SECULETTER CDR WHITEPAPER · V1.0

탐지의 시대는 끝났다 — 재조립의 시대가 시작된다.

CDR이 답하는 N2SF 시대의 콘텐츠 보안

망분리 30년의 마지막 장(章), 그리고 다음 장의 첫 문장 —
공공·금융 의사결정자를 위한 CDR 백서.

발행	주식회사 시큐레터	일자	2026년 5월
판본	1.0 (공공·금융 결재자 판)	문의	sales@seculetter.com

Executive Summary

공격자는 더 이상 코드로 침투하지 않습니다. 합법적으로 보이는 문서·이미지·압축 파일 그 자체가 무기로 진화했고, 탐지·격리·차단을 전제로 한 30년 된 방어 모델은 N2SF 라는 새로운 분류 체계 앞에서 구조적 한계를 드러냈습니다. CDR(Content Disarm & Reconstruction · 콘텐츠 무해화 및 재조립) 은 위협을 찾는 일을 그만두고, 콘텐츠를 안전한 형태로 재조립함으로써 이 문제를 닫습니다.

5가지 결론

- **N2SF-CD-6 은 "콘텐츠 무해화(CDR) 적용" 을 직접 명시한 의무 보안통제다.** 2026년 5월 '국가 사이버보안 기본 지침' 본격 시행과 함께 CDR 은 권고가 아닌 의무로 작동합니다.
- **공격은 콘텐츠 그 자체가 되었다.** 매크로·임베디드 객체·하이퍼링크는 더 이상 예외가 아니라 표준 페이로드입니다.
- **탐지 기반 방어는 N2SF 분류 체계와 정합하지 않는다.** 등급별로 다른 신뢰 모델을 적용하려면 "차단" 이 아니라 "변환" 이 필요합니다.
- **CDR 은 판정하지 않는다 — 분해하고 재조립한다.** 그래서 0-day 와 미탐을 원천적으로 무효화합니다.
- **공공·금융은 더 이상 SaaS·웹 콘텐츠 채널을 닫아둘 수 없다.** 업무 연속성과 보안 등급을 동시에 만족시키는 단 하나의 기술이 CDR 입니다.

> *이 백서는 CISO · 정보보호팀장 · 시스템 운영 책임자 · CFO 결재라인을 위해 작성되었습니다. 우리는 시큐레터를 팔기 위해 이 문서를 쓰지 않았습니다. N2SF 시행 이후 한국의 모든 공공·금융 기관이 곧 마주칠 의사결정 — "탐지를 계속 신뢰할 것인가, 아니면 콘텐츠를 안전하게 재조립할 것인가" — 에 대한 합리적 비교 근거를 제공하기 위해 이 문서를 씁니다.*

목차

1장. 변곡점 — 규제·위협·기술이 동시에 바뀐 24개월

> *2024년부터 2026년 사이, 한국의 콘텐츠 보안은 두 번 다시 돌아갈 수 없는 강을 건넜습니다. N2SF 가 망분리 30년의 끝을 선언했고, 그 다음 문장은 아직 쓰여지지 않았습니다.*

1.1 규제 축 — N2SF, 그리고 금융 규제 재설계

2025년 9월 9일, 국가정보원은 코엑스 사이버 서밋 코리아에서 **국가 망 보안체계(N2SF, National Network Security Framework) 보안가이드라인 정식판 1.0** 을 공개했습니다.[1] 정부 전산망을 업무 중요도에 따라 **C(Classified · 기밀) · S(Sensitive · 민감) · O(Open · 공개)** 등급으로 분류하고, 등급별 보안수준에 따라 보안통제 항목을 선택·적용하도록 한 새 체계입니다. 보안 통제 항목 수는 기존 Draft 약 176개에서 정식판 약 260여 개로 확대되었습니다.[2] 그리고 2026년 4월 17일 코엑스 NetSec-KR 2026에서 국정원은 N2SF가 명문화된 **'국가 사이버보안 기본 지침'을 2026년 5월부터 본격 시행**한다고 공식 발표했습니다 — 기존 '국가 정보보안 기본 지침'에서 명칭을 변경하고, 획일적 망 분리 규제를 폐지하며 데이터 중요도 차등 보안으로 전환하는 3년 만의 대대적 정비입니다.[2a] 같은 개정에는 **정보화 예산 대비 보안 예산 15% 이상 · 정보화 인력 대비 보안 인력 10% 이상**이 권고에서 의무로 격상되었고, 원격 근무자·시스템 관리자 **다중 인증(MFA) 의무화**, AI 시스템·민간 클라우드 보안 대책 신설이 함께 포함되었습니다.[2a]

금융 영역에서는 2024년 8월 금융위원회가 **전자금융감독규정** 일부개정고시안을 통해 행위규칙을 **293개 → 166개** 로 정비하고, "규칙(Rule) 중심 → 원칙(Principle) 중심" 의 자율보안 체계로 방향을 전환했습니다.[3] 동시에 같은 달 발표된 **금융분야 망분리 개선 로드맵**은 SaaS 이용 확대·생성형 AI 활용·연구개발망 분리 완화를 공식화했습니다.[4] 2026년 금융보안원의 IT·보안 평가는 **15개 분야 869항목**(전년 14개 분야 789항목 대비 9.2% 증가)으로 확대되며, 그 가운데 **73항목**은 클라우드 환경 평가 기준으로 신설되었습니다.[5]

1.2 위협 축 — "코드 없는 침투" 가 표준이 된 한국

한국을 표적으로 한 APT 캠페인은 분기 단위로 신기법을 갈아치우고 있습니다. 2025년 1분기 ASEC 보고는 **LNK > CHM > HWP/HWPX** 순으로 진입점을 정리했고,[6] 2025년 12월 Genians 가 공개한 **Operation Artemis** 는 HWP 내부 OLE 객체로 합법 Microsoft 유틸리티를 실행시킨 뒤 DLL 사이드로딩으로 RokRAT 을 떨어뜨렸습니다.[7] 2026년 2월에는 **CVE-2025-29867** — Hancom Office 2018·2020·2022·2024 전 라인에 영향을 미치는 Type Confusion(CWE-843, CVSS 8.5 HIGH) — 이 NVD 에 정식 공개되었습니다.[8] 한컴 오피스가 한국 공공·국방·학계의 사실상 표준이라는 점에서, 38 North 는 같은 시기 HWP 를 "한미동맹 차원의 사이버 자세에 영향을 미치는 공격 표면" 으로 격상시켰습니다.[9]

