Date : 2022.11

SOFTFLOW

Software V&V 및 Cyber Security 전문 기업

# 소프트플로우 Business Guide

# Company Profile

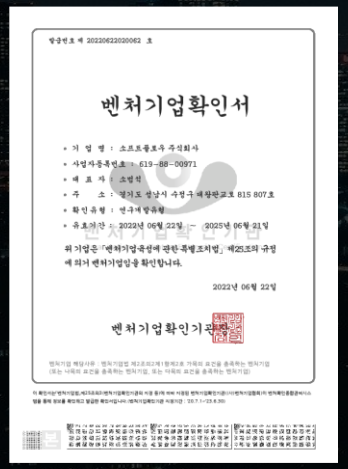
SOFTFLOW

**일반 현황**

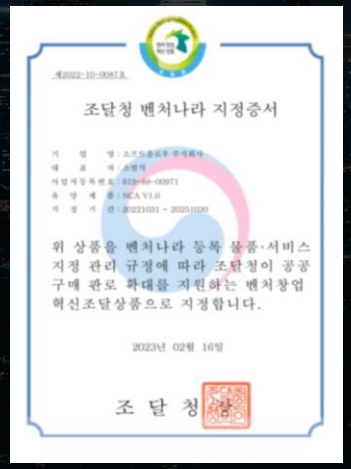
| 회 사 명 | 소프트플로우 ㈜ | 대 표 자 | 소 범 석 |
|---|---|---|---|
| 주 소 | 경기도 성남시 수정구 달래내로 46, 성남글로벌융합센터 A타워 8층 805호 | | |
| 회사 설립일 | 2018년 02월 14일 | | |
| 자격 현황 | [ 소프트웨어사업자 ] 컴퓨터 관련 서비스 사업 / 패키지 소프트웨어 개발 및 공급 사업 / 학술 및 연구용역 | | |

**인증서 및 수상**

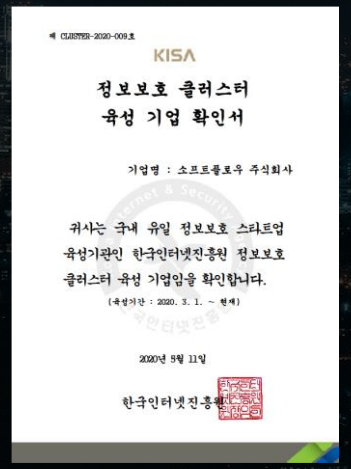

기업부설연구소 인정서
(2020.02)




벤처기업 확인서
(2022.06~2025.06)




NCA 벤처나라 지정증서
(2023.02.~2025.10)




정보보호 클러스터
육성 기업 확인서
(2020.03~)


스마트팩토리 어워드
보안솔루션부문
기업혁신 대상
(2019)

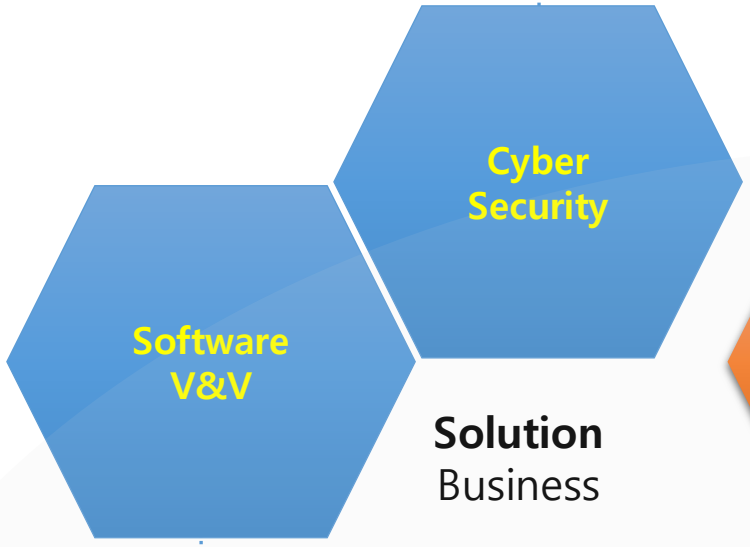
**비즈니스에 보안기술을 더하다.**

**여러분의 보안기술 파트너 소프트플로우가 함께하겠습니다.**

THALES DARKTRACE

- 민감 Data 보호를 위한 암호화 및 암호키 관리 시스템
- 통신 구간 보호를 위한 고속 구간 암호화 시스템
- AI 기반 시스템 Cyber 위협 탐지 및 차단 시스템

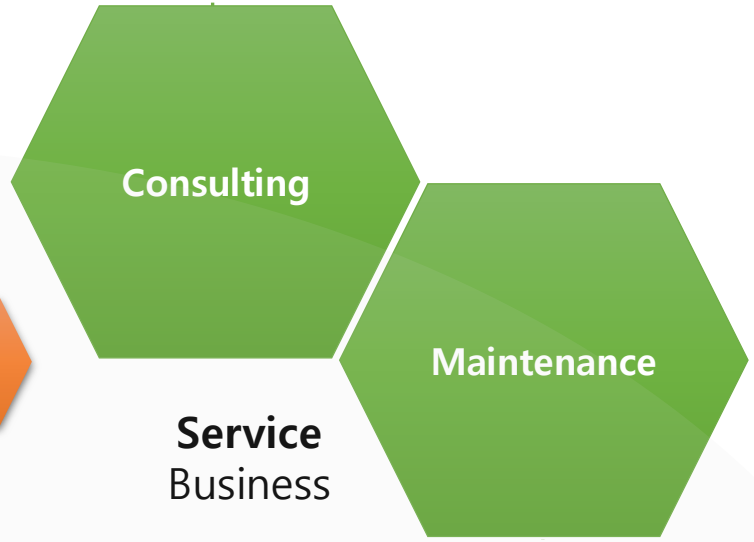
- SW 품질 관리 프레임워크 구축
- ISO 26262 / IEC 62443 등 국제 표준 인증 SW 관련
- Cyber Security 진단 및 대응




**Solution** Business

**R&D** Business

**Leading Technologies**




**Service** Business

- 소프트웨어 신뢰성 검증 & 취약점 확인
  ( 정적 / 동적 / 오픈소스 관리 / 퍼징 등)

SYNOPSYS® HEARTLAND.DATA Heartland.Data Inc.

[ 네트워크 패킷 수집 및 분석을 통한 위험 관리 기술 ]
[ SDP를 적용한 기기 인증 및 접속 기술 ]
[ AI 기반 드론 이상징후 탐지 기술 ]

NCA SOFLO.IoT

- Solution License Management
- Technical Support

# A. Solution Business

1. Software V&V
2. Cyber Security

SOFTFLOW

# A-1. SOFTWARE V&V

## ( Product 신뢰성 및 취약점 관리 )

**Software V&V는 올바른 SW를 올바른 방법을 통해 만들었는가를 검증 & 확인하는 과정 또는 프로세스 입니다.**

- **Validation (검증) : 사용자 요구사항을 만족시키는가? / 동적 테스트 (시스템 테스트) / 사용자 인수 테스트**
- **Verification (확인) : SW의 올바른 구현을 보장하는가? / 정적 분석 / 동적 테스트 (단위, 통합 테스트, 시스템 테스트)**


산업군의 급격한 Digital화

SW 비중이 크게 증가


Software 품질 관리 필요성 증가

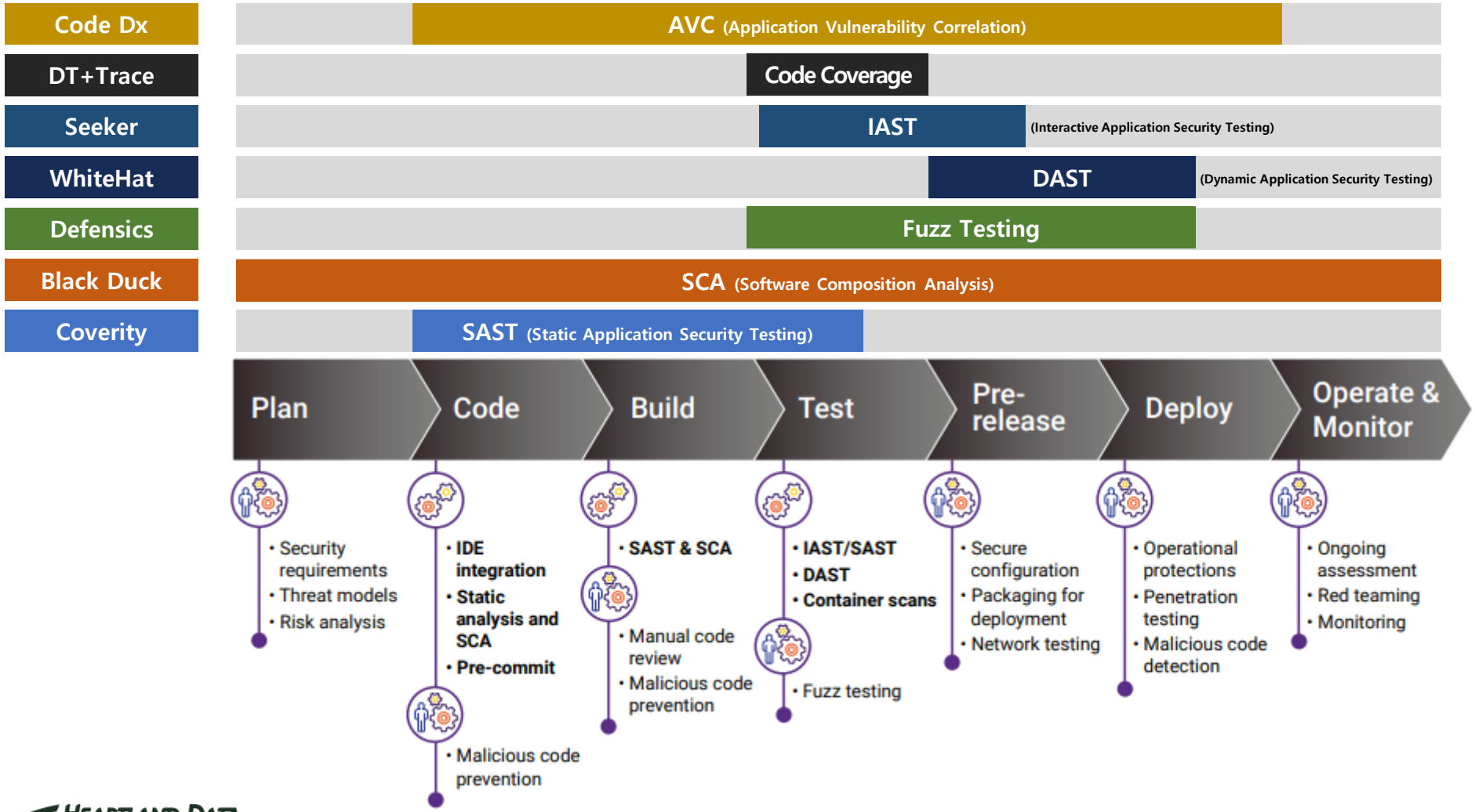
**당사는 SW 품질(안전&보안) 향상을 위하여 “Synopsys” 및 “Heartland.Data”와 함께 SW V&V 전반에 대한 솔루션을 공급**

