2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 5-4

Deep Learning, Forensic Big Data 무결성 및 딥러닝 기반 엔드 포인트 지능형 보안 위협 대응 기술

김종만 대표 (㈜소테리아)

[요약문]

최근 사이버 공격은 자가 학습 방식 악성 코드로 공격 패턴의 지능화, 신악성코드의 폭발적 증가 등으로, 정책(Rule) 기반의 보안 대응 기술은 한계를 드러내고 있다. 이러한 문제를 개선하기 위해 행위 분석에 기반한 탐지 시스템(IDS)을 필요로 하게 되었으나, 기존 Machine Learning 방식 혹은 Deep Learning 방식의 단편적인 응용으로는 혁신적인 행위 기반 탐지 기술이라 하기엔 그 성능이 미흡한 실정이며, 입력 데이터의 무결성 확보는 AI를 활용한 탐지 기술의 중요 요소 중 하나로 떠오르고 있다. 이러한 시장의 동향과 기술적 한계를 극복하기 위한 앙상블 모델(Neurotron - 커널 포렌식 빅데이터 딥러닝 지능형 분석 듀얼 엔진)을 개발, Neurotron이란 시스템 호출 순서의 비정상을 탐지하는 Sequence 엔진과 내용의 비정상을 탐지하는 Argument 엔진으로 구성된 듀얼 엔진을 의미하며, 협응을 통해 오탐, 미탐을 최소화하고 비정상 동작 및 해킹 등의 공격에 대한 탐지 정확도를 기존대비 99.9% 향상 시키는 등 혁신적으로 성능을 개선하였다. 한편, 최근의 사이버 공격은 조직화 지능화되어 흔적을 남기지 않거나(Fileless Attack), 추적을 불가능하게 고도화되고 있다. 이러한 문제점을 제거하기 위해, 커널 인터페이스로 전용 하드웨어 디바이스에 시스템 데이터를 직접 hook up 하고, 위변조를 원천 차단하여, 입력 데이터의 무결성을 보장하였다. 또한, System call trace를 분석하여 해킹, 장애 등의 탐지 및 Causality Relations Visualization을 구현하여 효과적인 대응 솔루션을 구성하였다.

[발표자 약력]

[학위]
펜실베니아 주립대학교 컴퓨터공학 박사, 2007
펜실베니아 주립대학교 전자공학 석사, 2001
서울대학교 전기공학 학사, 1990

[경력]
- 클리블랜드 주립대학교 전기컴퓨터공학부 교수, 2016 - , 클리블랜드, 오하이오
- 조지아 공대, 전기컴퓨터공학부 교수, 2007-2016, 아틀란타, 조지아주
- Soteria Systems 창업자, CEO & President
- 인포머시브 연구센터장 (Director of Center for Informersive Systems (CIS)), Georgia Institute of Technology, 2009 - 2014
- Samsung America in Dallas, Consultant, 2012/2013.
- LG 전자 연구원, 1993-1999

Deep Learning, Forensic Big Data 무결성 지반 엔드 포인트 지능형 보안 위협 대응 기술

㈜소테리아

Chapter

1.

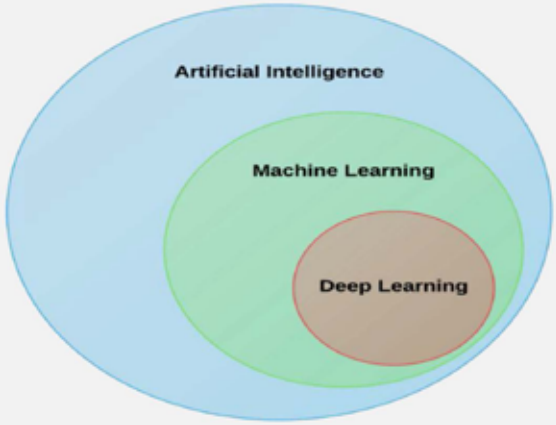
기술현황 및 AI 보안 기술개발의 필요성

SOTERIA
CYBER SECURITY

01 딥러닝 Multi AI 엔진

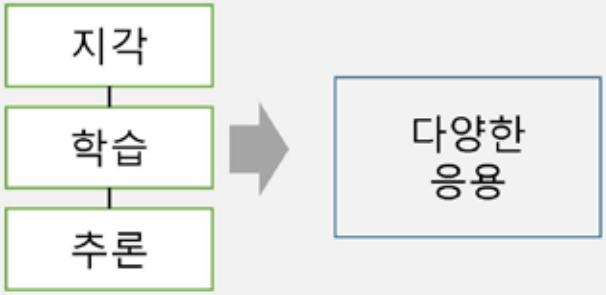
SOTERIA CYBER SECURITY

사람과 유사한 지능을 가지도록 인간의 학습능력, 추론능력, 지각능력, 자연어 이해능력 등을 컴퓨터 프로그램으로 실현하는 기술



기계학습(Machine Learning)은 인공지능의 한 분야로 기계 스스로 대량의 데이터로부터 지식이나 패턴을 찾아 학습하고 예측을 수행하는 것

딥러닝(Deep Learning)은 컴퓨터가 스스로 학습할 수 있게 하기 위해 인공 신경망을 기반으로 하는 기계학습 기술의 일종으로 인간의 두뇌가 수많은 데이터 속에서 패턴을 발견한 뒤 사물을 구분하는 정보처리 방식을 모방



1. 악성 행위 탐지와 공격 저지
2. 엔드포인트 분석
3. 사람의 분석 능력 및 결과 보강 — AI-SBB
4. 보안 반복 작업 자동화 — AI-SBB
5. 제로데이 취약점 제거

출처 : 보안을 위한 머신러닝 사용 사례 5가지 - ITWorld Korea - http://www.itworld.co.kr/news/107587

02 AI 기반 침해 위협 분석

SOTERIA CYBER SECURITY

❑ 딥뉴럴네트워크를 이용한 침해 위협 분석 기술

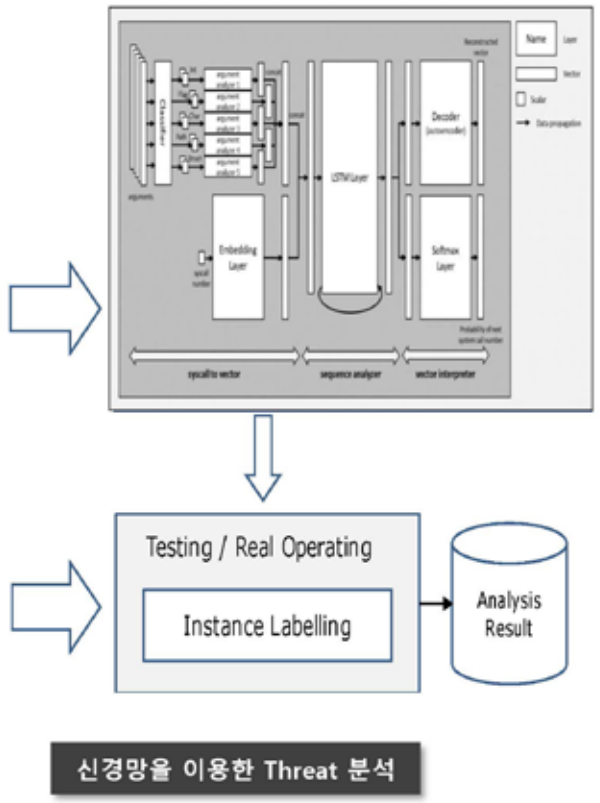
✓ **Algorithm :**

- 딥 뉴럴 네트워크 학습을 이용한 침해 위협 분석 기술 개발
- 침해 위협(Threat) 탐지를 위한 **뉴럴 네트워크 모델 생성** :

  98% Accuracy
- 다양한 심층 신경망 구조 실험에 의한 **뉴럴 네트워크 최적화 수행 및 검증**
- 학습 데이터 **: 정상적인 시스템 호출 데이터를** 통한 학습
- 학습 결과 : **침해 위협 분석을 위한 심층 신경망 모델**

✓ **Input : Raw Systemcall event**

✓ **Output : Analysis Result (Threat or Normal per Time)**



신경망을 이용한 Threat 분석

SOTERIA CYBER SECURITY

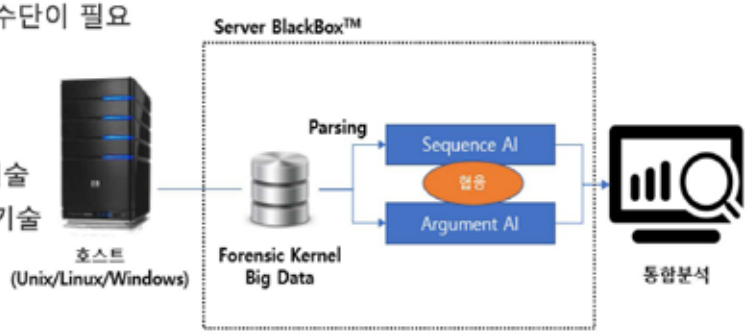
AI 포렌식 빅데이터 무결성 기반 지능형 보안위협 대응 기술

기술배경

- 사물인터넷 서비스 활성화에 따른 신종 악성 코드의 증가
- 공격패턴의 지능화와 고도화 등으로 규칙기반의 보안기술은 한계성을 가짐
- AI 행위분석을 통한 지능형 탐지 및 차단을 통한 즉각적인 대응시스템 필요
- 보안침해사고 관련 무결성을 보존하고 원인 분석을 위한 기술적 수단이 필요

