위협 차단 중심

차세대 방화벽

Jongman Kim, CSE, GSSO APJ

Cisco Systems

Apr 2017

지능화 되는 보안 위협

Phishing, Low Sophistication

Hacking Becomes an Industry

Sophisticated Attacks, Complex Landscape

1990 1995 2000 2005 2010 2015 2020

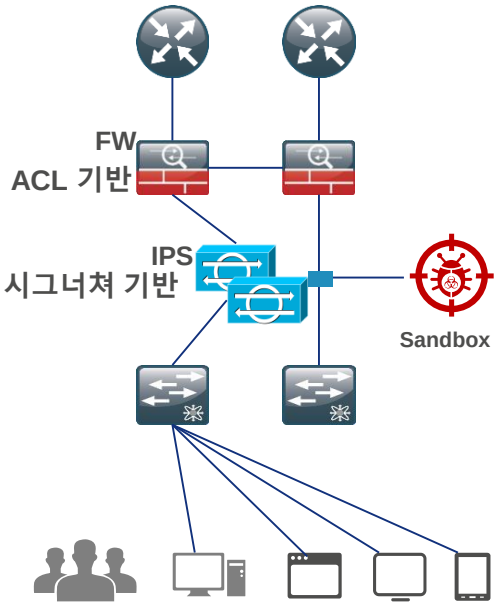
바이러스
1990–2000

웜
2000–2005

스파이웨어, 루트킷
2005–Today

APTs 크라임웨어
Today +

일반적인 네트워크 보안 구성



단순 Signature ?

Silo – Not talk

보안 위협은 여전히 증가

보안 강화에 가장 큰 걸림돌

제약조건

35%
예산
(-4%)

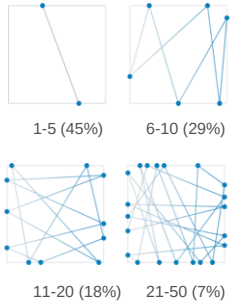
28%
호환성 이슈
(-4%)

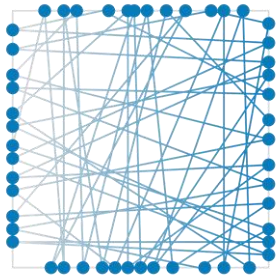
25%
전문인력부족
(+3%)

25%
각종 인증
(+/-0%)

(Change from 2015)

복잡도



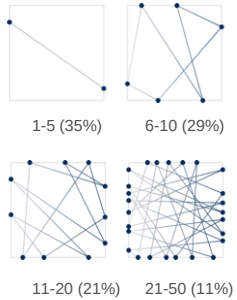


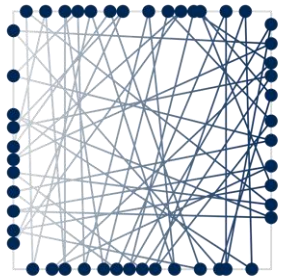
벤더

55%

의 기업이 보안 벤더 6 >50 개 사용

2016 (n=2,850)





제품

65%

의 기업이 6 >50 개의 보안 제품 사용

2016 (n=2,860)

통합(Integration)의 필요성?

Next Generation FireWall… Gartner

Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An **NGFW** should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated.

1. 기존(Legacy) 방화벽 역할(Port/Protocol/IP inspection and blocking)
2. 어플리케이션/사용자ID 로 차단(Application level inspection)
3. **IPS (Deep-packet inspection)**
4. **외부의 Intelligence 를 활용.**