SYNOPSYS®

HEARTLAND.DATA
Heartland.Data Inc.

## 고객의 Software Development Life Cycle 프로세스를 지원할 수 있는 신뢰성 및 취약점 검출 툴을 제공합니다.

- Software Risk를 조기에 발견 및 조치할 수 있도록 도움을 드립니다. (개발 시간 및 비용 절감 효과)



| | 파트너사 | 대표 솔루션 |
|---|---|---|
| Software V&V | Synopsys | **Software 신뢰성 확보 & 취약점 분석 Global No.1 “Synopsys”**<br>**Coverity** : 소스코드 품질/보안을 위한 코딩규칙 표준 준수, 시큐어 코딩, CWE 검사 수행 정적분석(SAST) 솔루션<br>**Black Duck** : 오픈소스 SW (OSS) 취약점 분석 및 라이선스 컴플라이언스 통합 관리 솔루션<br>**Defensics** : 알려지지 않은 취약점 검출에 최적화된 Test Case를 제공하는 지능형 퍼징 테스트 자동화 솔루션<br>**Seeker** : 대화형 application 보안 테스트 (IAST) 방식의 Web Application 보안 상태에 대한 가시성 제공 솔루션<br>**WhiteHat** : SaaS 기반의 동적 테스팅(DAST) 솔루션으로 웹 어플리케이션을 빠르게 진단하여 취약점 평가<br>**Code Dx** : 다수의 Application Security Testing Tools 데이터 취합, 연관성 분석(AVC) 및 코드 취약점 통합관리 솔루션<br>**Intelligent Orchestration** : Application Security Testing 실행을 DevOps 관점으로 최적화 & 자동화 관리 솔루션 |
| | Heartland.Data | **시스템 테스트를 위한 효율적이고 효과적인 방법론을 제시해 드립니다.**<br>**DT+Trace** : SW 동작의 장시간 트레이스를 통한 코드 커버리지 분석 및 성능 시각화 솔루션 |

* AVC (Application Vulnerability Correlation)

## Synopsys는 Global No.1으로 가장 빠르고 정확하게 어플리케이션 보안 및 품질, 컴플라이언스 위험을 관리

- Synopsys가 제공하는 업계 최대의 차세대 AppSec 솔루션 포트폴리오를 적용하여 소프트웨어 보안 위험을 전체적으로 관리

SYNOPSYS®

| Code Sight<br>IDE 기반 AppSec | Intelligent Orchestration<br>DevSecOps 통합과 자동화 | Code Dx<br>DevSecOps 통합과 자동화 |
|---|---|---|

| Coverity<br>SAST | Black Duck<br>SCA | WhiteHat<br>DAST | Seeker<br>IAST |
|---|---|---|---|
| Defensics<br>퍼징 | eLearning<br>개발자 트레이닝 | 오픈 소스 도구<br>통합 | 타사 도구<br>통합 |
| 보안 테스팅 서비스<br>침투, 모바일, 디바이스 | | | |

**최고의 소프트웨어 보안 솔루션 구축에 지금까지 20억 달러 넘게 투자해온 Synopsys**

**SDLC의 전체 스펙트럼을 커버하는 솔루션과 서비스를 공급하는 곳은 Synopsys가 유일합니다.**

## Coverity는 소스코드 품질 결함 및 보안 취약점 분석 솔루션으로 임베디드 SW, 엔터프라이즈, Web, Mobile 어플리케이션 분석

**Coverity (SAST)**

V&V 대상

**Software Source Code**

**( Embedded / Web / Mobile / Enterprise 용 SW 등 )**

V&V 목적

**개발 프로세스 초기의 코드 작성 과정에서 소프트웨어 품질 결함과 보안 취약점을 식별**

### 가장 강력한 정적 통합 분석 도구 : 코딩 규칙, 메트릭, 결함 및 취약점 분석

- 보안 취약점 분석 결과의 카테고리 별 필터링 및 트렌드 리포팅 제공, 보안정책 컴플라이언스 관리 지원
  > 예) OWASP Top 10, CWE/SANS Top 25, PCI DSS
- 코드 품질 이슈에 대한 업계 최고의 분석 엔진과 안전, 보안, 신뢰성과 관련된 표준에 대한 포괄적인 커버리지 제공
  > 예) MISRA, CERT C/C++, ISO/IEC TS 17961, AUTOSAR, CWE
- 통합 개발 환경 플러그인 Code Sight을 제공하여, IDE상에서 수 초 내에 코드 분석 결과 확인 가능
  > 분석 결과는 이슈 수정을 위한 모든 정보 포함 (상세 설명, 카테고리, 심각도, CWE 정보, 결함 발생 위치, 교정 지침, 데이터 플로우 추적 등)

**지원 개발 언어**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| • C/C++ | • Java | • PHP | • .NET Core | • Objective-C | • JSP | • Swift | • Scala | • iOS |
| • C# | • JavaScript | • Python | • ASP.NET | • Go | • Ruby | • Fortran | • VB.NET | • TypeScript |

**지원 프레임워크 : Java, JavaScript, C# 및 기타 다른 개발언어에 대한 70여종의 프레임워크를 지원**

**중요 검사 항목**

| | | | | |
|---|---|---|---|---|
| • API usage errors | • Concurrent data access violations | • Hard-coded credentials | • Memory-illegal accesses | • Resource leaks |
| • Best Practice coding error | • Control flow issues | • Incorrect expression | • Null Pointer dereferences | • Rule violations |
| • Buffer overflows | • Cross-site request forgery (CSRF) | • Insecure data handling | • Path manipulation | • Security best practices violations |
| • Build system issue | • Cross-site scripting (XSS) | • Integer handling issues | • Performance inefficiencies | • Security misconfigurations |
| • Class hierarchy inconsistencies | • Deadlocks | • Integer overflows | • Program hangs | • SQL injection |
| • Code maintainability issues | • Error handling issues | • Memory-corruptions | • Race Conditions | • Uninitialized members |

## Black Duck은 업계 최고의 SCA (Software Composition Analysis) 솔루션으로, 오픈 소스 보안 및 라이선스 컴플라이언스 위험 관리 제공

**Black Duck (SCA)**

V&V 대상

Open Source Software (OSS)

V&V 목적

오픈 소스 사용에 따른 보안 위협,
품질 문제 분석 및
라이선스 컴플라이언스 대응

### 소프트웨어 공급망 전반에서 이루어지는 오픈 소스의 보안 및 관리 도구

**SDLC의 각 단계에서 보안 취약점을 탐지하고 수정할 수 있도록 취약점별 세부 지침 및 기술적 통찰을 제공**

- 중요 위험 지표, 취약점 별 기술적 통찰, 세부 악용 정보 및 영향도 분석
- CVSS 2와 CVSS 3 점수 및 CWE 분류 데이터
- 일반적인 공격 패턴 목록 및 등급 (CAPEC)
- NVD에서 제공하지 않는 시간 점수 (Temporal score)

* NVD (National Vulnerability Database)

- 구성요소 업그레이드 및 개선 지침, 요인 완화 그리고 보정 제어
- 취약한 코드가 어플리케이션에 의해 호출되고 있는지 파악하는 취약점 영향도 분석
- 심각도, 솔루션 가용성, 악용 가능성, CWE 및 도달 가능성 등 여러 중요 데이터 점수에 따라 취약점 해결의 우선순위 지정 가이드

