



사이버 위협의 선제적 대응을 위한 Symantec Global Intelligence 활용 사례

최재우 부장

DEC 10, 2015

전략 변화의 필요성

공격의 증가

새로운 위협

탐지 우회

전문가 집단

”인텔리전스 기반”의 의사결정 시스템으로
효율적인 침해대응

선택과 집중

선제적인 대응

새로운 형태의
보호

빠르고
효율적인 대응



인텔리전스의 진화



공격자 인텔리전스



행위자



TTPs
(전술, 기술, 절차)



캠페인



인시던트

기술적 인텔리전스



취약점



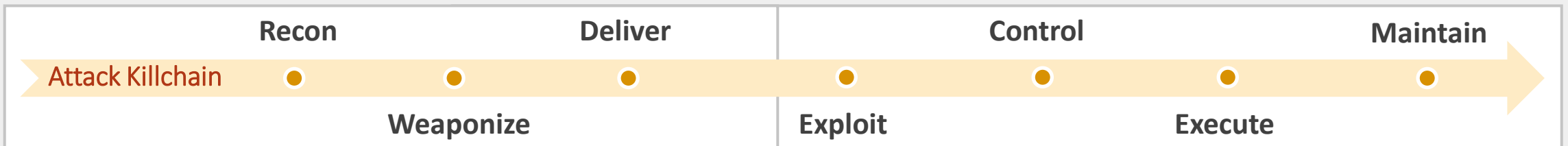
네트워크 평판
(IP/Domains/URLs)



보안위험 /
악성코드



파일의 평판



Outside your perimeter

Inside your perimeter

글로벌 인텔리전스 네트워크(GIN)

악성행위

- 1억7천5백만 클라이언트, 서버, 게이트웨이
- 전세계 데이터 수집

공격 센서

- 5천7백만개이상의 보안 장비
- 초당 수천개의 이벤트 수집

스팸/피싱

- 5백만 유인계정
- 80억개 이메일/월간
- 130억개 웹요청/일간

취약점

- 60,000+ 취약점 DB.
- 19,000+ 벤더
- 133,100+ 제품

Managed Adversary & Threat Intelligence

- 수백개 이상의 웹포럼 모니터링
- 250+ 공격집단 모니터링

시만텍 보안 인텔리전스

글로벌 데이터 수집

Attack Quarantine System

Malware Protection

Gateways

Phishing Detections

Global Sensor Network

3rd Party Affiliates

Online Operations

Social Media Monitoring

Open Sourcing Mining

Liaisons

Sharing Forums



Signals

Human

Global Intelligence Network

빅데이터 분석



데이터 통합 저장소

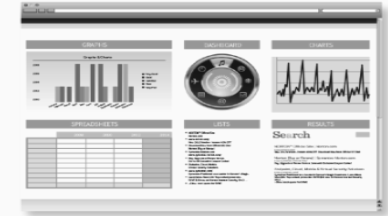


애널리틱



인텔리전스 애널리틱스

DeepSight



포탈

10010101101001010
↓ ↓ ↓ ↓ ↓
10010101101001010
데이터피드



직접 분석

확장된 인텔리전스 분석

MATI Team

Global Intelligence Network



인텔리전스 방법론

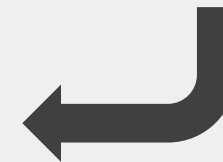
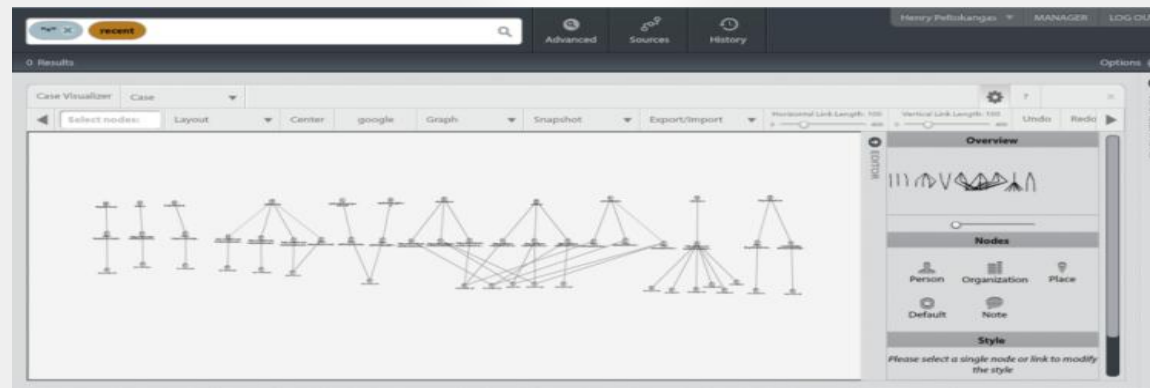
높은 신뢰도