1.3 기술 축 — AI 와 클라우드가 가져온 새 표면

2022년 2월 Microsoft 가 인터넷 다운로드 매크로를 기본 차단하자 VBA 매크로 캠페인은 약 66% 감소했으나, 같은 기간 ISO·LNK·RAR 컨테이너 첨부는 약 175% 증가했습니다.[10] 본질은 변하지 않았습니다 — 사용자가 문서를 연다는 행위 자체가 위험입니다. 그 위에 AI 시대의 신표면이 더해졌습니다. **EchoLeak(CVE-2025-32711)** 는 사용자가 메일을 열기도 전에 Microsoft 365 Copilot 의 RAG 가 본문을 가져가는 순간 프롬프트 인젝션이 발동되는 제로클릭 취약점이었고,[11] Hugging Face 에 업로드된 pickle 기반 모델 100여 개에서 백도어가 발견된 사건은 모델 자체가 페이로드가 되는 시대를 입증했습니다.[12]

[그림 1] 2024–2026 한국 보안 변곡점 타임라인. 망분리의 끝 → N2SF 의 시작. **2026년 5월 본격 시행**(국정원 NetSec-KR 2026, 2026.04.17). 출처: 국정원 보도자료·연합뉴스, 금융위·금융보안원 공시, ASEC·Genians·NVD.[1–8, 2a]

2장. 기존 방어가 무너지는 지점

> *안티바이러스는 시그니처를 보고, 샌드박스는 행위를 보고, EDR 은 엔드포인트를 봅니다. 셋 다 같은 가정을 공유합니다 — "악성을 식별할 수 있다." 이 가정이 무너지는 순간이 바로 지금입니다.*

2.1 시그니처·패치의 시간차

CVE-2017-11882(Equation Editor) 는 공개 8년이 지난 2024년에도 다수 캠페인의 핵심 컴포넌트입니다.[13] CVE-2023-36884 는 공개 3일 만에 NATO 회담 표적 캠페인에 무기화되었고,[14] CVE-2025-29867 은 한컴 오피스 4개 제품라인 전면에 영향을 미칩니다.[8] 시그니처와 패치는 항상 사후 대응입니다. 공격자가 0-day 한 건만 들고 와도, 탐지 모델은 그 시간 동안 침묵합니다.

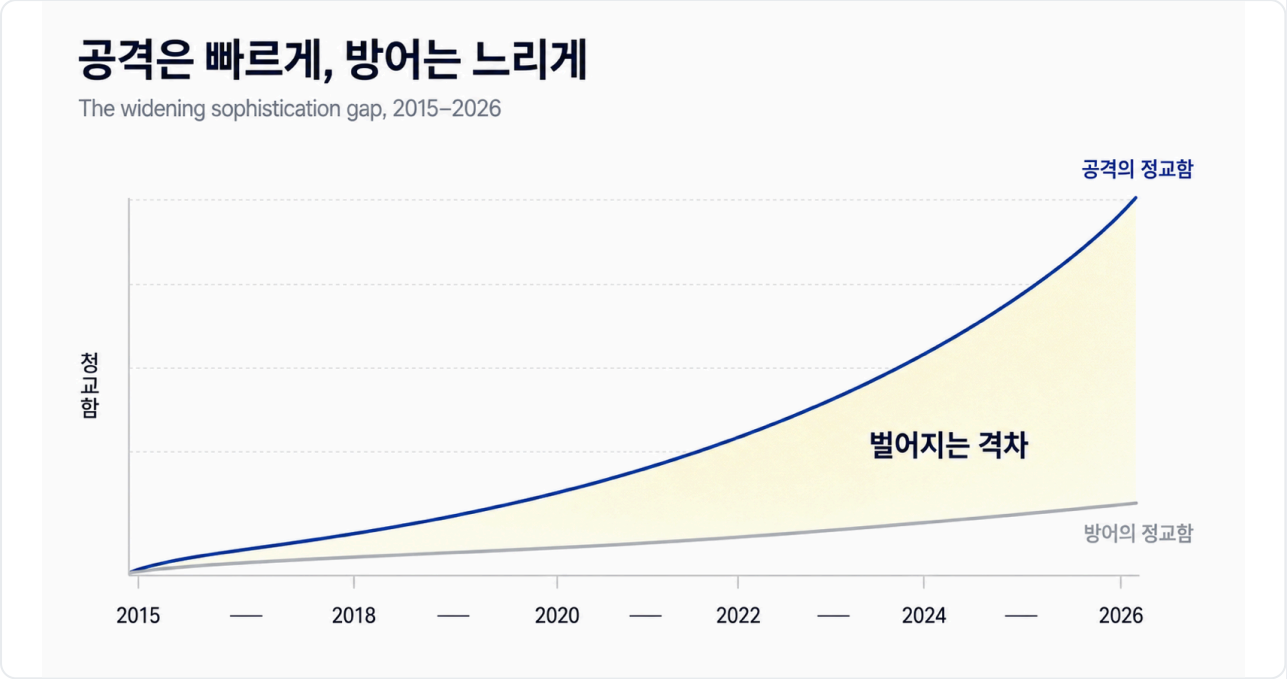
2.2 샌드박스 회피의 일상화

MITRE ATT&CK **T1497** 은 가상화·분석 환경 회피 기법을 3개 서브테크닉으로 표준화했습니다.[15] CPUID·MAC OUI·설치 프로그램 수 점검(T1497.001), 마우스 움직임·최근 문서·브라우저 히스토리 검사(T1497.002), GetTickCount·RDTSC 기반 Sleep 가속 탐지(T1497.003) 가 표준 키트가 되었습니다. **SUNBURST** 는 12–14일 잠복 후에야 페이로드를 실행했고,[16] Emotet 은 `CreateTimerQueueTimer` 로 분석 환경을 우회했으며,[17] APT37 의 RokRAT 은 디스크에 기록을 남기지 않는 인메모리 셸코드와 Dropbox·pCloud·Yandex Cloud C2 로 합법 트래픽에 위장합니다.[18]

CrowdStrike 2025 Global Threat Report 는 **2024년 사이버공격 탐지의 79% 가 malware-free** 였다고 보고합니다 (2019년 40% → 2024년 79%). 평균 eCrime breakout time 은 48분, 최단 51초였습니다.[19]

2.3 매크로 차단의 역설

2022년 2월 Microsoft 가 인터넷 매크로 기본 차단을 발표한 이후, Proofpoint 는 VBA·XL4 매크로 캠페인이 약 66% 감소한 반면 ISO·RAR·LNK 컨테이너 첨부가 약 175% 증가했다고 측정했습니다.[10] 한국에서는 이 효과가 더 제한적입니다. HWP 는 애초 VBA 를 쓰지 않고, OLE·임베디드 객체·CVE 기반 논리 결함으로 동등하거나 더 큰 표면을 가집니다.



