시스코의 지능형 위협 차단 전략
– AMP(Advanced Malware Protection)

Kwanjin Jung
APJC Security, Korea

July 2014

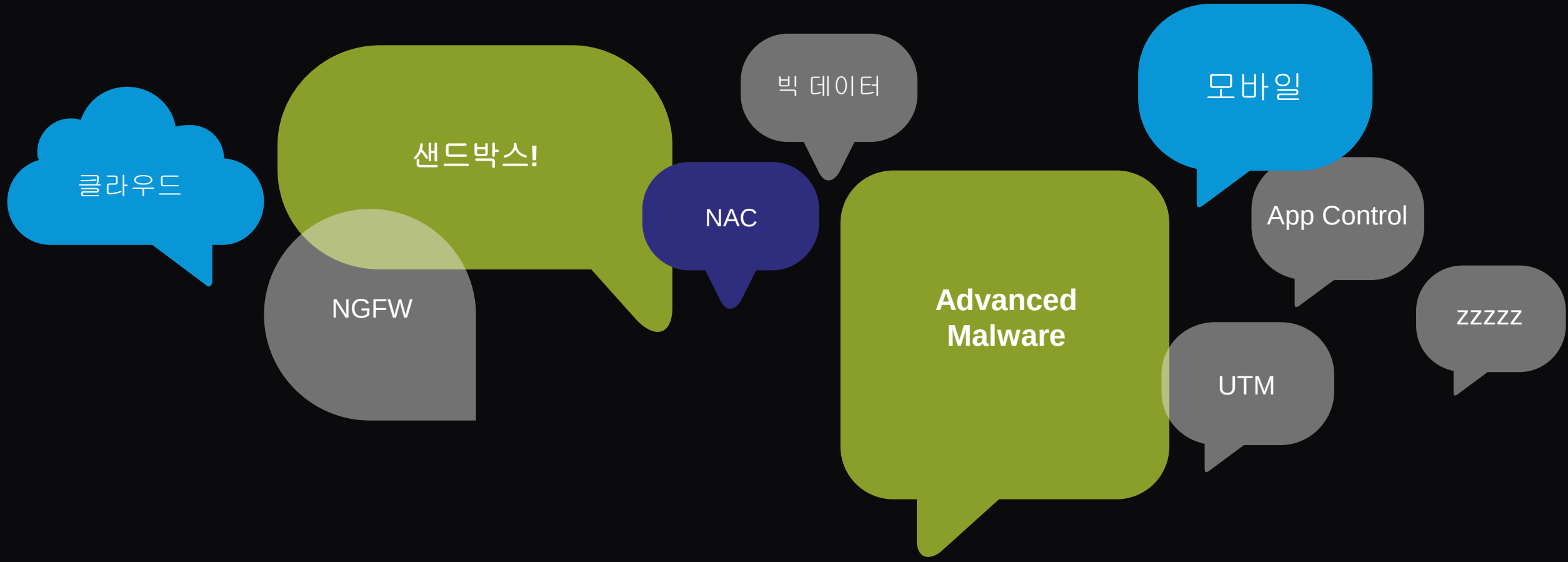
현 보안의 문제

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

마켓의 변신은 무죄



보안 문제는 멀리 있지 않습니다.

- 기업에 침투하기 위하여 해커는 전문적 기술을 통해 더욱 정교화 지능화 되고 있음
- 악성코드 또한 더욱 지능화되어 가고 있음

기업이 직면한 보안 문제

늘어나고 있는 다양한 보안 위협에 현재의 방법으로는, 지금의 문제를 해결하기가 어렵다.

- 제한된 시간
  - 기업은 악성코드 탐지에 몇일, 몇주 또는 몇달을 기다릴 여유가 없다. 빠른 대용 필요
- 제한된 지식
  - 악성코드 분석은 많은 리소스 사용과 분석에 많은 시간과 비용 소모
- 제한된 예산
  - 보안에 투자할 충분한 예산이 많지 않다. 보다 낮은 자원에 투자하는 것이 필요
- 제한된 가시성
  - 기업의 네트워크에서 무엇이 일어나고 있는지 들여다 보는 것이 쉽지 않다.

현실: 기업은 계속 공격 진행 중

- "95% 의 많은 기업들이 악성코드 트래픽에 의한 공격대상이 되었고, 100% 기업들이 악성코드에 감염된 웹 사이트에 접근하였다." -2014 Cisco Annual Security Report

- 네이트 개인정보 유출, 2011년 7월
  - 가입자 3,500 만명의 개인정보 유출

- Neiman Marcus 데이터 유출
  - 350,000 신용카드 정보

- Target 데이터 유출, 2013년 12 년
  - 4천만명의 신용카드 정보 유출
  - 7천만명의 개인 정보 유출

- ...그리고 더 많은 기업들

Neiman Marcus

오늘날 위협 : 위협의 진화와 전통적 방법의 회피

오늘날 보안한다 하면 이거 하나 쯤은 다 가지고 있죠 – FW, IPS, AV

하지만, 이런 솔루션만으로는 충분하지 않습니다.

