SECU LETTER

Secure Digital Content in One Solution

MPIS2020
시큐레터 발표 자료

2020.07.28

시큐레터는 악성코드 보안 제품 제조 및 클라우드 기반 이메일 보안 서비스, 악성코드 분석 서비스를 제공합니다.

보안 제품 제조

- 고도화된 공격을 탐지하고 분석하는 전문 솔루션 제조
- 메일 구간 고도화된 공격을 탐지하여 사전 차단
- 망연계, 문서집중화, 게시판 등 파일이 유인되는 구간에 고도화된 공격 탐지

클라우드 이메일 보안 서비스

- 클라우드 메일 보안 서비스
- 메일 수신 전 시큐레터 클라우드 서비스가 고도화된 공격 및 악성코드 분석

악성코드 분석 서비스

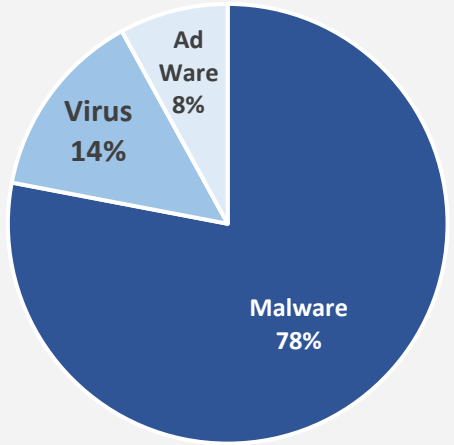
- 악성코드 분석 서비스
- 분석 보고서 제공
- 악성코드 분석 교육

악성코드 공격은 지속적으로 증가하고 있으며, 이 중 비실행형 파일(문서)를 통한 악성코드 공격이 급증하고 있습니다.

악성코드는 이메일의 첨부 파일을 통한 유입 비율이 가장 높으며, 일 평균 36만 건이 발생하고 있습니다.