[그림 2] 공격의 정교함 vs 방어의 정교함 — 벌어지는 시간차. 개념도. 데이터 포인트는 본문 1.2 · 2.1–2.3 출처 참조.

악성을 정의할 수 없는 시대에, 탐지는 영원히 한 발 늦습니다.

2.4 정리 — 같은 가정, 같은 한계

AV(시그니처)·샌드박스(행위)·EDR(엔드포인트). 세 기술은 도구가 다르지만 같은 가정을 공유합니다 — **"악성을 식별할 수 있다."** 0-day 와 malware-free 공격이 표준이 된 현실에서 이 가정은 더 이상 성립하지 않습니다. 따라서 다음 질문은 이것입니다 — **"식별하지 않고도 안전을 보장하는 방법은 없는가?"** 그 답이 3장의 CDR 입니다.

3장. CDR — 위협을 찾지 않고, 콘텐츠를 다시 만든다

> *CDR 은 위협을 찾지 않습니다. 콘텐츠를 분해하고, 위험 가능성이 있는 모든 액티브 요소를 제거한 뒤, 안전한 형태로 재조립합니다. 판정이 사라지면, 미탐도 사라집니다.*

3.1 정의

CDR(Content Disarm & Reconstruction · 콘텐츠 무해화 및 재조립) 은 입력된 파일을 신뢰하지 않는 것을 전제로, 컨테이너·스트림·객체 단위로 분해한 뒤 액티브 컨텐츠(매크로 · 스크립트 · OLE · ActiveX · DDE · 하이퍼링크 등) 를 제거하고 동일한 포맷으로 재생성하는 기술입니다. 핵심 명제는 단순합니다 — **위험한 파일을 찾으려 하지 마세요. 안전한 형태만 받으세요.**

CDR의 다섯 가지 원칙 — Positive Security Model

1. **모든 파일을 신뢰 불가로 가정한다 (Zero Trust File).** 화이트리스트 매크로조차 정책으로 명시되지 않으면 통과시키지 않습니다.
2. **탐지가 아니라 무해화한다 (Signature-less).** 시그니처·행위 패턴에 의존하지 않으므로, 0-day · AI 생성 변종 · 다형성 멀웨어에도 동일하게 작동합니다.
3. **포맷 구조 기반으로 작동한다 (Format-agnostic).** 새로운 파일 포맷·변형 구조에도 같은 분해·재조립 원리가 적용됩니다.
4. **메모리에서 처리하고 잔류하지 않는다 (In-memory · Non-retentive).** 원본 콘텐츠는 메모리에서만 다뤄지고, 무해화 처리 후 보존되지 않습니다.
5. **정책 기반 실시간으로 동작한다 (Real-time policy-driven).** 이메일·웹 업로드·망간 자료전송·SaaS 동기화 등 인라인 지점에서 지연 없이 처리합니다. 암호화·서명 파일은 사전 정의된 정책에 따라 분기됩니다.

3.2 방어 방식 비교

방어 방식	동작 원리	0-day 대응	가독성	N2SF 정합성
안티바이러스(AV)	시그니처 매칭	제한적	—	차단 위주
샌드박스	실행 후 행위 분석	회피 가능	—	지연·우회
EDR	엔드포인트 행위 탐지	사후 대응	—	탐지 의존
CDR	**분해·제거·재조립**	**원천 무력화**	**원본 레이아웃 유지**	**변환 기반 — 적합**

[표 1] 방어 방식 비교. CDR 행은 "판정하지 않는다" 는 구조적 차이에서 비롯되는 결과 정리입니다.

CDR 은 판정하지 않습니다. 분해하고, 다시 만듭니다.

3장 (계속) · CDR 은 실제로 어떻게 동작하는가

"분해 후 재조립" 은 슬로건이 아닙니다. 컨테이너를 식별하고, 액티브 콘텐츠를 카탈로그로 매칭하며, 시각 요소만 안전하게 재조립하는 5단계 엔지니어링 절차입니다.

3.3 5단계 파이프라인

CDR 의 내부 파이프라인은 다음 다섯 단계로 구성됩니다. 모든 단계는 **정적 분석** 이며, 어떤 단계에서도 파일은 실행되지 않습니다.

- **(1) Parse** — 확장자가 아닌 **magic number · 파일 시그니처** 로 컨테이너를 식별하고, 내부 구조(스트림 · 파트 · 오브젝트) 를 트리로 구축합니다. 위장 확장자(.docx 로 표시된 OLE2) 는 이 단계에서 탈락합니다.
- **(2) Identify** — 구축된 트리를 순회하며 **액티브 콘텐츠 카탈로그** 와 매칭합니다. 매크로 · 스크립트 · 외부 링크 · 임베디드 객체 · 메타데이터 · 자동 실행 트리거가 식별 대상입니다.
- **(3) Disarm/Sanitize** — 정책에 따라 제거(strip) 또는 무력화(neutralize). 화이트리스트 매크로 · 서명된 콘텐츠는 예외 통과가 가능합니다.
- **(4) Reconstruct** — 시각 요소(텍스트 · 표 · 이미지 · 서식) 와 편집성을 보존하면서 동일 포맷으로 재조립합니다.
- **(5) Validate** — 새 파일이 포맷 규격(예: ISO/IEC 29500, ISO 32000) 에 부합하는지 재검사. 불일치 시 재조립 단계로 회귀하거나 격리 처리합니다.

[그림 3] 한 파일의 0→안전 여정 — 5단계 파이프라인. 모든 단계는 파일을 실행하지 않는 정적 분석으로 구성됩니다.[37]

3.4 포맷별 분해 — 실제로 무엇이 사라지는가

포맷 family	제거 대상 (액티브 콘텐츠)	보존 대상 (시각·텍스트)
OOXML (docx · xlsx · pptx)	vbaProject.bin · external links · customXml · embedded OLE · macroSheets	본문 텍스트 · 표 · 이미지 · 차트 · 서식
HWP 5.0 / HWPX	BinData 실행 스트림 · BodyText OLE · 매크로 · HWPX JSE	본문 · 표 · 도형 · 이미지
PDF	/JavaScript · /OpenAction · /Launch · /EmbeddedFile · /RichMedia	페이지 · 텍스트 · 이미지 · 서명 정보
이미지 (JPEG · PNG · SVG)	EXIF 메타 · SVG `<script>` · 스테가노그라피 의심 페이로드	픽셀 · 색 · 치수
Archive (zip · 7z · rar · ISO)	재귀 중첩 검사 · LNK · 스크립트 파일 · MOTW 우회 시도	안전 처리된 내부 파일
메일 (EML · MSG)	첨부 재귀 처리 · HTML `<script>` · 자동 다운로드 링크	본문 · 발신자 · 서명

[표 2] 포맷별 제거·보존 카탈로그. 시큐레터 MARS 는 309종 파일 포맷을 단일 엔진으로 처리합니다.[20]

> **핵심 명제 — 판정하지 않으니 오탐도 없다.** CDR 의 비교 우위는 "더 잘 맞히는 판정기" 가 아니라, "판정 자체를 제거한 변환기" 라는 구조에서 나옵니다.

