

CounterTack Sentinel 5

Real-Time Enterprise Threat Detection, Analysis and Response

2015년

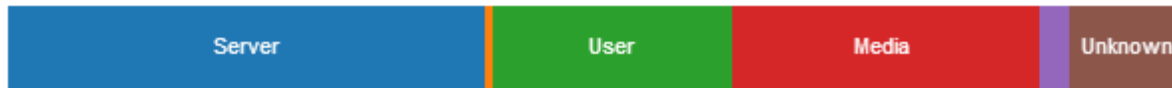
Agenda

- ❑ Endpoint 위협 탐지, 분석 및 대응 솔루션의 필요성
- ❑ Sentinel 소개
- ❑ Sentinel 의 주요 기능
- ❑ Sentinel 의 구성 요소
- ❑ Sentinel 의 특징점
- ❑ Sentinel 사용 사례
- ❑ CounterTack 소개

Endpoint 위협 탐지, 분석 및 대응 솔루션의 필요성

- 가장 취약한 정보 자산은 엔드포인트와 서버 - 공격의 기본 경로
 - 내부 시스템에서 발생하는 위협에 대한 가시성 확보가 필요함

Asset Categories



Servers



Network



User Devices



Media



69%

Source : 2013 Data Breach Investigations Report - Verizon

Endpoint 위협 탐지, 분석 및 대응 솔루션의 필요성

- 공격은 단 시간에 발생하지만, 침해 사고의 발견에는 많은 시간이 소요된다.
 - 진행 중인 공격의 빠른 탐지와 자동화된 분석이 필요함 (예: grr)

Timeline: Initial Attack to Compromise



Timeline: Compromise to Exfiltration



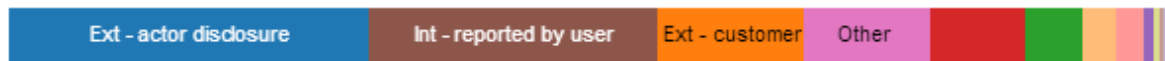
Timeline: Compromise to Discovery



Timeline: Discovery to Containment



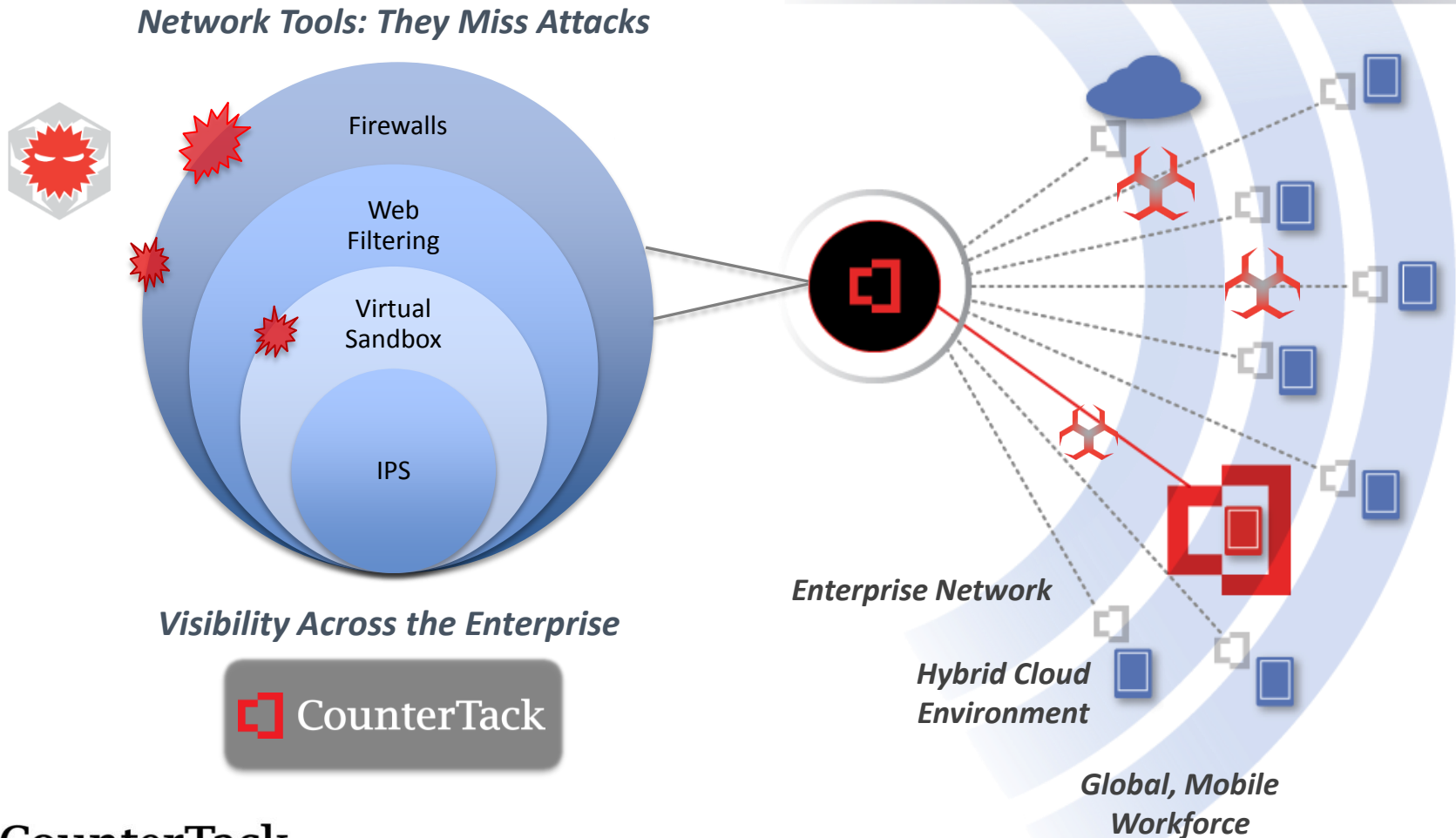
Discovery Method



Source : 2013 Data Breach Investigations Report - Verizon

타겟 공격에 대한 탐지 및 대응의 문제점

- ❑ 기업 내부 엔드포인트에 대한 가시성 확보를 통해 위협에 즉각적인 대응 필요



타겟 공격에 대한 기존 보안시스템의 한계

❑ 네트워크 Sandbox

- Sandbox 우회, 회피 기법의 발전
- 다양한 OS, Application 지원 미흡
- 암호화된 공격 시 탐지 어려움
- 악성코드 유입 후 내부 시스템 간 전이 및 확산 시 탐지 어려움
- 서비스 (Protocol)별 제품 도입 필요
- 공격 전/후 침해사고 대응/분석을 위한 데이터를 확보하기 어려움

❑ 엔드포인트 Anti-Virus

- '악성 코드 샘플 수집 → 분석 → 엔진 업데이트' 후 탐지 가능
- 변종과 customized 된 코드를 탐지하기 어려움
- 공격 과정 중 무력화 시도(실시간 감시 off)에 대한 방어책 미비
- 공격의 전 과정을 모니터링 할 수 없음
- 공격 전/후 침해사고 대응/분석을 위한 데이터를 확보하기 어려움

