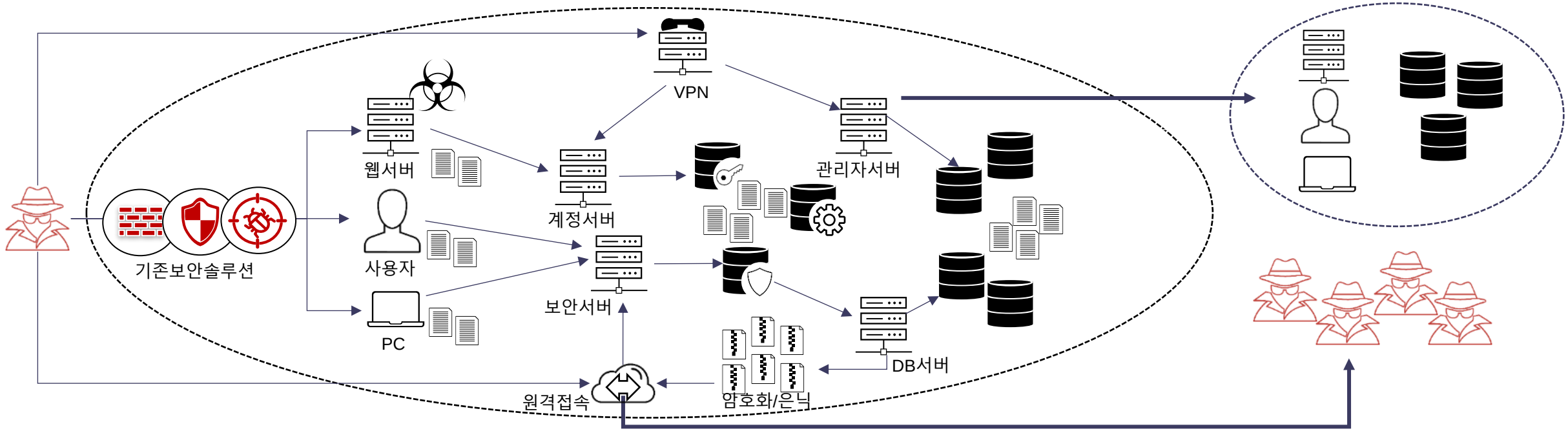
NETWITNESS

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

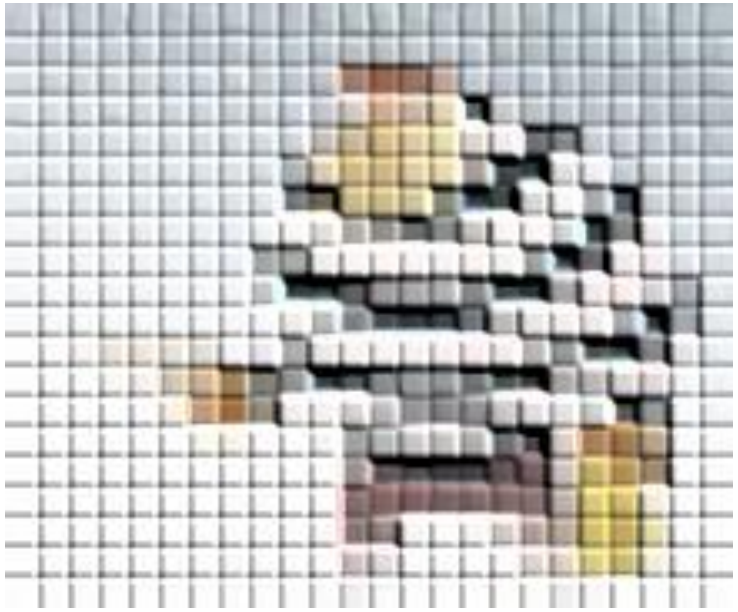
3. 정보 유출 및 추가 공격

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

NETWITNESS

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

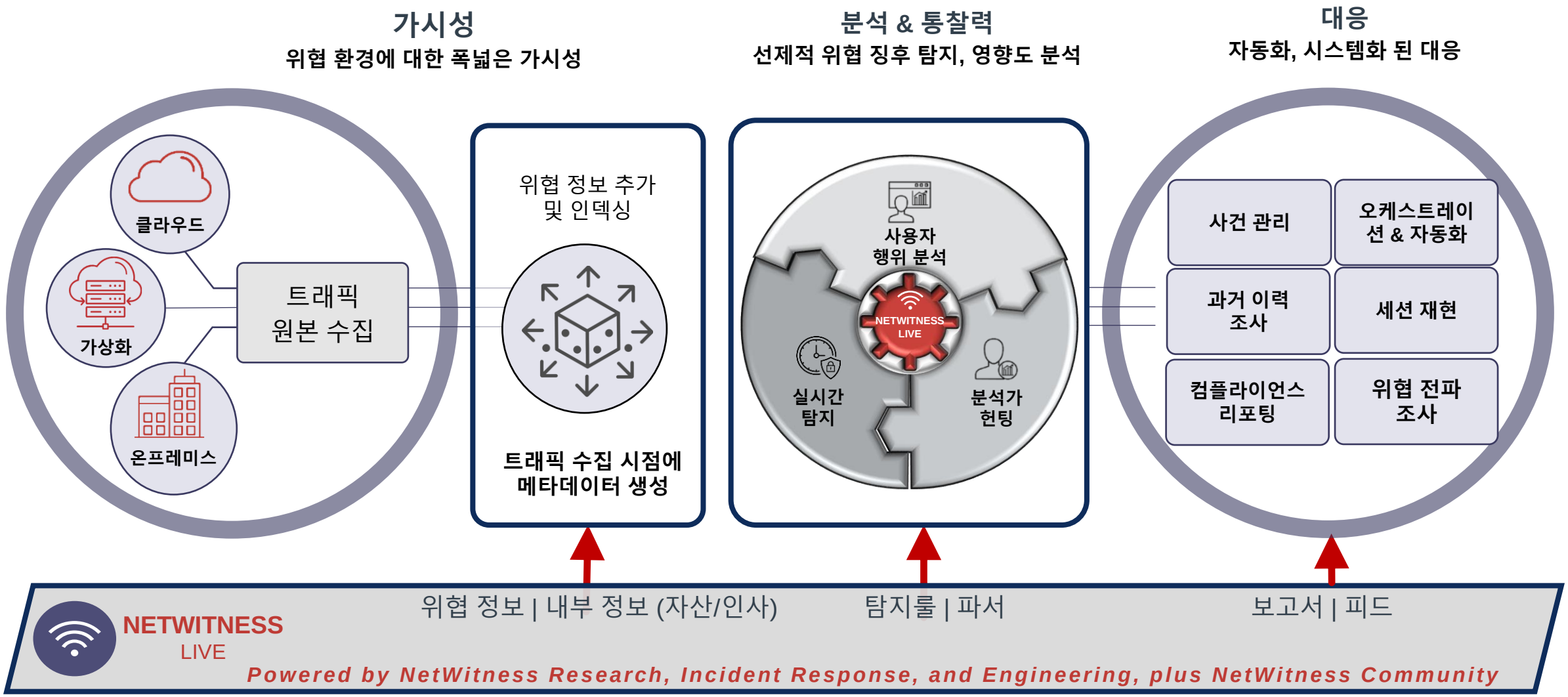
- **위협 행위 탐지**
  - 알려진 C&C 포인트 또는 감염 경로를 인식하는데 유용함
  - 비정상적인 연결 / 일반적이지 않은 프로토콜 탐지

- **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

NETWITNESS

네트워크 위협 헌팅을 위한 실시간 트래픽 수집 및 모니터링



NETWITNESS

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

NETWITNESS

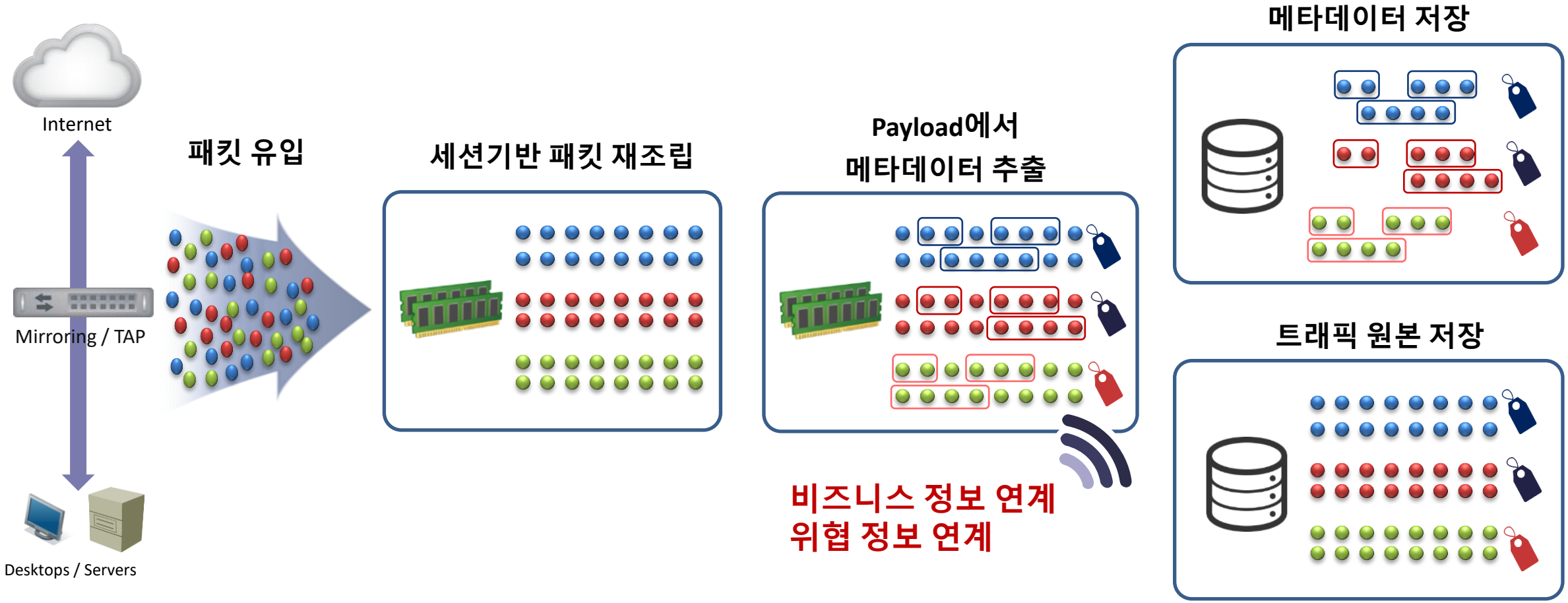
NETWITNESS

트래픽 수집/저장 및 추가 정보 연계

트래픽 수집 및 처리

실시간 이상행위 탐지를 위한 특허 받은 트래픽 처리 아키텍처

(특허: US7634557B2, US20100002704A1)



