엔드포인트 사용자 행위분석(UBA)

스플렁크 총판 SCK
박용 Splunk Consultant
andy.park@sckcorp.co.kr

splunk> turn data into doing™

보안의 현실

볼륨과 복잡성에 압도된 SOC

진화하는 위협

$6조

2021[1]까지 사이버 범죄 피해

데이터 침해

55%

지난 12개월 동안 최소 한 번의 침해 경험[2]

내부자 및 지능형 위협이 우위

64%

내부 및 외부 위협 행위자[2]

많은 경고

+15K

일일 보안 경고[3]

기술 부족

+3M

사이버 보안 인력 격차[4]

Sources:
[1]2019 Official Annual Cybercrime Report by Herjavec Group
[2]Forrester Research Top Cybersecurity Threats in 2019
[2]2017 Ponemon Study
[3](ISC)[2] Cybersecurity Workforce Study 201

splunk> turn data into doing™

고도화된 위협을 관리하는 것이 어려운 이유?

자금조달 잘됨	증식하도록 설계
신중하게 계획됨	우회하도록 설계됨
위장된 거짓 의도	무해한 것처럼 보임

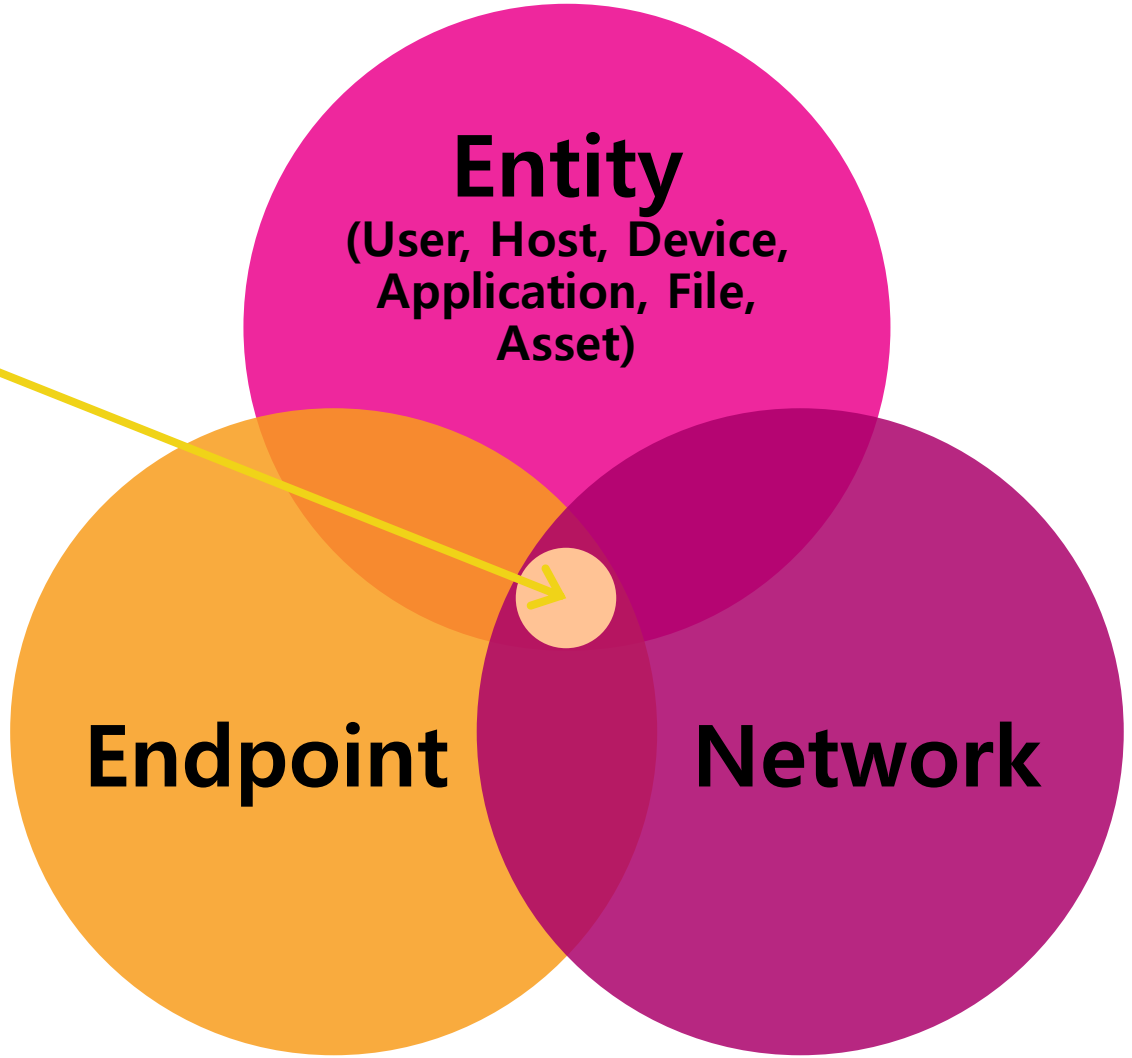
위협 탐지에는 조기 발견과 분석이 필요!!