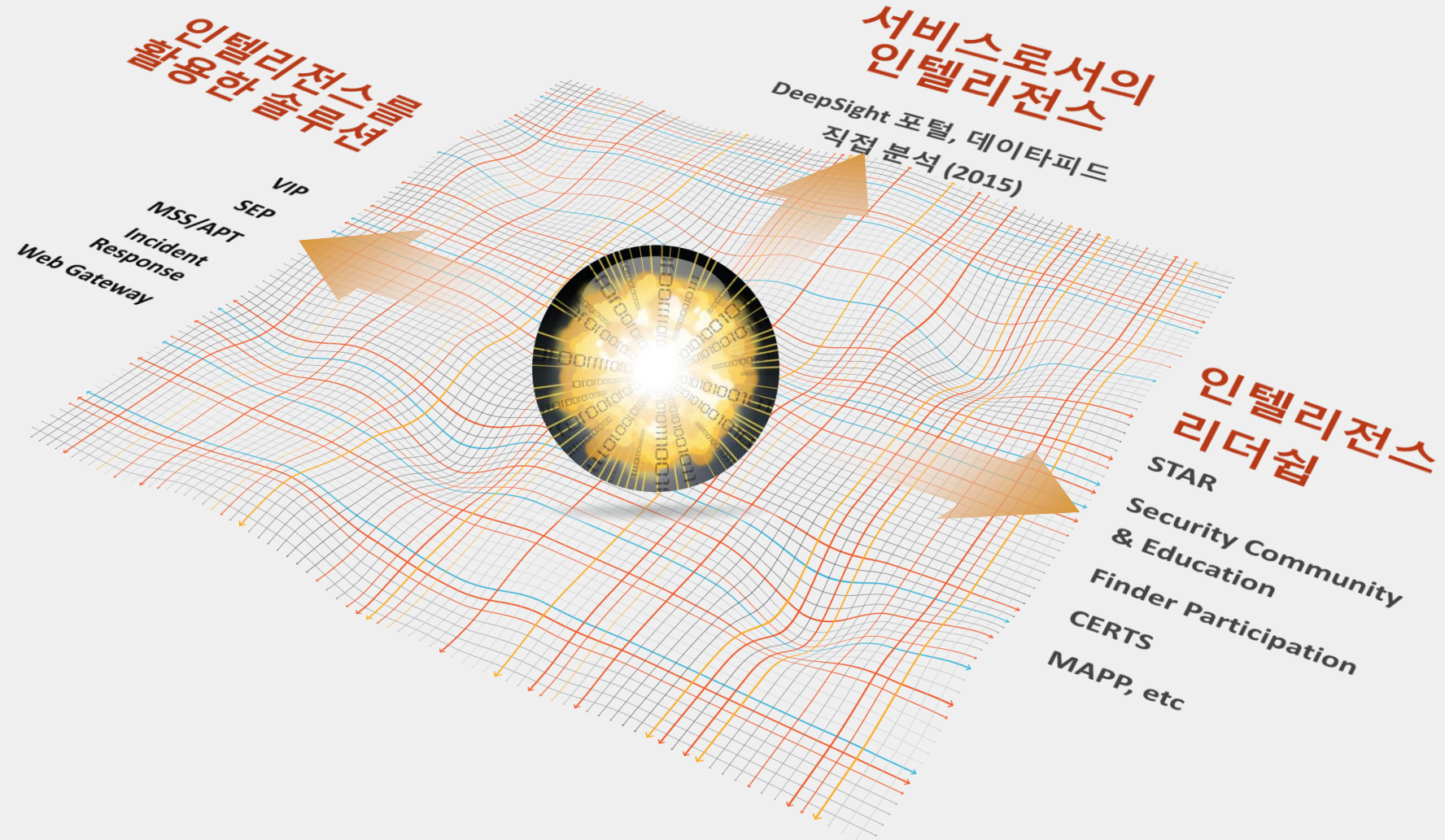
소스의 신뢰도

여러가지
소스

낮은 신뢰도

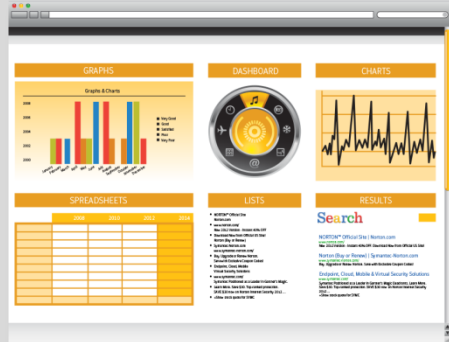


인텔리전스를 활용한 솔루션



DEEPSIGHT 인텔리전스 서비스 제공

DeepSight 인텔리전스 포털



글로벌 위협 및 취약점 데이터에
대한 인사이트
세부적인 연구, 분석 및 보고서
공격자 툴, 기술 및 캠페인

데이터 피드

10010101101001010
↓ ↓ ↓ ↓ ↓
10010101101001010






실시간 위협 데이터
전사의 다양한 형태로 연동
가능






상위 공격자 및 공격대상

Top offending ISPs	
ISP	Percent
ovh systems	10%
level 3 communications inc.	9%
softlayer technologies inc.	4%
theplanet.com internet services inc.	4%
facebook inc.	4%
akamai technologies inc.	4%
leaseweb b.v.	3%
apple inc.	3%
cogent communications	3%
godaddy.com llc	3%

Top offending IPs	
IP	Percent
91.121.174.146	4%
143.127.139.87	2%
109.163.231.119	2%
130.185.105.74	2%
50.63.121.1	1%
184.172.61.43	1%
5.135.67.166	1%
173.241.250.2	1%
50.28.72.149	1%
31.184.192.238	1%

Top offending Ports	
Port	Percent
445	11%
135	5%
80	2%
139	1%
123	1%
5900	0%
81	0%
49154	0%
49152	0%
3389	0%

Top Source Countries	
Source Country	Percent
 United States	46%
 France	8%
 Germany	8%
 Netherlands	6%
 Russia	6%

Top Destination Countries	
Destination Country	Percent
 United States	34%
 United Kingdom	9%
 India	6%
 Germany	5%
 Australia	5%

Top Attacked Products	
Products	Percent
Windows 2000 Server	8%
Contact Center NCC	8%
Contact Center Manager	8%
Self-Service MPS 100	8%
Contact Center - TAPI Server	8%
Windows Server 2003 Itanium	8%
Windows Vista Enterprise 64-bit edition	8%
Windows XP	8%
Windows XP Media Center Edition	8%
Windows Server 2003 Enterprise x64 Edition	8%



최신 보안사고에 대한 분석 보고서 제공

The screenshot displays the 'Analyst Journals' section of a website. At the top, there are navigation tabs for 'Alerts', 'Research', 'Analyst Journals', and 'DataFeeds'. Below the navigation is a search bar with the placeholder text 'Type a topic, date or author'. The main content area is titled 'Analyst Journal (3516)' and features a list of articles. On the left side, there are three filter panels: 'Archive' with a list of months from October 2012 to February 2013; 'Timeframe' with a date range picker and an 'Apply' button; and 'Author' with a list of names and their article counts, including Aaron Adams (379), Adrian Pilsarczyk (141), Alexey Lavrenyuk (50), Amanda Andrews (1), and Andy Chan (81), along with a 'Show All (50more)' link. The article list includes titles such as 'New Adobe PDF Zero-day Unleashes Trojan.Swaylib', 'Adobe Flash and PDF zero-day vulnerabilities', 'Trojan.Ransomgerpo Criminal Arrested', 'New Adobe Vulnerabilities Being Exploited in the Wild', 'Man Arrested in Relation to the "Remote Control Virus"', 'Microsoft Patch Tuesday for February 2013', 'Cross-Platform Frutas RAT Builder and Back Door', 'Adobe Zero-day Used in LadyBoyle Attack', and 'Malvertising and Dynamic DNS: A Never Ending Story'.

• 분석 보고서에 대한 검색 또는 아카이브

• RSS제공

상세한 분석 보고서 및 MATI 보고서

Alerts Research **Analyst Journals** DataFeeds

Analyst Journals

Trojan.Ransomgerpo Criminal Arrested

Spanish police have [reported](#) the arrest of an individual involved with a particular strain of police Ransom. This variant is one of the earliest active police Ransomware families, which Symantec has been tracking. Early versions of the locking screen were quite primitive but quickly evolved as the author obviously st

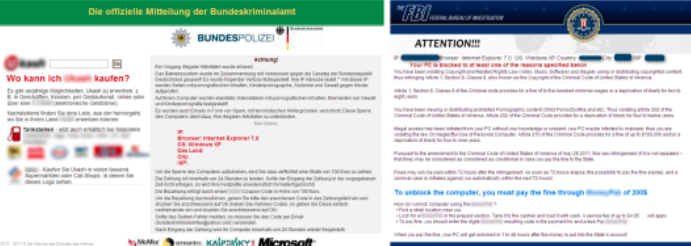



Figure 1. Early design of Trojan.Ransomgerpo and a more recent, sophisticated style. (The most recent Trojan, as Figure 1 implies, initially focused on German individuals, but in later months began to target individuals in the United States and other countries, as shown in Figure 3.)

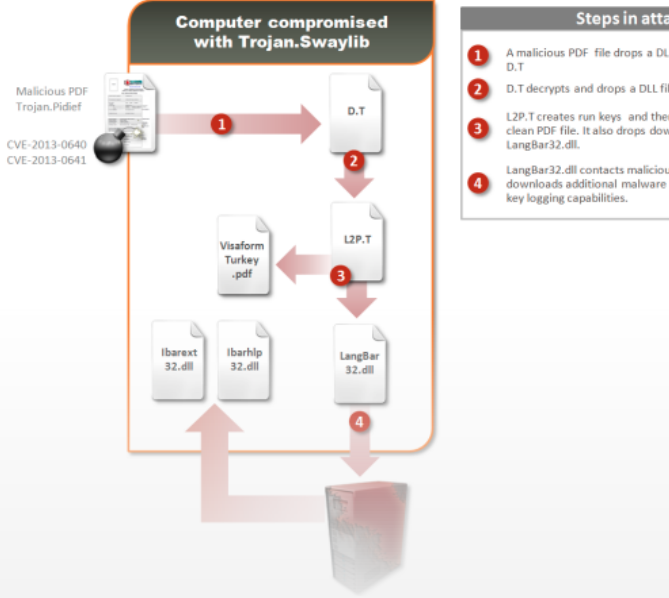


Alerts Research **Analyst Journals** DataFeeds

Analyst Journals

New Adobe PDF Zero-day Unleashes Trojan.Swaylib

In a previous [blog](#), Symantec reported on a new Adobe zero-day vulnerability (CVE-2013-0640), to release a patch for this zero-day, but in an [advisory](#) they have provided a means of mitigation. The initial report on this zero-day being actively used in the wild came from [FireEye](#). They [report](#) shows the stages of attack.



Steps in attack

- 1 A malicious PDF file drops a DLL file D.T
- 2 D.T decrypts and drops a DLL file c
- 3 L2P.T creates run keys and then d clean PDF file. It also drops downlo LangBar32.dll.
- 4 LangBar32.dll contacts malicious s downloads additional malware with key logging capabilities.