NETWITNESS

위협 인텔리전스 제공

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

RSA NETWITNESS® PLATFORM LIVE

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 Airelle Hrsk Domains
* Firebog Prigent Malware Domains
* Firebog Prigent Phishing Domains
* Firebog Shalla Malware Domains
* GreenSnow Blocklist
* Haley SSH Bruteforce IPs
* Rutgers Attacker IPs
* VXVault

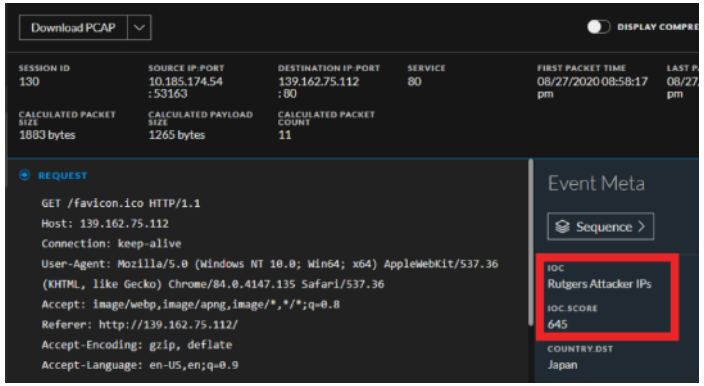
ThreatConnect의 CTI(상용 위협 정보) 제공

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

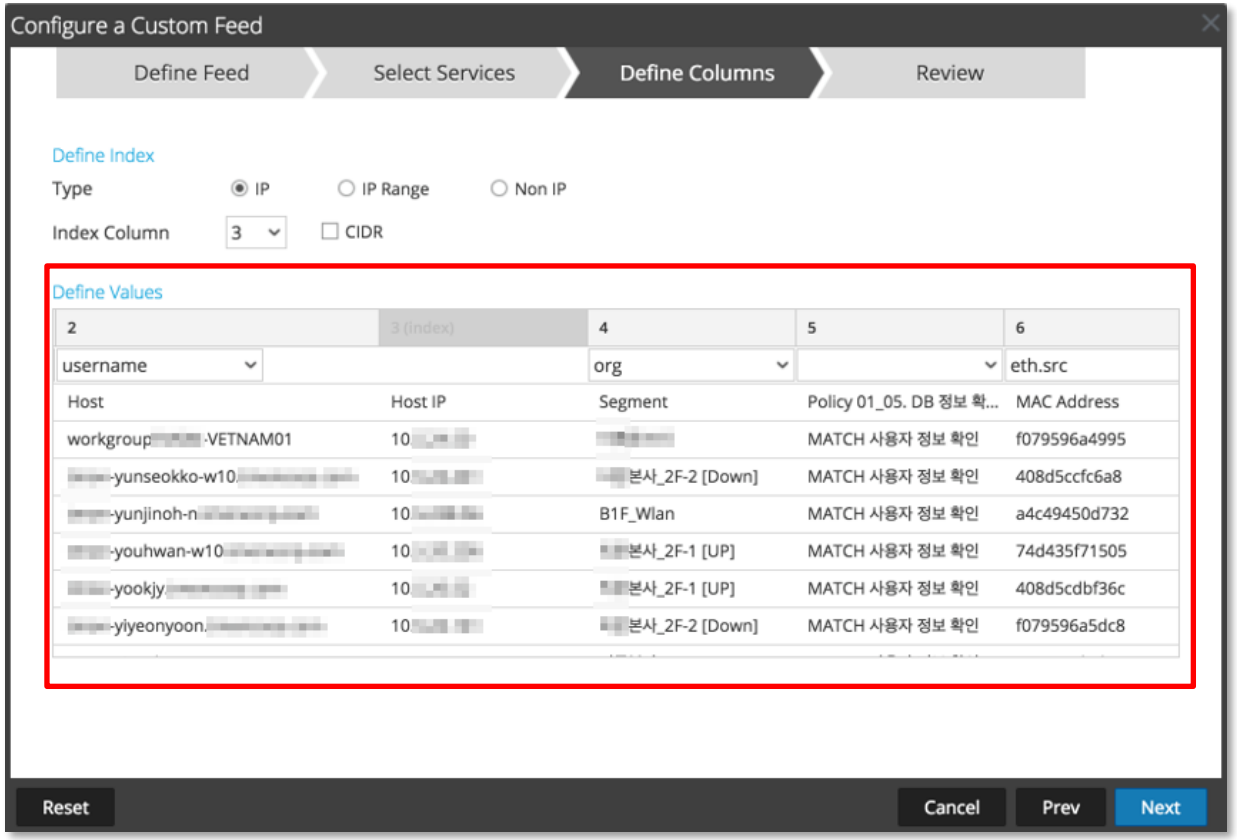


NETWITNESS

내부 환경 정보 연동

내부 환경 정보 연계를 통해 조직에 특화된 탐지/분석 체계 구현

<자산 정보 연동 예시>



- 내부 네트워크 망 정보
- 자산 항목, 담당자
- 자산 중요도

- 비즈니스 담당자
- 내부 조직, 부서
- 비즈니스 시스템 역할

NETWITNESS

메타데이터 및 위협 지표 실시간 추출

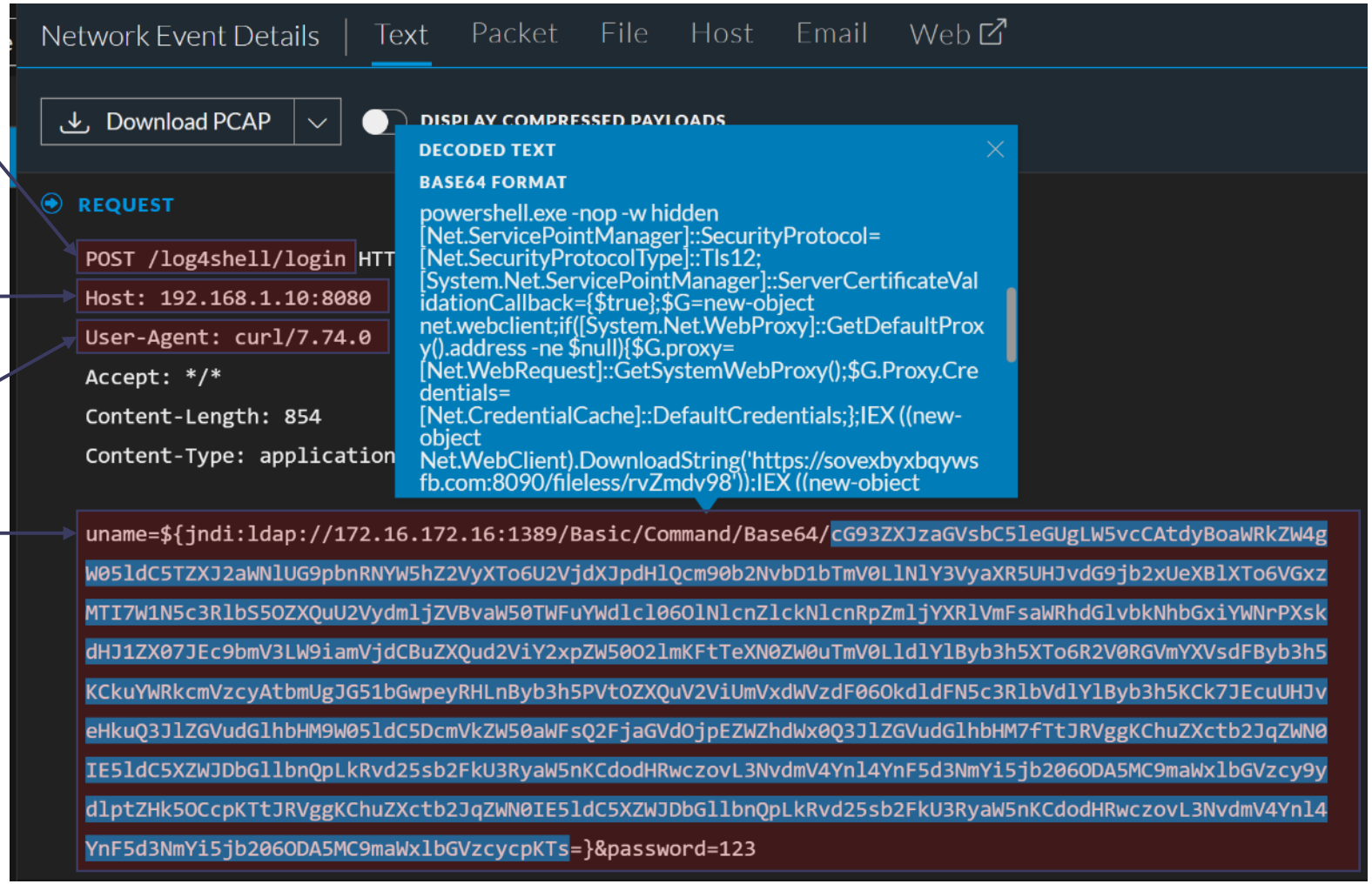
실시간으로 수집한 트래픽에서 150가지 이상의 메타데이터 및 다양한 위협지표 실시간 추출