AI 보안 기술 특징

- 최신 딥 러닝 기반 듀얼 엔진을 이용한 AI 기반 보안 침해 탐지 기술
- 서버의 시스템 호출 정보를 이용한 근본 원인(Root Cause) 분석 기술
- 하드웨어 기반 무결성 변조 불가 데이터 보존 기술
- 시스템 콜 이력 및 신뢰성 연관 포렌식 데이터 filtering 기술



기대효과

- 선제적 예방 보안 및 Dependability (신인성) 증대
- 로컬 딥 런닝 엔진으로 필요 정보의 최소 노출 및 무결성 IRM 자동 감사 기능으로 내부자 보안 강화
- FIN Tech, Smart Factory, 자율 주행 자동차 등 인공 지능 사이버 보안 연관 산업으로 확장

04 최근 Cyber Security 현상 및 문제점

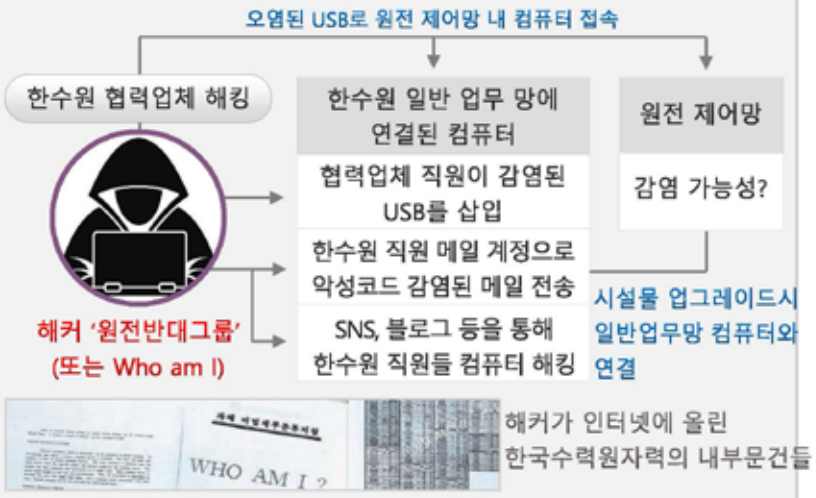
SOTERIA CYBER SECURITY

최근의 신종 악성코드는 흔적을 남기지 않거나 증거를 삭제할 정도로 지능화 되어 증거 보존이 쉽지 않으며, 피해자가 해킹 사실 자체를 인지할 수 없도록 고도화되고 있어 침해사고 관련정보의 무결성을 보존하고 그 원인을 정확하게 분석할 수 있는 기술적 수단이 요구되고 있음.

최근 이슈

- 최근의 악성코드는 root 권한을 확보, 침해 사고를 야기한 후 관련증거를 은닉, 제거하는 알고리즘을 탑재함
- 이에 따라 탐지, EDR, 침해 원인 파악이 곤란함

한수원 원전 제어망 해킹 시나리오



시 사 점

- 최근의 해킹은 전문가그룹이 장기적으로, 주도 면밀하게 준비하여 실행하므로, 감지 및 방어가 갈수록 어려워지고 있음
- 악성코드는 악의 없는 임직원의 손을 통해 전체시스템에 확산되며, 활동 후 피해사실을 감추기 위해 관련증거를 삭제, 변조하는 행태를 가짐
- root 권한을 탈취당한 상태에서 서버내부의 보안모듈은 동작하지 못하므로, 중앙의 관제시스템은 무력화됨.

- Privilege escalation in Intel®, still fighting Meltdown and Spectre

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

05 보안 기술의 발전 속도를 뛰어넘는 사이버 공격 기술

SOTERIA CYBER SECURITY

	대량트래픽차단 (DDOS)	IP차단 (방화벽)	유해사이트 차단 (IPS, 웹필터)	악성코드 삭제/차단 (SandBox)	스팸메일 바이러스메일 (Anti Spam)	엔드포인트 (백신, EDR)
보안 제품						
우회 공격 유형	▪ 최소 트래픽 공격	▪ HTTP/HTTPS 공격 ▪ SMTP 공격	▪ HTTPS 통신으로 악성코드 트래픽 전송 ▪ 변종/다형성 기반의 악성코드 전송	▪ SandBox 우회/회피 ▪ VM회피, 휴먼 인터페이스 공격	▪ 사회공학적 기법의 바이러스메일 전송	▪ 주요 백신 테스트 후 공격

7

06 최근 Cyber Security 현상 및 문제점

SOTERIA CYBER SECURITY

- 최신 공격에대한 통합적인 보안 체계가 필요하고, 분석 및 시스템 안정성을 위해 필수적인 **실행 이력, 로그 무결성 보장** 이 매우 중요함
- **무결한 포렌식 정보들의 원본 수집** 으로부터 정확한 탐지 및 새로운 공격의 **행위분석의 정확도**가 높아질 것임
- 외부에서 오는 공격 뿐만 아니라 내부에서 시작되는 공격 또한 감지하고 탐지 할 수 있어야 합니다. 그러므로 네트워크 보안 뿐만 아니라 서버 혹은 컴퓨터 **엔드 포인트 보안강화** 중요성
- **규칙 (Rule) 기반** 뿐 아니라 **행위 분석 AI**는 선택 아닌 필수

시큐리티월드 보안뉴스

Home > 전체기사

흔적 지우는 와이퍼와 파일리스 악성코드로 더욱 정교해진 표적형 공격

좋아요 34개 | 입력 : 2017-05-03 00:06

가 가

2019년 파일리스 공격의 탐지 건수가 전년 동기대비 265% 이상 증가

(출처: 2019 중간보안위협 보고서 – 트렌드 마이크로)

시스템 침입 흔적을 남기지 않으므로 차후의 침입을 위한 루트킷(Rootkit) 응용, Stealthy 원격 접근, 메모리상에만 존재하고 파일 이력 없는 지속적인 스텔스 공격 시도

- Injecting malicious code into harmless processes: Reflective DLL injection, Process Doppelganging
- Living off the land: Powershell, PsExec, Netsh, SC, WMI
- Fileless persistence methods: WMI, Registry

8

07 Fileless Malware Stealthy Attacks

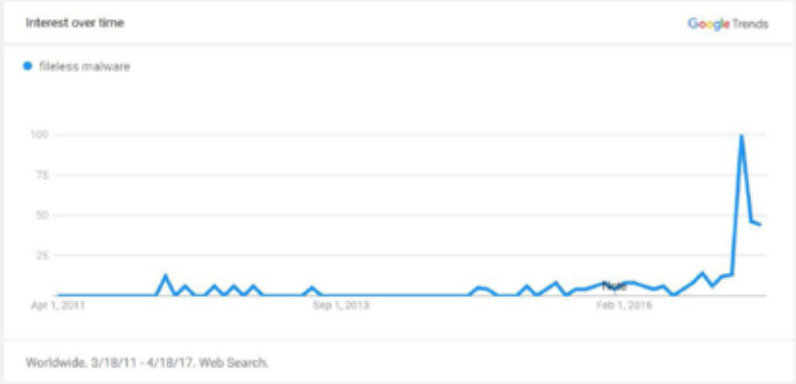
SOTERIA CYBER SECURITY

"Fileless malware is malware that operates without placing malicious executables on the file system."