Figure 1. Attack using CVE-2013-0640

DEEPSIGHT 인텔리전스 서비스 제공

DeepSight 인텔리전스 포털



글로벌 위협 및 취약점 데이터에
대한 인사이트
세부적인 연구, 분석 및 보고서
공격자 툴, 기술 및 캠페인

데이터 피드

10010101101001010
↓ ↓ ↓ ↓ ↓
10010101101001010

실시간 위협 데이터
전사의 다양한 형태로 연동
가능

DEEPSIGHT 인텔리전스

위협 요소 데이터피드

악성행위는 아래의 항목으로 분류함

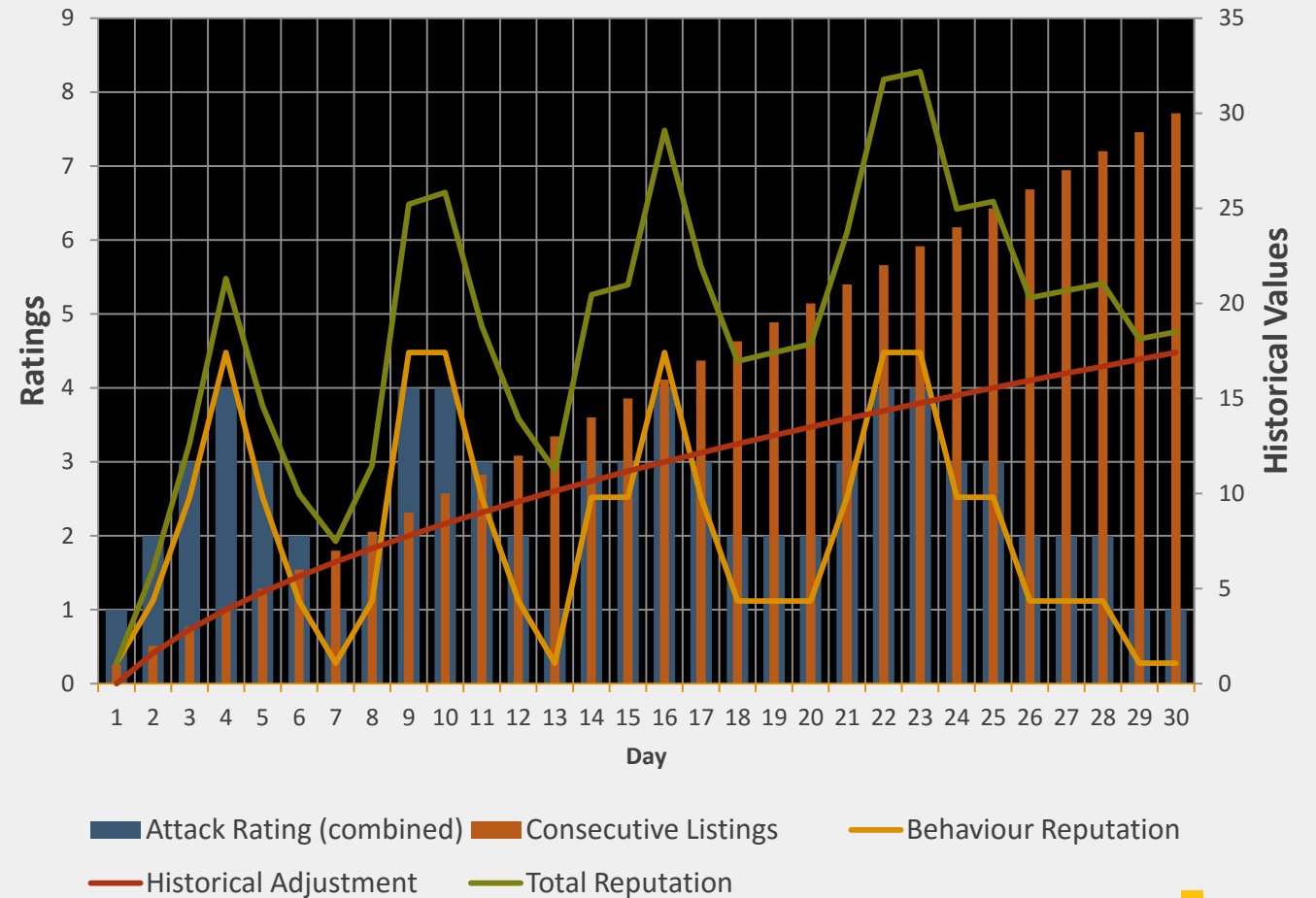
- 공격자(Attackers)
- 악성코드 유포지(Malware Spreaders)
- 피싱(Phishers)
- 스팸발송(Spammers)
- 봇넷 관련정보(Botnet Membership)
- 명령제어서버(Command and Control Server)
- 인터넷사기(Fraud)

```
<ip address="x.149.5.169" consecutive_listings="2" listing_ratio="2" reputation="10">  
  <attacks hostility="4" confidence="5" />  
  <malware hostility="3" confidence="4" />  
</ip>  
<ip address="x.185.252.100" consecutive_listings="2" listing_ratio="2" reputation="9">  
  <attacks hostility="4" confidence="5" />  
  <malware hostility="3" confidence="3" />  
</ip>  
<ip address="x.178.145.238" consecutive_listings="6" listing_ratio="6" reputation="9">  
  <attacks hostility="5" confidence="4" />  
  <malware hostility="5" confidence="1" />  
</ip>  
<ip address="x.52.110.51" consecutive_listings="2" listing_ratio="2" reputation="8">  
  <attacks hostility="2" confidence="4" />  
  <bot confidence="4" />  
</ip>
```

DEEPSIGHT 인텔리전스

평판 계산 매트릭스

- 각각의 사항은 개별적으로 평가되고 가중치
 - 위협도
 - 빈도
 - 데이터 신뢰도
- 수치의 변경은 다음의 사항에 따라 다름:
 - 악성행위의 연속적인 활동 기간
 - 최고 90일까지의 행적 기록



평판값



DEEPSIGHT 인텔리전스 데이터피드

IP 평판 데이터피드

글로벌 인텔리전스 네트워크로부터 수집되는 정보들을 기반으로 최고 10만개의 악성 IP 정보 제공

URL 및 Domain 평판 데이터피드

글로벌 인텔리전스 네트워크로부터 수집되는 정보들을 기반으로 최고 10만개의 악성 URL 정보 제공

취약점 데이터피드

취약점 정보, 조치방안, 영향도 분석 및 관련 링크 제공

보안위협 데이터피드

애드웨어, 스파이웨어, 및 악성코드에 대한 세부 분석 내용 제공



Utilizing Datafeeds in Security Solutions



Symantec DeepSight



MSS



VIP



.Cloud (Web)



ATP(Advanced Threat Protection)



Norton (Mac)



RuleSpace

Third Party Solution Integrations

SIEM & Analytics



DNS & Snort



GRC Applications



BAY DYNAMICS™

RSA ARCHER GRC



CONVENTUS

DeepSight Intelligence Use Cases

Vulnerability Portal Alerts & Vulnerability Datafeeds

기업에서 사용하고 있는 제품, 기술 기반으로 취약점에 대한 식별과 우선순위 결정을 도움

Enterprise IT Products in the organization

ORACLE
paloalto NETWORKS
Microsoft
Symantec
IBM
EMC²
hp
NetApp
SAP
Cisco
Polycom
Apache
OpenSSL
Apple
BROCADE
intel
openstack
vmware

1. SETUP "TECH LIST"

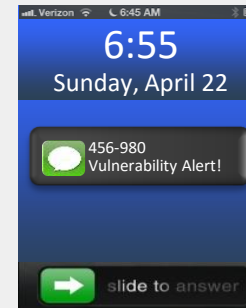
기업에서 사용하고 있는 제품을 기반으로 DeepSight 포털에 "Tech List" 셋팅 [Linux Kernel, Cisco, Protocol, Oracle, IE, Apach, Mysql, IBM]



2. DISCOVERY...

상세한 검색 조건에 따라 취약점 정보를 적시에 제공

3. GET ALERTERED



DeepSight Portal 사용시 보안팀은 SMS 혹은 메일을 통해 "Tech List" 기반의 취약점 알림을 받게 됨

DeepSight Vulnerability Datafeeds 사용시 고객관리, 거버넌스, 위험 및 규제준수 (GRC) 시스템에 공급됨.

