



EDR을 통한 제로 트러스트 아키텍처

2019. 12. 11

1. 보안 전략의 변화

Zero Trust Architecture

어떤 것도 신뢰할 수 있는 것은 없다.

1. 보안 전략의 변화

Zero Trust Architecture

검증된 것 이외에는
어떤 것도 신뢰할 수 있는 것은 없다.

2. 신뢰에 대한 고찰

검증

검증된 것만 신뢰할 수 있으며,

- 비즈니스의 효용성을 위해서는 모두 동일한 레벨의 검증 절차와 시간이 소요 되서는 안된다.

A type.

- 방문 기자

업무 목적 : 인터넷 업로드 및 메시지를 적기 위한 Tablet 이용 및 PC 이용

B type.

- 정 직원

인터넷 단말 : 외부 자료 송수신용 단말 : 망연계 솔루션 접근

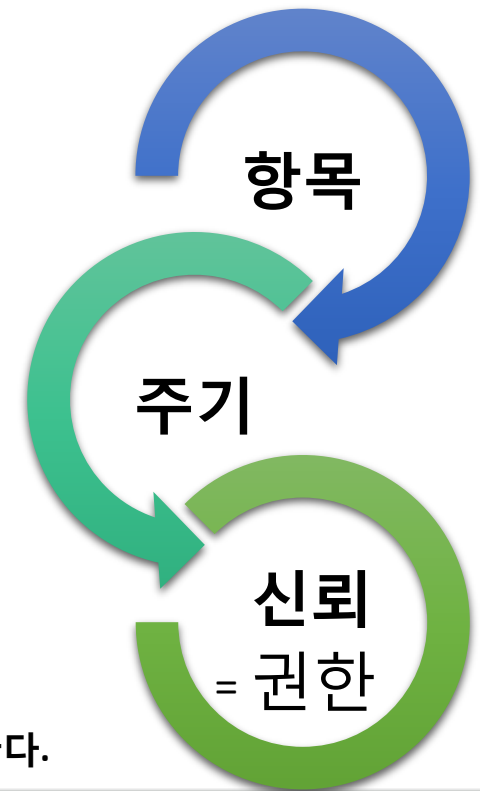
인트라넷 단말 : 업무 자료 작성 및 내부 기간망 시스템 접근

C type.

- 개인정보 관리자 및 회계 업무 관리자

인트라넷 단말 : 업무 자료 작성 및 기간 시스템 접근

신뢰성이 확보된 단말은 사용 목적에 맞는 적절한 권한 할당 및 관리가 이루어져야 한다.



2. 신뢰에 대한 고찰

검증의 사례

조직내부에 많이 볼 수 있는 검증 사례 및 이슈

검증 사례 1.

단말 실 사용자에게 대한 검증
[비-인가자 통제]



- 대다수의 고객사 내부 정직원은 최소 한번 이상의 인증을 거쳐 단말을 사용함.
- 대다수의 고객사는 인증 받은 이력에 대해 솔루션을 통해 기록하고 있으며, 감사로그에 대해 제출이 가능함.
- 본점을 제외한 지점 및 공용 PC에 대한 인증체계는 개인 단말보다 점검이 미흡함.

검증 사례 2.

필수 소프트웨어 설치 유무에 대한 검증
[필수 소프트웨어 통제]



- 대다수의 고객사 내부 정직원 대상으로 필수 소프트웨어의 현황에 대해 관리함
- 대다수의 고객사는 예외 처리시에 그에 대해 사유 및 요청자에 대한 기록을 표하고 있음
- 프로젝트 및 미러구성을 통해 식별하는 솔루션의 경우 누락되는 단말들이 존재함.

검증 사례 3.

이상 행위에 대한 검증
[단말 행위 분석]



- 일부 고객사 내부 인트라넷 단말 위주로 단말 내부 행위에 대한 정보 수집하고 있음
- 대다수의 고객사는 네트워크 기반으로 사용자 위협 행위를 분석하고 있음
- APT와 같은 보안 위협에 대하여, 네트워크 및 OS 로그를 기반으로 분석하고 있음.

