




ANOMALI[®]

Closing the Threat Defense Gap:
Automating Intelligence-Driven Security at Scale

(주)한국밸런스

A woman with curly hair is looking at a computer monitor in a server room. The room is filled with server racks and other people working at computers. The text is overlaid on the image.

우리는 공격
받고 있는가?

이미 공격을
받았는가?

어떻게 대응할
것인가?

“ I don't know. ”

인텔리전스 중심의 보안에 대한 필요

“조직이 직면한 위협과 시간이 지남에 따라 위협이 어떻게 진화했는지 그리고 어떤 전술이 활용될 가능성이 가장 높은지 잘 이해하면 이러한 위협을 관리할 수 있도록 준비할 수 있다.”

2019 Data Breach Investigations Report, Verizon



The Threat Defense Gap

제한된 위협 가시성



- 위협 데이터의 기하급수적 증가
- 조직과의 관련성 정제
- 인텔리전스 운영 가능화

데이터 과부하



- SIEM에 과중한 이벤트 로그 데이터
- 보안 제어에 과중한 IOC
- 현재 데이터 규모에 맞지 않게 설계된 보안 제품들

인력 갭



- 불안한 사이버 전문성
- 대부분의 매뉴얼 처리
- 오탐 및 알람 폭주

A Vision for Closing the Threat Defense Gap

“보안 운영의 미래는 위협 인텔리전스를
규모에 맞게 자동화하는데 있다”

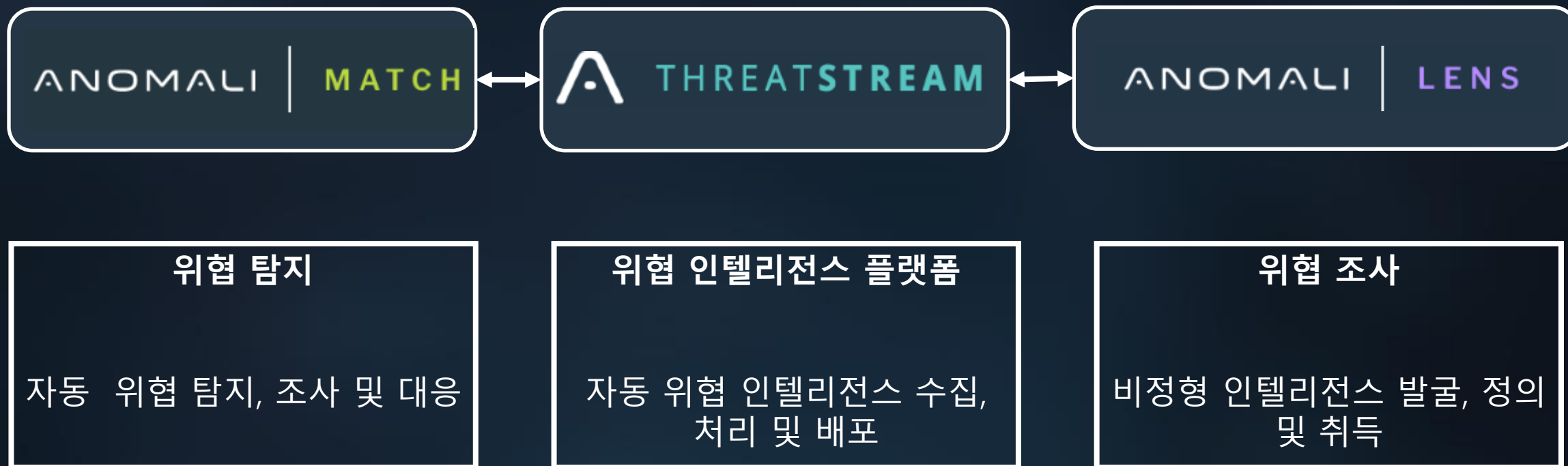
인텔리전스 기능
최대화

모든 위협 찾기

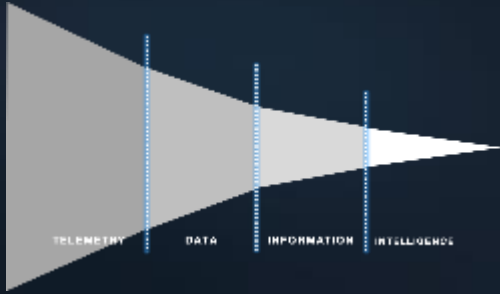
보안팀 생산성
향상

Anomali

Automating Intelligence-Driven Security at Scale



What problems are Anomali customers solving?



인텔 수집, 큐레이션 및 강화 자동화



3rd party 위협 인텔 검토 및 구매



보안 관제로 인텔을 자동 배포



위협, TTP 및 행위자 조사와
피봇팅 및 연구



조직 내 모든 위협 자동 탐지



수년간 이벤트 로그 데이터에서
Patient Zero 찾기



자산 위험 및 취약성에 따라
위협 치료 우선 순위 지정



신뢰할 수 있는 커뮤니티에서
안전하게 위협 공유

Anomali - Eliminate the Threat Defense Gap

완벽한 위협
가시성

매치 안된 위협
탐지

개선된 위협 방어

사전 보안 포스처
개선

즉각적이고 강력한 비즈니스 가치

80%
오탐지 감소

47%
해결 시간 감소

42%
전사적 가시성 향상

“

Anomali is the equivalent of adding two full-time employees by reducing our false positive rate by 80%.

IT Director, Health Care

Source: IT Director, Health Care
Published: Oct. 24, 2018

ANOMALI | TechValidate

“

Anomali allows us automation of indicator ingesting, thereby giving the analyst more time to investigate and contextualize incidents with additional data provided in Anomali.