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



NETWITNESS

메타데이터 실시간 추출 예

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

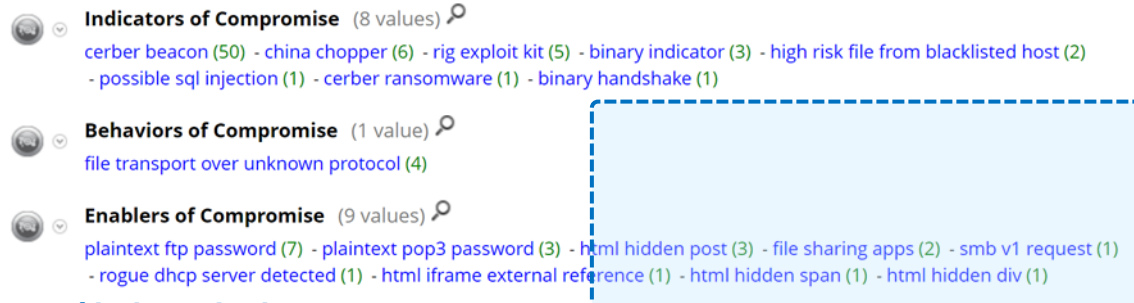
NETWITNESS

위협 지표 실시간 추출 예

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

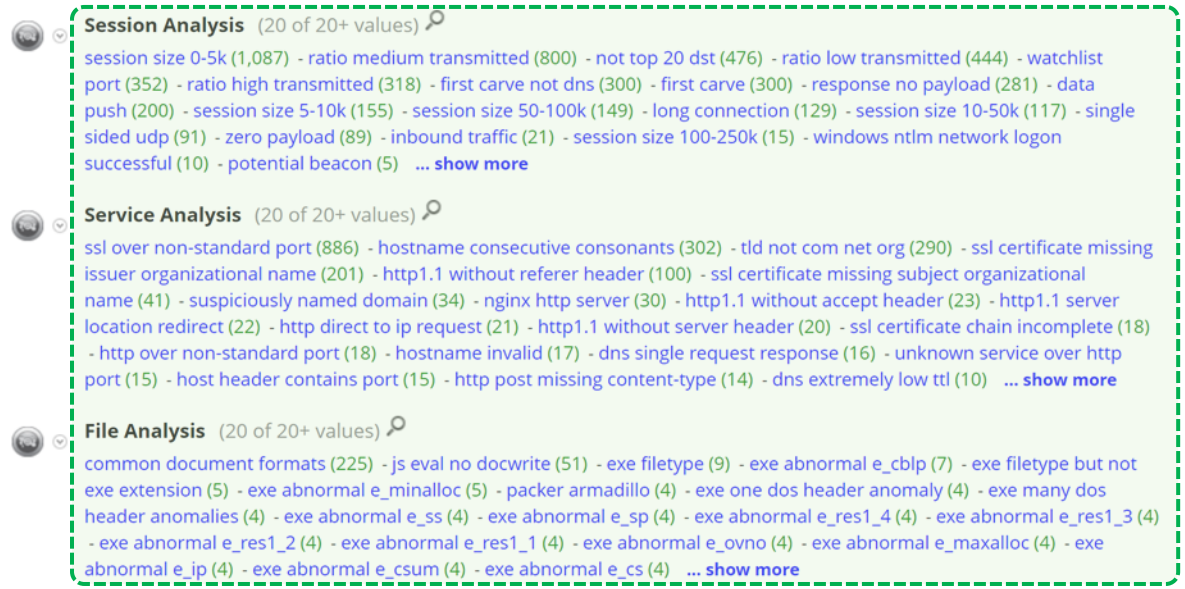
위협 관련 정보

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



침해 관련 정보

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



분석 관련 정보

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

NETWITNESS

위협 탐지 및 분석

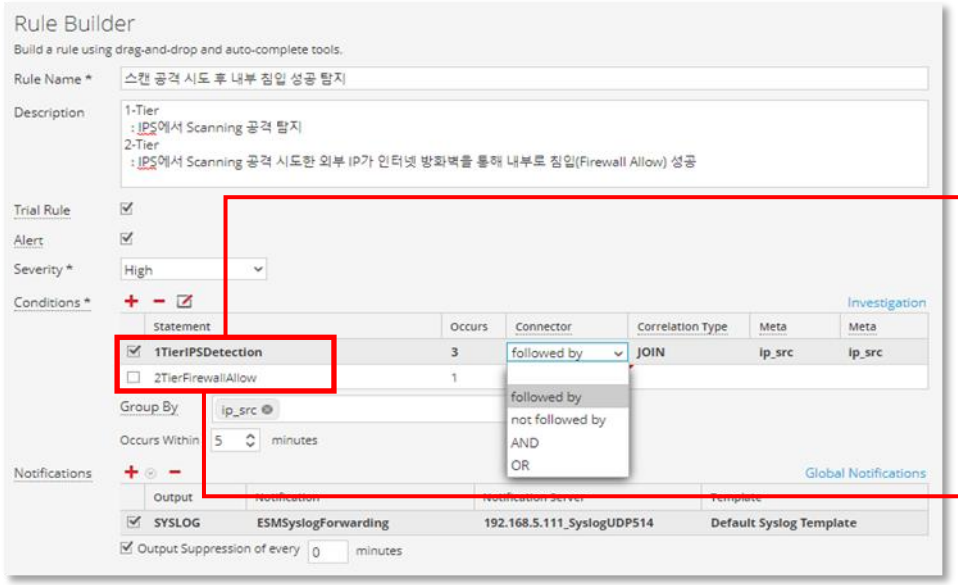
다양한 위협 지표 및 메타데이터를 이용한 실시간 연관성 분석

뛰어난 분석 능력: 고도화된 공격의 실시간 탐지

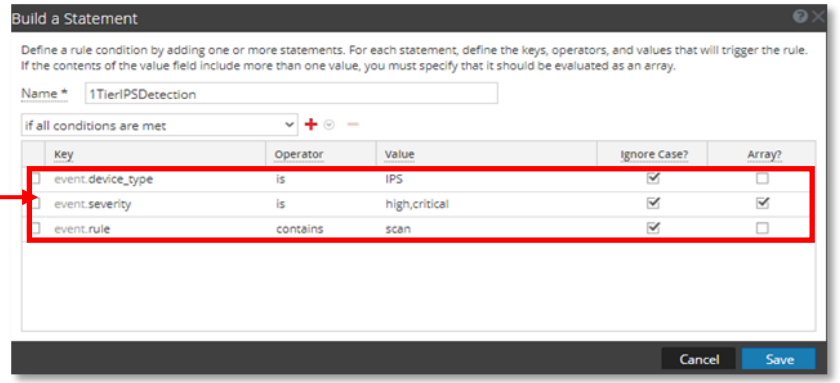
NETWITNESS

실시간 연관성 분석을 통한 행위 기반 위협 탐지

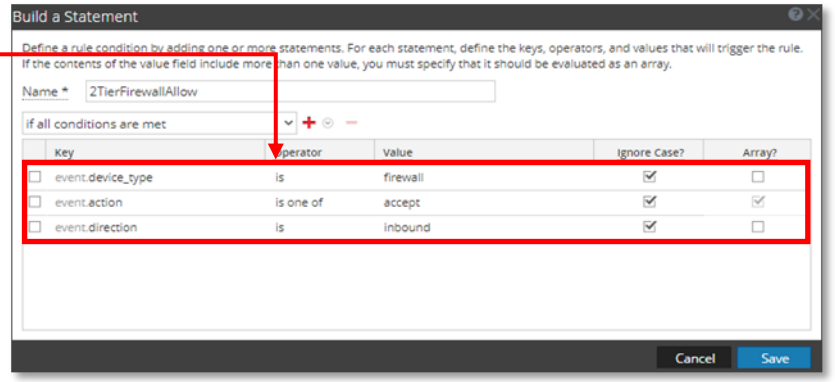
다양한 연관성 분석 탐지 시나리오 제공 및 고객 환경에 최적화된 탐지 시나리오 구현



<실시간 상관분석 탐지 정책>



<시나리오 1>



<시나리오 2>

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

NETWITNESS

유용한 연관성 분석 탐지 룰 제공

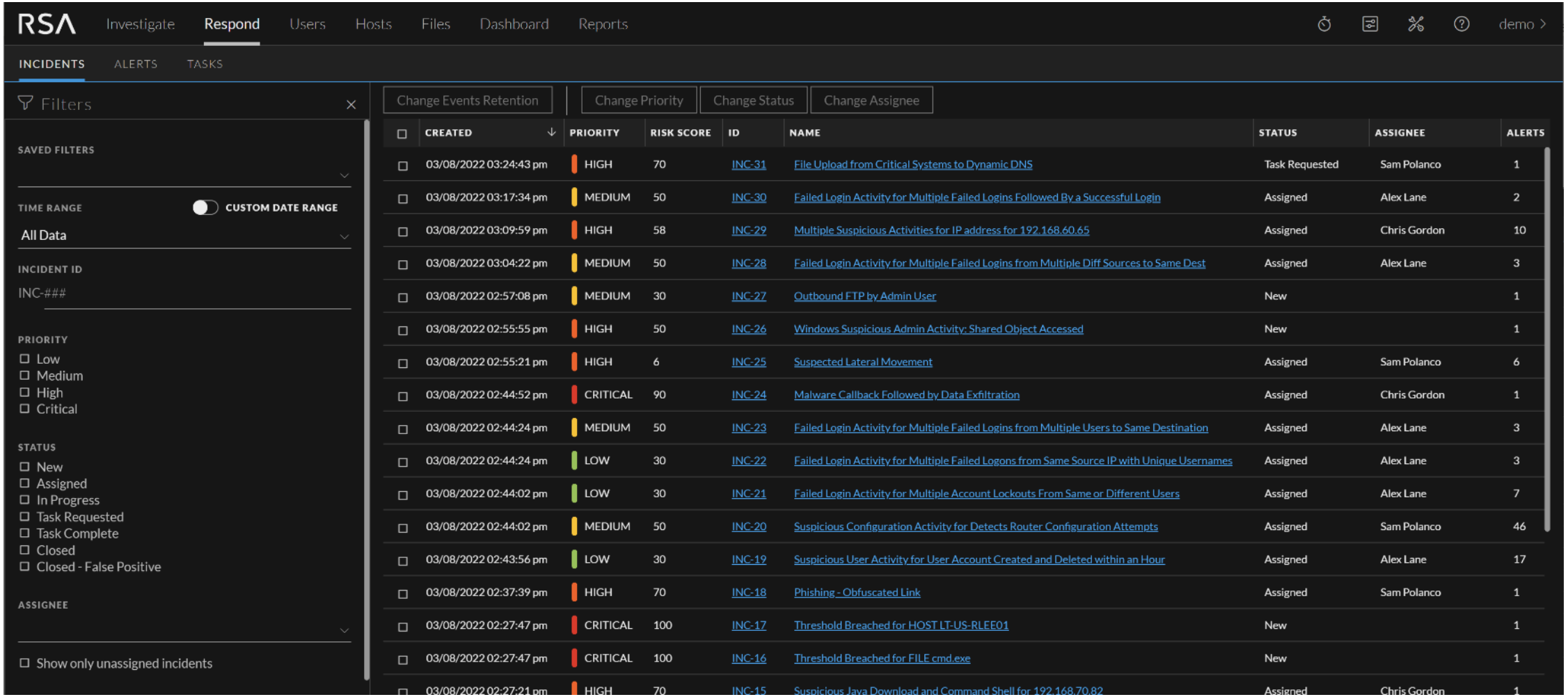
NetWitness-Live를 통해 지속적으로 업데이트되는 룰(연관성 분석) 사용

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 address 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
	Web DoS Attack
최초 침입	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