2. 신뢰에 대한 고찰

단말에 대한 검증

주기적 검증 요소

단말 사용자 인증



실시간 검증

단말 접근 파일 레지스트리

* 관련 소프트웨어

* 관련 소프트웨어

IT AM
Asset Management

NAC
Network Access Control

MS AD
Active Directory

DLP
Data Loss Prevention

EDR
EndPoint Detection & Response

EndPoint Forensics

3. 주기적 단말의 검증

주기적 검증 항목의 결과물

IP의 실명제 (ID가시성 제공)

NTAG SS	동작	IP주소	MAC주소	인증사용자	최근 사용자인증	호스트명(이름)	플랫폼	접속포트	SSID	동작상태차트
172.29.30.109	🟢	172.29.30.109	00:E0:4C:36:06:99	황	2019-11-26 08:34:49	DESKTOP-9KISQBM	Microsoft Windows 10 Home x64		Sentry#AP	
172.29.20.214	🟢	172.29.20.214	00:E0:4A:69:C4:A0	홍	2019-11-25 08:14:47	HJU-SPECTRE13	Microsoft Windows 10 Home x64	GigabitEthernet10/24	Sentry#AP	
172.29.20.115	🟢	172.29.20.115	E0:D5:5E:A5:D2:CA	홍	2019-11-25 08:01:48	DESKTOP-HIMHED	Microsoft Windows 10 Professional			
172.29.30.112	🟢	172.29.30.112	E0:D5:5E:86:9A:0C	홍	2019-11-25 08:57:47	DESKTOP-CQTMQJ	Microsoft Windows 10 Professional			
172.29.30.133	🟢	172.29.30.133	00:E0:4C:A1:63:AE	한	2019-11-25 07:37:40	hkhhan	Microsoft Windows 10 Home x64			
172.29.60.41	🟡	172.29.60.41	A8:2B:B9:7C:5A:30	한	2019-11-26 11:41:00	Galaxy-Note9	Samsung Galaxy Note 9 Professional			
172.29.25.66	🟡	172.29.25.66	A8:2B:B9:7C:5A:30	한	2019-11-26 11:41:00	Galaxy-Note9	Samsung Galaxy Note 9 Professional			
172.29.25.153	🟢	172.29.25.153	EC:2C:E2:7A:83:4C	하	2019-11-28 10:34:36	playdesignui-imac.local	Apple macOS			
172.29.30.63	🟢	172.29.30.63	38:F9:D3:03:5F:16	하	2019-11-25 14:39:24	playdesignui-imac.local	Apple macOS			
172.29.20.91	🟢	172.29.20.91	88:36:6C:F5:7E:34	최	2019-11-25 12:47:38	LAPTOP-5AT4N4JL	Microsoft Windows 10 Home x64			

시간 #	로그ID	관리장비명	IP	MAC	사용자ID	사용자명	부서명	설명
2019-11-29 08:17:27	IP사용시작	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = UP	
2019-11-28 18:45:22	AGENT사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 에이전트 동작상태 변경됨. STATUS = DOWN	
2019-11-28 18:37:31	IP사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = DOWN	
2019-11-28 18:03:14	IP사용시작	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = UP	
2019-11-28 12:38:32	AGENT사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 에이전트 동작상태 변경됨. STATUS = DOWN	
2019-11-28 12:30:43	IP사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = DOWN	
2019-11-28 08:36:13	IP사용시작	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = UP	
2019-11-26 18:13:32	AGENT사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 에이전트 동작상태 변경됨. STATUS = DOWN	
2019-11-26 18:05:28	IP사용종료	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = DOWN	
2019-11-26 16:38:49	IP사용시작	172.29.20.4	172.29.20.214	00:E0:4A:69:C4:A0	h	홍	EDR기 노드 동작상태 변경됨. STATUS = UP	

[감사로그]

- 단말의 IP/하드웨어 주소에 대한 ID 매핑

단말 주기적 보안 상태 현황 관리

IP주소	MAC주소	에이전트미설치자단	DESKTOP-BPCHKFO	시간 #	로그ID	관리장비명	IP	MAC	사용자ID	사용자명	부서명	설명	추가정보
172.29.111.144	24:F5:AA:D9:84:BA	에이전트미설치자단	DESKTOP-BPCHKFO	2019-11-27 14:41:07	정책	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88	h	김	Endpoin 1팀	노드정책 할당됨. OLD=?기본정책. NEW =?기본연구소 정책. BY=?사용자 로그인	
172.29.114.74	00:E0:4C:69:01:11	에이전트미설치자단	Junsuk-NOTEBOOK	2019-11-27 14:41:07	인증	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88	h	김	김	노드의 사용자가 인증됨. ID=?kuaanr, NA ME=?김태형, BY=?CWP	
172.29.116.244	00:E0:4C:69:01:11	에이전트미설치자단	Junsuk-NOTEBOOK	2019-11-27 14:40:23	노드정보	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				노드 검색AP 감지됨. SSID=Sentry#AP, BSSID=00:0E:8E:3F:0C:C7	
172.29.116.100	48:BA:4E:51:B8:C1	에이전트미설치자단	DESKTOP-7G5RCRQ	2019-11-27 14:39:58	정책	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				제어정책 변경됨. OLD=?Unknown, NEW =?에이전트미설치자단. BY=?신규노드동 용	
172.29.25.230	D4:25:8B:DB:4D:88	에이전트미설치자단	LAPTOP-IB43R95I	2019-11-27 14:39:58	노드정보	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				노드타입 변경됨. OLD=?미분류, NEW=?PC. BY=?DHCP Server Scan	
				2019-11-27 14:39:58	시스템정보	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				플랫폼 감지됨. PLATFORM_OLD=?, PLA TFORM_NEW=?Microsoft Windows, FLID _OLD=0, FLID_NEW=?15925, BY=?DHCP Server Scan	
				2019-11-27 14:39:58	노드관리	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				새로운 노드 등록됨. BY=?SENSOR	
				2019-11-27 14:39:58	DHCP	172.29.25.4	172.29.25.230	D4:25:8B:DB:4D:88				DHCP IP 할당됨. HOSTNAME=LAPTOP- IB43R95I	
				2019-11-27 14:39:49	노드정보	172.29.53.150		D4:25:8B:DB:4D:88				노드 검색AP 감지됨. SSID=Sentry#AP, BSSID=00:0E:8E:3F:0C:C7	
				2019-11-27 14:38:54	인증			D4:25:8B:DB:4D:88	h	ku		사용자인증 실패. ERRMSG=? (LOCALDB)	

