



“변화하는 위협에 대응하는
Security Information Event
Management 와 Intelligence 활용”

인텔코리아 김수영 부장(Senior Sales Engineer)



Agenda

- Challenges
- Security Information Event Management?
- Global Threat Intelligence
- Cyber Threat Intelligence
- See it Work
- Conclusion

GEORGE
CLOONEY

MARK
WAHLBERG

In the Fall of 1991,
the *Andrea Gail* left Gloucester, Mass.
and headed for the fishing grounds
of the North Atlantic.

Two weeks later, an event
took place that had never occurred
in recorded history.

A WOLFGANG PETERSEN...

THE PERFECT STORM

WARNER BROS.

© BALTIMORE SPRING CREEK PICTURES... RADIANT PRODUCTIONS... WOLFGANG PETERSEN... GEORGE CLOONEY MARK WAHLBERG "THE PERFECT STORM" DUANE LANE WILLIAM FICHTNER
KAREN ALLER BOB CUNYAN... MARY ELIZABETH MASTRANTONIO... JOEY C. REILLY... JAMES BURNER... RICHARD FRANCIS BRUCE, A.C.E. ... WILLIAM SANDELL... JOHN SEALE, A.C.S., R.S.C.
... MURRY LEVINSKY DUNCAN BENCIJONSON... SEBASTIAN JUNGER... BILL WITTLIFF... BO SOLENIUS... PHILLA WEINSTEIN WOLFGANG PETERSEN... GAIL KATZ... WOLFGANG PETERSEN

HITS JUNE 30TH

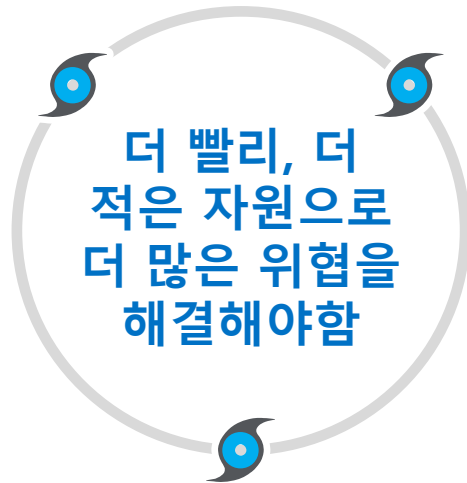
www.perfectstorm.net



Security's Perfect Storm

복잡성 증가

- 데이터 및 장치의 기하급수적인 성장
- “클라우드로의 전환” 가시성과 제어의 어려움
 - 분리된 보안환경



자원의 제약

- 급조된 인력과 기술력 부족
 - 심화된 경쟁
 - 예산 부족

시간 긴박성

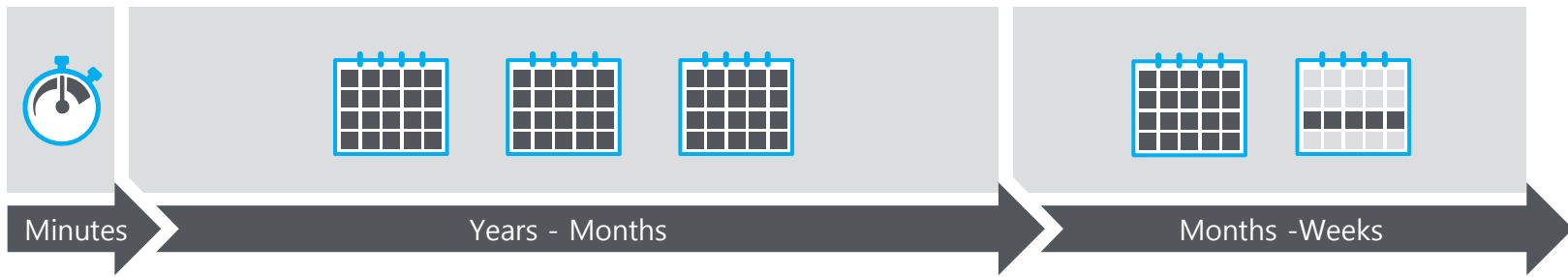
- 몇 분만에 조직이 침해
- 피해는 몇달동안 지속
 - 피해는 치명적

현재의 Threat Scape 현실은....

침해시간

발견시간

복구시간

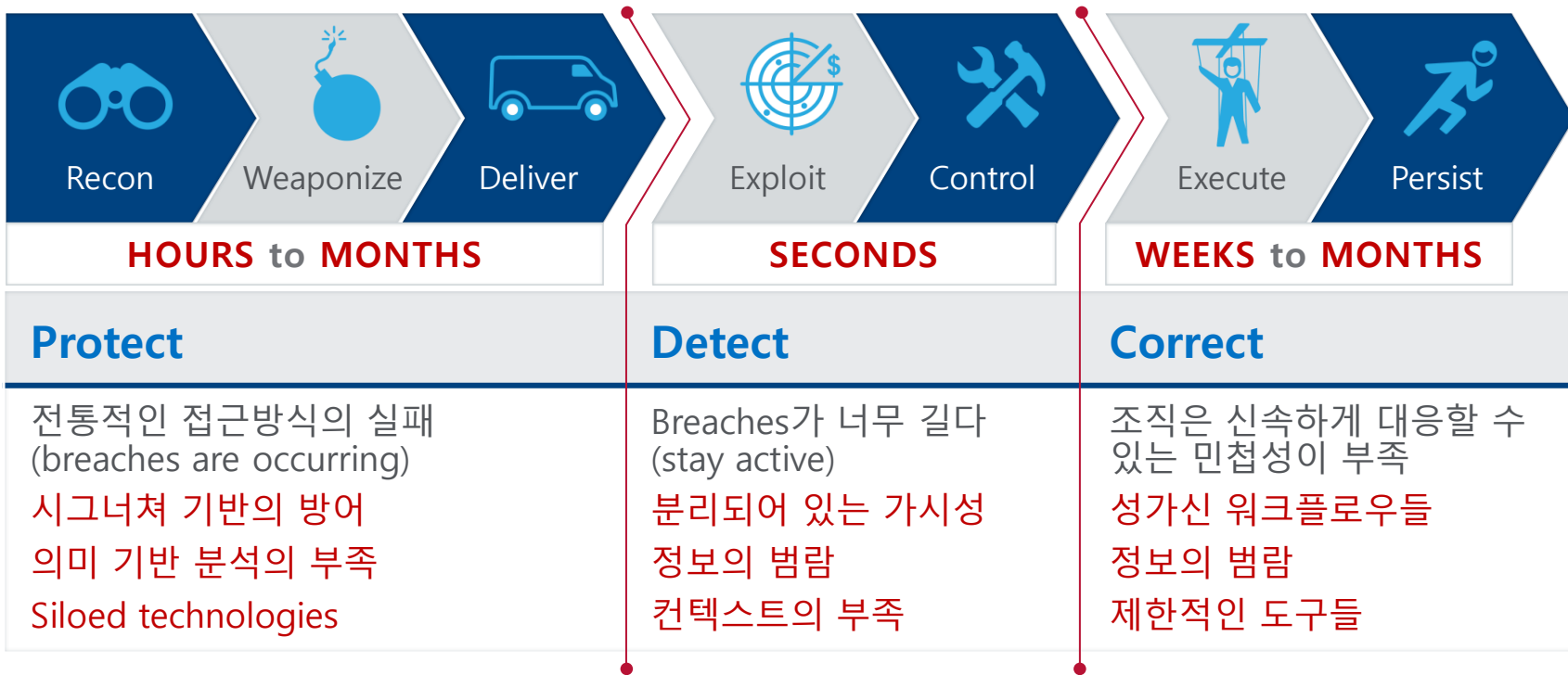


최소한의 사전
대응 노력

공격에 압도당한
보안팀

치명적인 금전적
영향

The Challenge

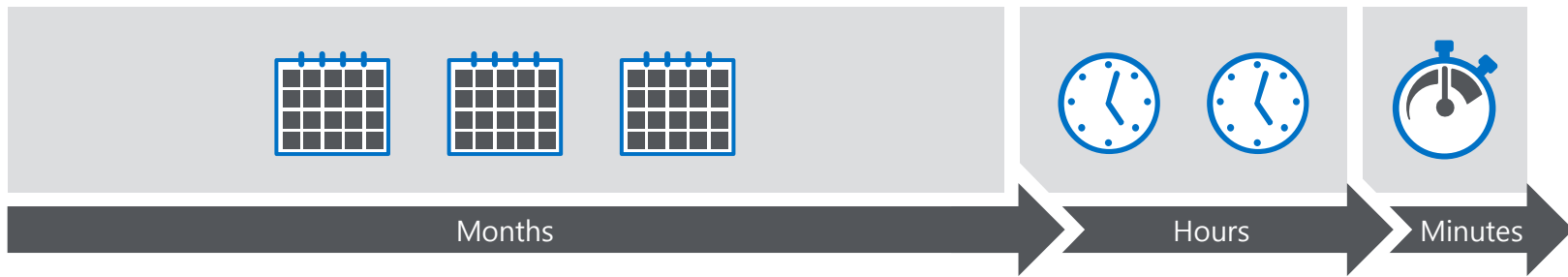


미래는...

침해시간

발견시간

복구시간

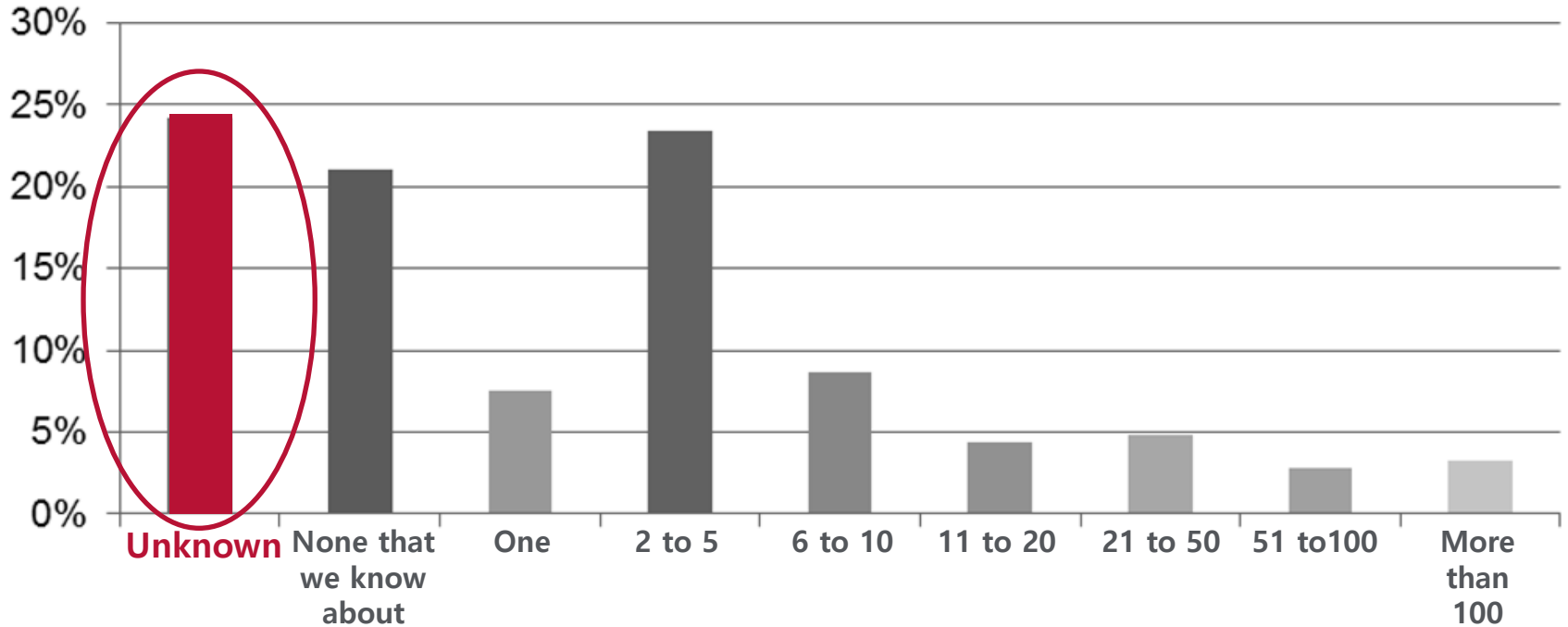


상당한 사전 대응
노력

최적화된 보안팀

금전적 영향
최소화

Have You Been Breached?