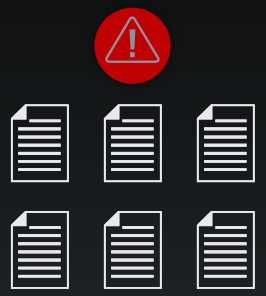
지능형 위협의 진실

침해사고 발생

침해당한 60% 데이터가 1시간 이내에 유출

54% 는 한달 이내에 발견되지 못하고 남아있음

과거3년동안 블랙마켓에서 거래된 자료는 **7억5천만명** 이상



START

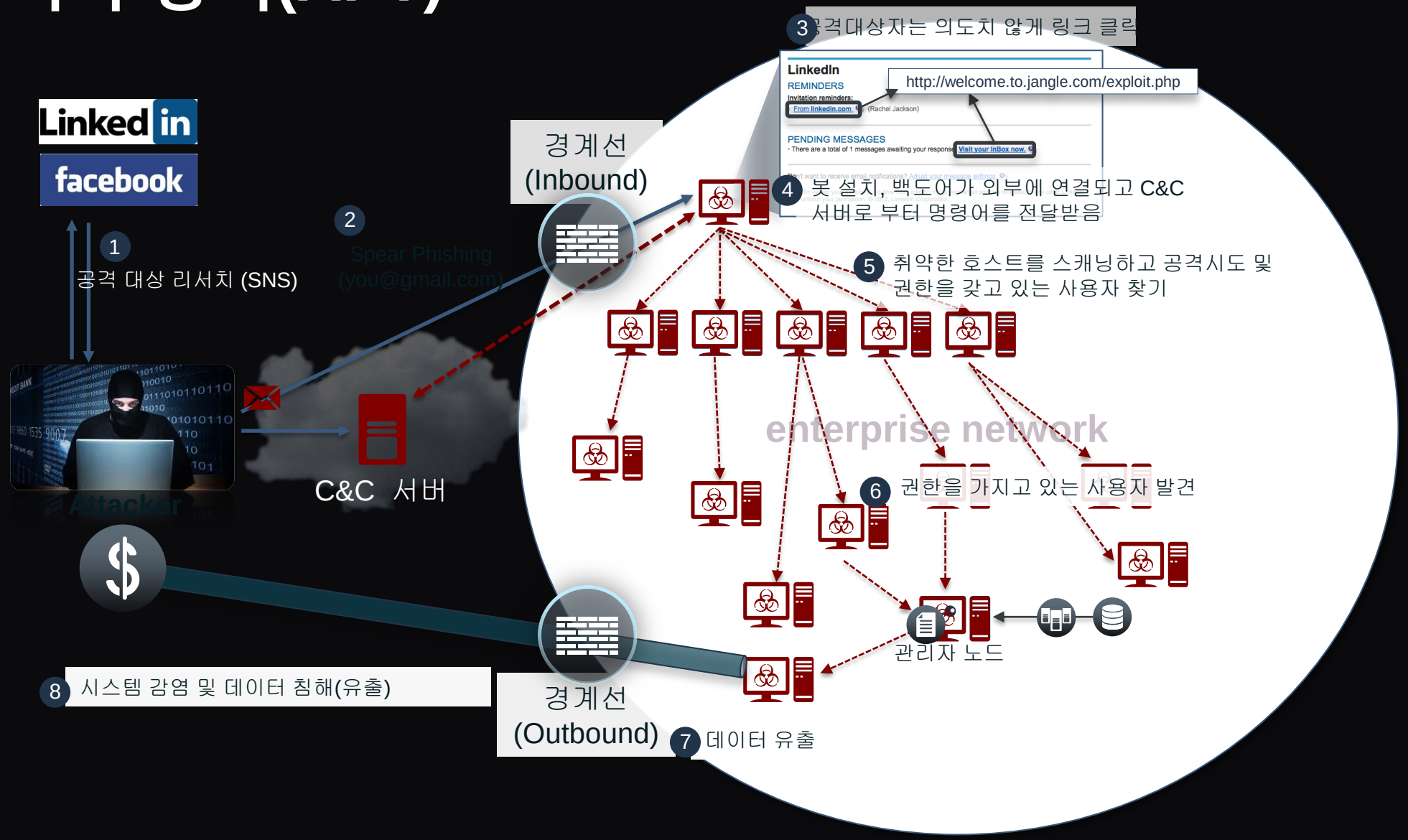
HOURS

MONTHS

YEARS

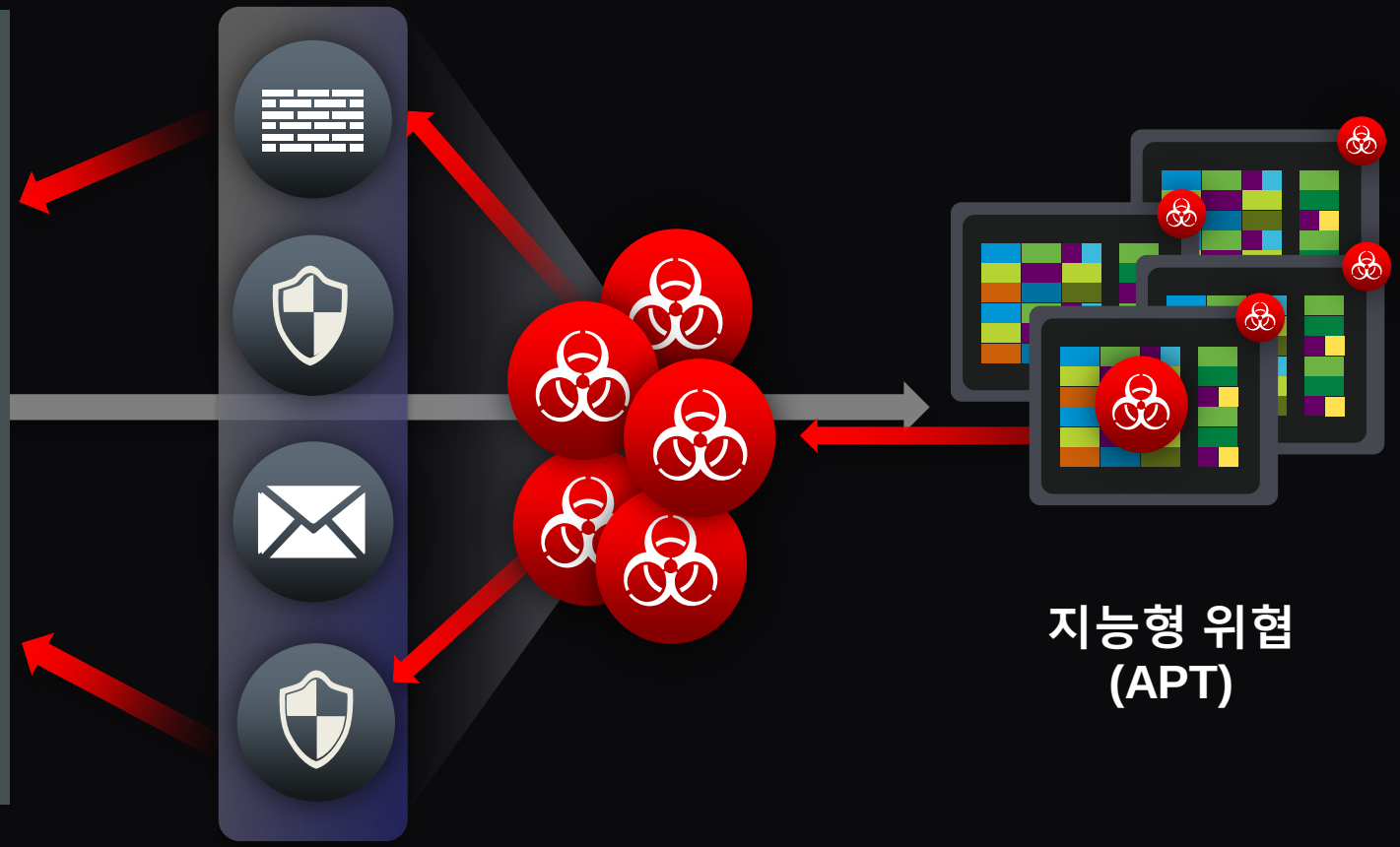
Source: Verizon Data Breach Report 2014

지능형 지속 공격(APT)



만약 악성코드가 시스템에 침입하였다면 ?

- 어디서 부터 시작한 것일까 ?
- 현재 상황이 얼마나 심각한가 ?
- 시스템들이 얼마나 영향을 받았나?
- 악성코드가 무엇을 했나 ?
- 어떻게 하면 복구할 수 있나 ?
- 다시 이러한 상황이 반복되지 않으려면 ?

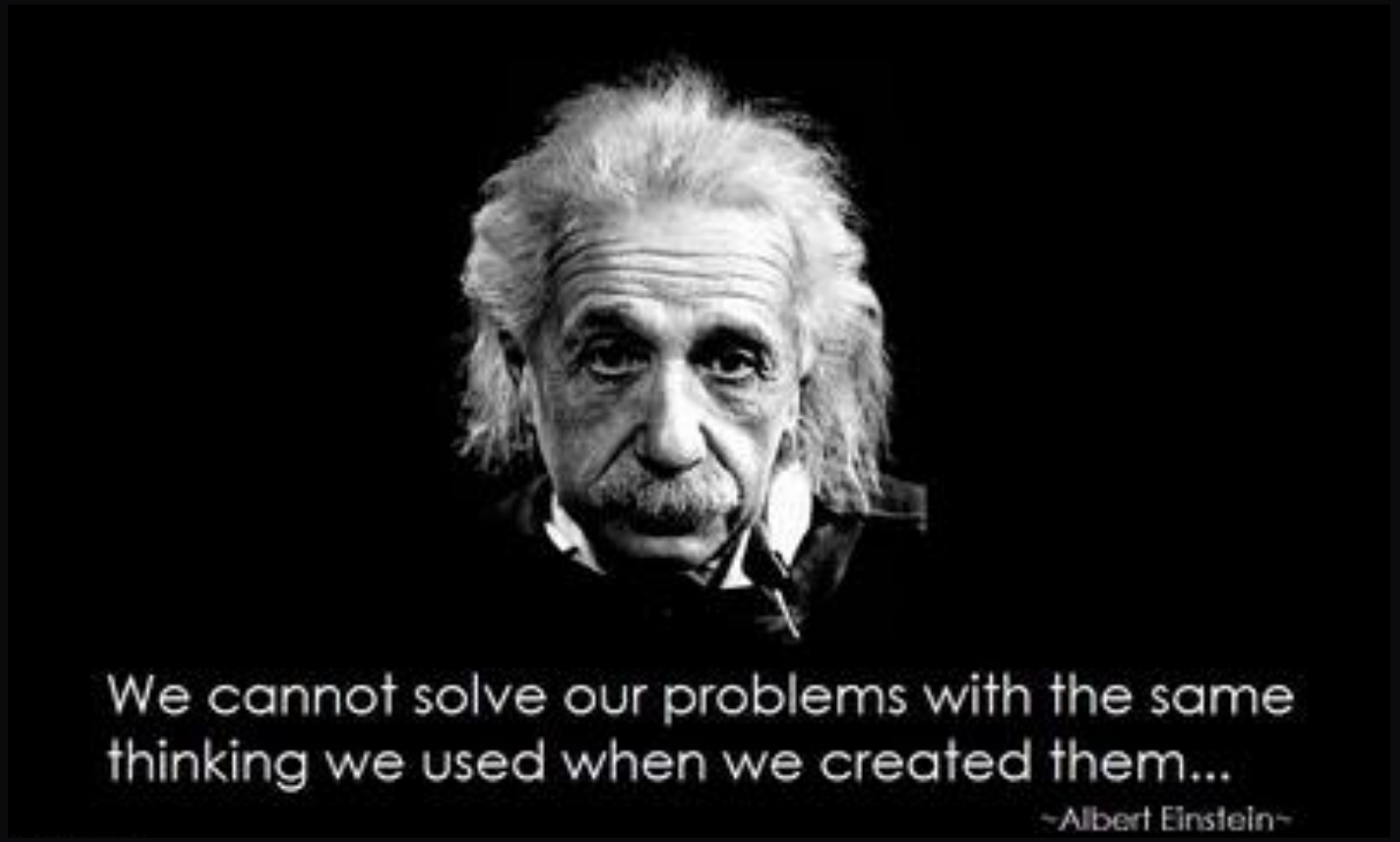


Tell the Story

악성코드의 스토리를 말하다

WHO, WHAT, WHEN, WHERE, HOW

HOW ?



1

Before

공격을 사전에 방어하라

2

During

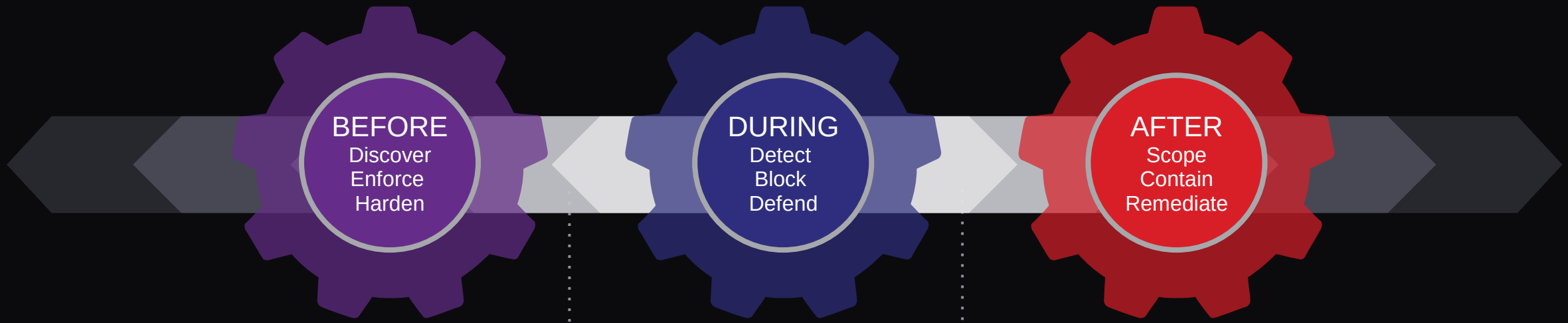
가시성 확보를 통한 감염시스템 판단과
감염원인 추적

3

After

감염시스템 추적과 지속적인 감염 차단

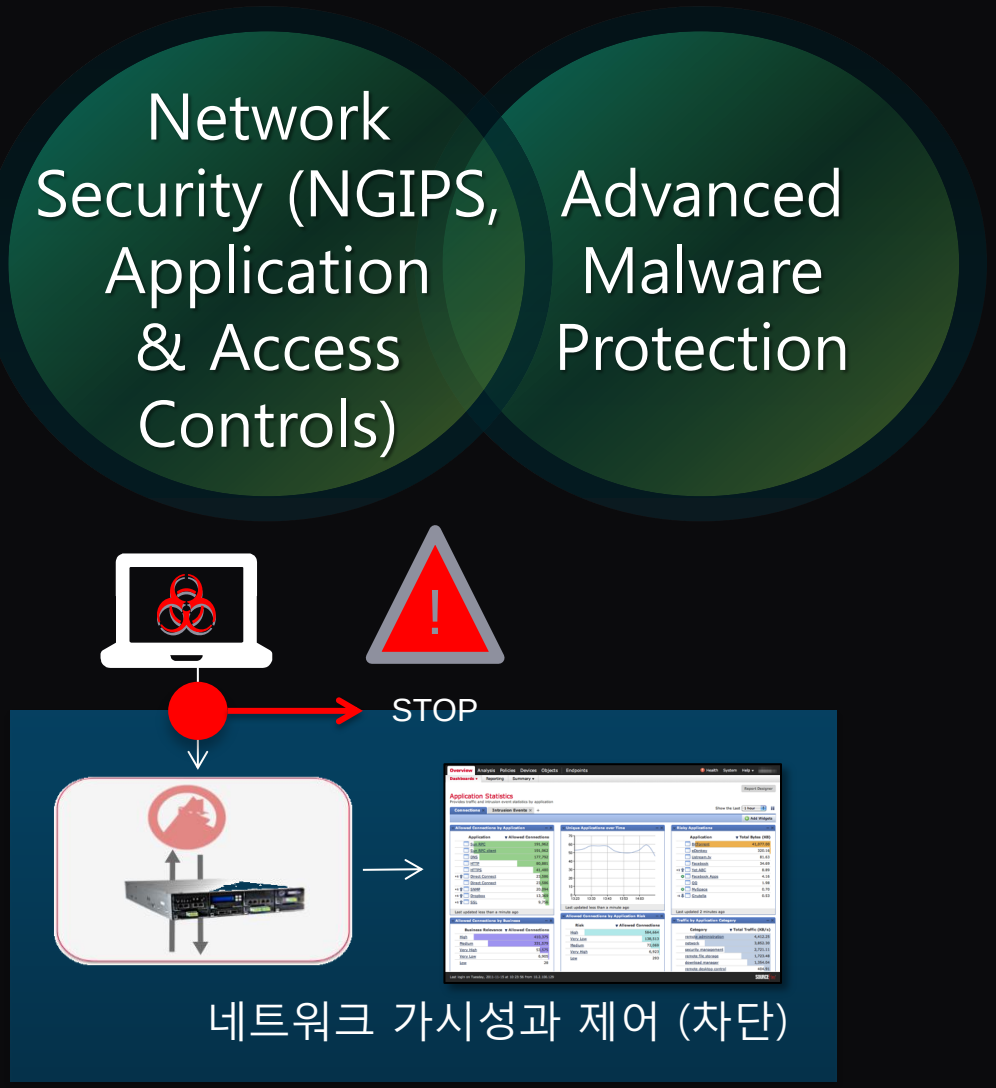
여기 새로운 방안을 여러분에게 소개합니다.



