AutoCrypt
Cybersecurity Monitoring Service
사이버보안 위협 모니터링 서비스

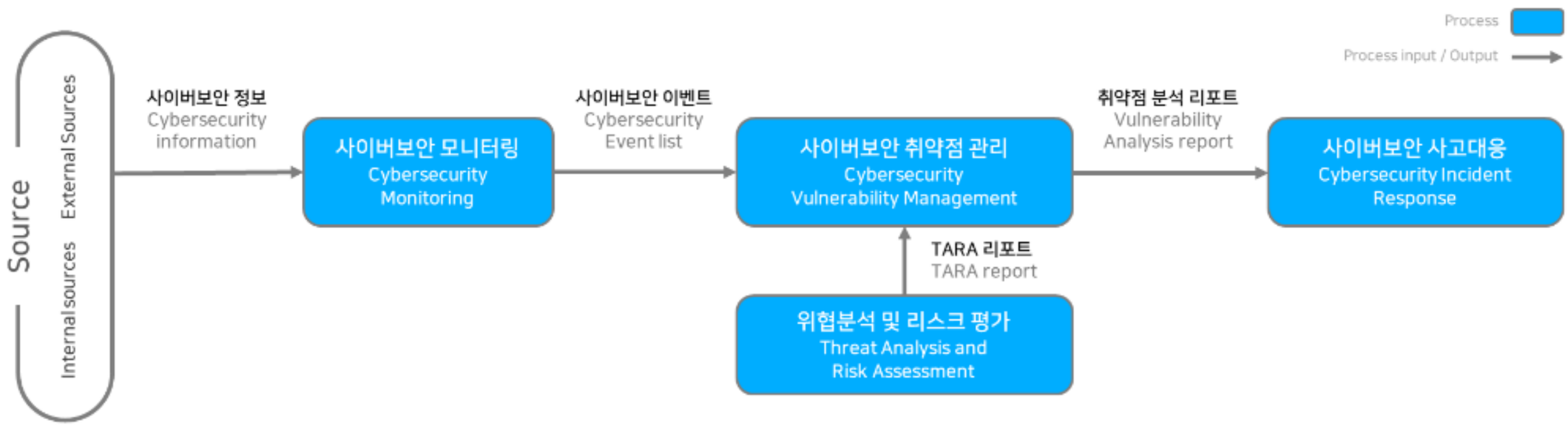
ISO/SAE 21434기반 차량 사이버보안을 상시 모니터링하고 대응방안을 제시하는 보안 위협 모니터링 서비스