**오픈 소스 라이선스 컴플라이언스 위반 및 취약점 점검**

> 업계 최대 규모의 오픈 소스 “2,750+개 라이선스” Knowledge Base를 구축하여 라이선스 식별 및 컴플라이언스 위반을 예방

**코드 프린트, 소스 코드, 바이너리 등 다양한 방식의 분석기법으로 구성요소의 포괄적인 SBOM 및 취약점 분석 제공**

> NVD보다 평균 2주 빠른 취약점 정보 제공

**소스 코드 없이도 오픈 소스 식별 및 취약점 탐지**

> 소스 코드에 엑세스없이 벤더에서 공급받은 바이너리를 분석 가능하여 취약점 탐지 가능

**[ 탐 색 ]**

- 식별 : 코드, 바이너리 및 컨테이너에서 OSS 식별
- 탐지 : 구성요소의 일부분 및 수정된 구성요소 탐지
- 자동화 : DevOps 통합으로 스캔 자동화

**[ 보 호 ]**

- 매핑 : 구성요소를 알려진 취약점에 매핑
- 식별 : 라이선스 및 구성요소 품질 리스크를 식별
- 개발 및 생산 과정에 나타나는 새로운 취약점을 모니터링

**[ 관 리 ]**

- 정책 설정 및 시행 : OSS 사용 및 보안 정책을 설정하고 시행
- 자동화 : DevOps 통합으로 정책 시행을 자동화
- 수정활동의 우선순위 지정 및 추적

SOFTFLOW

## Defensics는 포괄적인 블랙박스 테스팅 솔루션으로 소프트웨어의 제로데이 취약점을 효과적이고 효율적으로 발견하고 해결 가능

### Defensics (퍼징)

V&V 대상

**개발 단계의 Software**

( OS, PC, 서버, 모바일 앱,
임베디드 시스템 펌웨어, 시스템 온 칩
등 프로세스에서 실행되는 모든
실행코드 테스트 )

V&V 목적

소프트웨어 상의
알려지지 않은 취약점을 사전에
발견하여 제로데이 공격 방지

### 더 스마트한 퍼징을 통해 더 빠르고 안전하게 소프트웨어 보안성 시험

- 사전 정의된 스마트한 Test Case 제공, 테스터가 수동으로 Test Case를 만드는 부담을 경감
  - > 차세대 퍼징 기법을 통한 Test suite를 지속적으로 업데이트 중 (Template, Generational, Evolutionary 등)
  - > 290여개 이상의 프로토콜 데이터 링크(L2)~어플리케이션 계층(L7)의 유/무선 프로토콜과 파일 형식의 퍼징 테스트 지원
- 커스터마이징을 위한 추가 확장 지원
  - > 파일 형식 및 프로토콜의 리버스 분석을 통해 사용자 정의 Test case를 생성
- 사용자 지정 입력이 있는 경우에는 Java, Python 및 선택한 전송 계층을 지원
  - > 계측 장비가 장착된 Defensics SDK를 사용하여 자체 Test suite를 작성 가능
- 문제 해결을 위한 상세한 데이터 보고서 제공
  - > 취약점 매핑 : CVE/CWE 및 Injection 유형 등의 취약점을 업계 표준에 매핑
  - > 문제 재현 : 취약점 트리거를 단일 테스트 사례로 좁혀 문제를 재현하고 수정 사항을 확인
  - > 문제 해결 패키지 : 소프트웨어 공급업체에 암호화된 문제 해결 패키지를 제공하여 공급망 전체에서 문제를 안전하게 협업하여 해결

국방, 항공, 선박, 산업용 기기, 의료용 기기

금융, 엔터프라이즈, 정부 및 공공

네트워크 사업자, 통신, 자동차, 기반 시설 등

SYNOPSYS®

## Seeker는 웹 어플리케이션의 취약점을 간단하고 정확하게 식별 및 검증하는 엔터프라이즈용 IAST

**Seeker (IAST)**

V&V 대상

Enterprise Web Application

V&V 목적

웹 어플리케이션의 보안표준 규정 준수에 대한 관리 및 취약점 탐지

### Synopsys의 대화형 어플리케이션 보안 테스트 (IAST)로 테스트 생산성 향상

- Seeker만의 능동 검증 기능(특허 기술)로 수십만개의 HTTP(S) 요청을 신속하게 처리하고 취약점을 식별 및 오탐률 제로 수준 유지
- 쉬운 설치 및 사용
  - > 코드가 실행되는 어플리케이션의 각 계층 또는 노드에 에이전트를 설치하면 실행 중인 어플리케이션에서 수행하는 모든 작업을 추적
  - > 웹 어플리케이션의 실행에 따라 취약점을 분석하여 별도의 스캔 없이 실시간으로 결과 확인 가능
- HTTP Request 시 입력가능한 Parameter 식별, 미 시험된 Parameter 확인, 악의적 입력 재수행 테스트
  - > 어플리케이션 공격 경로, 숨은 매개변수, 백도어 등을 더욱 폭넓게 탐색
- 자동화된 URL 매핑 : 웹 어플리케이션 Test Coverage(Endpoint 기반) 확인 및 테스트된 항목을 시각화
  - > 동일한 어플리케이션의 버전 간 테스트 범위 차이를 쉽게 확인 가능
- 업계 최초로 민감한 데이터 추적 기능 제공
  - > 사용자가 민감한 데이터를 지정하면 민감한 데이터가 암호화되지 않은 상태로 로그, DB 또는 File에 저장될 때마다 해당 데이터를 추적
  - > 데이터 암호화가 필요한 PCI DSS 섹션은 물론 GDPR과 같은 기타 산업 표준 및 규정을 준수하는데 도움

**실시간 분석 결과**

- 보안 취약점 위험도 평가
- 위험에 대한 명확한 설명
- 런타임 메모리값 및 컨텍스트
- 기술적 설명
- 취약한 코드 라인의 위치
- 컨텍스트 기반의 효과적 수정 지침

**지원 개발 언어**

- ASP.NET
- C#
- Clojure
- ColdFusion
- Go
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Kotlin
- PHP
- Python
- VB.NET
- Scala (incl. Lift)

**어플리케이션 유형**

- Ajax
- JSON
- 마이크로서비스
- 모바일 (HTTP/S 기반)
- RESTful
- 단일 페이지 어플리케이션
- 웹 (HTML5 포함)
- 웹 API
- 웹 서비스

**클라우드 플랫폼**

- Azure PaaS
- AWS
- AWS Lambda
- Google Cloud
- Tanzu (PCF)

## WhiteHat은 웹 프레임워크 및 어플리케이션 모두에 적합한 최신 웹 어플리케이션 보안 진단 도구

**WhiteHat (DAST)**

V&V 대상

Enterprise Web Application

V&V 목적

웹 어플리케이션의 보안표준 규정
준수에 대한 취약점 추이를 파악

### SaaS 기반의 DAST 솔루션으로 어떤 환경이든 적용하여 신속한 분석 가능

**WhiteHat만의 장점**

> 웹 어플리케이션의 코드 변경 자동 탐지, 분석을 무제한 지속하여 상시 위험 분석 가능
> 오픈 API 통합 : 보안 정보 시스템, 이벤트 관리 솔루션, 버그 추적 시스템, 웹 어플리케이션 방화벽
> WhiteHat Security Index를 통한 웹 어플리케이션 보안 현황 지표를 점수화하여 직관적 평가 가능
> 성능 저하 없이 프로덕션 웹사이트에 안전하게 적용 가능한 솔루션
> PCI DSS에서 요구하는 비즈니스 로직 분석과 침투 테스팅을 모두 실시 가능

**머신러닝(ML)과 인공지능(AI), 전문가 취약성 분석을 결합하여 최고 수준의 보안 테스팅 결과를 산출**

> 빠른 결과 도출을 통하여 사이버 공격을 초기에 탐지 및 대응 할 수 있음

**클라우드 기반 솔루션으로 별도의 하드웨어나 스캐닝 소프트웨어를 설치할 필요가 없음**

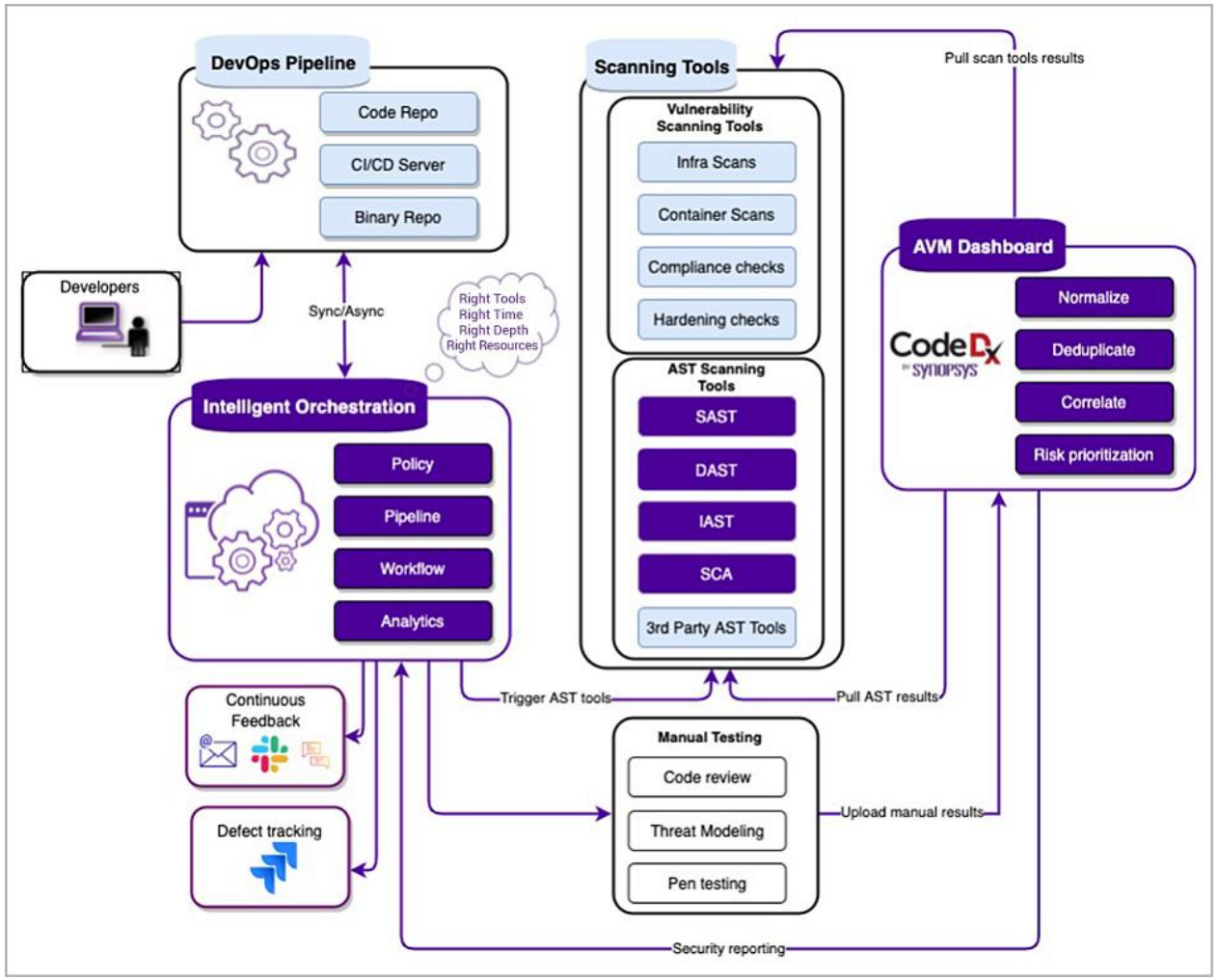
> 웹 서비스의 속도 저하 없이 1만개 이상 웹사이트를 동시에 온보딩하고 테스팅이 가능