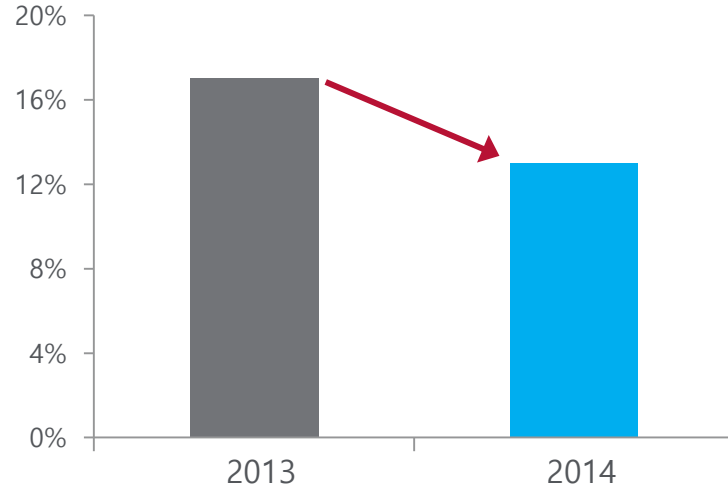


Source: Sans survey

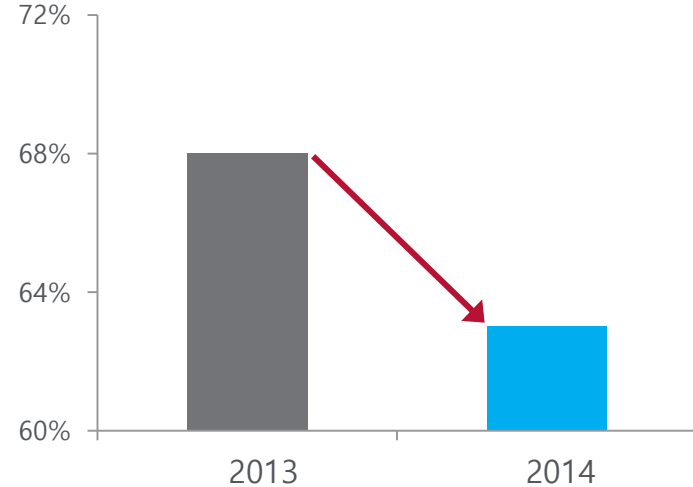
Are We Winning?

Or are we losing...

Security fully meets my needs



Security partially meets my needs



Source: Sans survey

Intel Threat Defense Life Cycle

연속적인 방어 사이클로 이동



Protect – 이전에 본적 없는 기술과 페이로드를 방해하는동안 보급경로를 중단



Detect – 고급 인텔리전스와 분석을 통해 낮은 임계값을 조명하는 것을 기동



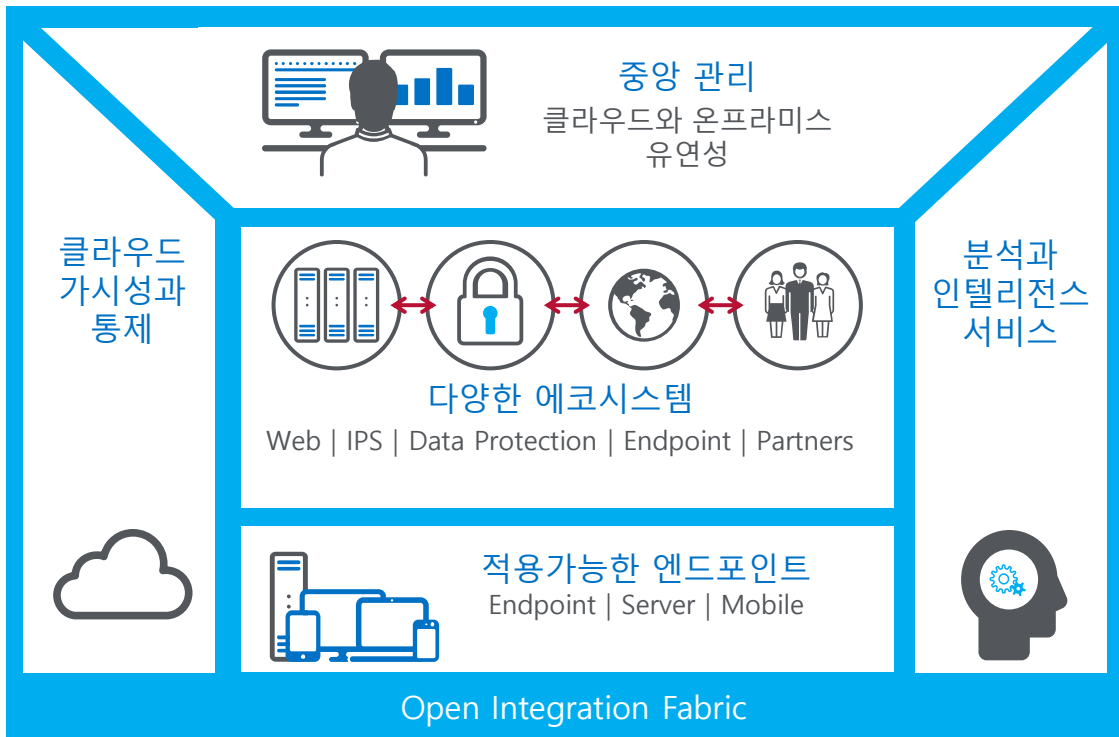
Correct – 유동성 조사의 일환으로 선별을 개선하고 응답의 우선순위에 따라 교정



Adapt – 통합된 보안시스템을 통해 통찰력을 즉시 적용

통합보안시스템 구축

적은 리소스로 더 많은 위협을 신속하게 해결



- 엔드포인트 및 클라우드 센서로 가시성과 제어 향상
- 분석 및 인텔리전스 서비스로 위협 방어 라이프사이클 가속화
- 인텔시큐리티와 3rd party solutions 아키텍처의 연결로 기능 자동화
- 클라우드와 온프레미스의 유연한 중앙 집중 관리 통한 보안운영 간소화

Security Information Event Management

최적화된 위협 관리를 위한 전략

INTELLIGENT



실시간 고급 분석(Real Time Advanced Analytics)

자동화 된 룰, 리스크/행위 그리고 통계적 상관관계(correlation)

위협 우선 순위(Threat Prioritization)

Turns billions of “so what” events into actionable information

ACTIONABLE



액티브 커스터마이징 대쉬보드(Active and Customizable Dashboards)

위협 조사 분석 확인 및 쉬운 반응

고성능의 데이터 관리 엔진(High Performance Data Management Engine)

위협 분석 조사, 데이터 섭취에 빠른 응답

쉬운운영(Ease of Operation)

수백의 out-of-the-box 룰과 리포트

INTEGRATED



포괄적인 보안(Comprehensive Security)

광범위한 장치 데이터 수집, cloud 와 VM 지원, McAfee Security Connected active integrations 로 효율적이며, 효과적인 대응

Global Threat Intelligence

Global insights, plus more volume and intelligence than anyone else



100 만개의 글로벌 위협 센서가 **120** 개 국가에 설치

500 이상의 분석가/연구진

공공서비스를 위한 100% 가동 시간 SLA

45+ billion queries/day

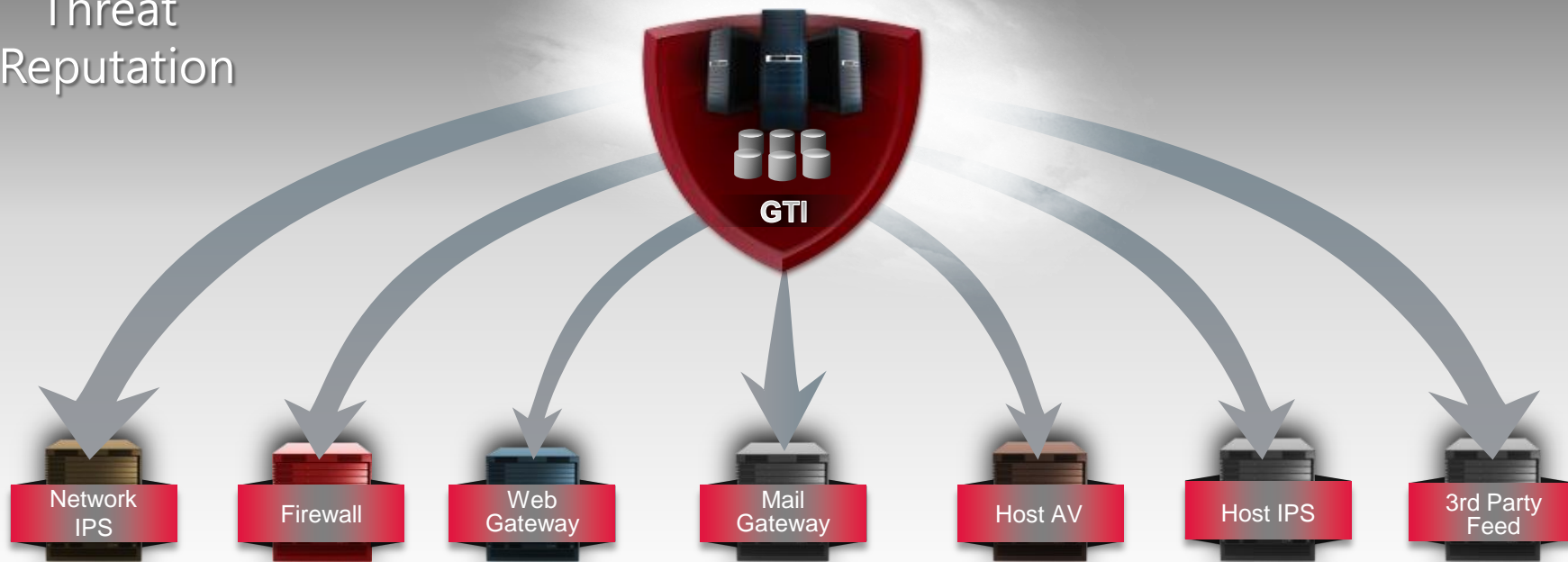
Over 1.5 million files and 1 million URLs analyzed per day

500,000 virtual machine sandboxes a day for behavior

We see more, we protect more, and we offer the market's **strongest** global threat intelligence.