4장. N2SF · 금융 규제와 CDR 의 정합성

> *N2SF 는 데이터를 등급으로 나누고 등급별로 다른 신뢰 모델을 적용하라고 요구합니다. "차단" 만 가능한 솔루션은 등급 간 흐름을 막아 업무를 정지시킵니다. "변환" 이 가능한 솔루션만이 분류 체계와 함께 살아남습니다.*

4.1 N2SF 통제군과 CDR 의 구조적 정합

N2SF 가이드라인 1.0(정식판)은 권한·인증·통제·데이터·정보자산 등 여러 영역에 걸쳐 약 260여 개 통제항목으로 구성됩니다.[2] 그 중에서도 망 분리 폐지와 함께 새로 명문화된 핵심은 게이트웨이 영역의 네 가지 통제 — **CD-4 외부 유입 통제 · CD-5 비정형 데이터 관리 · CD-6 정보 이동 통제 · CD-7 메타데이터 통제** 입니다. 이 네 가지는 모두 NSA NCDSMO 의 Cross Domain Solution(CDS) 가드 원칙 — 항상 호출되어야 하고, 우회 불가능해야 하며, 독립적이고 검증 가능해야 한다 — 과 같은 자리에 서 있습니다.[21]

2026년 5월 시행과 함께 적용되는 신규 의무사항은 CDR 도입 결정에 직접 영향을 미칩니다. 정보화 예산 대비 보안 예산 **15% 이상**, 정보화 인력 대비 보안 인력 **10% 이상**이 "노력해야 한다" 권고에서 "운영하여야 한다" 의무로 격상되었고, 원격근무자·시스템 관리자에 대한 **다중 인증(MFA) 의무화**, AI 시스템 구축·민간 클라우드 도입 시 보안 대책 신설이 함께 명문화되었습니다.[2a]

4.2 CDR ↔ N2SF 정합성

N2SF 요구 개념	CDS 통제항목	CDR 역할
외부 유입 통제	**N2SF-CD-4**	무해화 후 반입
비정형 데이터 관리	**N2SF-CD-5**	문서·이미지 직접 처리
정보 이동 통제	**N2SF-CD-6**	이동 전 구조 재작성 — CDR 의무화
메타데이터 통제	**N2SF-CD-7**	메타데이터 정책 적용·제거 후 전송

[표 3] N2SF 요구 개념 ↔ CDS 통제항목 ↔ CDR 역할 매핑. 출처: 시큐레터 Solution Brief p.9, 국가정보원 「국가 망 보안체계(N2F) 보안 가이드라인 1.0」(2025.9).[1,2,27]

→ N2SF-CD-6 — "콘텐츠 무해화(CDR) 적용"이 의무 보안통제로 명문화되었습니다.

국가정보원 「국가 망 보안체계(N2F) 보안 가이드라인 1.0」은 N2SF-CD-6 항목에서 **"콘텐츠 무해화(CDR) 적용"**을 게이트웨이 통제로 직접 명시하고, "전송 전 파일 내 삽입된 숨겨진 객체, 매크로, 스크립트 등을 제거하고 안전한 형식으로 콘텐츠를 정제" 하도록 규정합니다.[1,27] 즉 **CDR 은 가이드라인이 권장하는 옵션이 아니라 N2SF 의 정보 이동 통제를 충족하기 위해 직접 호명된 의무 보안통제**입니다. 2026년 5월 '국가 사이버보안 기본 지침' 본격 시행과 함께 적용 의무가 발생합니다.[2a]

→ CDR의 본질은 탐지가 아닌 "무해화" 입니다. 판정을 하지 않으므로 미탐도 없으며, N2SF 가 요구하는 "위험하지 않은 형태만 허용" 원칙을 기술적으로 충족합니다.

4.3 금융 규제와의 정합

2024년 8월 개정 전자금융감독규정은 "원칙 중심 자율보안" 으로 방향을 전환했고, 금융분야 망분리 개선 로드맵은 SaaS·생성형 AI·외부 협업 채널을 합법화했습니다.[3,4] 자율보안 체제는 사고 발생 시 입증 책임이 금융회사에 귀속됩니다. **"우리는 탐지에 의존했다" 는 진술은 더 이상 면책 사유가 되지 않습니다.** CDR 은 사고 발생 가능성 자체를 콘텐츠 변환 단계에서 제거하므로, 자율보안의 입증 부담을 구조적으로 낮춥니다.

차단은 업무를 멈추고, 변환은 업무를 잇습니다.

4장 (계속) · 해외 규제 비교

4.4 해외 규제와 CDR 의 위치

주요국의 정보보안 규제 체계는 등급 분류와 게이트웨이 통제 원칙을 공유합니다. CDR 은 각 체계의 "경계 변환 통제" 위치에서 동일한 역할을 수행합니다.

국가/체계	핵심 구조	CDR 의 위치
US · FedRAMP High	NIST SP 800-53 Rev.5 기반, High 370개 통제[22]	SC-7(21)·SC-7(22) 경계 보호에 CDS·CDR 권장
UK · GSC	OFFICIAL / SECRET / TOP SECRET 3등급 (2014, 2024.8 갱신)[23]	OFFICIAL-SENSITIVE 캐비닛에서 첨부 무해화 권고
EU · EBA Outsourcing	EBA/GL/2019/02, 2019.9 시행[24]	제3자·SaaS 협업 시 콘텐츠 무해화 요건과 정합
SG · MAS TRM	2021.1 개정, 클라우드·제3자 위험·사고대응 포함[25]	비실행형 파일 흐름 통제 요건과 정합
US · EO 14028 / SBOM	2021.5 행정명령, NIST SBOM 최소 요소[26]	모델·코드·문서 공급망 전체에 변환 통제 적용

[표 4] 주요국 규제 체계와 CDR 의 위치. 한국의 N2SF 가 CDR 을 의무 보안통제(CD-6) 로 명문화한 것은 동급 체계 중 가장 명시적인 사례에 해당합니다.

한국 N2SF 가 특별한 이유

FedRAMP·EBA·MAS 등 주요국 체계는 모두 "콘텐츠 변환 통제"를 권장하지만, **특정 기술 명칭(CDR)을 직접 호명하여 의무로 명시한 사례는 N2SF-CD-6 이 최초**입니다. 이는 한국 공공·금융 시장에서 CDR 이 단순 "권장 옵션" 이 아니라 "법적 통제 항목" 으로 작동함을 의미합니다.