- 조직내부의 필수 소프트웨어 및 패치 상태값 식별 및 미 - 설치 단말에 대한 조치 (예제)

[감사로그]

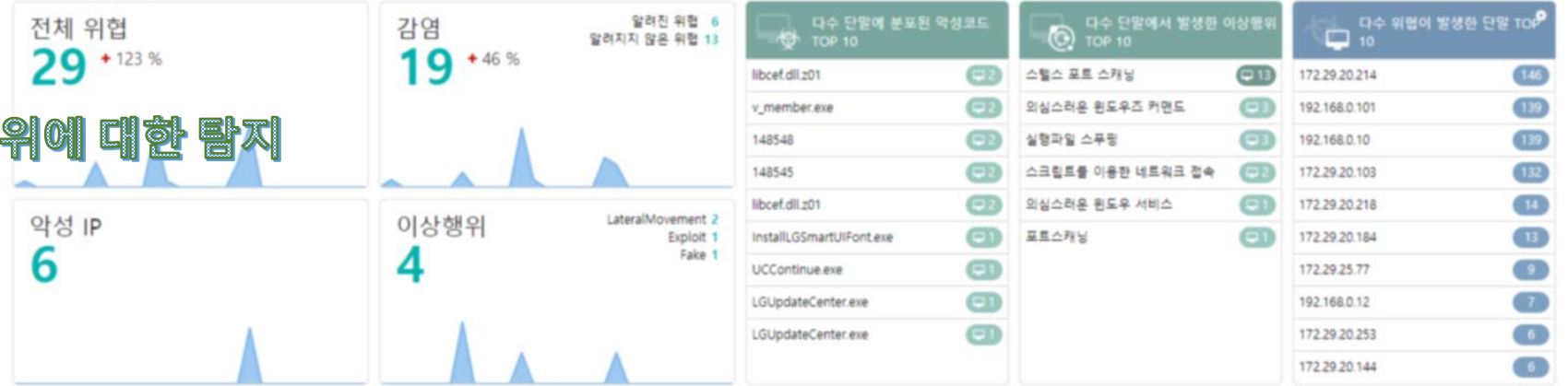
4. 실시간성 단말 검증

실시간성 검증 항목의 결과물

1. 단말 내부의 모든 행위에 대한 기록



2. 위협 행위에 대한 탐지

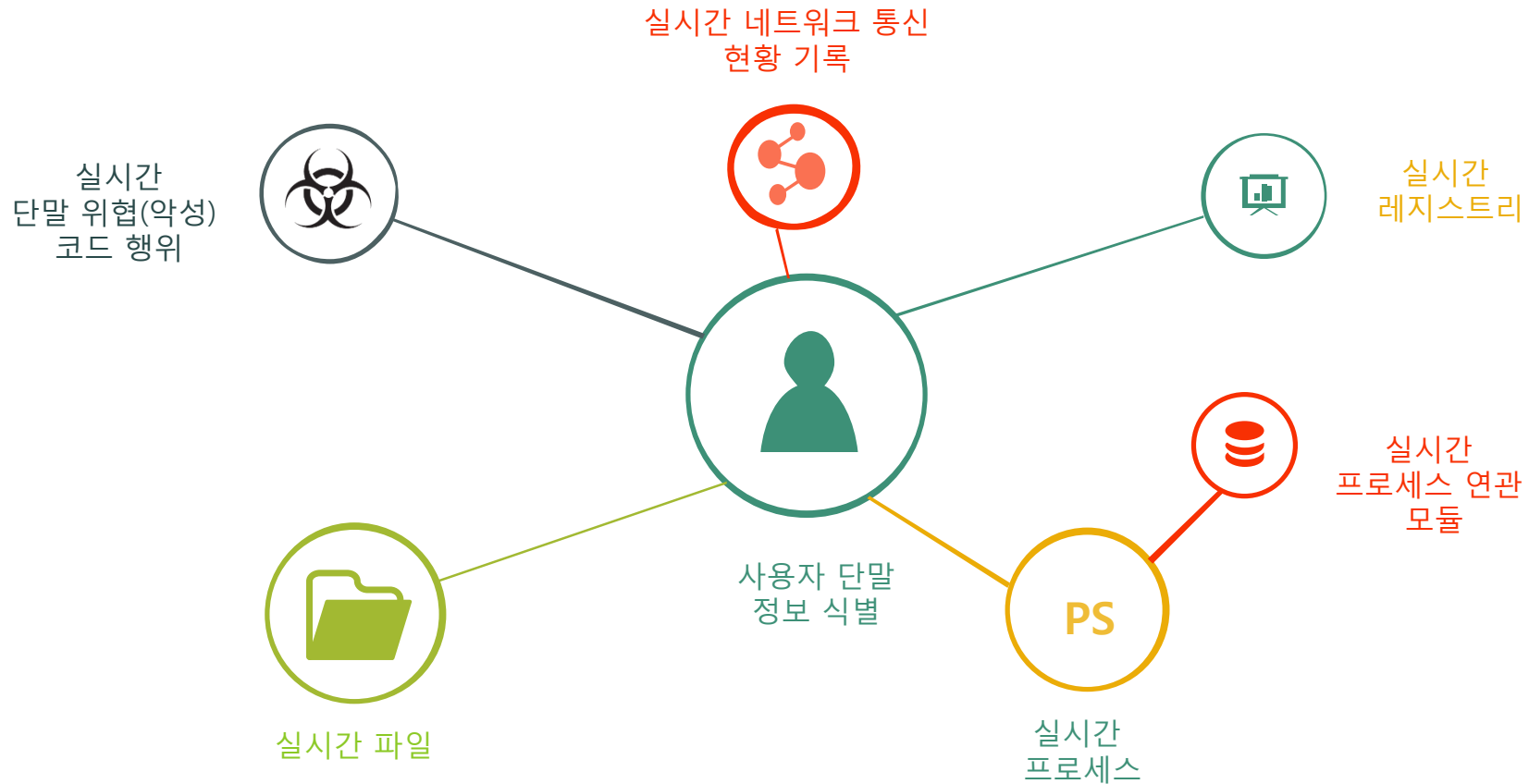


3. 위협 행위 발생에 대한 대응



4. 실시간성 단말 검증

검증을 위한 기능



4. 실시간성 단말 검증

파일 : 상세정보, 유입/유출, 변경 정보

로그 타입	Event time 2019-11-29 10:48:39	로그 발생 시간(파일 생성 시간)
	Event type HttpDownload	로그를 발생 시킨 프로세스
해당 파일의 원본 위치	Process name IEXPLORE.EXE	
	Download URL http://appdown.naver.com/naver/ndrive/NDrive64/setup/NDriveInst.exe	다운로드 받은 파일의 위치
	Download path C:\Users\leeki\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\D3B68K3H\NDriveInst.exe	
	파일 정보	
	File name http://appdown.naver.com/naver/ndrive/NDrive64/setup/NDriveInst.exe	
- 파일 이름	MD5 dbd7ee60b8bb4ccf5182b7f3b04db49	
- MD5 해시	Size 16.9 MB	
- 크기	File type PE	
- 종류	파일 상세정보	
	Internal name NAVER Cloud Explorer	
	Product name NAVER Cloud Explorer	
	Description NAVER Cloud Explorer	
	File version 1.5.10.11	
	Company NAVER Corp.	
	Language Korean	
	CopyRight All rights reserved.	
	Architecture x86	
	ExeType EXE	
	CodeSign	
	서명여부 <input checked="" type="checkbox"/> 서명됨	
	전자서명 검증 <input checked="" type="checkbox"/> 신뢰할 수 있는 서명	
	발급자 Symantec Class 3 Extended Validation Code Signing CA - G2	
	주체 NAVER Corp.	
	서명날짜 2019-06-26 15:58:44	
	지문 82830036FEE670ACF24778DBAD6083329EA081	

- 파일 속성 정보**
- 내부 이름
 - 제품 이름
 - 버전
 - 제조사
 - 언어
 - 코드사인 정보
 - 서명 여부
 - 전자서명 검증
 - 발급자
 - 주체
 - 서명 날짜
 - 지문(해시)