탐지 경보 취합 및 우선순위 제공

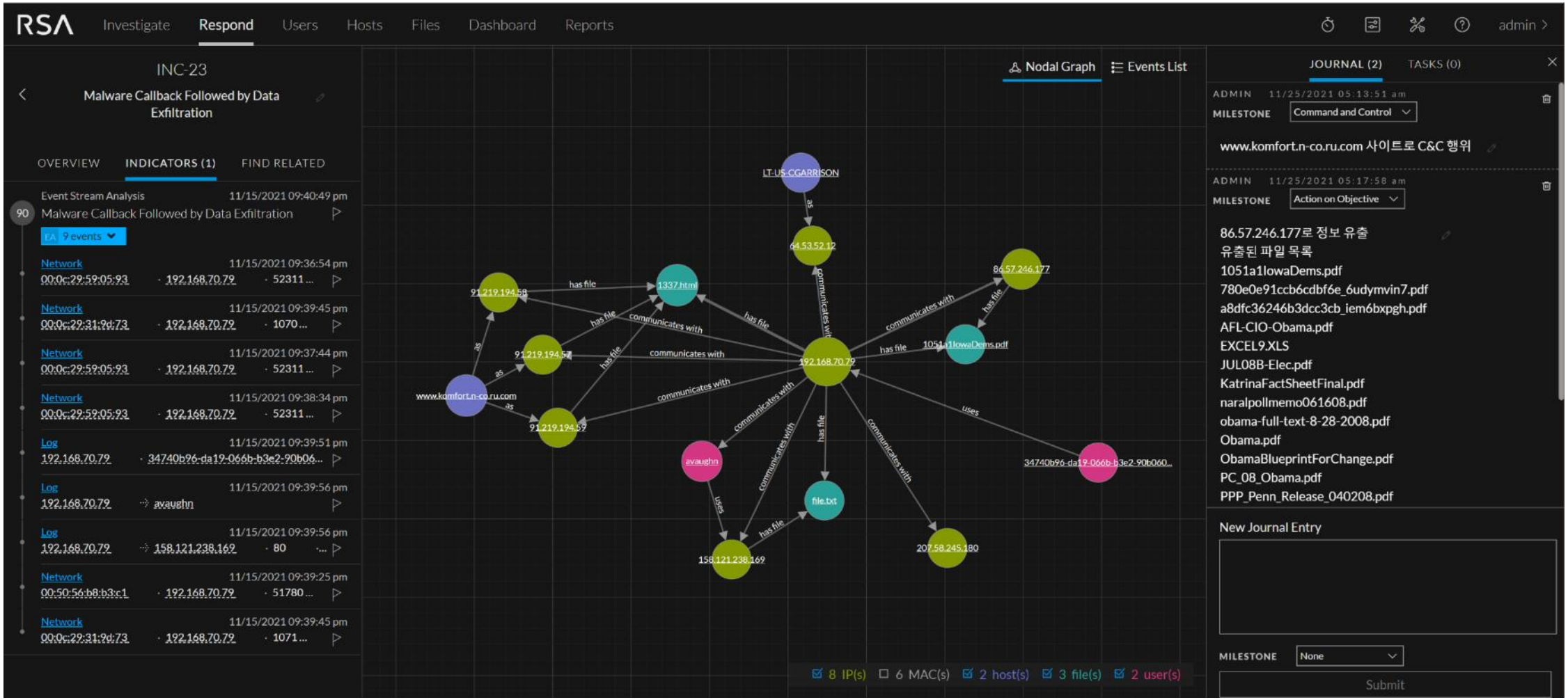
연관된 경보를 하나의 사건으로 취합하여 우선순위/위험도 점수와 함께 제공



NETWITNESS

탐지된 위협 도식화

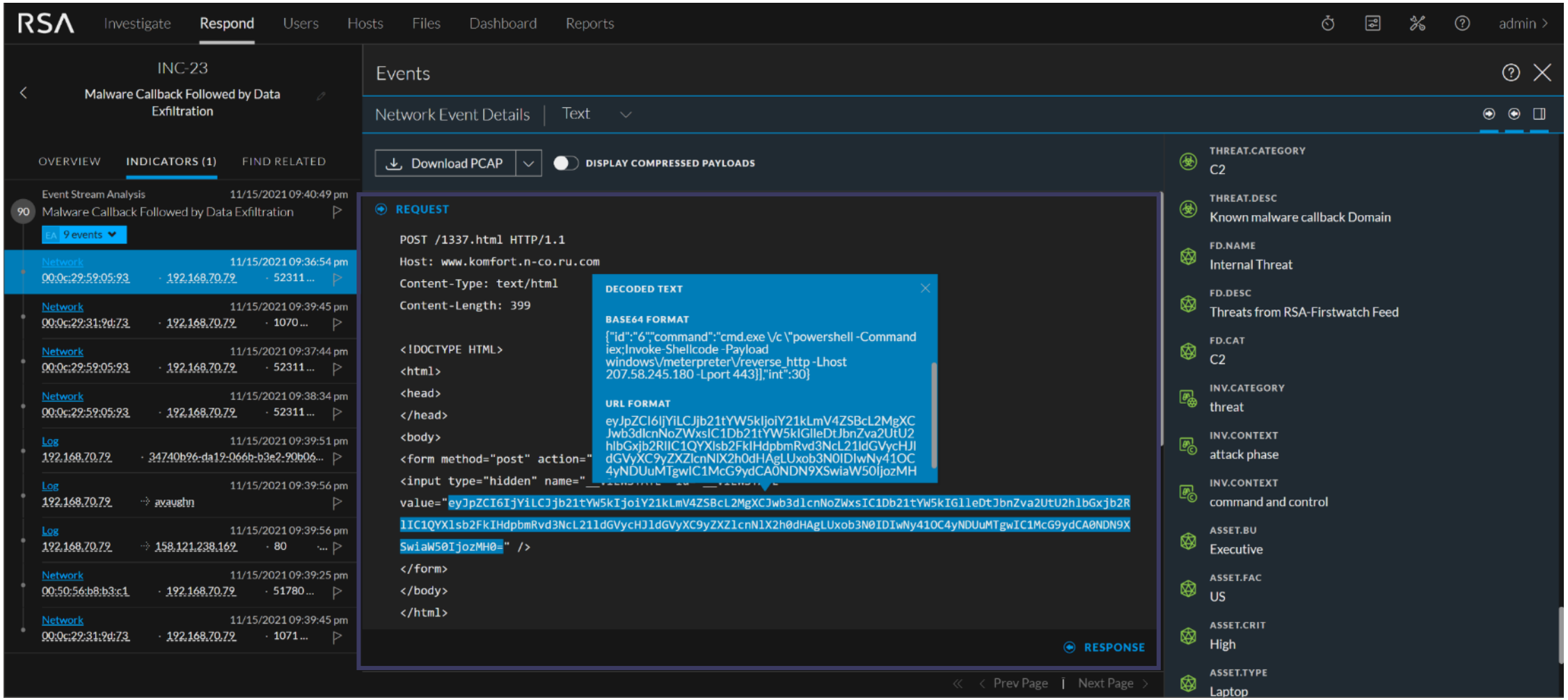
탐지된 복수의 이벤트를 취합하여 하나의 사건으로 생성 및 직관적인 공격 파악을 위한 도식화



NETWITNESS

트래픽 원본 즉시 조회를 통한 공격 확인

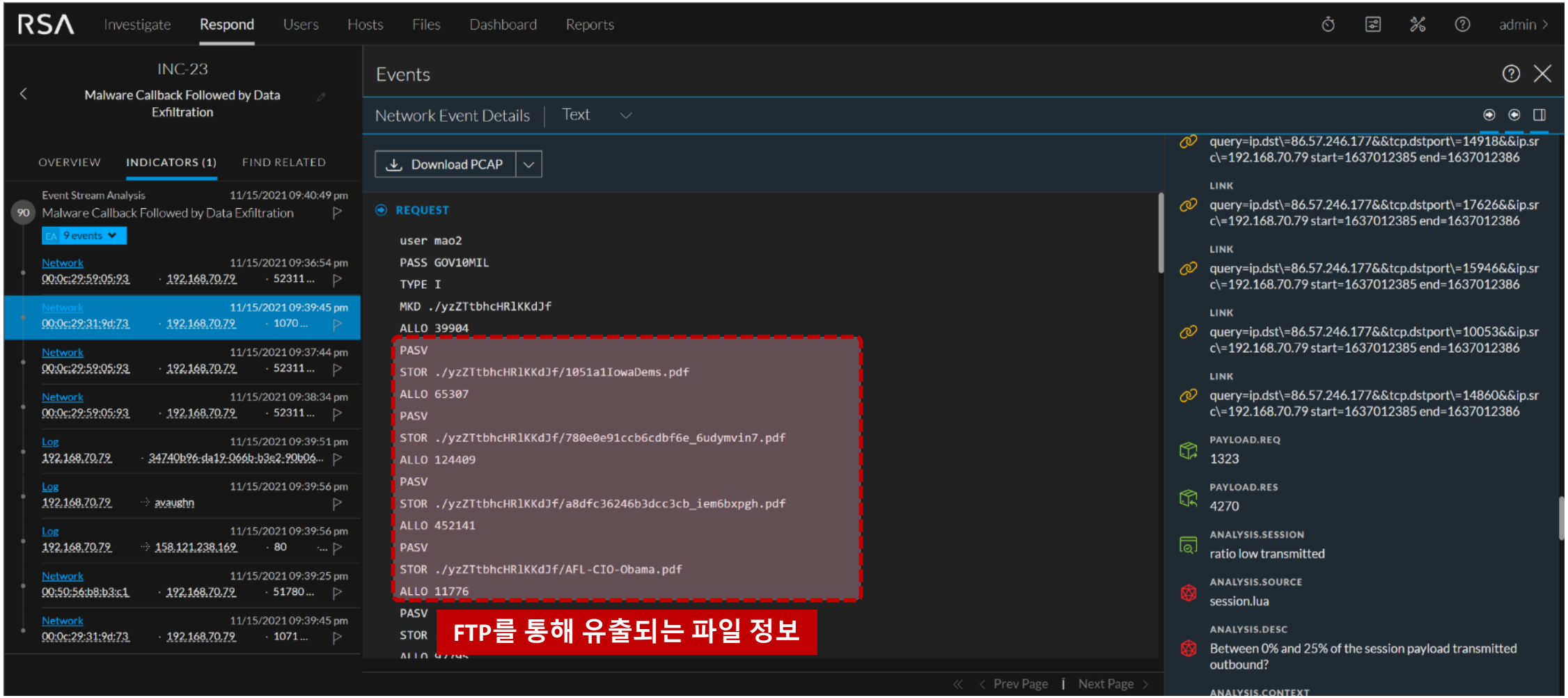
탐지된 이벤트에서 트래픽 원본을 단일 클릭으로 즉시 조회하여 실 공격 여부 및 상세 내용 확인