Global Threat Intelligence

Threat
Reputation



Global Threat Intelligence

Why McAfee Is Best Positioned to Deliver GTI 360° Correlation Across All Threat Vectors



Global Threat Intelligence

DNS

의심스런 호스트와 IRC통신

Group By Source IP

AND [Filters -> Destination IP (In) [GTI Malicious IPs], Destination Port (In) [53]]

Edit Logical Element

Logical element type:

- AND
- OR

1 of 1 conditions

Sequence

This logical element should trigger when its components match an event this many times (Threshold) within this amount of time (Time Window).

Threshold: 10

Time Window: Hours: 0, Minutes: 5, Seconds: 0

5분 동안 10회 발생

Match Component

The fields that are provided below match on a single event that comes through the correlation engine. When all the fields match on a given event then this component will trigger.

The filters defined below should apply to:

- Events
- Flows

Destination IP (In) [GTI Malicious IPs]

Destination Port (In) [53]

Destination Port 탐지

GTI 에서 알려진 IP 들 중에 Destination IP 탐지

Match Component

The fields that are provided below match on a single event that comes in through the correlation engine. When all the fields match on a given event then this component will trigger.

The filters defined below should apply to:

- Events
- Flows

Destination IP (In) [GTI Malicious IPs]

Destination Port (In) [194, 531, 6660, 6661, 6662, 6663, 6664, 6665, 6666, 6667, 6668, 6669, 6679, 7000]

194,531,6660,6661,6662,6663,6664,6665,6666,6667,6668,6669,6679,6697,7000 인 Destination Port 탐지

GTI 에서 알려진 IP 들 중에 Destination IP 탐지

OK Cancel



- 표적에 대한 의지 및 계획성
- 특수한 종류의 멀웨어 또는 익스플로잇 킷과 같은 위협할 수 있는 능력
- 취약점 같이 공격의 여지가 있을 때→기회

Cyber Threat Intelligence

“최근 발생하고 있는 실질적인 근거들을 기반으로 한 지식, 메커니즘, 지표, 관계, 건설적인 충고 등을 말한다.” - Gartner -

Cyber Threat Intelligence

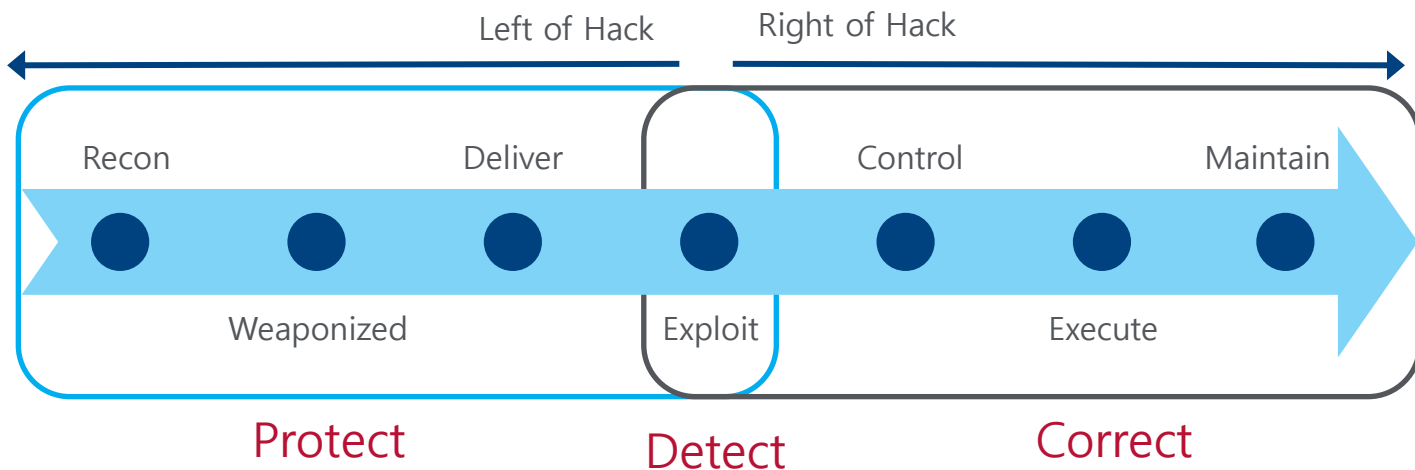
Customer value

- ✓ Increased threats, borderless security ✓
- ✓ Response time, mergers, acquisitions
- IOT, Need for proactive approach ✓
- ✓ Expanding attack surface, shortages ✓

Cyber Threat Intelligence

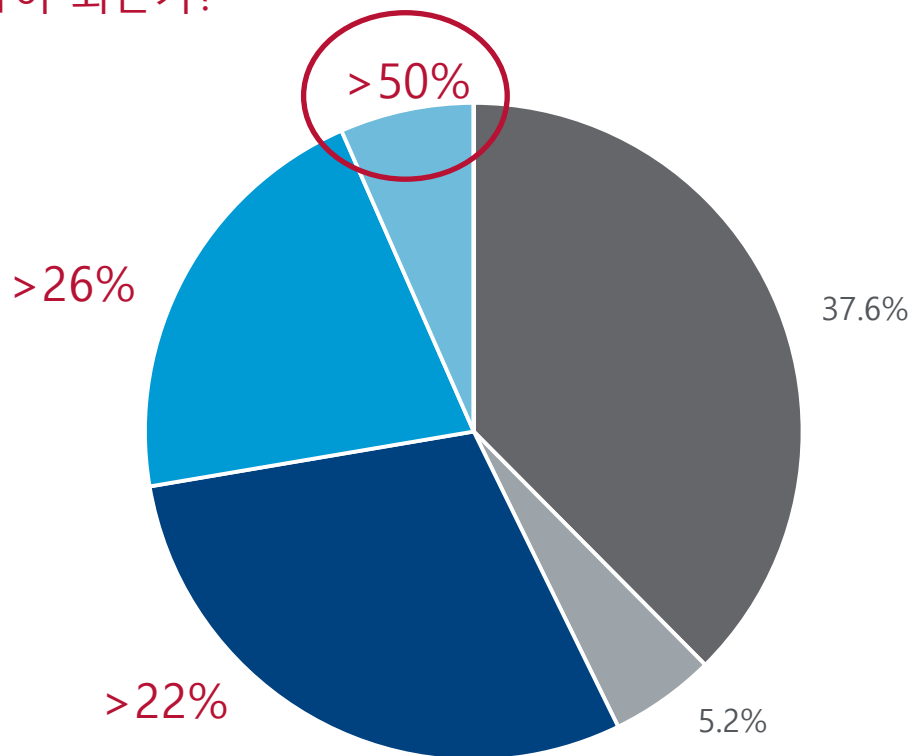
The kill chain

- IOCs 적용은, left of the exploit으로 가기 위한 Change of the Game이다!
- IOC's feed 는 Intel SIEM로 적용해서 위협에 대해서 즉시 detect , correct



Cyber Threat Intelligence

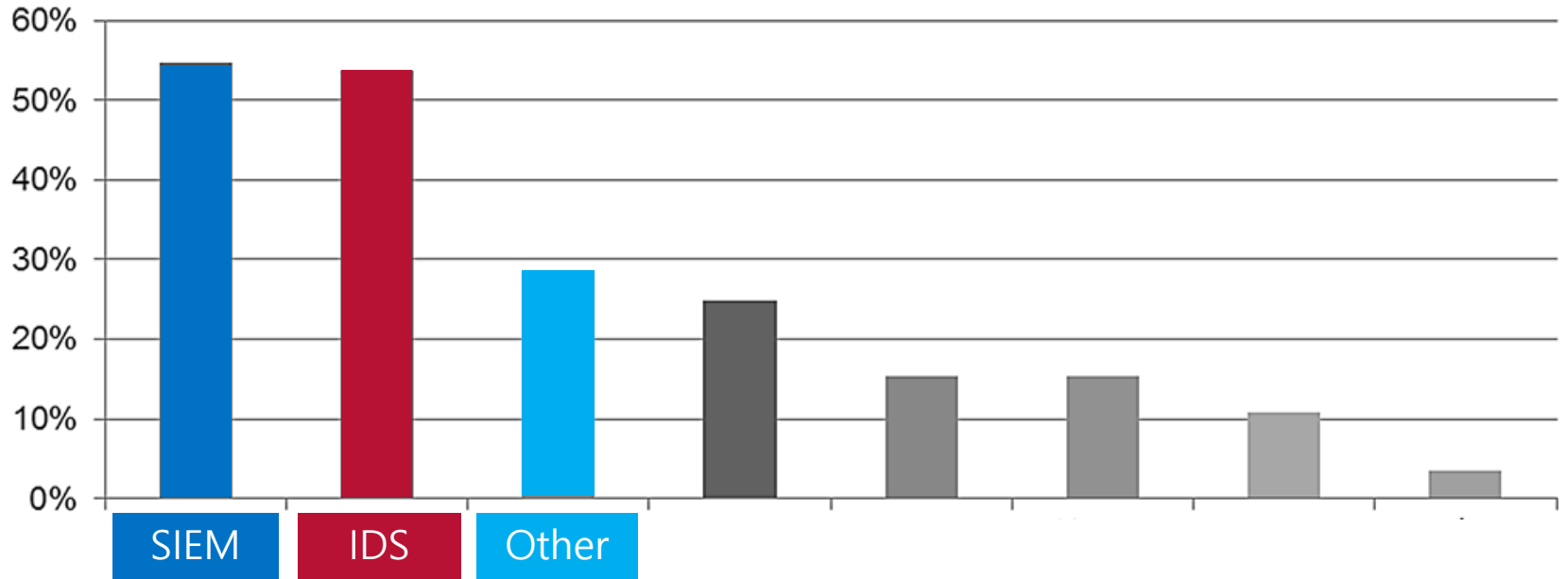
당신의 조직에 도움이 되는가?



Source: Sans Survey

Cyber Threat Intelligence

어떤 도구가 사용되는가?



Source: Sans Survey

Cyber Threat Intelligence

Indicate Of Compromise?