**탐지 가능 취약점**

[ WASC Threat Classification 2.0 ]
- 어플리케이션 구성 오류
- 디렉토리 인덱싱
- HTTP 응답 스머글링
- 부적절한 입력 취급
- 불충분한 트랜스포트 레이어 보호
- OS 커맨딩
- 원격 파일 포함
- SQL Injection
- XML 외부 개체
- Xquery Injection
- 콘텐츠 스푸핑
- 핑거 프린팅
- HTTP 응답 분할
- 부적절한 출력 취급
- 메일 명령 Injection
- 경로 조작
- 라우팅 우회
- SSL Injection
- Injection
- 크로스 사이트 스크립팅
- 포멧 스트링 공격
- 부적절한 파일 시스템 권한
- 정보 유출
- 널 바이트 Injection
- 예측 가능한 리소스 위치
- 서버 설정 오류
- URL 리디렉터 오용
- Xpath Injection

[ OWASP Top 10 ]
- A1 – Injection
- A2 – 취약한 인증과 세션 관리
- A3 – 민감한 데이터 노출
- A4 – XML 외부 개체 (XXE)
- A5 – 취약한 접근 통제
- A6 – 잘못된 보안 구성
- A7 – 크로스 사이트 스크립팅 (XXS)
- A8 – 알려지지 않은 역직렬화
- A9 – 알려진 취약점이 있는 구성요소
- A10 – 불충분한 로깅 및 모니터링

## Code Dx는 Application Security Data를 한 곳에 모아 인사이트를 제공하는 Synopsys의 지능형 통합 AVC 솔루션




- 전사적인 보안 취약점 통합 관리 및 위험도 시각화
- 각종 Application Security Testing 도구 통합 Dash-Board 구성 지원
  - ✓ 사용성 높은 SCA, SAST, DAST, IAST 도구 100가지 이상 통합
  - ✓ DevOps와 보조를 맞춰 통합과 확장 가능
    - ➢ Jira, Jenkins, Visual Studio, Eclipse 등 기타 이슈 트래커와 통합 가능
    - ➢ 성능 클러스터로 빠르고 효과적인 상관관계 정립
- 결과 보고서 작성 시, 보안 위험에 따라 자동으로 우선순위를 부여
  - ✓ Triage Assistant 기능(머신러닝)을 기반으로 우선순위 산정
  - ✓ NIST, PCI, HIPAA, DISA, OWASP Top 10 등 컴플라이언스 표준에 따라 우선순위 결정
  - ✓ 자동으로 우선순위 높은 취약점을 개발자 이슈 트래커로 보내 시정 조치 (정확한 코드 라인과 링크하여 결함별로 검토 가능)

**PLUS POINT !!**

AST 도구들의 중복 결과를 통합하고 불필요한 결과를 제거하여 데이터 표준화

SYNOPSYS®

* AVC (Application Vulnerability Correlation)

## DT+Trace는 타겟 트레이스를 통한 “Software 시각화” 및 코드 커버리지를 분석하여 개발의 효율 및 품질 향상을 실현

- 통합 시험 + 성능 프로파일링: Test Point 자동 삽입을 통한 다양한 코드 커버리지 및 소프트웨어 성능 확인
- 유연한 시험 환경 지원: C, C++, C#, Java 및 Android, Linux, VxWorks, Windows 등 다양한 환경 지원


### 활용 #1 ( SW 품질 향상 )

**Real-time 코드 커버리지 측정 !!!**

- Statement, Branch, MC/DC, Function Coverage

- 타겟 기반의 코드 커버리지 측정
- 요구사항 기반의 코드 커버리지 확인
- Test 누락과 Unused code의 정확한 확인
- Statement coverage의 실시간 확인

### 활용 #2 ( 성능 개선 )

**간단한 성능 평가 !!**

- 실행 시간 – 주기 시간
- 처리시간의 분석
- CPU 부하 – 프로세스 점유율

- Core/Task/함수의 실행 시간 및 주기 측정
- 병목현상 확인 – 부하 높은 프로세스와 함수 발견
- SW 실행 흐름 파악
- CPU 로드 및 메모리 사용량 측정

### 활용 #3 ( 디버깅 )

**정확한 원인 분석 !**

- SW 실행 경로 및 Task 스위칭 확인
- 변수 모니터링
- 하드웨어 신호와 소프트웨어 동작 확인

- 장시간 Trace로 재현이 어려운 결함분석에 효과적
- 다양한 통신 인터페이스를 통한 시험 환경 구성
- 코드 커버리지 기준의 Tester간 Test 평준화
- SW 수정 후, 의도한 대로 동작하는지 확인

## Synopsys의 Software Integrity Portfolio는 ISO 26262 & 21434 표준에 부합하여 자동차 분야 SW V&V에 대응 가능합니다.

### Challenges in Automotive Software Development

**변화된 개발 환경**

- IT 기술 융합으로 자동차 SW 개발환경에서 민첩성 및 통합성 증대
- 자율주행 차량의 등장과 함께 연결성, 위험 및 노출의 범위가 확대

**개발 시 요구사항**

- Software의 규모가 더욱 커지고 복잡해짐
- 여러 Software의 통합으로 SW 공급망 및 공급자 관리 필요
- 연결된 구성 요소에 대한 통신 안정성 및 견고성 요구됨
- 개발 및 양산 중 Cyber security 취약성 관리 필요
- 개발 중 사용할 적격한 SW V&V 툴 채택 필요



ISO 26262
ISO 21434
MISRA C
MISRA C ++
AUTOSAR

### Synopsys Software Integrity

Synopsys의 솔루션은 품질 보증(QA), 기능 및 성능 테스트, 보안 감사를 통해 개발팀이 코드의 결함을 테스트 할 수 있는 쉬운 방법을 제공

**Coverity**

Code 품질 향상을 위한 결함 & Cyber Security 탐색 및 수정을 지원

활용 예) ISO 26262 & 21434 가이드라인 기반으로 Coding 표준 대응 MISRA C/C++, AUTOSAR C++, CERT C/C++ 외 기타

**Black Duck**

Software에서 third-party 또는 open source 컴포넌트들을 식별 지원

활용 예) Automotive Grade Linux 또는 Android와 같은 오픈소스 플랫폼에서 수백개의 SW Package 포함한 일반적인 HMI에서의 SW 구성을 쉽게 식별

**Defensics**

Fuzzing을 통해 SW 충돌 원인 식별, Cyber Security 취약성 또는 안전 문제의 근본 원인이 될 수 있는 소프트웨어 결함 식별 지원

활용 예) Defensics는 2014년 Heartbleed SSL 취약점을 발생시킨 이상 현상을 식별

## Synopsys는 의료 기기 보안 지식과 전문성을 겸비하였으며 FDA 등 주요 기관 및 세계 최고의 의료기기 기업이 신뢰하는 기업

IEC 62304 / UL 2900-2-1 / AAMI TIR57 / FDA 510 (K) / FDA Premarket Cybersecurity Guidelines

Synopsys는 여러 의료기기 가이드라인의 Cyber Security 요구사항에 맞춰 알맞은 도구 및 서비스를 제공합니다.