2026년 5월 본격 시행 이후 RFP·BMT·감사 단계에서 CDR 도입 여부가 직접 평가 항목이 됩니다.[2a]

5장. 어디에 어떻게 적용하는가 — 6대 시나리오

> *CDR 은 한 위치에서만 일하지 않습니다. 메일 게이트웨이, 망간 자료전송, 웹 업로드, SaaS 협업, API 임베디드, 위협 인텔리전스 — 콘텐츠가 흘러 들어오는 모든 인입 채널에 배치됩니다. 시큐레터 4종 제품이 N2SF CD-4~7 통제 위에 놓이는 6가지 표준 형태를 정리합니다.*

5.1 시나리오 1 — 이메일 게이트웨이 (SEG 후단)

외부 메일 흐름 → SEG → **CDR(SLE)** → 메일박스 → 사용자. SEG 가 1차 필터(스팸 · DMARC · URL 평판) 를 수행한 뒤 SLE 가 첨부 무해화와 본문 URL 검사를 수행합니다. N2SF **CD-5 외부 통신 · 외부 유입** 통제와 정합합니다. 적합 제품: SLE

5.2 시나리오 2 — 망간 자료전송 (CDS 게이트와 결합)

저등급망 → 자료전송 게이트 → **CDR(SLF)** → 고등급망. N2SF 의 C · S · O 등급 간 흐름에서 CDS 통제와 결합되어 동작하며, 망연계 게이트의 파일 흐름을 비실행형 분해·재조립으로 처리합니다. N2SF **CD-4 외부 유입 통제** 의 표준 배치입니다. 적합 제품: SLF

5.3 시나리오 3 — 웹 업로드 · 포털 입수

사용자 업로드 → **CDR(SLCDR)** → 내부 저장소. 민원 포털 · 고객 응대 시스템 · 증권사 신청서 등 외부 사용자가 직접 업로드하는 비정형 문서에 적용합니다. N2SF **CD-5 비정형 데이터 관리** 및 **CD-6 정보 이동 통제** 와 정합합니다. 적합 제품: SLCDR

5.4 시나리오 4 — 클라우드 SaaS 협업 (M365 · Workspace · Box)

외부 협업 파일 동기화 → SaaS 커넥터 → **CDR(SLE / SLCDR)** → 내부 사용자. 2026년 금융보안원 평가에 신설된 클라우드 관련 73항목과 정합하며, 망분리 개선 로드맵 이후 합법화된 SaaS · 외부 협업 채널의 콘텐츠 무해화를 담당합니다.[5] 적합 제품: SLE SLCDR

5.5 시나리오 5 — API · SDK 임베디드 (DMS · ECM 통합)

내부 애플리케이션이 파일 처리 시점에 CDR API 를 호출하고 변환 결과를 동기·비동기로 수신합니다. 보험사 청구 시스템 · 법무 ECM · CRM 첨부 처리 등 업무 시스템 단위로 깊이 통합되는 패턴입니다. N2SF **CD-6 정보 이동 통제** 의 시스템 내장 형태입니다. 적합 제품: SLCDR

5.6 시나리오 6 — ConTI 위협 인텔리전스 피드백 루프

CDR 이 제거한 액티브 콘텐츠 메타데이터(난독화 매크로 패턴 · 외부 호출 URL · 임베디드 OLE 시그니처) 를 **ConTI** 가 IoC 로 축적하고, SOC · CISO 보고에 가시화합니다. N2SF **CD-7 메타데이터 통제** 와 정합하며, KISA C-TAS 연계 운영도 이 경로에 포함됩니다. 적합 제품: ConTI

[그림 4] CDR 통제 위치 통합도 — 6대 시나리오 한 장. ConTI 는 다른 다섯 경로의 CDR 처리 결과를 피드백으로 수집하는 메타 위치입니다.

5.7 적용 매트릭스

시나리오	적합 제품	주요 통제항목 (N2SF)	핵심 가치
① 이메일 게이트웨이	SLE	CD-5 외부 통신	첨부 무해화 + 본문 URL · BEC 대응
② 망간 자료전송	SLF	CD-4 외부 유입 통제	등급 간 흐름의 비실행형 변환 통제
③ 웹 업로드 · 포털	SLCDR	CD-5 · CD-6 정보 이동	외부 사용자 업로드 즉시 CDR
④ 클라우드 SaaS 협업	SLE SLCDR	CD-5 · 금융 클라우드 평가	SaaS 협업 채널의 콘텐츠 무해화[5]
⑤ API · SDK 임베디드	SLCDR	CD-6 정보 이동 통제	업무 시스템 내장형 변환 통제
⑥ ConTI 피드백 루프	ConTI	CD-7 메타데이터 통제	CDR 결과의 IoC 화 · SOC/CISO 가시화

[표 5] 시나리오 × 제품 × 통제 매트릭스. 실제 도입 시 ① ~ ⑤ 중 복수를 혼합 운영하고, ⑥ 은 그 위에 항상 얹는 패턴이 일반적입니다.

6장. 도입 평가 — 5개 변수로 본 CDR 시장

> *"어디에 쓰는지" 를 5장에서 확인했다면, 다음 질문은 "어떤 CDR 인가" 입니다. 답을 가르는 변수는 다섯 개 — 포맷 커버리지, 가독성 보존, 처리 속도, 운영 통합성, 인증·레퍼런스. 전제 하나 — **'CDR 자체' 에 대한 별도 인증은 존재하지 않습니다.** KISA·TTA 인증은 SLF·SLE·SLCDR 같은 **제품 단위** 로 발급됩니다.*

6.1 RFP 체크리스트

평가 항목	최소 요구	가중치	우리의 입장
포맷 커버리지	MS Office · PDF · HWP/HWPX · 이미지 · 압축 다단계	높음	309종 포맷, 국내 표준 1위
가독성 보존	레이아웃·코멘트·하이퍼링크 스키마 유지	높음	코멘트 유지, 하이퍼링크 스키마 보존
처리 속도	인라인 게이트웨이 흐름에서 사용자 체감 지연 없음	높음	SLCDR 평균 34ms 무해화
인증 (제품 단위)	KISA / TTA / Gartner 등재 — 제품별 시험 결과	높음	SLF KISA · MARS V2 TTA GS 1등급 · Gartner 등재
레퍼런스	공공·금융 운영 실적 · 동일 등급망 사례	중간	100+ 한국 주요 기관 운영

[표 6] RFP 작성 시 가중치 칸은 기관 자체 정책에 맞춰 재설정하십시오.