https://zeltser.com/fileless-malware-beyond-buzzword/

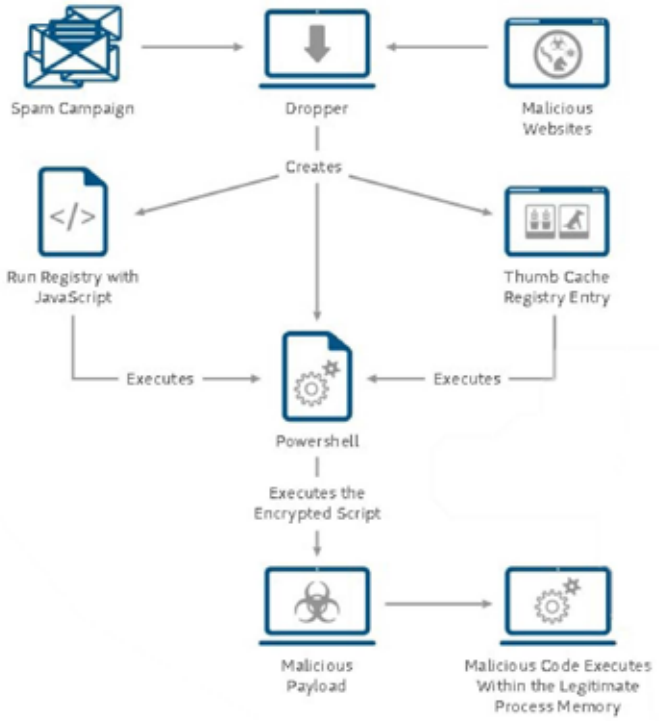
- ❑ **Non-malware attacks**
- ❑ **Memory only attacks**
- ❑ **Bodiless**
- ❑ **Advanced Volatile Threat (AVT)**
- ❑ **Non-PE attack**

*파일 없는 멀웨어 공격의 비율은 최근 1~2년 새 급증하고 있음



08 Fileless Malware Stealthy Attacks

SOTERIA CYBER SECURITY



-이런 공격은 사용자의 컴퓨터에 소프트웨어를 설치하는 행위를 수반하지 않기 때문에 바이러스 백신 도구들이 놓칠 확률이 다른 유형의 공격보다 높음.

-파일 없는 공격은 또한 승인된 어플리케이션만 시스템에 설치되도록 허용하는 화이트 리스팅(whitelisting)도 빠져 나가고 있으며, 이미 설치된 응용 프로그램을 이용하거나 화이트 리스트 목록에 올라 있는 승인된 앱을 이용하기 때문

[표 1] 파일 없는 공격의 작동 방식 사례

구분	사례
1 단계	- 사용자가 악성 웹사이트로 가는 링크가 포함된 스팸 메시지를 받음
2 단계	- 사용자가 링크를 클릭함
3 단계	- 악성 웹사이트는 사용자의 컴퓨터에 보안 취약점이 있는 어도비 플래시를 로딩함
4 단계	- 플래시는 윈도 파워셸 도구를 여는데, 파워셸은 명령어 라인을 통해 지시 사항을 실행할 수 있으며 메모리에서 작동함
5 단계	- 파워셸은 해커의 "실행과 제어(C&C) 서버"로부터 스크립트를 다운로드 받아 실행
6 단계	- 파워셸 스크립트는 사용자의 데이터 위치를 알아내 해커에게 전송

<자료> CSO, IITP 재정리

Chapter

2.

주요 기술

SOTERIA
CYBER SECURITY

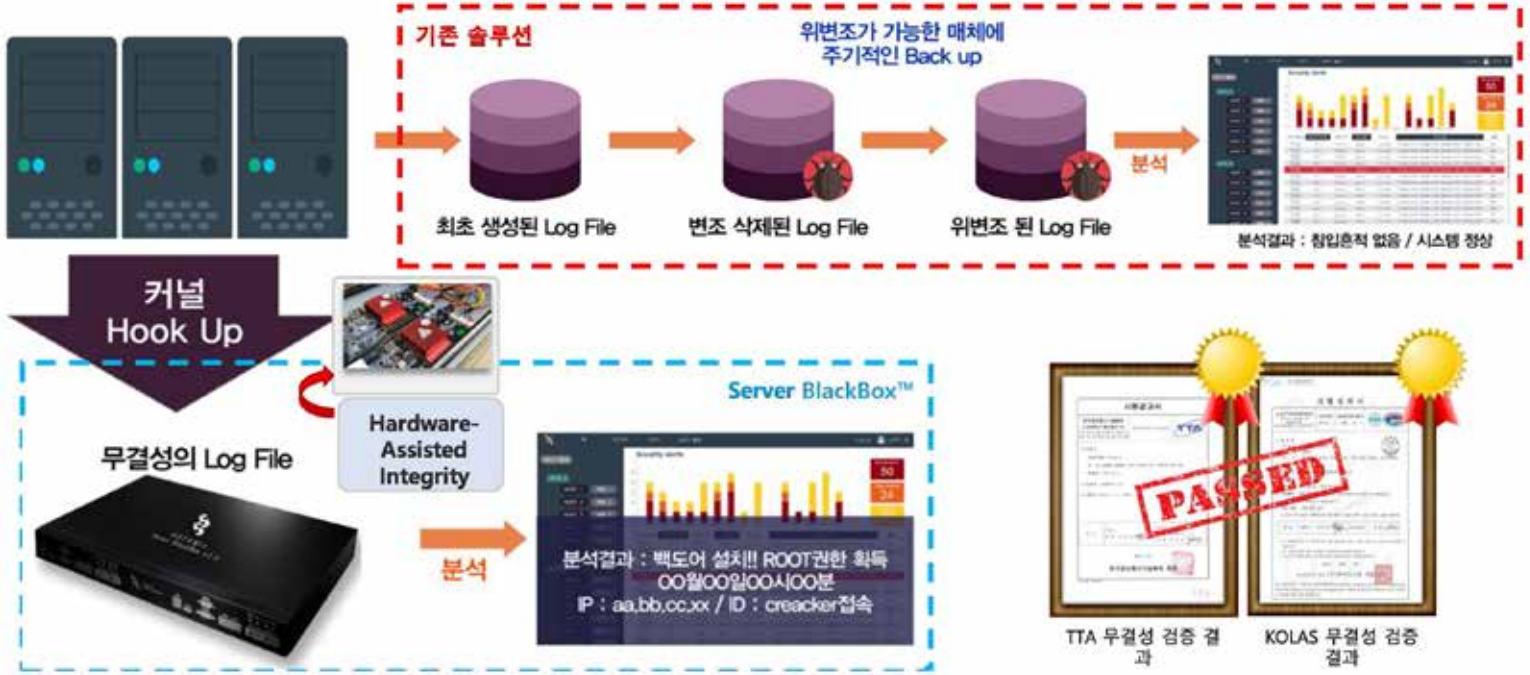
01 Input Data Integrity

SOTERIA CYBER SECURITY

무결성 수집 기술의 강점

1.로그를 파일에 쓰기 전에 커널 레벨에서 로그를 수집 저장
2.하드웨어 기반 Append Only Storage 기능으로 Data 보호 강화
3.분산형 로그 수집 방식으로 중앙 집중형 로그 수집 시 생기는 병목현상 완화(병목현상으로 인해 손실 되는 로그 missing방지)

기존 로그 수집 솔루션 대비 차이점



02 현장 적용 가능성 - KISA Hack The Challenge 해킹대회

SOTERIA CYBER SECURITY

SOTERIA CYBER SECURITY

Auditing events are generally defined at a system call level. A single Operation of a command, such as 1s, will record a log similar to Table 1.

Table 1. Audit record generated by the is command using event auditing

Event	Login	Status	Date/Time	Command
PROC_Create	root	OK	Fri Jun 09 11:02:41 2000	ksh
FILE_Close	root	OK	Fri Jun 09 11:02:41 2000	ksh
FILE_Open	root	OK	Fri Jun 09 11:02:41 2000	ksh
FILE_Read	root	OK	Fri Jun 09 11:02:41 2000	ksh
FILE_Close	root	OK	Fri Jun 09 11:02:41 2000	ksh
PROC_Execute	root	OK	Fri Jun 09 11:02:41 2000	ls
FILE_Open	root	OK	Fri Jun 09 11:02:41 2000	ls
FILE_Close	root	OK	Fri Jun 09 11:02:41 2000	ls
FILE_Write	root	OK	Fri Jun 09 11:02:41 2000	ls
FILE_Close	root	OK	Fri Jun 09 11:02:41 2000	ls
PROC_Delete	root	OK	Fri Jun 09 11:02:41 2000	ls

** IBM Redbooks " Auditing and Accounting on AIX*

- 호스트에서 특정명령 (옆의 예에서는 ls) 실행 시 시스템로그에서는 1줄 정도의 정보가 남지만 시스템 호출 데이터는 커널을 동작시키는 모든 이벤트가 저장됨
- 커널에서 실행되는 모든 데이터를 저장함으로써 해킹/장애의 근본원인을 찾는데 우수한 장점이 있음