동적 위협 차단 방안

동적 환경에 대응 하는 위협 차단

일반적 동작

시그너쳐 기반

WinXP

동적 환경에 대응

실시간 네트워크 인지

위협 차단 기반 NGFW

OS, Application

룰 자동화

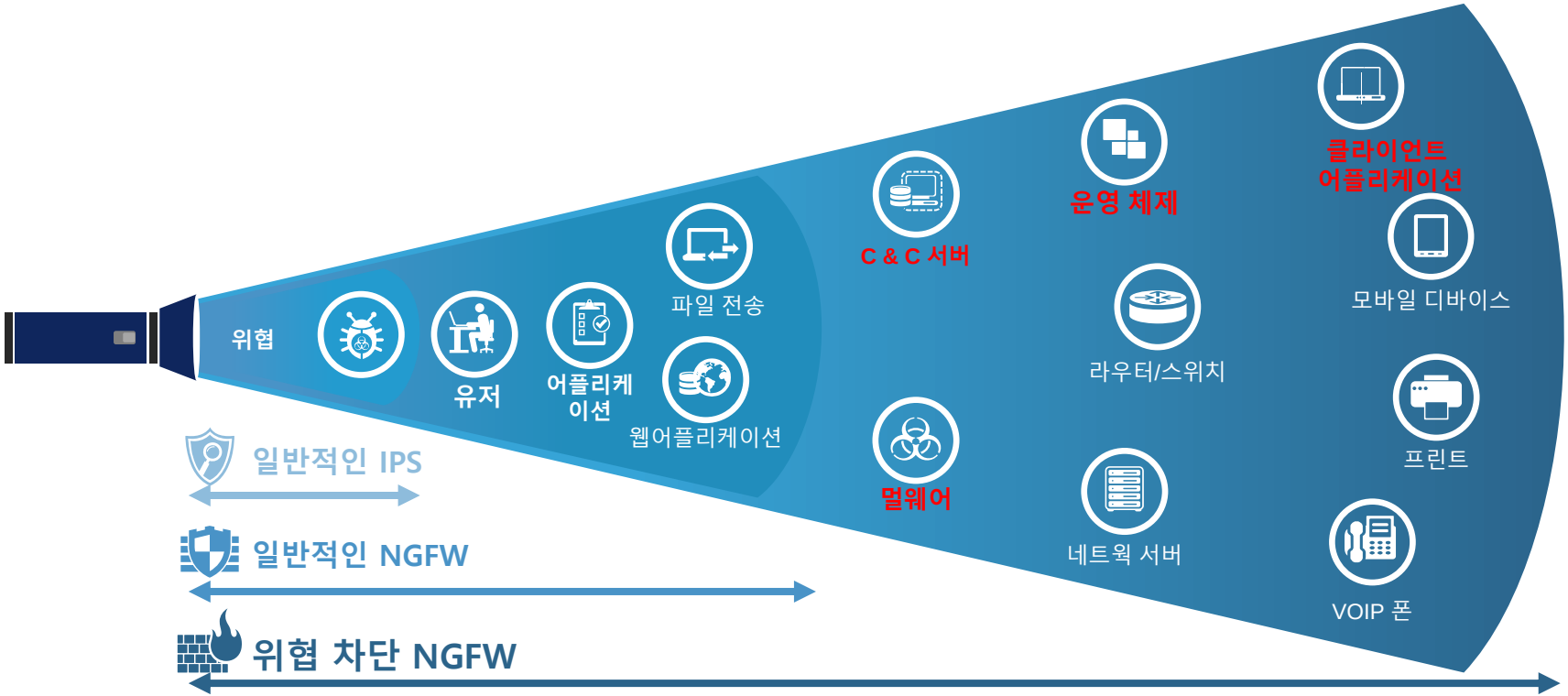
상관 관계 분석

영향도 분석

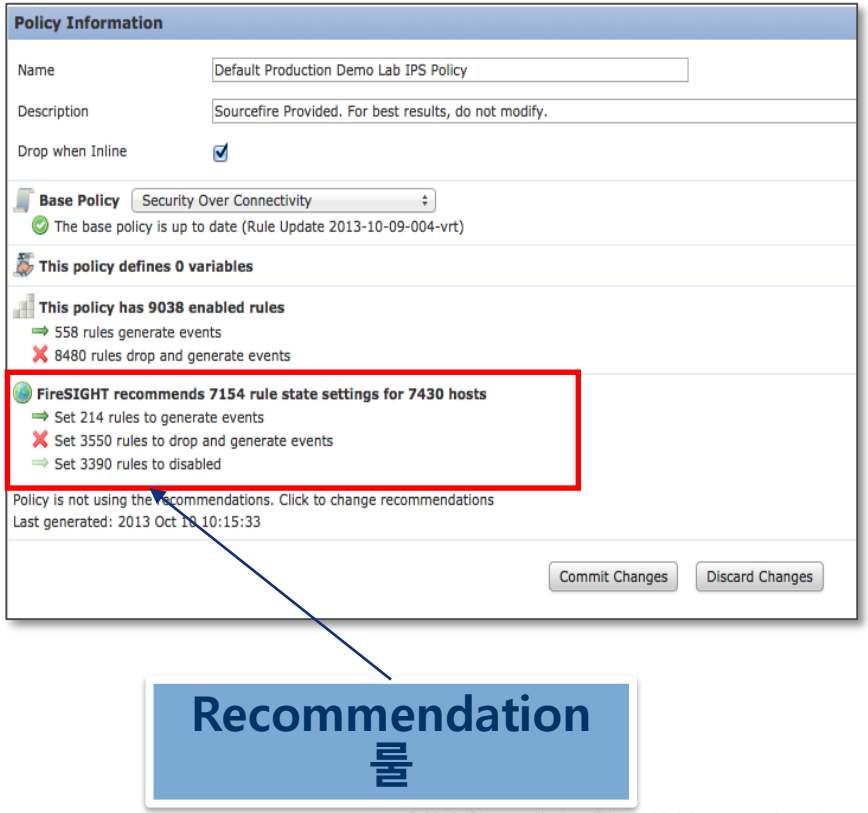
Traffic

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Microsoft Internet Explorer 6 on Windows XP"; flow:to_server,established; content:".php?a=h4"; http_uri; content:".php?a=h1&f="; fast_pattern:only; http_header; content:"&u=Mozilla"; http_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2011-1255; reference:cve,2013-1489; reference:url,jsunpack.jeek.org/?report=2a298ffa14fd2772bd646bd559f610b0c3b51862; reference:url,jsunpack.jeek.org/?report=977b49ea5dc5ef85d8f50d1f1222befee8bf3581; classtype:trojan-activity; sid:30006; rev:2; gid:1;)