- IOC 는 침입에서 남은 forensic artifact 이며 host 또는 network에서 식별
- Artifacts 는 in memory, file system, registry, running processes에 존재
- IOC 는 '측정이벤트(measurable event)' 또는 '상태특성(stateful property)' 의 '관찰(observable)'을 의미
- MD5 hash, file name, URL, IP addresses

Source	Summary	Attribute	Timestamp	Summary
File System	C:\Users\bob\Desktop\UltraWidget.pdf	Created	10/10/13 20:19:07 UTC	Malicious PDF
File System	C:\WINDOWS\SysWOW64\acmCleanup.exe	Created	10/10/13 20:24:44 UTC	HTTP backdoor
Registry	HKEY_CURRENT_USER\Microsoft\Windows\CurrentVersion\Run Type: REG_SZ Value: C:\WINDOWS\SysWOW64\acmCleanup.exe	Modified	10/10/13 20:24:44 UTC	Persistence mechanism for "acmCleanup.exe"
Prefetch	Prefetch file: ipconfig.exe-36A2A03F.pf	Created	10/11/13 20:24:00 UTC	Prefetch file indicating "ipconfig" was executed
File System	C:\\$RECYCLE.BIN\wce.exe	Created	10/11/13 20:29:30 UTC	Windows Credentials Editor, used to obtain credentials
File System	C:\\$RECYCLE.BIN\filewalk32.exe	Created	10/11/13 20:29:39 UTC	Custom file system search utility
File System	C:\\$RECYCLE.BIN\getlsasrvaddr.exe	Created	10/11/13 20:29:54 UTC	Required for Windows Credentials Editor
File System	C:\\$RECYCLE.BIN\rar.exe	Created	10/11/13 20:34:48 UTC	WinRAR archive utility
File System	C:\\$RECYCLE.BIN\update.exe	Created	10/11/13 20:35:11 UTC	PwDump, used to obtain password hashes
File System	C:\Users\svcBackup	Created	10/11/13 20:38:36 UTC	"svcBackup" user profile directory
File System	C:\\$RECYCLE.BIN\Psexec.exe	Created	10/15/13 12:15:37 UTC	Sysinternals PsExec remote command execution utility
URL History	URL: file:///C:/\$/RECYCLE.BIN/c.txt Title: Browser: Internet Explorer (8.0.6001.18702)	Last Visited	10/15/13 16:11:03 UTC	Text file containing output of "tree c:."
URL History	URL: file:///C:/\$/RECYCLE.BIN/a.txt Title: Browser: Internet Explorer (8.0.6001.18702)	Last Visited	10/15/13 16:11:06 UTC	Text file containing output of "ipconfig /all"
Registry	HKEY_USERS\S-1-5-21-567270542-30467956377-4044443844-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\#10.20.30.101#C\$ Type: REG_KEY	Modified	10/15/13 16:17:55 UTC	Registry key depicts a mountpoint created by the attacker between Bob's PC and 10.20.30.101 using the hidden C\$ share
Prefetch	Prefetch file: tree.exe-06E1F9FF.pf	Created	10/15/13 16:20:29 UTC	Prefetch file indicating "tree" was executed
File System	C:\\$RECYCLE.BIN\rar	Created	10/15/13 17:37:37 UTC	WinRAR archive containing "a.txt" and "c.txt"

Open IOC

- XML-based format
- 이러한 테스트 레지스트리 값을 간단한 조건으로 표현가능
- IOC format의 지정의 데이터 유형은 networking, browser, persistent storage, memory, 등을 포함.
- 대부분의 일반적인 유형은 적용가능 하지만, 확장도 가능

Name: STUXNET VIRUS (METHODOLOGY) T.. R..

Author: Mandiant

GUID: ea3cab0c-72ad-40cc-abbf-90846fa4afec

Created: 0001-01-01 00:00:00Z

Modified: 2011-11-04 19:35:05Z

Description:

Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state. The malware then maps in its own executable section and fixes up the CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allows the malware to execute under the pretense of a known and trusted process.

add: AND OR Item

- OR
 - File Section Name contains .stub
 - File Name contains mdmcpq3.PNF
 - File Name contains mdmcr3.PNF
 - File Name contains oem6C.PNF
 - File Name contains oem7A.PNF
- AND
 - Driver Attached To Driver Name contains fs_rec.sys
 - Driver Attached To Driver Name contains mrxsm.sys
 - Driver Attached To Driver Name contains sr.sys
 - Driver Attached To Driver Name contains fastfat.sys
- AND
 - File Name contains mrxcls.sys
 - File Certificate Subject contains Realtek Semiconductor Corp
- AND
 - File Name contains mrxnet.sys
 - File Certificate Subject contains Realtek Semiconductor Corp
- AND
 - Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Secur...

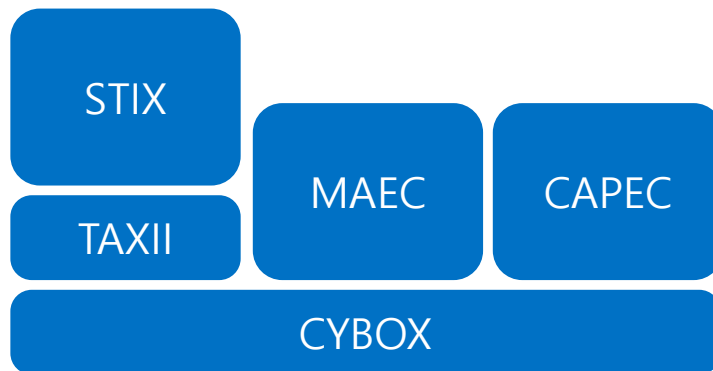
Threat Formats

MITRE

- Open source projects now hosted by OASIS
- 적극적으로 프로젝트에 참여중이거나 관심을 보이는 보안 회사, 정부 및 업계의 많은 수의 그룹이 존재

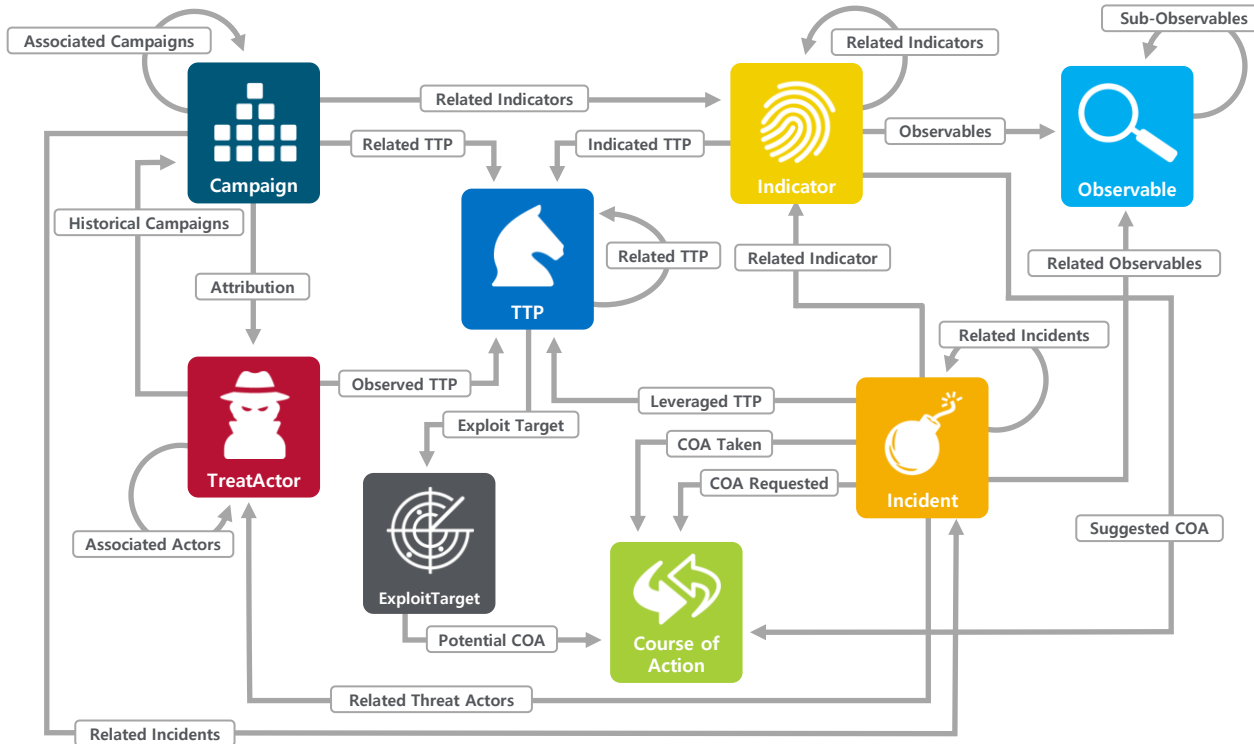


MITRE Threat Format Family



Threat Formats

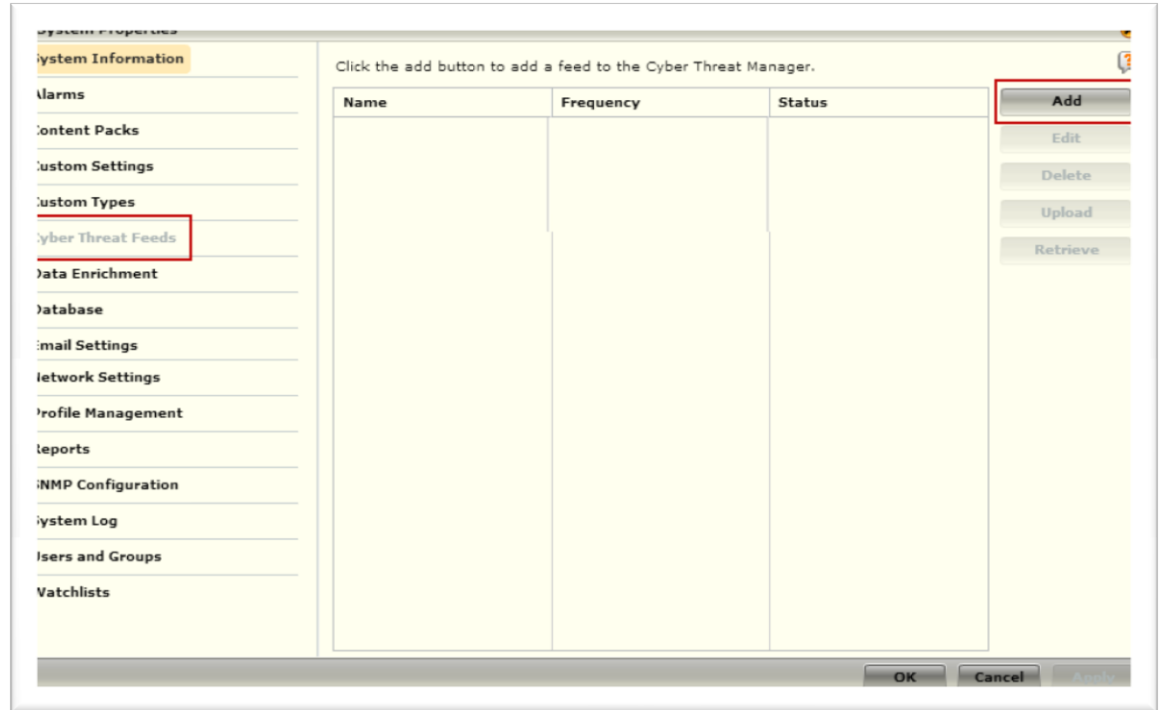
STIX



McAfee Enterprise Security Manager (ESM)

Cyber threat feeds

- ESM system properties
- Cyber threat feeds
- Options
 - Add
 - Edit
 - Delete
 - Upload
 - Retrieve



McAfee ESM

Cyber threat feed wizard

- | Name | Enabled |
|------------|-------------------------------------|
| TAXII | <input checked="" type="checkbox"/> |
| NFS | <input type="checkbox"/> |
| SCP | <input type="checkbox"/> |
| CIFS | <input type="checkbox"/> |
| FTP | <input type="checkbox"/> |
| Manual | <input type="checkbox"/> |
| McAfee ATD | <input type="checkbox"/> |
| SFTP | <input type="checkbox"/> |

The screenshot shows the 'Cyber Threat Feed Wizard' window with the 'Main' tab selected. The window contains the following fields and options:

- Name:** An empty text input field.
- Enabled:** A checked checkbox.
- Type:** A dropdown menu set to 'TAXII'.
- URL:** An empty text input field.
- Authentication:** Radio buttons for 'None' (selected) and 'Basic'.
- Method:** Radio buttons for 'GET' (selected) and 'POST'.
- Ignore Invalid Certificates:** A checked checkbox.
- Collection Name:** An empty text input field.
- Start Date:** A date and time picker set to '01/01/1970 00:00:00'.
- Test Connection:** A button labeled 'Connect'.