[Backup slide] ETDR Tools

□ 설명

- 가트너는 최근 증가하고 있는 고도화된 공격에 대해 대규모 환경에서의 침해 사고 대응과 즉각적인 포렌식에 도움을 줄 수 '엔트포인트에서의 위협에 대한 탐지와 대응' 역량 있는 솔루션의 필요성과 운영사례에 대한 보고서 발행
- ETDR Tools을 제공하는 전문 업체로 CounterTack 을 소개하고, 커널 레벨에서 실시간 데이터 수집의 장점과 대규모 환경 지원 등의 특징을 언급함

□ ETDR Tool Name Explained

Name	Function
Endpoint	Laptops, desktops server – but not the network infrastructure
Threat	All badness (threat), not just malware
Detection	Detect compromise, malware, traces of incidents
Response	Help investigators during alert triage, threat investigation and incident response

CounterTack Technology

☐ Sentinel의 주요 구성 요소 및 특징

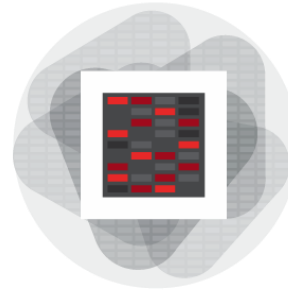
Kernel Module

- 엔드포인트 (OS) 에 설치
- 공격자는 발견할 수 없음
- Tamper-resistant, anti-evasion
- 시스템의 모든 행위 모니터링
- 실시간 데이터 수집 및 전송



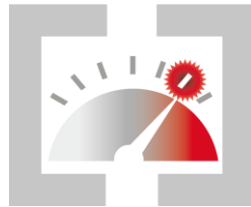
Analysis Cluster

- 검증된 Big Data 기술 적용
- 수집된 위협에 대한 자동 분석
- 행위 분석에 기반한 탐지
- 기업 내 위협의 상관관계 분석
- 증거 자료의 안전한 관리 및 보존



Management Console

- 다양한 데이터 뷰 제공
- 강력한 검색 기능 제공
- Dashboard options:
 - Intelligence
 - Endpoints
 - Behaviors
 - Search



Knowledge Library

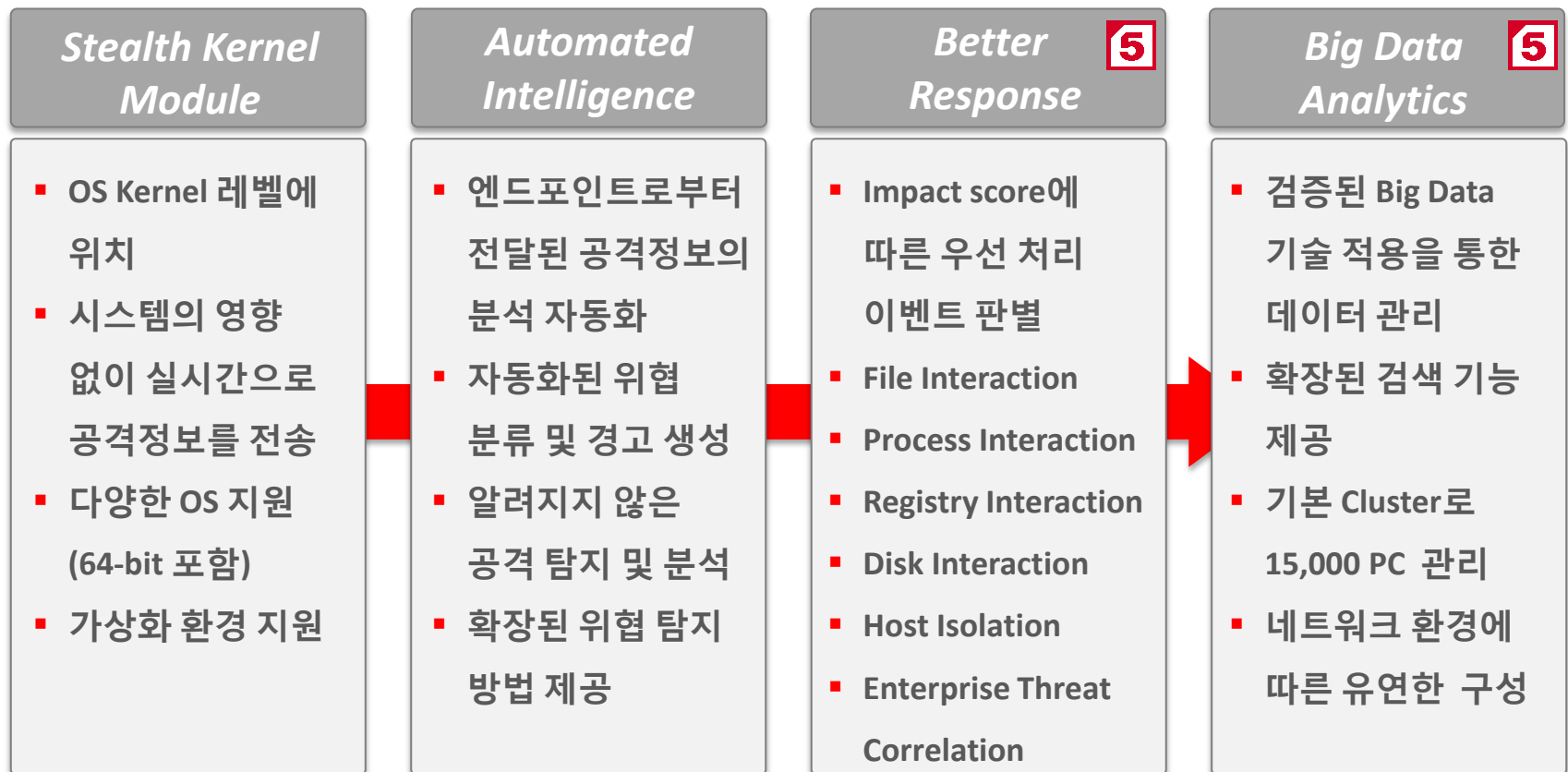
- 위협에 대한 자동 분류
- 다양한 탐지 profiles 제공
- 사용자 정의 Basic condition
- CyBOX, IOC 호환 및 지원



Sentinel 소개

□ 엔드포인트 위협 탐지, 분석 및 대응 플랫폼

- 다양한 위협에 대한 즉각적인 분석/대응과 Big Data 기술이 접목된 최신 보안솔루션



CounterTack Approach

- ❑ '탐지→ 분석→ 치료(교정)→ 예방' 의 전체 사이클에 대응할 수 있는 새로운 기능을 제공



❑ DETECT

- Stealth collection module을 통한 악성행위를 실시간으로 탐지

❑ ANALYZE

- 수집된 다양한 정보를 기반으로 위협에 대한 상세분석 및 검색 지원

❑ REMEDIATE

- 공격으로 인해 발생할 수 있는 부정적인 영향을 차단
- File, Process Interaction, Host Isolation, Disk Interaction, etc.