<Source : 2018, Kaspersky>

일일 악성코드 위협 유형

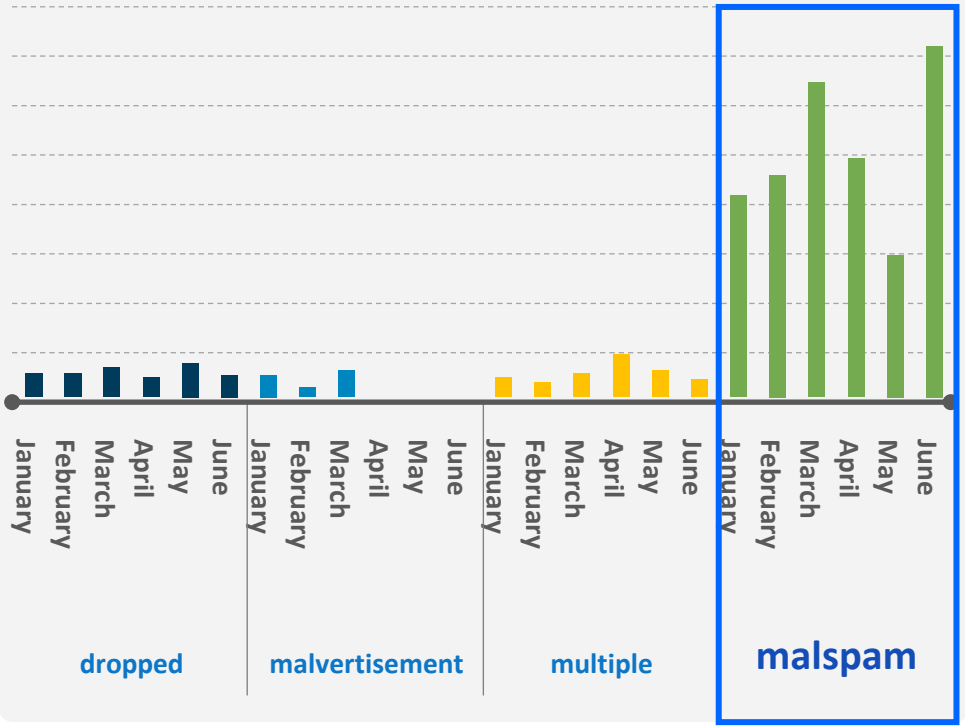


☑ 2017년 기준 일 평균 360,000건 악성코드 발생

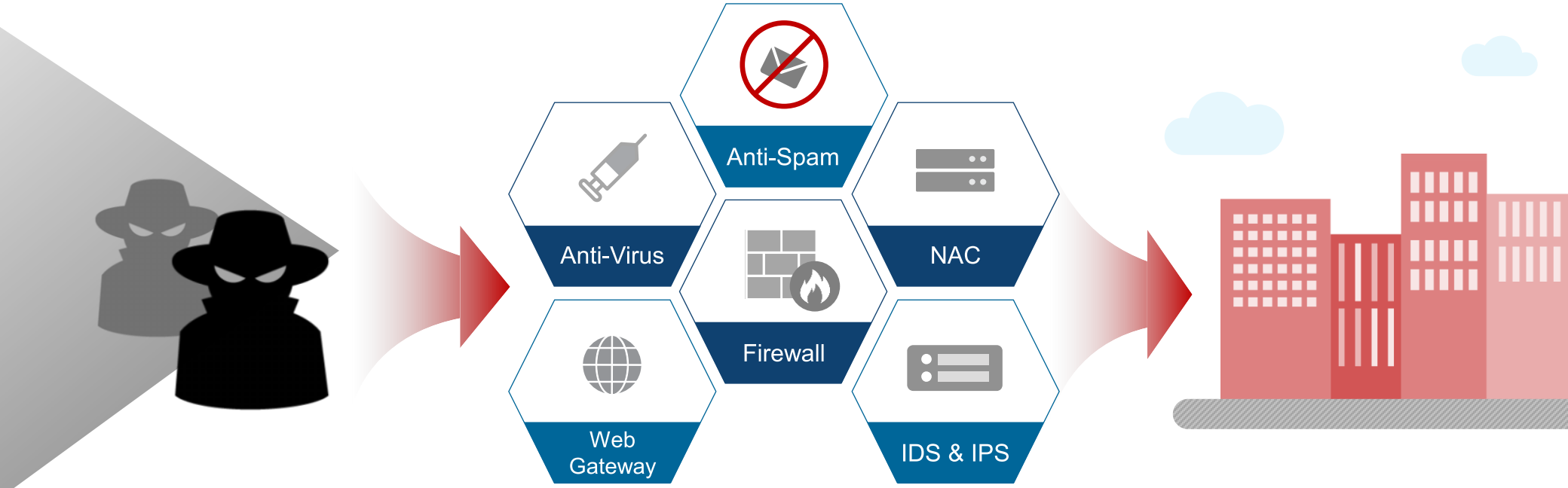
☑ **악성코드 발생, 전년대비 11.5% 증가**

<Source: 2018 Microsoft's alliance ISAAC Report >

Top 10 Malware – 초기 감염 경로



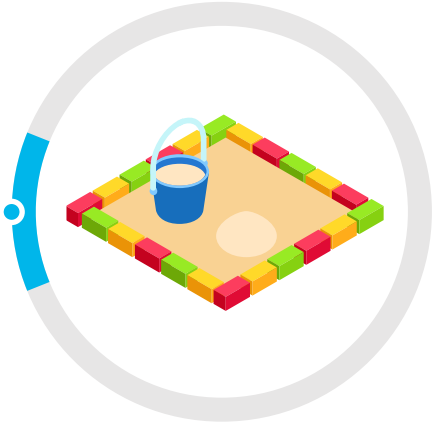
다수의 시그니처 기반 보안 솔루션을 갖추더라도
알려지지 않은 공격을 막을 수 없습니다.



시그니처 기반 **보안시스템**을 무력화하는 알려지지 않은 공격이 급증하고 있습니다

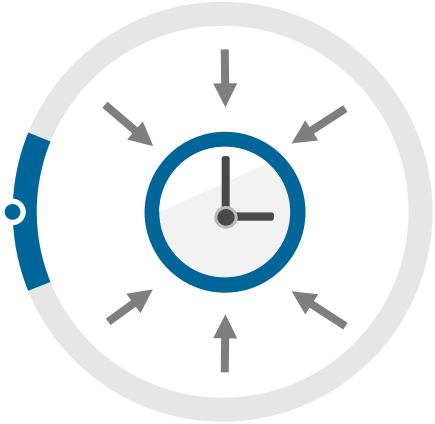
Why SecuLetter? | 샌드박스(행위 기반) APT 솔루션에 대한 대책 필요

샌드박스(행위 기반) APT 솔루션은 **행위가 일어나지 않을 시 탐지 불가**하고,
여러 형태의 환경에서 행위를 분석하기 때문에 **많은 진단 시간이 소요**되며
가상환경 회피, 시간차 공격, 사용자 행위 조건 공격에 대한 대처가 안됩니다.