공격에 대한 전체 과정을 충분히 이해해야 합니다.

Filtering	Malware Signature	File Retrospection
Usage Controls	File Reputation	Threat Analytics
Reputation	File Behavior	Actionable Reporting

Better Together

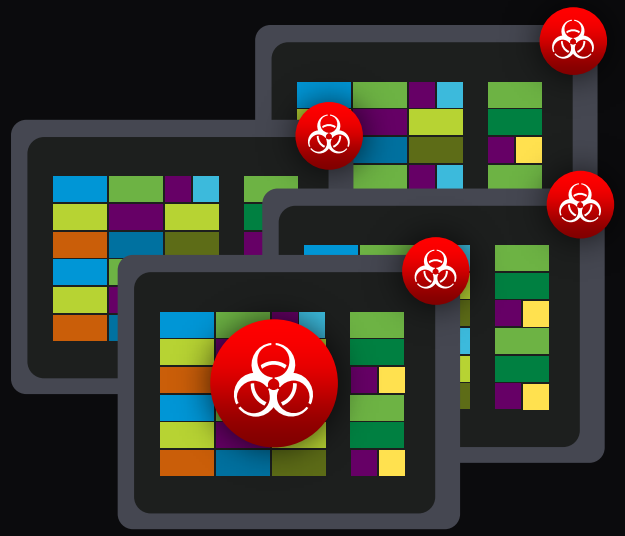


네트워크와 앤드포인트단까지 통합된 AMP 전략

오늘날 지능형 위협을 차단하기 위해서는 멀티 레이어 차단 전략이 필요합니다. AMP 기능과 NGIPS 기능이 함께하면 더 좋은 이유가 여기에 있습니다.

내부에 악성코드가 감염되기전 사전에 내부 시스템이 외부의 위협으로부터 안전하게 보호되면 어떨까요? 내부 유입전 Before 단계의 사전 차단이 중요한 이유입니다.

AMP 가 무엇인가요 ?



AMP(Advanced Malware Protection) 는

지능형 악성코드 차단 시스템으로 APT 와 같은 지속적인
위협 공격에 효과적으로 대응할 수 있는 솔루션입니다.

어떤 사용자가 무엇을 통해 어디서 언제 어떻게 위협으로부터
영향을 받았는지 알 수 있다면 어떨까요?

단순히 악성코드가 유입되었다는 것을 알려주고 샌드박스를 통해 분석 정보를
제공해주는 것만으로 끝나서는 지능화된 위협으로부터 안전해 질 수 없습니다.
전방위적인 가시성을 제공해주고 그것을 보고 제어할 수 있어야 합니다.

AMP Key Feature

악성코드 탐지 차단	• 디바이스 감염전 악성코드의 차단
회귀적 탐지	• 파일의 지속적 분석
파일 추적	• 문제가 되는 악성코드 영역 빠른 파악
디바이스 추적	• 감염원인의 파악 분석
위협지표, 감염원인	• 자동화된 감염시스템 분석 및 감염원인 파악
파일 상세 분석	• 샌드박스를 통한 빠르고 안전한 파일 분석
Outbreak Control	• 악성코드 전파 확산을 빠르게 차단

Cisco Advanced Malware Protection

Cisco® SIO

Email Endpoints Web Networks IPS Devices

1.6 million
글로벌 센서

35%
전세계 이메일 트래픽

100 TB
매일 전달받는 데이터

13 billion
웹 요청

150 million+
설치된 앤드포인트

24x7x365
운영

600+
엔지니어, 기술자, 연구원

40+
언어

Sourcefire VRT® (Vulnerability Research Team)

매일 180,000+ 샘플 파일

FireAMP™ 커뮤니티

Advanced Microsoft and Industry Disclosures

Snort and ClamAV 오픈소스 커뮤니티

허니팟

소스파이어 AEGIS™ 프로그램

Private and Public Threat Feeds

Dynamic Analysis

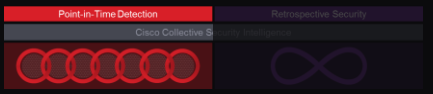
Cisco Collective Security Intelligence

AMP
Advanced Malware Protection

지속적인 위협 분석 – 어떻게 판단해야 하나 ?

