럽연합의 외국 기술 의존도를 줄이기 위한 포괄적인 법안과 전략을 이번 주 발표했습니다. 이번 제안은 반도체, 클라우드 컴퓨팅, 인공지능(AI), 오픈소스 소프트웨어를 아우르며, 집행위원회의 기술 담당 책임자인 Henna Virkkunen이 "유럽이 기술 주권에 접근하는 방식의 중대한 전환"이라고 표현한 내용을 담고 있습니다.

이번 패키지는「Chips Act 2.0」,「Cloud and AI Development Act(CADA)」등 두 개의 법안 초안과 함께 오픈소스 전략(Open Source Strategy) 및 에너지 시스템 디지털화 로드맵을 포함하고 있으며, 이를 통해 EU 기업, 시민 및 공공기관이 핵심 기술 분야에서 보다 다양한 선택지를 확보할 수 있도록 지원하는 것을 목표로 합니다.

💬 애널리스트 코멘트 : 기술 주권의 수사와 달리, 이 패키지는 자동차가 의존하는 성숙 공정 칩의 공급난을 풀어주지 못합니다. 차량 보안에 실질적으로 의미 있는 건 EU 소유를 강제하는 클라우드 등급제가 아니라 XZ Utils 사태가 드러낸 핵심 오픈소스 인프라에 대한 보안 투자이며, 결국 관건은 '주권'이 아니라 '복원력'입니다.

자세히 보기

---

4. 백악관, 연방기관의 사이버보안 로그 관리 정책 개편

by CYBERSCOOP

백악관은 연방기관이 네트워크 내 주요 사이버 활동에 대한 로그를 보관하도록 하는 규정을 개정했습니다. 이는 불필요한 행정 절차를 줄이고, 변화해 온 사이버보안 리스크에 초점을 맞추기 위한 조치라고 설명했습니다. 금요일 발표된 미국 예산관리국(OMB) 메모는 조 바이든 당시 대통령이 서명한 2021년 메모를 대체합니다. 이번 메모 M-26-14는 기존 메모 M-21-31의 취지를 언급하며, 해당 메모의 이행이 사이버공격 탐지 및 대응을 위한 로그 기준 수립과 기록 관리 개선 등 연방기관 전반의 기본 역량 강화에 기여했다고 밝혔습니다.

💬 애널리스트 코멘트 : 폐지된 메모 **M-21-31**은 연방기관 전반의 기본 로그 관리 기준을 수립했습니다. 이를 대체하는 **M-26-14**는 위험 기반의 우선순위 접근 방식으로 전환하며, CISA가 90일 이내에 로그 참조 아키텍처를 개발하도록 지시합니다.

자세히 보기

5. 가트너 "공급망, 지정학 및 AI 관련 과제에 직면"

by EETimes

지난주 열린 가트너 공급망 심포지엄/Xpo(Gartner Supply Chain Symposium/Xpo)에서 가트너의 수석 디렉터 애널리스트인 Alejandro Santalo는 EE Times와의 인터뷰를 통해 현재 최고공급망책임자(CSCO)들이 직면한 주요 과제와 전략적 대응 방안을 설명했습니다. Santalo는 데이터센터 증가에 따른 생산능력 제약과 새로운 수입 규제에 대응하기 위해, 기업들이 복잡한 글로벌 시장 환경에 맞춰 운영 모델을 조정해야 한다고 강조했습니다. 기술 수입을 규율하는 규제 환경은 더욱 강화되고 있으며, 이는 공급망 탈동조화(Supply Chain Decoupling)로 이어지는 보다 큰 흐름을 시사합니다.

2026년 5월 개최된 미·중 정상회담은 분석가들이 '기업 지정학(Corporate Geopolitics)'이라고 부르는 흐름이 더욱 가속화되고 있음을 보여주었습니다. Santalo에 따르면 기업 지정학이란 기업의 자본, 산업 생태계, 그리고 민간 부문의 실행 속도를 지정학적 영향력과 경제 전략의 수단으로 활용하는 개념이다. 전통적인 외교는 규제 검토와 정책 시행에 오랜 시간이 소요되는 반면, 기업은 민간 부문의 빠른 실행력을 통해 이러한 과정을 크게 단축할 수 있습니다.

💬 애널리스트 코멘트 : 관세 및 정책 변화에 따른 리스크를 분산하기 위해 제조시설을 베트남, 인도, 멕시코 및 미국으로 이전하려는 움직임은 새로운 제3자 협력업체 및 부품 공급원을 확보하게 되며, 이에 따라 각각 새로운 사이버보안 위험에 노출될 수 있습니다.