4. 실시간성 단말 검증

파일 : 상세정보, 유입/유출, 변경 정보

이벤트 시각	탐지	이벤트	프로세스명	통신	파일명
2019-12-01 15:48:27		FileMove	Explorer.EXE		putty-b.exe
2019-12-01 15:48:24		FileMove	Explorer.EXE		putty-a.exe
2019-12-01 15:48:20		FileMove	Explorer.EXE		putty.exe

파일명 변경
파일명 변경

Event time 2019-12-01 15:48:24
 Event type FileMove
 Process name Explorer.EXE
 Source file C:\Users\forest\Documents\WTEST\putty-a.exe
 Target file C:\Users\forest\Documents\WTEST\putty-b.exe

파일 정보

File name putty-a.exe
 MD5 33c9d1e56152e212367e9c5b01671e45
 Size 512.0 KB
 File type PE

파일 상세정보

Internal name PuTTY
 Product name PuTTY suite
 Description SSH, Telnet and Rlogin client
 File version Release 0.66
 Company Simon Tatham
 Language English
 CopyRight Copyright © 1997-2015 Simon Tatham.
 Architecture x86
 ExeType EXE
 CodeSign

파일명 변경

파일 속성 정보

- 내부 이름
- 제품 이름
- 버전
- 제조사
- 언어
- 코드사인 정보

파일 변경 전후의 어떤 일이 발생되었는가?
"단말 내부 이벤트 뷰"

4. 실시간성 단말 검증

실시간 네트워크 접속 정보

2019-12-01 16:22:16	NetworkConnect	chrome.exe	172.217.20.42:443	OUT
2019-12-01 16:22:03	NetworkConnect	spoolsv.exe	172.29.20.6:3910	OUT
2019-12-01 16:21:56	TcpPortBind	SYSTEM	172.29.71.110:139	Listening
2019-12-01 16:21:53	NetworkConnect	GnPCInspector.exe	172.29.90.33:443	OUT

세션 정보

Open Port

172.29.71.110:139

네트워크 연결 정보

- Event time: 2019-12-01 16:21:56 (Connecting)
- Event type: TcpPortBind
- Process name: SYSTEM
- Protocol: TCP
- Connection: Listening 172.29.71.110:139 (성공)
- Tag: NetBIOS