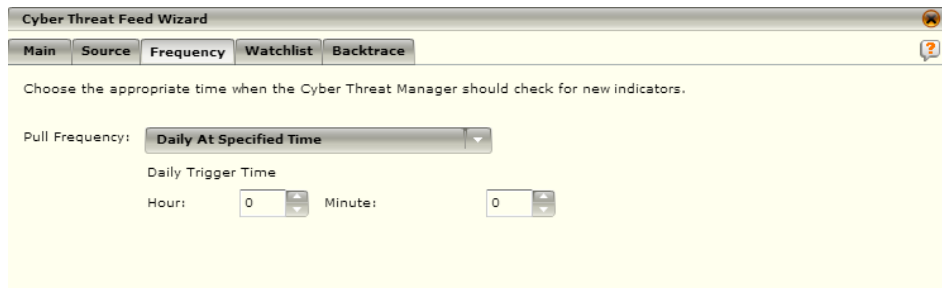
At the bottom of the window are navigation buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

McAfee ESM

Cyber threat feeds

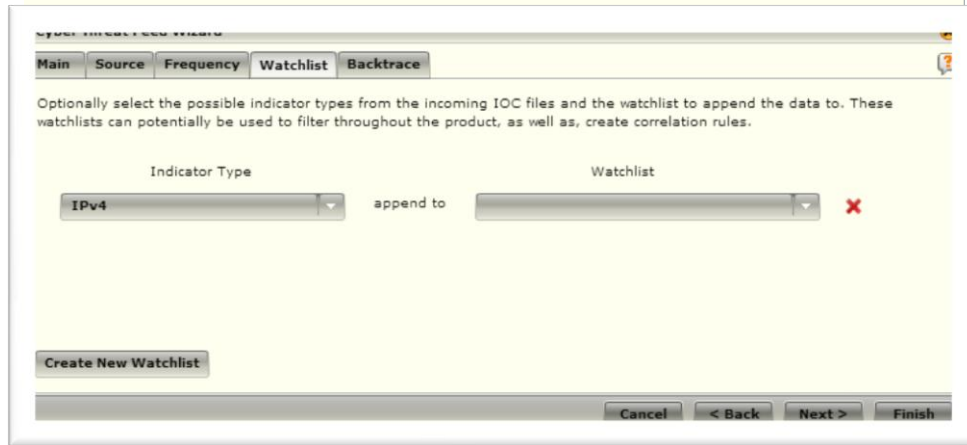
Frequency

- 표시 목록을 검색하는 시점의 간격(Interval at which to retrieve indicator list)



Watch list

- 적절한 유형의 watchlist에 표시값을 추가(Add indicator values to a watchlist of the appropriate type)
- 식별된 IOC로 Watchlist를 사용하여 현재의 이벤트나 historical 이벤트를 검색



McAfee ESM

BackTrace

- ESM 이벤트 / 또는 흐름을 최대 60 일 이전 검색
- 이벤트와 IOC 일치된 부분을 장비에서의 자동식별.
- 지표(indicator values) 가 Events/flows 일치하면,
 - 이 화면에서 지정한 기준에 따라 경보를 트리거
 - Cyber threat feed view 에서 View 일치

The screenshot shows the 'BackTrace' configuration window in the McAfee ESM interface. The window has a title bar 'Cyber threat feed view' and a navigation bar with tabs: 'Main', 'Source', 'Frequency', 'Watchlist', and 'Backtrace'. Below the navigation bar, there is a descriptive text: 'Perform a Backtrace analysis with the indicators that come in from this feed. Choose a time frame to compare prior events and/or flows against the indicator and then what actions to take when a match is found, plus the assignee and severity for the alarm that will be created.'

The configuration options include:

- Time Frame:** A dropdown menu set to 'Last 7 days'.
- Assignee:** A dropdown menu set to 'All Privs'.
- Severity:** A dropdown menu set to '50'.
- Event Selection:** Two checkboxes, 'Events' (checked) and 'Flows' (unchecked).
- Action List:** A list of actions with checkboxes and 'Configure' buttons:
 - Log event
 - Auto-acknowledge Alarm
 - Visual Alert: [Configure]
 - Create Case: [Configure]
 - Update Watchlist: [Configure]
 - Send Message: [Configure]
 - Generate Reports: [Configure]
 - Execute remote command: [Configure]
 - Send to Remedy: [Configure]
 - Assign Tag with ePO: [Configure]
 - Blacklist: [Configure]
 - Custom alarm summary: [Configure]

At the bottom left, there is a link 'Add recipient'. At the bottom right, there are buttons for 'Cancel', '< Back', 'Next >', and 'Finish'.

McAfee ESM

Cyber threat indicator views

Access view from

- Quick link (highlighted)
- Views → event workflow views
→ cyber threat indicators

View shows

- Indicator name
- Feed name which triggered
- Date
- BackTrace hit count
(number of matching events/flows)
- Event/flow listing

The screenshot displays the McAfee ESM interface for Cyber Threat Indicators. At the top, there's a navigation bar with 'Local ESM' and 'Cyber Threat Indicators' tabs. Below this is a table of indicators. One indicator is highlighted in yellow, with a 'download' link. Below the indicator table, there are tabs for 'Description', 'Details', 'Source Events', and 'Source Flows'. The 'Source Events' tab is active, showing a table of events with columns for Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype. Below the event table, there are tabs for 'Details', 'Advanced Details', 'Geolocation', 'Description', 'Notes', 'Custom Types', and 'Packet'. The 'Details' tab is active, showing a form with fields for First Time, Last Time, Duration, Source IP, Dest. IP, Protocol, Source Port, Dest. Port, Event Subtype, Source MAC, and Dest. MAC. The bottom of the interface shows 'Page 1'.

Indicator Name	Feed Name	Date Received	Backtrace ...
This IOC has been generated from collective threat intelligence	IP Bad Actors	05/26/2015 16:04:48	1000

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	An account was logged off.	1	172.25.5.40	::	n/a	05/26/2015 16:01:49	success
25	An account was logged off.	1	172.25.5.40	::	n/a	05/26/2015 16:01:46	success
25	An account was successfully logged on.	1	172.25.5.24	172.25.5.40	n/a	05/26/2015 15:48:37	success
25	An account was successfully logged on.	1	172.25.5.56	172.25.5.40	n/a	05/26/2015 15:48:11	success



IOC from Open IOC



Convert to STIX

Not a one to one conversion

- Github openioc-to-stix
- Python 2.7
- Python-stix
- Python-cybox
- `$ python openioc-to-stix.py -i <OpenIOC XML file> -o <STIX XML file>`

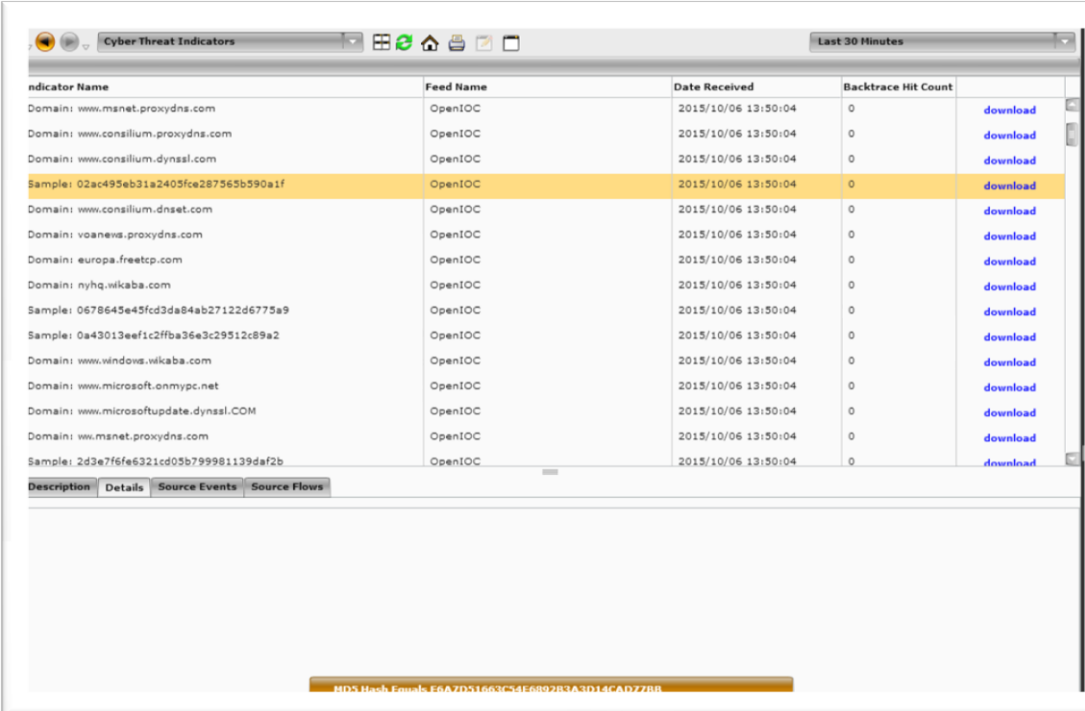
McAfee ESM

Cyber threat feeds—XML

```
<stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator with a set of three IP addresses in the watchlist.</indicator:Description>
  <indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
    <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
      <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
        <AddressObject:Address_Value condition="Equals"
apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
```

McAfee ESM

Cyber threat indicators



The screenshot displays the McAfee ESM Cyber Threat Indicators interface. The window title is "Cyber Threat Indicators" and the refresh interval is set to "Last 30 Minutes". The table below lists various indicators, with the fourth row highlighted in yellow.

indicator Name	Feed Name	Date Received	Backtrace Hit Count	
Domain: www.manet.proxydns.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.consillium.proxydns.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.consillium.dynssl.com	OpenIOC	2015/10/06 13:50:04	0	download
Sample: 02ac495eb31a2405fce287565b590a1f	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.consillium.dnset.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: voanews.proxydns.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: europa.freetp.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: nyhq.wikaba.com	OpenIOC	2015/10/06 13:50:04	0	download
Sample: 0678645e45fcd3da84ab27122d6775a9	OpenIOC	2015/10/06 13:50:04	0	download
Sample: 0a43013eef1c2fba36e3c29512c89a2	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.windows.wikaba.com	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.microsoft.onmypc.net	OpenIOC	2015/10/06 13:50:04	0	download
Domain: www.microsoftupdate.dynssl.COM	OpenIOC	2015/10/06 13:50:04	0	download
Domain: ww.msnet.proxydns.com	OpenIOC	2015/10/06 13:50:04	0	download
Sample: 2d3e7f6fe6321cd05b799981139daf2b	OpenIOC	2015/10/06 13:50:04	0	download

At the bottom of the interface, there are tabs for "Description", "Details", "Source Events", and "Source Flows". Below the table, a yellow bar displays the MD5 Hash: Equals:E6A7D51663C54E6892B3A3D1FCAD77B8.

McAfee ESM

Cyber threat alarm

The screenshot displays the McAfee ESM interface. At the top, a navigation bar includes a 'Triggered Alarms' dropdown menu, indicated by a red arrow. Below this is a table listing several alarms. The second row, representing a 'poison ivy' alarm, is highlighted in yellow and also indicated by a red arrow. Below the table, there are tabs for 'Details', 'Triggering Event', and 'Actions'. The 'Details' tab is active, showing the title 'Cyber Threat Backtrace alarm triggered for feed poison ivy', also indicated by a red arrow. Underneath, it lists the 'Associated Indicator' as 'IP: 22.126.130.37'. A form below contains fields for 'Alarm Name', 'Trigger Date', 'Escalation Date', 'Status', 'Acknowledge Date', 'Assignee', 'Acknowledged By', and 'Severity'. A 'Create Case' button is located at the bottom of the form.