6.2 배포 옵션 × 요구사항 적합도

배포 형태	적합 환경	운영 부담	비고
어플라이언스	망분리·내부망·금융·국방·정부	중간	SLF 표준 배치. SMB/NFS/SFTP 연동.
가상 어플라이언스	프라이빗 클라우드·VDI	낮음~중간	SLE/SLCDR 통합 운영 시 가용성 확보 권장.
게이트웨이 통합 (이메일)	대규모 메일 흐름 · BEC 위험	중간	SLE — 메일서버 앞단, MX 라우팅 단순.
API · SaaS 연동	웹 업로드 · M365 · 외부 협업	낮음	SLCDR API + SLE M365 Graph 연계.

6.3 비용·운영 관점

CDR 의 TCO 는 (1) 라이선스, (2) 어플라이언스/호스팅, (3) 운영 인력, (4) 사고 대응 비용 절감의 4축으로 평가됩니다. IBM Cost of a Data Breach 2024 에 따르면 글로벌 평균 침해 비용은 USD 4.88M 로 전년 대비 10% 상승했으며,[27] Sophos State of Ransomware 2024 는 평균 복구 비용(몸값 제외)이 USD 2.73M 로 전년 대비 50% 상승했다고 보고합니다.[28] CDR 은 사고 확률을 가장 큰 인입 채널(메일·웹·망연계)에서 차단함으로써 4축 중 (4) 의 기대값을 가장 효과적으로 낮춥니다.

사용자가 첨부파일을 클릭하기 전, 우리는 이미 그 파일을 다시 만들었습니다.

7장. 시큐레터의 답 — MARS 와 4종 제품

> *우리의 답은 한 줄로 줄어듭니다 — **MARS 엔진 위에 4종 제품(SLF · SLE · SLCDR · ConTI) 으로 N2SF CD-4~7 통제를 단일 아키텍처로 닫는다.** 그 중 CD-6 은 가이드라인이 "콘텐츠 무해화(CDR) 적용" 을 명문화한 의무 보안통제입니다.*

7.1 MARS — 리버스 엔지니어링 기반 비실행형 파일 분석

MARS(Malware Analysis & Response System) 는 파일을 실행하지 않고 바이너리·어셈블리 레벨에서 분해·검사하는 시큐레터의 단일 엔진입니다.[20] 정적 분석·동적 분석·리버스 엔지니어링을 하나의 파이프라인으로 결합해, 헤더·메타데이터·본문·함수 호출·API 시퀀스를 4단계로 검사합니다. 전통적인 리버스 엔지니어링이 IDA Pro · Ghidra 같은 수동 디스어셈블러에 의존했다면, MARS 는 이 분석을 자동화·파이프라인화함으로써 평균 진단 시간을 분 단위에서 초·밀리초 단위로 단축했습니다.

7.2 4종 제품

SLF · SecuLetter File

파일 보안 / 망분리·망연계 환경

외부↔내부 파일 흐름 정밀 분석. PE + Non-PE(MS Office·PDF·이미지·영상) 동시 탐지, 압축·다중 압축 검사. 3rd-Party 망연계 솔루션 연동.

SLE · SecuLetter Email (DISARM 통합)

이메일 보안 · 사용자 도달 전 차단

리버스 엔지니어링 기반 정적 코드 분석. 본문 악성 URL 탐지, 첨부 매크로·JS 위협, 위장 파일 형식 감지. M365 Graph API Zero-Trust 첨부 무해화.

SLCDR · SecuLetter CDR

웹 콘텐츠 CDR · 어플라이언스/클라우드

309종 파일 포맷, CFB+OOXML 모두 지원, 평균 34ms 무해화, 코멘트 유지, 하이퍼링크 스키마 보존, AI 매크로 해석, QR 코드 무해화.

ConTI · Content Threat Intelligence

위협 인텔리전스 · 상관 분석

SLF/SLE/SLCDR 탐지 결과를 글로벌 위협 트렌드와 상관 분석. KISA C-TAS · VirusTotal · OSINT 연계. IoC 자동 추출 + 공격 체인 식별.

[그림 5] 4종 제품 × N2SF CD-4 ~ CD-7 매핑. 단일 엔진 MARS · 4종 제품 · 전 등급 커버.

7.3 증명된 숫자

※ 아래 인증은 모두 **해당 제품 단위**로 발급된 것입니다 — CDR 기능 자체에 대한 별도 인증은 존재하지 않으며, CDR 기능이 포함된 파일·이메일 보안 제품 단위로 인증·시험이 이루어집니다.

업계 최고 수준 탐지율

KISA 인증 — SLF450 (2019)[29]

난독화·임베디드 악성코드, 샌드박스 우회 기법 포함 실 악성코드 데이터셋에 대해 KISA·KSEL 공동 시험 기준 업계 최고 수준의 파일 탐지 성능을 인증.

업계 선도 응답

TTA GS 1등급, MARS V2[30]

20만 건 실제 파일(Office · PDF · HWP · 압축 포함) 대상 TTA 시험 인증에서 업계 선도 수준의 응답 시간을 인증받았습니다.

309종 포맷 / 34ms

SLCDR 기준[20]

국내 표준 포맷 1위, CFB + OOXML 동시 지원. 평균 34ms 무해화로 인라인 흐름에 사용자 체감 지연 없이 배치.

7.4 한국 특화 — HWP/HWPX · 망분리 · APT

시큐레터는 HWP(CFB 기반) 와 HWPX(OOXML 기반) 를 자체 파서로 분석합니다. 한컴 오피스 제로데이 사례에서 다수 보고된 OLE·DLL 사이드로딩·임베디드 객체 패턴은 MARS 의 정적 리버스 엔지니어링 단계에서 동일 원리로 무력화됩니다. 시큐레터는 북한 연계 김수키(Kimsuky) 그룹의 코인 관련 해킹 캠페인 분석 경험을 보유하고 있으며,[31] 한국 망분리·N2SF·금융 규제 환경에 네이티브로 대응합니다.

7.5 인증 · 등재

- KISA 보안기능 확인서 / 보안적합성 검증 — 국가·공공기관 도입 요건 충족.[29,34]
- TTA GS 1등급 — MARS V2 시험인증.[30]
- Gartner — 글로벌 이메일 보안 Vendor Identification 등재 (40개 글로벌 벤더 중 유일한 한국 기업).[35]

- 국내 CDR 관련 특허 다수 보유 (대표 KR10-2468434 외).[36]

4종 제품, 하나의 엔진 — MARS. N2SF-CD-6 "콘텐츠 무해화(CDR) 적용" 의무를 단일 아키텍처로 충족.