실시간 네트워크 인지 기반 위협 차단

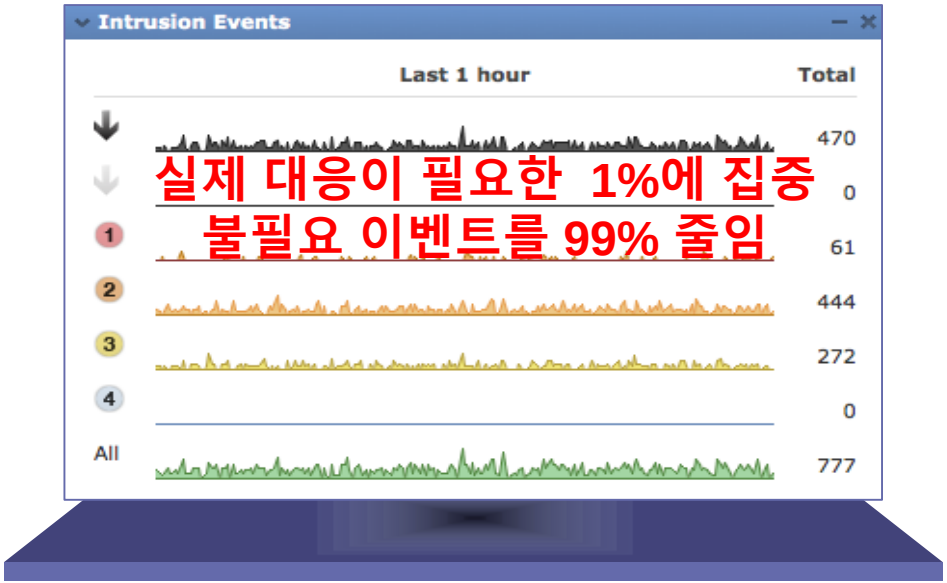


룰 자동화



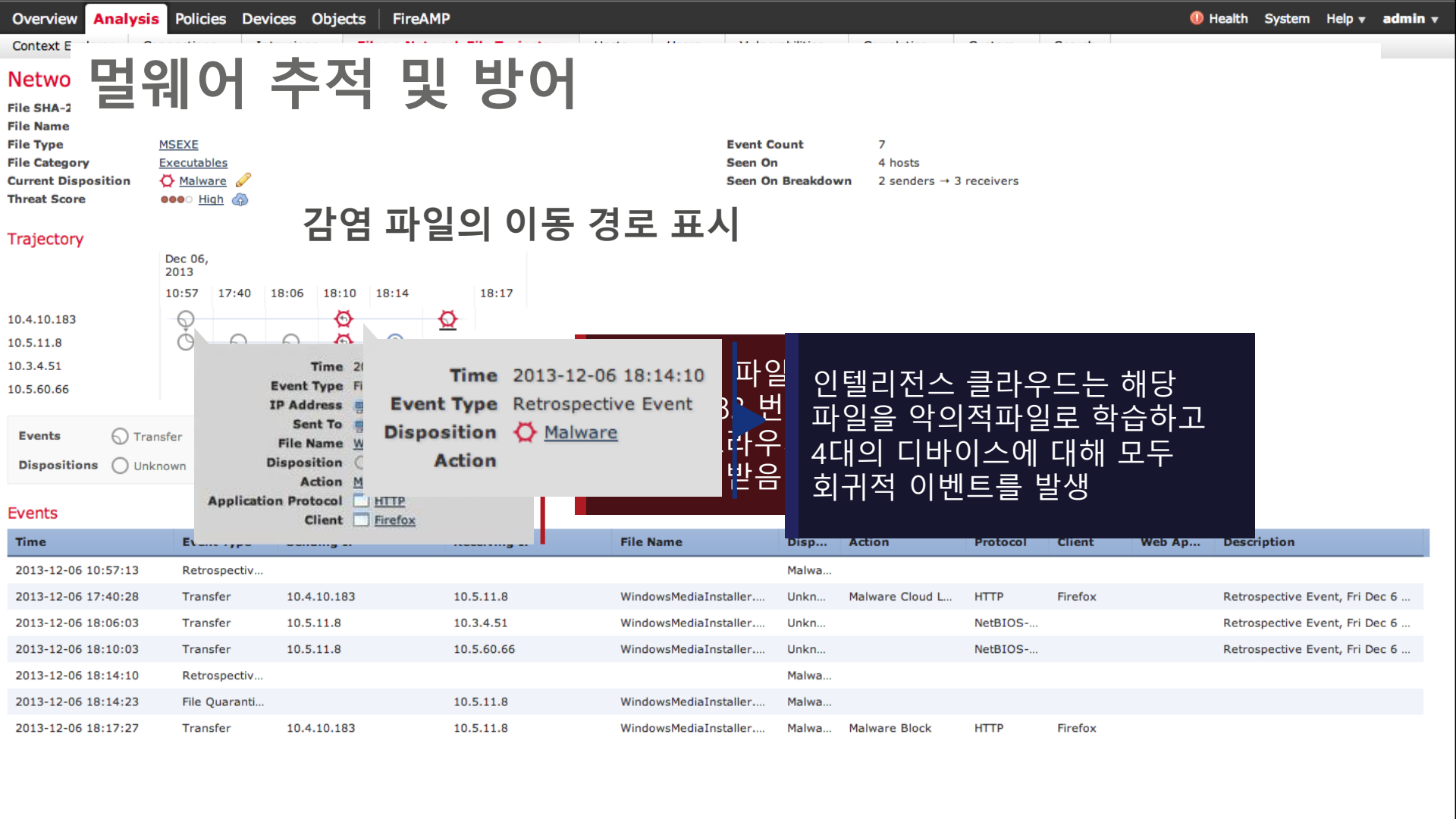
위협 영향도 분석

모든 침입 이벤트에 대한 연관성을 분석하여 공격 및 위협에 대처



영향도 플래그	관리자 조치 사항	이유
1	**즉각 조치 필요, 취약함**	**이벤트 연관성이 호스트 취약점과 매핑됨**
2	조사 필요, 잠재적 취약	관련있는 포트가 오픈또는 프로토콜이 사용중, 그러나 취약점은 매핑되지 않음
3	관심 필요, 현재는 취약하지 않음	관련있는 포트가 오픈되지 않았고, 프로토콜도 미사용중임
4	관심 필요, 알려지지 않은 타겟	네트워크 모니터링함, 그러나 알려지지 않은 호스트
5	관심 필요, 알려지지 않은 네트워크	모니터되지않은 네트워크

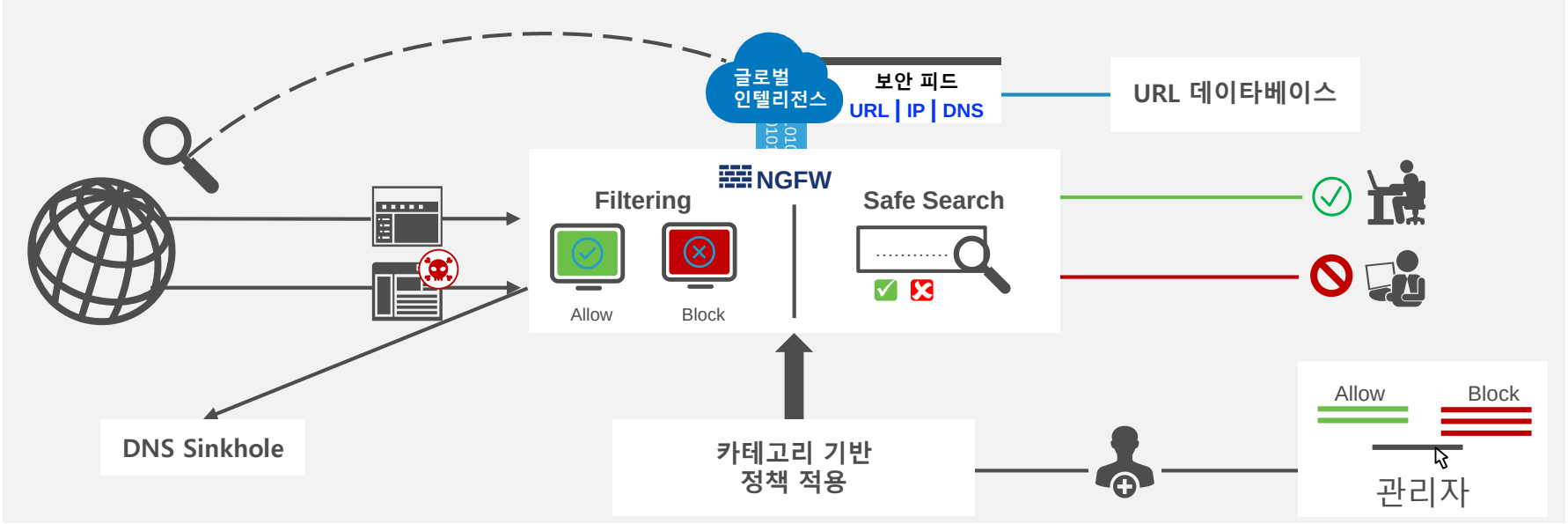
멀웨어 추적 및 방어


Overview
Analysis
Policies
Devices
Objects
FireAMP
Health
System
Help
admin
Netwo
File SHA-2
File Name
File Type
MSEXE
File Category
Executables
Current Disposition
Malware
Threat Score
High
Event Count
7
Seen On
4 hosts
Seen On Breakdown
2 senders → 3 receivers
감염 파일의 이동 경로 표시
Trajectory
Dec 06, 2013
10:57
17:40
18:06
18:10
18:14
18:17
10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66
Events
Transfer
Dispositions
Unknown
Time
Event Type
IP Address
Sent To
File Name
Disposition
Action
Application Protocol
HTTP
Client
Firefox
Time 2013-12-06 18:14:10
Event Type Retrospective Event
Disposition Malware
Action
인텔리전스 클라우드는 해당 파일을 악의적파일로 학습하고 4대의 디바이스에 대해 모두 회귀적 이벤트를 발생
Events
Time
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