Alarm Name	Summary	Assignee	Severity	Trigger Date	Acknowledge Date	Acknowledged By
poison ivy	Cyber Threat Backtrace alarm triggered for feed poison	rgarrett@MCP.EBC	75	2015/08/28 13:02:49	2015/08/28 13:11:21	rgarrett@MCP.EBC
poison ivy	Cyber Threat Backtrace alarm triggered for feed poison	rgarrett@MCP.EBC	75	2015/08/28 13:02:35	2015/09/08 18:09:21	NGCP
Successful Brute Force	Field match alarm triggered on Adv Correlation Engine	SIEM	99	2015/08/10 16:25:34	2015/09/02 11:40:47	bdespain@MCP.EBC

Cyber Threat Backtrace alarm triggered for feed poison ivy

Associated Indicator: [IP: 22.126.130.37](#)

Alarm Name: Trigger Date: Escalation Date:

Status: Acknowledge Date:

Assignee: Acknowledged By:

Severity: Case: [Create Case](#)

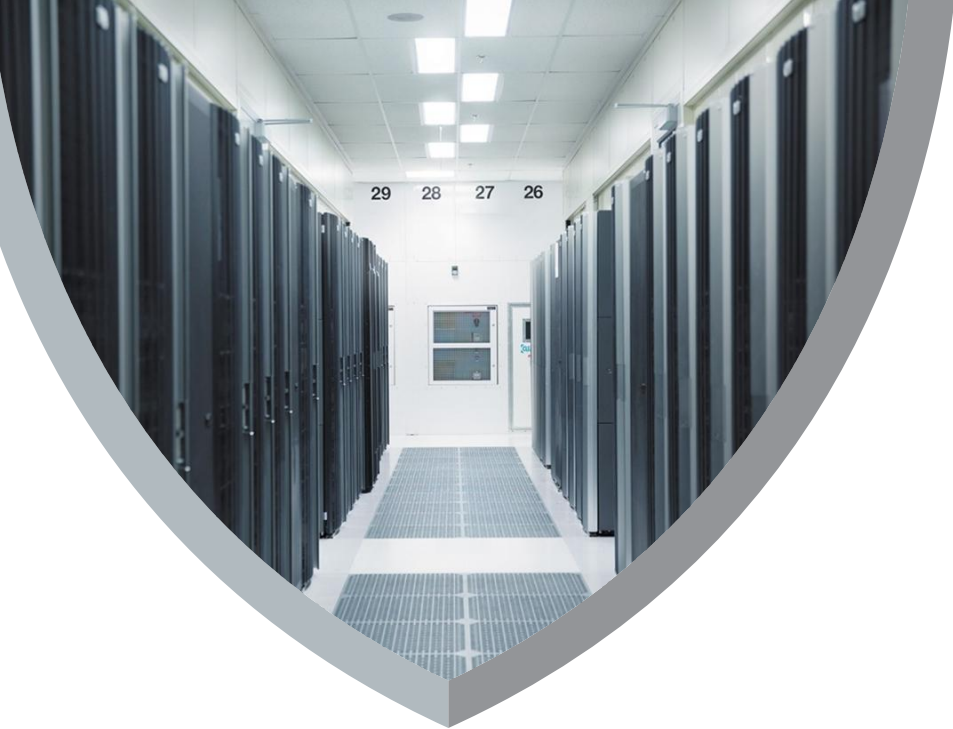
McAfee ESM

Cyber threat alarm

The screenshot displays the McAfee ESM interface with a 'Triggered Alarms' window. The main table lists several alarms, with two 'poison ivy' alarms highlighted in yellow. Below this, a 'Details' section is open, showing a table of triggering events. Three red arrows originate from the 'poison ivy' alarm rows in the top table and point to specific rows in the 'Triggering Event' table: one points to the first row (Source IP 172.20.1.163), another to the second row (Source IP 172.20.1.152), and a third to the fourth row (Message 'Email protection').

Alarm Name	Summary	Assignee	Severity	Trigger Date	Acknowledge Date	Acknowledged By
poison ivy	Cyber Threat Backtrace alarm triggered for feed poison	rgarrett@MCP.EBC	75	2015/08/28 13:02:49	2015/08/28 13:11:21	rgarrett@MCP.EBC
poison ivy	Cyber Threat Backtrace alarm triggered for feed poison	rgarrett@MCP.EBC	75	2015/08/28 13:02:35	2015/09/08 18:09:21	NGCP
Successful Brute Force	Field match alarm triggered on Adv Correlation Engine	SIEM	99	2015/08/10 16:25:34	2015/09/02 11:40:47	bdespain@MCP.EBC

Event Count	Source IP	Destination IP	Last Time	Message	Subtype	Protocol	Severity
1	172.20.1.163	22.126.130.37	2015/08/26 13:06:00	Email protection	alert	n/a	25
3	172.20.1.152	22.126.130.37	2015/08/26 13:08:00	File system protection	alert	n/a	75
1	172.20.1.219	22.126.130.37	2015/08/26 13:09:00	Email protection	alert	n/a	25
1	172.20.0.163	22.126.130.37	2015/08/26 13:09:00	Email protection	alert	n/a	25
2	172.20.1.219	22.126.130.37	2015/08/26 13:11:00	File system protection	alert	n/a	50
2	172.20.0.134	22.126.130.37	2015/08/26 13:12:00	Email protection	alert	n/a	50
3	172.20.1.127	22.126.130.37	2015/08/26 13:13:00	Email protection	alert	n/a	75
1	172.20.1.100	22.126.130.37	2015/08/26 13:14:00	Email protection	alert	n/a	75



IOC from TIE/DXL and ATD

IOC

From TIE/DXL and ATD

DETECT

1. 새로운 unknown 실행 파일이 endpoint에 도착
2. Code 실행됨
3. TIE 정책은 모든 unknown 파일들은 검사를 위해 ATD에 제출 하도록 지시
4. ATD 는 파일을 샌드박스 분석과 악성판정으로 'known malicious' 판정
5. ATD 는 TIE reputation 에 바로 known 악성파일로 업데이트
6. 동일한 형태의 known 악성파일이 endpoint 2 에 도착
7. TIE reputation 에서 'known malicious' 로 Code 실행 실패

CORRECT

1. SIEM 알람 triggers 'patient 0' (endpoint 1)
2. MAR 은 추가로 식별된 악성 실행 파일을 포함 endpoints를 검사, 아직 실행되지 않은 원하지 않는 원천 프로그램을 제거

위협 방지 및 탐지 적응

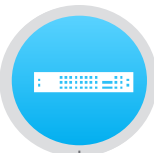
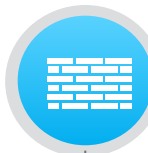
Network & Gateway

NGFW

NIPS

Web Gateway

Email Gateway



네트워크 및
엔드포인트에
적용

Sandbox



IOC 1
IOC 2
IOC 3
IOC 4

페이로드 분석

SIEM



new IOC intelligence
pinpoints historic
breaches

Endpoints



이전에 문제가
있었던 시스템은
격리 및 교정

DXL Ecosystem

DXL Ecosystem

IoC Threat Details

The screenshot displays the 'Cyber Threat Indicators' interface. At the top, there is a navigation bar with a 'Previous Day' dropdown. Below this is a table with the following columns: Indicator Name, Feed Name, Date Received, and Backtrace Hit Co... The first row of the table contains the following data: 'This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2E...', 'TIE Use Case', '09/14/2015 06:01:48', and '6'. A 'download' link is visible to the right of the 'Backtrace Hit Co...' column. Below the table, there are three numbered steps in light blue boxes: 1. New IoC is delivered to SIEM via TAXII, DXL or automated file import; 2. Artifacts are extracted to determine potential threat vectors; 3. Automated 'Backtrace' searches previous event data for prior exposure. At the bottom, there are tabs for 'Description', 'Details', 'Source Events', and 'Source Flows'. The 'Source Events' tab is active, showing a list of events with a blue oval highlighting the list. The events are: File Name Equals SAMPLE_ZP9K2.EXE, MD5 Hash Equals D74441283CCFEEBF1A6B6A2B2E6F860D, SHA1 Hash Equals 0xae82eaefc8133248c6af26a61f86f432ad8cb6f0, File Name Equals Sample_zp9k2.exe, MD5 Hash Equals D74441283CCFEEBF1A6B6A2B2E6F860D, and SHA1 Hash Equals AE92EAefc8133248c6af26a61f86f432ad8cb6f0. The bottom of the interface shows a page number 'Page 1' and the Intel Security logo.

Indicator Name	Feed Name	Date Received	Backtrace Hit Co...
This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2E...	TIE Use Case	09/14/2015 06:01:48	6

1. New IoC is delivered to SIEM via TAXII, DXL or automated file import
2. Artifacts are extracted to determine potential threat vectors
3. Automated 'Backtrace' searches previous event data for prior exposure

Source Events:

- File Name Equals SAMPLE_ZP9K2.EXE
- MD5 Hash Equals D74441283CCFEEBF1A6B6A2B2E6F860D
- SHA1 Hash Equals 0xae82eaefc8133248c6af26a61f86f432ad8cb6f0
- File Name Equals Sample_zp9k2.exe
- MD5 Hash Equals D74441283CCFEEBF1A6B6A2B2E6F860D
- SHA1 Hash Equals AE92EAefc8133248c6af26a61f86f432ad8cb6f0

File with Unknown Reputation

Cyber Threat Indicators Current Day

Indicator Name	Feed Name	Date Received	Backtrace Hit C...	
This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6	download

Description Details Source Events Source Flows

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

Details Advanced Details Geolocation Description Notes Custom Types Packet

Filename: SAMPLE_ZP9K2.EXE File_Hash: D74441283CCFEEBF1A6B6A2B2E6F860D
SHA1: 0xae82eae8c8133248c6af26a61f86f432ad8ct

Page 1

04:13:28 – New file seen for first time in enterprise



Increased Malware Activity Detected

Cyber Threat Indicators Current Day

Indicator Name	Feed Name	Date Received	Backtrace Hit C...	
This IOC has been generated during execution of D74441283CCFE8BF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6	download

Description Details Source Events Source Flows

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

Details Advanced Details Geolocation Description Notes Custom Types Source Events Source Flows Deviation Data Correlation Details

Filename	Sample_zP9k2.exe	File_Type	PE32+ executable (GUI) x86-64
Job_Name	426	SHA1	AE82EAFC8133248C6AF26A61F86F432AD8C1

Page 1

04:13:28 – New file seen for first time in enterprise

04:14:00 – Potential malware detection



File Determined to be Malicious

Cyber Threat Indicators Current Day

Indicator Name	Feed Name	Date Received	Backtrace Hit C...
This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6 download

[Description](#) | [Details](#) | [Source Events](#) | [Source Flows](#)

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

[Details](#) | [Advanced Details](#) | [Geolocation](#) | [Description](#) | [Notes](#) | [Custom Types](#) | [Packet](#) | [Correlation Details](#)

Application	ATD2ESM	File_Type	PE32+ executable (GUI) x86-64
Filename	Sample_zP9k2.exe	Device_IP	172.25.109.113
Host	atd02	SHA1	AE82EAEFC8133248C6AF26A61F86F432AD8CF
Job_Name	426	File_Hash	D74441283CCFEEBF1A6B6A2B2E6F860D
Source User		File_Size	2488320

Page 1

04:13:28 – New file seen for first time in enterprise

04:14:00 – Potential malware detection

04:14:54 – Sandbox analysis convicts executable



Initial Execution Platform Quarantined

The screenshot shows the 'Cyber Threat Indicators' interface. At the top, there's a navigation bar with icons for home, refresh, and print, and a 'Current Day' dropdown. Below this is a table with columns: Indicator Name, Feed Name, Date Received, Backtrace Hit C..., and a download link. The first row is highlighted in yellow and contains the text: 'This IOC has been generated during execution of D74441283CCFE8BF1A6B6A2', 'TIE Use Case', '09/14/2015 06:01:48', '6', and a 'download' link.