7.6 도입 사례 (요약)

전 국민 건강보험 운영 공공기관 · SLF

민원 포털을 통해 국민이 제출한 문서를 SLF 가 검사·차단. 기존 솔루션 대비 빠른 탐지 응답과 운영 안정성을 확보.[32]

국내 1군 종합 금융투자회사 · SLE + SLF

이메일과 내부망 메일 존을 분리 배치, 사용자 도달 전 위협을 단일 엔진으로 차단.

국내 대표 보험 인프라 기관 · SLCDR

웹 게시판으로 들어오는 사용자 업로드 문서를 자동 무해화, 업무 흐름은 그대로 유지.

방산 전문 기업 · SLE + SLF

기존 글로벌 APT 솔루션을 SecuLetter 로 교체, 망분리 환경의 첨부·내부 흐름 통합 보호.

100+ 한국 주요 기관 운영 · 연금·금융 자산 800조 원 이상 보호 환경에서 검증.[33]

8장. 다음 단계

> *백서는 결재 테이블 위 30분의 토론을 위한 자료입니다. 그 다음은 PoC 입니다. 자사 환경의 실제 파일 100건으로 14일간 검증하시고, 데이터로 결정하십시오.*

PoC 신청 — 자사 환경의 실제 파일 100건으로 14일간 검증

비용 0원 · NDA 후 진행 · 결과 리포트 제공. 망연계·이메일·웹 업로드 흐름 중 선택 가능.

PoC 신청하기 →

블로그 라이브러리 — 더 깊이 읽기

N2SF · CDR · MARS · 공공·금융 사례를 분석한 30편 라이브러리.

블로그 보기 →

부록 A · 용어

CDR Content Disarm & Reconstruction (콘텐츠 무해화 및 재조립) · **N2SF** National Network Security Framework (국가 망 보안체계) · **MARS** Malware Analysis & Response System · **CFB** Compound File Binary (MS Office 구형 포맷군) · **OOXML** Office Open XML (신형 포맷군) · **CDS** Cross Domain Solution · **RTB / RAIN** NSA Raise the Bar / Redundant·Always Invoked·Independent·Non-Bypassable · **BEC** Business Email Compromise · **IoC** Indicator of Compromise · **EAL** Evaluation Assurance Level (ISO/IEC 15408).

부록 C_1 · CDR 일반 FAQ — CISO 결재 단계에서 자주 묻는 10가지

1. **Q1. CDR이 안티바이러스·샌드박스를 대체하나요?**
   아닙니다. CDR은 **defense-in-depth(다층 방어)의 보완 계층**입니다. AV는 알려진 위협, 샌드박스는 행위 인사이트, CDR은 미지의 0-day까지 포함한 모든 진입 파일을 사전 무해화합니다. 세 가지를 함께 두는 것이 표준 권장 구성입니다.

2. **Q2. 무해화하면 문서가 깨지지 않나요?**
   CDR은 매크로·임베디드 스크립트 등 액티브 요소만 제거하고 텍스트·표·이미지·서식·서명 정보 등 **본문 구조와 가독성은 보존**합니다. 업무 매크로 의존 부서는 화이트리스트 정책으로 예외 처리 가능합니다.

3. **Q3. 암호화·비밀번호로 보호된 파일은 어떻게 처리되나요?**
   복호화되지 않은 파일은 무해화가 불가능하므로 **정책 기반 분기 처리**합니다 — 격리, 수동 검토 대기열로 회송, 또는 정의된 신뢰 경로만 통과 등 사전 정의된 룰로 운영합니다.

4. **Q4. 시그니처를 자주 업데이트해야 하나요?**
   아닙니다. CDR은 **signature-less** 아키텍처라 시그니처 갱신 없이도 동작합니다. 새 파일 포맷·신종 기법이 등장해도 동일한 분해·재조립 원리가 적용되므로 운영 부담이 최소화됩니다.

5. **Q5. AI가 만든 악성코드도 막을 수 있나요?**
   네. CDR은 콘텐츠의 "악성/정상"을 판정하지 않고 **파일 구조 자체**를 기반으로 작동합니다. AI 생성·다형성·인위적 변형 멀웨어도 그 안의 액티브 요소만 보면 동일하게 제거됩니다.

6. **Q6. 대량 트래픽에서 지연이 생기지 않나요?**
   현대 CDR은 **실시간 처리**를 전제로 설계되어 이메일·웹 업로드·망간 자료전송 인라인 구간에서 사용자 인지 지연을 만들지 않습니다. 큐 기반 비

동기·수평 확장 패턴이 일반적입니다.

7. **Q7. 민감 정보가 외부에 잔류하지 않나요?**
   CDR은 **메모리에서 처리하고 잔류하지 않는(in-memory · non-retentive)** 방식으로 설계됩니다. 처리 후 원본·중간 산출물은 보존되지 않으며, 메타데이터 영역도 정책으로 제거 가능합니다.
8. **Q8. 도입 모델은 어떤 옵션이 있나요?**
   온프레미스 · SaaS · 하이브리드 세 모델 모두 일반적입니다. 데이터 주권·국가망 분리 요건이 있는 공공·금융은 온프레미스 또는 폐쇄망 어플라이언스, 글로벌 협업이 잦은 환경은 SaaS, 둘을 결합하는 하이브리드도 빠르게 확산되고 있습니다.
9. **Q9. 어떤 규제·인증과 정렬되나요?**
   국내에서는 **N2SF · 전자금융감독규정 · 금융 IT·보안 평가 · ISMS-P · CSAP**, 해외에서는 NIST SP 800-53, FedRAMP, HIPAA, PCI-DSS, GDPR 등의 데이터 보호 요건과 정합합니다.
10. **Q10. 어떤 파일 포맷·위협 벡터까지 다루나요?**
    일반적으로 Office · PDF · 이미지 · 아카이브 · 실행 파일·CAD·DICOM 등 산업 특화 포맷까지 지원합니다. 위협 벡터는 Office 매크로, PDF JavaScript 액션, 스테가노그라피, 파서 취약점 유발 임베디드 객체, 다형성·난독화 페이로드 전반입니다.