U(E)BA 란?

U (User)	**User-centric** 사용자 행위를 주된 목적으로하는 분석
E (Entity)	**Not user-exclusive** 사용자 이외에도 다른 것을 분석(host, device, file, asset, applicaton 등) 그래서 UEBA는 EBA가 아닌, (U+E)BA가 필수
B (Behavior)	**Focus on behaviors and activities** 역할, 속성, 파라미터가 아닌 행위에 집중되어 있음 주요 임무는 흥미롭고 악의적인 행동 및 행위를 찾는 것
A (Analytics)	**Advanced analytics** 단순한 룰-기반 매칭이 아닌 고급분석(통계, 아노말리, 머신러닝 등) 머신러닝 일 필요는 없지만 하드코딩 된 룰, 임계값 및 평균을 단독으로 사용하는 것보다 뛰어남

행위 탐지를 위한 세가지 집중 분야

Behavioral Detection
(일반적인 엔티티의 액션(Normal)과 경보(Alert)로부터 이상행위(Deviation) 찾기)



스플렁크 UBA의 3가지 핵심요소

1. **Use case(s)** 무엇입니까?
2. 유스케이스를 처리하기 위해 필요한 **Data source** 무엇입니까?
3. 그리고 **techniques / methods** 은 무엇입니까?

스플렁크 Use-Cases

계정 탈취

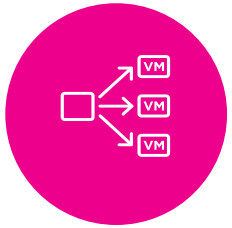
(Account Takeover)

비활성화된 계정 액티비티
종료된 사용자 액티비티
서비스 계정에 의한
인터랙티브 로그인
서비스 계정에 의한
VPN 로그인

의심스러운 행위

(Suspicious Behavior)

의심스러운 배지 액티비티
계정 복구 탐지



측면 이동

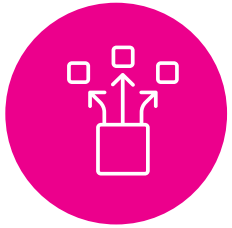
(Lateral Movement)

의심스러운 계정 잠금
파워쉘 액티비티 후 특권 권한
에스컬레이션
로컬 계정 생성
패스워드 정책 우회
다중 인증 및 실패

클라우드 스토리지

(Cloud Storage)

많은 다운로드
많은 삭제
비정상적 파일 액세스



데이터 유출

(Data Exfiltration)

비정상적 USB 디바이스
많은 USB 첨부
이메일 첨부

데이터 소스

SPLUNK ENTERPRISE
또는 SIEM

- 액티브 디렉토리 / 도메인 컨트롤러
- DNS, DHCP
- 방화벽
- 프록시 서버

최소한 사항

- VPN
- 엔드포인트
- DLP
- 서버
- 어플리케이션

옵션 사항

Techniques / Methods

임계치 기반 룰 생성

통계 기반 룰 생성

머신러닝 (ML)