가상환경 회피

열람 시
가상환경임을 확인하고
행위를 하지 않습니다



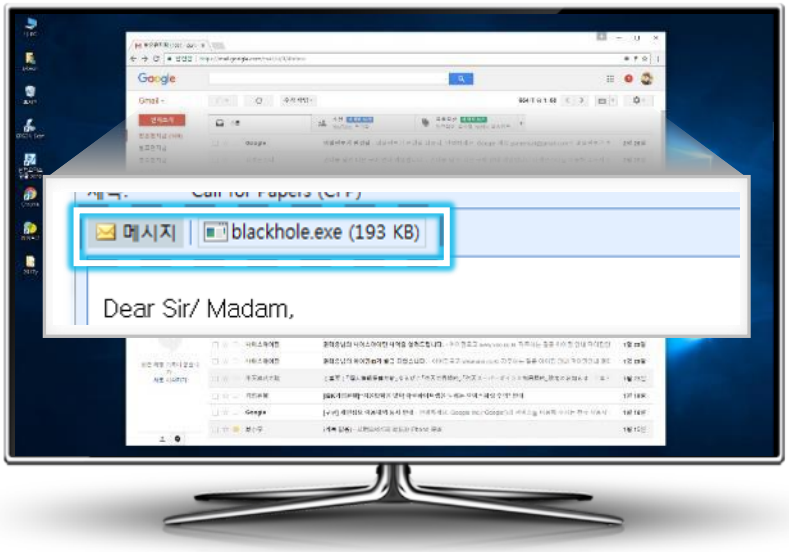
시간차 공격

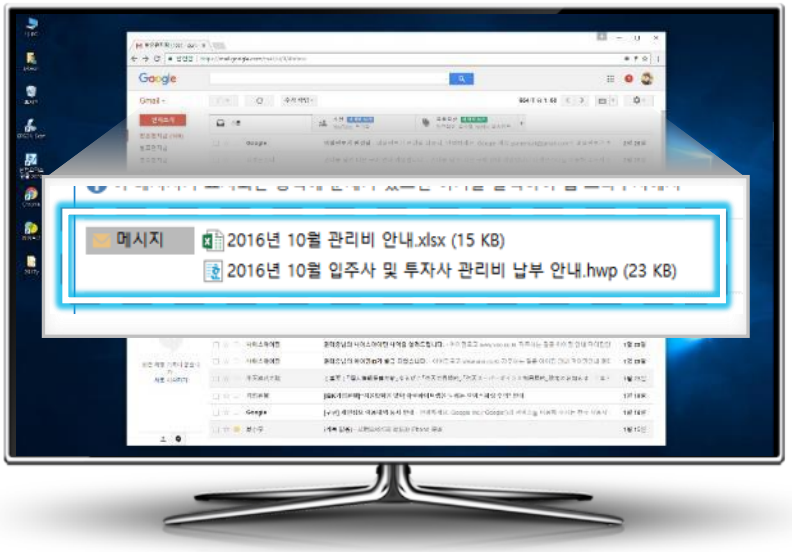
열람 시
바로 행위를 하지 않고
일정 시간을 기다립니다

사용자 행위 조건

특정 페이지 열람 등
사용자의 행위가 있을 시
악성행위가 시작됩니다

이제는 **어떠한 문서 파일**도 그대로 **믿을 수 없습니다.**





- 초창기 공격 유형은 실행 파일 자체를 첨부하여 실행 시 **악성행위를 바로 일으키므로 실행 파일 첨부 자체를 차단**

샌드박스 기반의 솔루션들 생겨남	GMail, Naver **메일 실행파일 첨부 차단**	**각 기업 및 기관 Email**

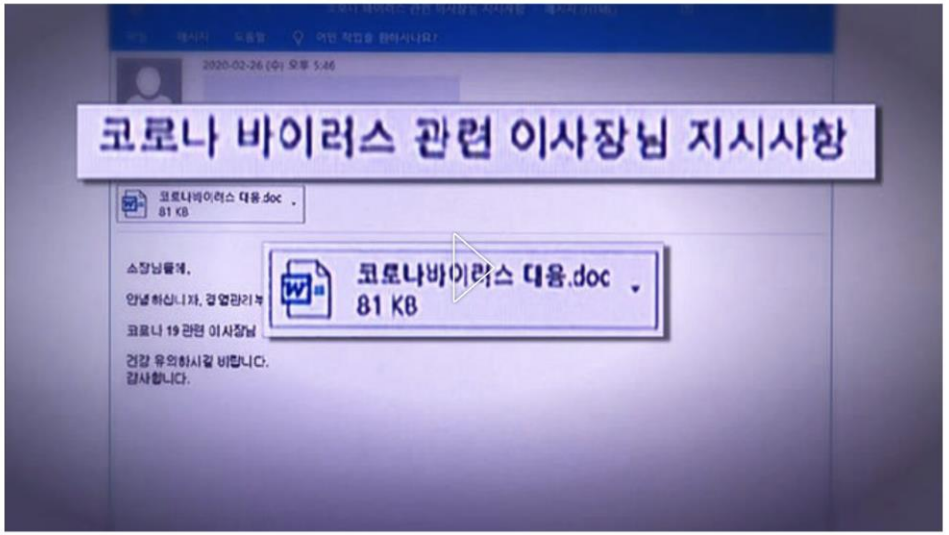
- 실행파일(.exe , .dll 등)이 첨부가 막히자 **공격자들은 비실행 파일, 즉, 일반 문서 파일의 취약점을 이용한 공격을 계획함**
- 파일에 사회공학적인 요소까지 추가하여 **사용자로 하여금 문서 파일을 열람하도록 유도하고 있습니다.**

SBS NEWS

8뉴스 코로나19 현황 사회

"코로나19 이사장 지시사항" 메일 열어보니 '해킹'

최고운 기자 gowoon@sbs.co.kr 작성 2020.05.03 21:26 수정 2020.05.03 22:34 조회 4,979



한국경제

'언택트 시대' 노리는 해커의 검은 손

입력 2020.04.27 15:46 | 수정 2020.04.27 15:46 | 지면 B2

코로나 공포심 악용한 '메일·사기 스미싱' 급증
1분기 사이버 공격 170만건…작년보다 21%↑

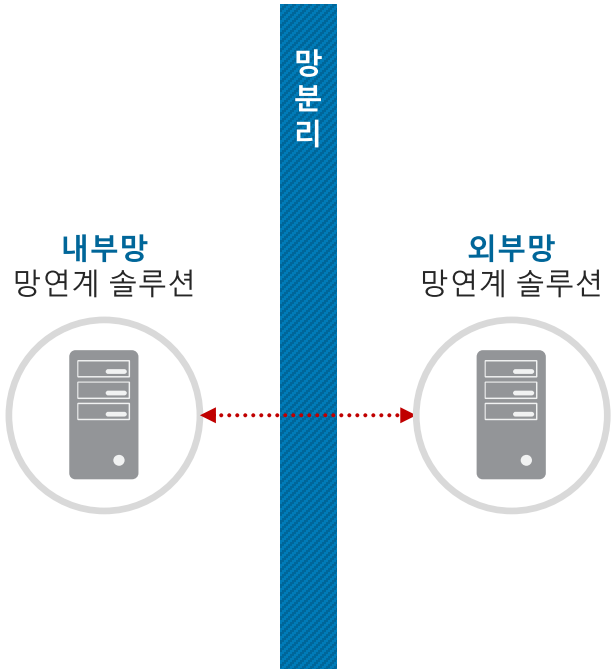
방역당국 등 정부 사칭한 악성 이메일 탐지
마스크·원격수업·게임파일 클릭했다 '낭패'도

신종 코로나바이러스 감염증(코로나19) 확산으로 원격 근무와 온라인 개학이 진행되고 있는 가운데 이를 노린 해커들의 공격 사례가 이어지고 있다. 마스크, 협업도구 등 코로나19와 관련해 높은 관심을 받는 주제를 이용한 악성메일 공격이 늘어나고 있다. '사회적 거리두기'로 인기를 끌고 있는 게임기기 판매 사이트로 위장해 정보를 빼내는 공격도 발견됐다.

Why SecuLetter? | 망연계 솔루션의 보안 허점

망연계 솔루션은 망분리 후 외부 파일을 유입 할 수 있는 유일한 수단입니다.

망분리 사고	망분리 원인
2016년 6월 13일 대기업 2곳 피씨관리시스템 솔루션 취약점 악용 해킹	• 14년 7월 부터 해킹 준비 한 것으로 파악 되며 솔루션에 대한 취약점을 노려 관리자 PC에서 내/외부망이 접근 되었다는 문제가 있음 - 기업 PC 관리시스템 취약점을 이용 하여 내부 접근 해킹 - 4만 여건의 산업/통신 시설 문서 유출
2016년 7월 25일 인터파크 DB접근통제의 관리 소홀 개인정보 유출	• 망분리 환경에서 담당자PC가 내/외부망에 연결이 가능하여 개인정보DB에 접근이 문제가 되었으며 DB접근통제도 문제가 있었음 - 해커는 스피어피싱으로 직원PC에 악성코드를 최초 감염 - 직원 PC에서 DB서버에 접속하여 개인정보를 탈취하고 외부로 유출
2016년 12월 06일 군 내부 사이버망 망연계 솔루션의 취약점 해킹	• 군업무망 인터넷용, 국방망, 전작망으로 구성 되어 있고 백신중계서버가 내/외부망 동시 연결로 인하여 발생된 문제 - 해킹으로 인하여 3200대 감염 중 700대가 내부망 - 국방망 일부 군사자료 유출
2017년 6월 10일 인터넷나야나 랜섬웨어 담당자 부주의	• 망분리 환경은 아니지만 담당자PC가 내/외부망에 연결 가능 하게한 부주의 - 해커는 지능형 지속 위협(APT) 공격 및 랜섬웨어(Erebus) 공격으로 담당자PC 장악 - 대량의 서버 랜섬웨어로 감염 피해

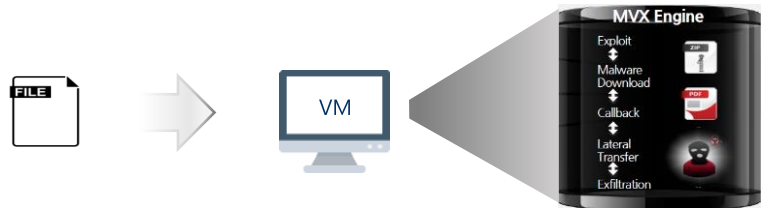


정책적으로 승인 되어 있는 망연계 시스템에 보안 조치를 취하지 않았을 경우 확인 되지 않은
악성코드(Unknown Attack)은 망분리 이전과 같이 동일 하게 유입이 됩니다.
즉, 망분리를 안 한 것과 같습니다.