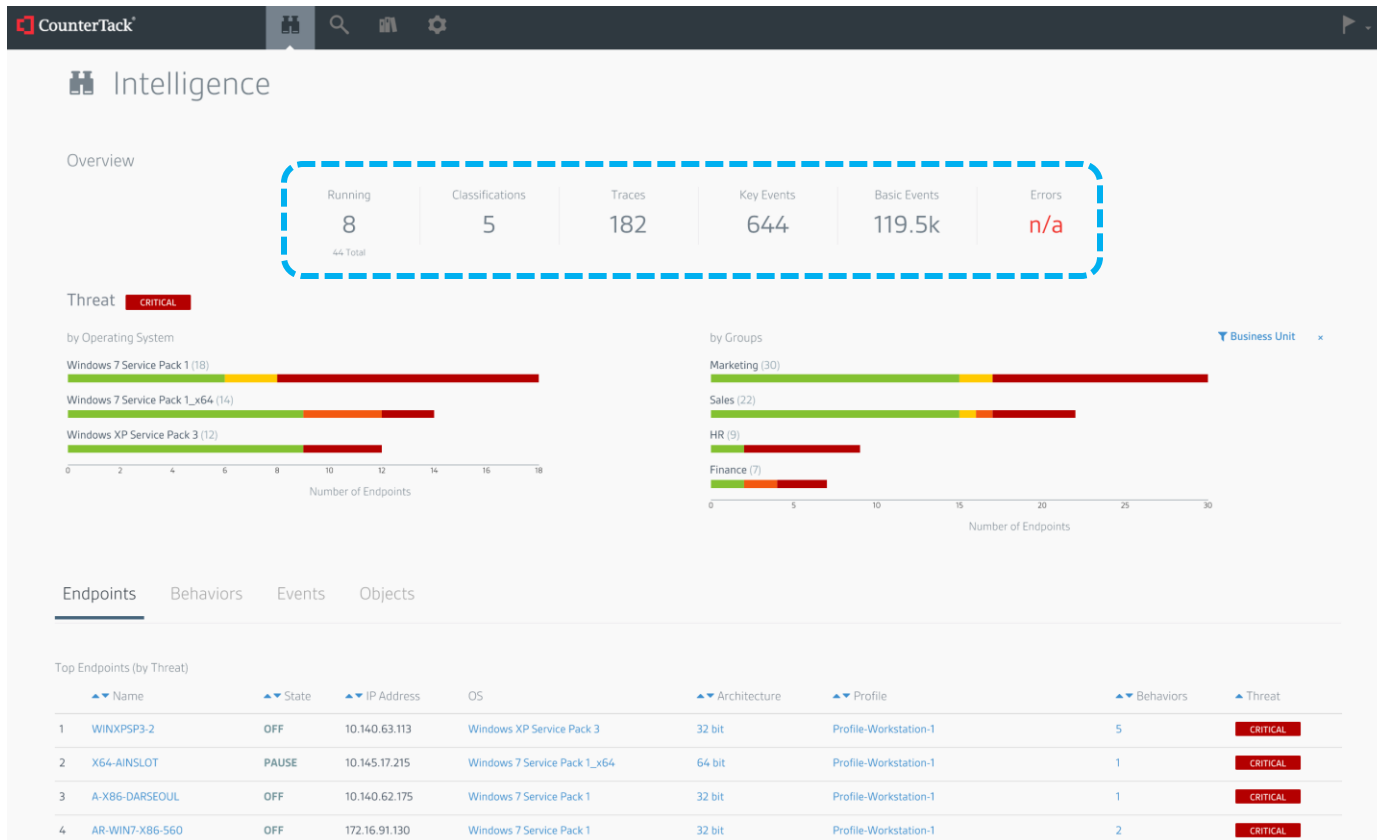
❑ RESIST

- 자동으로 생성된 Resistance profile에 의한 공격 방지 기능 제공 (예정)

Sentinel 주요 기능

Intelligence (Dashboard)

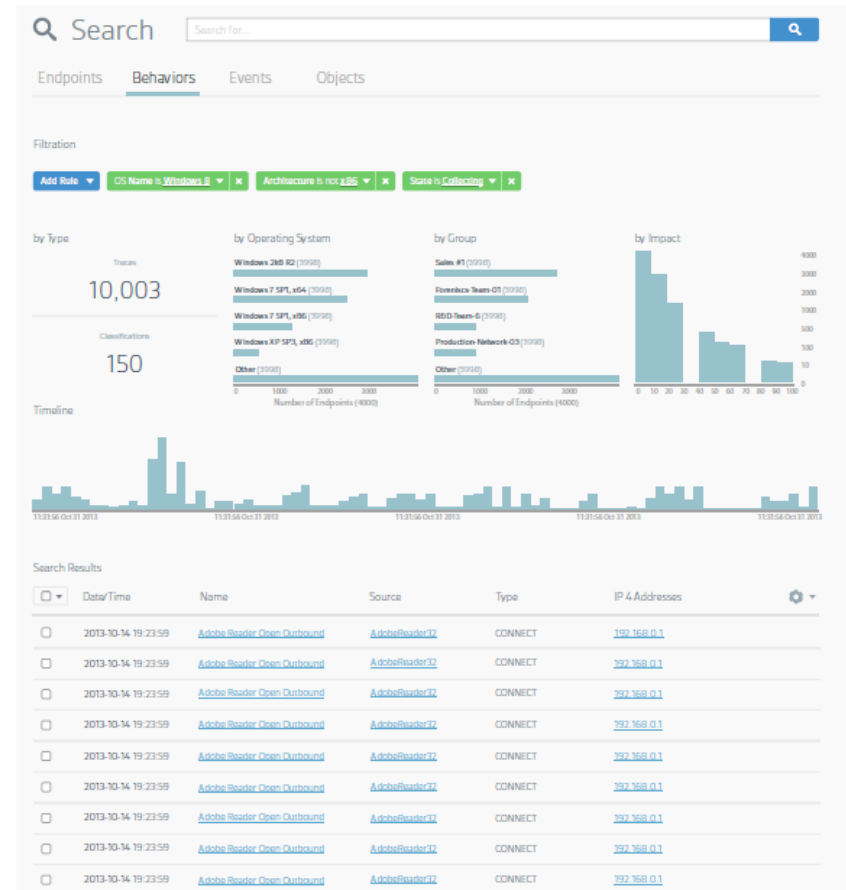
- 기업 전체의 엔드포인트에 대한 위협 레벨 및 KM 운영 현황 표시
- Classification, Key event, Trace, Basic event에 대한 실시간 통계



Sentinel 주요 기능

Search (검색)