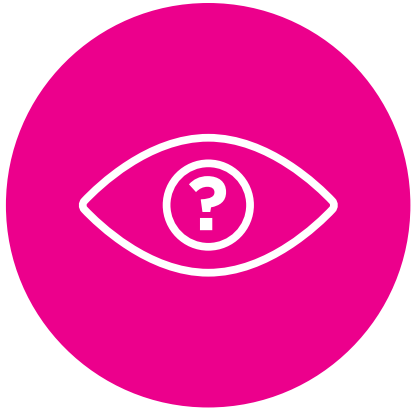
Human-driven

알려진 위협 영역

ML-driven

알려지지 않은 위협 영역

스플렁크 사용자 행위 분석



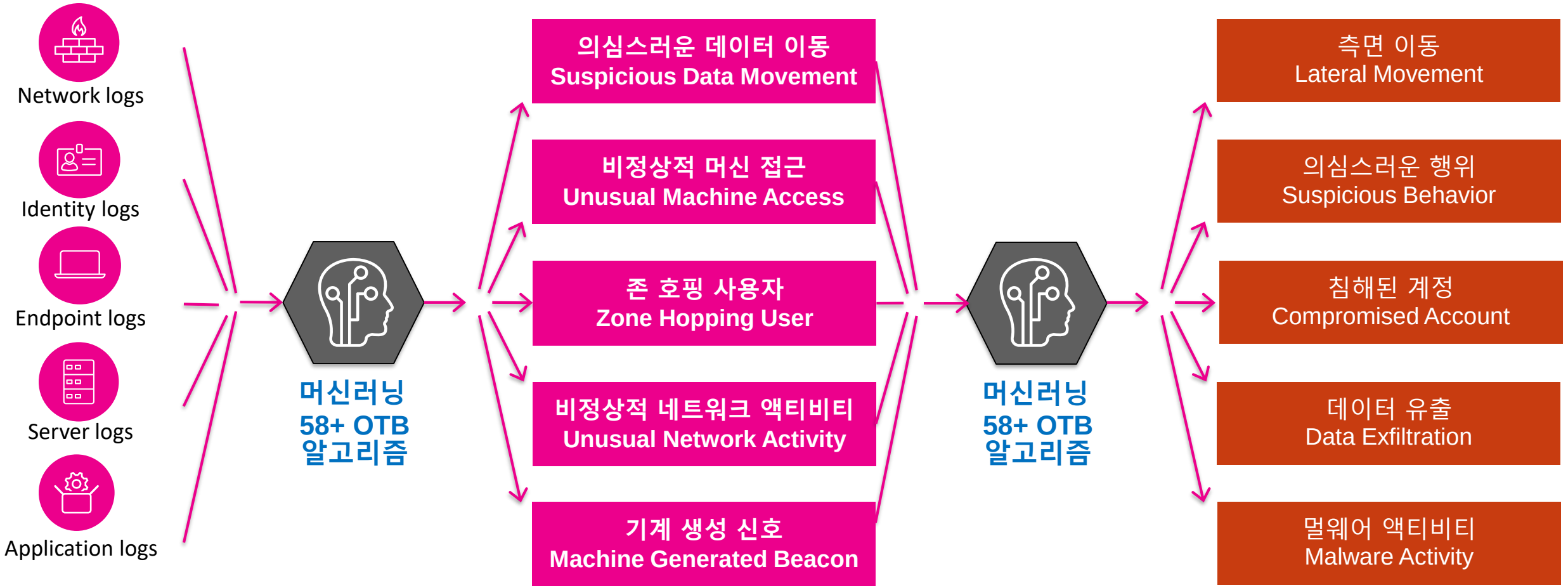
변칙적인
행위

위험한 사용자
모니터링

알려지지 않은
위협

unsupervised machine learning algorithms + platform (algorithms to detect unknown attacks and insider threats) + 58+ 머신러닝 알고리즘 + 65+ 이상징후 classification + 25+ 위협 classification