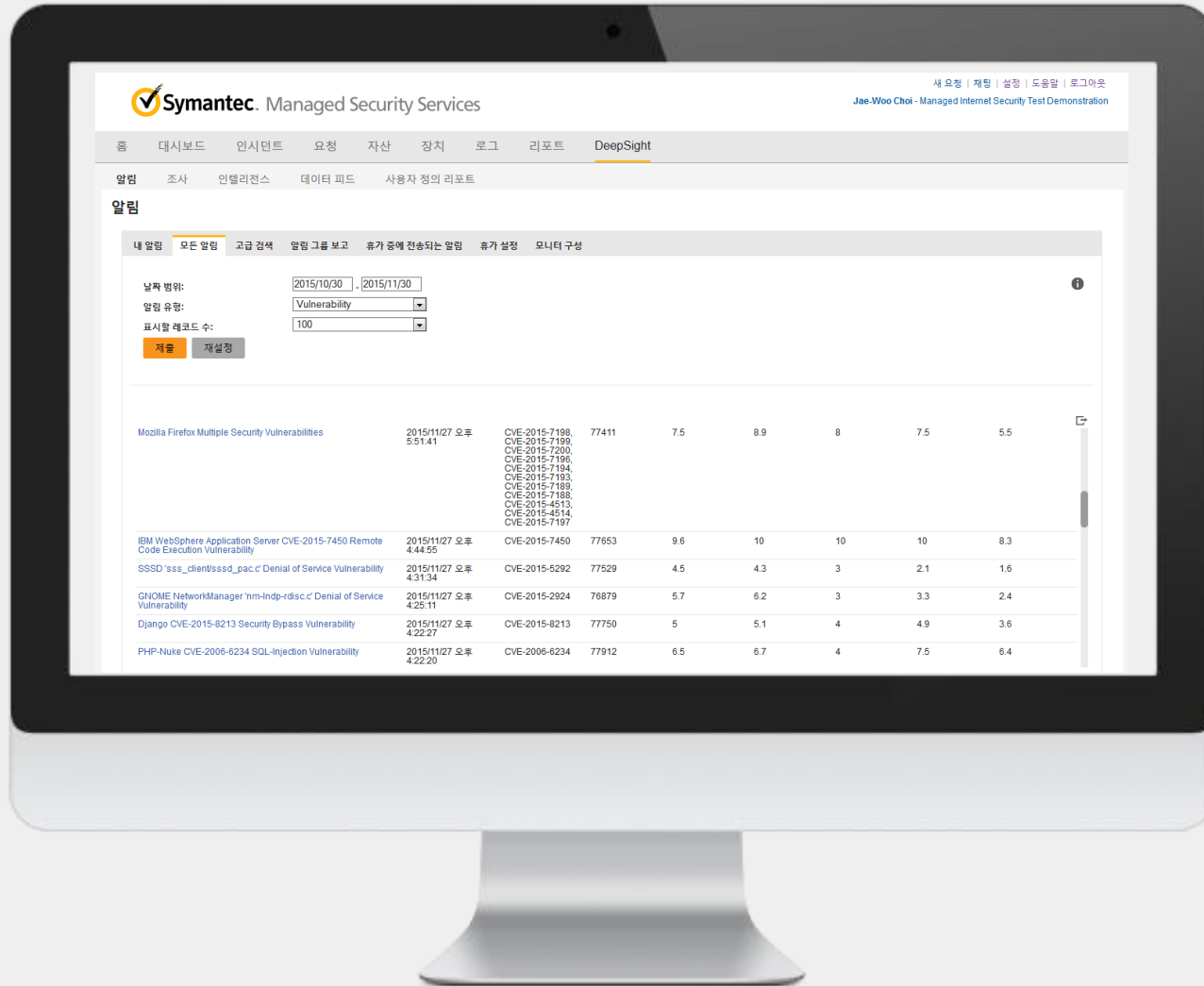
조직의 크기에 상관없이 제품의 취약점은 다음의 내용을 포함: CVSS Scores, Exploit details, Work Around, Solution & Fix, Availability of a Patch, and more.


4. APPLY PATCHES

보안팀은 DeepSight Portal 의 알림 혹은 Vulnerability Datafeeds 의 우선순위 기반으로 패치를 적용, IT 시스템의 보안에 초점을 맞추게 됨



DeepSight Intelligence Use Cases - Vulnerability Portal Alerts




Symantec Alert Vulnerability

Mozilla Firefox Multiple Security Vulnerabilities

Synopsis

Bugtraq ID 77411

CVE CVE-2015-7188
 CVE-2015-7189
 CVE-2015-7200
 CVE-2015-7190
 CVE-2015-7194
 CVE-2015-7193
 CVE-2015-7189
 CVE-2015-7188
 CVE-2015-4513
 CVE-2015-4514
 CVE-2015-7197

Published Nov 03 2015

Classification Unknown

Remote Yes Local No

Availability Always Authentication Not Required

Ease No Exploit Available

Last Update 11/27/2015 5:51:41 PM GMT

Last Change Multiple security advisories RHSA-2015:2519 and ELSA-2015-2519 are available.

CVSS Version 2

CVSS2 Base 7.5 CVSS2 Base Vector AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS2 Temporal 5.5 CVSS2 Temporal Vector E:U/RL:OF/RC:C

CVSS Version 1

CVSS1 Base 7 CVSS1 Temporal 5.2

NVD CVSS2 7.5 Component String AV:N/AC:L/Au:N/C:P/I:P/A:P

Urgency Rating 7.5

Threat Breakdown

Severity 8.9

Impact 8

Ease of Exploit 1

Credibility Vendor Confirmed

CVSS Version 2


CVSS2 Base 7.5

CVSS2 Temporal 5.5

Vulnerable Systems

- CentOS CentOS 5 ope:/o:centos:centos:5 NVD
- CentOS CentOS 7 ope:/o:centos:centos:7 SYMC
- Debian Linux 6.0 amd64 ope:/o:debian:debian_linux:6.0_amd64 SYMC
- Debian Linux 6.0 arm ope:/o:debian:debian_linux:6.0_arm SYMC
- Debian Linux 6.0 ia-32 ope:/o:debian:debian_linux:6.0_ia-32 SYMC
- Debian Linux 6.0 ia-64 ope:/o:debian:debian_linux:6.0_ia-64 SYMC
- Debian Linux 6.0 mips ope:/o:debian:debian_linux:6.0_mips SYMC

Mozilla Firefox Multiple Security Vulnerabilities



Create Date 11/27/2015 5:53:14 PM GMT

DeepSight Intelligence Use Cases

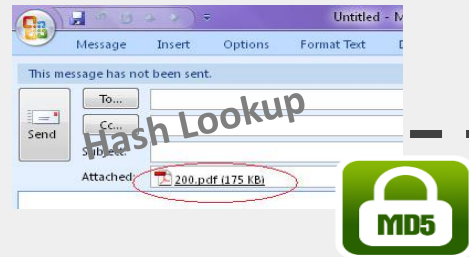
Incidence Response - Portal

감염된 시스템 분석



보안팀에서 감염된 시스템을 분석을 위해 제공받음. 시스템이 전달받은 이메일에 첨부된 URL과 첨부파일에 대한 추가 분석 필요

1. CHECK FOR MALWARE
첨부파일에 대한 악성코드 확인을 위해 DeepSight Portal 에서 파일에 대한 평판을 확인



DeepSight 에서 파일의 해쉬값을 확인하여 악성코드가 포함되어 있는 것을 확인

2. SECURITY RISK LOOKUP
멀웨어에 대한 상세정보 및 제거 정보 확인



DeepSight 는 분석을 위한 보안 위험에 대한 제거 전략과 추가적인 기술 지표에 대한 상세 정보를 제공

3. URL LOOKUP
DeepSight Portal 에서 URL 에 대한 평판정보 확인

Domain: lincolnpeak.com	
Registrar Name:	GODADDY.COM, LLC
Registration Information	Registration Dates
Organization:	Domains By Proxy, LLC
Contact Name:	Registration Private
Contact Email:	LINCOLNSPEAK.COM@domainsbyprox.com
City:	Scottsdale
State:	Arizona
Country:	UNITED STATES
Pushing	
Global Intelligence Network	
First Observed:	25 Jan 2015
Last Observed:	06 Apr 2015