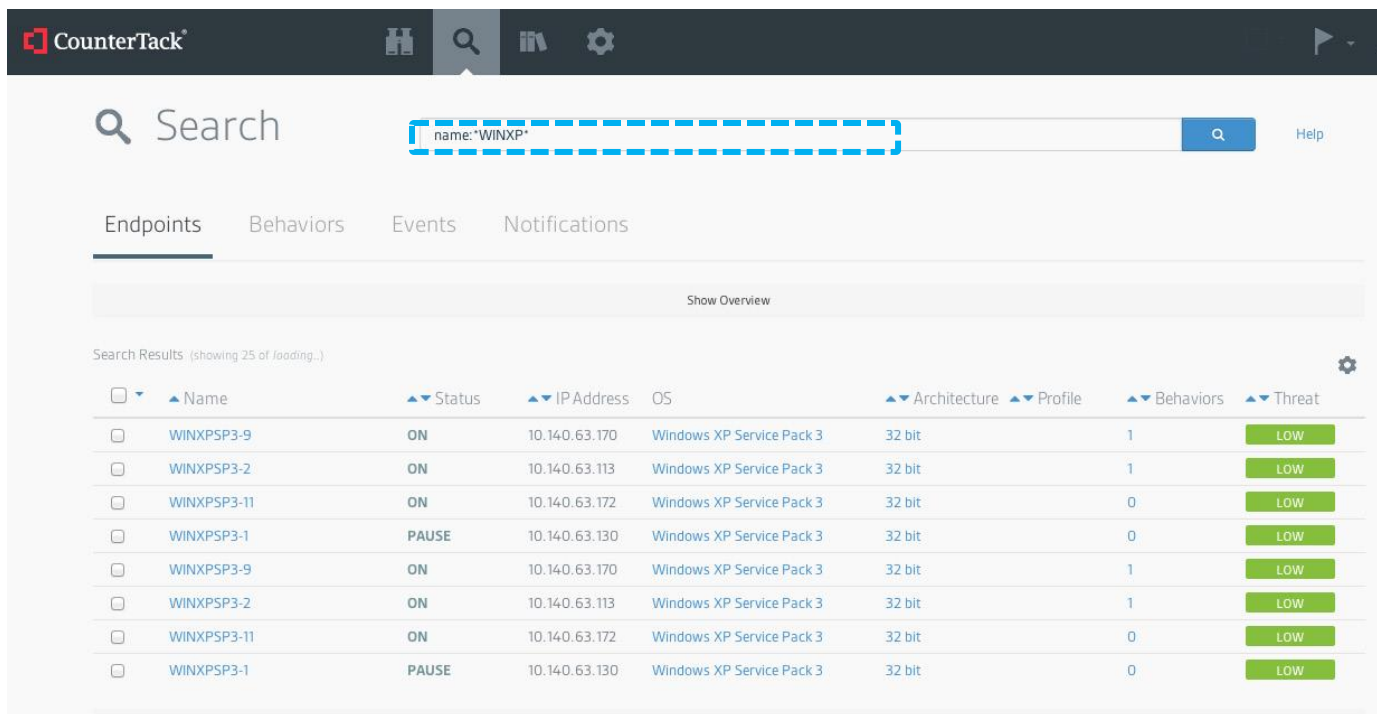
- Endpoint로 수집된 데이터를 다양한 인자를 사용할 수 있는 검색 기능 제공
- Endpoint (OS, Group), 특정 행위, 이벤트 및 Object 에 대한 검색 지원



Sentinel 주요 기능

❑ Search (계속)

- 특정 OS가 설치된 엔드포인트 검색
- Computer Name, Status, IP Address, Profile, Behaviors, Threat Level 표시



The screenshot shows the CounterTrack Sentinel interface. At the top, there is a search bar with the query "name:'WINXP'". Below the search bar, there are tabs for "Endpoints", "Behaviors", "Events", and "Notifications". The "Endpoints" tab is selected. Below the tabs, there is a "Show Overview" button. The search results are displayed in a table with the following columns: Name, Status, IP Address, OS, Architecture, Profile, Behaviors, and Threat. The results show 8 endpoints, all of which are Windows XP Service Pack 3. The threat level for all endpoints is "LOW".

Name	Status	IP Address	OS	Architecture	Profile	Behaviors	Threat
WINXPSP3-9	ON	10.140.63.170	Windows XP Service Pack 3	32 bit		1	LOW
WINXPSP3-2	ON	10.140.63.113	Windows XP Service Pack 3	32 bit		1	LOW
WINXPSP3-11	ON	10.140.63.172	Windows XP Service Pack 3	32 bit		0	LOW
WINXPSP3-1	PAUSE	10.140.63.130	Windows XP Service Pack 3	32 bit		0	LOW
WINXPSP3-9	ON	10.140.63.170	Windows XP Service Pack 3	32 bit		1	LOW
WINXPSP3-2	ON	10.140.63.113	Windows XP Service Pack 3	32 bit		1	LOW
WINXPSP3-11	ON	10.140.63.172	Windows XP Service Pack 3	32 bit		0	LOW
WINXPSP3-1	PAUSE	10.140.63.130	Windows XP Service Pack 3	32 bit		0	LOW

Sentinel 주요 기능

❑ Search (계속)

- 엔드포인트 기본 정보 표시 (OS, Patch level, Profile, IP Address, Group 등)
- 선택한 엔드포인트에서 탐지된 주요 이벤트 표시 (Trace)

The screenshot displays the CounterTack Sentinel web interface for an endpoint named WIN7X86-SYM-2. The interface includes a navigation bar with the CounterTack logo and icons for home, search, alerts, and settings. Below the navigation bar, the endpoint name is shown with a shield icon. An 'Overview' section provides a summary of endpoint metrics: 0 Classifications, 1 Traces, 0 Key Events, 188 Basic Events, and a Threat level of LOW. A detailed information section lists OS (Microsoft Windows 7 Service Pack 1), Domain, IPv4 Address (10.140.63.175), Profile (with a 'Change Profile' link), and Groups (with an 'Add Groups' link). Below this, there are tabs for Behaviors, Events, Objects, Notifications, and Info. At the bottom, two tables are visible: 'Top Classifications (by Impact)' which shows 'No data', and 'Top Traces (by Impact)' which shows one trace with the name 'Action-Condition-Process-Execution-From-Users-Folder-Win7' and an impact of 0. A 'Load More' button is located at the bottom right of the traces table.

Sentinel 주요 기능

❑ Search (계속)

- 행위 (Behaviors) 검색
- Origin condition을 통해 trigger된 행위에 대한 검색

The screenshot displays the CounterTack Search interface. At the top, there is a search bar with the placeholder text "Search behaviors...". Below the search bar, there are tabs for "Endpoints", "Behaviors", "Events", and "Notifications". The "Behaviors" tab is selected. The interface shows a summary of search results: "Traces: 313" and "Classifications: 140". Below this, there is a "Hide Overview" button. The main section is titled "Search Results" and contains a table with the following columns: "Time Started", "Description", "Type", "Endpoint", "Last Active", "Events", and "Impact". The table lists several search results, including "SCI_bootkit_common_001" and "Action-Condition-Process-Execution-From-Users-Folder-Win7". Two blue dashed boxes are drawn around the "Description" column (labeled with a circled '1') and the "Events" and "Impact" columns (labeled with a circled '2').