NETWITNESS

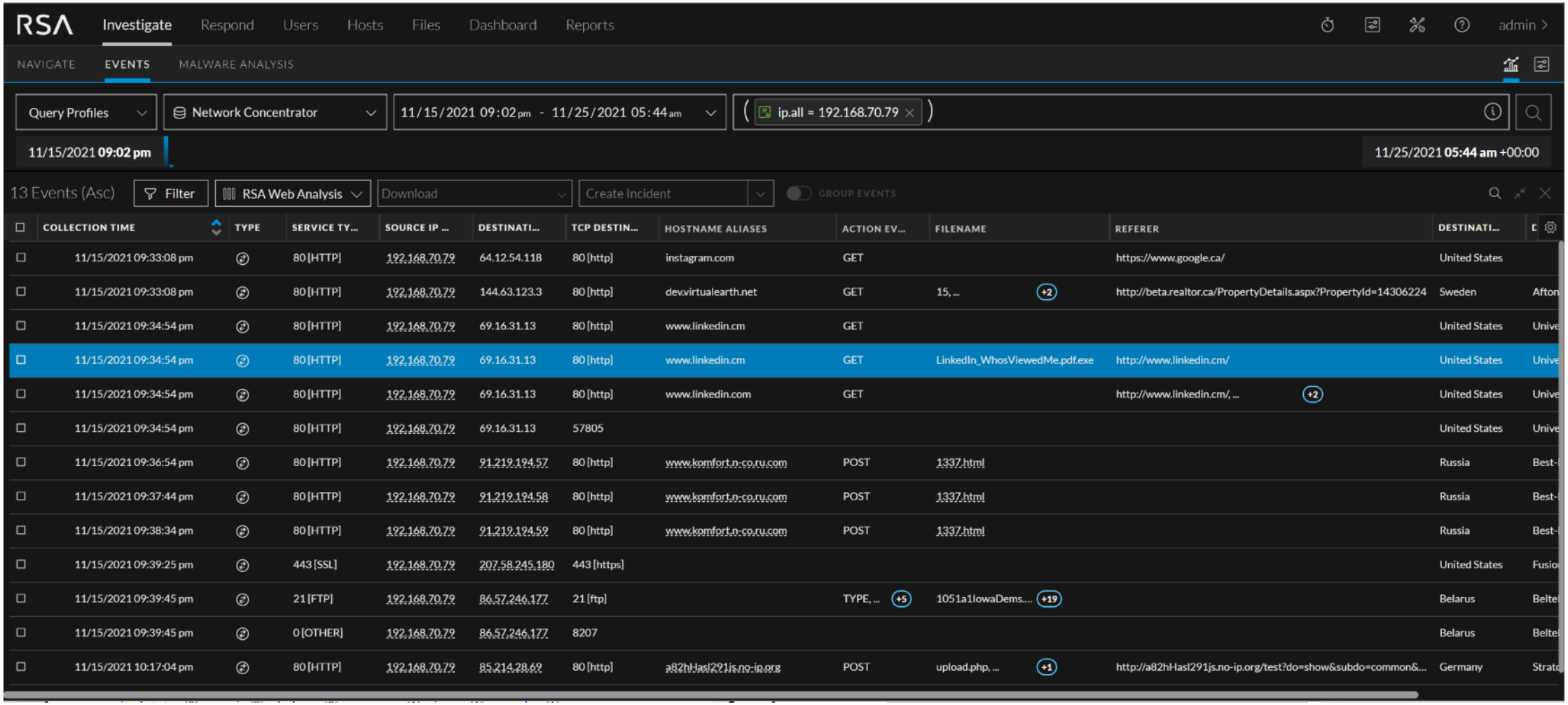
탐지된 사건 – 자료 유출 확인

탐지된 이벤트에서 트래픽 원본을 단일 클릭으로 즉시 유출된 증거 자료 확인



탐지와 연관된 모든 송수신 내역 조회

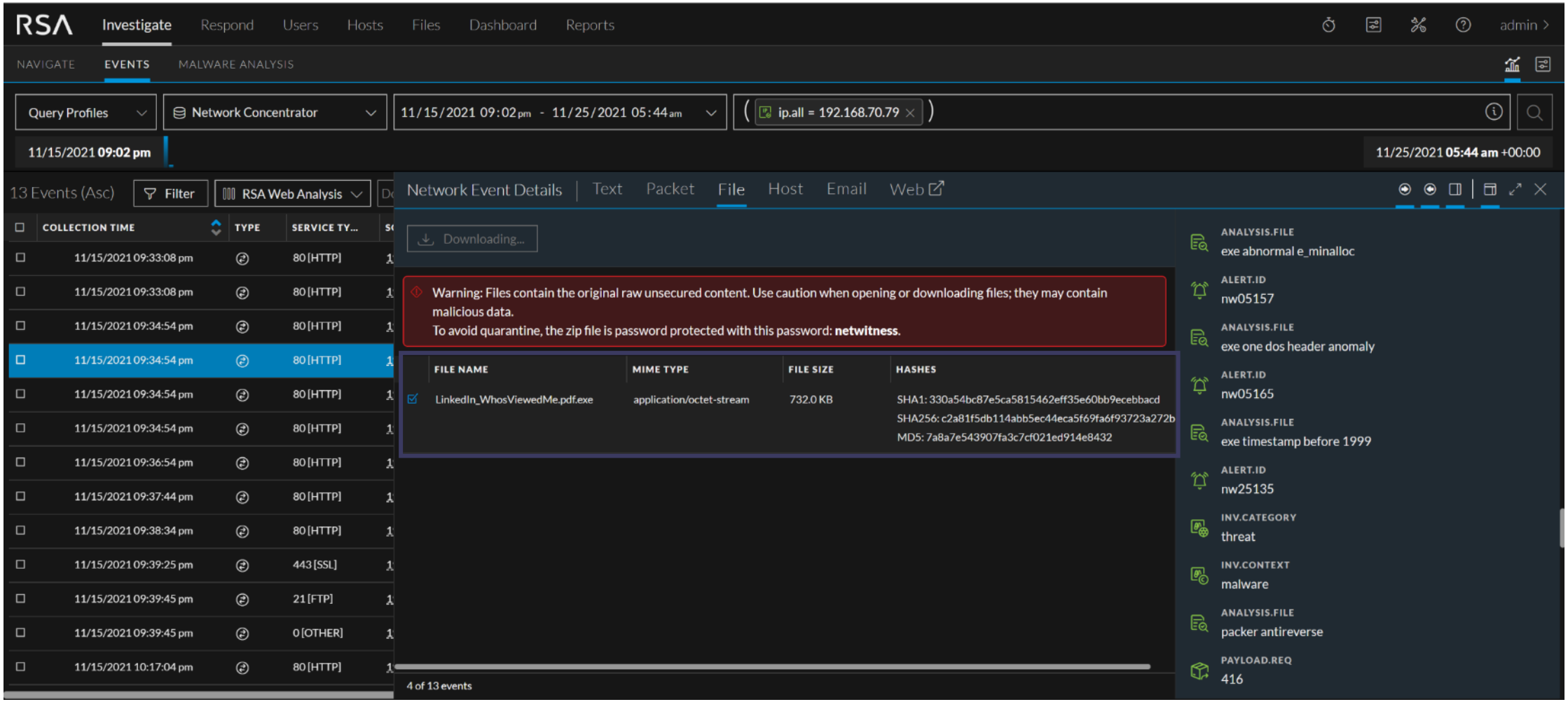
공격이 발견된 IP주소가 송수신한 모든 내역을 즉시 조회하여 최초 침입 및 내부 점령 등 공격의 전 과정 추적



NETWITNESS

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)