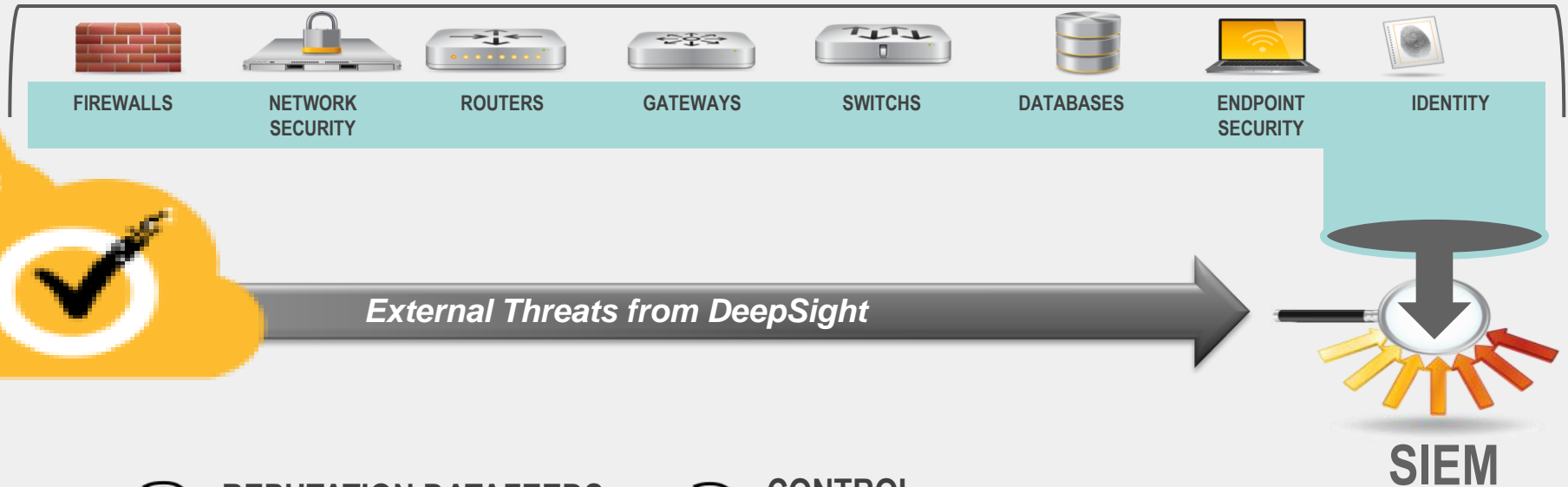
DeepSight는 악의적 행위를 보이는 URL과 멀웨어 분포, 도메인 소유자 정보등의 추가정보등 도메인 차단에 대한 결정을 내리기 위한 분석 정보를 제공

DeepSight Intelligence Use Cases

Detection of Unknown External Threats - Datafeeds

Security Operations Center (SOC)

Central location to collect information on threats such as: external, internal, user activity, and loss of sensitive data



1. EXTERNAL UNKNOWN THREATS

DeepSight Datafeeds 는 SOC와 SIEM에 탐지와 차단을 위해 보안 인프라가 제공하지 않은 외부의 위협 데이터를 제공합니다.

2. REPUTATION DATAFEEDS

DeepSight reputation Datafeeds는 민감한 정보의 유출을 탐지 및 차단하기 위해 C&C 서버의 최신 목록을 제공합니다.

3. CONTROL POINTS

SIEM은 DeepSight 데이터를 이용하여 방화벽과 게이트웨이가 민감한 데이터가 빠져나가는것을 탐지하고 차단하기 위해 사용됩니다.

DEEPSIGHT INTELLIGENCE USE CASES

Adversary Intelligence

ADVERSARY INTELLIGENCE



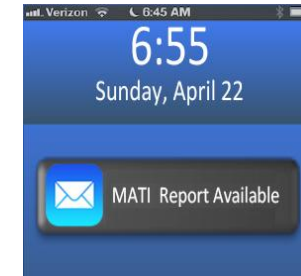
1

MATI 리포트
알림 설정



2

이메일을
통한 알림
수신



4

보호 조치 활동

3

보안 운영팀에
기술적 지표 제공



USES FOR MATI REPORT



Strategic Planning and Risk Mitigation



Get Ahead of Threats



Faster Detection and Incident Response

DEEPSIGHT INTELLIGENCE USE CASES

Adversary Intelligence

설정

빈도	Daily
	<input checked="" type="checkbox"/> 월요일 <input checked="" type="checkbox"/> 화요일 <input checked="" type="checkbox"/> 수요일 <input checked="" type="checkbox"/> 목요일 <input checked="" type="checkbox"/> 금요일
필터	Targeted Industry
대상 업계	Finance and Insurance
설명	금융관련 보고서
레코드 수	10



DeepSight™
INTELLIGENCE

JSOCKET PHISHING CAMPAIGN TARGETS FINANCIAL BUSINESSES

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE SUMMARY | SYMC - 300342 | V.1

DETAILS

In November 2015, DeepSight Intelligence identified a new phishing campaign using the JSocket RAT, developed by AlienSpy RAT authors to target financial businesses, hotels, gas stations, investment firms, insurance firms, and shipping companies. The first wave of phishing emails started in July 2015 and appears active as of 23 November 2015.

The emails used as part of the JSocket phishing campaign contained subject lines with financial themes such as Payment Swift, Payment Invoice, Invoice and Packing List for shipment, and Invoice of Payment NO#. The email attachments, DOC or JAR files, appear to be invoices and purchase orders, that when opened, direct the malware to connect to 1stopgameonline.com over port 80 and make two GET requests to download JSocket. As of 24 November 2015, the domain 1stopgameonline.com resolved to 192.254.186.253. The malware also connects to emenike.no-ip.info over port 2487. In July 2015, emenike.no-ip.info resolved to 180.74.47.237 but resolves to 46.244.21.11 as of this writing. According to Symantec telemetry, cyber criminals have used the domain emenike.no-ip.info to spread Kryptik and malicious adware malware. JSocket also installs a Java client on the victims' machines when necessary.

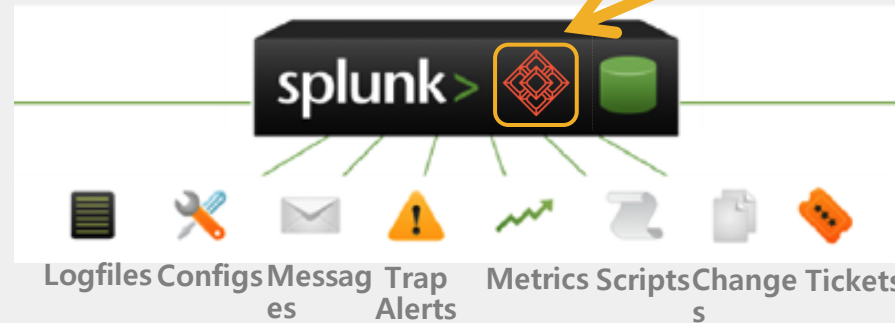
JSocket is sold on the website jssocket.org with rekings.com[1] as a reseller; both online stores appear to sell legitimate business software although the software is used for malicious reasons. Actors require a subscription to use the JSocket RAT builder with prices running from US\$25 for one month to US\$300 for a year payable in Bitcoins. When the online malware store rekings.com stopped selling AlienSpy in July 2015, the AlienSpy support blog encouraged AlienSpy users to change to JSocket's server (IP address 37.61.237.251) for AlienSpy subscription verification (see Figure 1). AlienSpy was on the market for about six months before being replaced by JSocket.