COM-PC \ 172.29.20.90

services.exe parent process

1 NaverAdminAPISvc.exe process

2 network event listening

59 network event outgoing

211.216.46.20:80

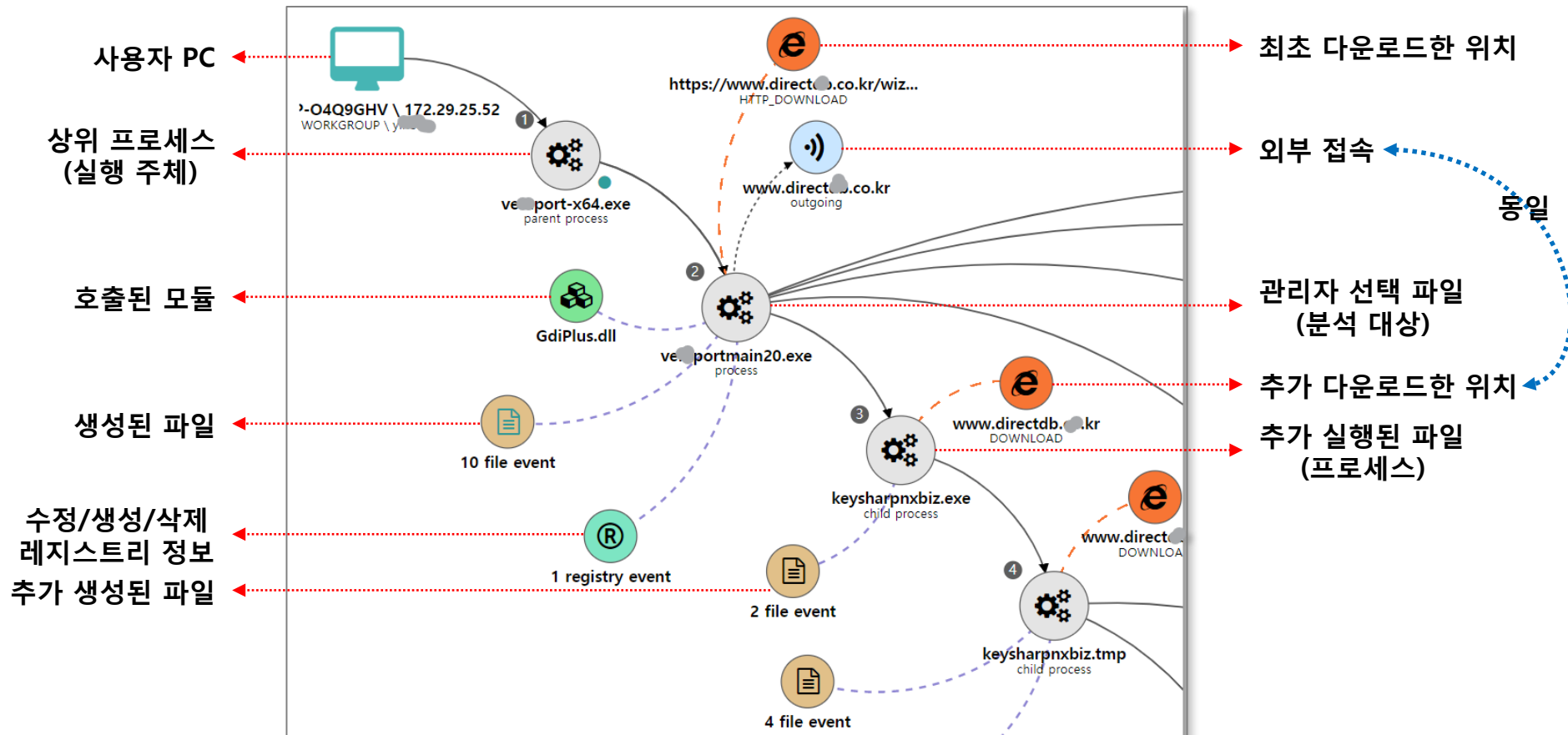
네트워크 연결 정보

- Event time: 2019-11-29 18:05:29 ~ 2019-11-29 18:07:29 (1분 동안 발생함)
- Events time: 2019-11-29 18:05:29 ~ 2019-11-29 18:27:29 (22분 동안 발생함)
- Event type: NetworkConnect
- Process name: NaverAdminAPISvc.exe
- DNS name: appdown.naver.com
- Protocol: TCP
- Direction: OUT
- Connection: 성공

통신이 왜 발생되었는지?
"단말 내부 이벤트 뷰"

4. 실시간성 단말 검증

파일, 프로세스, 모듈, 네트워크 정보



4. 실시간성 단말 검증

단말 위협 탐지

신규	신뢰도	탐지 시각	탐지 분류	탐지 세부분류	내용	위협 관정	상태	사용자 IP	사용자명	대응	역선
26	95 %	2019-11-12 13:02:05	XBA	Fake	ALZip.exe 에 의한 실행파일 스푸핑 이상...	신규	신규	172.29.20.253	Super A...		위협 분석
처리중	MLHigh	2019-11-08 08:31:39	Malware	ML	(46A1E49C-E719-4DFF-B954-9DEF6FE7...	신규	신규	172.29.20.64	이		위협 분석
3	8 %	2019-11-08 08:14:19	Malware	IOC	installer.exe 파일이 IOC에 의해 알려진 ...	처리중	처리중	192.168.0.16	이		위협 분석
해결됨	30 %	2019-11-07 12:43:05	XBA	LateralMove...	svchost.exe 에 의한 스텔스 포트 스캐닝 ...	처리중	처리중	172.29.30.107	이		위협 분석
0	30 %	2019-11-07 09:44:49	XBA	LateralMove...	SYSTEM 에 의한 스텔스 포트 스캐닝 이상...	처리중	처리중	172.29.25.77	신		위협 분석
전체	50 %	2019-11-01 18:13:47	Malware	IOC	SetupImgBurn_2.5.8.0.exe 파일이 IOC에...	신규	신규	172.29.20.38	이	발법	위협 분석

위협 요약

탐지 지표 **XBA** - SYSTEM 에 의한 스텔스 포트 스캐닝 이상행위가 진단됨 (30%)

탐지 엔진 **XBA / LateralMovement**

수행 프로세스 **SYSTEM**

이벤트 **network**

태그 **first_seen**

요약 내용 **스텔스 포트 스캐닝 (StealthPortScanning)**

포트 스캐닝은 타겟 PC를 공격하기 전에 정보를 수집하는 고전적인 방법이다. 따라서 포트스캐닝을 탐지하는 것은 Lateral Movement를 탐지하는 중요한 포인트가 된다. nmap 등 일부 포트 스캔 프로그램에서는 탐지를 회피하기 위해 실제로 커넥션을 맺지 않고 포트가 열려있는지 탐지하는 기능을 제공하는데 이러한 기능을 '스텔스 포트 스캐닝'이라고 부른다.