Below the table are tabs for 'Description', 'Details', 'Source Events', and 'Source Flows'. The 'Source Events' tab is active, showing a table with columns: Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype. The table contains several rows, with the row for 'ATD File Conviction - Patient Zero Quarantine' highlighted in yellow.

At the bottom, there's a 'Details' pane with tabs for 'Details', 'Advanced Details', 'Geolocation', 'Description', 'Notes', 'Custom Types', 'Source Events', 'Source Flows', and 'Correlation Details'. The 'Details' tab is active, showing fields for Application (ATD2ESM), Filename (Sample_zP9k2.exe), Host (atd02), Job_Name (426), Source User, File_Type (PE32+ executable (GUI) x86-64), and SHA1 (AE82EAFC8133248C6AF26A61F86F432AD8C1).

04:13:28 – New file seen for first time in enterprise

04:14:00 – Potential malware detection

04:14:54 – Sandbox analysis convicts executable

04:14:54 – Patient zero identified and quarantined



Correlated Event Triggers Alarm

The screenshot shows the 'Cyber Threat Indicators' interface. At the top, there's a search bar and a 'Current Day' filter. Below that is a table with columns: Indicator Name, Feed Name, Date Received, Backtrace Hit C..., and a download link. The main part of the interface is a list of events with columns: Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype. The event with severity 79 and rule 'Malware - Malware Sent from Internal Host' is highlighted. Below the list is a 'Details' section with tabs for 'Advanced Details', 'Geolocation', 'Description', 'Notes', 'Custom Types', 'Source Events', 'Source Flows', and 'Correlation Details'. The 'Advanced Details' tab is active, showing fields for Application, Filename, Host, Job_Name, Source User, File_Type, and SHA1.

Indicator Name	Feed Name	Date Received	Backtrace Hit C...	
This IOC has been generated during execution of D74441283CCFE8BF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6	download

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

Details	Advanced Details	Geolocation	Description	Notes	Custom Types	Source Events	Source Flows	Correlation Details
Application	ATD2ESM	Source User						
Filename	Sample_zP9k2.exe	File_Type	PE32+ executable (GUI) x86-64					
Host	atd02	SHA1	AE82EAFC8133248C6AF26A61F86F432AD8C1					
Job_Name	426							

04:13:28 – New file seen for first time in enterprise
04:14:00 – Potential malware detection
04:14:54 – Sandbox analysis convicts executable
04:14:54 – Patient Zero identified and quarantined
04:14:54 – High-severity event/alarm generated



File Reputation Changed

The screenshot shows a web-based interface for Cyber Threat Indicators. At the top, there's a navigation bar with icons and a 'Current Day' dropdown. Below that is a table with columns: Indicator Name, Feed Name, Date Received, Backtrace Hit C..., and a 'download' link. The first row contains the text 'This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2', 'TIE Use Case', '09/14/2015 06:01:48', and '6'. Below the table are tabs for 'Description', 'Details', 'Source Events', and 'Source Flows'. The 'Details' tab is active, showing a list of events with columns: Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype. The second event in the list is highlighted in yellow: Severity 25, Rule Message 'TIE File Reputation Change', Event Count 1, Source IP '::', Destination IP '::', Protocol 'n/a', Last Time '09/14/2015 04:14:58', and Event Subtype 'modify'. Below the event list are more tabs: 'Details', 'Advanced Details', 'Geolocation', 'Description', 'Notes', 'Custom Types', and 'Packet'. The 'Details' tab is active, showing a table with fields for 'Old_Reputatio...', 'New_Reputatio...', 'SHA1', and 'File_Hash'. The 'File_Hash' field contains the value 'D74441283CCFEEBF1A6B6A2B2E6F860D'. At the bottom left, there are navigation icons and 'Page 1'. At the bottom right, there is a small icon.

Indicator Name	Feed Name	Date Received	Backtrace Hit C...	
This IOC has been generated during execution of D74441283CCFEEBF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6	download

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

Details	Advanced Details	Geolocation	Description	Notes	Custom Types	Packet
Old_Reputatio...	0-REP_NOT_SET	New_Reputatio...	1-REP_KNOWN_DIRTY			
Old_Reputatio...	0-REP_NOT_SET	SHA1	0xae82eaefc8133248c6af26a61f86f432ad8ct			
New_Reputatio...	0-REP_NOT_SET	File_Hash	D74441283CCFEEBF1A6B6A2B2E6F860D			
New_Reputatio...	0-REP_NOT_SET					

04:13:28 – New file seen for first time in enterprise
04:14:00 – Potential malware detection
04:14:54 – Sandbox analysis convicts executable
04:14:54 – Patient Zero identified and quarantined
04:14:54 – High-severity event/alarm generated
04:14:58 – File reputation updated to 'malicious'



All Future Execution Attempts Blocked

The screenshot shows the 'Cyber Threat Indicators' interface. At the top, there's a navigation bar with 'Current Day' selected. Below it is a table with columns: Indicator Name, Feed Name, Date Received, Backtrace Hit C..., and a download link. The first row is highlighted in yellow.

Indicator Name	Feed Name	Date Received	Backtrace Hit C...	
This IOC has been generated during execution of D74441283CCFEF1A6B6A2	TIE Use Case	09/14/2015 06:01:48	6	download

Below the table are tabs: Description, Details, Source Events, Source Flows. The 'Details' tab is active, showing a list of events with columns: Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype.

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
25	TIE File Detection	1	172.25.108.156	::	n/a	09/14/2015 04:16:44	block
25	TIE File Reputation Change	1	::	::	n/a	09/14/2015 04:14:58	modify
79	Malware - Malware Sent from Internal Host	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	ATD File Conviction - Patient Zero Quarantine	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
100	Sample is malicious	1	172.25.109.113	::	n/a	09/14/2015 04:14:54	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert
70	Malware - Increasing Number of Malware Events Occurring	1	::	::	n/a	09/14/2015 04:14:00	infected
25	TIE File First Instance	1	172.25.108.155	::	n/a	09/14/2015 04:13:28	alert

At the bottom, there are more tabs: Details, Advanced Details, Geolocation, Description, Notes, Custom Types, Packet. The 'Details' tab is active, showing fields for Filename, Device_Action, New_Reputatio..., SHA1, and File_Hash.

Filename	SAMPLE_ZP9K2.EXE	SHA1	0xae82eaeefc8133248c6af26a61f86f432ad8ct
Device_Action	Block	File_Hash	D74441283CCFEF1A6B6A2B2E6F860D
New_Reputatio...	15-REP_ASSUMED_DIRTY		

Page 1

04:13:28 – New file seen for first time in enterprise
04:14:00 – Potential malware detection
04:14:54 – Sandbox analysis convicts executable
04:14:54 – Patient Zero identified and quarantined
04:14:54 – High-severity event/alarm generated
04:14:58 – File reputation updated to 'malicious'
04:16:44 – All subsequent attempts to execute file are automatically blocked



SIEM + MAR Search Options

The screenshot displays a SIEM interface with a table of events and a context menu. The table has columns for Event Count, Source IP, Destination IP, and Protocol. A context menu is open over the 'MAR Query' option, showing three sub-options: 'Historical process info from source IP, and time', 'Current process info from source IP and dest IP', and 'Historical Host information from source ip and a time range'.

Event Count	Source IP	Destination IP	Protocol
1	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a
2	10.10.10.10	10.10.10.10	n/a
7	10.10.10.10	::	n/a
2	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a
14	10.10.10.10	::	n/a
2	10.10.10.10	::	n/a
2	10.10.10.10	::	n/a
1	10.10.10.10	::	n/a

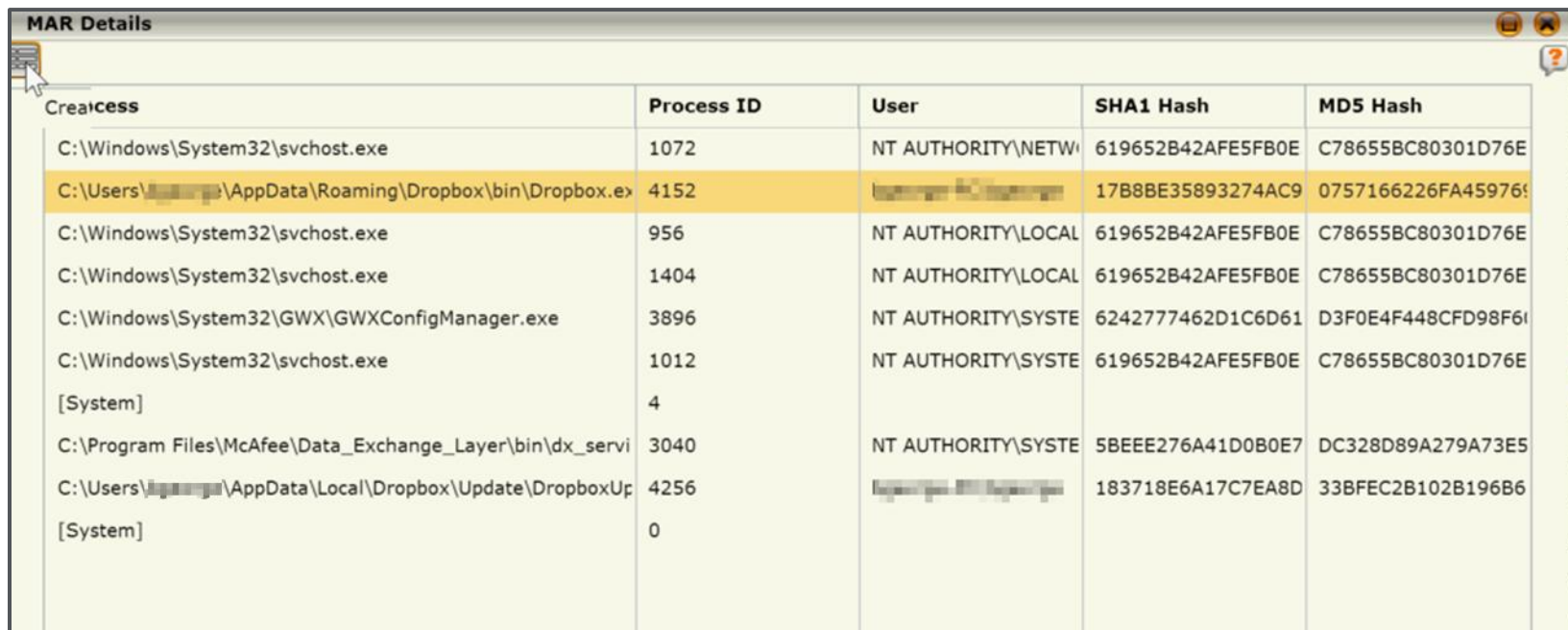
Context Menu Options:

- Historical process info from source IP, and time
- Current process info from source IP and dest IP
- Historical Host information from source ip and a time range