Why SecuLetter? | 시큐레터 서비스 특징

**시큐레터는 악성코드에 대한 전문 진단 및 분석 엔진을 사용하여,
행위가 없는 비실행형 파일을 정확하게 진단합니다.**

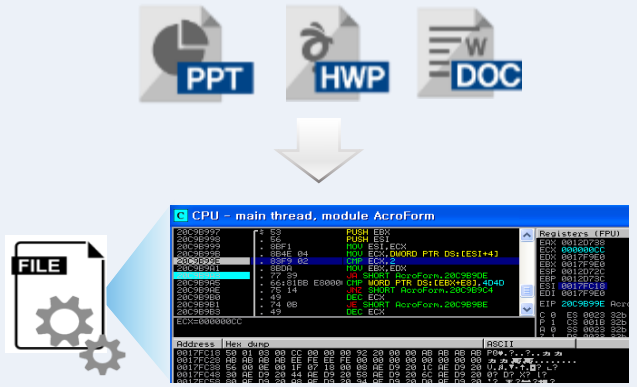
행위기반 악성코드 분석 기법



행위 기반 분석

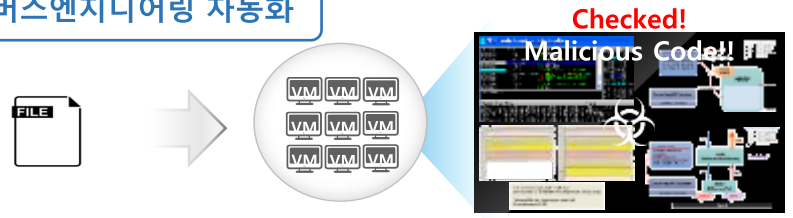
- 행위기반의 악성코드 분석은 파일을 실행하면서 악성행위를 분석하여 악성코드를 진단함
- **비실행형 파일은 행위가 없는 파일이기 때문에 악성코드 탐지율이 낮음**

비실행형 파일 악성코드 분석 기법



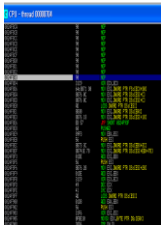
비실행형 파일은 리버스엔지니어링 기술로 악성코드를 분석해야 함

리버스엔지니어링 자동화

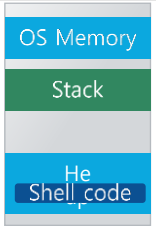


CPU Register 분석

SEH Chain 분석



메모리 분석 확인

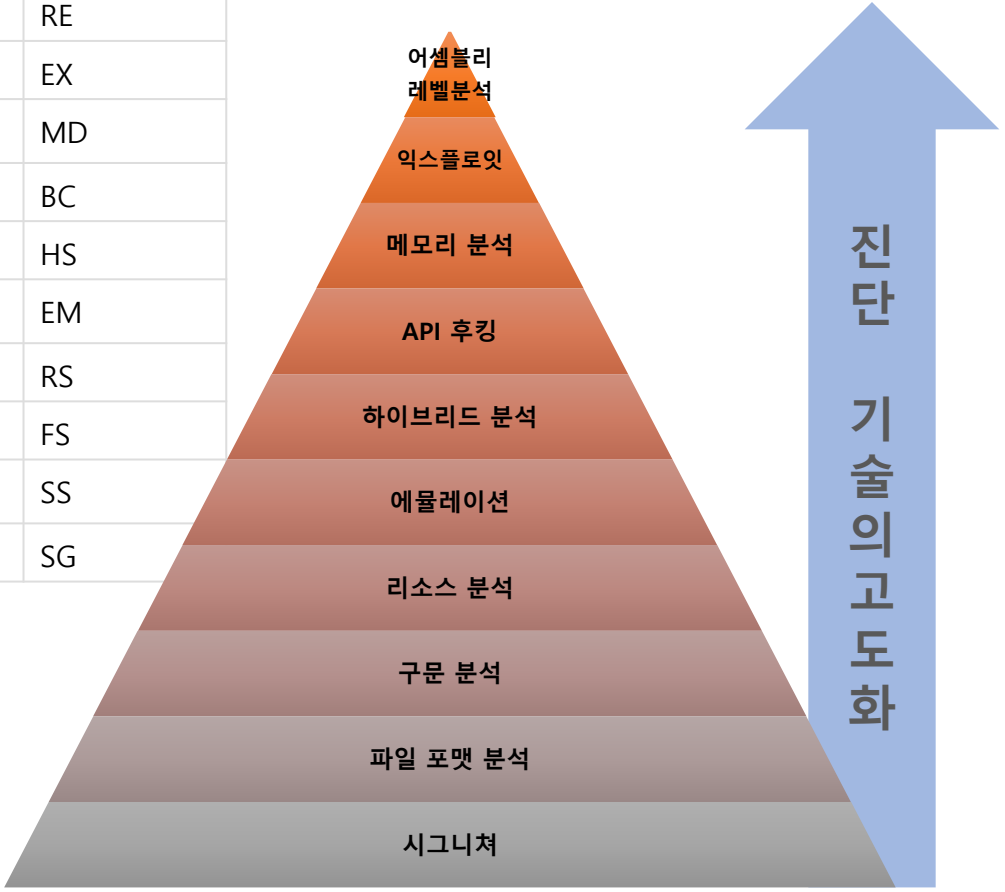


시큐레터 제품

- 시큐레터는 전문 진단 및 분석엔진을 이용하여 악성코드를 정확하게 진단함
- **행위가 없는 비실행형 파일에 대한 악성코드를 정확하게 탐지함**