지능적인 탐지, 추적, 대응

지능형 악성코드 탐지를 위한 다단계 방어층



평판 필터링

행동기반 탐지

One-to-One Signature

Fuzzy Finger-printing

Machine Learning

Indications of Compromise

Dynamic Analysis

Advanced Analytics

Device Flow Correlation

가시성을 통해 A-Z 까지

Who

어떤 사용자가
처음 접근했나

What

어떤
애플리케이션이
영향을 받았나

Where

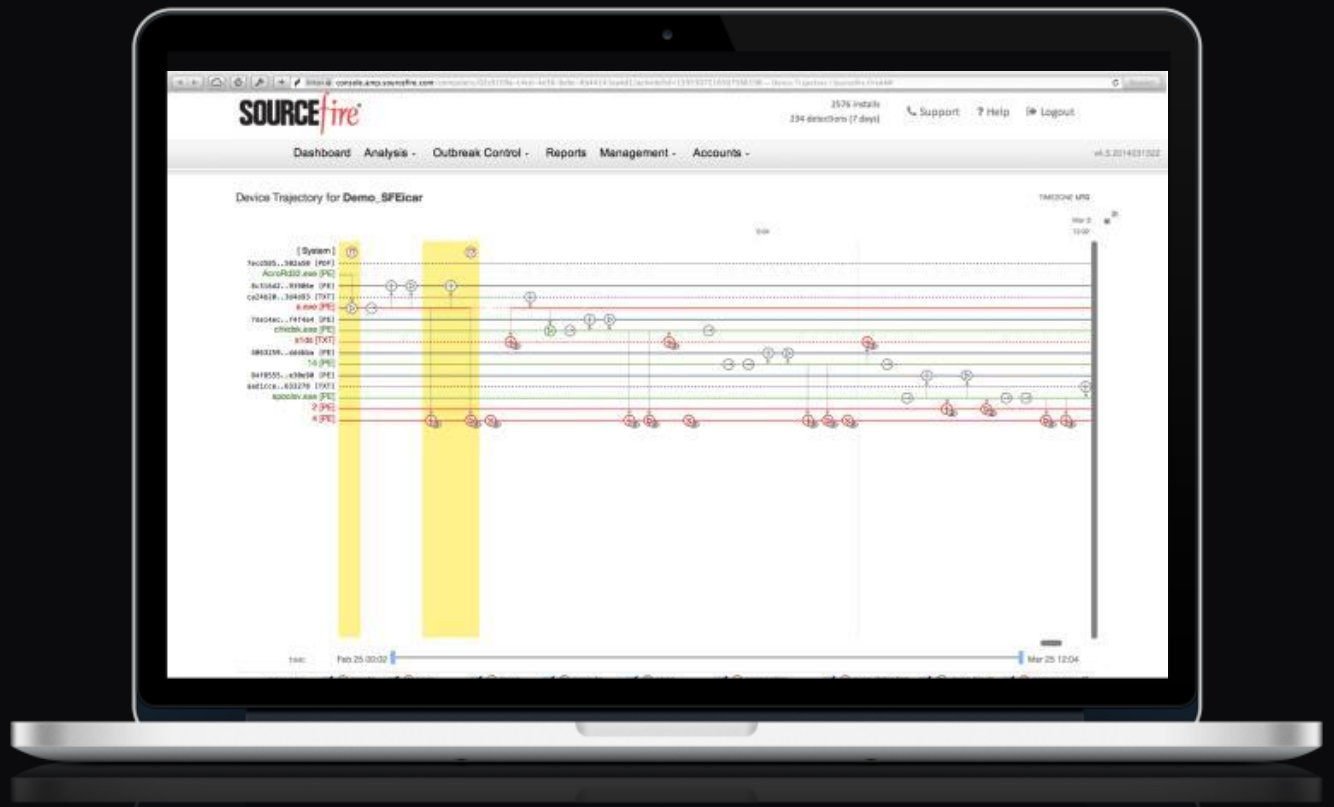
침해당한 영역 범위

When

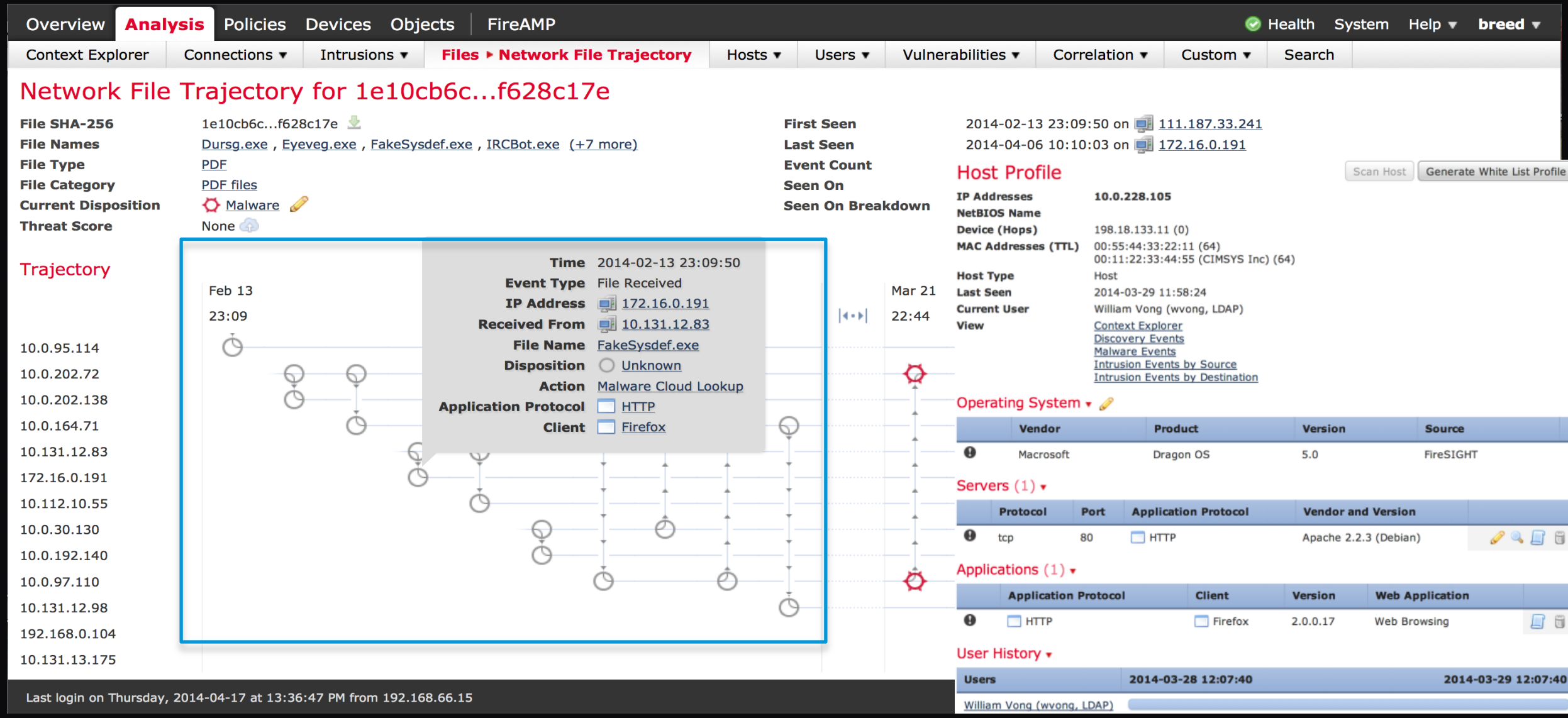
위협에 노출된
시간과 타임라인

How

위협의
진행상황과
감염원인



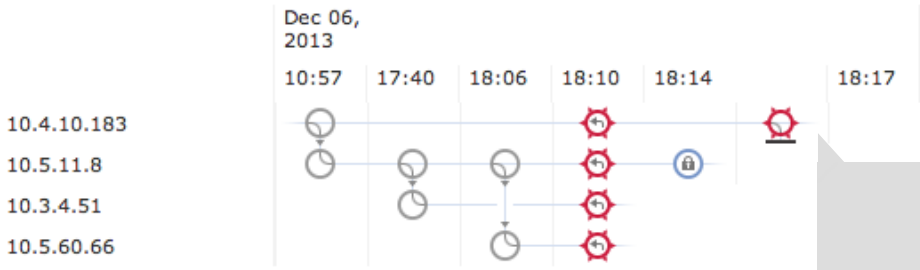
네트워크 기반의 경로 추적, 타임라인



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	High		

Trajectory



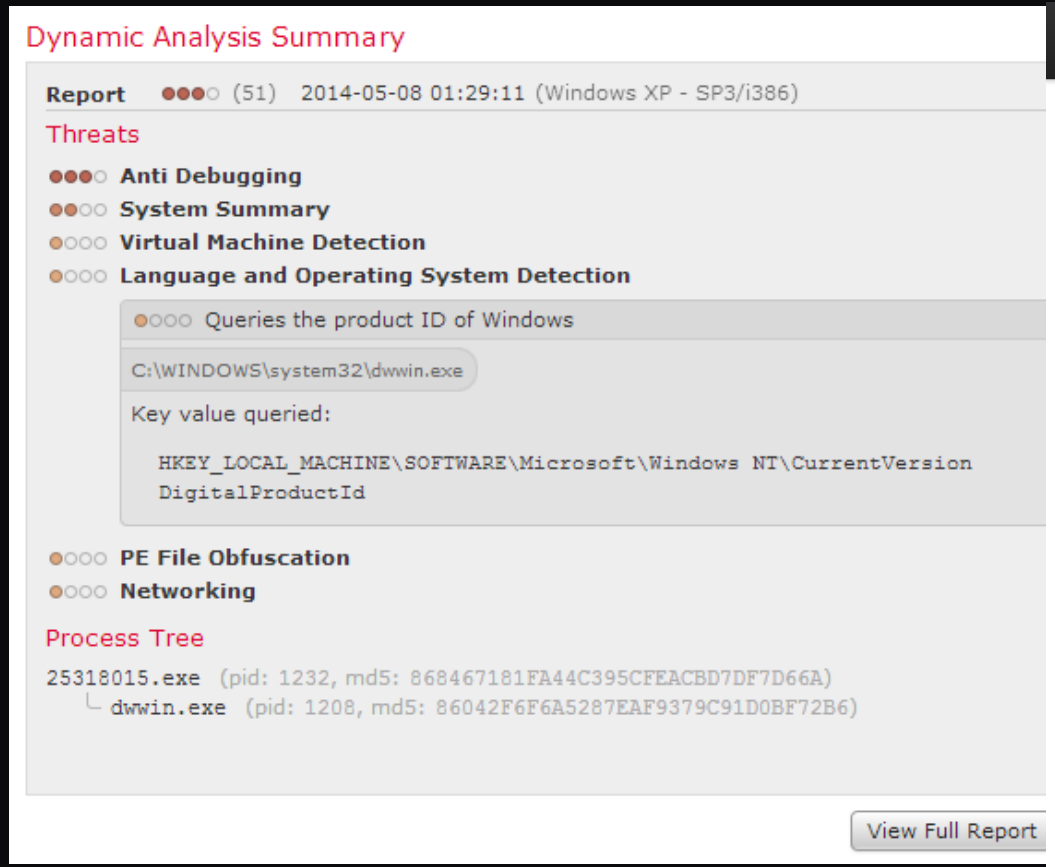
Time 2013-12-06 18:17:27
Event Type File Sent
IP Address 10.4.10.183
Blocked Recipient 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action Malware Block
Application Protocol HTTP
Client Firefox

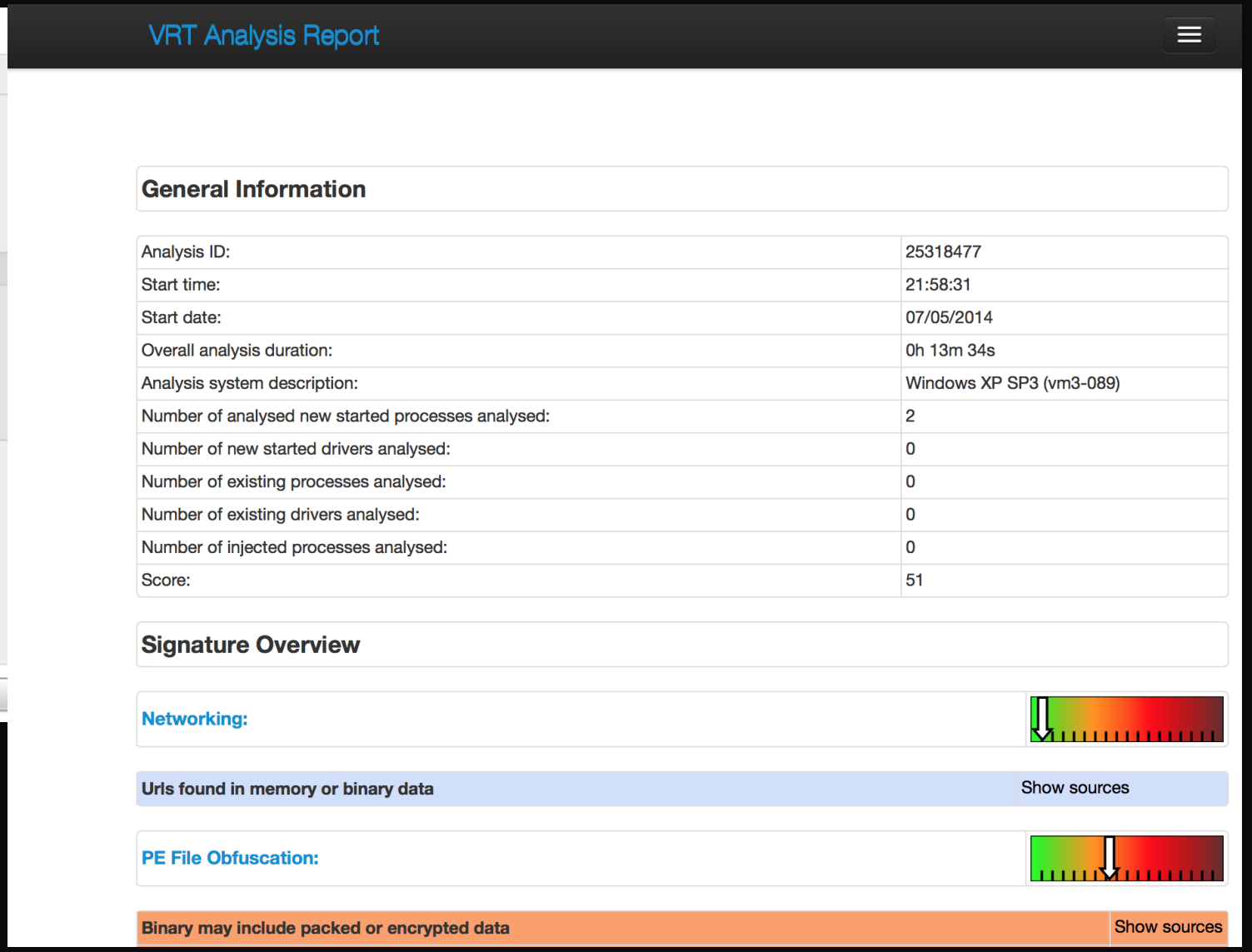
첫 공격후 8시간이 지난 시점에 악성코드는 초기 진입하였던 지점을 통해 재시도하려고하나 악성코드로 인지되어 차단됨