Intelligence Analyst, S&P 500 Banking Company

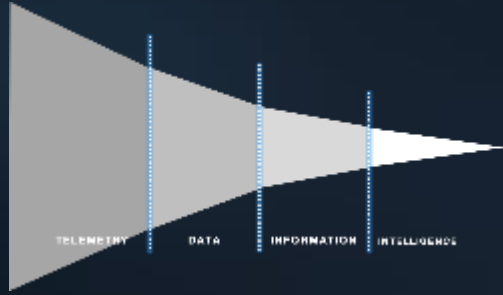
Source: Intelligence Analyst, S&P 500 Banking Company
Published: Oct. 25, 2018

ANOMALI | TechValidate

ANOMALI | THREATSTREAM

Automate threat intelligence collection, curation and distribution

What problems are ThreatStream customers solving?



인텔 수집, 큐레이션 및 강화 자동화



3rd party 위협 인텔 검토 및 구매



보안 관제로 인텔을 자동 배포



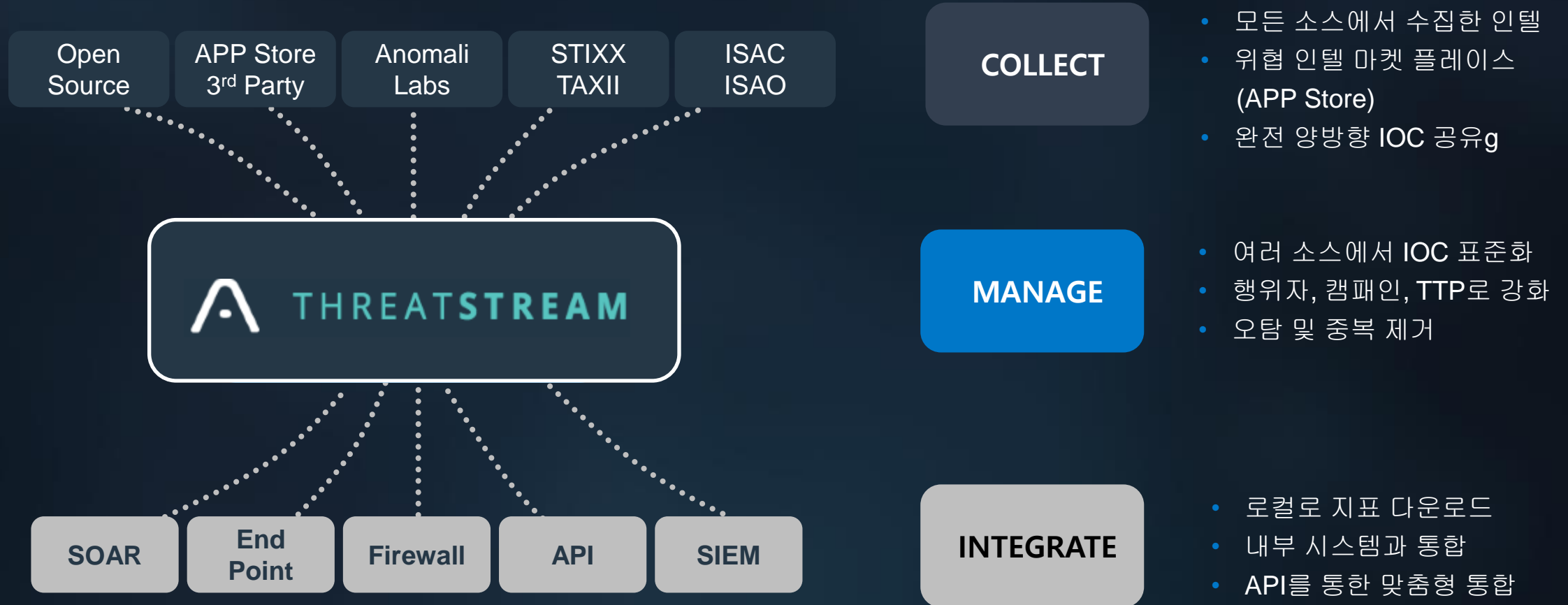
위협, TTP 및 행위자 조사와
피봇팅 및 연구



신뢰할 수 있는 커뮤니티에서
안전하게 위협 공유

Anomali ThreatStream

The industry's leading Threat Intelligence Platform (TIP)