자세히 보기

---

6. KDDI 사이버 공격으로 이메일 계정 최대 1,422만 건 정보 유출 가능성

by the japan times

KDDI는 인터넷 서비스 제공업체(ISP)를 위한 자사의 이메일 시스템이 사이버 공격을 받아, 최대 **1,422만 건의 이메일 주소와 비밀번호**가 유출되었을 가능성이 있다고 화요일 밝혔습니다. 영향을 받은 서비스 제공업체는 **STNet, JCOM, Chubu Telecommunications, Nifty, Biglobe, KDDI Web Communications** 등입니다. KDDI는 6월 17일 사이버 공격을 확인했으며, 현재 보호 조치를 시행했다고 밝혔습니다. 회사에 따르면 이번 공격은 이메일 시스템에서 사용된 **제3자 소프트웨어의 취약점**을 악용해 이루어졌습니다. 또한 KDDI는 피해를 입은 인터넷 서비스 제공업체들과 협력해 사용자들에게 비밀번호 변경을 권고하는 한편, 피해 규모에 대한 조사를 계속 진행할 예정이라고 밝혔습니다.

💬 애널리스트 코멘트 : 이번 사고는 하나의 공통 플랫폼이 침해될 경우 여러 서비스 제공업체와 수백만 명의 사용자에게 동시에 영향을 미칠 수 있음을 보여주는 사례로, 상호 연결된 서비스 생태계에서 제3자 리스크 관리(Third-Party Risk Management)의 중요성을 다시 한번 강조합니다.

자세히 보기

---

7. 2026년 사이버 사고 대응 성공의 핵심 요소

by Morgan Lewis

- 사고 대응은 팀 단위의 활동입니다. 핵심 대응팀에는 경영진 후원자(Executive Sponsor), 사고 대응 책임자(Incident Lead), IT, 법무·컴플라이언스, 인사(HR), 홍보(PR), 고객 서비스 부서가 포함되어야 하며, 필요 시 외부 전문기관도 참여해야 합니다. 또한 법률 자문, 디지털 포렌식, 사이버 보험, 신용 모니터링, 사고 통지, 전자증거개시(eDiscovery), 협상 및 커뮤니케이션 지원 조직은 사고 발생 이전에 미리 지정되어 있어야 합니다.
- 효과적인 사고 대응 계획은 잡지나 책보다 브로슈어에 가깝습니다. 사고 대응 계획은 방대한 매뉴얼이 아니라 팀별 역할과 체크리스트 중심으로 구성되어야 합니다. 또한 내부 및 외부 연락처, 예비 연락처, 역할과 책임, 대응을 개시하는 기준 이벤트(Triggering Events), 그리고 사고 발생 시 확인해야 할 핵심 질문을 포함해야 합니다.
- 사고 발생 이전에 경영진의 의사결정 권한이 명확해야 합니다. 고위 경영진 후원자는 C레벨 경영진과 이사회에 상황을 공유하고, 시스템 중단, 사고 통지, 복구 및 대응 수준(Escalation)과 관련된 주요 의사결정을 내려야 합니다. 빠르게 전개되는 사고에서는 일부 의사결정이 정식 의사결정 절차를 거치기 전에 수분 내에 이루어져야 할 수도 있습니다.
- IT는 사고 대응의 사실관계를 주도하는 역할을 합니다. IT는 정보 취합을 총괄하고, 디지털 포렌식을 지원하며, 위협 확산 방지(Containment)를 수행하고, 취약점을 조치하며, 사고 통지 여부를 판단하기 위한 분석을 지원합니다. 사고 대응 책임자는 IT 환경 전반을 폭넓게 이해하고 있거나, 여러 기술 담당자의 지원을 받을 수 있어야 합니다.