### Black Duck (SCA)

Black Duck은 Software Composition Analysis (SCA)으로 Open-Source bill of materials (BOM)을 생성하여 전체적인 SBOM을 제공

### Coverity (SAST)

Coverity Static Analysis를 통하여 의료 기기의 소스 코드에서 결함 및 보안 취약점을 식별하고 수정을 지원

### Defensics (Fuzz Testing)

Defensics는 의료 기기에서 사용되는 다양한 프로토콜(Bluetooth, HL7, DICOM 등)로부터 유발될 수 있는 Zero Day 취약점을 Fuzzing Test를 통하여 식별 가능

# A-2. Cyber Security

## ( Data & Cyber Risk 관리 중점 )

## 전세계적으로 사이버 위협이 증가하면서 위협 별 Cyber Security 대응 방법 수립의 필요성이 높아지고 있음

- Cyber Security 전략 수립을 위하여 개인 또는 조직을 대상으로 공격 목표와 공격 유형을 아래와 같이 식별 필요
- Data Risk 관점 : 원천적 Data 보호를 위한 File 암호화, Data 전송구간 암호화, 암호화 키에 대한 관리 솔루션 추천
- Cyber Risk 관점 : 갈수록 진화하는 Cyber-attack 유형에 대한 지능형 탐지 및 신속한 대응 솔루션 추천

| World Top 5 Data Risk (공격 목표) | |
|---|---|
| 1 | R&D information |
| 2 | Financial information |
| 3 | Business communication (E-mail) |
| 4 | Company confidential information |
| 5 | Trade secrets |

| World Top 5 Cyber Risk (공격 유형) | |
|---|---|
| 1 | Ransomware |
| 2 | Phishing and Social engineering |
| 3 | Denial of Services (DoS) |
| 4 | Botnets |
| 5 | Man-in-the-middle attack |

## 당사는 Cyber Security 전략을 위한 최적의 솔루션을 제안 드리기 위하여 검증된 Thales 및 DarkTrace사의 제품을 공급합니다.

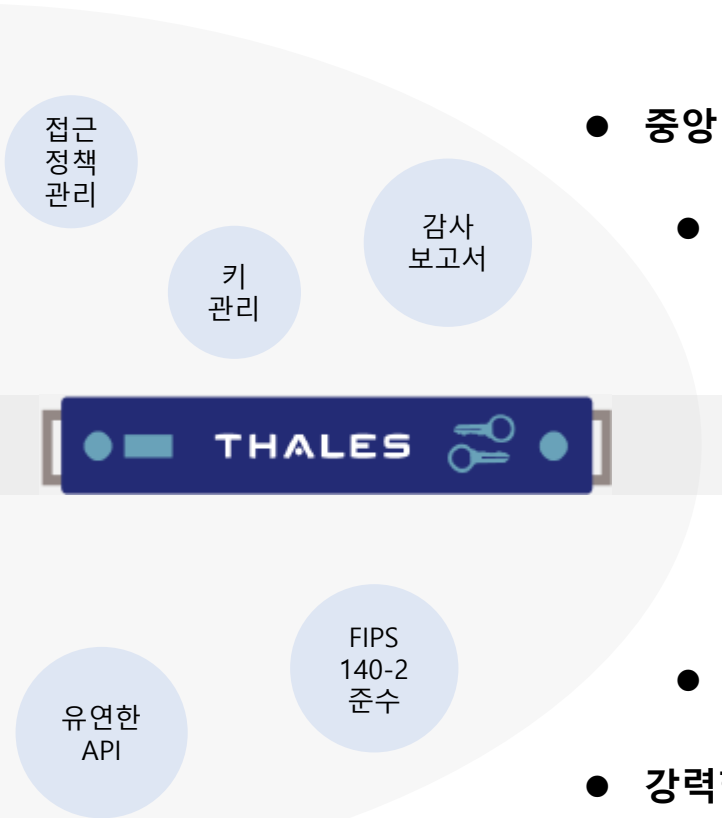
THALES

DARKTRACE

| | 파트너사 | 대표 솔루션 |
|---|---|---|
| Cyber Security | Thales | **Data Risk 분야 Global Leader "Thales", 다양한 환경에서 민감 Data를 안전하게 보호해 드립니다.**<br>CipherTrust Manager ( CTM ) : 중앙 집중식 Key Management System (암호키 Lifecycle 관리 및 HSM을 통한 안전한 보호)<br>CipherTrust Encryption ( CTE ) : File 암호화 솔루션 (CTM과 연동하여, 파일 서버의 데이터를 빠르게 암복호화 지원)<br>High Speed Encryption ( HSE ) : 고성능 통신 구간 암호화 솔루션 (Data 지연이 없는 통신 암호화 기술을 적용한 고성능 Encryptor) |
| | DarkTrace | **디지털 자산(클라우드 / 앱 / 이메일 / 앤드포인트 / 네트워크 / 제로트러스트 / OT) 전체를 안전하게 보호**<br>(DarkTrace 제품군은 DarkTrace 만의 Self-Learning AI를 지원하여 다양한 위협에 지능적으로 대처가 가능합니다.)<br>DarkTrace Prevent : 취약점 우선순위화 및 취약 포인트 보안 강화를 통한 Cyber risk 관리 솔루션<br>DarkTrace Detect : 최신 AI 알고리즘 기술을 통한 디지털 자산의 Cyber Attack 실시간 가시화 솔루션<br>DarkTrace Respond : Detect로 가시화된 Attack이 발생될 때마다 Respond가 자동으로 작동하여 공격을 무력화 하는 솔루션<br>DarkTrace Heal : (2023년 출시 예정) Cyber Attack의 피해 복구를 위한 시스템 복구 솔루션 |

## CipherTrust Manager는 다양한 구축환경에 적용 가능한 중앙 집중화된 간결한 데이터 보안 정책 및 키 관리를 지원

- 강력한 연동성을 바탕으로 Data Security Platform을 구축하여 전체 Data 관련 시스템에서의 암호 키 생명 주기를 관리 가능합니다.



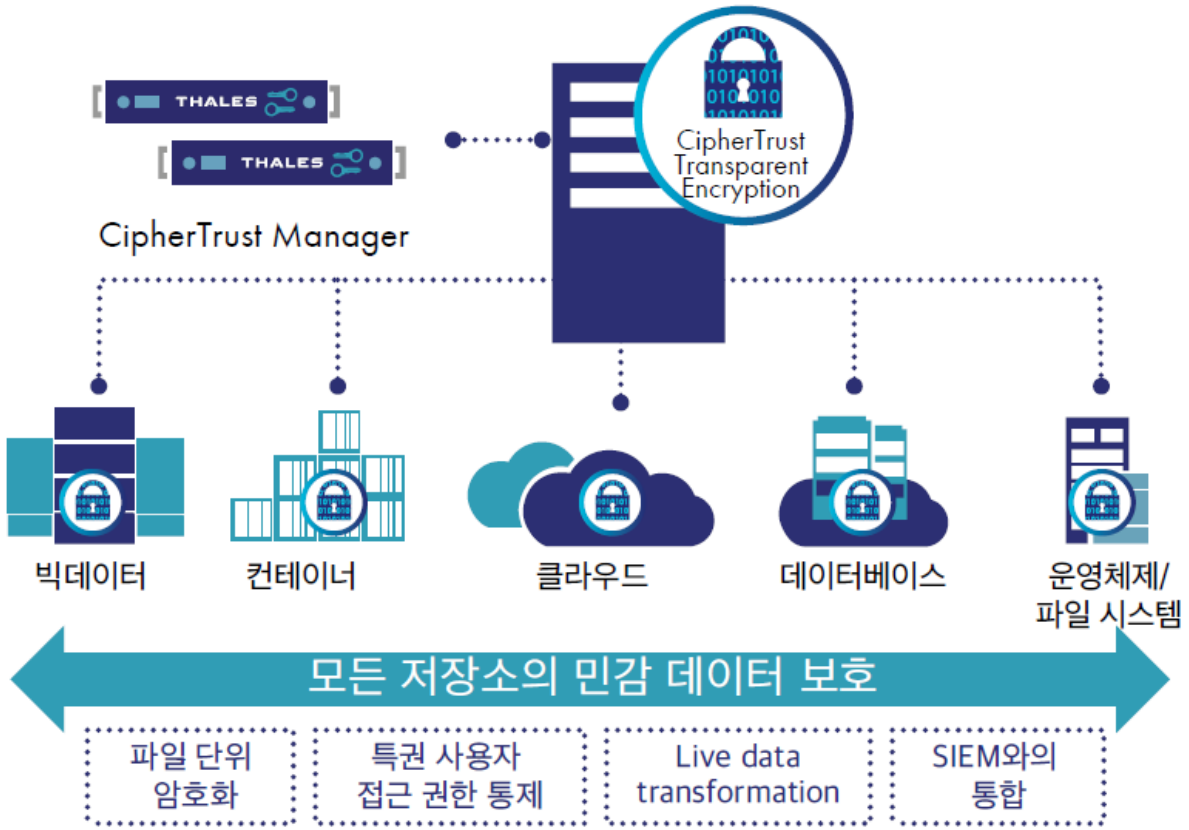

- 중앙 집중화된 키 관리 및 역할 기반 정책에 따른 통제
  - 자사의 다양한 암호화 제품(파일 암호화, 구간 암호화 등)의 통합 관리 기능
    - 다양한 로그 포멧 지원을 통해 향상된 감사 및 보고서 기능, 맞춤형 경보 기능

**CipherTrust Manager (CM)**

  - On-Prem or Cloud 형태로 시스템 구축, HSM 내장 또는 연동을 통해 FIPS 140-2 L3 지원
  - 자동화된 암호화 및 관리 기능 구현을 위해 다양하고 유연한 REST API 지원
- 강력한 역할 분리와 Multi-tenant 지원