부록 C_2 · 자가 진단 10문항

1. **Q1.** 우리 기관은 N2SF C·S·O 등급 분류를 시작했는가?
2. **Q2.** 외부에서 들어오는 문서·이메일 첨부의 매크로·임베디드 객체를 인라인으로 변환·제거하는 통제가 있는가?
3. **Q3.** 망연계 파일 흐름에서 HWP/HWPX 를 자체 파서로 분석하는가, 아니면 PDF 변환으로 대체하는가?
4. **Q4.** 샌드박스가 사용자 활동·시간 기반 회피 기법(T1497.002·003)을 탐지하는지 최근 12개월 내 검증했는가?
5. **Q5.** 사고 발생 시 "탐지에 의존했다" 외에 자율보안 입증 자료가 있는가?
6. **Q6.** SaaS·M365·외부 협업 채널의 첨부에 대해 동일한 통제가 적용되는가?
7. **Q7.** 웹 민원·제안 접수 게시판의 업로드 문서가 사용자 다운로드 전에 무해화되는가?
8. **Q8.** 위협 인텔리전스가 자사 탐지 결과와 상관 분석되어 의사결정에 반영되는가?
9. **Q9.** PoC 시 자사 실제 트래픽·실제 파일로 14일 이상 검증할 수 있는 운영 자원이 확보되어 있는가?
10. **Q10.** 도입 비용을 라이선스 + 운영 + **사고 회피 기대값** 의 4축으로 평가하는 TCO 모델이 있는가?

부록 B · 참고 문헌

1. 국가정보원, 「N2SF 보안가이드라인」 정식판 공개 보도자료, 2025.09.09. https://www.nis.go.kr/CM/1_4/view.do?seq=373
2. NCSC, N2SF 가이드라인 1.0 (정식판) 공식 게시. https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do ; ZDNet Korea, "국정원 보안 통제 항목 176→260여개로", 2025.09.09.
3. **(2a)** 연합뉴스, "국정원, 망분리 폐지…N2SF 보안체계 5월 시행", 권하영 기자, 2026.04.17. https://www.yna.co.kr/view/AKR20260417079000017 — NetSec-KR 2026 발표 기준 '국가 사이버보안 기본 지침' 5월 본격 시행, C/S/O 명문화, 보안 예산 15%·인력 10% 의무화, MFA 의무화, AI·민간 클라우드 보안 대책 신설.
4. 금융위원회, 「전자금융감독규정」 일부개정고시안 보도자료, 2024. https://www.fsc.go.kr/no010101/83954
5. 금융위원회, 「금융분야 망분리 개선 로드맵」, 2024.08.13. https://www.fsc.go.kr/no010101/82885
6. 금융보안원, "2026년도 취약점 분석·평가 실시" 공식 공지. https://www.fsec.or.kr/bbs/detail?menuNo=69&bbsNo=11882
7. ASEC AhnLab, "February 2026 APT Attack Trends — South Korea". https://asec.ahnlab.com/en/92972/
8. Genians Security Center, "Operation Artemis — HWP DLL Side-loading", 2025.12. https://www.genians.co.kr/en/blog/threat_intelligence/dll
9. NVD, CVE-2025-29867 (Hancom Office Type Confusion, CVSS 4.0 8.5 HIGH). https://nvd.nist.gov/vuln/detail/CVE-2025-29867
10. 38 North, "HWP as an Attack Surface", 2025.10. https://www.38north.org/2025/10/hwp-as-an-attack-surface/
11. Proofpoint, "How Threat Actors Are Adapting Post-Macro World", 2022.07.28. https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world ; Microsoft 365 Blog, 2022.02.07.
12. HackTheBox, "CVE-2025-32711 EchoLeak". https://www.hackthebox.com/blog/cve-2025-32711-echoleak-copilot-vulnerability
13. JFrog Security Research, "Malicious Hugging Face ML Models with Silent Backdoor", 2024.02.

14. NVD, CVE-2017-11882. https://nvd.nist.gov/vuln/detail/CVE-2017-11882 ; ASEC, 관련 캠페인 보고. https://asec.ahnlab.com/en/87724/
15. Microsoft Security Blog, "Storm-0978 attacks reveal financial and espionage motives", 2023.07.11.
16. MITRE ATT&CK, T1497 Virtualization/Sandbox Evasion. https://attack.mitre.org/techniques/T1497/
17. Mandiant, "SUNBURST Additional Technical Details", 2020.12.
18. Trend Micro, "New EMOTET Hijacks Windows API, Evades Sandbox Analysis", 2017.11.
19. Zscaler ThreatLabz, "APT37 RokRAT Cloud-Based C2 Analysis".
20. CrowdStrike, "2025 Global Threat Report Findings". https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-global-threat-report-findings/
21. 시큐레터, SecuLetter at a Glance (Ensecure v2), 2025.12.17 ; DISARM Solution Introduction KO, 2025.06.13.
22. **(27)** 시큐레터, *SecuLetter Solution Brief — The Value, Beyond Security*, p.9 「CDR: N2SF 의 정보 이동 통제를 구현하는 기술」.
23. BAE Systems, "What is the NCDSMO?" ; Owl Cyber Defense, "Raise the Bar and One-Way Transfer".
24. NIST SP 800-53 Rev.5 ; FedRAMP Rev.5 Baselines Transition Guide.
25. UK Cabinet Office, Government Security Classifications Policy.
26. EBA, "Guidelines on Outsourcing Arrangements" (EBA/GL/2019/02).
27. MAS, Technology Risk Management Guidelines, 2021.01.18.
28. White House Executive Order 14028, "Improving the Nation's Cybersecurity", 2021.05.12.
29. IBM, "Cost of a Data Breach Report 2024". https://www.ibm.com/reports/data-breach
30. Sophos, "The State of Ransomware 2024". https://www.sophos.com/en-us/blog/the-state-of-ransomware-2024
31. 시큐레터, KISA 인증 (SLF450, 2019). EV2 2025.12 §인증.
32. 시큐레터, TTA GS 1등급 (MARS V2). EV2 2025.12 §인증. 한국정보통신기술협회 시험인증 현황.
33. 시큐레터 facts-official §위협 그룹 (Kimsuky 코인 관련 해킹 캠페인 분석 사례).
34. 시큐레터 내부 도입 사례 정리 (NHIS 민원 포털 운영 사례). REF/customers.md.
35. 시큐레터, 회사소개서 2025 외부용 §고객.
36. KISIA, "보안적합성 검증 안내". https://www.kisia.or.kr/industry_support/security_compatibility_check_info/
37. 시큐레터, Gartner Vendor Identification for Email Security 등재 (40 글로벌 벤더 중 유일한 한국 기업). EV2 2025.12 §Recognition.
38. 시큐레터 facts-official §특허 (대표 KR10-2468434, KR10-2494836, KR10-2494838).
39. CDR 5단계 파이프라인(Parse · Identify · Disarm · Reconstruct · Validate) 및 정적 분석 기반 처리 구조는 산업 표준 정의에 따른다. NIST SP 800-177 (Trustworthy Email) 첨부 처리 권고 및 NCSC-UK "Pattern: Safely Importing Data" 문서 참조. 시큐레터 MARS 엔진은 309종 포맷에 동일 5단계 절차를 적용한다 (EV2 2025.12 §기술).