Threat Intelligence Marketplace

Anomali APP Store – 130+ feeds, enrichments and tools

Feeds



Enrichments



Integration



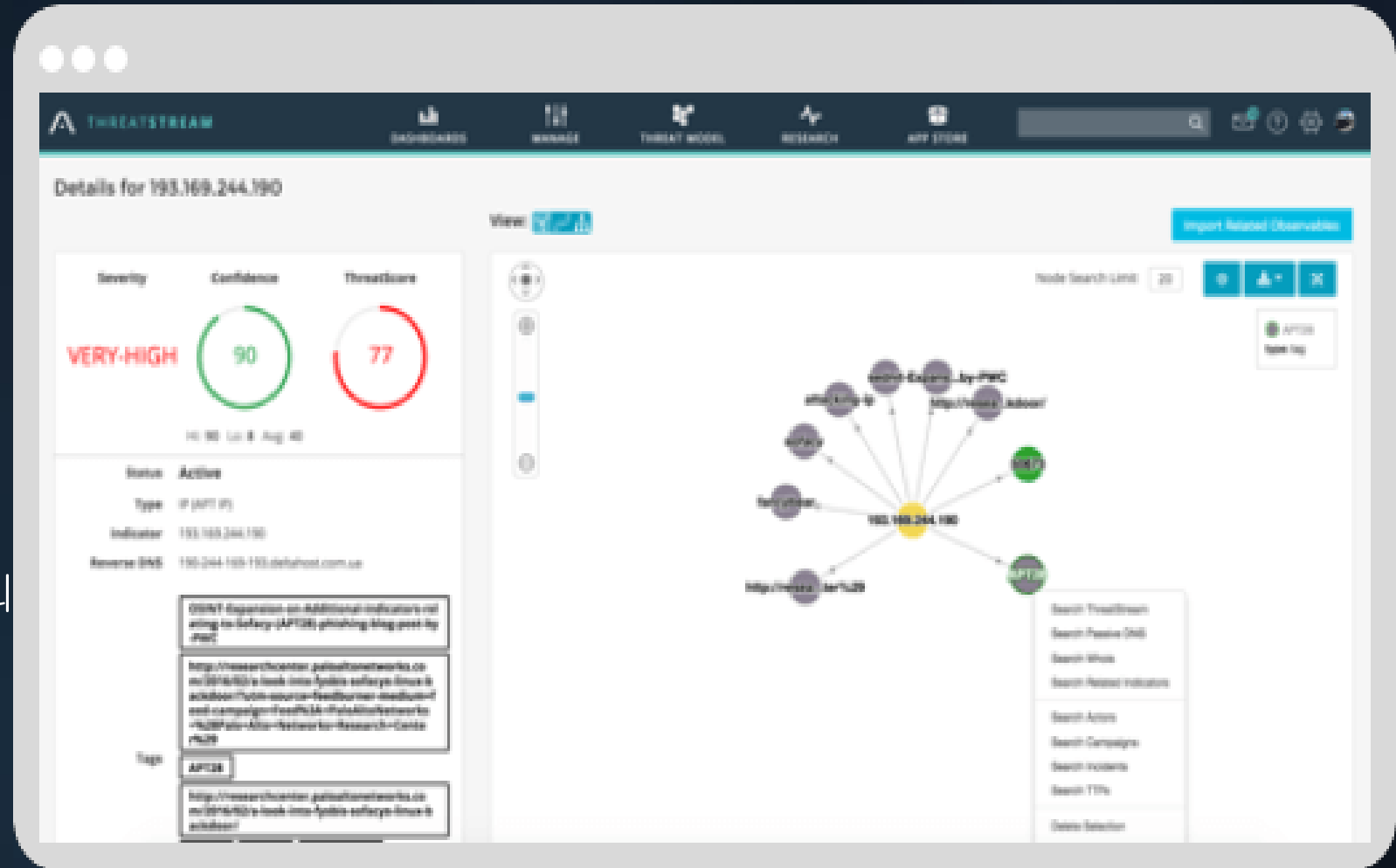
Tools



Operationalized Threat Intelligence

Automation to accelerate access to machine-readable threat intelligence

- 피드를 일반적인 분류 체계로 정규화
- 피드 전체에서 중복 제거
- 머신러닝을 통해 오탐 및 오래된 지표 제거
- 액터, 캠페인, TTP로 데이터 강화
- WHOIS, PassiveDNS, GeoIP 등의 컨텍스트 추가
- 관련 위협 지표 연계



Turnkey Integrations

Automate distribution of threat intelligence into your security controls

- 사전 구축되고 인증된 통합
- 내부 시스템과 통합
- 차단, 모니터링 규칙 생성
- SIEM, FW, endpoint, SOAR 등 지원
- 맞춤형 통합을 위한 API

BANDURA
CYBER

Bro IDS

CARBON
BLACK

Check Point
SOFTWARE TECHNOLOGIES LTD.