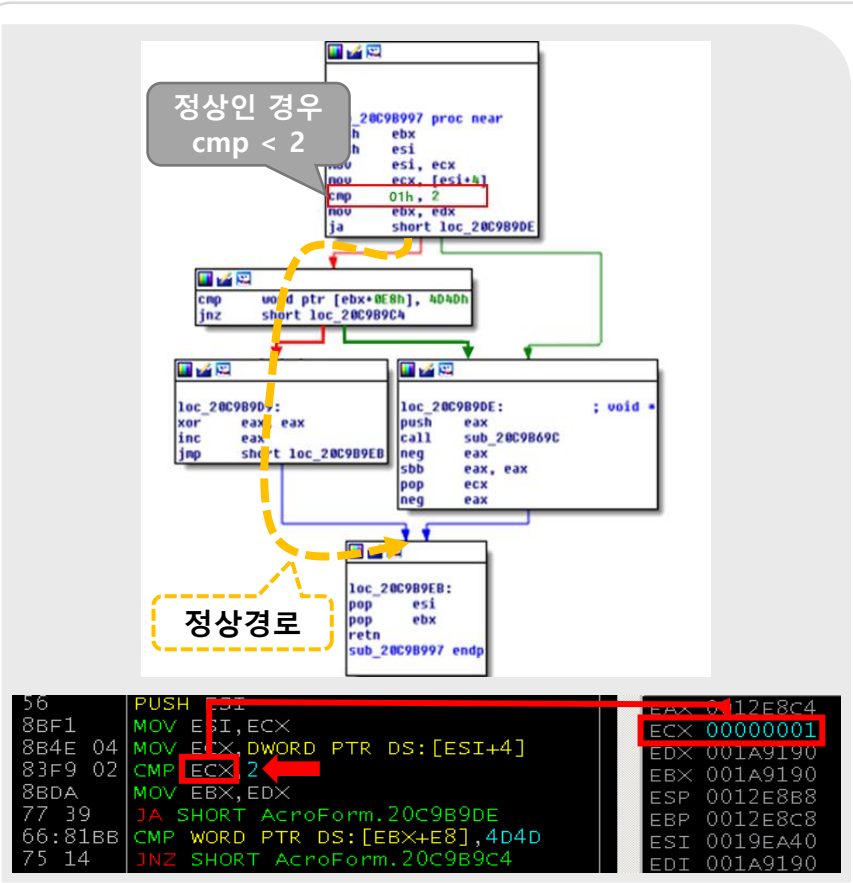
분석엔진 아키텍처

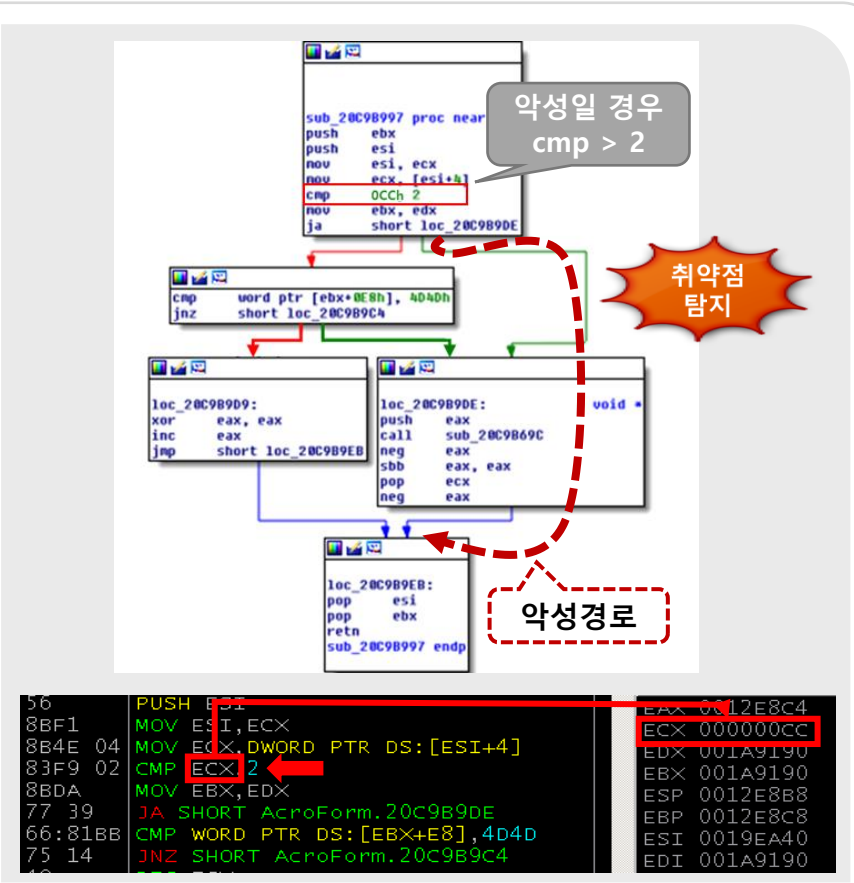
대분류	소분류	분류 코드1	분류 코드2
동적 분석	어셈블리 레벨	Reverse engineering	RE
	익스플로잇	Exploit monitor	EX
	메모리 분석	Memory based detection	MD
	API(행위) 분석	Behavior chasing	BC
동/정적분석	하이브리드 분석	Hybrid analysis	HS
정적 분석	에뮬레이션	Emulation based lexical analysis	EM
	리소스 분석	Resource inspection	RS
	구문 분석	Feature deep scan	FS
	파일 포맷 분석	Structure abusing scan	SS
	시그니쳐	Signature	SG



어셈블리 레벨 분석 기술 – 취약점 분석

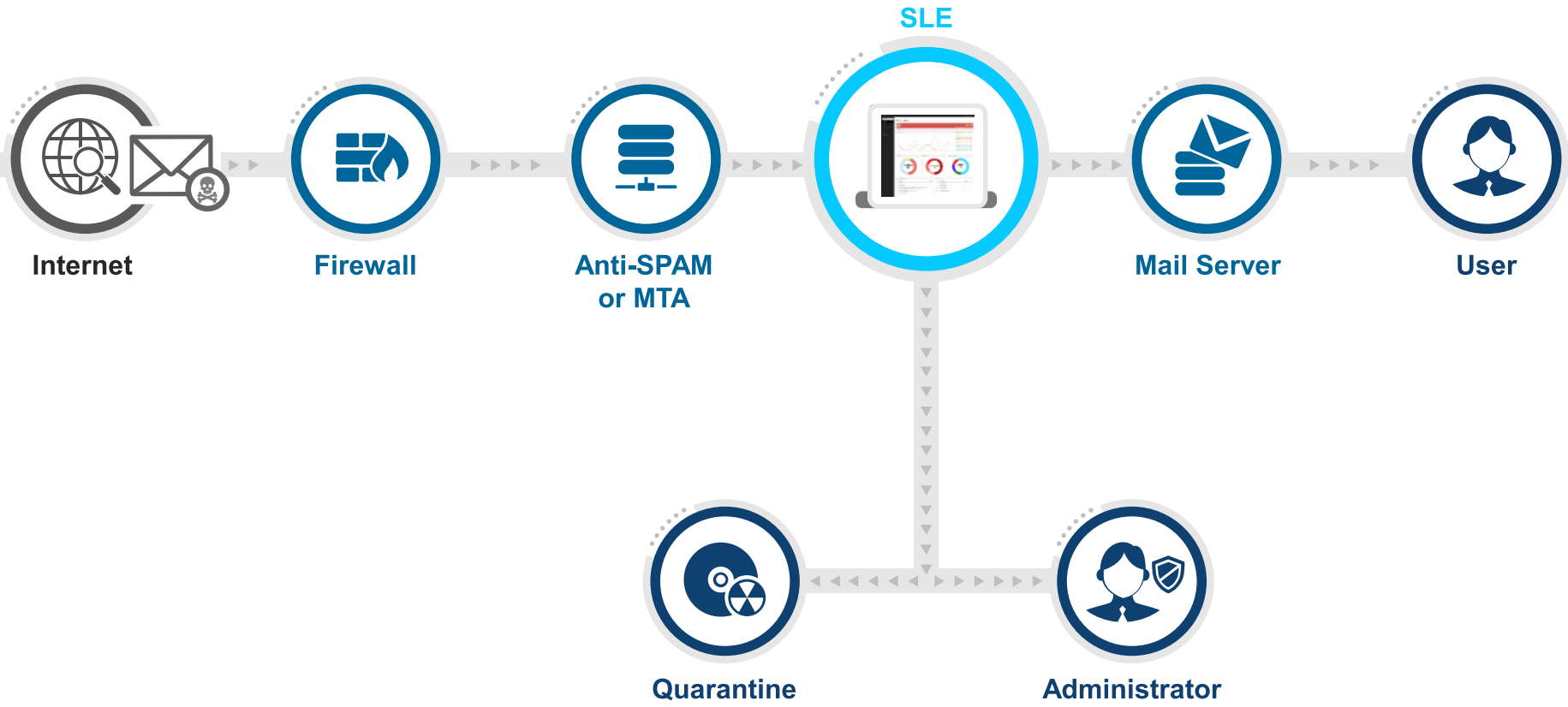
분석가가 직접 취약점 발생 원인을 분석하여 자동화 분석 엔진에 적용, 이를 이용하여 취약점이 발생 지점을 확인하여 진단