Splunk 통한 활용 예



데이터
플랫폼

DeepSight App



Customer Facing Data

- > Click-stream data
- > Shopping cart data
- > Online transaction data

Outside the Datacenter

- > Manufacturing, logistics...
- > CDRs & IPDRs
- > Power Consumption
- > RFID data
- > GPS Data

윈도우즈

- > 레지스트리
- > 이벤트로그
- > 파일 시스템
- > sysinternals

Linux/Unix

- > 구성설정
- > syslog
- > 파일 시스템
- > Ps, iostat, top

가상화&클라우드

- > Hypervisor
- > Guest OS, Apps
- > Cloud

애플리케이션

- > Web logs
- > Log 4J, JMS, JMX
- > NET events
- > Code and scripts

데이터베이스

- > Configurations
- > Audit/query logs
- > Tables
- > Schemas

네트워크

- > 구성설정
- > syslog
- > SNMP
- > netflow

스플링크용 앱제공(무료)

Symantec DeepSight Security Intelligence App for Splunk Enterprise

OVERVIEW | DOCUMENTATION

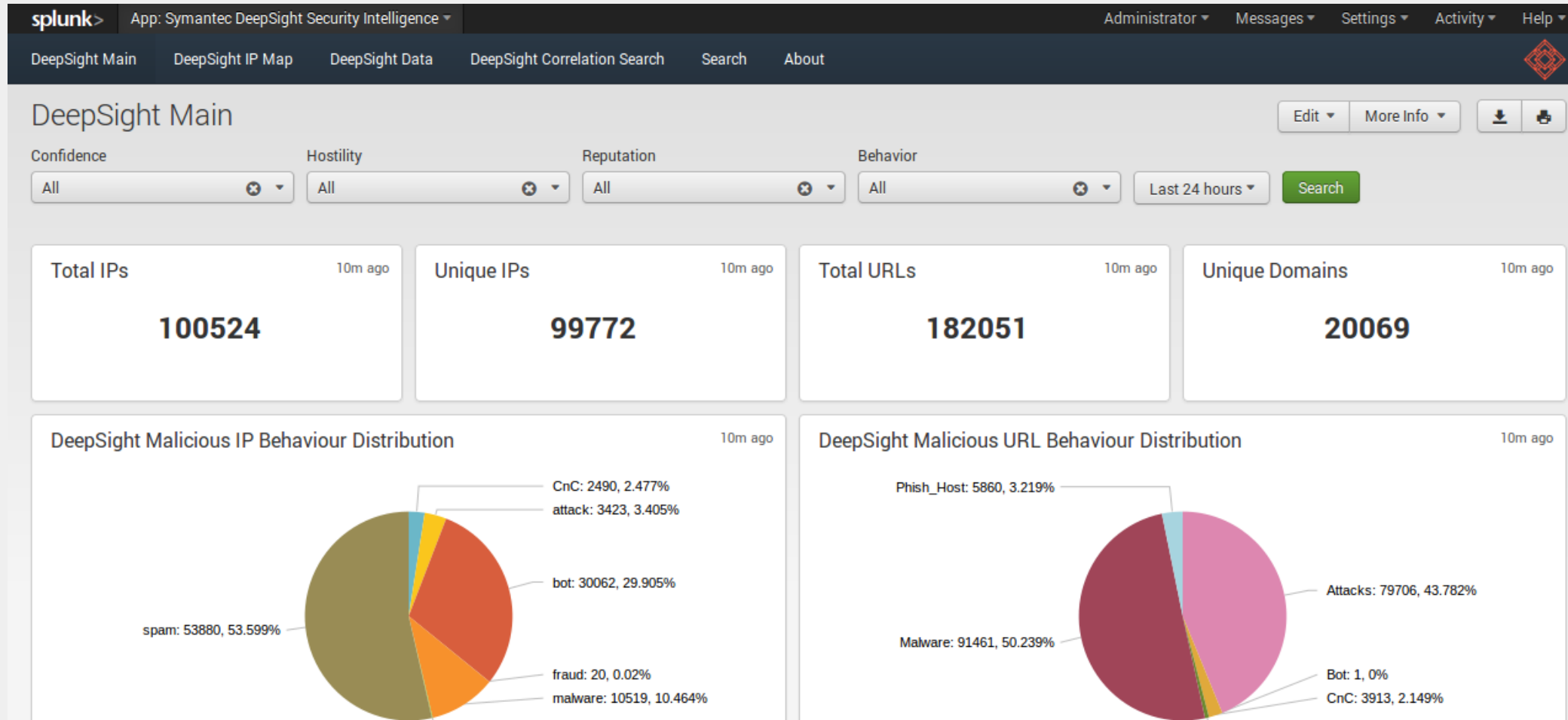
Monitor cyber threats and malicious activities in your network with the Symantec DeepSight Security Intelligence App for Splunk Enterprise. By correlating data sources in your Splunk environment to flagged threats from Symantec's datafeeds, you will have visibility into any risks posed against your data in real time. Take control of your network and fight cyber crime with the Symantec DeepSight Security Intelligence App for Splunk Enterprise.

The technology add-on for this app is currently only available for RedHat 6.x and CentOS 6.x. We will expand the functionality of the TA to other operating systems in future releases.

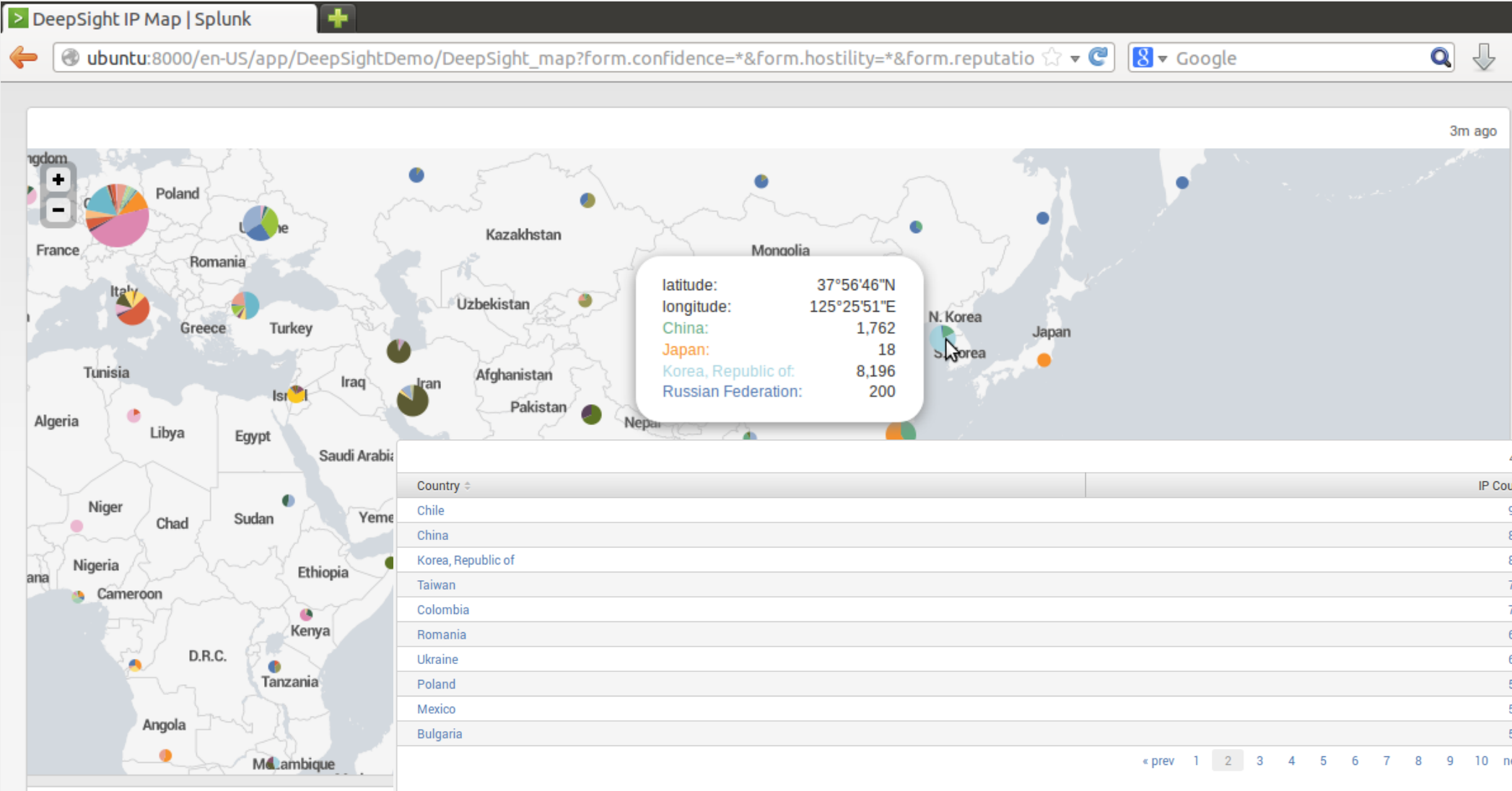
<http://apps.splunk.com/app/1833>

VERSION: 1.1

스플링크 앱(DepoSight) - Dashboard



Geo 데이터



상관관계 분석

splunk> App: Symantec DeepSight Security Intelligence Messages Settings Activity Help