보안 인텔리전스

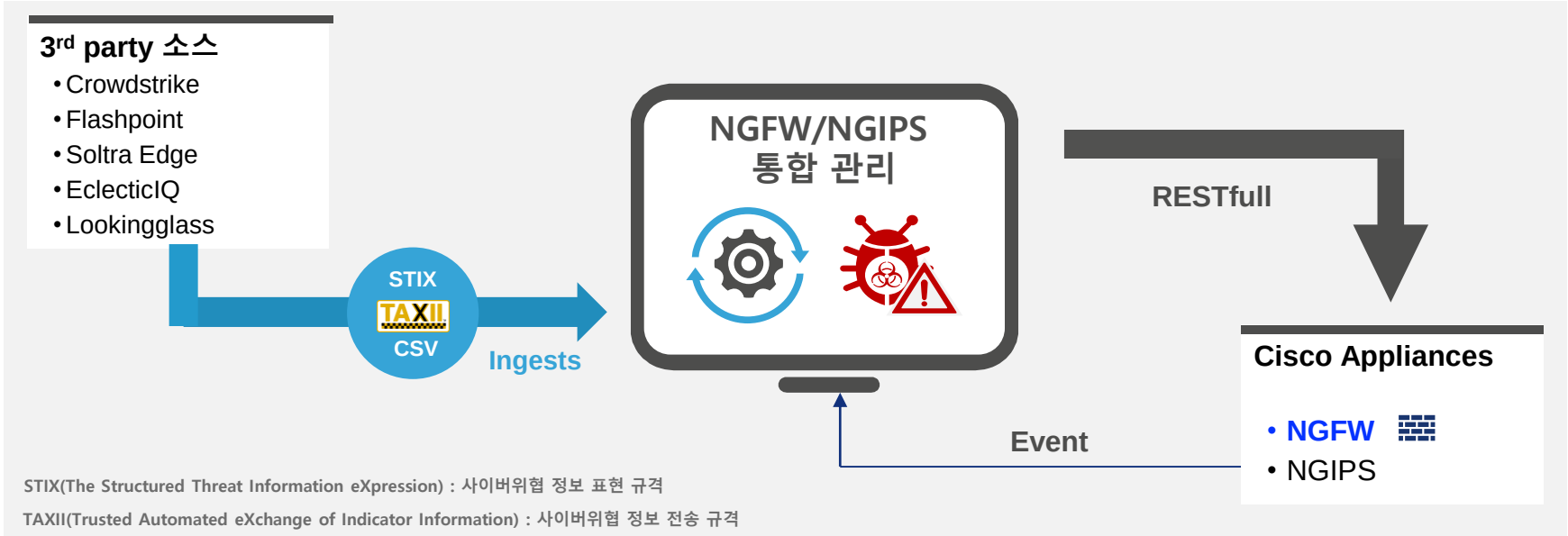
보안 위협 인텔리전스란?