cloudera

CROWDSTRIKE

cuckoo

CYBERSENSE
ADAPTIVE SECURITY

FIREEYE

FORTINET

hadoop

IBM Radar

Resilient
an IBM Company

Infoblox

JOE Security

lastline

LogicHub

LogRhythm

McAfee

MICRO
FOCUS

NSS
LABS

okta

paloalto
NETWORKS

Phantom

RSA
READY

SECURONIX

servicenow

SNORT

splunk

sqrll

Symantec

TANIMUM

tripwire

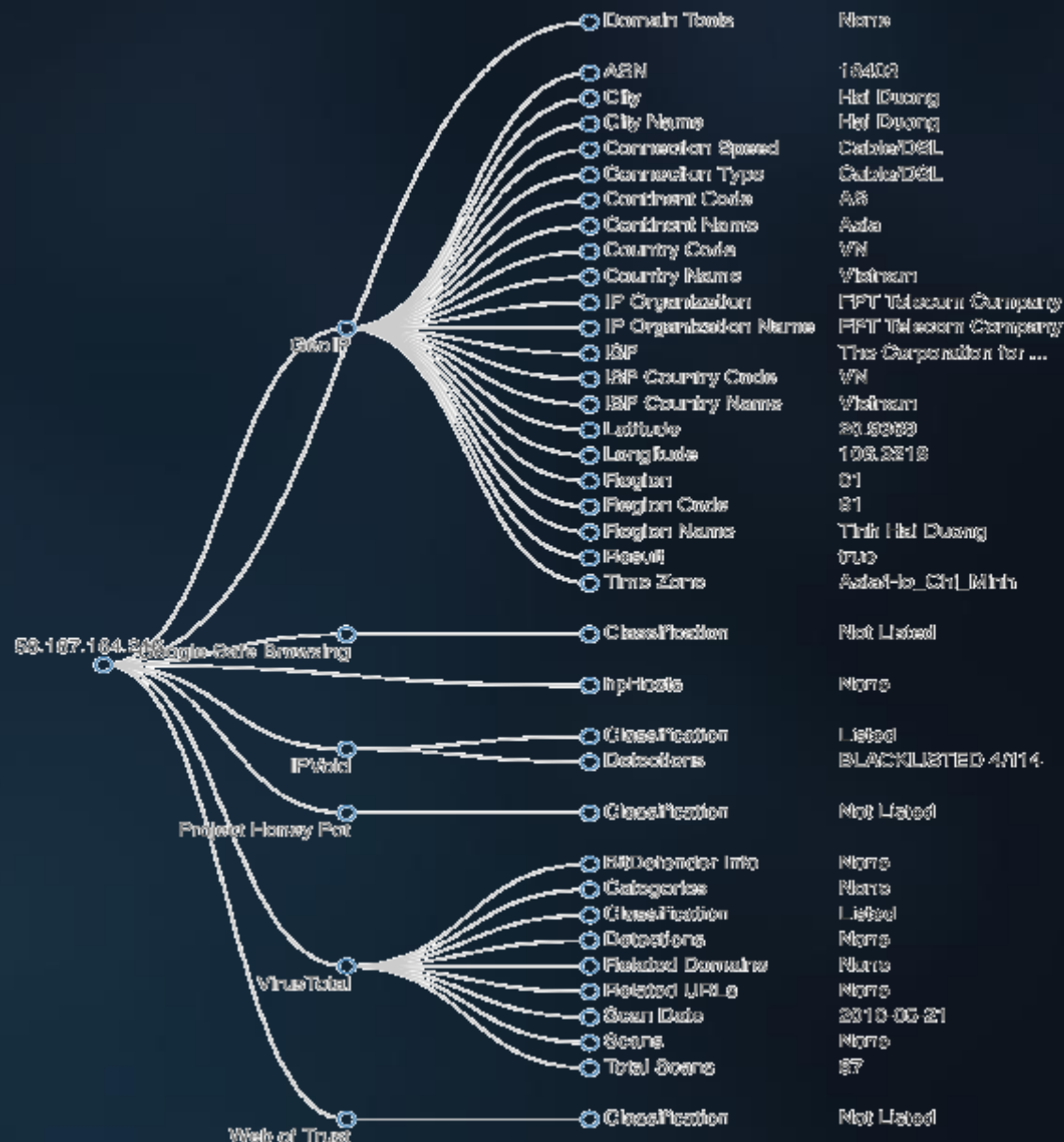
VERODIN
LOW PART OF FIREEYE

zscaler

Comprehensive Threat Investigation

Enabling SOC Teams and Analysts to Respond to Threats

- 위협 조사 엔진
 - 분석가 워크 플로우
- 모델 기반 분석
 - MITRE ATT&CK, Kill Chain, Diamond 등
- 위협 게시판 생성
 - 저작, 관리 및 협업
- 샌드 박스
 - 악성 코드 폭파 및 관련 지표 추출
- 피싱
 - 의심되는 이메일에서 지표 추출
- 브랜드 모니터링
 - 브랜드 남용 탐지



Secure Platform for Trusted Collaboration

Trusted Circles within ThreatStream powers 20+ global ISACs.

Anomali 는 안전한 협업을 강화하기 위해 ISAC 및 ISAO가 신뢰하는 완벽한 위협 공유 플랫폼을 제공합니다.

- 유명 위협 공유 커뮤니티 포털
- Anomali 플랫폼의 전용 신뢰할 수 있는 서클
- 전문가와 특별 회원에 대한 무제한 관리자 계정 액세스
- 프로그래밍 방식 액세스를 위한 STIX/TAXII 서버
- 모든 커뮤니티 회원을 위한 Anomali Analyst 라이선스
- Anomali 위협 분석 센터의 산업별 연구
- 커뮤니티 교육 및 지원



ANOMALI | MATCH

Automated threat detection, investigation and response

What Problems Are Match Customers Solving?