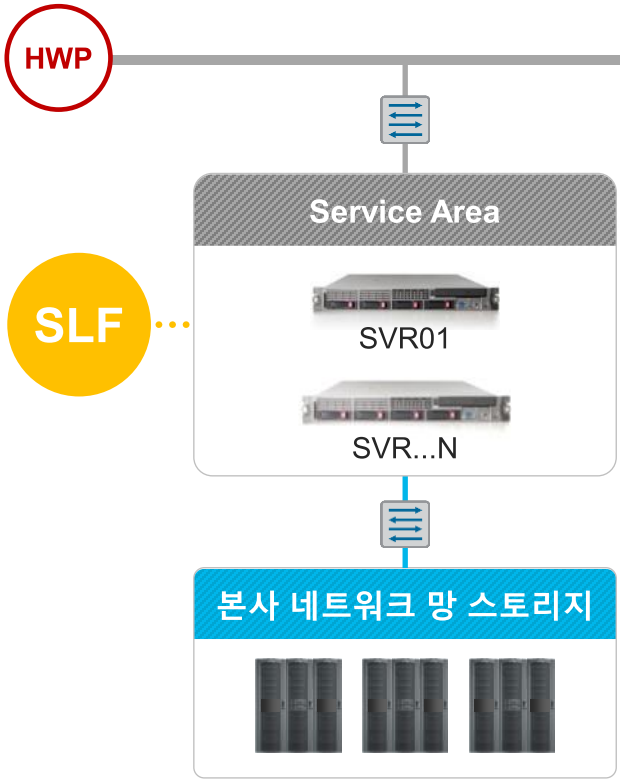
간단한 구성으로 최상의 이메일 보안을 구축합니다.

메일에 포함된 지능화된 악성코드 미리 탐지

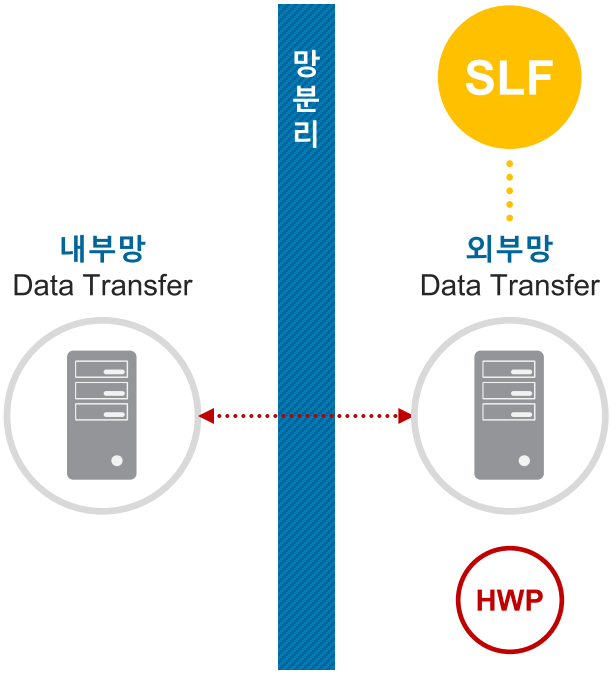


파일이 **내부 시스템에 들어오는 경로**에 배치하여 **효율적으로 위협을 제거**합니다.