04 Call Classification

SOTERIA CYBER SECURITY

Table 1 System call categories

Call group	Threat level	System calls	Number of calls
File system	1	chmod, chown, chown32, fchmod, fchown, fchown32, lchown, lchown32, link, mknod, mount, open, rename, symlink, unlink	15
	2	close, creat, dup2, flock, ftruncate, ftruncate64, ioctl, mkdir, nfsservctl, quotactl, rmdir, truncate, truncate64, umount, umount2	15
	3	chdir, chroot, dup, fchdir, fcntl, fcntl64, fsync, llseek, lseek, newselect, poll, pread, putpmsg, pwrite, read, readv, select, sendfile, umask, utime, afs_syscall, write, writev	23
	4	access, bdflush, fdatasync, fstat, fstat64, fstatfs, getcwd, getdents, getdents64, getpmsg, lstat, lstat64, oldfstat, oldlstat, oldolduname, oldstat, olduname, pipe, readahead, readdir, readlink, stat, stat64, statfs, sync, sysfs, ustat	27
Process	1	execve, setfsgid, setfsgid32, setfsuid, setfsuid32, setgid, setgid32, setgroups, setgroups32, setregid, setregid32, setresgid, setresgid32, setresuid, setresuid32, setreuid, setreuid32, setuid, setuid32	19
	2	vfork, adjtimex, brk, clone, exit, fork, ioperm, iopl, kill, modifyldt, nice, ptrace, reboot, sched_setparam, sched_setscheduler, sched_yield, setpriority, setrlimit, vhangup, vm86, vm86old	21
	3	capset, personality, prctl, setpgid, setsid, uselib, wait4, waitpid	8
	4	acct, capget, getegid, getegid32, geteuid, geteuid32, getgid, getgid32, getgroups, getgroups32, getpgid, getpgrp, getpid, getppid, getpriority, getresgid, getresgid32, getresuid, getresuid32, getrlimit, getrusage, getsid, getuid, getuid32, sched_get_priority_max, sched_get_priority_min, sched_getparam, sched_getscheduler, sched_rr_get_interval	29
Network	1	accept, bind, connect, listen, socket, socketpair	6
	2	recv, recvfrom, recvmsg, sedmsg, send, sendto, setsocketopt, shutdown	8
	4	getpeername, getsocketname, getsocketopt	3
Module	1	init_module, create_module	2
	2	deletemodule	1
	4	get_kernel_syms, query_module	2
Signal	2	rt_sigaction, rt_sigpending, rt_sigprocmask, rt_sigqueueinfo, rt_sigreturn, rt_sigsuspend, rt_sigtimedwait, sgetmask, sigaction, sigaltstack, signal, sigpending, sigreturn, sigsuspend, sigprocmask, ssetmask	16
Other	2	alarm, madvise, madvise1, mlock, mlockall, pivot_root, setdomainname, sethostname, setitimer, settimeofday, stime, swapoff, swapon, sysctl, syslog, ugetrlimit	16
	3	mincore, mmap, mmap2, modify_ldt, mprotect, mremap, munlock, munlockall, munmap, nanosleep, security	11
	4	break, ftime, getitimer, gettid, gettimeofday, gtty, idle, lock, mpx, msync, pause, prof, profil, stty, sysi, time, times, ulimit, uname	19

* Xu M, Chen C, Ying J. Anomaly detection based on system call classification. Journal of Software: 391~403.

1: Allows full control of the system

2: Used for a denial of service attack

3: Used for subverting the invoking process

4: Harmless

05 시스템 호출 분석 기술

SOTERIA CYBER SECURITY

○ 솔루션별 수집 가능 데이터(로그)

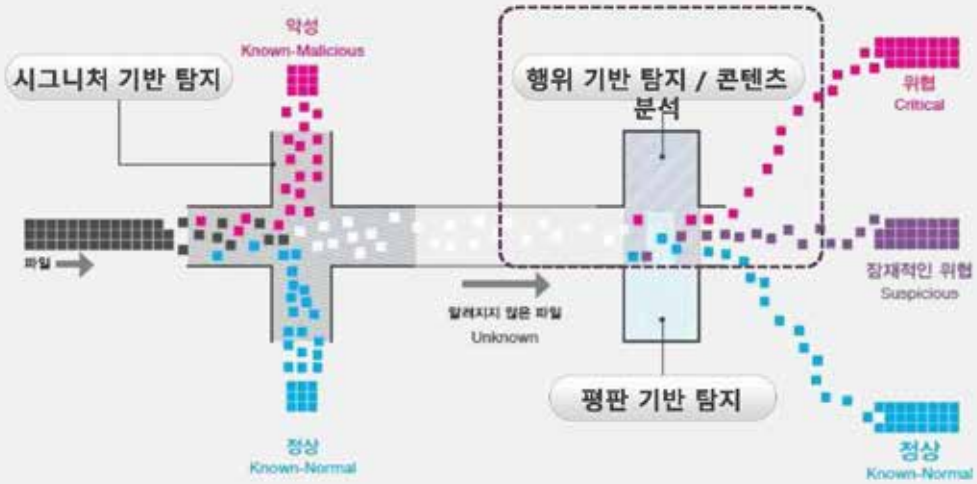
솔루션 / 로그 유형		수집시간정보	로그인 아웃시간	접속계정정보	출발지IP	출발지PORT	목적지IP	목적지PORT	출발지/목적지국가	VPNIP	MAC	Protocol	TTL	송수신량	접근승인 상태	공격자정보	공격유형	공격정보(payload)	탐지기간	탐지대상	탐지방법	탐지결과	위험도	유해웹트루여부	패치정보	접속장비정보	운영체제정보	유무선정보	그룹정보	도메인정보	호스트정보	명령어정보	발생이벤트정보	프록시정보	사이트코드	웹접근상세정보	송수신메일주소	첨부파일	리소스 - CPU - Memory - Process - Disk 무결성 - process - Port - File	Session Wtmp Utmp History Secure Messag App log	시스템 호출 System Call로
솔루션별 수	Anti-DDos	o			o	o	o	o				o	o	o	o		o	o	o			o	o	o					o											
	FW	o			o	o	o	o				o		o	o				o													o									
	VPN	o		o	o	o	o	o		o		o		o	o				o																						
	웹방화벽	o		o	o		o	o	o			o			o		o	o	o			o	o	o								o	o	o	o					
	DB보안	o	o	o	o	o	o	o				o			o									o		o				o	o									
	시스템 접근제어	o	o		o	o	o	o				o			o															o	o									
위협탐지	IPS	o		o	o	o			o		o	o	o	o	o	o	o	o	o		o	o	o	o																
	SIEM	o	o	o	o	o	o	o	o			o				o		o	o		o	o	o	o		o	o		o	o	o						o		o	
	TMS	o			o	o			o			o		o	o	o	o	o	o	o	o	o	o	o		o														
PC보안 (사용자)	유해사이트 차단	o			o	o	o	o				o							o	o	o	o	o	o								o			o					
	APT대응시스템	o			o	o	o	o	o		o	o		o		o	o	o		o	o	o	o								o				o	o	일부		
	스팸메일	o			o				o						o																				o	o				
	VMS(백신)	o															o			o	o	o	o	o																
	NAC	o			o										o		o		o	o		o	o	o						o			o							
	DRM/DLP	o			o	o											o		o			o	o	o																
	PMS	o				o					o								o						o		o	o												
인프라장비	IP관리 솔루션	o		o	o						o														o	o		o												
	DNS 보안	o			o	o									o														o						o					
	웹로젝 서버	o	o	o	o	o	o	o			o	o		o	o											o			o	o	o				o		o		o	△
Hardware-Assisted Integrity		o	o	o	o	o	o	o	△		o	o	△	o	o	△		△	o	o	o	o	o		o	o	o	△	o	o	o	o			o		o		o	o

기존 솔루션과는 새로운 솔루션 / 시스템 호출(System Call) 데이터를 이용해 분석하는 End Point Solution / 서버의 이상행위를 분석하는 새로운 방법 제시

06 AI 행위 분석 탐지

SOTERIA CYBER SECURITY

- 기존 룰 (시그니처)기반 탐지 방식 만으로는 알려지지 않은 최신 공격(Zero-day attack 등) 이나 우회 공격에 대응이 어려움
- 기존 룰 기반 탐지 방식에 행위 기반 탐지 방식의 상호 보완이 필요하며 데이터의 양이 급격히 증가하는 추세를 고려할 때 빅데이터 처리에 효율적인 AI 방식의 행위 분석 기법이 필요함