조직 내 모든 위협 자동 탐지



수년간 이벤트 로그 데이터에서 Patient Zero 찾기



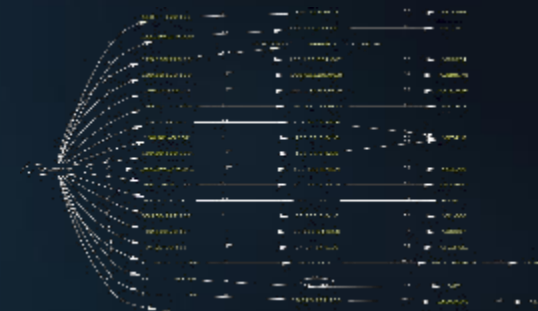
몇 초 안에 네트워크에서 위협 찾기

Letter number	Abbreviation	Symbolism	Idioms/Idiomata	Metaphors and/or	Emblem	Common name	Latin/Etymology	Idiomata	Order of and content	Idiomata	Legend
1	Alpha	First letter of the alphabet	Beginning, start, origin	First, initial, first	Alpha	First	Alpha	First	1	Alpha	First
2	Beta	Second letter of the alphabet	Second, second, second	Second, second, second	Beta	Second	Beta	Second	2	Beta	Second
3	Gamma	Third letter of the alphabet	Third, third, third	Third, third, third	Gamma	Third	Gamma	Third	3	Gamma	Third
4	Delta	Fourth letter of the alphabet	Fourth, fourth, fourth	Fourth, fourth, fourth	Delta	Fourth	Delta	Fourth	4	Delta	Fourth
5	Epsilon	Fifth letter of the alphabet	Fifth, fifth, fifth	Fifth, fifth, fifth	Epsilon	Fifth	Epsilon	Fifth	5	Epsilon	Fifth
6	Zeta	Sixth letter of the alphabet	Sixth, sixth, sixth	Sixth, sixth, sixth	Zeta	Sixth	Zeta	Sixth	6	Zeta	Sixth
7	Eta	Seventh letter of the alphabet	Seventh, seventh, seventh	Seventh, seventh, seventh	Eta	Seventh	Eta	Seventh	7	Eta	Seventh
8	Theta	Eighth letter of the alphabet	Eighth, eighth, eighth	Eighth, eighth, eighth	Theta	Eighth	Theta	Eighth	8	Theta	Eighth
9	Iota	Ninth letter of the alphabet	Ninth, ninth, ninth	Ninth, ninth, ninth	Iota	Ninth	Iota	Ninth	9	Iota	Ninth
10	Kappa	Tenth letter of the alphabet	Tenth, tenth, tenth	Tenth, tenth, tenth	Kappa	Tenth	Kappa	Tenth	10	Kappa	Tenth
11	Lambda	Eleventh letter of the alphabet	Eleventh, eleventh, eleventh	Eleventh, eleventh, eleventh	Lambda	Eleventh	Lambda	Eleventh	11	Lambda	Eleventh
12	Mu	Twelfth letter of the alphabet	Twelfth, twelfth, twelfth	Twelfth, twelfth, twelfth	Mu	Twelfth	Mu	Twelfth	12	Mu	Twelfth
13	Nu	Thirteenth letter of the alphabet	Thirteenth, thirteenth, thirteenth	Thirteenth, thirteenth, thirteenth	Nu	Thirteenth	Nu	Thirteenth	13	Nu	Thirteenth
14	Xi	Fourteenth letter of the alphabet	Fourteenth, fourteenth, fourteenth	Fourteenth, fourteenth, fourteenth	Xi	Fourteenth	Xi	Fourteenth	14	Xi	Fourteenth
15	Omicron	Fifteenth letter of the alphabet	Fifteenth, fifteenth, fifteenth	Fifteenth, fifteenth, fifteenth	Omicron	Fifteenth	Omicron	Fifteenth	15	Omicron	Fifteenth
16	Pi	Sixteenth letter of the alphabet	Sixteenth, sixteenth, sixteenth	Sixteenth, sixteenth, sixteenth	Pi	Sixteenth	Pi	Sixteenth	16	Pi	Sixteenth
17	Rho	Seventeenth letter of the alphabet	Seventeenth, seventeenth, seventeenth	Seventeenth, seventeenth, seventeenth	Rho	Seventeenth	Rho	Seventeenth	17	Rho	Seventeenth
18	Sigma	Eighteenth letter of the alphabet	Eighteenth, eighteenth, eighteenth	Eighteenth, eighteenth, eighteenth	Sigma	Eighteenth	Sigma	Eighteenth	18	Sigma	Eighteenth
19	Tau	Nineteenth letter of the alphabet	Nineteenth, nineteenth, nineteenth	Nineteenth, nineteenth, nineteenth	Tau	Nineteenth	Tau	Nineteenth	19	Tau	Nineteenth
20	Upsilon	Twentieth letter of the alphabet	Twentieth, twentieth, twentieth	Twentieth, twentieth, twentieth	Upsilon	Twentieth	Upsilon	Twentieth	20	Upsilon	Twentieth
21	Phi	Twenty-first letter of the alphabet	Twenty-first, twenty-first, twenty-first	Twenty-first, twenty-first, twenty-first	Phi	Twenty-first	Phi	Twenty-first	21	Phi	Twenty-first
22	Chi	Twenty-second letter of the alphabet	Twenty-second, twenty-second, twenty-second	Twenty-second, twenty-second, twenty-second	Chi	Twenty-second	Chi	Twenty-second	22	Chi	Twenty-second
23	Psi	Twenty-third letter of the alphabet	Twenty-third, twenty-third, twenty-third	Twenty-third, twenty-third, twenty-third	Psi	Twenty-third	Psi	Twenty-third	23	Psi	Twenty-third
24	Omega	Twenty-fourth letter of the alphabet	Twenty-fourth, twenty-fourth, twenty-fourth	Twenty-fourth, twenty-fourth, twenty-fourth	Omega	Twenty-fourth	Omega	Twenty-fourth	24	Omega	Twenty-fourth