Time Started	Description	Type	Endpoint	Last Active	Events	Impact
02/05/14 09:19:19.838	SCI_bootkit_common_001	classification	\15-PC	02/05/14 09:19:19.838	24	100
02/05/14 09:19:19.838	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	\15-PC	02/05/14 09:19:19.838	43293	100
02/06/14 15:39:57.347	Origin - Adobe Filetype writing to Disk	trace	\15-PC	02/06/14 15:39:57.347	6810	55
02/06/14 13:43:45.588	Origin - Adobe Filetype writing to Disk	trace	t-PC	02/06/14 13:43:45.588	1084	50
02/06/14 13:01:03.920	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	t-PC	02/06/14 13:01:03.920	100	100
02/06/14 13:00:52.683	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	t-PC	02/06/14 13:00:52.683	15	15
02/05/14 15:31:57.270	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	\15-PC	02/05/14 15:31:57.270	4256	100
02/05/14 15:58:25.339	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	\15-PC	02/05/14 15:58:25.339	8639	100
02/05/14 15:29:26.750	Action-Condition-Process-Execution-From-Users-Folder-Win7	trace	\15-PC	02/05/14 15:29:26.750	10789	100

Sentinel 주요 기능

Behaviors

- 특정 행위에 발생한 엔드포인트 정보 표시
- 특정 행위에 대한 상세 분석 결과 표시 (Source / Action / Target)

The screenshot displays the CounterTack Behavior interface. The top navigation bar includes the CounterTack logo, user profile, search, and settings icons. The main header shows 'Behavior' with a search icon. Below this is an 'Overview' section with several metrics: 'Time Started (UTC)' at 13:34:54 on Feb 05, 2014; 'Last Active (UTC)' at 19:14:56 on Feb 05, 2014; 'Key Events' at 0; 'Total Events' at 54.7k; and 'Impact' at CRITICAL (Max. Impact 100). A red dashed box labeled '1' highlights the 'Classification' section, which includes: SCI_Zeus_bot_base, Endpoint YSKIM-PC, OS Microsoft Windows 7 Service Pack 1, Domain skinfosec.co.kr, IPv4 Address 0.0.0.0, 0.0.0.0, 10.1.0.217, and Status DISCONNECTED. Another red dashed box labeled '2' highlights a specific event entry: '02/05/14 14:18:01.036 YSKIM-PC S Thread svchost.exe: thread 4724'. Below this entry, a table provides detailed source and target information. The source table lists: Type thread, Name svchost.exe: thread 4724, PID 1708, Parent PID 624, Backing File \\Windows\System32\svchost.exe, Thread Time Started 02/05/14 02:17:56.280 (1391577476280689700), and Process Time Started 02/05/14 01:22:57.663 (1391574177663244500). The target table lists: Type registry, Key \\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime, Name RecentCluster, Type 3, and Data.

Source		Target	
Type	thread	Type	registry
Name	svchost.exe: thread 4724	Key	\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime
PID	1708	Name	RecentCluster
Parent PID	624	Type	3
Backing File	\\Windows\System32\svchost.exe	Data	
Thread Time Started	02/05/14 02:17:56.280 (1391577476280689700)		
Process Time Started	02/05/14 01:22:57.663 (1391574177663244500)		

Sentinel 주요 기능

Behaviors (계속)

- Processes / Files / Registries / Network
- 탐지된 행위 중 'Files (Created)'에 대한 정보 표시

The screenshot shows the CounterTack interface with the 'Files' tab selected. The 'Created' filter is active, and the table displays a list of file creation events. The 'Path' column is highlighted with a dashed blue box.

Event Time	Action	Path
02/05/14 13:46:37.722	FILE_CREATE	\\Windows\\Temp\\AUTmpV3IS80\\dnad.scd1
02/05/14 13:46:37.730	FILE_CREATE	\\Windows\\Temp\\AUTmpV3IS80\\dnac.scd1
02/05/14 13:46:41.389	FILE_CREATE	\\Windows\\Temp\\AUTmpV3IS80\\moduler.scd4
02/05/14 13:46:52.012	FILE_CREATE	\\Windows\\Temp\\TMP0000006C8186762F6600DBEE
02/05/14 13:46:52.448	FILE_CREATE	\\Windows\\Temp\\TMP0000006D187DC592E17B6778
02/05/14 13:46:52.601	FILE_CREATE	\\Windows\\Temp\\TMP0000006E9E9CF9CD6599C69F
02/05/14 13:50:53.811	FILE_CREATE	\\Windows\\Temp\\TMP0000006FC8454EEFC8124591
02/05/14 13:51:04.094	FILE_CREATE	\\Users\\yskim\\Music\\iTunes\\Temp.tmp
02/05/14 13:51:06.589	FILE_CREATE	\\Windows\\Temp\\TMP0000007047F01801552012DD
02/05/14 13:51:08.680	FILE_CREATE	\\Windows\\Temp\\TMP000000712670CD662B0F5D78
02/05/14 13:51:15.237	FILE_CREATE	\\Windows\\Temp\\TMP000000725057C17CDA0F41A8
02/05/14 13:51:19.192	FILE_CREATE	\\Windows\\Temp\\TMP0000007368FD79014CEEC4F1
02/05/14 16:46:11.395	FILE_CREATE	\\Windows\\Temp\\AUTmpV3IS80\\moduler.scd1
02/05/14 16:46:11.403	FILE_CREATE	\\Windows\\Temp\\AUTmpV3IS80\\ispe1.scd1

Sentinel 주요 기능

Behaviors (계속)

- Processes / Files / Registries / Network
- 탐지된 행위 중 'Registries (Overwritten)'에 대한 정보 표시

CounterTack

Domain: skinfosec.co.kr

IPv4 Address: 0.0.0.0, 0.0.0.0, 10.1.0.217

Status: DISCONNECTED

Events Processes **Registries** Network

1

All Created Read **Overwritten** Renamed Erased Deleted

2

Registries (by Most Active)

Event Time	Action	Key	Variable
02/05/14 14:18:01.036	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	BaseCluster
02/05/14 14:18:01.036	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	RecentCluster
02/05/14 14:18:01.037	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	CurrentCluster
02/05/14 16:18:01.065	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	BaseCluster
02/05/14 16:18:01.067	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	RecentCluster
02/05/14 16:18:01.068	REGISTRY_OVERWRITE	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance\Shell\StartStop\StartMenu\Runtime	CurrentCluster

Sentinel 주요 기능

Behaviors (계속)

- Processes / Files / Registries / Network
- 탐지된 행위 중 'Network (Incoming / Outgoing)'에 대한 정보 표시

The screenshot displays the CounterTack Sentinel interface. The top navigation bar includes the CounterTack logo and several icons. The main content area is divided into sections for network monitoring. The 'Inbound Connections' section shows 'Top Remote Hosts (by Most Active)' and 'Top Local Ports (by Most Active)', both currently displaying 'No data'. The 'Outbound Connections' section, highlighted with a blue dashed box, shows 'Top Remote Hosts (by Most Active)' and 'Top Remote Ports (by Most Active)'. The 'Top Remote Hosts' table lists 8 entries with their respective IP addresses and event counts. The 'Top Remote Ports' table lists 3 entries with their respective port numbers and event counts.