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

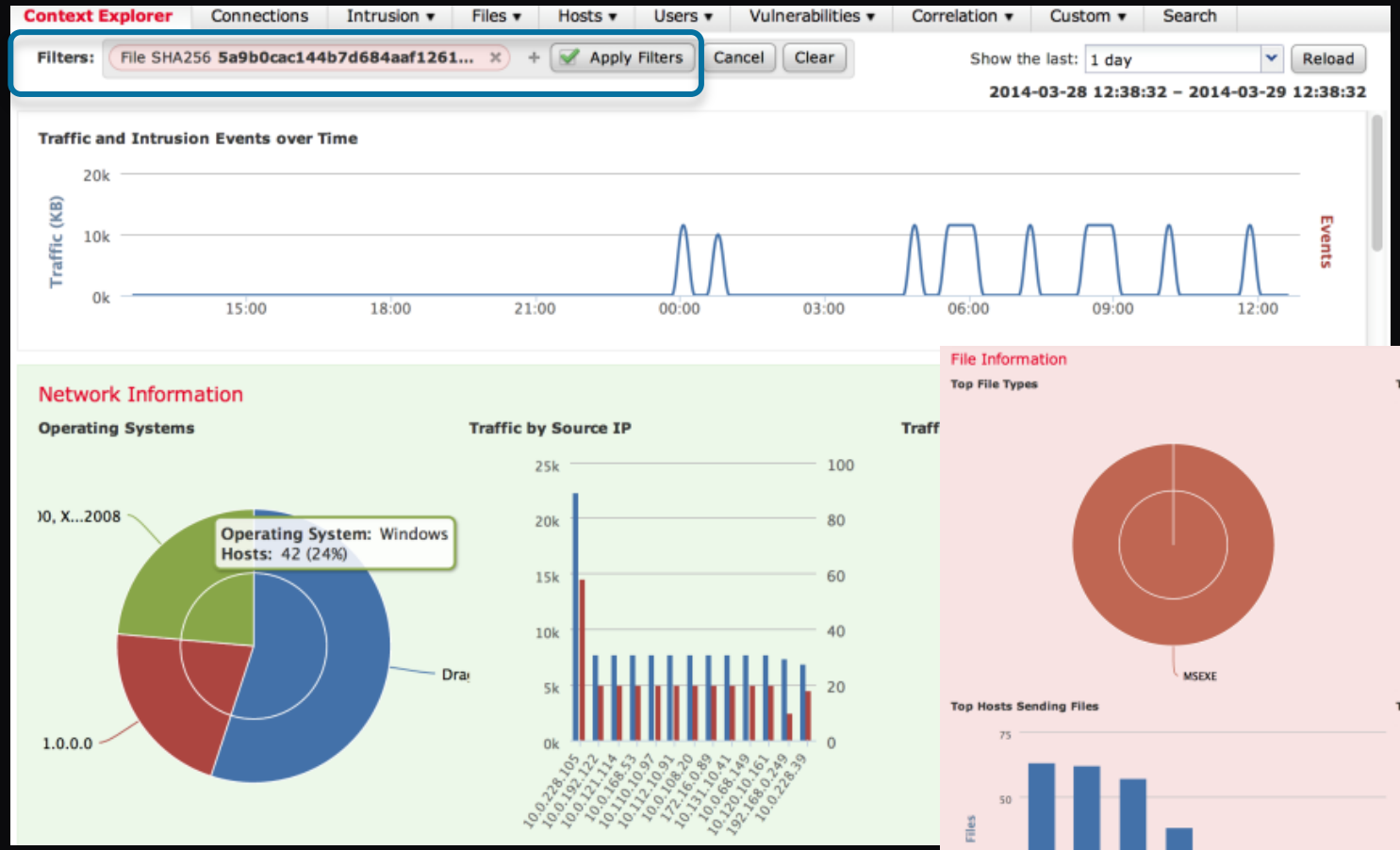
File Analysis – 파일 세부 행동분석

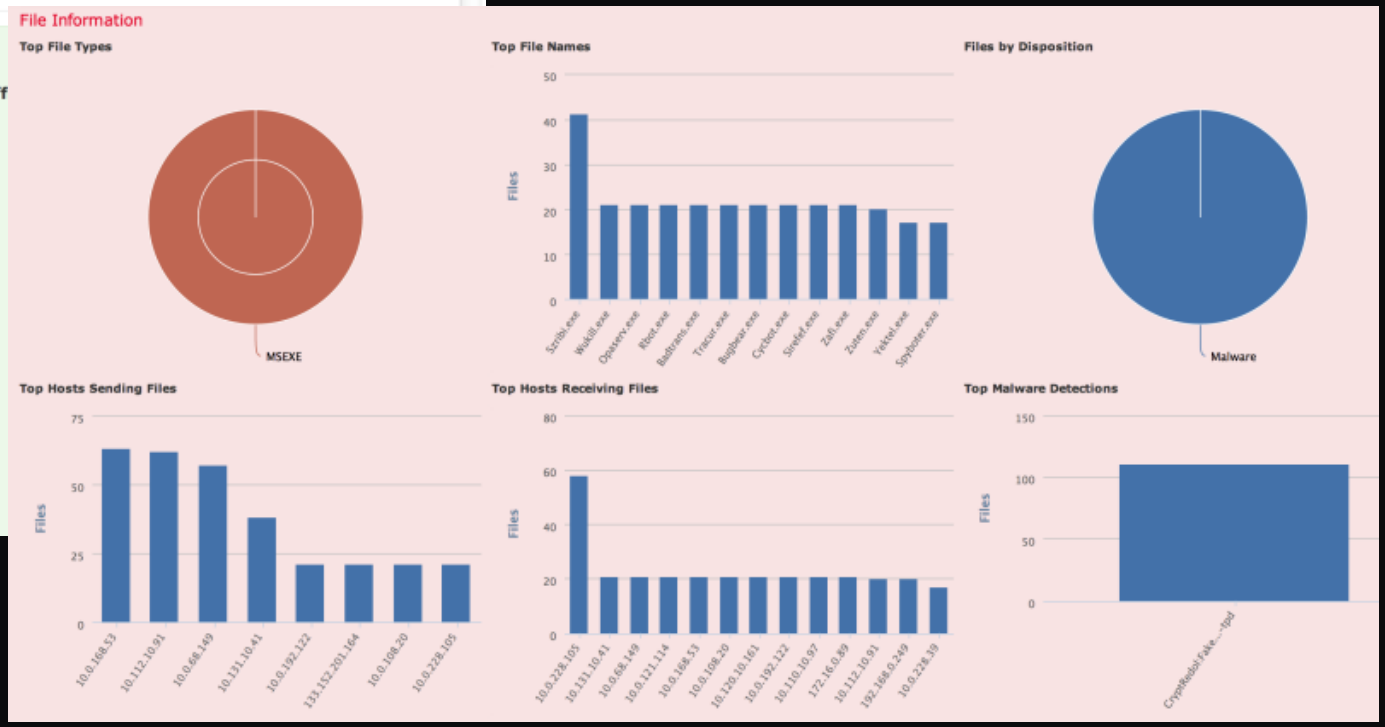




파일을 동적분석하여 얻은 모든 정보를 보여준다. 위협 스코어와 요약정보 그리고 각 컴포넌트별 세부정보가 있다.

탐색기를 통한 다양한 통계 정보 확인





필터를 통해 특정 기준 중심으로 정보 출력
- 시간대별 탐지 그래프
- 네트워크 기반 정보
- 어플리케이션 정보
- 침입 관련 정보, 파일 정보
- GeoLocation 정보, URL 정보

시스템 감염경로 상관관계

호스트 기반의 모든 네트워크 행동을 기록하라

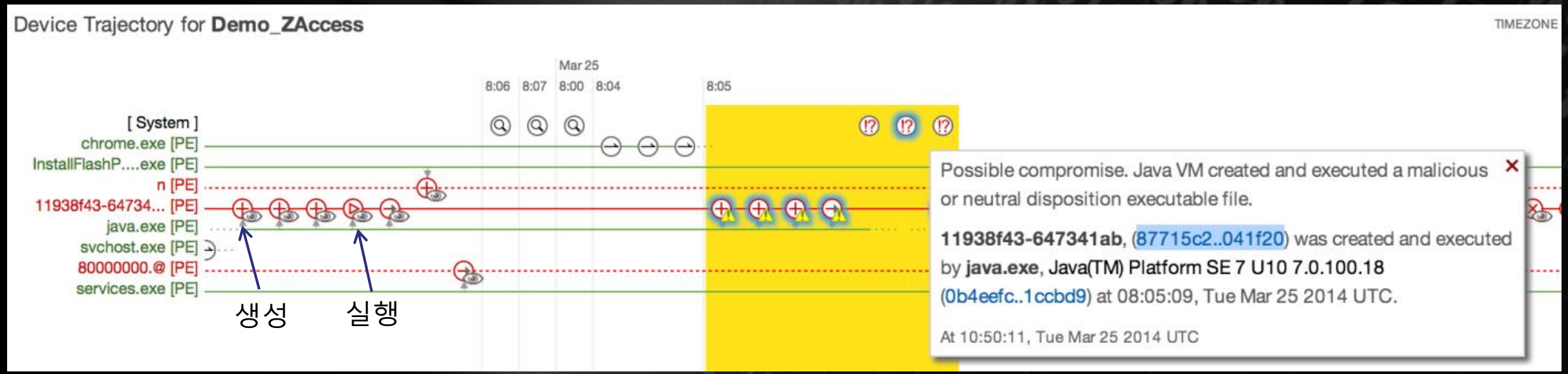
가시성 확보

모든 TCP/UDP 트래픽 추적

어떤 웹 사이트(URL)로부터 악성코드가 다운로드 되었나 ?

악성코드가 외부와 통신을 한적이 있는가 ?

어떤 호스트가 알려진 C&C 서버와 접속했나 ?