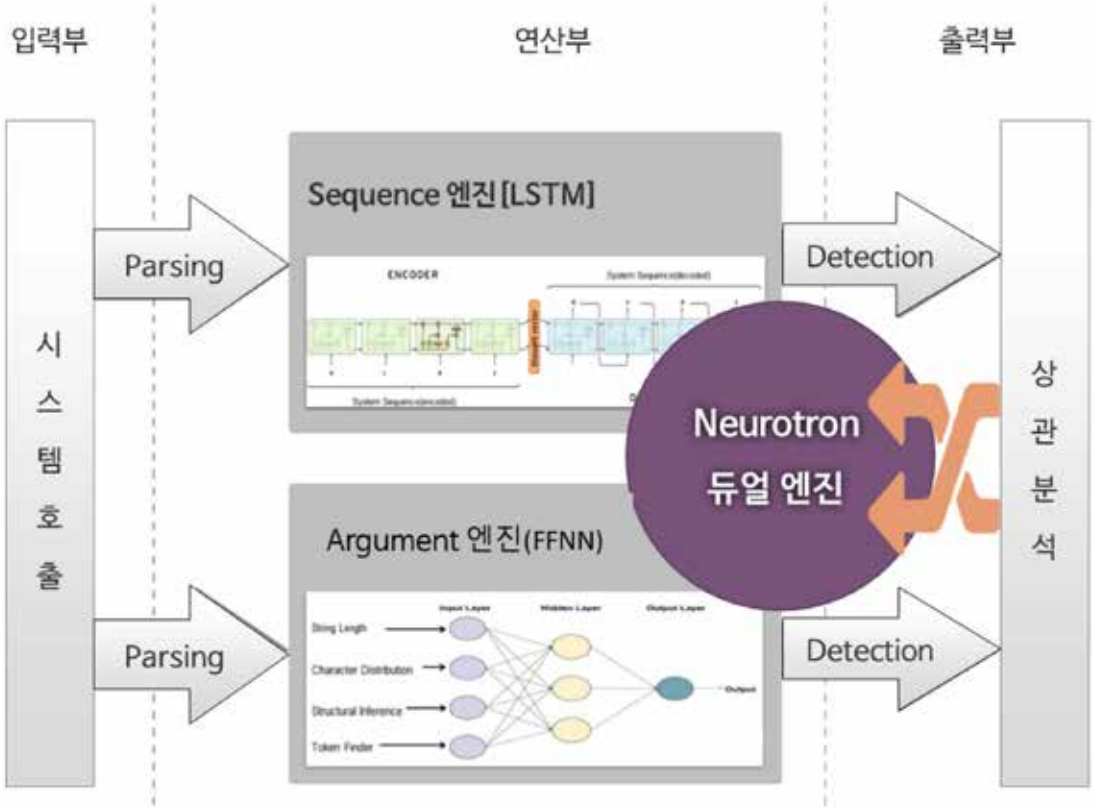


"99.999%는 0%와 같다."
없어진 0.0001%의
정보가 해커를 추적하는 핵심 단서이다.

07 AI 인공지능

SOTERIA CYBER SECURITY

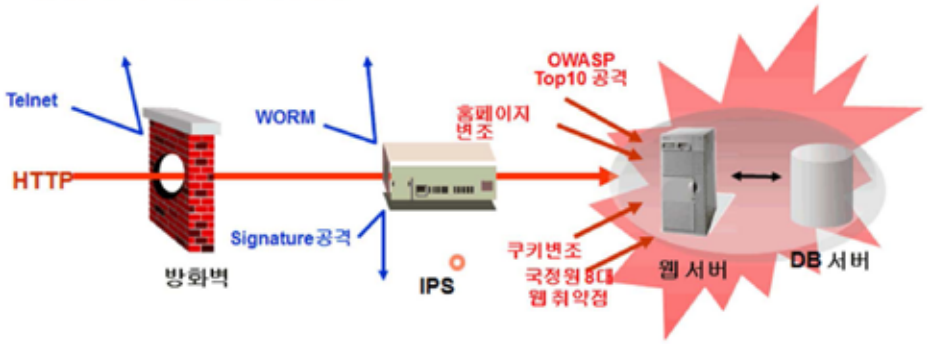
- "Neurotron" 듀얼 엔진 - 시계열의 비정상을 탐지하는 Sequence 엔진과 내용의 비정상을 탐지하는 Argument엔진
- 두가지 엔진의 결과물을 협응 분석
- 특허 - "시스템 호출 빅데이터 무결성 기반 인공지능을 통한 행위 분석 및 이상 징후 탐지 기술 "

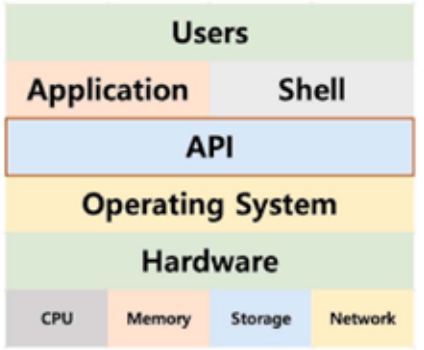


08 시스템콜을 이용한 AI 분석 방법 및 공격 시나리오

SOTERIA CYBER SECURITY

기존 보안 시스템의 한계





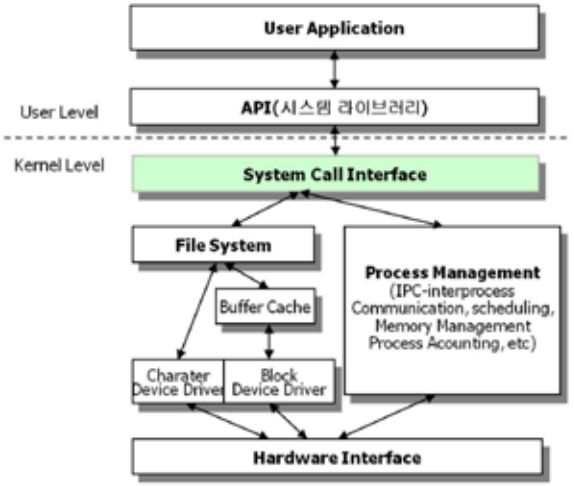
1.OpenSMTPD 6.6.2 - Remote Code Execution

2.Sudo 1.8.25p - 'pwfeedback' Buffer Overflow

3.Linux Kernel 4.10 < 5.1.17 – 'PTRACE_TRACEME' pkexec Local Privilege Escalation

4.Webmin <=1.920 - Remote Code Execution

5.phpFileManager 0.9.8 - Remote Code Execution



09 딥러닝을 이용한 현장 시험

SOTERIA CYBER SECURITY

✓ 적용 알고리즘 : Chebyshev inequality equation, ICD Deduction Process, Markov model and Bayesian theorem, Restricted Boltzmann Machine(RBM), Token Finder, FFNN, LSTM

System Call Unsupervised Learning

학습 환경

WISESTONE

순서	시험 내용
36	순서 14, 35의 결과를 확인하여 인공지능 탐지 기능을 확인한다. ○ 인공지능 탐지 = Σ(회피성 공격 시 탐지된 횟수) / 측정 횟수 × 100 = 10 / 10 × 100 = 100 % ○ Functional correctness = 1 - A / B = 1 - 0 / 10 = 1 - 0 = 1 - A = Number of functions that are incorrect - B = Number of functions considered
시험 결과	인공지능 탐지 = 100 %
측정 결과	Functional correctness = 1

2) 인공지능 탐지

시험 기준 및 방법	시험대상	시험환경	시험도구
시험 기준 : 인공지능 탐지 기능이 100 % 인가? 시험 방법 : 로그를 초기화하여 측정을 시작한 후 서버에 회피성을 공격하고 서버의 로그 파일에 저장된 정보를 이용하여 공격 탐지 유무를 확인한다. 시험 공격 유형별 5회 반복 수행하여 인공지능 탐지 기능이 수행되는지 확인한다. ※ 공격 유형(2종) : Excel, MariaDB	1식	폐쇄망	- 터미널

ISO/IEC 25023:2016 측정 지표		
품질 특성	품질 부특성	측정 지표
8.2 Functional suitability	8.2.2 Functional correctness	Functional correctness = 1 - A / B - A = Number of functions that are incorrect - B = Number of functions considered

KOLAS 시험성적서

Phase2 Hardware
- CPU : Multi-CPUs
- Memory : 8~32GB
- OS : Archlinux 5.0.5

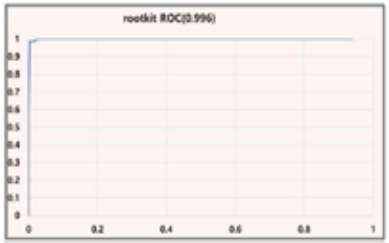
Upgrade
- CPU : Clustered
- Memory : 32~64GB
- OS : CentOS 7.5

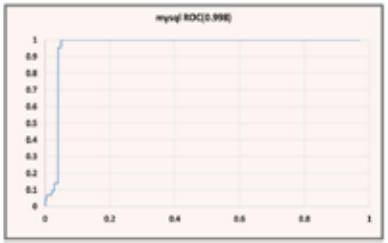
✓ 시스템콜 평균 처리시간
분당 약 86만건
(855,974 tpmC)