보안 위협 인텔리전스 장점



모든 Packet 의 패턴 매칭 대비 Performance 향상

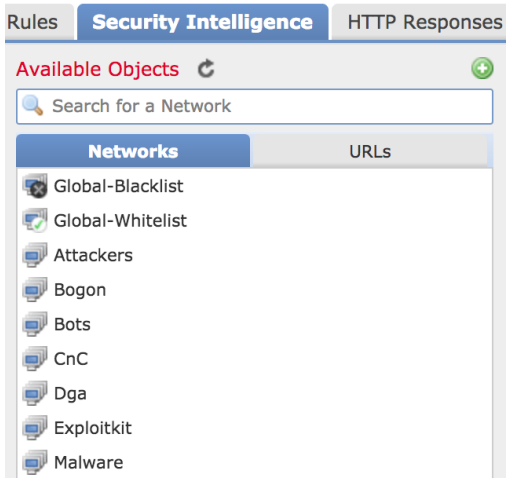
3rd party 위협 인텔리전스 활용

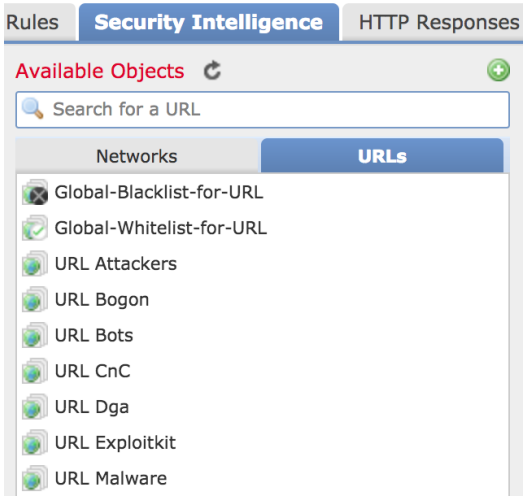


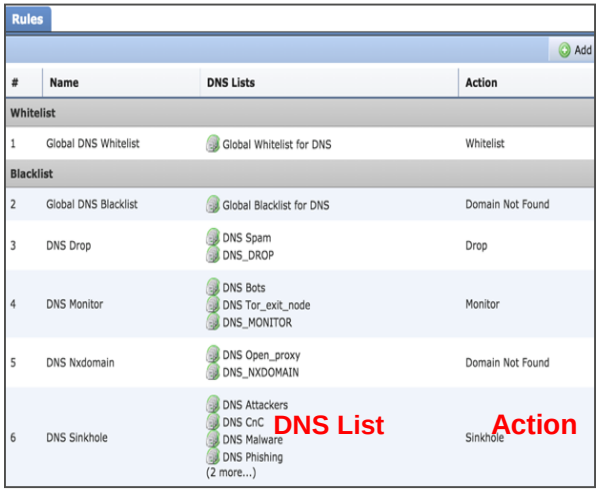
Free TAXII intelligence source