위협지표 (Indication of Compromise)

Indications of Compromise

Demo_ZAccess — Mark Resolved

Threat Detected , Java compromise , Executed malware , Potential Dropper Infection

Demo_SFEicar — Mark Resolved

Threat Detected , Adobe Reader compromise

Host Profile

Scan Host | Generate White List Profile

IP Addresses	165.13
NetBIOS Name	
Device (Hops)	165.132.(
MAC Addresses (TTL)	00:11:5D:16:88:C0 (CISCO SYSTEMS, INC.) (252) 00:11:5D:16:8A:40 (CISCO SYSTEMS, INC.) (252)
Host Type	NAT Device
Last Seen	2014-05-10 00:08:04
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (2)

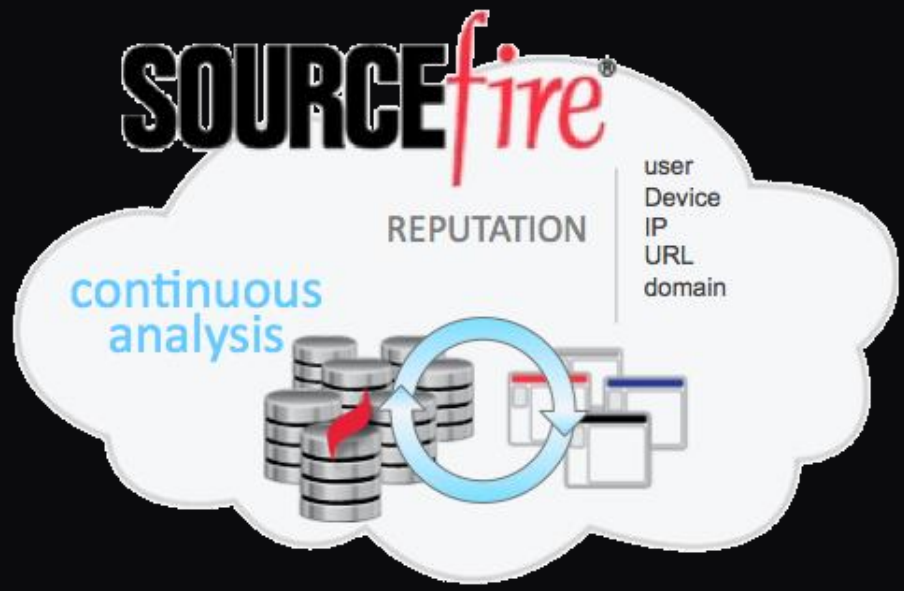
Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2014-05-09 23:59:33	2014-05-09 23:59:33
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2014-05-09 23:53:54	2014-05-09 23:53:54

Systems (3)

Edit Operating System | View Operating Systems

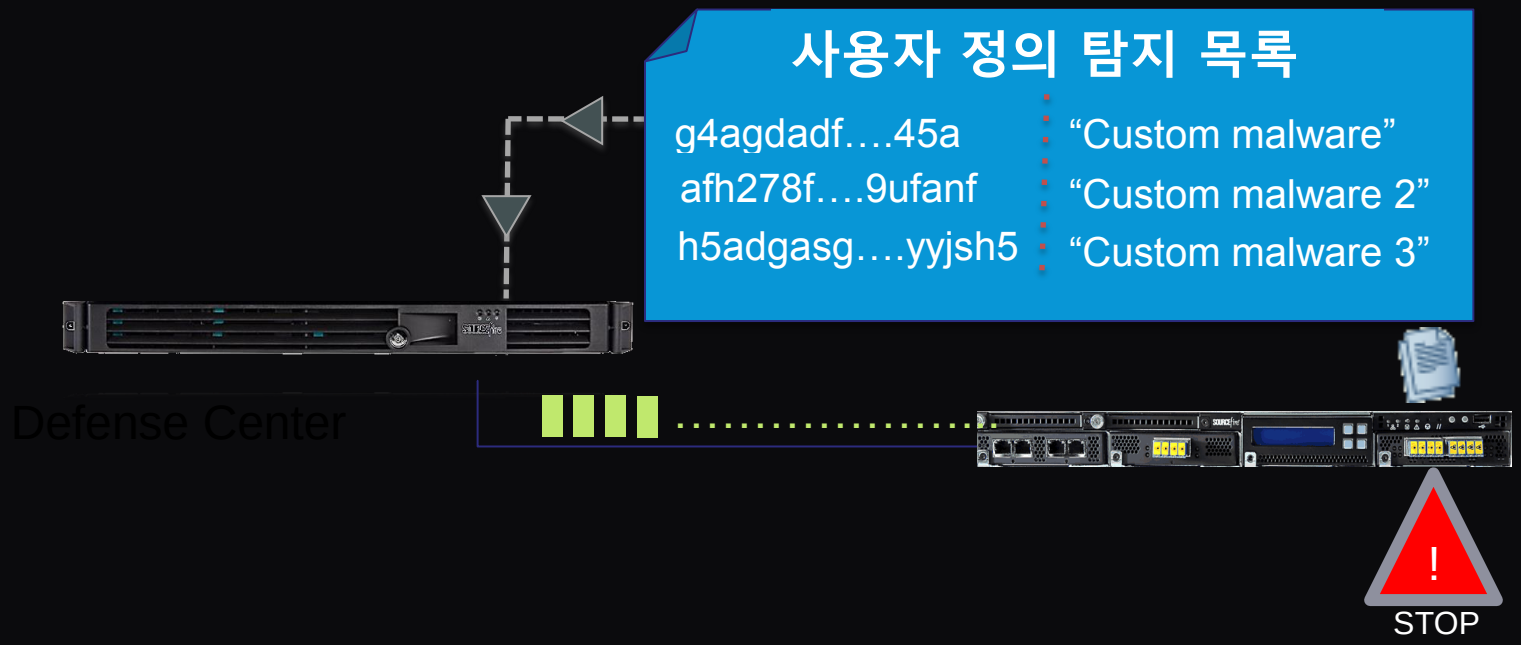
Hardware	OS Vendor	OS Product	OS Version	Source
	Microsoft	Windows	8, 8.1	FireSIGHT



- 빅데이터 분석을 통해 감염이 의심되는 시스템을 우선 강조해주는 위협지표
- 사용자 네트워크 환경에서 발생한 지능형 악성코드를 조사할 수 있도록 작업흐름을 제공해준다.

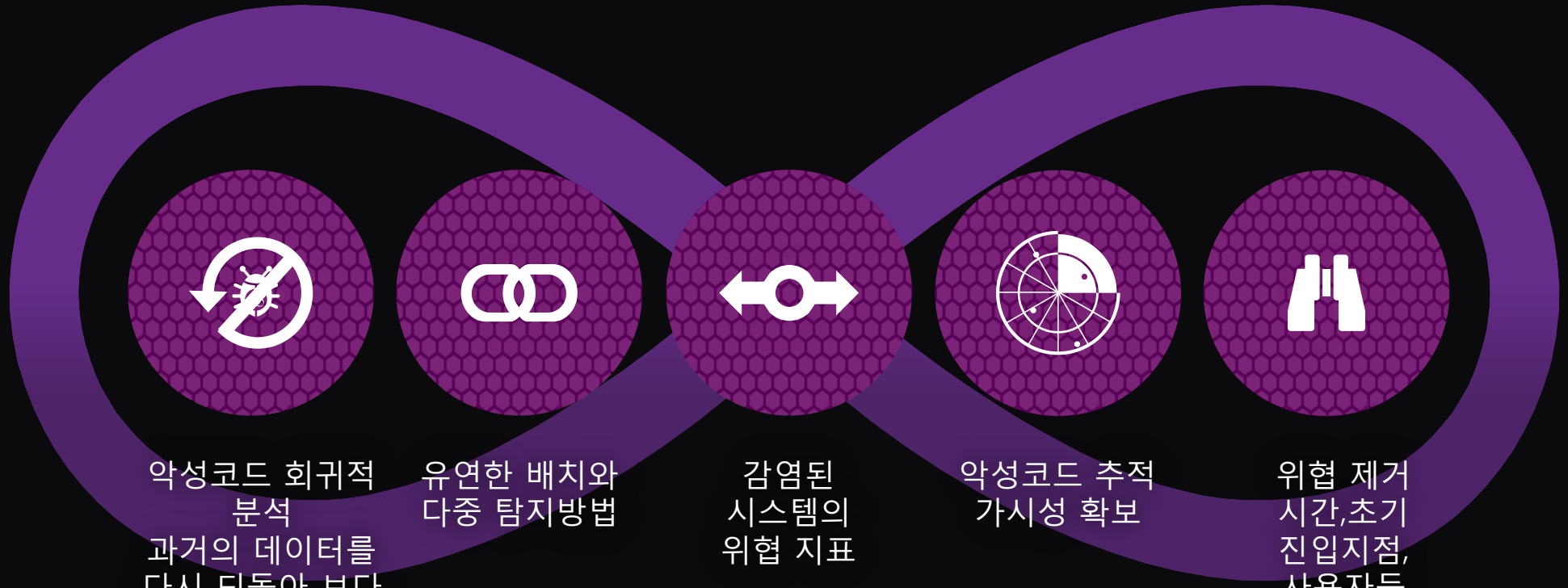
사용자 정의 탐지를 통한 긴급제어 – Outbreak Control

- 의심스러운 파일이 탐지될 경우 시그너처 패턴이 업데이트 될때까지 기다리지 않고 바로 적용
- 사용자가 정의한 파일의 탐지, 추적 그리고 차단



제어방법
Simple Custom Detections
Advanced Custom Signatures
Application Blocking Lists
Custom Whitelists