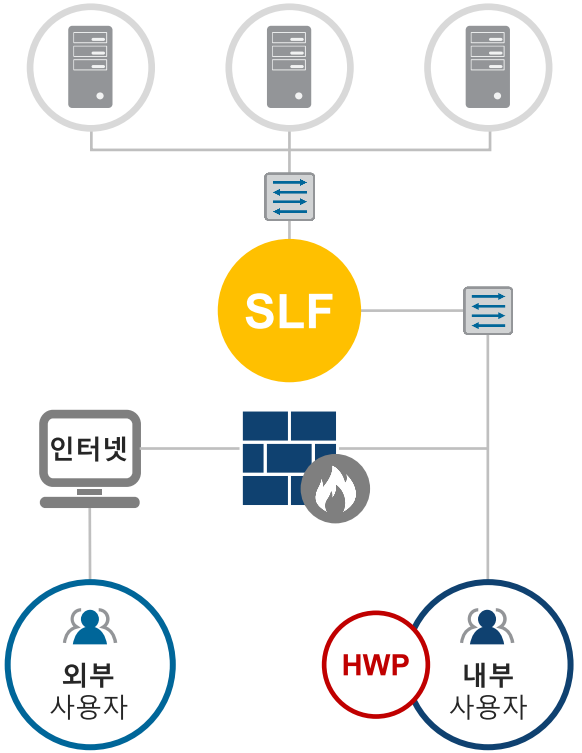
문서 집중화 솔루션 연계



망연계 솔루션 연계



웹 공용 게시판



악성코드 진단 및 처리 현황

간단한 요약 화면으로 최신 악성코드 **진단 현황**을 보여드립니다

Results

CRITICAL 55%

Exploits

Exploit/ HWP. MalFunction 47%

Malicious File types

HWP 49%

Top 10 Malicious File List

#	File Name	Count
1	청와대 비서실의 보고서 작성법.hwp	5
2	이력서-이광희.hwp	3
3	0683fac0b564fe5d2096e207b374a238a811e67b87856fc19bdf8eb3d6f76b49	2
4	ad251fd7427c0334f34aabe100a216b4af48b1ab4a01705f44b3421edd0be6ae	2
5	이력서-이광희_3.hwp	2
6	af2cc5bb8d97bf019280c80e2891103a8a1d5e5f8c6305b6f6c4dd83ec245a7d	2
7	이력서-이광희_2.hwp	1
8	e13a0357cd51795100dbce25fe846783fbb7fd22c5efe438d9059edc10492f49	1
9	d8359ceec234e2dac2e18307a7986c25b3f08a9e6f707d61d4c006d20c83e7b8	1
10	1140e06fa8580cf869744b01cc037c2d2d2b5af7f26f5b3448d9a536674d681c	1

Top 10 Exploit List

#	Exploit Name	Count
1	Exploit/HWP.MalFunction	31
2	Suspicious/PDF.MalFunction	15
3	Exploit/RTF.ExecuteWinExec	12
4	Exploit/DOC.ExecuteWinExec	4
5	Exploit/HWP.HWPNOP	2
6	Exploit/HWP.A_SEH	1
7	Exploit/HWP.E_PE	1

Appendix: 언론 속의 시큐레터

$600만달러 시리즈B 투자 유치 (2019.11)

전자신문 Conference allshowTV ETEdu English

통신&방송 SW&게임&성장기업 소재&부품 전자&자동차&유통 경제&금융 산업&과

시큐레터, 600만달러 시리즈B 투자 유치

발행일 : 2019.11.26 기사만 콕 종료 가 가

[올쇼TV] IBM이 소개하는 차별화 된 전략 '컨테이너화' (5/22 생방송)

<임차성 시큐레터 대표(왼쪽부터), 칼리드 알-살레 RVC CEO, 이윤수 시큐레터 COO, 모하메드 알자랄라 RVC 사업개발 총괄, 하템 알타리크 RVC 컨설턴트가 투자 유치 확정후에 기념촬영했다.>

$800만달러로 시리즈B 투자 유치 완료 (2020.02)

yahoo! finance

Search for news, symbols or companies

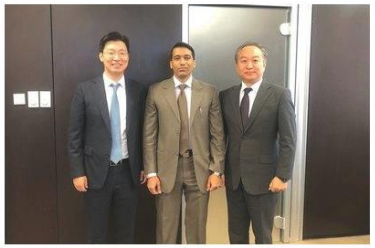
Markets News Personal Finance Videos Industries Tech

Funding round led by UTC Investment, RVC, KDB Bank, and KIP, brings total funding US$10.02M

SecuLetter to accelerate global expansion into the cyber security market

SEOUL, South Korea, March 20, 2020 /PRNewswire/ -- SecuLetter Co., Ltd, a member company of the Born2global Centre, successfully closed US$8 million in Series B funding round - gaining US$2 million from UTC Investment in late February, just three months after attracting US$6 million in November 2019. This brings SecuLetter's total funding to US$10.02 million. SecuLetter's valuation is estimated to be US$38 million.

The company's Series B funding round led Riyadh Valley Company (RVC), a Saudi Arabian venture capital firm, KDB Bank (Korea Development Bank), Korea Investment Partners (KIP), and UTC Investment.



SecuLetter closes US$8M Series B funding round to accelerate global expiation into cyber security market.

BNK부산은행 MARS SLF 도입 (2019.11) 중부대학교 MARS SLE 도입 (2020.01)

시큐리티월드 보안뉴스

#전체기사 #시큐리티월드 #사건사고 #2020년 보안시장 #코로나19

Home > 전체기사

BNK부산은행, APT 공격 차단 위해 '시큐레터 보안 솔루션'

▲BNK부산은행 정보보호 관제센터팀 모습[사진=부루글로벌센터]

WRDE COAST TV HOME NEWS WEATHER TRAFFIC SPORTS

Joongbu Univ. to strengthen its email security with SecuLetter

SOURCE Born2Global Centre

SecuLetter's SEG responded to advanced email hacking attacks effectively.

SEOUL, South Korea, June 10, 2020 /PRNewswire/ -- Joongbu University has strengthened its email security by adopting MARS SLE which is SecuLetter's Secure Emil Gateway(SEG) solution for intelligent email hacking attacks and successfully handled malicious code threats sent through email. SecuLetter has been a member of the Born2Global Centre since 2017.

MARS SLE Email Security

이메일을 통해서 유입되는 알려진 악성코드 공격과, 알려지지 않은 악성코드 공격을 탐지, 진단, 분석, 차단하는 완전한 이메일 해킹 보안 솔루션입니다.
특히, 비실행 파일 전문 분석 엔진을 탑재하여, 문서를 통해 발생하는 악성행위를 가장 정확하고 신속하게 사전에 탐지 및 차단합니다.

SLE 주요 기능

- 이메일 첨부 파일에 대한 악성코드 분석
- 이메일 본문의 링크를 통해 다운로드 되는 파일에 대한 악성코드 검사
- 악성코드로 판단된 메일 격리 및 저장
- 악성코드 탐지 결과에 대한 상세 리포트 제공

Add-on

- CDR: 문서 내, 악성 URL 및 실행코드가 포함된 액티브 컨텐츠(Macro, JS 등) 제거

MARS SLF File Security

외부 및 내부망을 통해 파일을 주고 받는 환경에서 파일을 통해 유입되는 악성코드를 사전에 탐지, 차단해주는 망 연계 보안 솔루션입니다.
SLF는 망연계서버, 문서중앙화 서버, 웹 게시판 서버 등에 적용되어, 다양한 컨텐츠로부터 발생할 수 있는 악성코드 위협을 철저히 제거 및 차단함으로써 고객의 시스템을 안전하게 보호해 줍니다.

SLF 주요 기능

- 내부망으로 유입되는 파일의 악성코드를 진단하여 사전 차단
- 스토리지 파일에 대한 악성코드 감염 여부 진단
- 파일의 용량에 상관 없이 악성코드 진단 지원
- 악성코드 탐지 결과에 대한 상세 리포트 제공

Add-on

- CDR: 문서 내, 악성 URL 및 실행코드가 포함된 액티브 컨텐츠(Macro, JS 등) 제거

MARS SLCS Cloud Email Security

시큐레터의 어플라이언스 제품인 SLE나 SLF가 수행하는 전문 악성코드 분석 기법을 클라우드 환경에서 제공하는 이메일 해킹 보안 클라우드 서비스입니다.
SLCS는 이메일에 포함되어 유입될 수 있는 랜섬웨어, 제로데이공격, 등의 각종 위협을 차단하며, 알려지지 않은 공격에 대해서도 탐지 및 원천 차단합니다.