URL: http://hailataxii.com/taxii-discovery-service

보안 위협 인텔리전스 예







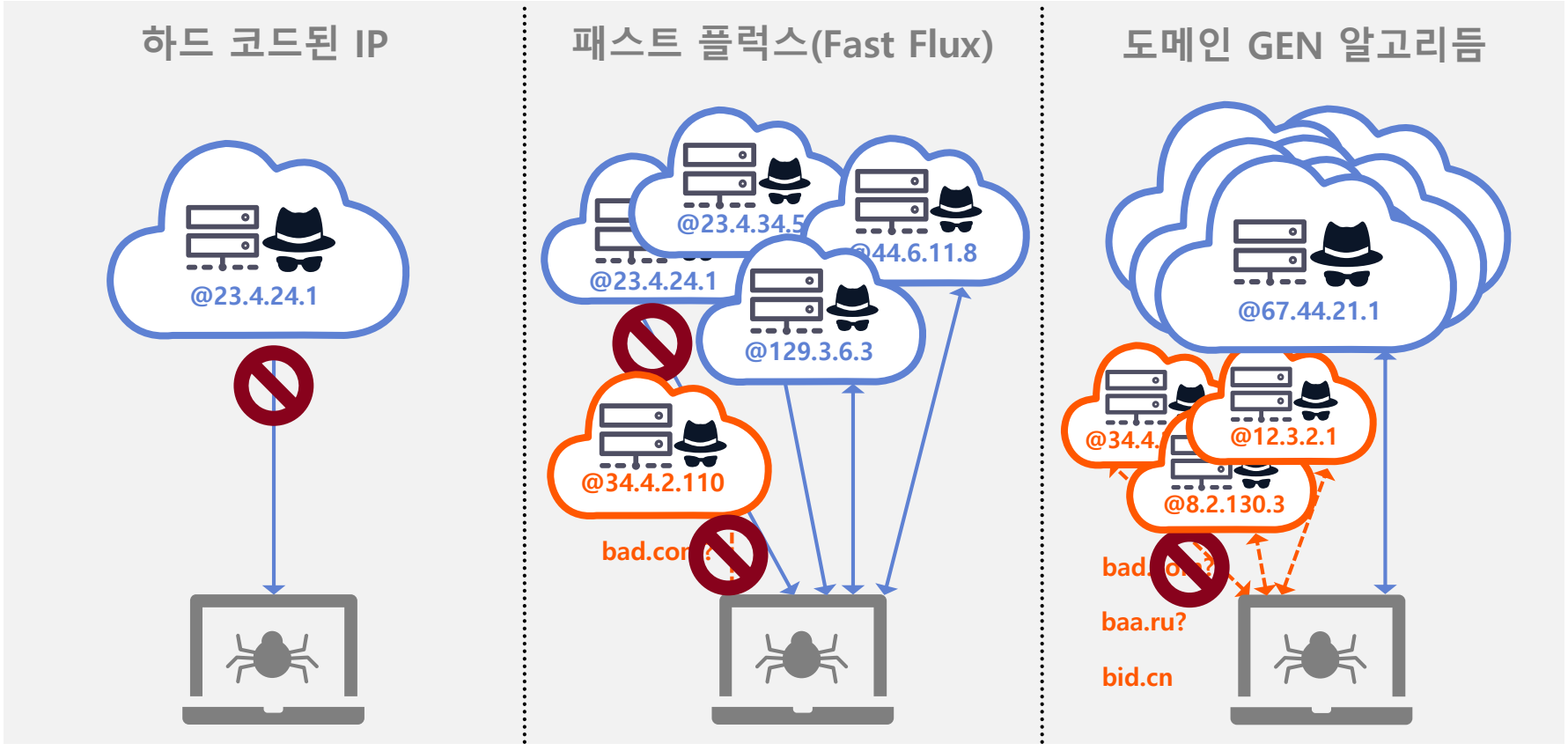
Network-SI 카테고리

URL-SI 카테고리

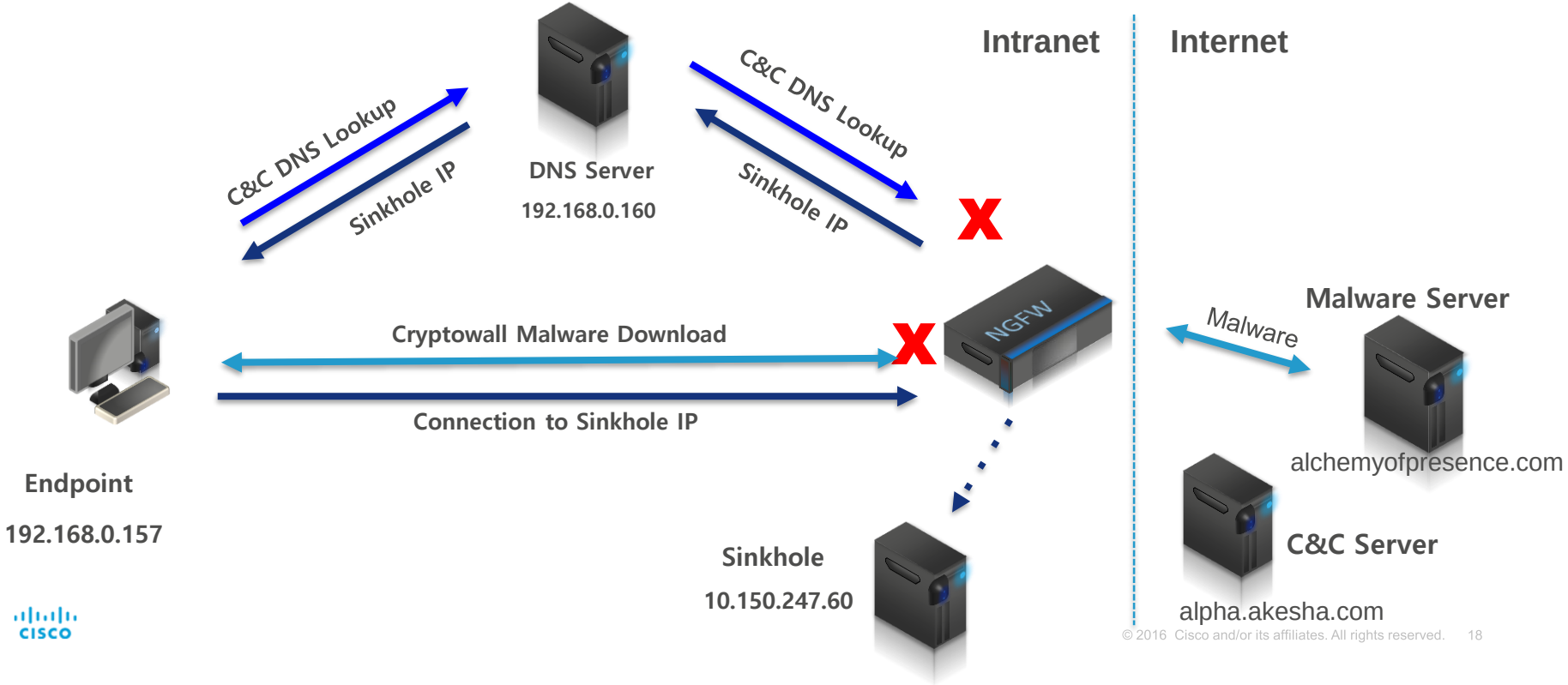
DNS-SI 카테고리

C&C (C2) 콜백의 진화

https://en.wikipedia.org/wiki/Command_and_control_(malware)