Key Differentiators



네트워크부터 엔드포인트까지 전방위 APT 대응
Not point in Time

AMP 플랫폼

AMP for Content

- ESA
- WSA
- CWS

SOURCEfire

- Continuous File Analytics
- Reputation Determination

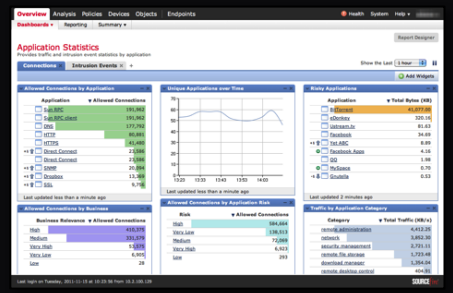
fireAMP™

- 지속분석
- 평판 기반 탐지
- 샌드박스

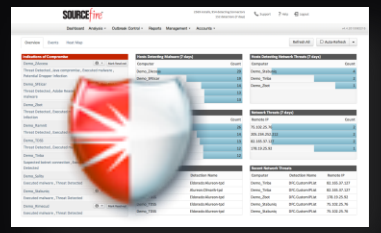
AMP for Networks

- 유연한 배치
  - NGIPS 기능
  - NGFW 기능
  - AMP 전용
- 악성코드 탐지/차단
- 파일 탐지/차단
- C&C 탐지/차단

AMP for Private Cloud



- 중앙집중화된 관리
- GUI 환경
- 다양한 정보의 순쉬운 확인



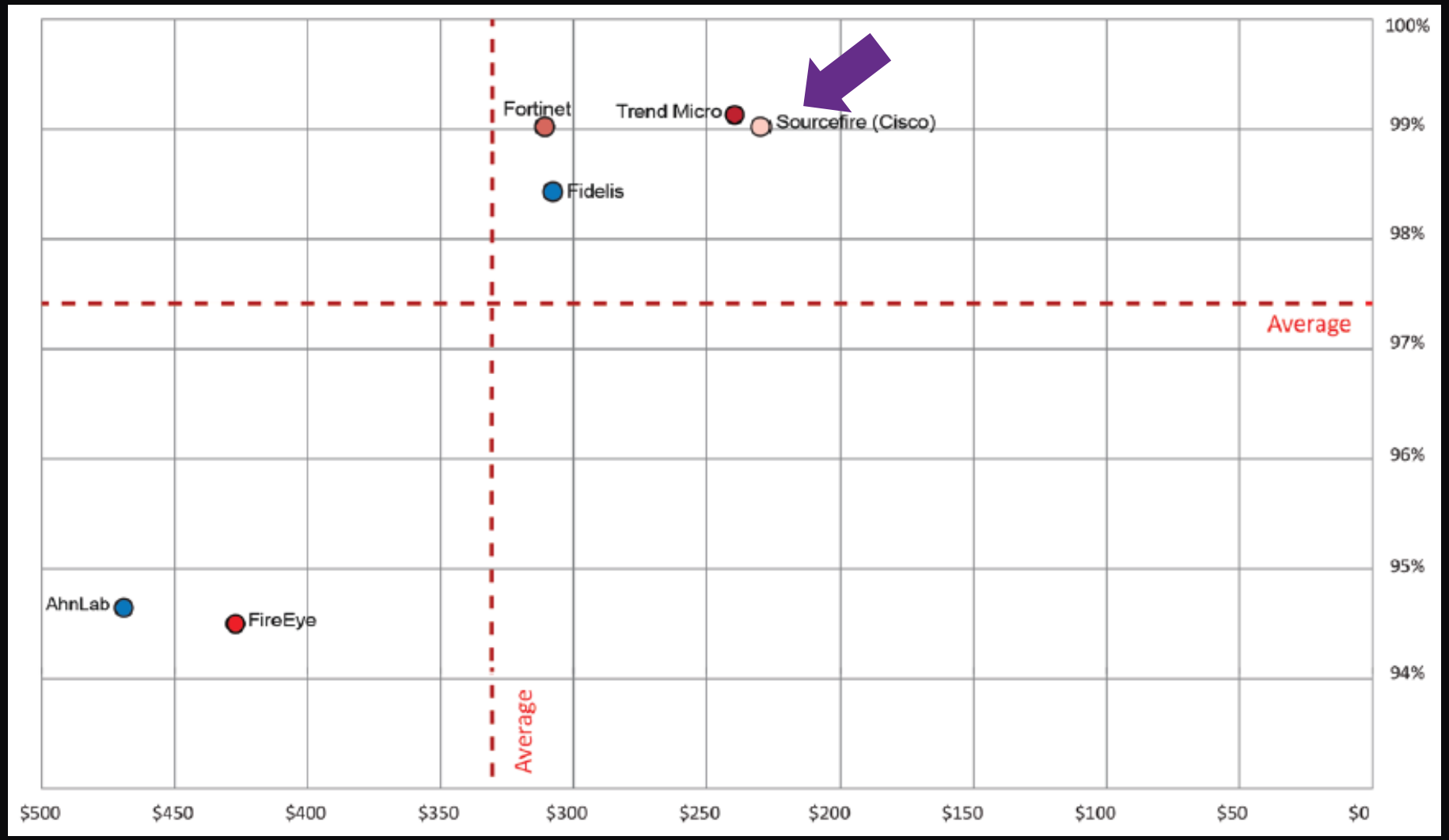
AMP for Endpoints

- PC, mobile 지원
- 악성코드 탐지
- 자동화된 위협지표 생성
- 추적
- 파일 분석
- 긴급 제어

NSS Labs 결과

시스코 AMP는 보안평가, TCO 그리고 차단에서 최고 성능을 보여줌

NSS Labs Security Value Map (SVM) for Breach Detection Systems



Cisco Advanced Malware Protection

Best Protection Value

99.0% Breach Detection Rating

Lowest TCO per Protected-Mbps

Summary

가시성

여러분들의 네트워크를 알고,
위협을 인지하라

회귀적 분석

과거로의 회귀 그리고
지속적인 분석

긴급상황 제어

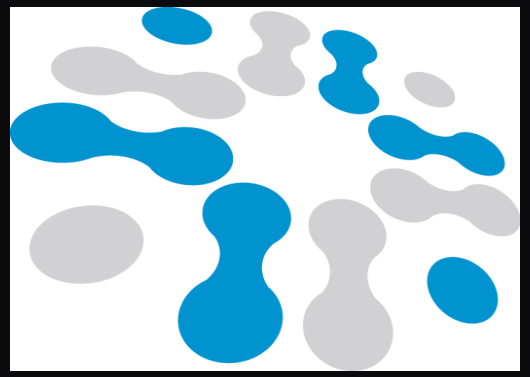
통합된 대응환경

다 단계 방어층을 이용한 전방위적인 차단
Better Together

ThreatGRID

ThreatGRID 소개

ThreatGRID 는 확장성, 통합된 악성코드 분석 및 위협 인텔리젼스 솔루션

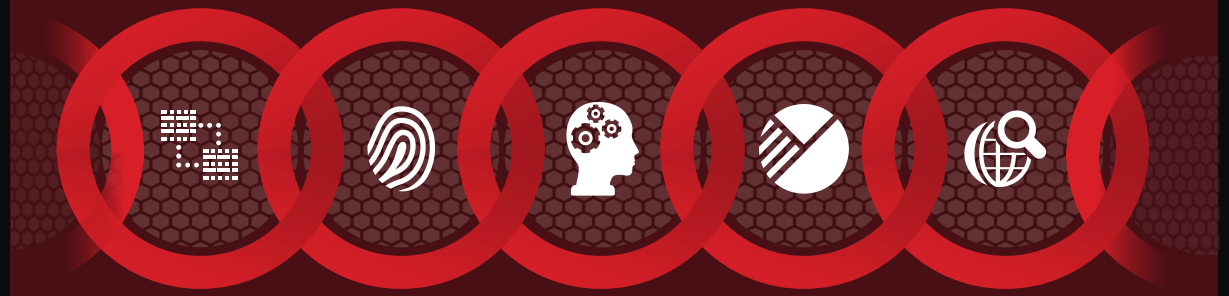


- 지능형 악성코드 분석 기술
- 상관관계를 이용한 행동분석 기술
- 클라우드 기반의 샌드박스 (로컬 어플라이언스도 존재)
- 강력한 API 기능 제공 (해당 기술이 다른 제품과의 통합이 쉬워짐)
- 정적 & 동적 분석 기술을 통한 위협 여부 판단
- 위협 인텔리젼스 데이터
- 분석되는 악성코드의 연관관계 파악 (DB 에 축적된 데이터를 통한 히스토리 추적)

ThreatGrid 인수를 통한 '위협 중심 보안' 전략 전방위 확장

Cisco AMP 행동분석 샌드박스 기능의 강화

Point-in-Time Protection



One-to-One Signature | Fuzzy Finger-printing | Machine Learning | Advanced Analytics | Dynamic Analysis

ThreatGRID 의 기술은 AMP 기능의 특정시점탐지 샌드박스 기술을 더욱 향상시켜줍니다.

파일 평판 & 샌드박스

Retrospective Security

Breadth and Control points:

- Email
- Network
- Endpoints
- IPS
- Web
- Devices

Telemetry Stream

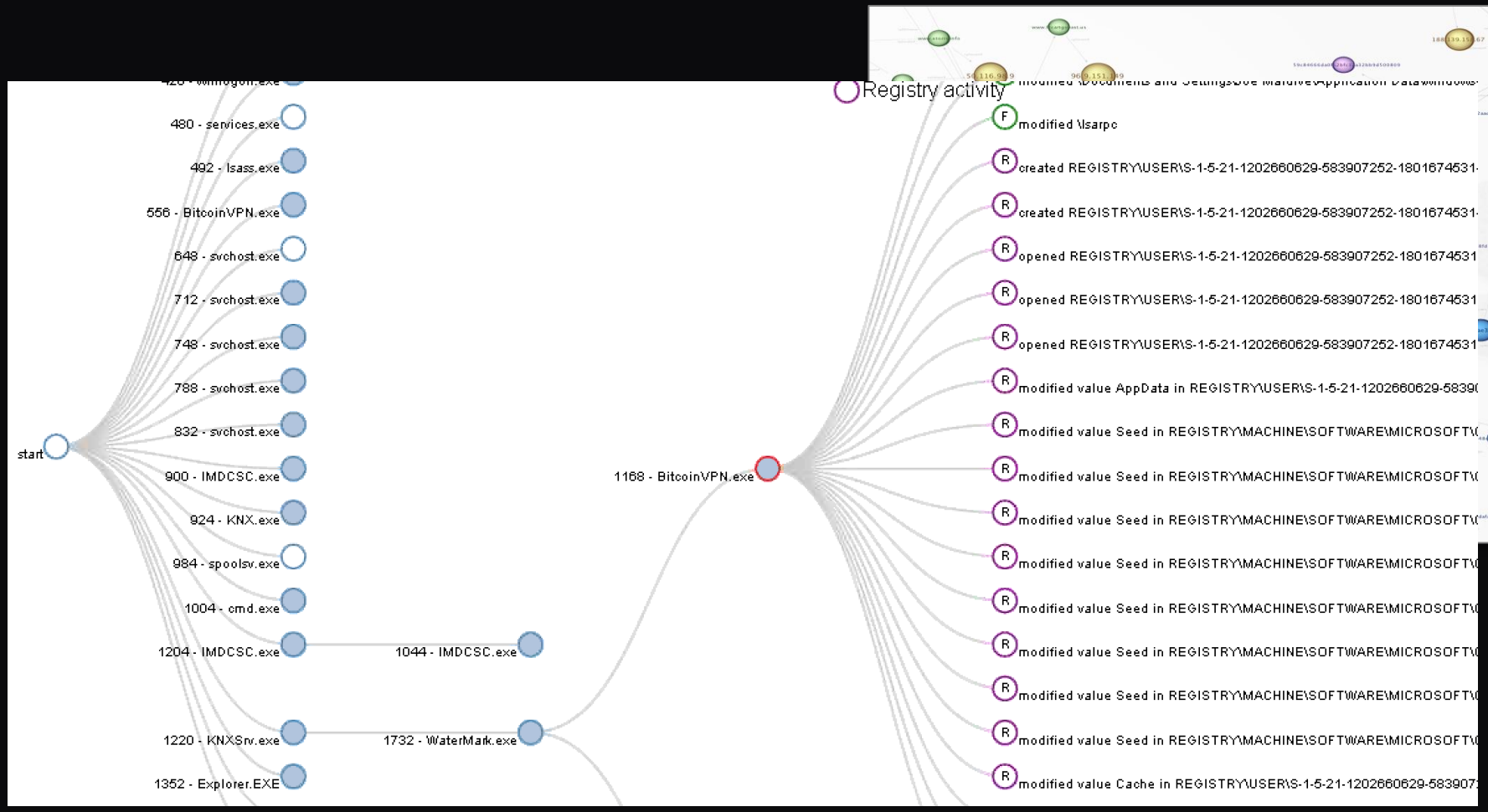
- 파일 핑거프린트 및 메타데이터
- 파일 및 네트워크 I/O
- 프로세스 정보