Remote Host	Events
1 23.67.162.110	1
2 121.156.109.60	1
3 101.79.247.68	1
4 222.122.117.55	1
5 74.125.235.130	1
6 121.156.109.59	1
7 74.125.31.95	1
8 54.239.186.76	1

Remote Port	Events
1 80	115
2 443	26
3 2250	1

Sentinel 주요 기능

Knowledge Library

- SCIs, Profiles, Conditions, Key Event 등의 Library 관리 화면
- Library 수정 및 편집 기능 제공 (향후 UI를 통한 관리 기능 제공)

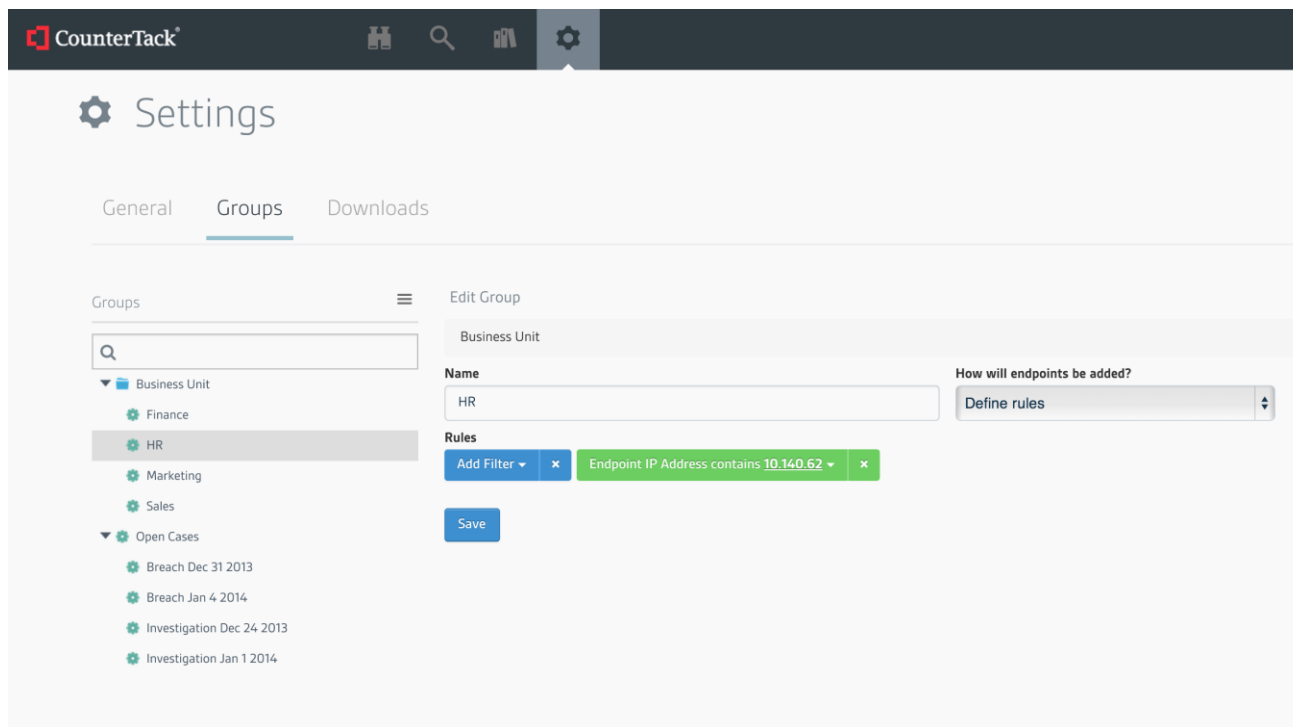
The screenshot displays the CounterTack Knowledge Library interface. On the left, a sidebar titled 'Definitions' contains a search bar and a list of categories: SCIs, Profiles, and Conditions. Under 'Profiles', several items are listed, including 'Profile-Workstation-1' which is currently selected. The main area shows the XML configuration for 'Profile-Workstation-1'. The XML code defines an observable package source and an observable with a description: 'Origin Conditions for the profile that detects suspicious activity on the workstation assuming that host in a secure environment.' The XML includes namespaces for CounterTack and Cybox, and references to external schema files. At the bottom right of the editor, there are 'Validate' and 'Save' buttons.

```
1 <cybox:Observables
2 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:countertack="https://www.countertack.com"
3 xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
4 xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
5 xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2"
6 xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2" xmlns:example="http://example.com"
7 xsi:schemaLocation="http://cybox.mitre.org/cybox-2 http://cybox.mitre.org/XMLSchema/core/2.0.1/cybox_core.xsd
8 http://cybox.mitre.org/objects#ProcessObject-2
9 http://cybox.mitre.org/XMLSchema/objects/Process/2.0.1/Process_Object.xsd
10 http://cybox.mitre.org/default_vocabularies-2
11 http://cybox.mitre.org/XMLSchema/default_vocabularies/2.0.1/cybox_default_vocabularies.xsd
12 cybox_major_version="2" cybox_minor_version="0">
13 <cybox:Observable_Package_Source name="Profile-Workstation-1"></cybox:Observable_Package_Source>
14
15 <cybox:Observable id="Origins-Profile-Workstation-1">
16 <cybox:Title>Profile-Workstation-1</cybox:Title>
17 <cybox:Description>
18   Origin Conditions for the profile that detects suspicious activity on the workstation assuming that
19   host in a secure environment.
20 </cybox:Description>
21 <cybox:Keywords>
22 <cybox:Keyword-Type>Origins</cybox:Keyword>
23 </cybox:Keywords>
24 <cybox:Observable_Composition operator="OR">
25 <!-- MBR overwrite -->
26 <cybox:Observable idref="countertack:observable-10f7f5be-7a9e-43a0-9fea-b4e767e393a8">
27 <cybox:Keywords>
28 <cybox:Keyword>Impact:20</cybox:Keyword>
29 </cybox:Keywords>
30 </cybox:Observable>
```

Sentinel 주요 기능

Settings (환경 설정)

- Default Profile, Smart Group, Kernel Module, Symbol 관리 기능
- 다양한 조건을 통한 엔드포인트 그룹핑 기능 제공



Sentinel의 특징점

- ❑ Kernel Module
- ❑ 자동화된 분석기능
- ❑ 표준에 근거한 확장된 위협 분석
- ❑ Big Data 기술 적용
- ❑ 구축 시 확장성 제공

Sentinel의 특징점

□ Kernel Module

- 커널 레벨에서 시스템 내 행위를 실시간으로 캡처 (특허 기술)
- Remediation (치료) 기능도 커널 레벨에서 구현
- 암호화된 공격, Shell code 공격 캡처
- 시스템의 성능과 기존 어플리케이션에 영향을 최소화
- 공격 과정에서 무력화 시도에 대한 원천 대응
- 다양한 OS 지원



Sentinel의 특징점

- ❑ 자동화된 분석 기능 (Automated Intelligence)
 - 특정 조건 (Origin)에 맞는 행위 발생 시 자동으로 행위 수집 및 분석 시작
 - 모든 행위를 Source / Action / Target으로 구별하여 분석하고,
 - File, Process (Thread), Registry, Network Communication의 세부 정보 제공
 - 사전에 정의된 주요 이벤트는 Key Event로 분류하여 표시
 - SCI (Stateful Compromise Indicator)에 의한 위협의 분류 제공
 - Dark Seoul
 - Zeus
 - Trojan, Boot-kit
 - Crimeware family, etc.