DeepSight Main DeepSight IP Map DeepSight Data DeepSight Correlation Search Search About

DeepSight Correlation Search

Searching DeepSight for:

Enter a valid sourcetype: Enter a valid IP or URL field name: Confidence: Hostility:

Reputation: Behavior: All time

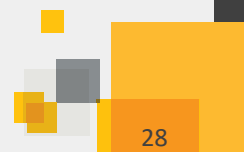
Entries Matched: 1 (5m ago) Max Reputation Score: 10 (5m ago) Max Confidence Score: 5 (5m ago) Max Hostility Score: 5 (5m ago)

DeepSight Hits

ip	Time	Confidence	Hostility	Reputation	Behavior
54.230.21.108	05/01/2014 23:25:07	5	5	10	malware
	05/01/2014 23:07:08	5	5	10	malware
	05/01/2014 22:47:05	5	5	10	malware

Event Details

_time	src_ip	_raw
2014-01-23 08:01:27	54.230.21.108	Jan 23 08:01:27 10.208.35.87 Jan 23 07:58:59 PA-VM 1,2014/01/23 07:58:58,007000001148,TRAFFIC,end,1,2014/01/23 07:58:59,54.230.21.108,192.168.2.255,0.0.0.0,0.0.0.0,Test,,netbios-ns,vsys1,Untrust,Untrust,ethernet1/2,ethernet1/2,Log Forwarding,2014/01/23 07:58:58,95,1,137,137,0,0x64,udp,allow,552,552,0,6,2014/01/23 07:58:27,2,any,0,362105,0x0,192.168.0.0-192.168.255.255,192.168.0.0-192.168.255.255,0,6,0, service map: <eventmap version="2"><field name="vendor_severity">info</field><field name="facility">user</field><field name="event_dt">1390492887056</field><field name="proxy_machine_ip">10.208.35.87</field><field name="proxy_machine">10.208.35.87</field></eventmap>



데이터피드 정보

splunk > App: Symantec DeepSight Security Intelligence > Messages > Settings > Activity > Help >

DeepSight Main DeepSight IP Map DeepSight Data DeepSight Correlation Search Search About

DeepSight Data

DeepSight Data

Edit > More Info > [Download] [Print]

Confidence: All [X] Hostility: All [X] Reputation: All [X] Behavior: All [X] Consecutive Listings: All [X]

Listing Ratio: All [X] Last 24 hours [Search]

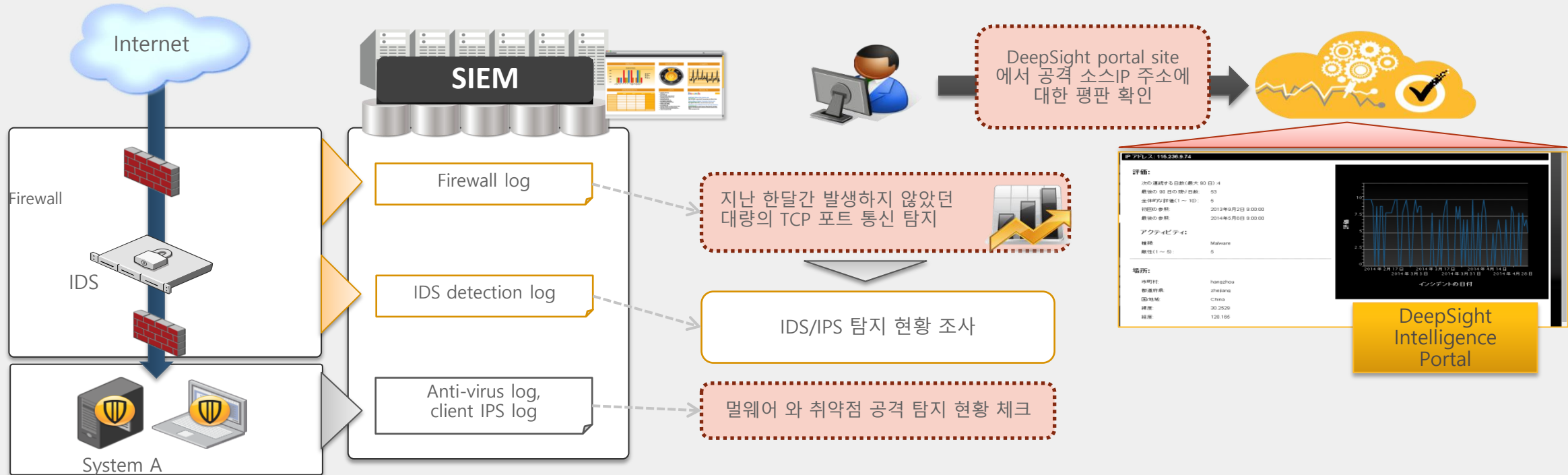
IP	Confidence	Hostility	Reputation	Behavior	Consecutive Listings	Listing Ratio
24.232.31.249	4	N/A	2	bot	1	2
24.232.31.249	4	5	2	spam	1	2
24.229.234.67	4	N/A	2	bot	1	2
24.229.234.67	4	5	2	spam	1	2
24.231.183.143	4	N/A	2	bot	1	3
24.231.183.143	4	5	2	spam	1	3
24.101.145.40	4	N/A	2	bot	1	2
24.101.145.40	4	5	2	spam	1	2
24.107.244.83	4	N/A	2	bot	1	1
24.107.244.83	4	5	2	spam	1	1

As is 기존 대응

To be Splunk+DeepSight

Case Example of SIEM and DeepSight

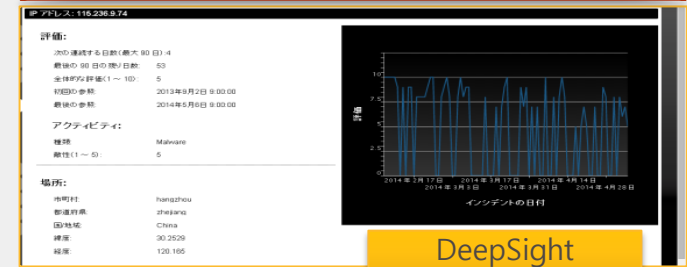
- 통계 분석에 의한 비정상적인 통신의 감지 (비정상 탐지)



지난 한달간 발생하지 않았던 대량의 TCP 포트 통신 탐지

IDS/IPS 탐지 현황 조사

멀웨어 와 취약점 공격 탐지 현황 체크



예) 다음과 같은 기준으로 처리를 실시

- 극히 악성 IP 주소로 판명 된 경우 by DeepSight
- 클라이언트에서 알려지지 않은 실행형 파일 다운로드 탐지
- 클라이언트 IPS 에서 처리된 것으로 판명
- 시스템 담당자가 오탐지 한것으로 확인