사이버보안 위협 모니터링 서비스

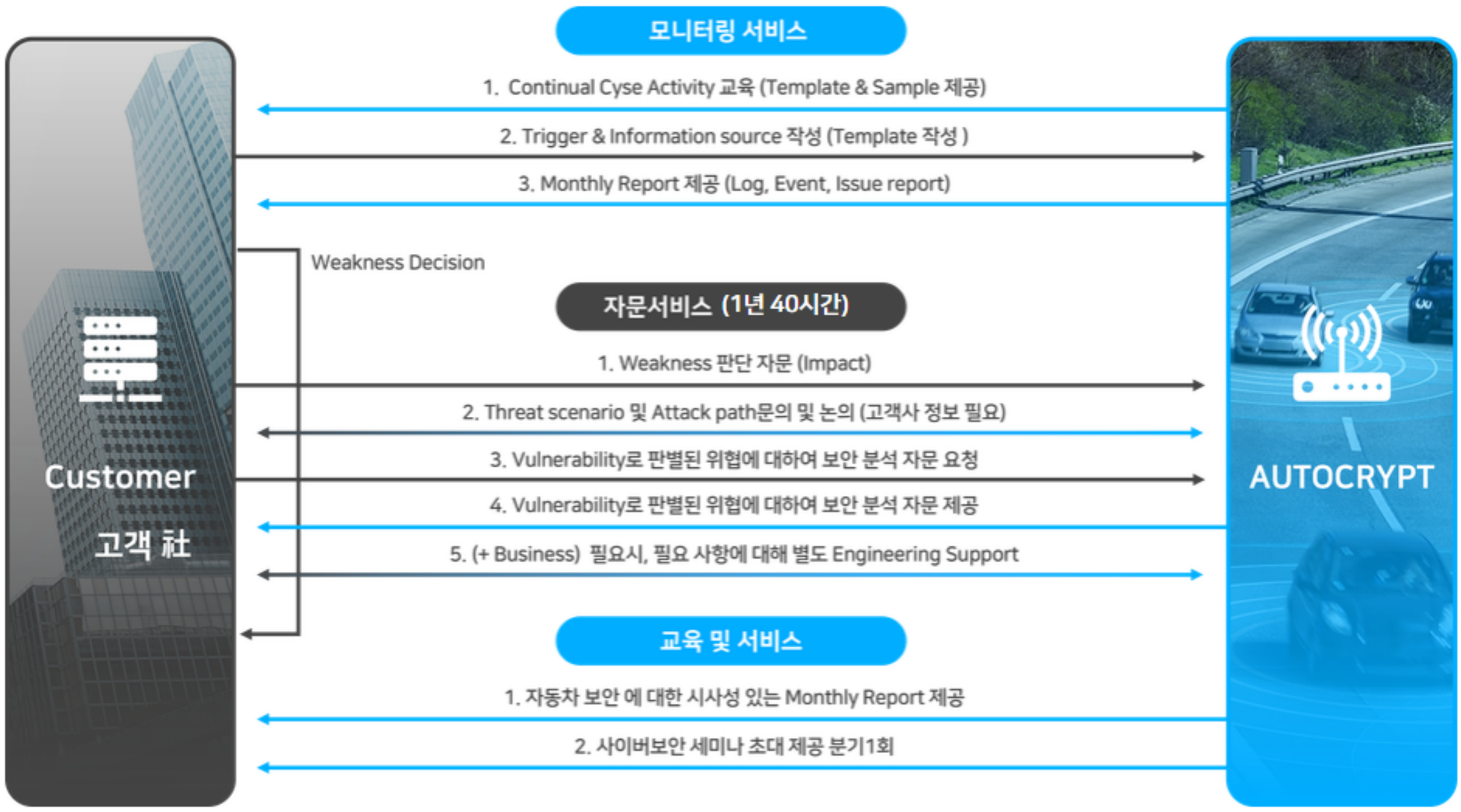
UN R155 및 ISO/SAE 21434 요구사항에 따라 CSMS를 구축한 OEM 및 공급업체들은 지속적인 사이버보안 활동을 수행하며 관련 증적자료를 계속 남겨야 합니다. 그러나 방대한 정보원에서 자사 제품에 맞는 소스와 키워드를 등록하고 체계적으로 관리하기 위해서는 많은 리소스가 필요하며, 개발부터 운영까지 다양한 환경으로 인해 어려움이 있습니다.

아우토크립트의 사이버보안 위협 모니터링 서비스는 고객사 제품에 맞춘 소스와 키워드로 지속적인 모니터링을 수행하고 대응 방안을 제시합니다. 당사 서비스를 이용하면 사이버보안 데이터 관리를 위한 체계적인 시스템 운영 관리와 비용 절감의 체계적인 서비스를 제공합니다.

사이버보안 모니터링 프로세스



사이버보안 모니터링 수행 로직



AUTOCRYPT

아우토크립트
TEL 02-2125-4000
ADDRESS 서울특별시 영등포구 여의공원로 115, 세우빌딩 B1, 1, 6, 7, 8층

www.autocrypt.co.kr
info@autocrypt.io

전문 지원 / 대응

1. 정기 & 비정기 사이버보안 모니터링 리포트 (월1회 & 비정기) + Offline 사이버보안 세미나 초대 (분기 1회)