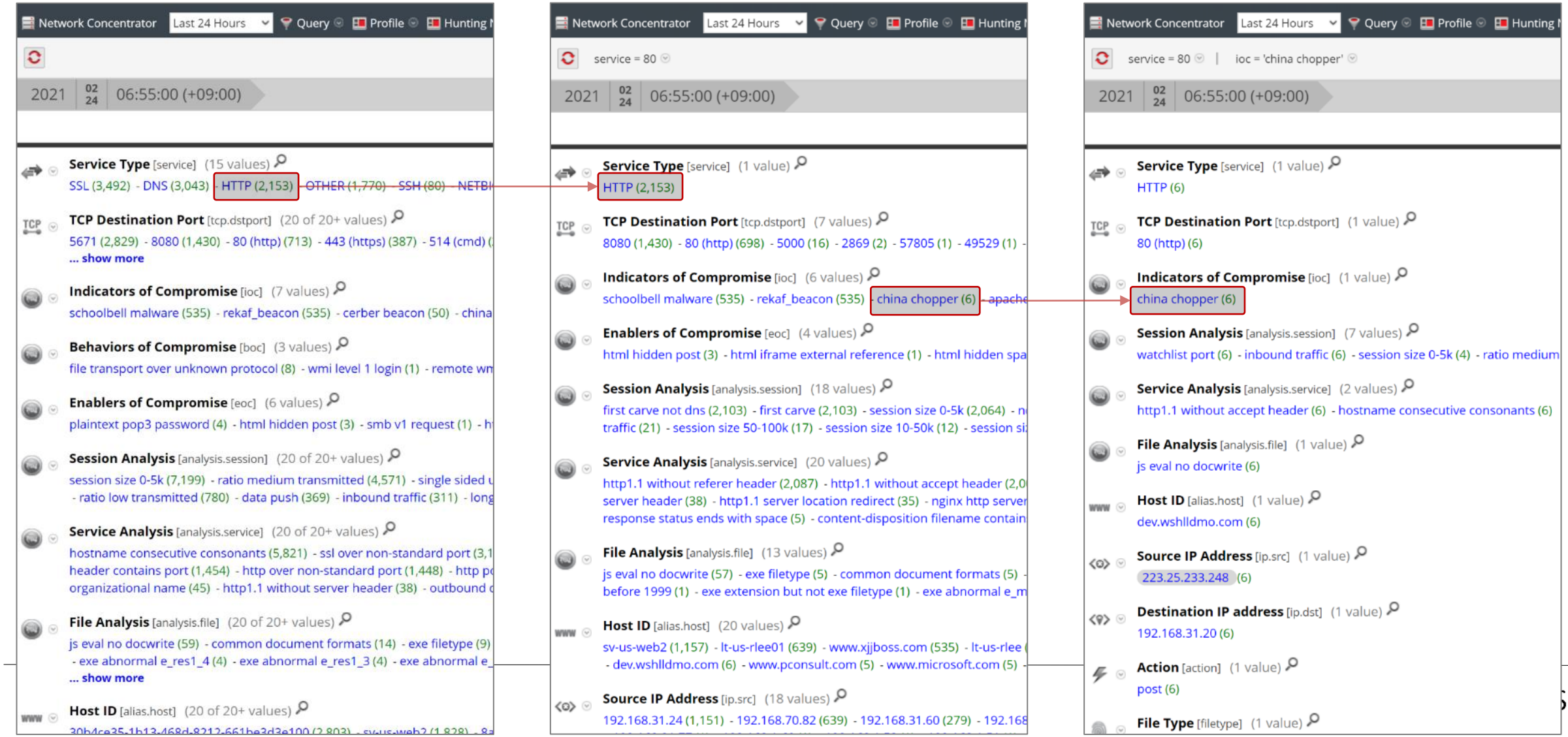


NETWITNESS

대화형 고속 검색을 통한 트래픽 위협 헌팅

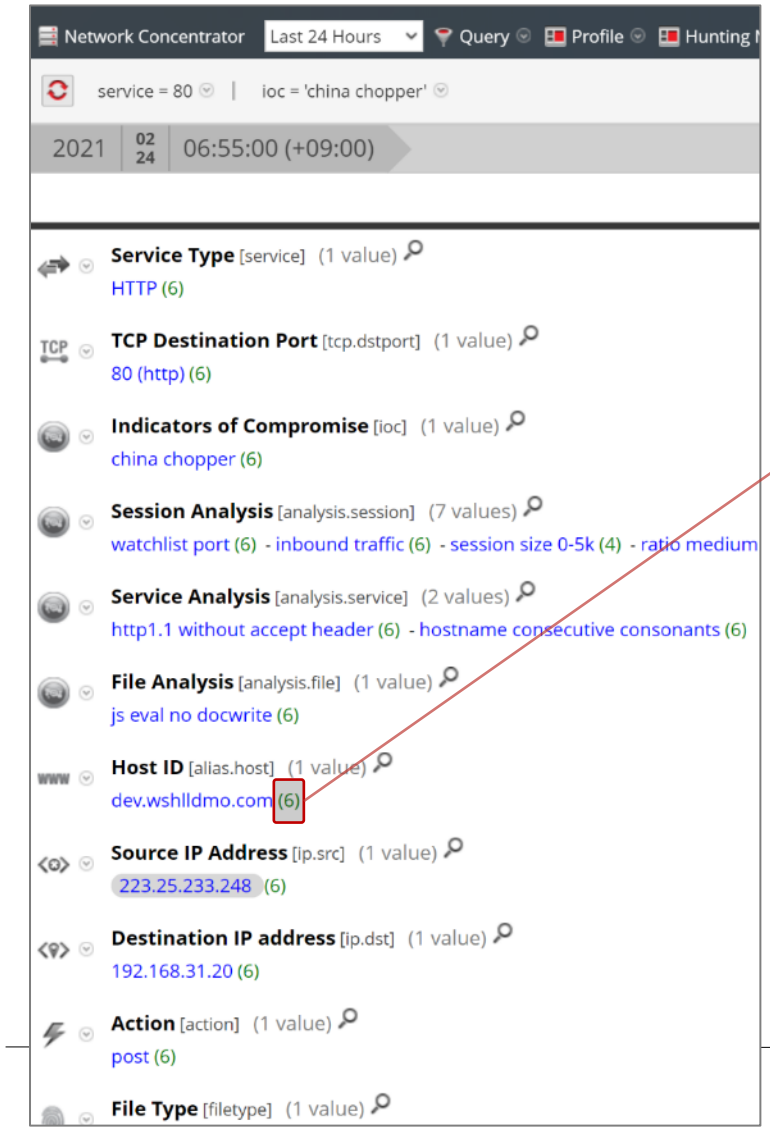
특허 받은 트래픽 현황 표현 방식 및 대화형 고속 검색 기능을 통해 사전에 예측하지 못한 침해 행위에 대한 능동적 위협 헌팅

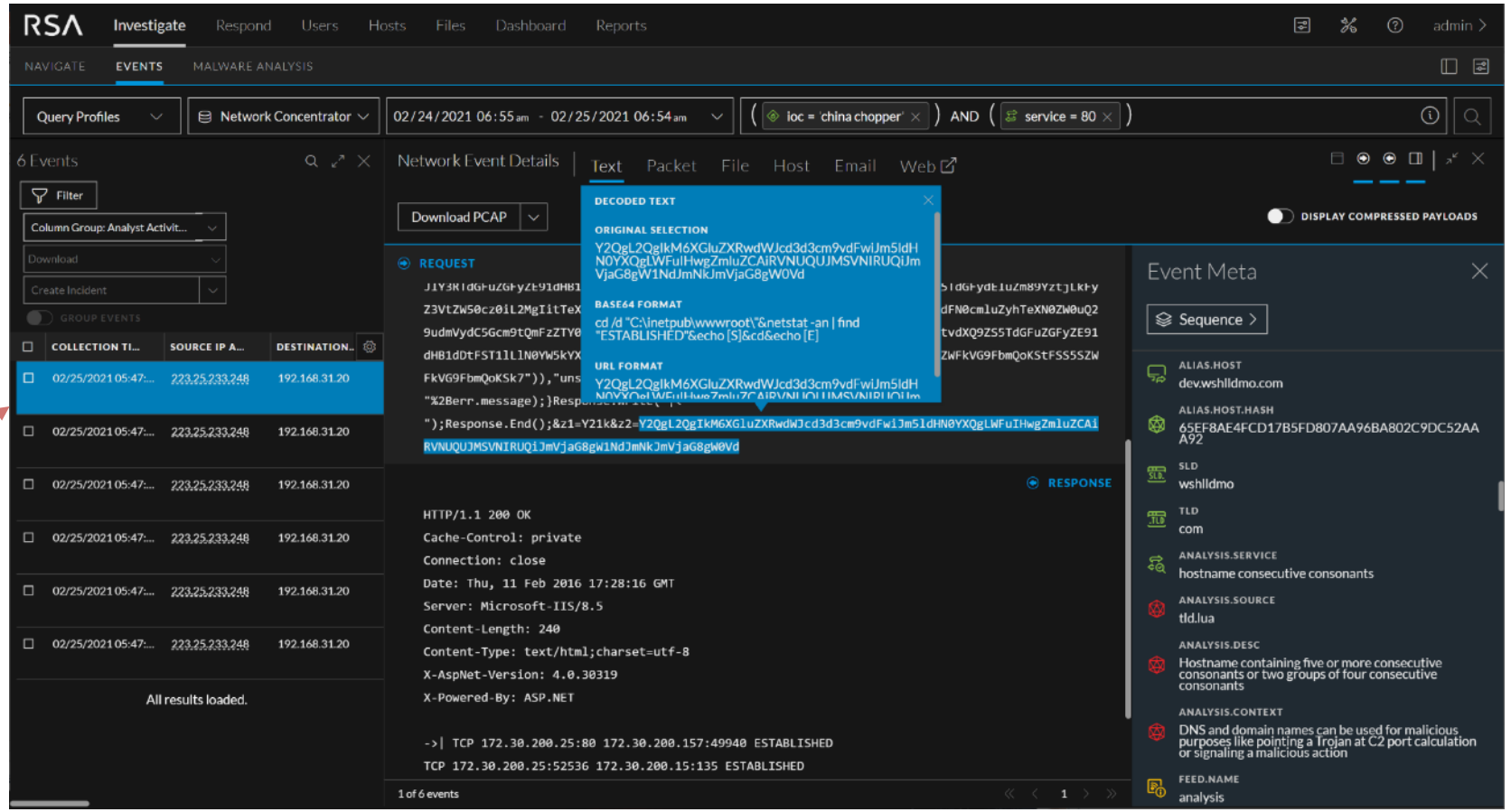
(특허: US20090067443A1)