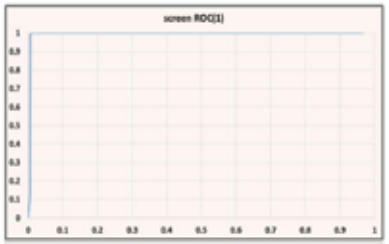
Accuracy formulation

'0' = Normal = positive data
'1' = Anomal = negative data

	Actual label (a)	Detected label (b)	Error (|a-b|)
True Positive (TP)	0	0	0
False Negative (FN)	0	1	1
False Positive (FP)	1	0	1
True Negative (TN)	1	1	0







성능 테스트결과 보고서

20

10 딥러닝을 이용한 현장 시험

SOTERIA CYBER SECURITY

- "Neurotron" 듀얼 엔진 - 시계열의 비정상을 탐지하는 Sequence 엔진과 내용의 비정상을 탐지하는 Argument엔진
- 두 가지 엔진의 결과물을 협응 분석
- 특허 출원 - "시스템 호출 빅데이터 무결성 기반 인공지능을 통한 행위 분석 및 이상 징후 탐지 기술"

KOLAS [한국시험인정기구] 시험결과 2019.08.12

횟수	결과 화면		결과
	Kernel 공격 무	Kernel 공격 유	
1			Kernel 공격 시 인공지능 탐지 기능이 수행됨을 확인

Kernel exploit탐지				
탐지 데이터	공격시작 시간	탐지결과 완료시간	탐지결과까지 걸린시간	탐지성공 여부
#3	12:41	13:24	**2분33초**	O
#4	15:27	16:18	**51초**	O
#5	18:06	19:35	**1분29초**	O

횟수	결과 화면		결과
	mariaDB 공격 무	mariaDB 공격 유	
1			mariaDB 공격 시 인공지능 탐지 기능이 수행됨을 확인

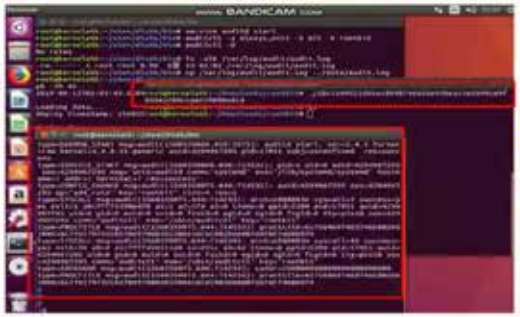
MariaDB exploit탐지				
탐지 데이터	공격시작 시간	탐지결과 완료시간	탐지결과까지 걸린시간	탐지성공 여부
#3	48:48	51:21	**2분33초**	O
#4	54:36	56:30	**1분54초**	O
#5	00:02	19:35	**2분14초**	O

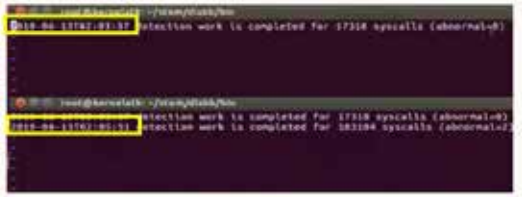
11 딥러닝을 이용한 현장 시험

SOTERIA CYBER SECURITY

Rootkit 공격 탐지

detected



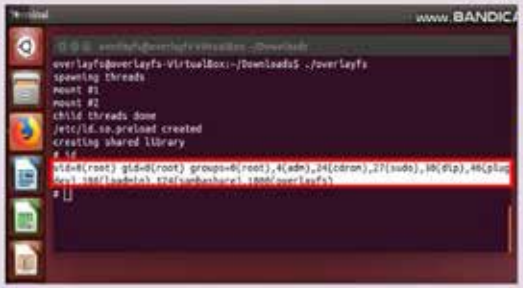


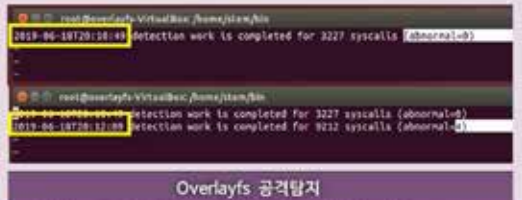
Root kit 탐지

탐지 데이터	공격시작 시간	탐지결과 완료시간	탐지결과까지 걸린 시간	탐지성공 여부
System call Sequence	3:37	5:51	2분14초	O

Overlay File system 공격 탐지

detected



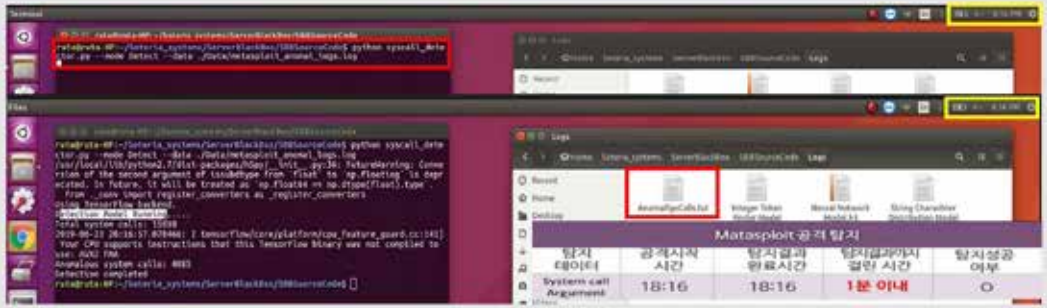


Overlayfs 공격탐지

탐지 데이터	공격시작 시간	탐지결과 완료시간	탐지결과까지 걸린 시간	탐지성공 여부
System call Sequence	10:49	12:09	1분20초	O

Metasploit 공격 탐지

detected

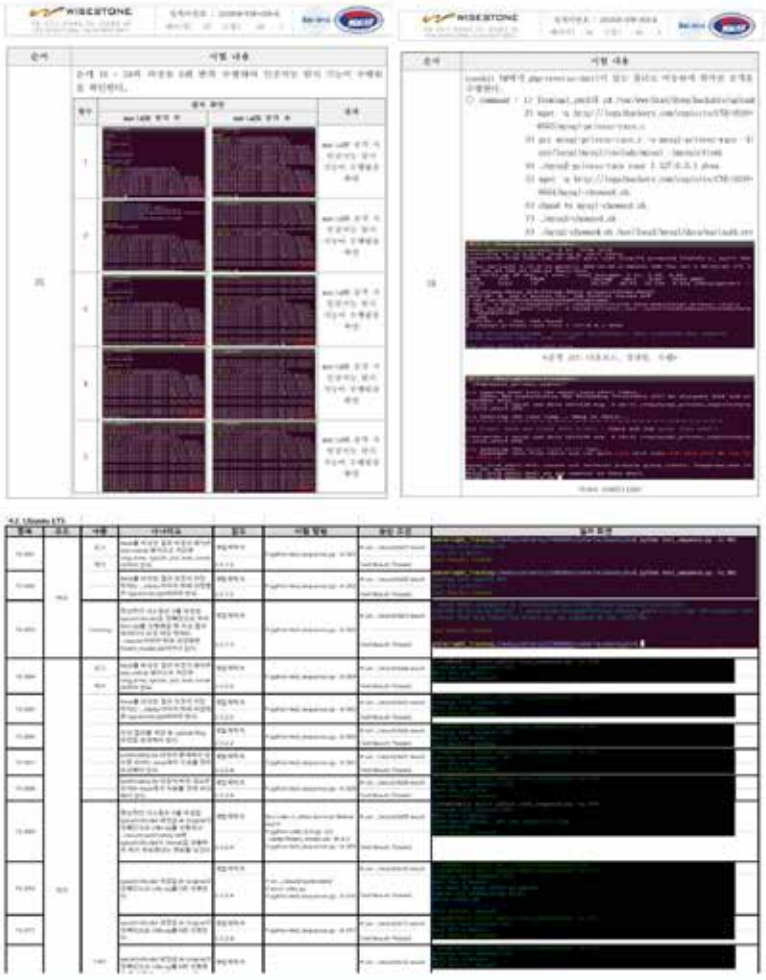


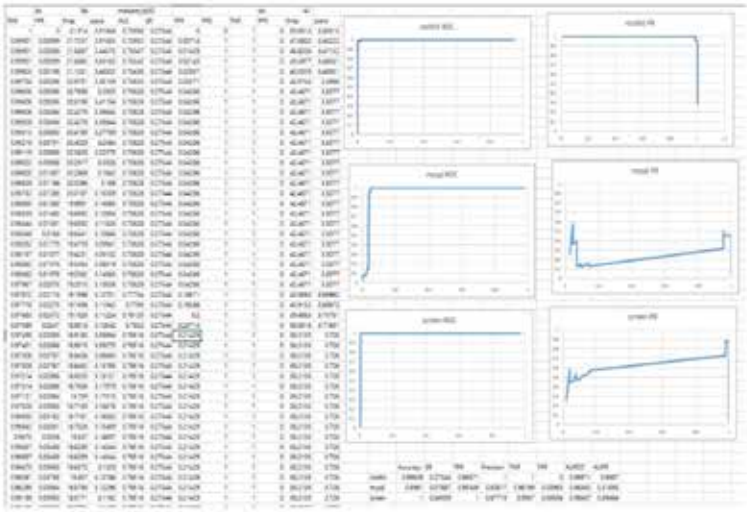
Metasploit 공격 탐지

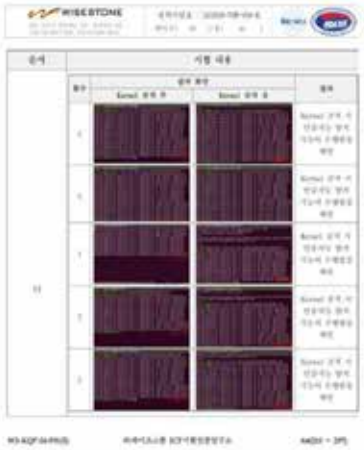
탐지 데이터	공격시작 시간	탐지결과 완료시간	탐지결과까지 걸린 시간	탐지성공 여부
System call Argument	18:16	18:16	1분 이내	O