Sources

- 신규 보안 위협에 대한 주요 소스 모니터링 리포트(Cybersecurity Information) (월 1회)
  e.g., CVE, CWE, OWASP, NVD, GitHub
- 시사점 있는 보안 위협을 선별하여 전문가 분석 리포트 제공 (월 1회)
- 주요 위협 뉴스 발생 시 비정기 Cybersecurity Information 리포트 발행
- 고객사 / 제품 특성 별 정보 소스 추가 지원

Triggers

- 고객사 / 제품 별 Trigger Keywords에 기반하여 필터링 된 보안 위협 리스트 (Event) 제공 (월 1회)
  e.g., Chip IDs, ECUs, Open Sources
- 공통 Trigger Keywords 외 고객사 별 Trigger 등록 및 정의 지원
- 고객사 Triggers에 해당하는 주요 위협 발생 시 비정기 Event 리포터 발행
  e.g., 고객사 요청 등록 소스, 제품 Trigger

Regular Seminar

- 신규 보안 위협 및 대응 방안에 대한 Offline 사이버보안 세미나 초대 (분기 1회)
  - 고객사 별 최대 4명 초대권 제공
  - Offline 참석 불가 시 Online 참여 기회 제공
- 외부 보안 전문가 초빙 Session 제공
  -KAIST, 고려대 등 학계 및 관련 업계 전문가
- 각 분야 자동차 사이버보안 담당자 간 네트워킹 및 커뮤니티 조성

2. Weakness 식별, Vulnerability Analysis, 대응 방안 모색 등에 대한 사이버보안 전문가의 자문 서비스 제공 (1년 40시간)

Weakness

- Triggers로 필터링 된 Events에 대해 Weakness Evaluating 서포트
  - 정의된 Events 별 자산/속성 정의
  - CVSS Scoring
  - 위협 시나리오 및 공격 경로 분석
- Weakness로 판정된 Events에 대해 패치 권장 코멘터리
  - 알려진 (Already Known) 권장 내용 기반

Analysis Consulting

- Vulnerability로 판별된 위협에 대하여 보안 분석 자문 제공
- Vulnerability별 상세 분석 컨설팅
  - After Attack Feasibility Rating
  - Risk Value
- 취약점 검증 방법 및 권장 패치 방안 제공
- 연 최대시간 외 추가 자문 필요 시 유상 지원

Engineering Support

- 취약점 분석 후 필요한 사항에 대해 별도 Engineering Support 제공 가능
  - 취약점 특성에 따라 필요 분야 별 유상 지원
- 취약점 검증을 위한 보안 테스트 수행
- 분석 결과에 기반한 실제 SW패치 개발
- 해킹 사례에 대해 고객사 제품 대상 재현 가능성 분석 및 실제 모의해킹 진행

*별도 유상 지원

사이버보안 위협 사고 리포트 [예시]

Monitoring and Hacking Reconstruction

자동차 해킹 사례 및 신규 공격법 Monitoring 분기별 리포팅
사례 중 재현 가능한 Attack Case 선별 및 해킹 재현

당사 제공 서비스 범위

✓ **Cybersecurity Information Collection**
- Source List 선정 (차량 단위 정보 / 해킹 사례 위주)
- 해킹 / 보안 위협 사항 분기별 리포트 발행

✓ **Hacking Reconstruction**
- 고객사와 연관성 있는 Attack Case 선별
- 재현 가능한 Case에 재현 방비 및 시험 방법 분석
- 실제 Hacking 재현 및 관련 리포트 발행

Figure 1. (Left) Location of the crash on northbound Mill Avenue, showing the paths of the pedestrian in orange and of the Uber test vehicle in green. (Right) Postcrash view of the Uber test vehicle, showing damage to the right front side.

그림1 Uber 자율주행 차량 사고

AUTOCRYPT

아우토크립트
TEL 02-2125-4000
ADDRESS 서울특별시 영등포구 여의공원로 115, 세우빌딩 B1, 1, 6, 7, 8층

www.autocrypt.co.kr
info@autocrypt.io