트래픽 원본과 메타데이터 상세 분석

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

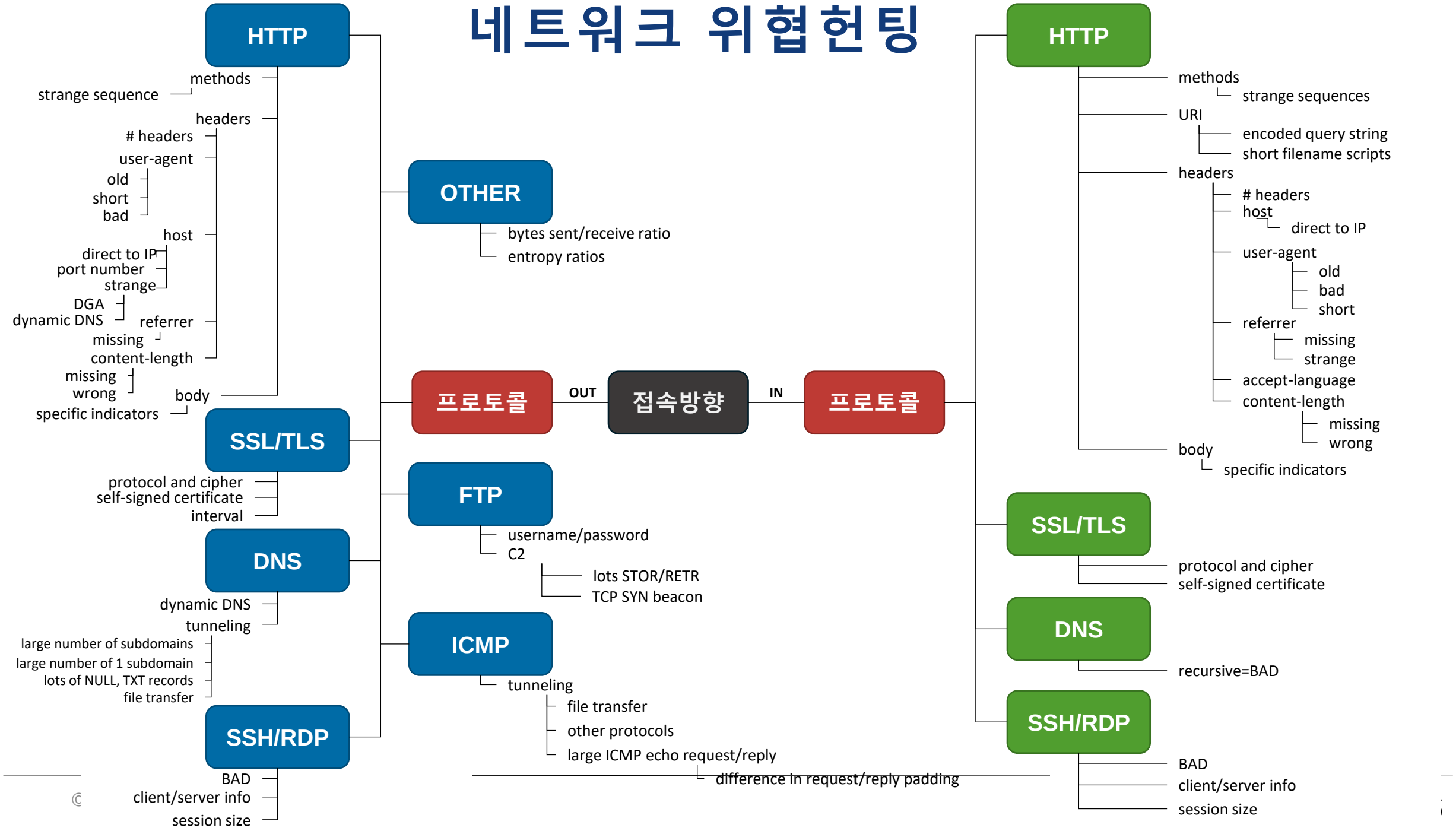




이벤트 목록 | 원본 데이터 | 메타 데이터

NETWITNESS

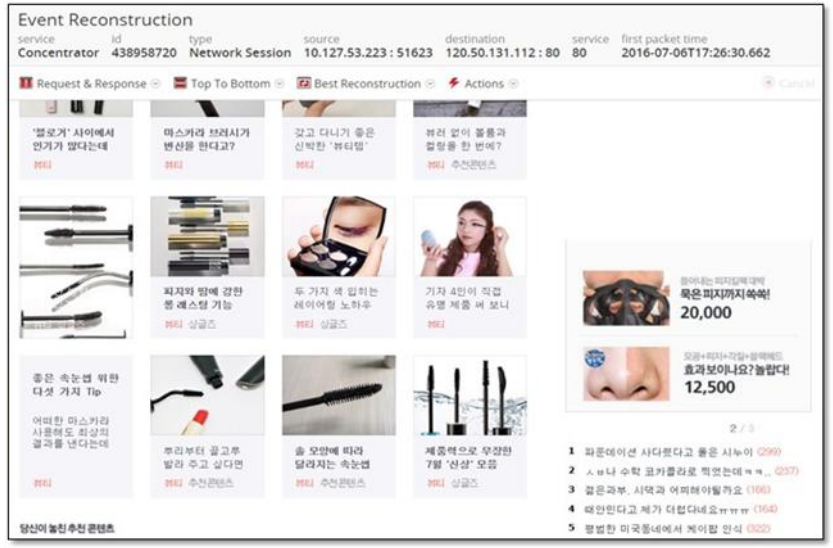
네트워크 위협헌팅


HTTP
methods
strange sequence
headers
headers
user-agent
old
short
bad
host
direct to IP
port number
strange
DGA
dynamic DNS
referrer
missing
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
interval
DNS
dynamic DNS
tunneling
large number of subdomains
large number of 1 subdomain
lots of NULL, TXT records
file transfer
SSH/RDP
BAD
client/server info
session size
OTHER
bytes sent/receive ratio
entropy ratios
프로토콜
OUT
접속방향
IN
프로토콜
FTP
username/password
C2
lots STOR/RETR
TCP SYN beacon
ICMP
tunneling
file transfer
other protocols
large ICMP echo request/reply
difference in request/reply padding
HTTP
methods
strange sequences
URI
encoded query string
short filename scripts
headers
headers
host
direct to IP
user-agent
old
bad
short
referrer
missing
strange
accept-language
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
DNS
recursive=BAD
SSH/RDP
BAD
client/server info
session size

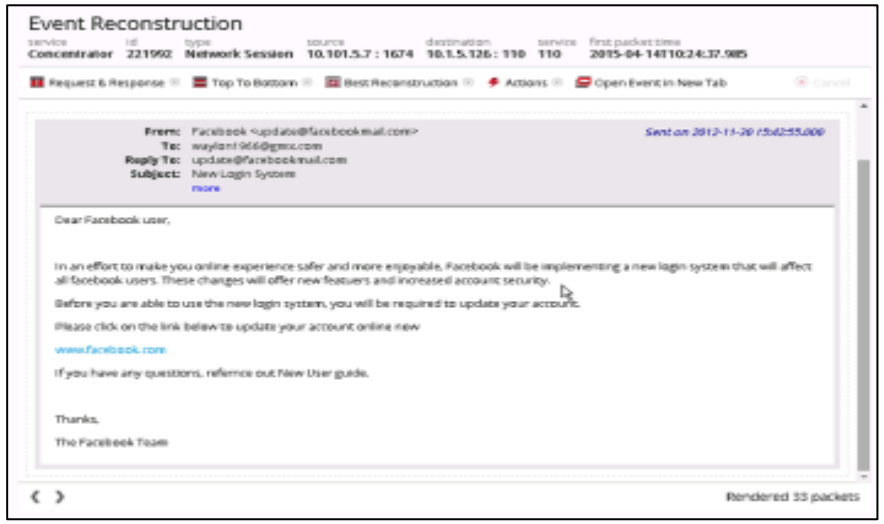
트래픽 기반 원본 재현 및 파일/패킷 추출

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

웹 페이지



이메일



파일추출

NETWITNESS

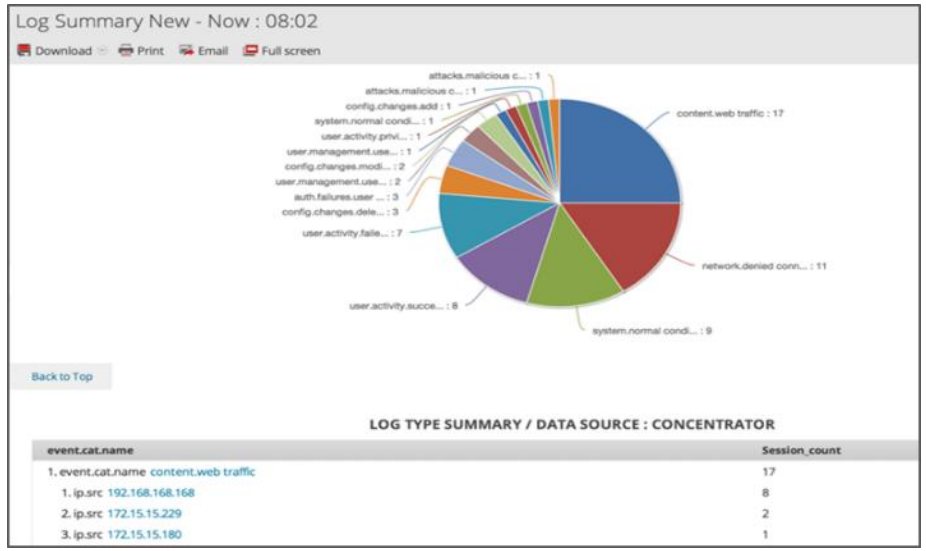
NETWITNESS

위협 처리 및 관리

대시보드 및 리포트

중요한 이벤트들을 쉽게 모니터링하기 위한 대시보드 및 리포트 생성

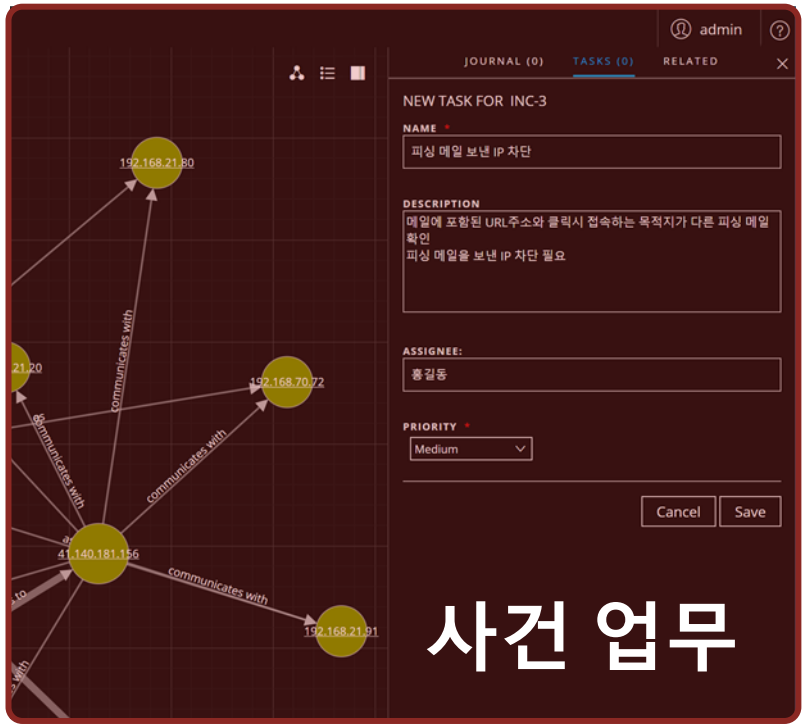
원하는 정보를 편집하여 현재 현황을 파악하는 대시보드

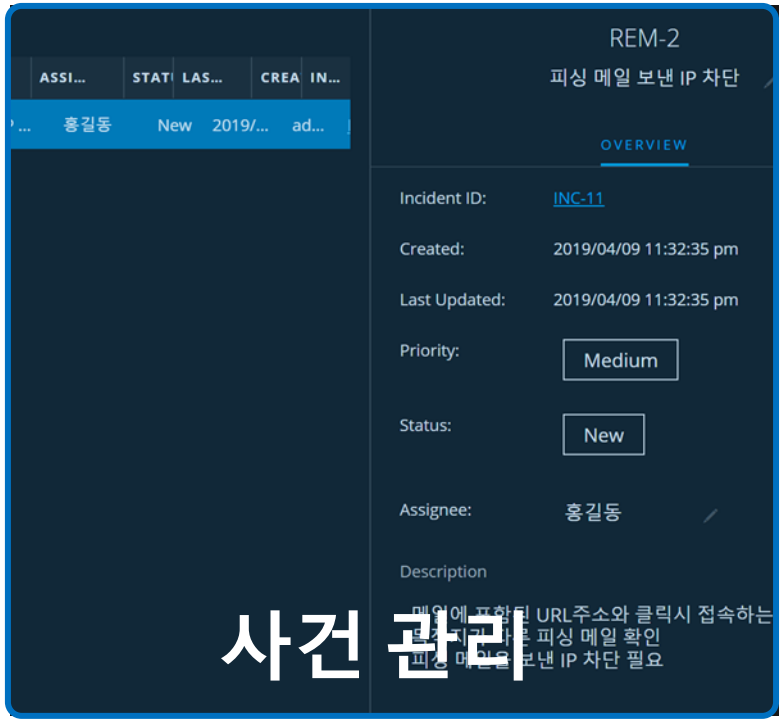


주기적으로(일별/주별/월별) 원하는 형태의 리포트 생성

탐지된 사건 관리

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





NETWITNESS

SIEM으로 사건 통합 관리

경보 연동 시나리오 예제

2 **SIEM**
경보 수신 5분 이내에
해당 IP의
Windows 로그에서
계정 생성 및 권한 상승

Syslog 경보 발송

1 **NetWitness**
특정 IP에서
PDF파일 다운로드
이후 5분 이내
실행파일 다운로드

3 악성이벤트 감지 경보 발생

NETWITNESS

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.

© 2024 NetWitness LLC. All rights reserved.

NETWITNESS

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

NETWITNESS

침투한 지능화된 공격 대응 방안

1 체류 시간을 줄이자!

2 대응을 더 빠르게!