12 딥러닝을 이용한 현장 시험

SOTERIA
CYBER SECURITY







13 딥러닝을 이용한 현장 시험 | 탐지 시간

SOTERIA CYBER SECURITY

상용 IPS 제품군과의 탐지 성능 비교 결과 최대 5분 이내 100% 탐지의 우수한 결과를 보임

KOLAS 결과와 상용IPS제품군의 NSS에서 진행한 탐지 성능 비교표

Detection Time Scoring

Time to Detect	Product A	Cisco	Product B	Product C	Product D	Product E	Product F	Product G	Product H	Neurotron Kernel	Neurotron Mysql
⟨3min	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%	100.00%	75.00%
⟨5min	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%		
⟨10min	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%		
⟨30min	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%		
⟨60min	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%		
⟨120min	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%	100.00%	100.00%
⟨240min	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%		
⟨480min	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%		
⟨720min	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%		
⟨1080min	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%		
⟨1440min	99.40%	100.00%	96.80%	99.40%	99.90%	100.00%	98.90%	90.10%	99.80%		
Overall Detection Score	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.90%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**		

= > 90
= 80~89%
= 60~79%
= 40~59%
= < 40%

- 상용 IPS 제품군과의 탐지 성능 비교 결과 최대 5분 이내 100% 탐지의 우수한 결과를 보임
- NSS Labs, Inc. is recognized globally as the most trusted source for independent, fact based cybersecurity guidance.

Chapter

3.

결론 및 기대 효과

SOTERIA
CYBER SECURITY

01 딥러닝 신산업

SOTERIA CYBER SECURITY

딥러닝 분야의 새로운 시장

자율주행 EDR
자율주행차 신규 제조업체 등장 예상
자율 주행 데이터 블랙박스 접목 필요

Smart Factory AI
IoT / Smart Factory Dependability(신인성),
생산 데이터 보호, AI기반의 맞춤형 제조

인텔리전트 메디컬 케어
바이탈과 유전자정보 활용 건강관리
의료진 대상 지적 서포트 서비스 등장

인텔리전트 인프라
전력, 수도, 가스 등의 AI기반 자동 조절다리
및 발전소 등 공공인프라 이상 감지

AI기반 스마트 농업
작업 자동화 및 드론을 이용한 정밀 농업
AI기반 기상예측 및 농업보험 등장

비즈니스 업무 환경 변화
서류관리 및 데이터 분석 AI기반 자동화
비전문성 업무인 번역, 법률 AI도입

NEW
DEEP LEARNING
MARKET

인텔리전트 시큐리티
빅데이터 분석에 따른 범죄 예측/예방
사람 행동 분석으로 이상 행동 사전 감지

맞춤형 스마트 교육
학생 개별에 맞는 교육 콘텐츠 제공
AI기반 대학 커리큘럼 지원

자율형 안전보장 로봇
재해 지역에서 구조 활동
극한 환경 등에서 자율적 행동

인텔리전트 커머스
점포에서 얼굴 인식으로 자동 추천 서비스
구매 데이터 분석으로 맞춤형 광고 제공

AI기반 핀테크
주식, 투자상품의 로보어드바이저
이상 금융거래 정보 분석 / 탐지 (FDS)

자율유통
자율화물배송, 무인화물선, 드론, 자율배달
물류 창고 내 AI로봇 이용

02 딥러닝 신산업 | IoT/Smart Factory

SOTERIA CYBER SECURITY

최근 **성장하고 있는 산업 자동화 솔루션들이** 등장함에 따라 스마트팩토리 시장에서도 **보안이슈**가 대두되고 있음

국내외로 빠르게 성장하고 있는 스마트팩토리 마켓

스마트 팩토리 개념도

글로벌 스마트 팩토리 시장규모

지역별 스마트 팩토리 시장규모

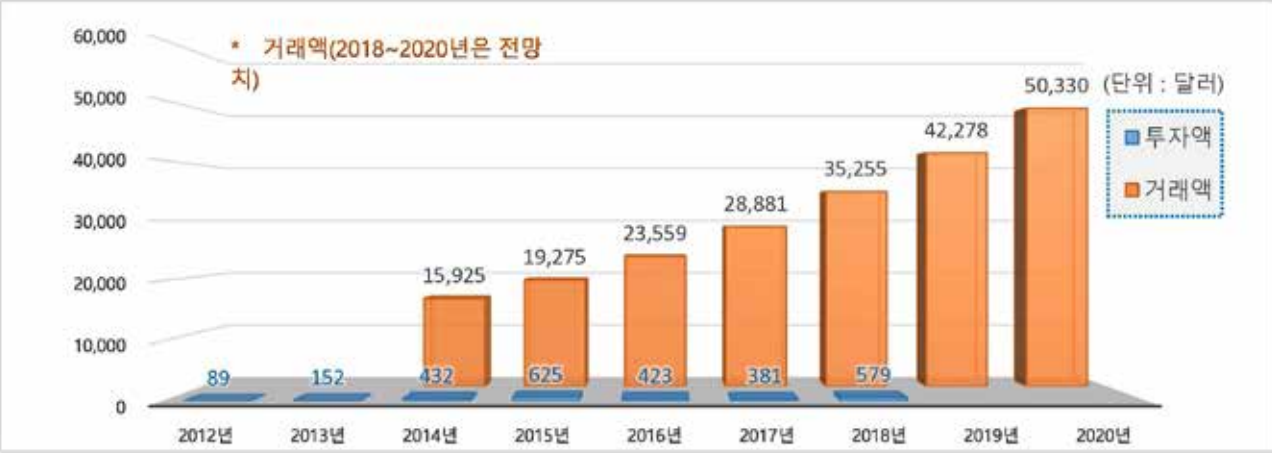
최근의 산업 제어 시스템 공격사례

연도	구 분	대 상	침해내용
2009	국방	프랑스 해군	지상의 항공기에 대한 비행계획 다운로드 불가
2010	원자력	이란 원자력 시설	Stuxnet 감염으로 인해 농축시설 내 약 50개의 원심 분리기 파괴
2011	석유	Exxon, BP, Shell등	SCADA 시스템에 대한 운영 자료를 수집하여 유출
2012	석유	이란 석유 시설	Malware가 이란 국영 석유회사의 중요 자료를 빼낸 후 삭제
2012	석유	사우디 아람코	악성코드 감염으로 인한 네트워크 마비로 석유 생산에 차질 발생
2014	전력	한국 에너지 기업 다수	한전과 한국수력원자력 외 기타 에너지 기업의 중요 자료 유출
2014	원자력	일본 원자력 발전소	악성코드 감염으로 인한 직원 정보 유출
2014	생산설비	독일 제철소	제어시스템의 파괴로 인한 용광로의 제어 및 정상적인 Shutdown 불가로 큰 피해발생
2015	사회기반시설	한국 교통시설	항만, VTS,지하철, 대중 교통 등 관련 시설에 대한 공격 발생
2015	전력	우크라이나 전력시설	Industroyer 감염으로 인해 전력 Grid내 상당수 데이터가 삭제되고 성능 저하를 유발하여 22만5천 이상의 가구에 전력이 차단
2016	수처리	미국 수처리 회사	PLC 조작을 통해 수처리 관련 화학 물질의 양을 조작하고 2백50만명 이상의 고객 지불정보 유출
2016	원자력	독일 원자력 발전소	악성코드가 바이에른에 위치한 원자력 발전소의 연료 적재 시스템을 조작하여 발전소 중단
2017	사회기반시설	미국 미주리주 도서관	미주리주내 모든 도서관 컴퓨터가 랜섬웨어에 감염되어 정지됨에 따라 정상 서비스 불가
2017	사회기반시설	미국 달러스 비상사이렌	무선통신망의 해킹으로 인한 달러스의 비상사이렌이 15시간 동안 가동