## CipherTrust Encryption (CTE)의 기업의 민감 데이터 보안을 위하여 포괄적인 보호 기능을 제공하고 있습니다.

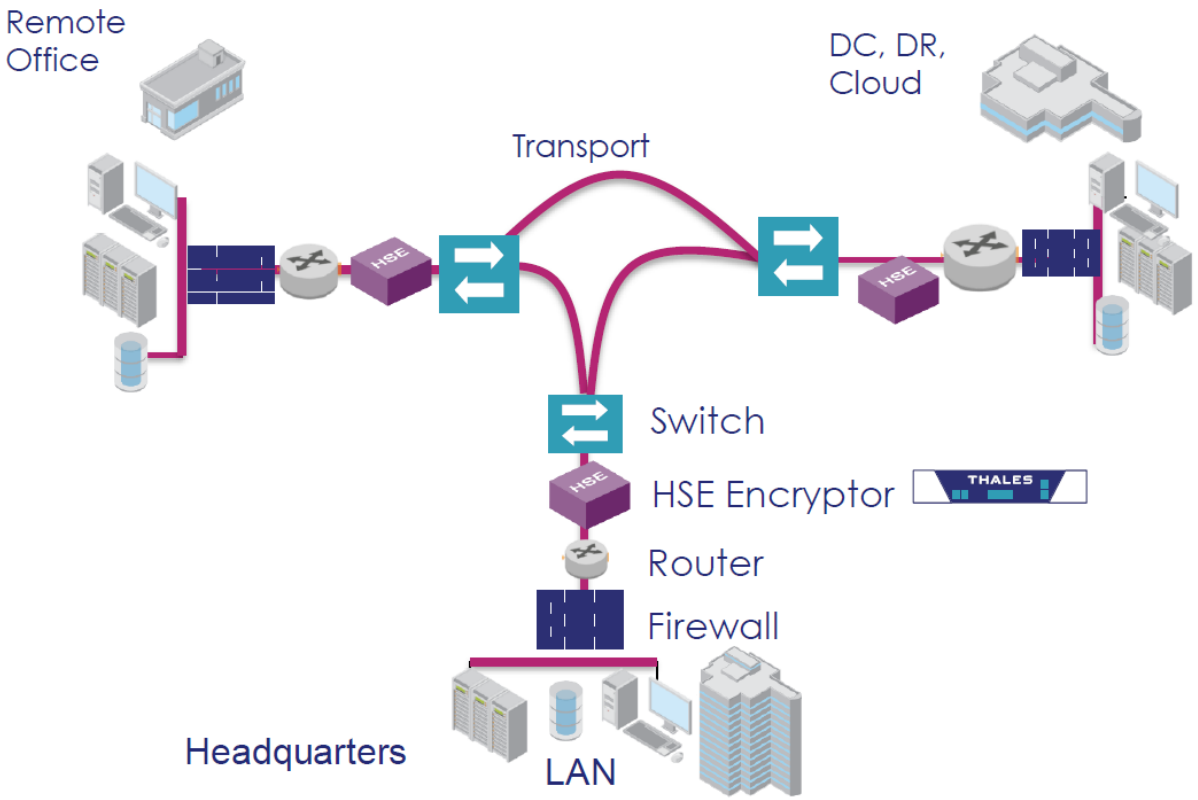
- CTE는 CipherTrust Data Security Platform에 포함되어 CM을 통하여 데이터 보안 운영을 통합하여 전사적 위험관리를 가능하게 합니다.




- 모든 형태의 저장소의 민감 데이터 투명하게 보호
  - ✓ 파일, 볼륨, 클라우드 스토리지를 보호와 동시에 접근 통제 및 접근 감사 로그 제공
  - ✓ 고성능 하드웨어 가속 암호화로 파일 단위 암호화
- 세분화된 접근 권한 지정 방식
  - ✓ 시스템, LDAP/Active Directory, Hadoop 및 컨테이너에서 사용자별, 그룹별 정책 적용
  - ✓ 이외에도 프로세스와 파일 유형, 날짜, 기타 변수에 따라 접근 통제 가능
- Live Data Transformation
  - ✓ 중단 없는 암호화와 CM과의 키 교체가 가능
- 포괄적인 보안 분석
  - ✓ 보안 분석 로그 및 보고서는 SIEM 시스템을 사용하여 규정 준수 보고 체계를 간소화

## HSE는 고성능의 Ethernet Encryptor로 모든 네트워크 구간에서 데이터 암호화를 지원합니다.

- HSE는 방화벽과 스위치 사이에 설치되어 구간 통신을 암호화하고 CipherTrust Data Security Platform에 포함되어 CM과 연동
- 1/10Gbps Link 기준 전송률이 IPSEC은 255Mbps/2.3Gbps이나 HSE는 983Mbps/9.5Gbps로 3배 이상의 암호 통신 성능을 구현
- 네트워크 환경에 맞춰 Virtual Encryptor 부터 최대 100Gbps Encryptor 까지 네트워크 구간 성능 별 선택 구성이 가능




**Model: CV1000**

- Support : Virtual Encryptor
- Level : Sever to Sever
- 목적 : Cloud 서비스 endpoint 간 구간 암호화 구축용

**Model: CN4000 시리즈**

- Support : 100Mbps – 1Gbps 용
- 특징 : 저비용, 고성능
- 목적 : 원격지 보안 연결을 위한 소형 Encryptor

**Model: CN6000 시리즈**

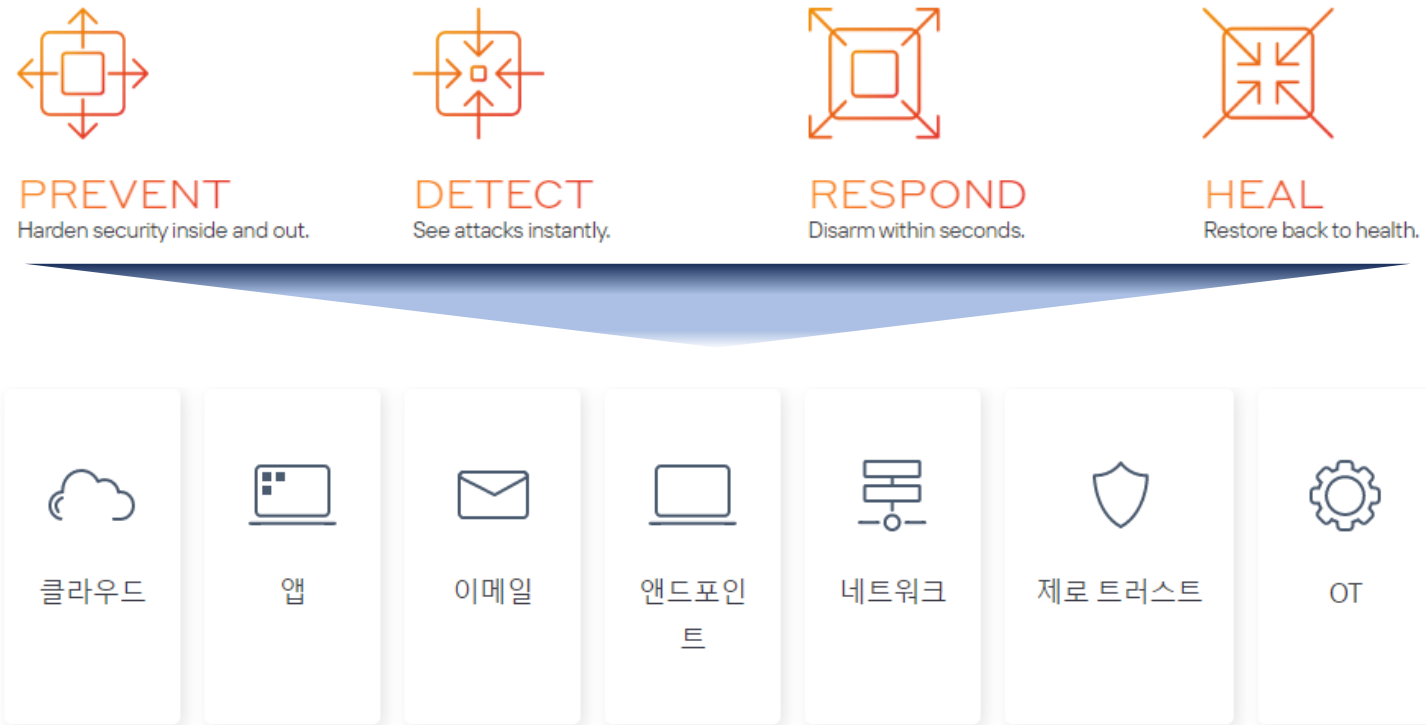
- Support : 1 – 10 Gbps
- 특징 : 랙 마운트 1U type
- 목적 : 사설 네트워크망 또는 데이터 센터급 구간 암호화 구축용

**Model: CN9000 시리즈**

- Support : 100 Gbps
- 특징 : 랙 마운트 2U type
- 목적 : 차세대 데이터 센터 또는 코어 네트워크 구간 암호화 구축용

## DarkTrace의 Cyber AI Loop는 사이버 보안에 대한 Prevent (예방) / Detect (탐지) / Respond (대응) / Heal (치료) 제품

- Loop의 모든 사이버 보안 AI 기술을 접목하여 Cyber Attack에 대한 신속하고 지속적인 지능형 대응으로 공격 방어 능력을 강화합니다.
- Cyber AI Loop는 머신러닝 기반의 자가 학습 탐지 기능을 탑재하여 공격 식별 및 대응이 즉각 자동적으로 이루어집니다.
- Cyber AI Loop는 Cloud 부터 OT 영역까지 모든 형태의 IT 자산을 보호 가능합니다.
- 모든 업종에 대한 Best Practice 보유
  - ✓ 금융 / 제조&공급 / 에너지&공공 / 정부&국방 / 미디어 / 기술&통신 / 의료&제약 / 교통&운송 / 소매&전자상거래 / 법률&인사