TTP 및 행위자를 기반으로 조직 환경의 위협 분석

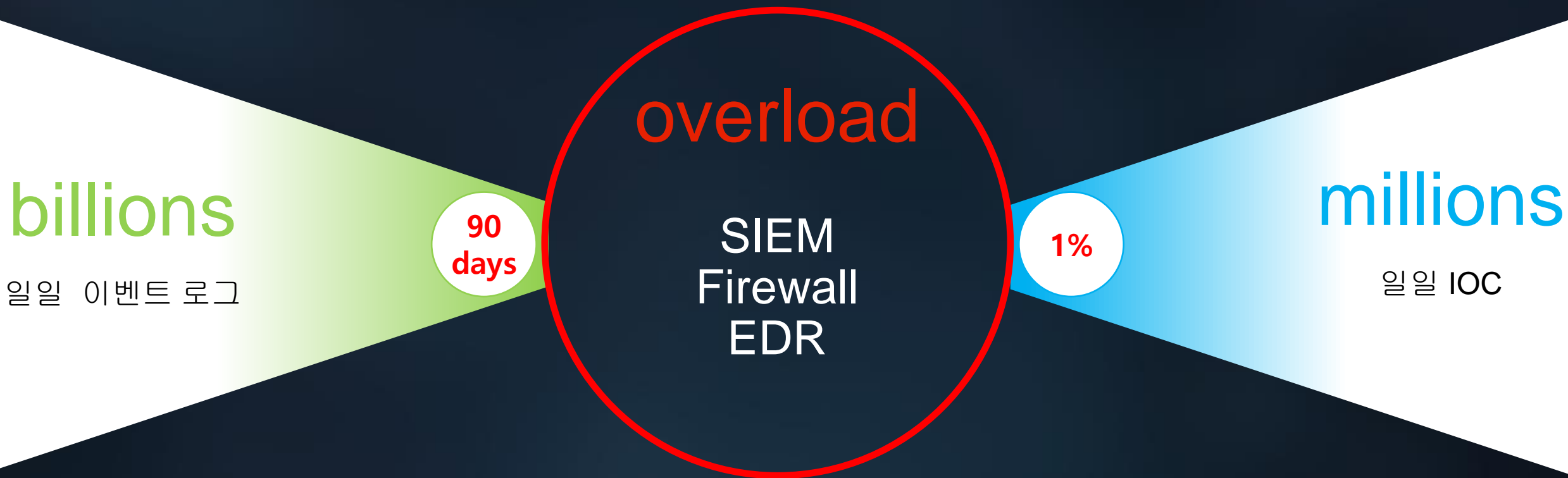


자산 위험 및 취약성에 따라 위험의 치료 우선 순위 지정

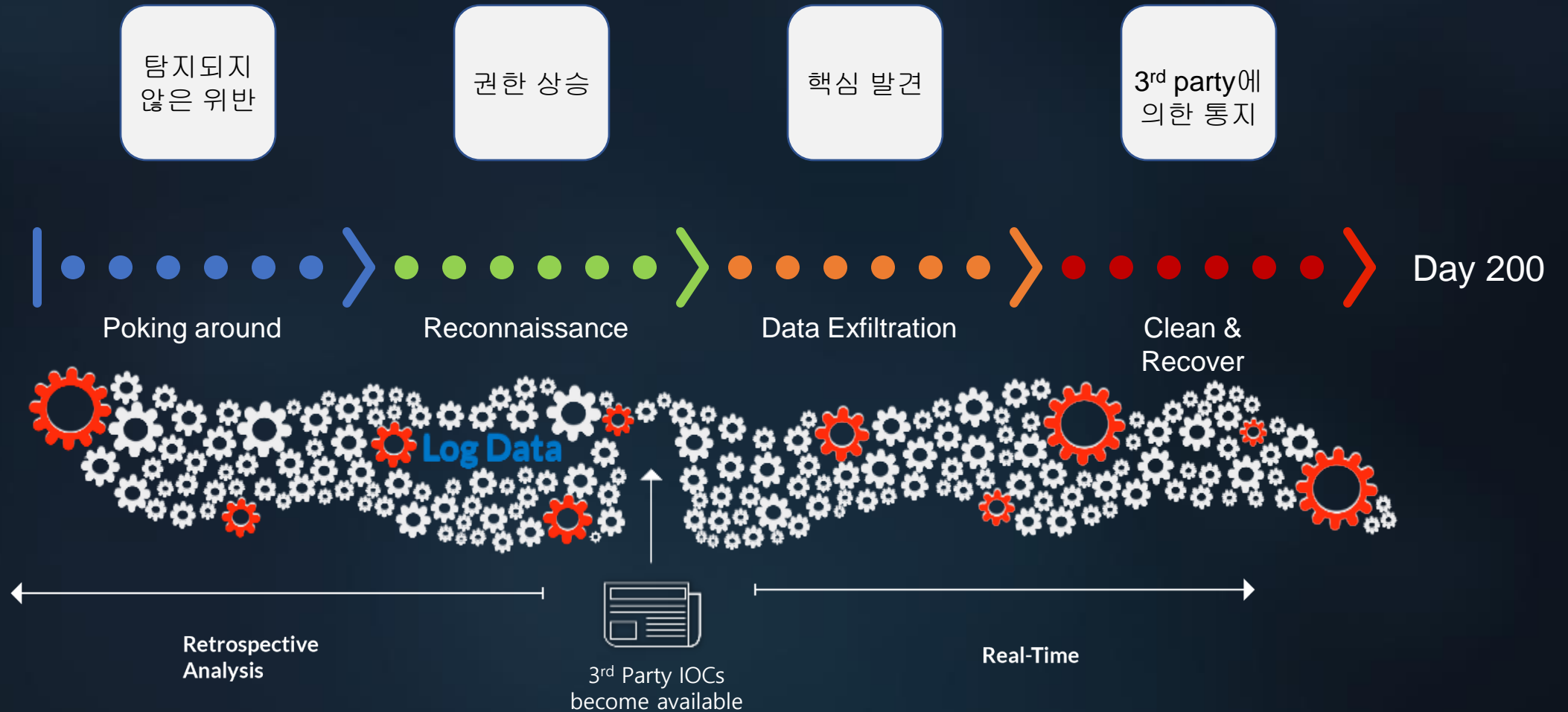


DGA 공격 예측 및 차단

Security Data Overload Problem



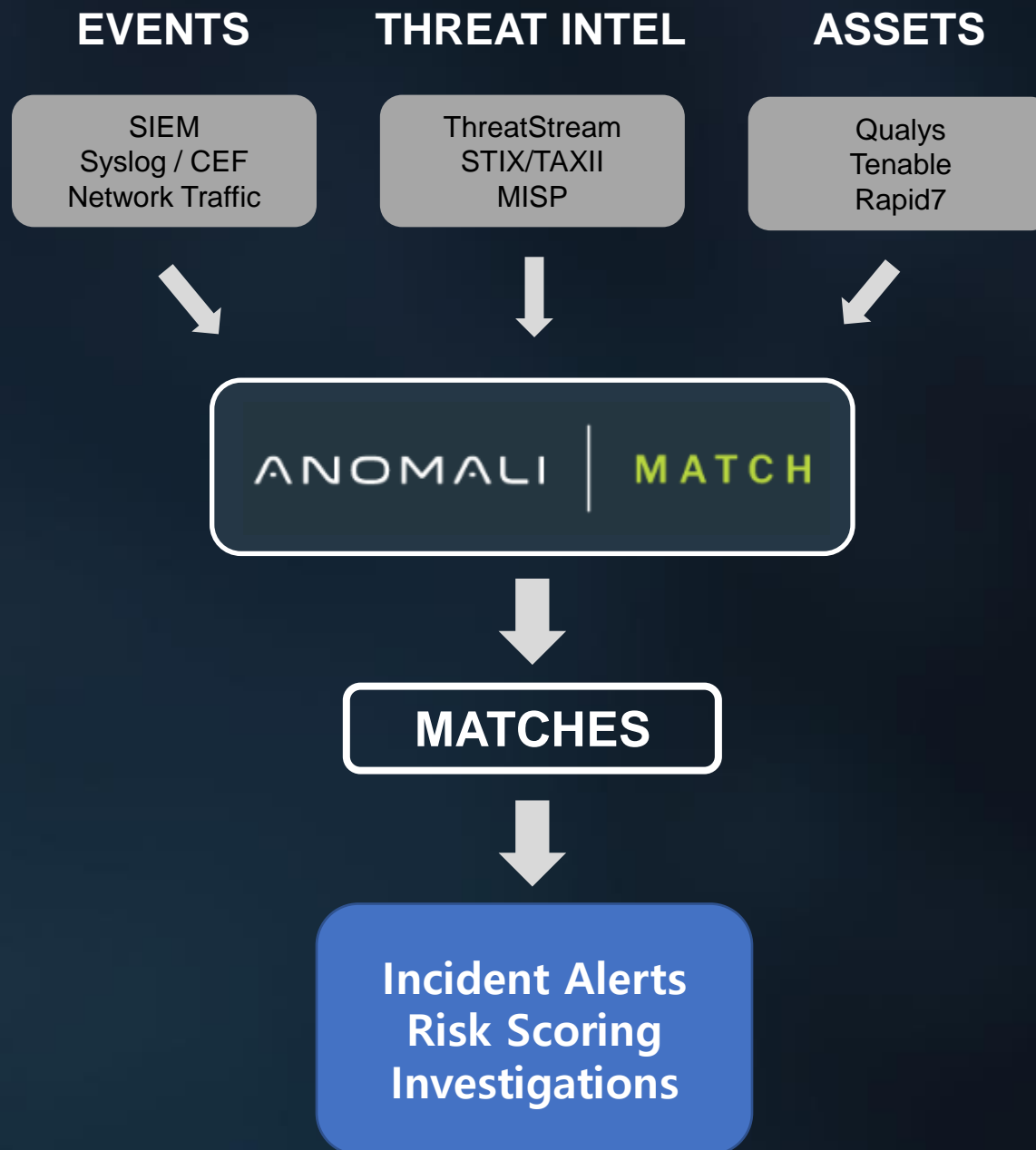
The 200 Day Dwell-Time Problem



Anomali Match

Threat Detection Engine

- 네트워크에 활동 중인 위협 탐지
- 365일 이상 이력 데이터 검색
- 로그 저장소 이중 복제 없음
- 심각한 IOC 필터링, 우선 순위화, 추측 제거
- SIEM, SOAR, 대시보드에 일치 항목 보냄
- 조사 도구 및 워크 플로우 내장



ANOMALI | LENS+

Automate the discovery, definition, and ingestion of unstructured intelligence

What Problems Are Lens Customers Solving?