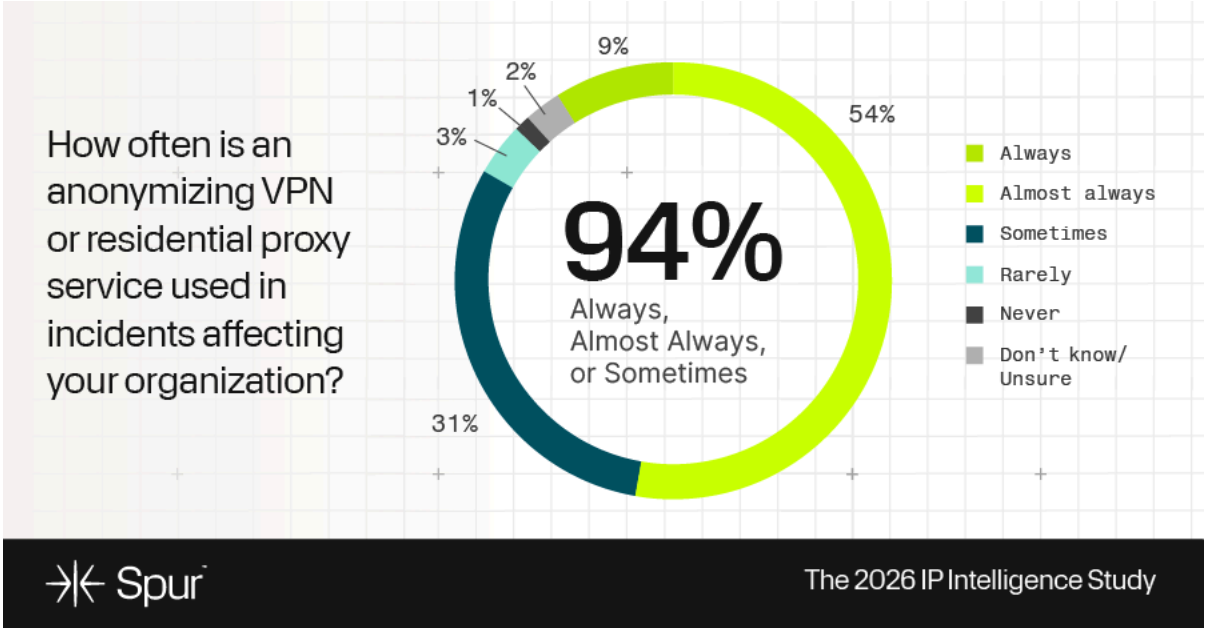
💬 애널리스트 코멘트 : 여기에서 제시하는 실무 권고 사항 중 하나는 실제로 발생했던 공격 사례 중 성공 직전까지 갔던 사례를 검토하고, 마지막 방어 계층이 실패했다면 어떤 결과가 발생했을지를 분석하는 것입니다. 이러한 방식은 정형화된 테이블탑(Tabletop) 훈련만 수행하는 것보다 조직의 사고 대응 준비 수준을 더욱 효과적으로 향상시킬 수 있습니다.

자세히 보기

---

8. 설문조사: 사이버사고의 94%, 익명화 인프라와 연관... 보안팀은 여전히 사후 대응에 머물러

by The Hacker News



보안 조직은 그 어느 때보다 많은 IP 관련 데이터를 활용할 수 있게 되었습니다. 보안 분석가들은 매일 다양한 공급업체와 플랫폼으로부터 제공되는 정보 보강(Enrichment) 데이터, 위치 정보(Geolocation), 평판 점수(Reputation Score), 텔레메트리(Telemetry), 위협 인텔리전스 등 다양한 데이터를 수집하고 있습니다.

그러나 이러한 방대한 정보에도 불구하고, 많은 조직은 여전히 'IP 뒤에 누가 있는지'를 파악하고 '어떤 대응을 해야 하는지'를 판단하기 위해 방대한 데이터 속에서 필요한 정보를 선별해야 하는 근본적인 과제에 직면해 있습니다. 실제로 Spur Intelligence가 200명 이상의 보안 실무자를 대상으로 실시한 최근 업계 조사에 따르면, VPN과 주거용 프록시(Residential Proxy) 네트워크를 포함한 익명화 인프라(Anonymizing Infrastructure)가 거의 모든 보안 사고에서 확인된 것으로 나타났습니다. 또한 많은 조직이 이러한 IP 데이터를 효과적으로 활용하기 위해 필요한 가시성(Visibility), 맥락(Context), 그리고 운영 프로세스(Operational Workflows)가 부족하다고 인정한 것으로 조사됐습니다.

💬 애널리스트 코멘트 : 설문에 참여한 200명 이상의 보안 실무자 중 절반에 가까운 응답자는 익명화 인프라를 이용한 계정 탈취(Account Takeover) 시도와 자격 증명 악용(Credential Abuse)으로 인해 상당한 운영상 또는 재무적 영향을 경험했다고 답했습니다. 또한 동일한 비율의 응답자는 IP 활동을 분석할 때 가장 큰 어려움으로 맥락(Context) 부족을 꼽았습니다.