Bottom Bar: Details | Advanced Details | Geolocation | Description | Notes | Custom Types | Packet

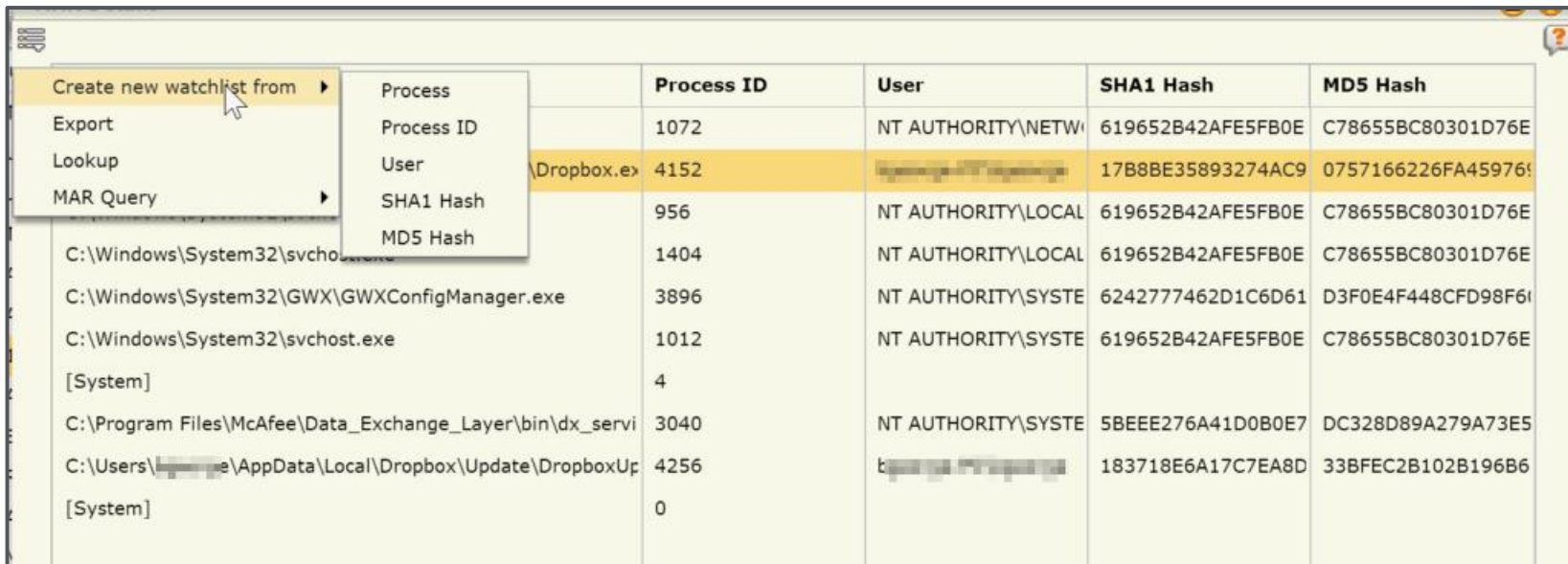
Message: 1107-.net runtime optimization service-.NET Runtime Optimization Service (clr_optimization_v4.0.30319_64) - Failed to execut

MAR Search Results (in SIEM)



Process Name	Process ID	User	SHA1 Hash	MD5 Hash
C:\Windows\System32\svchost.exe	1072	NT AUTHORITY\NETWORK	619652B42AFE5FB0E	C78655BC80301D76E
C:\Users\... \AppData\Roaming\Dropbox\bin\Dropbox.exe	4152	...	17B8BE35893274AC9	0757166226FA459769
C:\Windows\System32\svchost.exe	956	NT AUTHORITY\LOCAL	619652B42AFE5FB0E	C78655BC80301D76E
C:\Windows\System32\svchost.exe	1404	NT AUTHORITY\LOCAL	619652B42AFE5FB0E	C78655BC80301D76E
C:\Windows\System32\GWX\GWXConfigManager.exe	3896	NT AUTHORITY\SYSTEM	6242777462D1C6D61	D3F0E4F448CFD98F61
C:\Windows\System32\svchost.exe	1012	NT AUTHORITY\SYSTEM	619652B42AFE5FB0E	C78655BC80301D76E
[System]	4			
C:\Program Files\McAfee\Data_Exchange_Layer\bin\dx_servi	3040	NT AUTHORITY\SYSTEM	5BEEE276A41D0B0E7	DC328D89A279A73E5
C:\Users\... \AppData\Local\Dropbox\Update\DropboxUp	4256	...	183718E6A17C7EA8D	33BFEC2B102B196B6
[System]	0			

Add items to Watchlists



	Process ID	User	SHA1 Hash	MD5 Hash
C:\Windows\System32\svchost.exe	1072	NT AUTHORITY\NETWORK SERVICE	619652B42AFE5FB0E	C78655BC80301D76E
C:\Windows\System32\svchost.exe	4152	NT AUTHORITY\SYSTEM	17B8BE35893274AC9	0757166226FA45976E
C:\Windows\System32\svchost.exe	956	NT AUTHORITY\LOCAL SERVICE	619652B42AFE5FB0E	C78655BC80301D76E
C:\Windows\System32\GWX\GWXConfigManager.exe	1404	NT AUTHORITY\LOCAL SERVICE	619652B42AFE5FB0E	C78655BC80301D76E
C:\Windows\System32\GWX\GWXConfigManager.exe	3896	NT AUTHORITY\SYSTEM	6242777462D1C6D61	D3F0E4F448CFD98F6E
C:\Windows\System32\svchost.exe	1012	NT AUTHORITY\SYSTEM	619652B42AFE5FB0E	C78655BC80301D76E
[System]	4			
C:\Program Files\McAfee\Data_Exchange_Layer\bin\dx_service.exe	3040	NT AUTHORITY\SYSTEM	5BEEE276A41D0B0E7	DC328D89A279A73E5
C:\Users\user\AppData\Local\Dropbox\Update\DropboxUpdate.exe	4256	NT AUTHORITY\SYSTEM	183718E6A17C7EA8D	33BFEC2B102B196B6
[System]	0			

Identify Dormant Executables

The screenshot displays the McAfee ATD interface. The main window is titled 'Local ESM - Event Receiver - 4600 (135) - McAfee ATD' and shows a 'Cyber Threat Indicators' section. A table lists indicators, with one highlighted: 'This IOC has been generated during execution of D74441283CCFEFBF1A6B6A2B2E6F860 TIE Use Case' received on 09/14/2015 06:01:48 with a hit count of 6. Below this, a 'Source Flows' table shows event details for source IP 172.25.108.156. A context menu is open over the 'Execute remote command' option. An 'Execute Remote Command' dialog box is overlaid, listing various commands such as 'AbuseIPDB - Host', 'Blacklist', and 'MAR Search by Filename', which is currently selected.

Indicator Name	Feed Name	Date Received	Backtrace Hit Count	
This IOC has been generated during execution of D74441283CCFEFBF1A6B6A2B2E6F860	TIE Use Case	09/14/2015 06:01:48	6	download

Description	Event Count	Source IP	Destination IP
AbuseIPDB - Host	1	172.25.108.156	::
Blacklist	1	::	::
Disable Windows User	1	172.25.109.113	::
IPVoid - Dest IP	1	172.25.109.113	::
IPVoid - Source IP	1	::	::
MAR Search by Filename	1	172.25.108.155	::
MAR Search by MD5	1	172.25.108.155	::
MX Toolbox Dest IP	1	172.25.108.155	::
MX Toolbox Source IP	1	172.25.108.155	::
McAfee Threat Center - DIP	1	172.25.108.155	::
McAfee Threat Center - SIP	1	172.25.108.155	::
NTR Incident Drill Down	1	172.25.108.155	::

Custom Types	Packet
A1	0xae82eae8133248c6af26a61f86f432ad8
s_Hash	D74441283CCFEFBF1A6B6A2B2E6F860D

Name	Type
AbuseIPDB - Host	Launch URL
Blacklist	Execute Command
Disable Windows User	Execute Command
IPVoid - Dest IP	Launch URL
IPVoid - Source IP	Launch URL
MAR Search by Filename	Launch URL
MAR Search by MD5	Launch URL
MX Toolbox Dest IP	Launch URL
MX Toolbox Source IP	Launch URL
McAfee Threat Center - DIP	Launch URL
McAfee Threat Center - SIP	Launch URL
NTR Incident Drill Down	Execute Command
...	...

MAR Search Results (in MAR)

Menu ▾ Dashboards System Tree Queries & Reports Global IOC Artifact Analysis Policy Catalog Active Response Search ▾ Log Off ?

Systems

Active Response Search

Search

Click **Search** to get results or select a suggestion from the list.

Search for:

Quick filter:

	hostname	ip_address	os	full_name	md5	status	count ▾
<input type="checkbox"/>	CLIENT-0CPHR2	10.0.240.44	Microsoft Windows [Version 6.1.7601]	C:\Sample_zP9K2.exe	C2E1E6F8F7BA66AA2490D1FD37D7A045	current	1
<input type="checkbox"/>	CLIENT-NLATBV	10.0.240.114	Microsoft Windows [Version 6.1.7601]	C:\User_Agreement_LinkedIn.pd_	C2E1E6F8F7BA66AA2490D1FD37D7A045	current	1
<input type="checkbox"/>	CLIENT-5Z0G4M	10.0.13.55	Microsoft Windows [Version 6.1.7601]	C:\User\Sample_zP9K2.exe	C2E1E6F8F7BA66AA2490D1FD37D7A045	current	1
<input type="checkbox"/>	CLIENT-5Z0G4M	10.0.13.55	Microsoft Windows [Version 6.1.7601]	C:\User_Agreement_LinkedIn.pdf	A1526D1B39D10533AB45C81232400294	deleted	1
<input type="checkbox"/>	CLIENT-2WRCQ8	10.0.240.94	Microsoft Windows [Version 6.1.7601]	C:\Sample_zP9K2.exe	A1526D1B39D10533AB45C81232400294	deleted	1
<input type="checkbox"/>	CLIENT-D4HX9P	10.0.12.22	Microsoft Windows [Version 6.1.7601]	C:\User_Agreement_LinkedIn.pd_	C2E1E6F8F7BA66AA2490D1FD37D7A045	current	1

Walk the Entire Attack Chain

Time to Detect: 32s

04:13:28 – New file seen for first time in enterprise

04:14:00 – Potential malware detection

Time to Protect: 1m30s

04:14:54 – Sample submitted to ATD sandbox—identified as

04:14:54 – Patient Zero identified and quarantined

Time to Correct: 4s

04:14:58 – File reputation updated to 'malicious'

04:16:44 – All subsequent attempts to execute malicious file

00:00:00 – Search and remove all dormant version of malicious file

결론

- 우리의 공격 표면은 *지속적으로 증가*
- SIEM 과 인텔리전스는 *전략적으로 접근*
- 장기검출시간(Prolonged detection times) + 남은시간의 증가(increasing dwell time) = *보안상태를 감소(diminishing security posture)*
- 인텔리전스는 산업 표준화 *공통언어를 제공*
- *시간 (또는 일) 에서 초단위로 detect, correct* 자동으로 격차 감소
- 개선된 포렌식은 *분석가를 사냥꾼으로 변모*
- 적은 콘솔(Fewer consoles) + 원클릭 개선(one-click remediation) = *MTTR 감소 (mean time to respond)*



Learn more by visiting:

<http://www.mcafee.com/kr/products/siem/index.aspx>