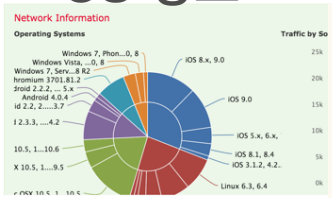
Angler & Cryptowall 방어 예



Cisco 차세대 방화벽

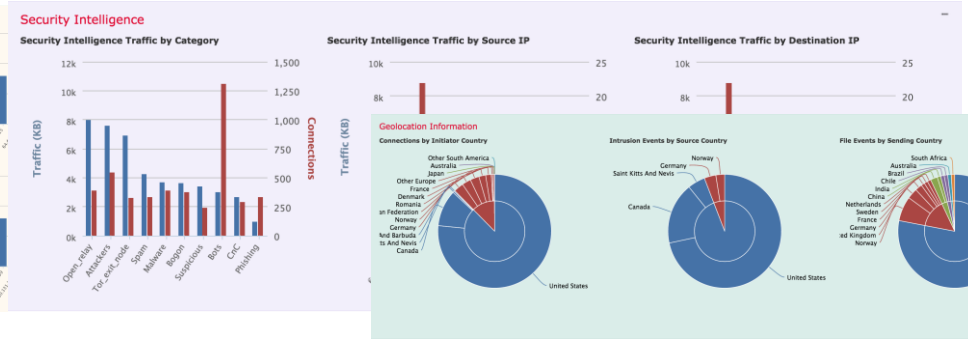
가시화 기반의 위협 차단

OS 정보



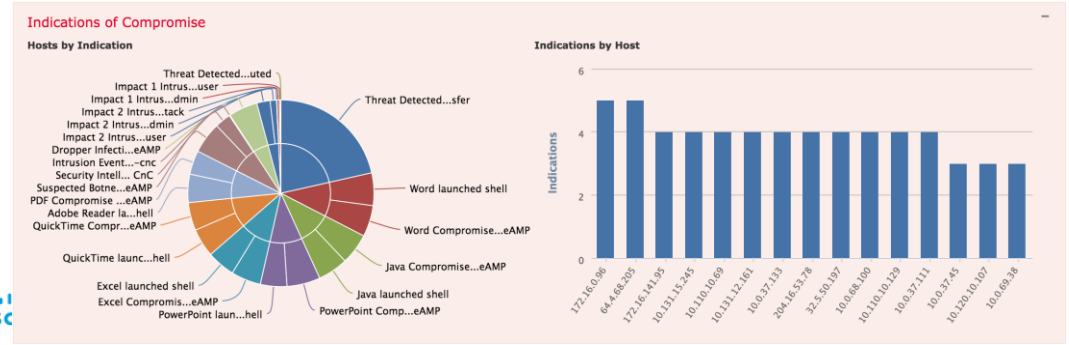
IPS 정보

평판 정보



Geo Location 정보

감염 정보



파일(APT) 정보

시스코 보안 위협 인텔리전스

TALOS

보안 인텔리전스

1.5 million daily malware samples

600 billion daily email messages

16 billion daily web requests

시스코 보안 장비


Endpoints

WW Web

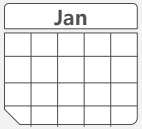

Networks


NGIPS


Devices

Research Response


250+ Researchers



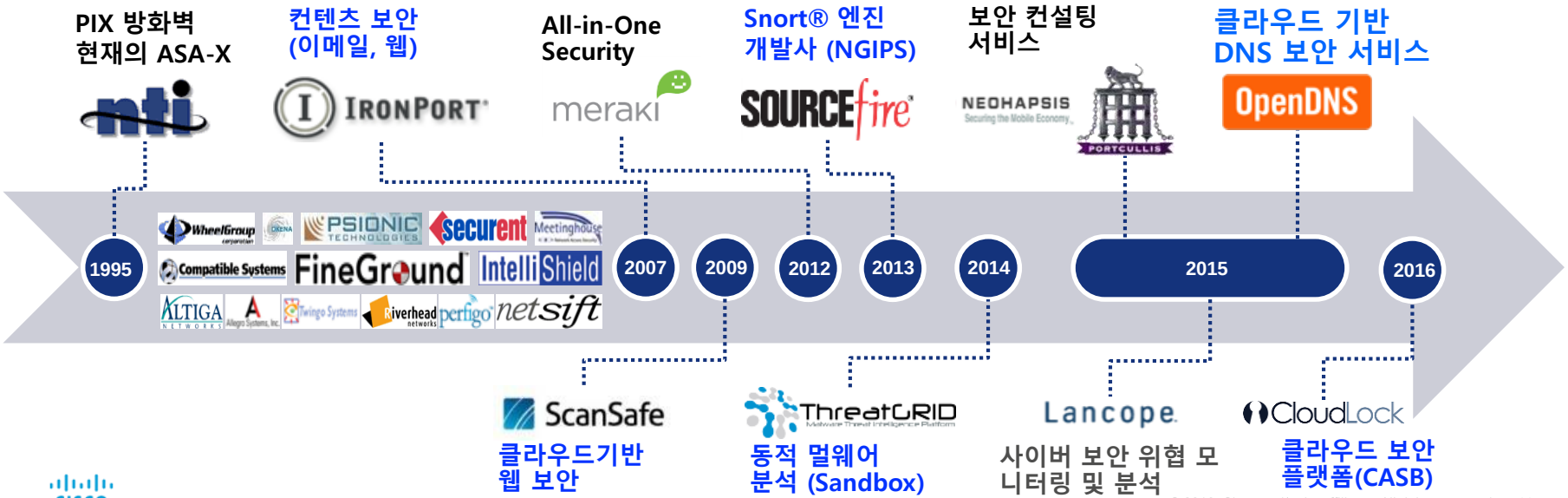
24 x 7 x 365 Operations

Dynamic 한 위협에 대해 실시간 대응

Why 시스코 TALOS?

시스코 TALOS

인수 합병을 통한 최고의 인텔리 전스 구축



시스코 위협 차단 중심의 차세대 방화벽

Cisco Firepower™ NGFW

위협 탐지/차단

가시성

TTD

단순화

효율성

위협 차단

보안 인텔리전스

시스코 위협 차단 중심의 차세대 방화벽


CISCO

지능화 되는 보안 위협

간편하고 효과적인 암호화와 공격킷트 및 피싱의 대중화로 감염자들의 증가와 비용 지불등 이런 형태는 랜섬웨어의 변종을 다양하게 만들어 내게 되었음