Sentinel의 특징점

□ 표준에 근거한 확장된 위협 분석 기능

- MITRE에 개발된 CybOX와 Open IOC (Indicator of Compromise) 지원
- CybOX - 운영 영역에서 관찰되는 이벤트의 특성을 표현하는 기술 표준
- 보안제품 간의 '위협 정보'를 공유하거나 재사용할 수 있는 방법으로,
- 다양한 기관 또는 산업군 내의 '위협 정보'를 확인하고, 분석할 수 있다.
- '14. 2Q STIX, TAXII 지원 예정

※ CybOX : Cyber Observable eXpression

※ IOC : Indicator of Compromise

※ STIX : Structured Threat Information

※ TAXII : Threat Information Change



Sentinel의 특징점

□ Big Data Analytics 기술 적용

- Hadoop 관련 전문 기술을 보유한 Cloudera Big Data 엔진 적용
- 다양한 open source 사용으로 인한 유지보수 및 기술지원 문제 해결
- 대규모 데이터의 수집, 저장 및 운영에 대한 검증된 플랫폼 제공
- 강력한 검색을 기능을 통한 Enterprise threat correlation 지원
- Impala, HUE, HBASE 등의 내장된 Query를 사용하여, 다양한 분석을 제공



Sentinel의 특징점

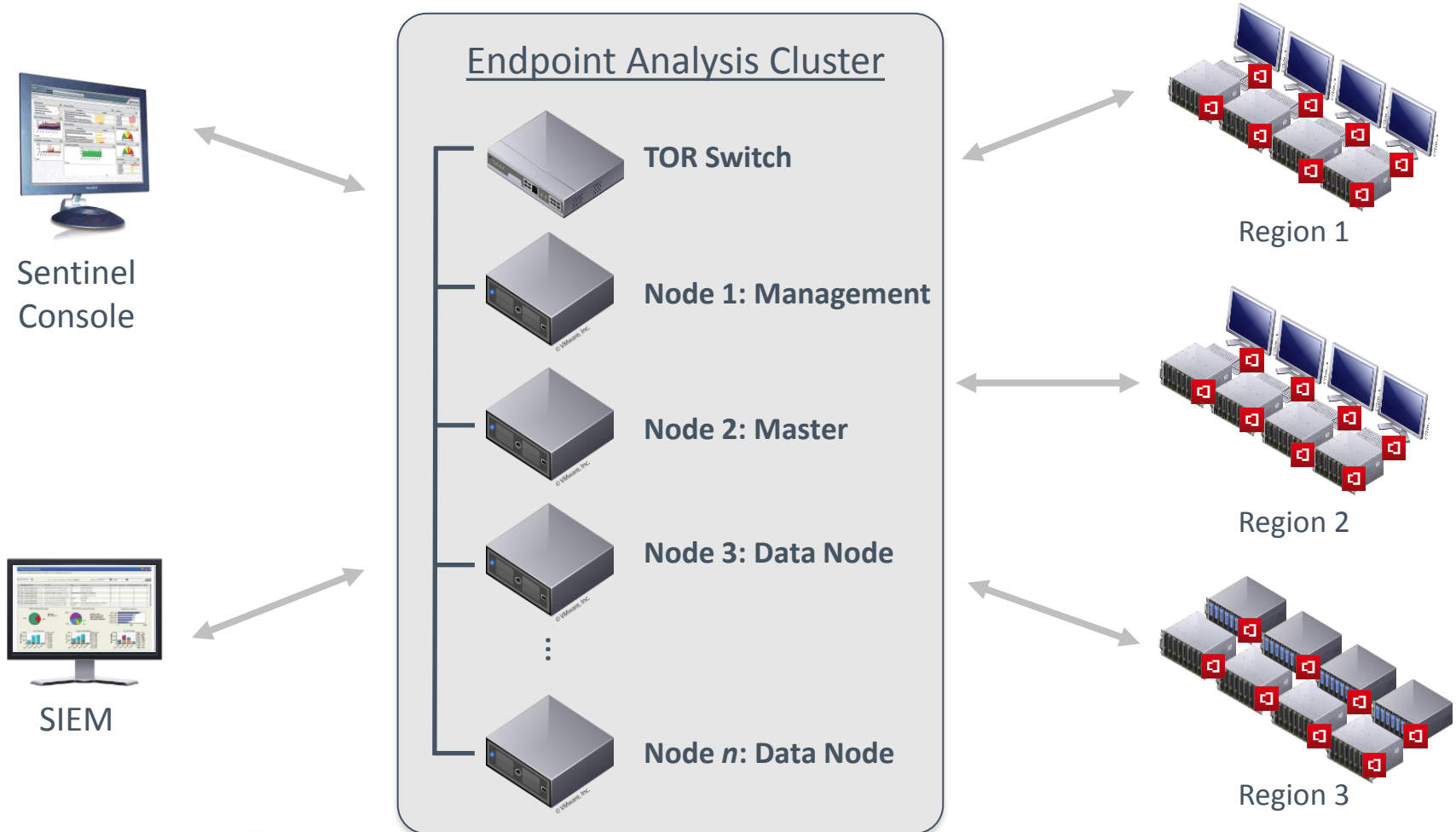
□ 구축 시 확장성 제공

- 기본 Cluster 당 최대 15,000 개의 Endpoint를 수용할 수 있음
- 최대 50,000 개의 Endpoint를 단일 뷰에서 관리가 가능함
- 데이터 노드의 확장을 통해 증가하는 엔드포인트를 관리할 수 있음
- 다양한 네트워크 구성에 대응할 수 있는 유연한 아키텍처 제공
(Multi-tier Flume configuration, DMZ configuration)



Sentinel 시스템 구성도

❑ Kernel Module / Analysis Cluster / Management Console (Web browser)



Kernel Module Specification

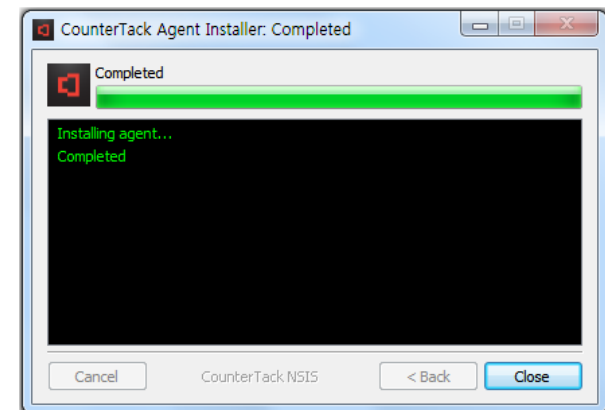
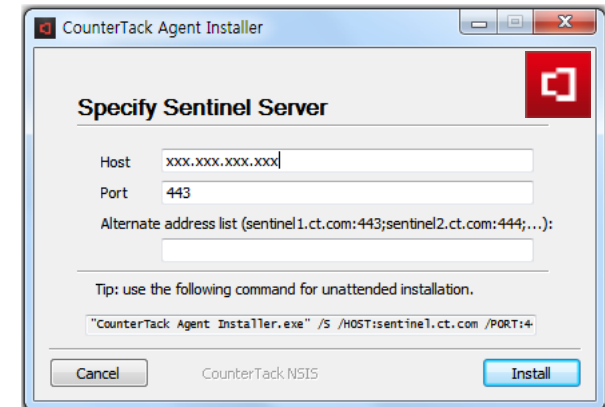
❑ 다양한 Operating systems 지원

- Windows XP SP3
- Windows 7 SP 1 (32-bit, 64-bit)
- Windows Server 2008 R2 SP1
- Windows Server 2003, Linux 지원 예정