# B. R&D Business

1. 자체 Solution 개발
2. 연구 Project

# B-1. 자체 Solution 개발

## ( Network Security Management 관련 기술 )

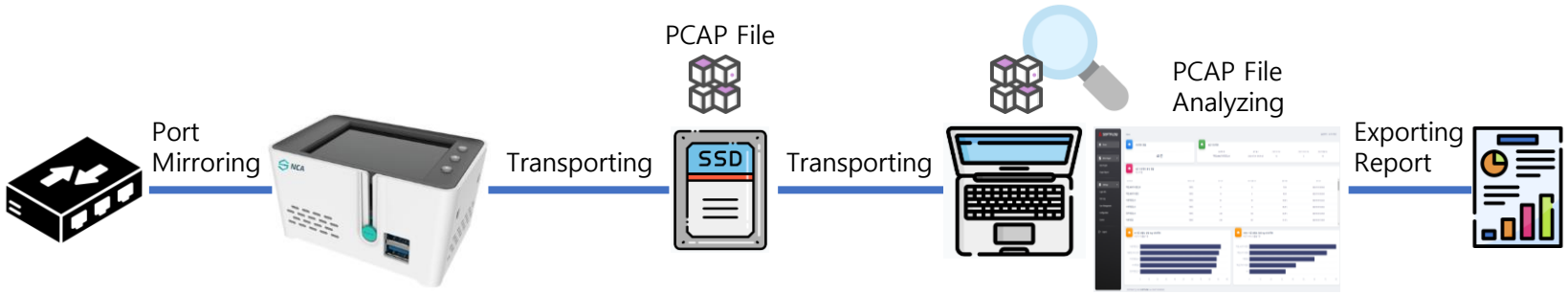
## 당사는 망분리 또는 폐쇄망 환경에서의 네트워크 보안 관리 기법을 연구하여 자체 개발한 NCA 제품을 공급하고 있습니다.

### 시장 요구 사항

- 요구 시장
  1) 망분리 환경 : 국가 및 공공 기관 / 국방 / 금융
  2) 폐쇄망 환경 : 산업 및 국가 주요 기반 시설

- 요구 사항
  1) 망분리 또는 폐쇄망의 분리된 네트워크 환경에서의 보안 이상 징후 (비인가 행위) 분석 및 보고서 생성
  2) 네트워크 보안 감사 시 이상 징후에 대한 평가 지표 제시 (비인가 자산, 연결 등)

### 개발 제품




**NCA Capture**

소형 네트워크 트래픽 수집 장치 (포트 미러링 방식)
- 휴대 및 설치가 용이하여 현장 보안 점검에 적합

**NCA Analyzer**

- 수집된 네트워크 트래픽을 빠르게 분석하는 SW
- 관리자 네트워크 정책을 기준으로 이상 징후 탐지 (비인가 IP / 비인가 서비스 포트 / 비인가 연결)

**제품명 : NCA** (Network Capture and Analyzer)

- 구성 : NCA 수집기 & 분석기 Set

분리된 네트워크 환경에서의 네트워크 보안 이상 징후 분석 및 보고서 생성의 기능을 가진 보안 관리 지원 도구

비인가 행위에 대한 탐지 자료 및 증거 패킷 파일 제공을 통한 보안 감사 대응

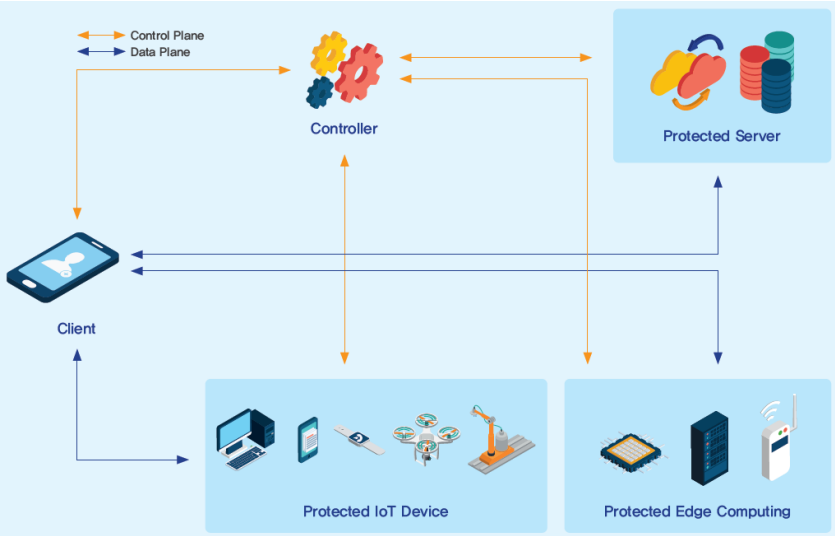
# B-2. 연구 Project

## ( IoT 플랫폼 보호 및 기기 이상징후 탐지 기술 )

## 소프트플로우의 SOFLO.IoT는 각종 IoT 기기 접근 관리 보안성 향상을 위하여 보안 플랫폼을 구현하고자 진행하는 연구 Project

### SOFLO.IoT의 핵심 보안 기능

1) Zero Trust 기반 SPA 매커니즘 : Data 채널 연결 전 / 기기 및 사용자 인증 절차 수행
2) SDP 기반 동적 경계망 기술 : 기기 신원 중심 동적 경계망 생성 및 배포
3) Data 전송 보호 기술 : 기기 간 Data를 mTLS를 기반으로 암호화 하여 전송




### SOFLO.IoT 적용 가능 분야

스마트홈 / 스마트국방 / 스마트공장 / 스마트시티 / 자율주행차 / 디지털헬스케어

### SOFLO.IoT 연구 Project 목표

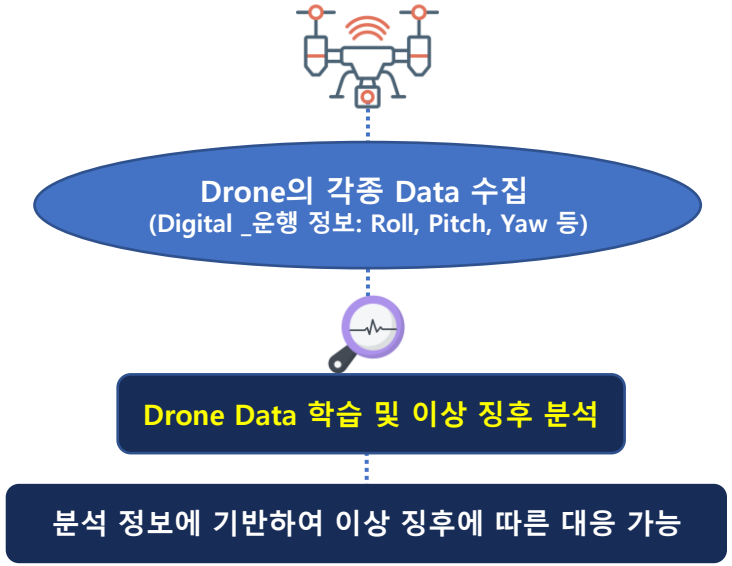
- SOFLO.IoT 플랫폼 구축 시연 : ~ 2023년 2분기 / 홈네트워크 기기 환경의 데모 환경 구현
- SOFLO.IoT Client SDK 적용 가능 기기 확대 : 지원 OS, HW 사양, 통신 환경 등 추가 연구 진행
- SOFLO.IoT 모델 사업 협력 파트너 구축 및 시장 진입

## 소프트플로우는 21년 부터 국방벤처 지원사업 과제를 통하여 AI 기반의 드론 이상 징후 탐지 기술을 연구하고 있습니다.

### 연구 Project 핵심 기능

1) Drone Data 수집 : 드론 통신 및 제어 모듈과 연계하여 각종 Data를 실시간 수집 (연계 기술 협업 중)

2) Drone Data 학습 및 분석 : 수집 데이터의 머신러닝을 통한 분석




### 연구 Project 적용 가능 분야

국방 (드론 이외 각종 무인 체계) / 민수 (무인 드론, UAM, 자율주행차량 등)

### 연구 Project 목표

- 분석 정확도 향상 : Drone 이상 징후 탐지 실증 시험 (~2023년 예정) / 드론 시험 비행을 통한 이상 징후 조건 및 Data 수집 & 학습
- 드론 관제 센터용 드론 이상 징후 탐지 시스템 모델 개발 : 드론 제조사와 협력 모델 탐색 중
- 드론 이외 타형상의 무인 기체 이상 징후 탐지 추가 연구 진행