진단사유: 445/TCP, 135/TCP, 139/TCP 등 주요한 포트에 접속하는 INBOUND TCP 커넥션 중에서 SYN, SYN/ACK까지는 진행되었으나, 마지막 ACK가 수신되지 않은 경우 진단

MITRE ATT&CK **T1046 - Network Service Scanning**

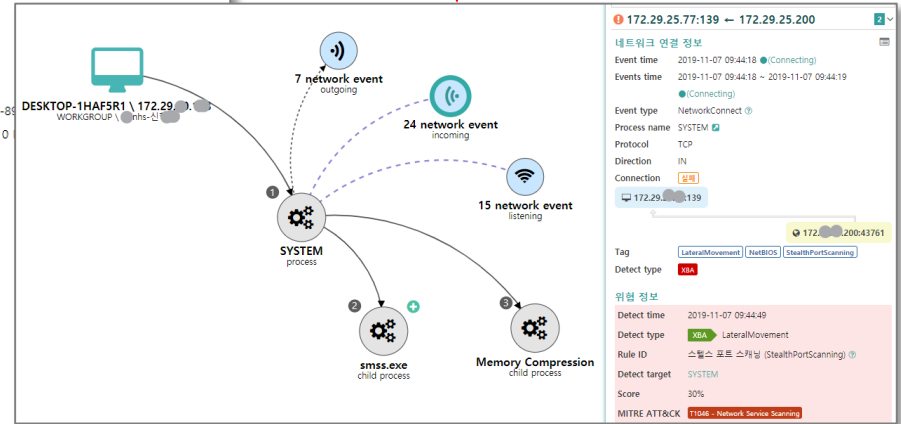
처리 상태 **처리중**

탐지 시각

최초 탐지시각 2019-11-07 09:44:49

최종 탐지시각 2019-11-07 09:44:49

이벤트 조회



4. 실시간성 단말 검증

수집 자료 활용 : 자료(Data) 에서 정보(Information) 제공

The screenshots display the following information:

- Download File Summary:**
 - Total Downloads: 10
 - Average Download Size: 1006.4 KB
 - Smallest Download: 43.0 KB
- Download File List:**

EventTime	AuthDepth	AuthName	IP	FileName	FileSize	ProcName
2019-12-01 16:04:47:09	5	slack.exe	172.29.20.218	Genians 단말	84,188	C:\Users\Forest
2019-12-01 19:20:31:028	1	slack.exe	172.29.20.218	Genians 단말	111,360	C:\Users\Forest
2019-11-28 16:18:38:287	5	chrome.exe	192.168.105.1	알기쉬운_기어차기16.3.2019.png	21,504	C:\Users\Forest
2019-11-27 16:38:29:596	5	slack.exe	172.29.20.218	Genians 단말	28,864	C:\Users\Forest
2019-11-27 19:55:56:961	5	slack.exe	172.29.20.218	Genians 단말	27,776	C:\Users\Forest
2019-11-27 19:55:56:976	5	slack.exe	172.29.20.218	Genians 단말	38,848	C:\Users\Forest
2019-11-27 19:20:38:287	5	slack.exe	172.29.20.218	Genians 단말	54,528	C:\Users\Forest
- Upload File Summary:**
 - Total Uploads: 22
 - Average Upload Size: 2.2 MB
 - Smallest Upload: 7.4 KB
 - Largest Upload: 6.9 MB
- Upload File List:**

EventTime	AuthDepth	AuthName	IP	FileName	FileSize	ProcName
2019-12-01 18:27:50:118	5	slack.exe	172.29.20.218	Genians 17일	3,735,987	slack.exe
2019-12-01 18:27:01:181	5	slack.exe	172.29.20.218	Genians 17일	7,931,956	slack.exe
2019-12-01 16:00:16:589	5	slack.exe	172.29.20.218	Genians 단말	893,394	slack.exe
2019-11-27 18:30:18:407	5	Genian Insight, 탐방팀	172.29.20.218	Genian Insight, 탐방팀	3,385,618	slack.exe
2019-11-26 15:05:4:243	5	slack.exe	172.29.20.218	Genians 단말	939,854	slack.exe
2019-11-25 16:40:07:009	5	slack.exe	172.29.20.218	Genians 단말	274,893	slack.exe
2019-11-23 13:10:19:725	5	slack.exe	172.29.20.218	Genians 단말	7,217,385	slack.exe
2019-11-23 13:10:13:101	5	slack.exe	172.29.20.218	Genians 단말	2,242,249	slack.exe
- File Type Distribution:**
 - chrome.exe: 81.7%
 - slack.exe: 17.2%
 - system.exe: 0.7%
 - explorer.exe: 0.2%
 - cmd.exe: 0.1%
 - chrome.exe: 0.1%
- Upload File Summary (Detailed):**
 - Total Uploads: 11
 - Average Upload Size: 2.8 MB
 - Smallest Upload: 1.4 MB
 - Largest Upload: 2.1 MB
- Upload File List (Detailed):**

EventTime	IP	AuthID	AuthName	FileName	FileSize	FilePath	FileHash2
2019-11-25 13:12:55:531	172.29.20.218	forest	forest	2019-Genian Insight E.pdf	2,242,249	C:\Users\Forest\Documents\2019-Genian Insight E.pdf	...
2019-11-25 13:12:55:234	172.29.20.218	forest	forest	Genian Insight E.pdf	680,407	C:\Users\Forest\Documents\Genian Insight E.pdf	...