NETWITNESS

Appendix :

NetWitness 구축 사례

NetWitness 구축 및 추가 도입 사례

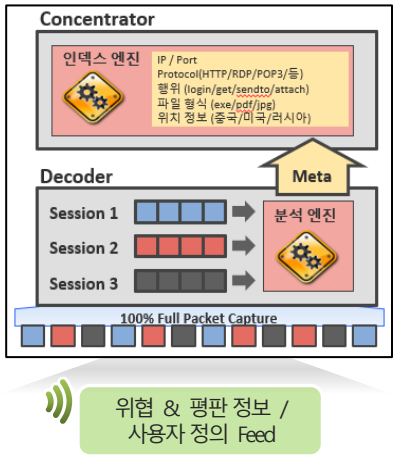
- 국내 주요기업에 성공적 적용사례 다수 보유
- 높은 솔루션 활용도 및 도입효과로 인해 적용 이후 2~5년 간 지속적인 추가도입 발생
    - S사: 2013년 최초 도입 이후 5년 이상 지속적 추가 도입. 그룹사 전체로 적용범위 확장
    - H사 : 2012년 최도 도입 이후 2년 후 추가 도입 → 성능 및 저장공간 확장
    - N은행 : 2012년 최초 도입 이후 2년 후 추가 도입 → 트래픽 수집 구간 확대
    - S은행 : 2012년 최초 도입 이후 2년 후 추가 도입 → 트래픽 저장공간 확장
    - B은행 : 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

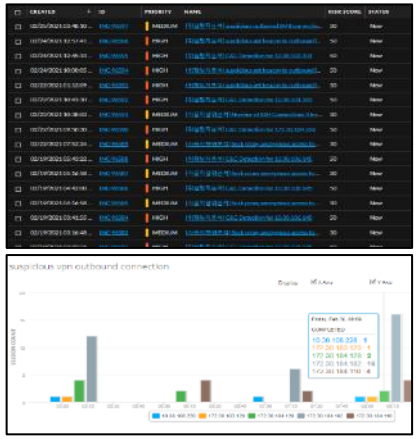
네트워크 트래픽을 기반으로 탐지 시나리오를 통해 발견된 보안 위협 확인 및 조치

정보 수집



트래픽 수집 및 다양한 보안 정보 연계

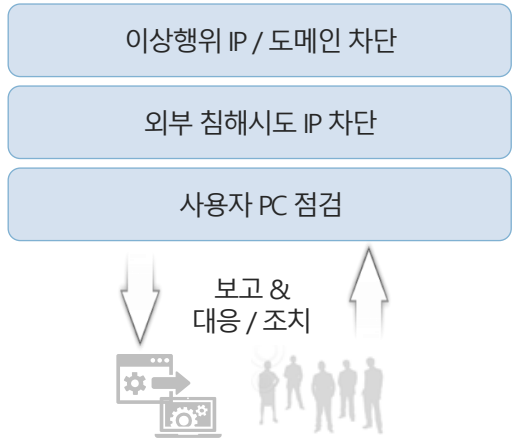
위협 탐지



위협 행위 / 보안정책 위반 탐지

150개 이상의 메타데이터를 활용하여 위협 탐지

위협 조치



정의한 대응 절차에 따라 위협 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)

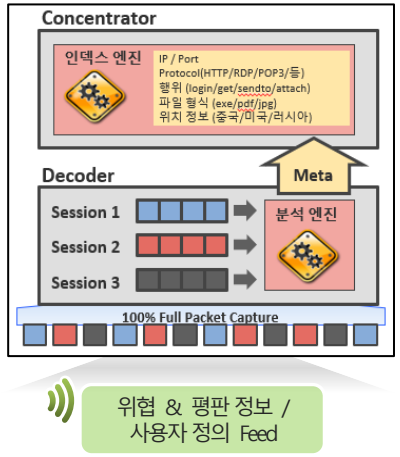
- **담당 : 보안 운영팀**
- 탐지된 위협 행위에 대해 관련된 절차에 따라 조치
- 위협 조치 결과 보안 관리자에게 보고

NETWITNESS

운영 예 – 2단계: 탐지된 이상행위 및 연관 행위 분석 및 처리

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

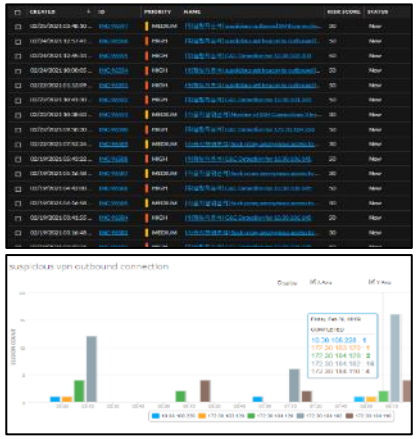
정보 수집



트래픽 수집 및 다양한 보안 정보 연계

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

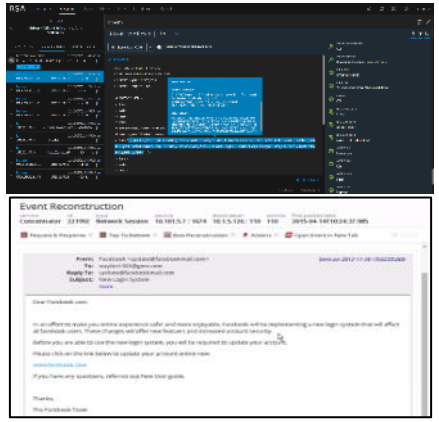
위협 탐지



150개 이상의 메타데이터를
활용하여 이상행위 탐지

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

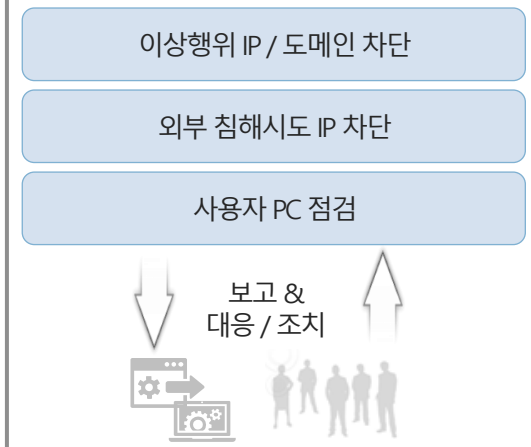
연관행위/추가위협 분석



탐지된 이상행위를 트래픽 원본과
재현 데이터를 이용해 분석 및 판단

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

위협 조치



정의한 대응 절차에 따라 위협 조치

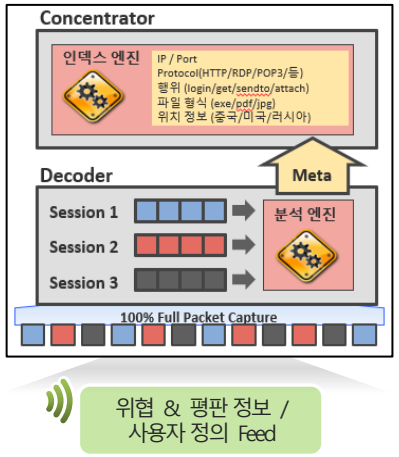
- **담당 : 보안 운영팀**
- 탐지와 관련된
  모든 위협 행위에 대한 조치
- 공격 유입 경로에 대한
  재발 방지 조치
- 위협 조치 결과 보안 관리자에게
  보고 (분석팀 공유)

NETWITNESS

운영 예 – 3단계: 능동적 위협 헌팅, 연관 행위 분석 및 처리

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

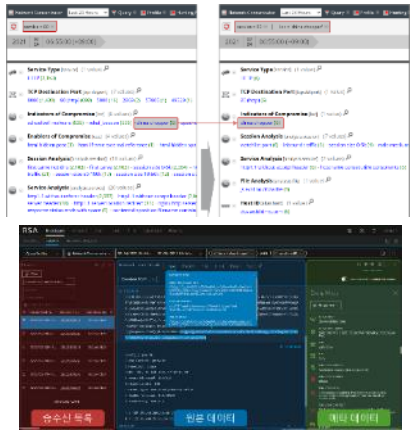
정보 수집



트래픽 수집 및 다양한 보안 정보 연계

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

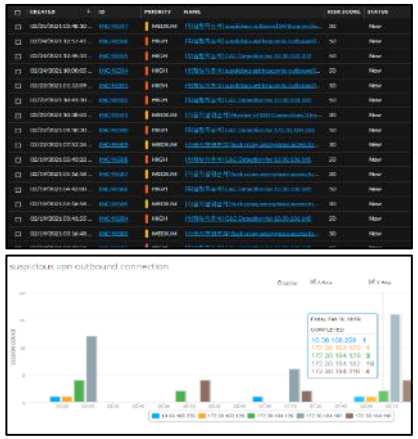
위협 헌팅



TI정보, MITTRE ATT&CK정보, 위협/침해/파일 지표 등을 활용 헌팅

- **담당 : 헌터 / 관리자**
- 수집된 네트워크 메타정보와 위협 지표를 활용해 이상행위, 의심트래픽, 위협, 공격 행위의 능동적 수색
- 새로운 취약점, 공격 경로 파악을 위한 위협 헌팅
- 새로운 탐지룰 지속적 보완

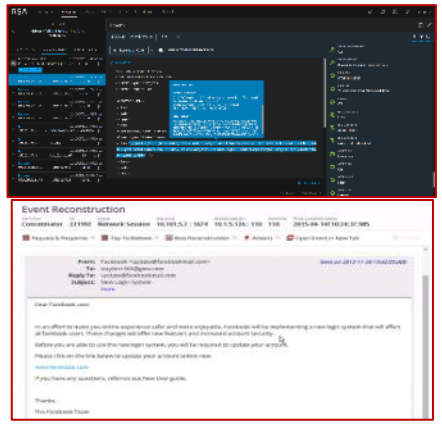
위협 탐지



150개 이상의 메타데이터를 활용하여 이상행위 탐지

- **담당 : 보안 분석팀 / 헌터**
- 조직에 최적화된 공격시나리오와 정책 위반 사례 탐지
- 내부 비즈니스 환경 및 중요 자산에 따른 탐지 심각도 정의 및 우선순위 할당

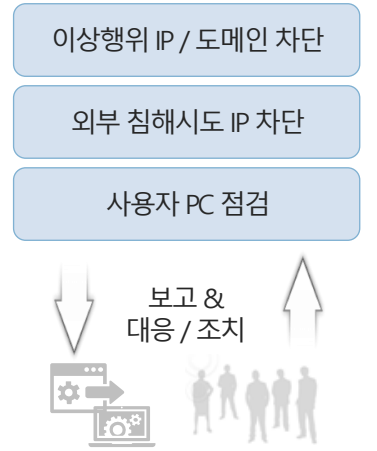
연관행위/추가위협 분석



탐지된 이상행위를 트래픽 원본과 재현 데이터를 이용해 분석 및 판단

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

위협 조치



정의한 대응 절차에 따라 위협 조치

- **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)

NETWITNESS