몇 초 안에 비정형 데이터에서
위협 인텔리전스 식별



손끝에서 인텔
컨텍스트를 얻고 정의



시간 소모적인 수동 복사 및
붙여 넣기 방식 지표 검색 제거



자산 위험 및 취약성에 따라
위협의 치료 우선 순위 지정

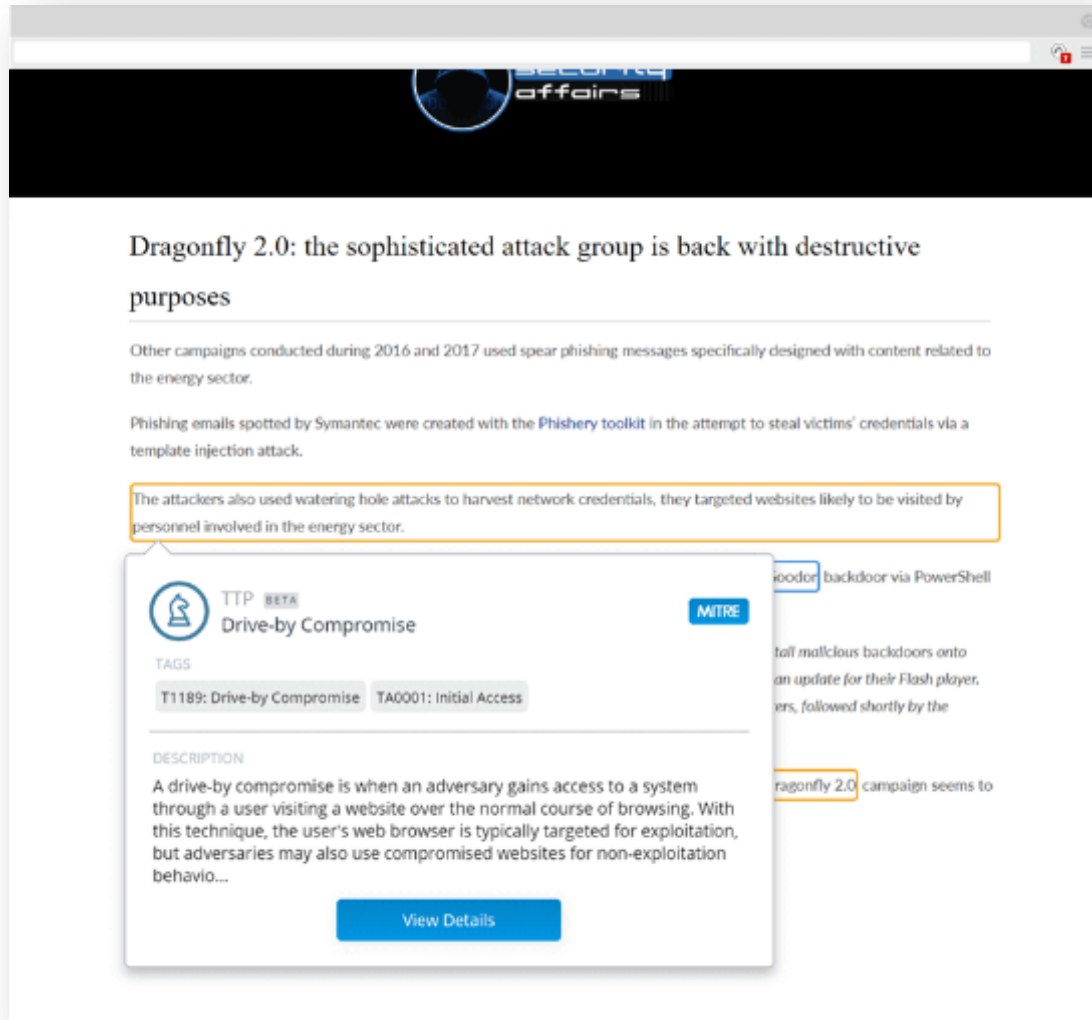


TTP 및 행위자를 기반으로
조직 환경의 위협 분석



몇 초 안에 네트워크에서 위협 찾기

Automatically Recognize MITRE ATT&CK TTPs



- 문서 스캔
- 전술, 기법 및 절차(TTP)가 포함된 문구를 자동 식별
- TTP를 MITRE ATT&CK ID와 자동 연계
- 마우스 오버 툴 팁을 통한 자동 교육/"Wikipedia" 스타일 정의
- Anomali의 자연어 처리 엔진 사용

Automatically Operationalize MITRE ATT&CK Data into ThreatStream

- 한 번의 클릭으로 MITRE ATT&CK TTP를 Anomali ThreatStream Investigation으로 가져옴
- Anomali 위협 모델에 MITRE ATT&CK TTP 라이브러리가 포함되어 있음
- Threatstream은 MITRE ATT&CK 히트맵을 자동 생성하여 위협 환경을 이해하도록 함
- 프레임워크를 기반으로 피봇과 위협 행위자 조사
- 방어되지 않은 위협이나 방어에 취약한 벡터를 식별하고 위험 수준을 지정
- 관련 MITRE ATT&CK 매트릭스를 포함한 완성된 인텔 보고서(FINTEL)의 조사 결과를 내보냄

Ongoing development of tools

APT28 uses a number of tools to compromise its targets. The group's primary malware is **Sofacy**, which has two main components. **Trojan Sofacy** (also known as **Seduplader**) performs basic operations such as downloading further malware. **Backdoor SofacyX** (also known as **X-Agent**) is responsible for stealing information from the infected computer. A Mac version of the malware is also available.

APT28 has continued to develop its tools over the past two years. For example, in 2015 the group used to maintain access to infected networks using an encrypted tunnel, but this has since been replaced by a more sophisticated method.

In addition to this, as reported by our peers at ESET last week, the group has developed a new tool called **Lojax**. This is a rootkit that resides within a computer's flash memory, allowing it to maintain access to a compromised machine even if the hard drive is replaced or the operating system is reinstalled.

The screenshot shows the MITRE ATT&CK framework interface. It displays a grid of attack techniques categorized by the 12 pillars of the framework. The categories are: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each category contains a list of specific attack techniques, such as 'Initial Access: Drive-by Compromise', 'Execution: Windows Remote Management', 'Persistence: Account Manipulation', 'Privilege Escalation: Access Tokens', 'Defense Evasion: Process Injection', 'Credential Access: Account Manipulation', 'Discovery: Cloud Service Discovery', 'Lateral Movement: Application Access Token', 'Collection: Data from Cloud Storage Object', 'Command and Control: Encrypted Channel', 'Exfiltration: Exfiltration over Cloud Service', and 'Impact: Account Access Removal'.

Anomali Lens+

- NLP를 사용하여 비정형 데이터를 스캔하고 실행 가능한 인텔리전스로 변환
- MITRE ATT&CK TTP를 식별하여 Threatstream Investigation으로 가져옴
- Anomali Threatstream 및/또는 Anomali Match와 통합
- 대상 품:
 - 브라우저
 - Threatstream 유틸리티
 - IOS/Android 디바이스(future)

The screenshot displays the Anomali Lens+ interface. On the left, a ThreatStream article titled "Russia's Elite Hackers Have a Clever New Trick" is visible, with several terms highlighted in orange boxes: "FANCY BEAR", "LoJack", "LoJax", "Sednit", and "Fancy Bear". The article text discusses a hacking group's attacks and the discovery of a new technique. On the right, a sidebar titled "ANOMALI LENS" lists various threat intelligence categories with checkmarks: "Actors (3)" including "Fancy Bear", "Sednit", and "fancy bear"; "Malware (3)" including "Computrace", "LoJack", and "LoJax"; and "Domains (2)" including "ouremedy.com" and "customertoday.org". At the bottom of the sidebar, there are buttons for "Create Threat Bulletin" and "Investigate". Below the article, a section titled "In a Flash" provides a brief summary of the "LoJax" threat, noting its familiarity and potential impact. A pop-up window titled "Actor" provides detailed information about "APT28", including its attribution to the Russian government and a list of tags: "APT28", "Sofacy", and "STRONTIUM".

Anomali Lens

Threat Analyst Research Tool

UNSTRUCTURED INTEL

Blogs
Email/Chat
Twitter...

THREAT BRIEFINGS

Intel Providers
Security Vendors
Industry/ISACs...

SECURITY TOOL DASHBOARDS

SIEM
Firewall
EDR...

ANOMALI | LENS

IOCs and TTPs

- Definitions at a glance
- Is it known to us (in TIP)?
- Sighted in our environment?

ANOMALI®

Thank you

Contact :

(주)한국밸런스

김 형덕 영업대표

Mobile : 010-7138-8889

Email : hdkim@valence.co.kr