High

MID

LOW

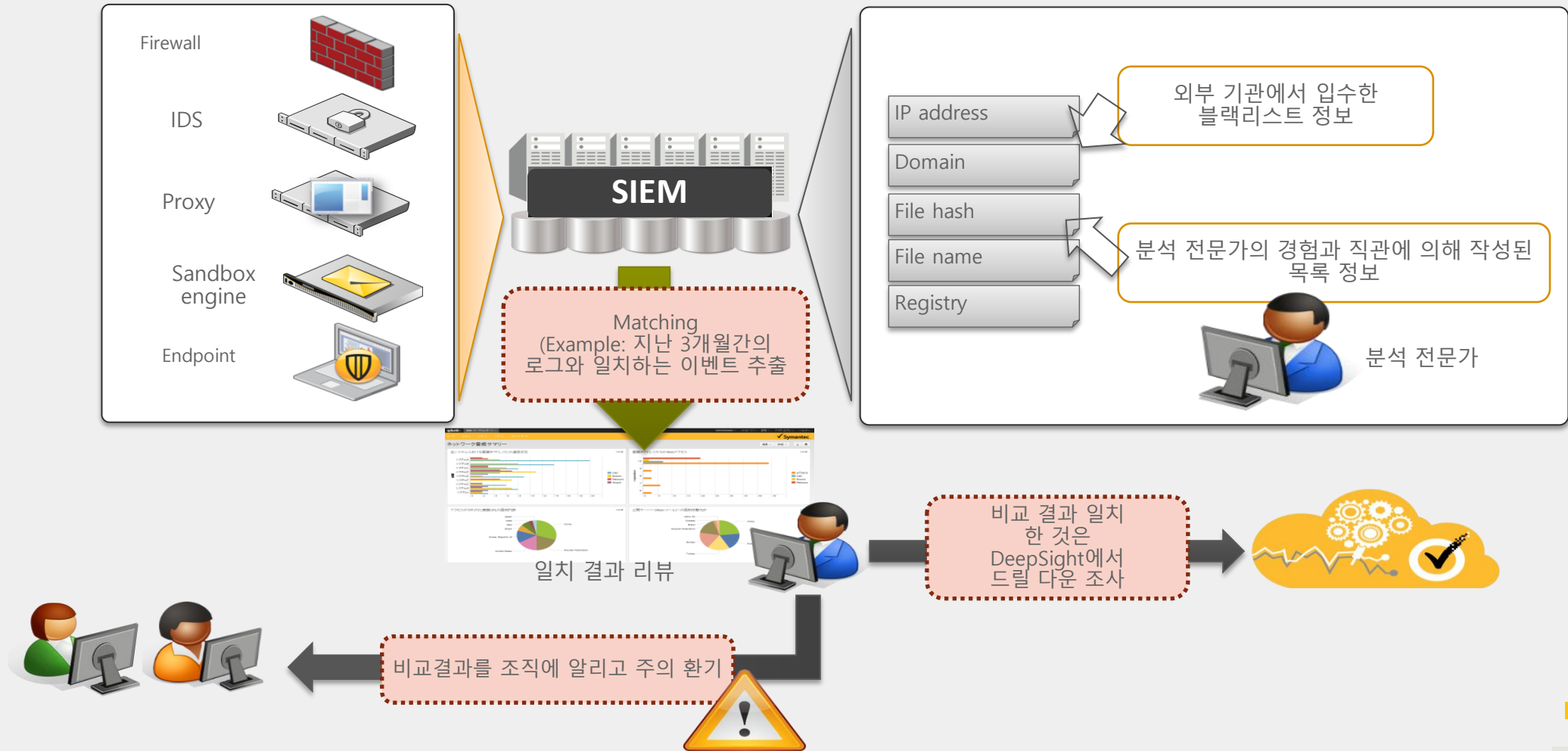
LOW

As is 기존 대응

To be Splunk+DeepSight

Case Example of SIEM and DeepSight

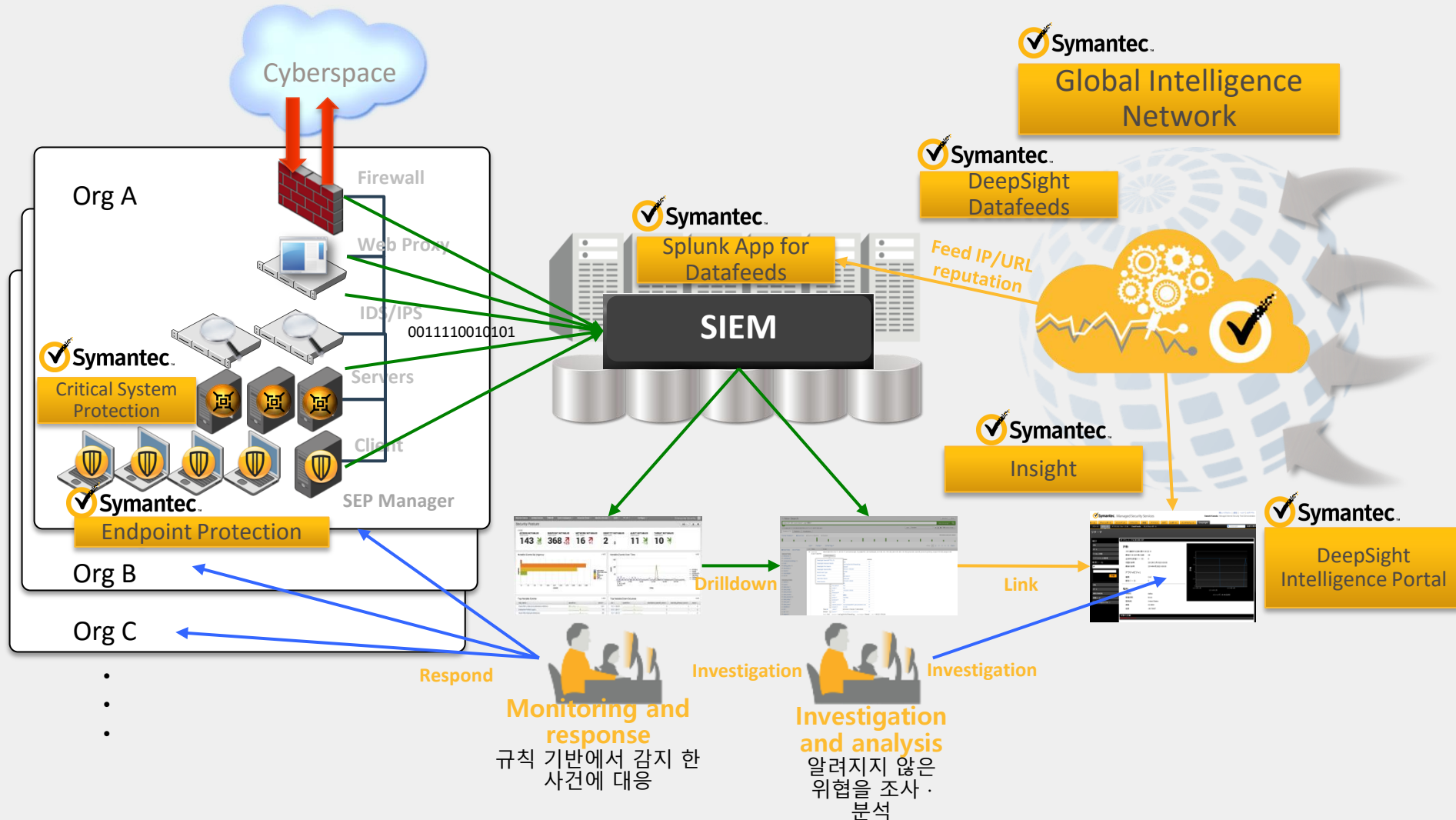
- 외부 기관 또는 내부에서 제공된 블랙 리스트와의 비교 간소화





Summary

Overview of Proposed Solution



Advantages in Utilizing Proposed Solution



Quality

- ✓ 위협 탐지의 차별화
- ✓ 처리를 하는데 있어서 판단의 차별화



Speed

- ✓ 조사 분석의 속도
- ✓ 엔드 포인트 처리 속도



Skill

- ✓ "실제 업무를 통해"사안 대처 능력의 육성
- ✓ 위협 정보 분석 능력 향상



Thank you!

최재우 부장

Jae-woo_choi@symantec.com

02) 3468-2141

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.