# C. Service Business

1. Consulting
2. Maintenance


# C-1. Consulting

## ( SW V&V and Cyber Security 분야 전문 상담 )

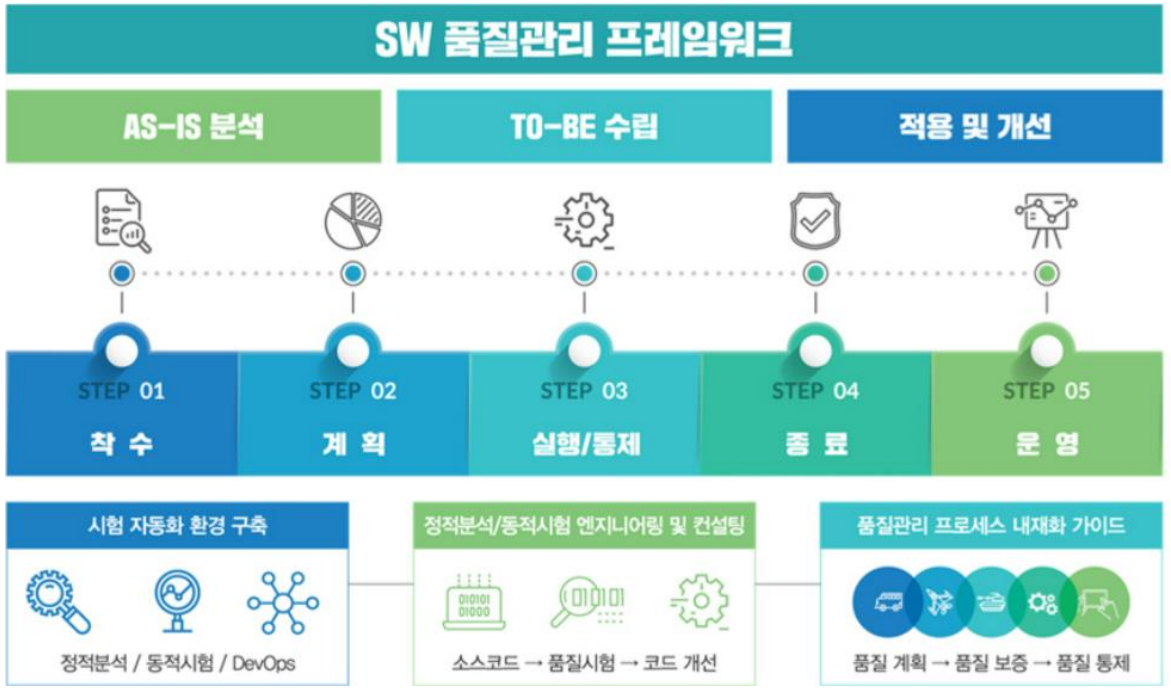
## 소프트플로우는 국제 표준과 다양한 산업 도메인의 경험과 특수성을 바탕으로 SW 품질관리 프레임워크를 구축

- SW 품질 향상과 신뢰성 확보를 위해서는 SW 개발 생명주기 전반에 걸친 품질 관리 활동과 시험 자동화 환경이 필요합니다.

### 시험 자동화 환경 구축
- 테스트 전략 도출 및 시험 환경 구축
- 품질 시각화 및 결과 확인 자동화

### 정적분석 / 동적시험 엔지니어링
- SW 품질활동 및 현황 진단
- SW 품질 요구사항 및 목표 도출
- SW 품질활동 수행 및 품질 점검

### 품질관리 프로세스 내재화
- SW 품질관리 계획 및 프로세스 수립
- SW 품질관리 방안 가이드





### Consulting 기대효과

- 정적분석 및 동적시험 기반의 SW 품질 향상 및 신뢰성 확보
- 다양한 테스팅 기법 및 품질 분석을 활용한 정량적인 품질 측정, 결함 및 취약점 제거
- 도구 기반의 테스트 자동화 환경 구축 및 효율적인 테스트 방안 컨설팅
- 품질관리 현황 분석, 품질 프로세스 구축, 개선 및 효율화

## 소프트플로우는 다양한 보안 기술을 활용하여 보안 컨설팅 및 엔지니어링 서비스를 제공합니다.

- 보안 기술은 각각의 산업 도메인과 기업의 비즈니스 환경을 고려하여 맞춤형 적용이 필요합니다.

### 산업제어시스템 보안 점검 및 컨설팅

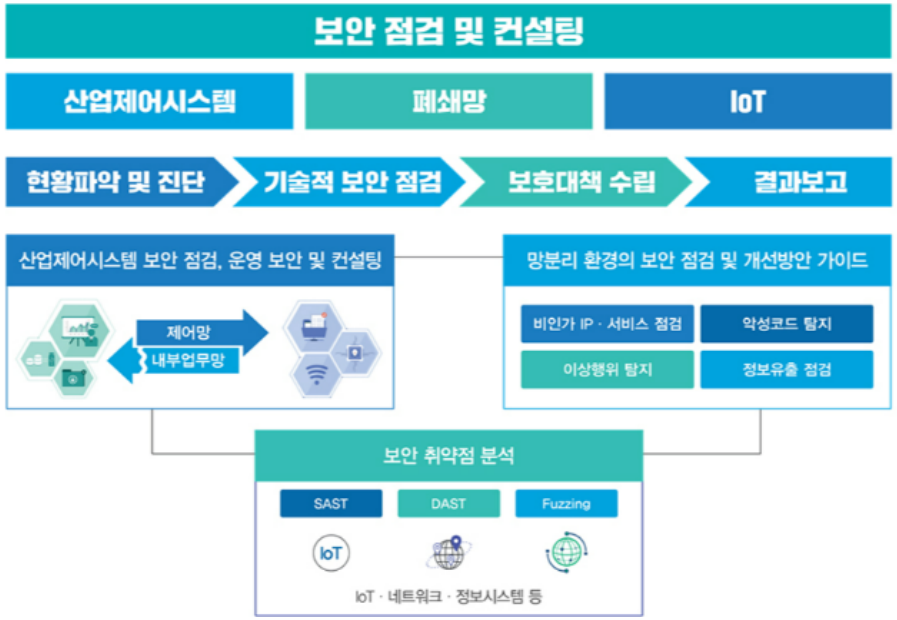
- 네트워크 트래픽 분석 기반의 이상징후 점검
- 업무망/제어망의 취약점 점검
- 산업제어시스템 운영보안 환경 구축 및 가이드
  ex) IEC 62443 등
- 보안 공격, 침투 테스트, 취약점 분석 교육

### 폐쇄망 보안 점검 및 개선방안 가이드

- 망분리 환경의 내부망/외부망 보안 상태 진단
- IT 인프라, 네트워크, 서버 등의 취약점 점검
- 기술 기반의 보안 대책 및 대응방안 수립을 통한 보안 방어체계 구성 가이드

### 임베디드 취약점 및 Anti-Tampering

- IoT, 산업용 장비 및 기기 대상의 다양한 테스트 기법을 활용한 보안 테스트
- 개발, 양산, 운영 단계의 안티 탬퍼링 솔루션 제공
- 보안 테스트 자동화 환경 구축 및 내재화





### Consulting 기대효과

- 주요정보통신기반시설 및 정보시스템의 침해위협 식별과 제거
- 보안 관리 체계의 성숙도 파악
- 보안침해 사고 예방을 위한 정보보호 계획 및 대책 수립
- 보안 기술 관련 중복 투자 방지 등의 효율적인 보안 기술 투자


# C-2. Maintenance

## ( Solution license management & Technical support )

**복잡해지는 Solution들의 License 정책으로 고민이 많은 고객을 위하여 사용 환경에 맞는 최적의 설계를 제공합니다.**

당사를 통하여 Solution을 도입한 고객들을 대상으로 라이선스 갱신 정보의 체계적 관리 지원

- License Renewal 관리 : 갱신 정보 관리 (갱신 일정 정보, 제조사 라이선스 변동 사항 정보, 기술 지원 종료 일정 정보 등)
- License Upgrade 제안 : 현 버전과 비교 정보, 업그레이드 경제성 분석 의견 제시 등
- 관련 Sales 전문가가 Solution License 관련 상담을 신속하게 진행

**소프트플로우는 공급한 솔루션을 위한 최선의 노력과 책임을 다하고 있습니다.**

취급 Solution

SYNOPSYS®

HEARTLAND.DATA
Heartland.Data Inc.

[ Software V&V Solution ]

THALES

DARKTRACE

[ Cyber Security Solution ]

**소프트플로우는 다양한 산업군에서 풍부한 경력을 보유한 보안 인력 전문가를 바탕으로 양질의 기술 지원 서비스를 제공합니다.**

고객의 기술적 문제를 진단하고 빠르게 대응 할 수 있도록 고객별 특이사항 정보를 History화하여 지속 관리합니다.

- 고객 기술 지원 포털 (23년 하반기 오픈 예정) : 포털에서 기술지원 Ticket 생성으로 간편하게 신청
  - ✓ 당사를 통한 Solution 구매 고객을 대상으로 포털 ID 발급
  - ✓ 고객별 기술 지원 이력 History 제공을 통한 빠른 진단 및 대응 가능
  - ✓ 고객 기술 지원 포털 내에 관련 분야 기술 문서 공유하여 최신 기술 습득 가능하게 지원

고객의 Solution에 대한 기초 사용 능력 및 최신 기술 소양을 한 단계 높여 드릴 수 있도록 교육 프로그램을 제공 하고 있습니다.

- 유료 기술 교육 또는 세미나 신청 : Solution 사용자 교육을 위한 전문 교육 또는 세미나 서비스 이용 가능
  - ✓ 기술 교육 : 신규 보안 담당자 or 신규 입사자 등 대상으로 Starter 교육 / 고급 기술 획득을 위한 중급자 교육

    예) Software V&V 도구 사용 가이드 (초급/중급)
  - ✓ 기술 세미나 : 최신 기술 트랜드 습득

    예) Software V&V Tool 통합 관리 기술 및 AVM 트랜드

# Question & Answer

여러분의 궁금증을 해결해 드리겠습니다.

SOFTFLOW

# Thank you!

SOFTFLOW

소프트플로우㈜

연락처 : ( Tel ) 070-7724-2752 / ( E-mail ) info@softflow.io

주　소 : (13449) 경기도 성남시 수정구 달래내로 46, A타워 8층 805호