4. 실시간성 단말 검증

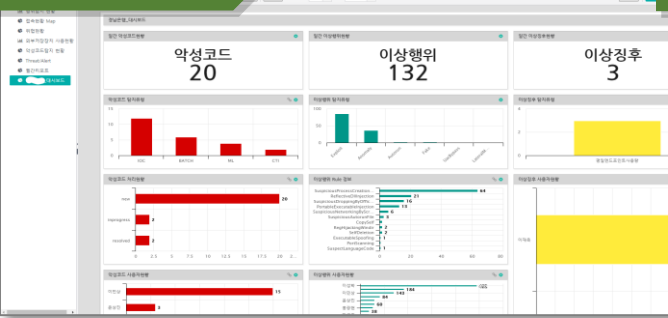
관리를 위한 기능

보고를 위한 리포트

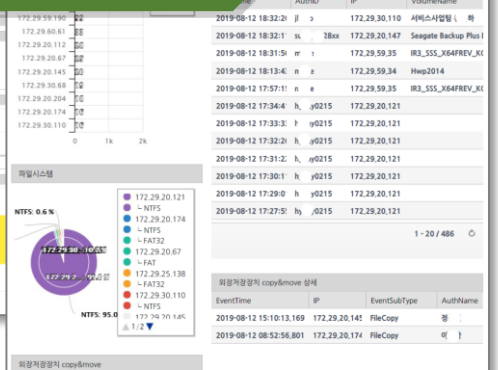
악성코드 탐지 현황



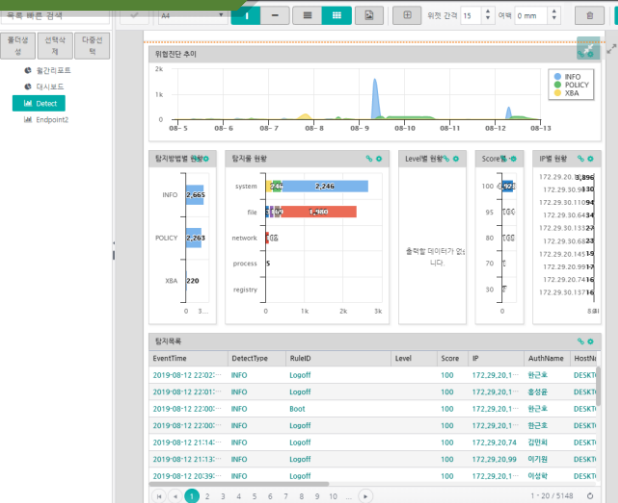
탐지 및 분석결과



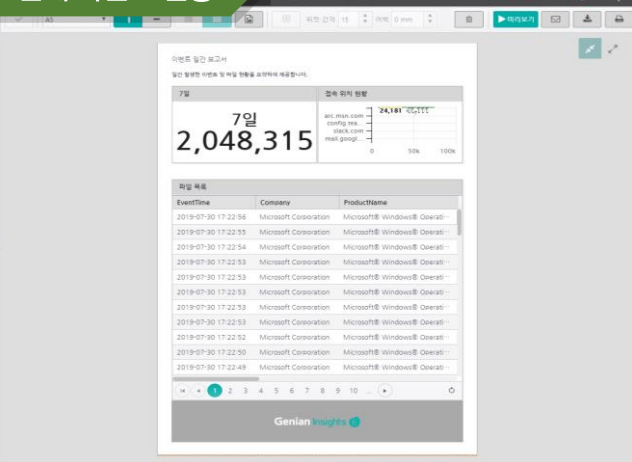
파일 유출 현황



악성코드 탐지 현황



전체 이벤트 현황



탐지 리포트



5. 검증을 통한 단말의 신뢰성 회복

검증을 통한 내부 단말의 신뢰 회복 및 보안 아키텍처 확립



자산 손실 및 유출에 대한 리스크

자산을 이용하는 사람들은 누구이며, 어떻게 접근하는가?

접근 권한 세분화

권한부여를 위한 점검사항



설정된 보안 아키텍처 옹바름에 대한 관찰

필요에 따른 업데이트 수정체계



Thank you!

스타워즈 4편 1977년 개봉
스타워즈 1편 1999년 개봉