❑ Virtual environments 지원

- VMWare ESXi
- Microsoft Hyper-V
- Citrix Xen

❑ Unattended installation 지원



Endpoint Analysis Cluster Hardware Specification

❑ Layer 3 1/10 Gigabit Ethernet Switch

- 노드 간 네트워킹 용도 (Health check, Replication)
- 48 Gigabit Ethernet ports
- 10 Gigabit uplink ports



❑ SuperServer F627R3-RTB+ (4U Rack Mount)

- 기본 4개의 노드로 구성
- Intel Xeon 2600 Series (6Core) * 2EA
- 64GB
- 1TB Disk * 8EA
- Gigabit Ethernet NIC * 2EA

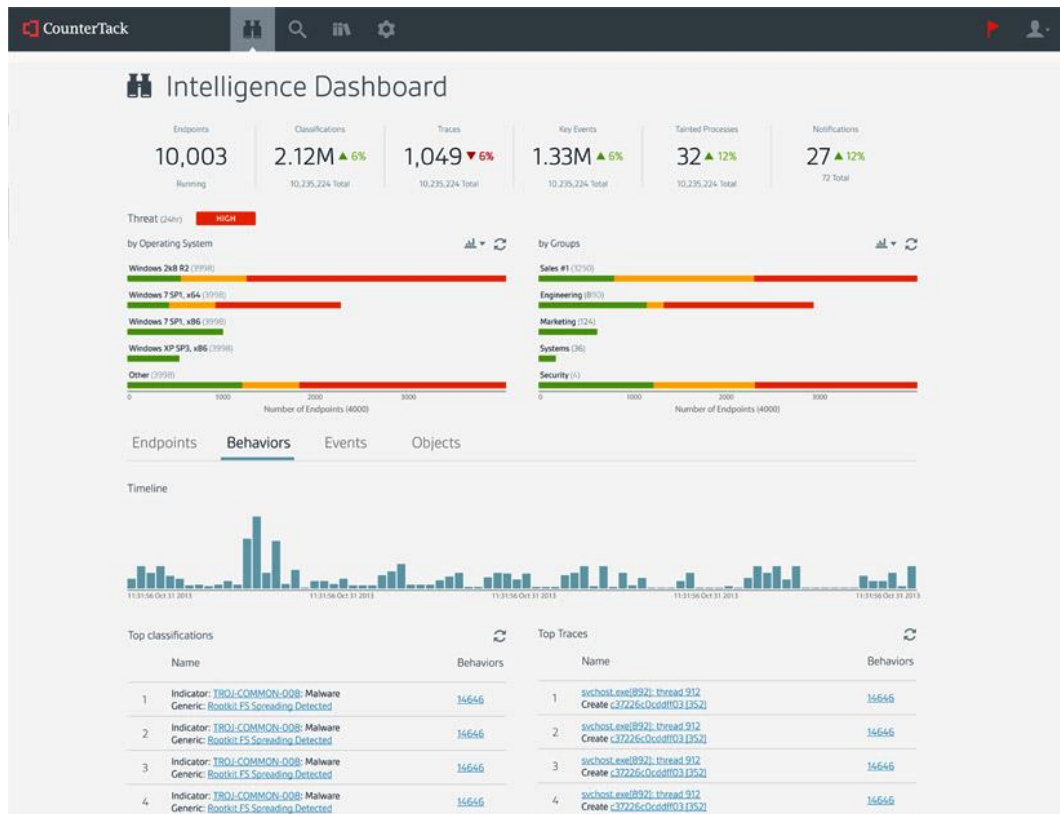
SUPERMICRO®



Management Console Specification

☐ Sentinel Console

- HTTPS 지원, 별도의 관리 소프트웨어나 Database 필요 없음
- Web Browser 접속 - Microsoft Internet Explorer 10, 11 / Google Chrome



Sentinel 다양한 적용 사례 (Use case)

- ❑ 침해 사고 예방 및 사고 대응 프로세스 강화
 - 침해 대응을 위한 특정 데이터와 조건에 대한 검색과 조사
 - 침해 사고 분석을 위한 증거 데이터 확보
 - 기존 보안시스템과 연계 운영을 통한 사고 대응 프로세스 강화

- ❑ 알려지지 않은 악성 행위 탐지
 - 시스템 내의 악성행위 (malicious activities)에 대한 실시간 탐지
 - 악성행위에 대한 분류 및 검증
 - 보호해야 하는 주요 데이터의 접근(access)에 대한 모니터링

- ❑ 기업 내의 엔드포인트에 대한 가시성 확보 및 타겟 공격에 대한 적극적인 대응

CounterTack 회사 개요



- ❑ 설립연도 : 2004년
- ❑ 본사 소재지 : Waltham, MA USA
- ❑ Innovation Center : Santa Monica, CA USA
- ❑ Management
 - Neal Creighton - CEO (GeoTrust)
 - Alen Capalik - Founder / Chief Architect (Barclay Bank)
 - Michael Dairs - CTO (McAfee)
 - Sean Bodmer - Chief Researcher (DoD, Federal Agency)
- ❑ Board
 - William J. Fallon - Chairman (US Military's Central Command)
 - Stuart McClure - Cylance CEO (McAfee, Foundstone)
 - Mark Hatfield - Fairhaven Capital

CounterTack 회사 개요

❑ Product & Services

- Event Horizon 3.2 (Next-Generation Honeynet)
- Scout 4 (Tactical System Monitoring)
- Sentinel 5

❑ Patent

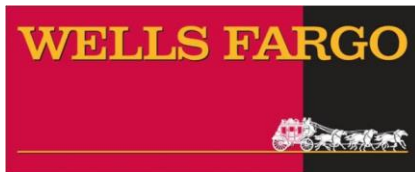
- Deep System Inspection : US Patent No.11,488,743; AU Patent No. 2008242296

❑ VC Backed

- Fairhaven Capital Partners
- Goldman Sachs
- SIEMENS Venture Capital
- Millennium Technology Value Partners

주요 고객사

- ❑ 글로벌 금융, 군수 (Defense), 통신, IT 등의 다양한 레퍼런스 보유
- ❑ 대부분 최초 제품 도입 후 Sentinel의 대규모 환경지원에 따라 전사 적용 예정



ZURICH

Deloitte.



Partners

Technology Partners



Solution Partners



[Backup slide] 차세대 엔드포인트 보안 솔루션 점검 항목

- ❑ 엔드포인트에 설치되는 소프트웨어의 자체 보호 기능 제공 여부
- ❑ 엔드포인트의 부하 최소화, 기존 보안 시스템과의 호환 여부
- ❑ 다양한 64-bit OS, 가상화 환경에 대한 지원 여부
- ❑ 알려지지 않은 위협 발생 시 실시간 탐지 여부
- ❑ 암호화된 공격과 내부 확산의 탐지 여부
- ❑ 자동적인 공격의 분류 및 유형 탐지
- ❑ Enterprise Threat Correlation 기능 지원 여부
- ❑ 식별된 위협에 대한 효과적인 대응 방법 제공 여부
- ❑ 3rd Party 보안 솔루션과의 통합 및 연계 지원 여부
- ❑ 대규모의 네트워크 환경 지원 및 확장성 제공 여부





CounterTack

Own Every Endpoint.