SLCS 주요 기능

- 랜섬웨어, 제로데이 해킹공격 등 악성 공격 탐지
- 알려지지 않은 신, 변종 악성코드 탐지
- 간단한 MX 레코드 값 변경으로 악성메일에 대한 알람 기능 제공
- 연 과금 형태로 악성코드 진단서비스 제공

Appendix: 시큐레터 제품

	MARS V2 Standard	MARS V2 Enterprise
Software Package	· License : 1~2999 User · CPU: 2.1GHz 20Core · Memory: 128GB · SSD 960GB (RAID 5) · SAS 2.4TB (RAID 5) · NIC : 1G Copper 2 Port · OS: CentOS 8 이상 	· License : 3000 User 이상 · CPU: 2.1GHz 40Core · Memory: 256GB · SSD 1.92GB (RAID 5) · SAS 4.8TB (RAID 5) · NIC : 1G Copper 2 Port · OS: CentOS 8 이상 
	SLE1000 | SLF450	**SLE5000 | SLF1800**
Appliance	· Dynamic Analysis AV Engine · 가상 디버깅엔진 VDE 32개 · Email 일 180,000건 | File 일 45,000건 처리 · CPU: 2.1GHz 10 Core · Memory: 32GB · SSD 480GB (RAID 1) · SAS 1.2TB (RAID 1) · NIC : 1G Copper 2 Por 	· Dynamic Analysis AV Engine · 가상 디버깅엔진 VDE 122개 · Email 일 640,000건 | File 일 180,000건 처리 · CPU : 2.1Ghz 40 Core · Memory : 256GB · SSD : 1.92TB (RAID 5) · SAS : 4.8TB (RAID 5) · NIC : 1G Copper 2 Port 

주요인증 및 수상내역

TI-3 기술평가등급
NICE평가정보

우수 정보보호기술
지정서

과기부 표창장

CC인증서

과학기술정보통신부
우수 정보보호 제품・기술 보유기업

중소기업 확인서

벤처기업확인서

메모리분석 특허증

퍼스트펭귄형 기업선정서

GS 인증서

소프트웨어사업자
신고서

ISO9001

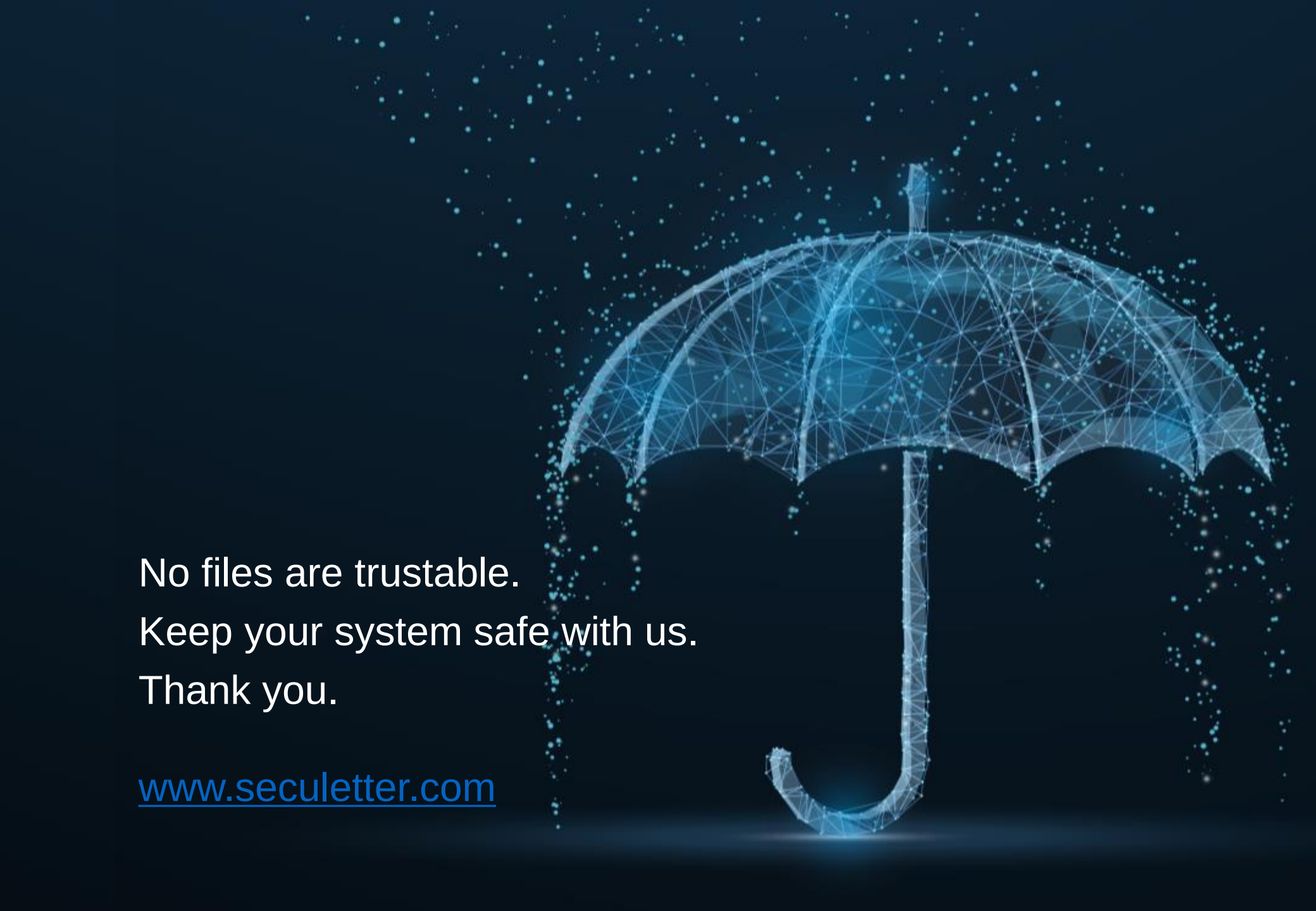
ISO14001

KCGA
보안솔루션대상

SLF 소프트웨어
품질인증서

SLE 소프트웨어
품질인증서

직접생산
확인증명서


No files are trustable.
Keep your system safe with us.
Thank you.
www.seculetter.com