지속적 데이터 전달

지속적 분석

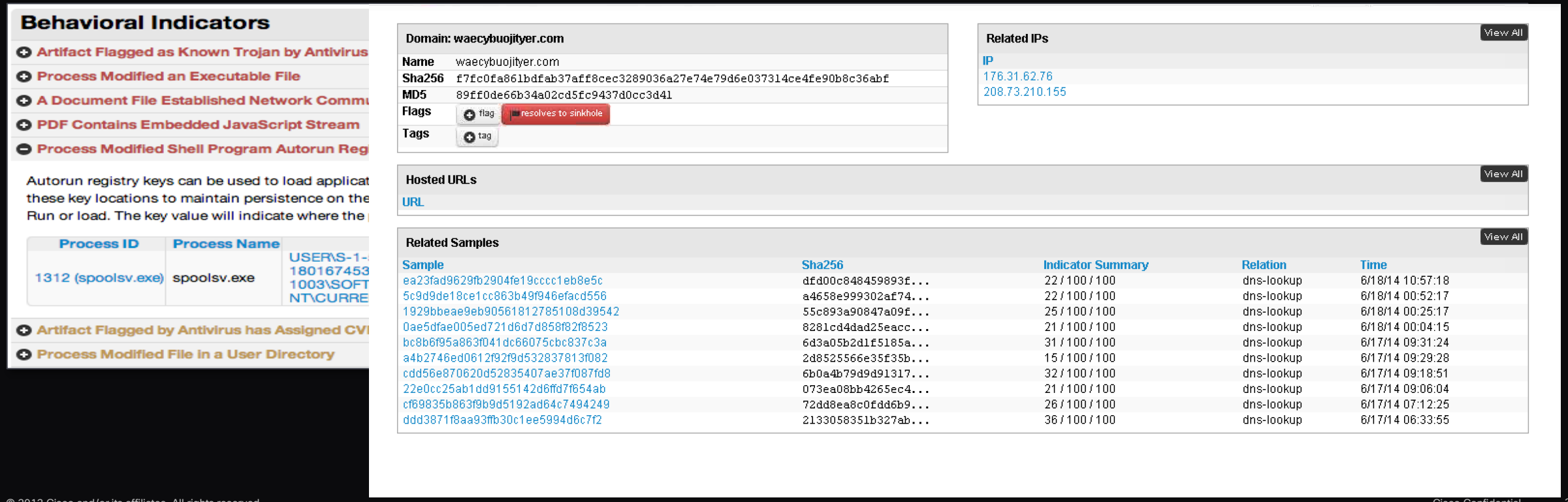
ThreatGRID 분석기술

- ThreatGRID 만의 특화된 기술을 통한 정적,동적 분석
  - 호스트에서 발생되는 모든 변화와 네트워크 통신을 추적,관찰



Threat Score

- 300 개 이상의 행동 지표 (계속 증가 중)
  - 악성코드 연관, 악의적인 행동
  - 세부적인 설명 및 행동 지침
- 위협에 대한 중요도와 우선순위
  - SOC 분석가와 IR 팀의 인지 그리고 이에 따른 효과 증대



Behavioral Indicators

- Artifact Flagged as Known Trojan by Antivirus
- Process Modified an Executable File
- A Document File Established Network Commu
- PDF Contains Embedded JavaScript Stream
- Process Modified Shell Program Autorun Reg

Autorun registry keys can be used to load applicat
these key locations to maintain persistence on the
Run or load. The key value will indicate where the

Process ID	Process Name	
1312 (spoolsv.exe)	spoolsv.exe	USER\S-1- 180167453 1003\SOFT NT\CURRE

- Artifact Flagged by Antivirus has Assigned CV
- Process Modified File in a User Directory

Domain: waecybuojityer.com

Name	waecybuojityer.com
Sha256	f7fc0fa861bdfab37aff8cec3289036a27e74e79d6e037314ce4fe90b8c36abf
MD5	89ff0de66b34a02cd5fc9437d0cc3d41
Flags	flag, resolves to sinkhole
Tags	tag

Related IPs View All

IP
176.31.62.76
208.73.210.155

Hosted URLs View All

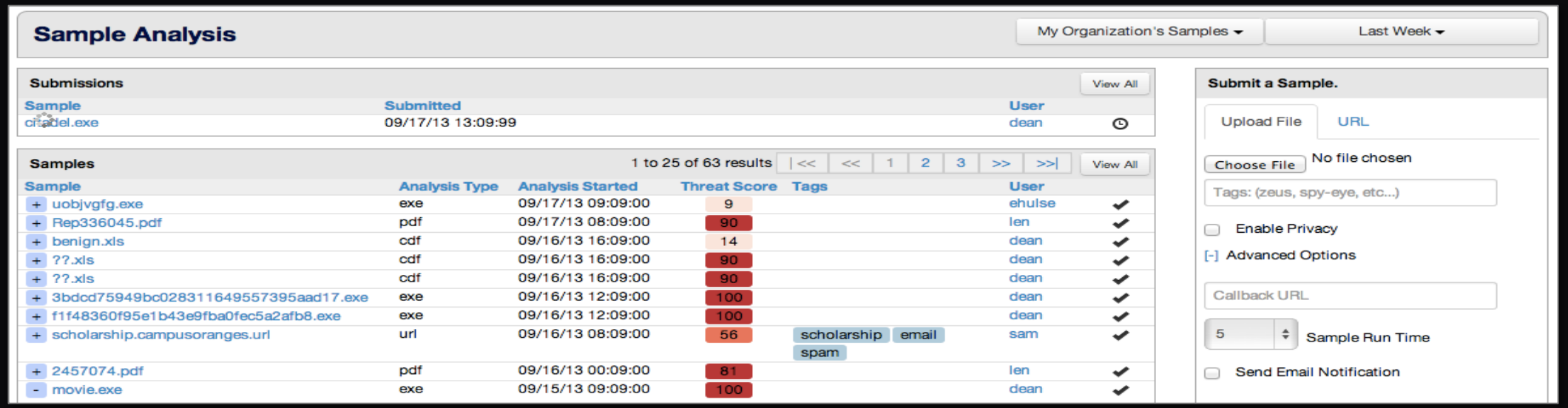
URL

Related Samples View All

Sample	Sha256	Indicator Summary	Relation	Time
ea23fad9629fb2904fe19cccc1eb8e5c	dfd00c848459893f...	22 / 100 / 100	dns-lookup	6/18/14 10:57:18
5c9d9de18ce1cc863b49f946efacd556	a4658e999302af74...	22 / 100 / 100	dns-lookup	6/18/14 00:52:17
1929bbeae9eb90561812785108d39542	55c893a90847a09f...	25 / 100 / 100	dns-lookup	6/18/14 00:25:17
0ae5dfae005ed721d6d7d858f82f8523	8281cd4dad25eacc...	21 / 100 / 100	dns-lookup	6/18/14 00:04:15
bc8b6f95a863f041dc66075cbc837c3a	6d3a05b2d1f5185a...	31 / 100 / 100	dns-lookup	6/17/14 09:31:24
a4b2746ed0612f92f9d532837813f082	2d8525566e35f35b...	15 / 100 / 100	dns-lookup	6/17/14 09:29:28
cdd56e870620d52835407ae37f087fd8	6b0a4b79d9d91317...	32 / 100 / 100	dns-lookup	6/17/14 09:18:51
22e0cc25ab1dd9155142d6ffd7f654ab	073ea08bb4265ec4...	21 / 100 / 100	dns-lookup	6/17/14 09:06:04
cf69835b863f9b9d5192ad64c7494249	72dd8ea8c0fdd6b9...	26 / 100 / 100	dns-lookup	6/17/14 07:12:25
ddd3871f8aa93ffb30c1ee5994d6c7f2	2133058351b327ab...	36 / 100 / 100	dns-lookup	6/17/14 06:33:55

컨텍스트 중심의 악성코드 분석

- 실시간적으로, 정확하게 공격의 판단
  - 악성코드 행동 지표에 대한 세부적인 분석 정보 (위협 스코어)
- 각 데이터 요소의 손쉬운 접근
  - 분석정보의 JSON 다운로드



시큐리티 통합 & 자동화

- 기 존재하는 시큐리티 제품에 대한 통합 제공
  - ThreatGRID's REST API 를 통한 자동화된 샘플분석, 리포팅
    - ✓ 샘플분석 요청 자동화 (호스트 또는 네트워크)
    - ✓ 분석된 데이터 결과를 쉽게 통합

ThreatGRID + Cisco = 지능형 위협에 대한 차단기능 강화

Cisco

- 공격의 전체흐름을 이해하는 Before, During, After 의 방어
- 앤드포인트 부터 네트워크까지 포괄하는 보안 솔루션
- 클라이드 기반의 행동분석을 통한 특정 시점 & 지속적 분석을 통한 보안 위협 차단

Better Together

- ThreatGRID 기술을 통한 시스코 AMP 제품 기능의 향상 (특히 샌드박스)
- Private 클라우드는 고객들의 데이터를 외부로 전달하지 않고 내부에만 존재하게 만들어 더욱 안전하게 운영할 수 있습니다.
- 보다 많은 위협 데이터의 통합과 상관관계를 통한 상황인식과 위협 인텔리전스 데이터는 고객의 가치를 더욱 높여줍니다.

ThreatGRID

- 악성코드 행동분석을 위한 Private 클라우드 기반의 샌드박스
- 더욱 많은 파일 타입에 대한 분석 제공
- API 통합과 이를 통한 자동화
- MBR(Master Boot Record) 탐지 – 즉, 기존 샌드박스 보다 더 많은 탐지 영역을 가지고 있음

Thank You