- 해커의 악의적 공격에 의해 일부 설비만 오작동 하게 되더라도 공장 전체의 안전과 제품 품질에 큰 피해를 입게됨
- 또 잘못된 오작동으로 인명과 재산에 큰 피해가 발 생 할 수도 있음

SOTERIA CYBER SECURITY

글로벌 핀테크 시장 현황



● IT 기술을 이용한 글로벌 핀테크 시장은

● 자사의 Neurotron AI 엔진을 통한 핀테크 산업의 은행,증권, 보험 등 금융거래의 이상 거래를 기존의 비즈니스 룰로 탐지하는 단순한 방식에서 빅데이터 분석을 통한 행위 분석을 통한 정교한 탐지하여 AI를 이용한 금융/핀테크 산업으로 파급/발전 시킬 예정임

04 딥러닝 신산업 | 자율주행

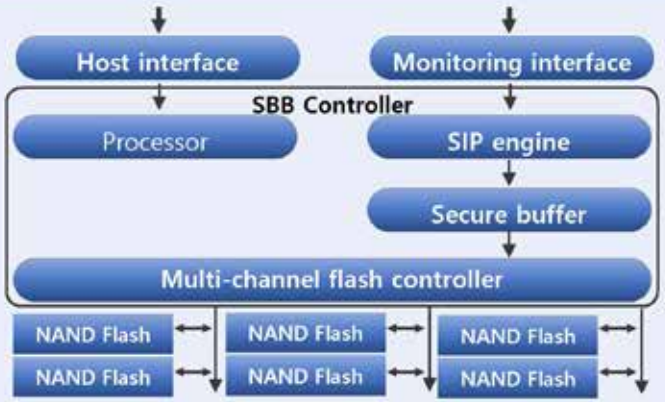
SOTERIA CYBER SECURITY

초기단계(2014)	현 재	Near Future	Soteria SBB-UV
• 속도 • 브레이크 • 에어백상태, 동작 • 안전벨트	초기단계(2014) + • 타이어 압력 • 카메라 레이더 • 운전자 프로파일 • 좌석위치 세팅 • 위치정보	현재 + •자동차 내부상황 • 이동거리/이동위치 • 도로 상황 / 차도 상태 • 신호등, 탑승인원 정보 • 주위 사물 / 불빛	Near Future + • ESS(Energy Storage System) • Computer Vision, 컨트롤, 커널 • 실행이력 • 통신이력 • 포렌식 빅테이터 • 고신뢰성 분산저장 • 시스템 무결성 • PUF Cryptography • 위변조방지/ 손실방지 • 행위 분석 탐지 • 통합보안



* 독립된 전용 하드웨어를 이용한 차량 제어용 컴퓨터(Server)에 대한 독립적이고 안전한 감시, 기록, 비정상적 상황 분석 및 모니터링, 탐지가 필요

1단계 : 기존 SBB와 유사한 형태(SSD 구조와 유사)




- 기존 SBB기술 + SBB-UV만을 위한 기술 개발
  - SBB-FTL 설계 : SBB-UV를 위한 전용 경량화된 FTL 및 파일시스템
  - 차량제어용 컴퓨터 시스템과 연동할 수 있는 HW/SW 인터페이스 및 SIP (Security-exe In Place)모듈 설계
  - High Dependable Tera-Scale SCM : 물리적/전자기적 파손 / 훼손 방지를 위한 제품설계
  - scalable Fault-tolerance Distributed Append-only-Storage for Unmanned Vehicle
  - Server BlackBox™

* 소테리아 SBB (Server BlackBox™) 기술을 자율주행 자동차영역으로 (SBB-Unmanned Vehicle) 확장하여, eUFS (embedded Universal Flash Storage) 기술과 Soteria 의 포렌식, 데이터/시스템 무결성, Hybrid Hardware Security (Challenge-Response Pair) 기술들을 이용하여, SIP (Security-exe In-Place) 기술로 진화 파

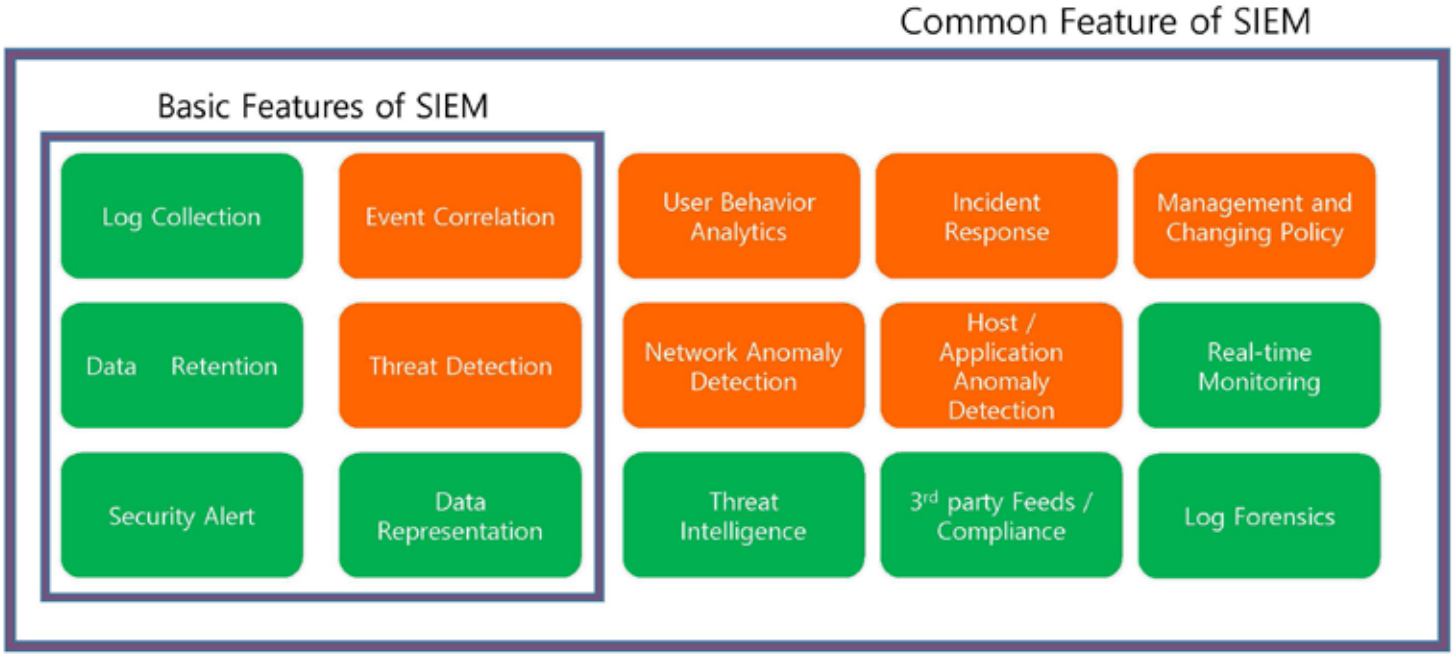

Q&A
SOTERIA
CYBER SECURITY

APPENDIX

SOTERIA
CYBER SECURITY

A1 Key Features of SIEM

SOTERIA CYBER SECURITY



AI 적용이 필요한 분야

- Log Collection : 보안 장비로부터 로그 수집
- Data Retention : 수집된 데이터 관리 및 저장 검색
- Event Correlation : 수집된 로그 및 이벤트의 연관성 분석
- Threat Detection : 침해 위협 탐지
- Data Representation : 데이터 시각화 및 SOC 제공
- User Behavior Analytics : 사용자 행위 분석
- Network Anomaly Detection : 네트워크 비정상 행위 탐지
- Incident Response : 침해 위협 사고 대응
- Host/Application Detection : 호스트/응용(멜웨어) 탐지
- Threat Intelligence : 침해 위협 관리 및 정보 구축
- 3rd party Feeds / Compliance : 3rd party 시스템 연동 및 보고서 제공
- Management and Changing Policy : 분석 정책 관리 및 업데이트
- Real-time Monitoring : 실시간 데이터 모니터링 및 통계화
- Log Forensics : 침해 위협 사고에 대한 로그 및 데이터 포렌직

A2 소테리아 하드웨어 디자인 히스토리

SOTERIA CYBER SECURITY

a. 물리적 전자기적 파손 및 훼손 방지 설계
b. 장비 집적도 향상 으로 공간 효율성 달성
c. FPGA 및 SIP (Security.exe in Place) Engine 개발로 다양한 IoT/ Mobile 적용 가능 제작