자세히 보기

---

9. 대부분의 CISO, 부정적인 보안 이슈를 은폐하라는 압박 경험

by DARKREADING

- 최고정보보호책임자(CISO)는 사업 목표와 기업 이미지를 보호하기 위해 이사회, 경영진 및 사업부로부터 보안 관련 문제를 축소하거나 공개를 지연하라는 강한 압박을 받고 있습니다.
- Checkmarx의 보고서에 따르면, 설문에 참여한 CISO의 95%는 컴플라이언스 관련 보안 이슈를 공개하지 말라는 압박을 경험한 것으로 나타났으며, 이는 투명성 확보와 보안 우선순위 설정에 구조적인 문제가 있음을 보여줍니다.
- CISO는 충분한 권한이나 자원을 확보하지 못하는 경우가 많으며, 투명성을 유지하는 동시에 신속한 제품 출시, 규제 준수, 평판 및 재무적 위험 최소화라는 상충되는 요구 사이에서 균형을 맞춰야 합니다.
- 전문가들은 CISO가 사업 전략과 C레벨 경영진 논의에 더욱 적극적으로 참여해야 한다고 강조하며, 사이버보안을 핵심 경영 의사결정에 통합하는 것이 조직의 복원력과 신뢰를 높이고, 투명한 정보 공개를 일상적인 활동으로 정착시키는 데 도움이 된다고 설명했습니다.

💬 애널리스트 코멘트 : 기사에 인용된 여러 전문가들은 CISO가 디지털 자산을 보호하기 위해 임명되었지만, 실제로는 위험을 충분히 관리할 수 있는 권한, 영향력 또는 자원을 갖지 못하는 경우가 많다고 지적했습니다. 또한 컴플라이언스를 운영 복원력의 핵심 요소가 아닌 단순한 체크리스트 수준으로 인식할 경우, 보안 이슈는 위험을 줄이기 위한 정보가 아니라 사업 목표를 저해하는 장애물로 받아들여질 수 있다고 설명했습니다.

자세히 보기

---

10. 5선 CISO가 진단한 사이버보안의 여섯 번째 시대: 이제 '보안 기본 관리'가 전략이다

by The Cybersecurity Pulse

저는 Wells Fargo, Jack Henry, DTCC에서 총 다섯 차례 CISO를 맡는 등 20년 넘게 기업의 보안 프로그램을 운영해 왔습니다. 그동안 저는 보안이 다섯 번의 뚜렷한 시대를 거치는 과정을 지켜봤습니다. 각 시대는 공격자의 공격 방식, 감사 요구사항, 그리고 워크로드가 운영되는 환경의 변화에 대응하기 위해 등장했습니다. 그리고 모든 시대에서 동일한 일이 반복되었습니다. 기본적인 보안 위생(Security Hygiene)은 항상 우선순위에서 뒤로 밀려났습니다.

이제 우리는 여섯 번째 시대에 접어들고 있습니다. 이번에는 보안 위생이 전략적인 핵심 요소가 되었습니다. 이는 보안 프로그램 전체가 제대로 작동할 수 있는지를 결정하는 중요한 업무입니다. 여기서 말하는 보안 위생(Security Hygiene)이란 공격 표면을 줄이기 위해 반복적으로 수행해야 하는 운영 활동을 의미합니다. 여기에는 장기간 사용되지 않은 계정(Dormant Accounts), 오래된 OAuth 애플리케이션, 운영 환경에 읽기 가능한 상태로 남아 있는 비밀 정보(Secrets)와 환경 변수(Environment Variables), 만료된 인증서, 시스템 연동 이후 한 번도 검토되지 않은 제3자 접근 권한, 평문으로 저장된 민감정보, 그리고 보안팀도 존재를 알지 못하는 상태로 조직 환경에 연결된 AI 도구 등이 포함됩니다. 이러한 업무는 항상 로드맵에는 포함되어 있었지만, 그 중요성에 걸맞은 수준으로 예산과 자원이 배정되는 경우는 거의 없었습니다. 그러나 올해 발생한 세 가지 사건은 이러한 상황이 반드시 바뀌어야 하는 이유를 더 이상 외면할 수 없게 만들었습니다.

💬 애널리스트 코멘트 : 보안이 다섯 시대(경계→컴플라이언스→탐지·APT→클라우드·제로트러스트→SOAR·AI SOC)를 거쳐 여섯 번째 '보안 기본 관리(security hygiene)의 시대'에 진입했습니다. 2026년 4월 세 사건(Mythos 제로데이 대량 발굴, Copy Fail 커널 결함, Vercel OAuth 침해)을 근거로 "발견 비용이 0에 수렴하니 실패 지점은 놓친 알림이 아니라 인벤토리 안 된 신뢰관계"라 주장하며, 기본 관리만이 복리로 누적되는 분야라 강조합니다.

자세히 보기

📌사보연 TI 뉴스레터 6호는 아래 구성원들의 기여를 바탕으로 제작되었습니다.

전문가 의견

- 전상훈 교수 (국민대학교)

추진 및 편집

- 이해승 상무 (피아이코드)
- 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.