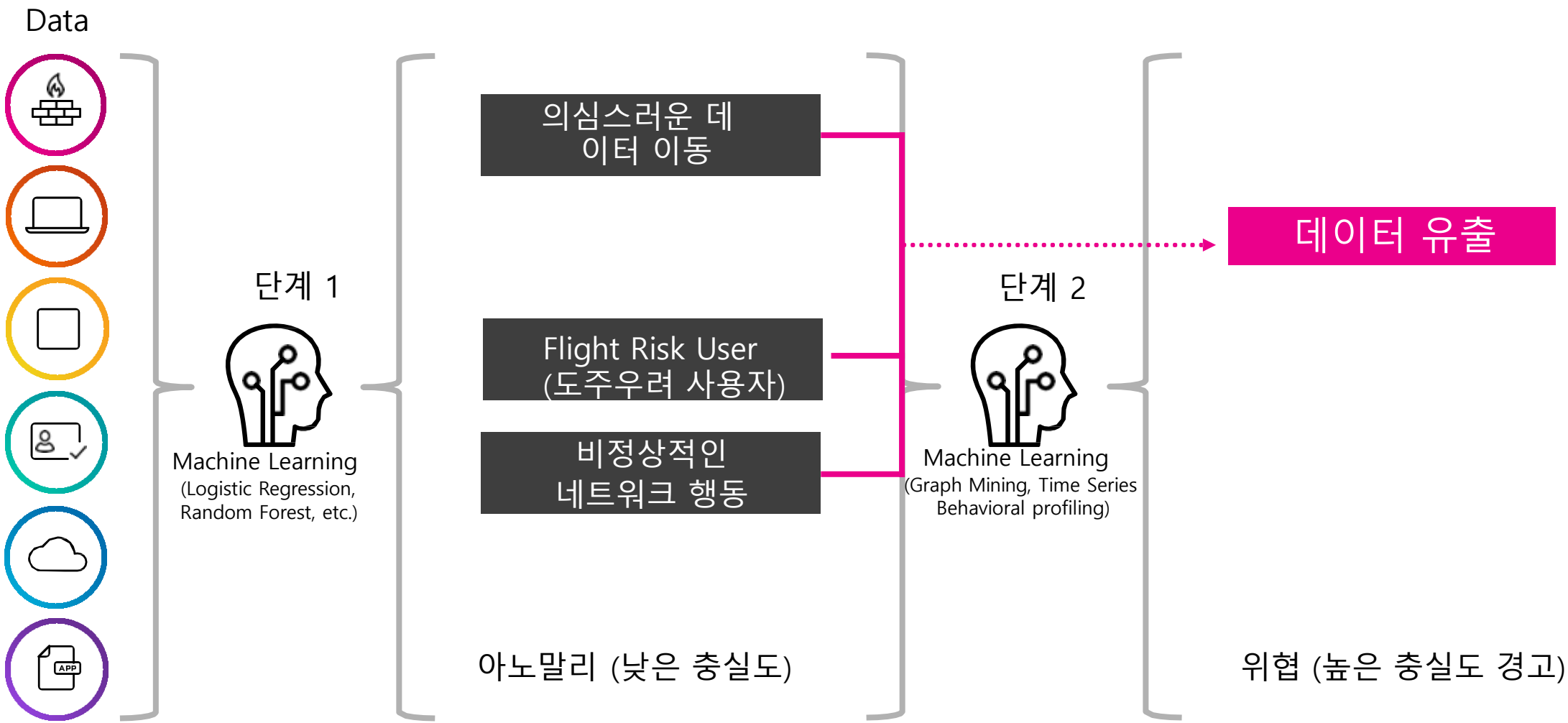
Splunk UBA 어떻게 동작하나?



OTB : Out-Of-The-Box

splunk> turn data into doing

Splunk UBA 어떻게 동작하나?



스플렁크 사용자 행위 분석 핵심요소(Pillars)

Five Foundational Pillars

실시간 & 빅데이터 아키텍쳐

행위 기준선 & 모델링

비지도 머신러닝

이상징후 탐지

위협 탐지

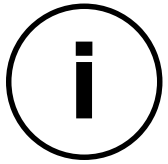
Splunk User Behavior Analytics™

splunk> Platform for Machine Data

분석기반 보안 포트폴리오

Enterprise Security
Detect, Investigate & Response

- 글래스 테이블(커스텀 개인별 대시보드)
- 보안 메트릭 & 인시던트 응답
- 적응적 응답(Adaptive Response)



Splunk Enterprise
Investigate

알려진 영역

- 로그 수집
- 룰, 통계, 상관분석
- 애드혹 서치

Human-driven

Splunk UBA
Detect

알려지지 않은 영역

- 위험 행위 탐지
- 엔티티 프로파일링, 스코어링
- 사이버 킬체인, 그래프 분석

ML-driven

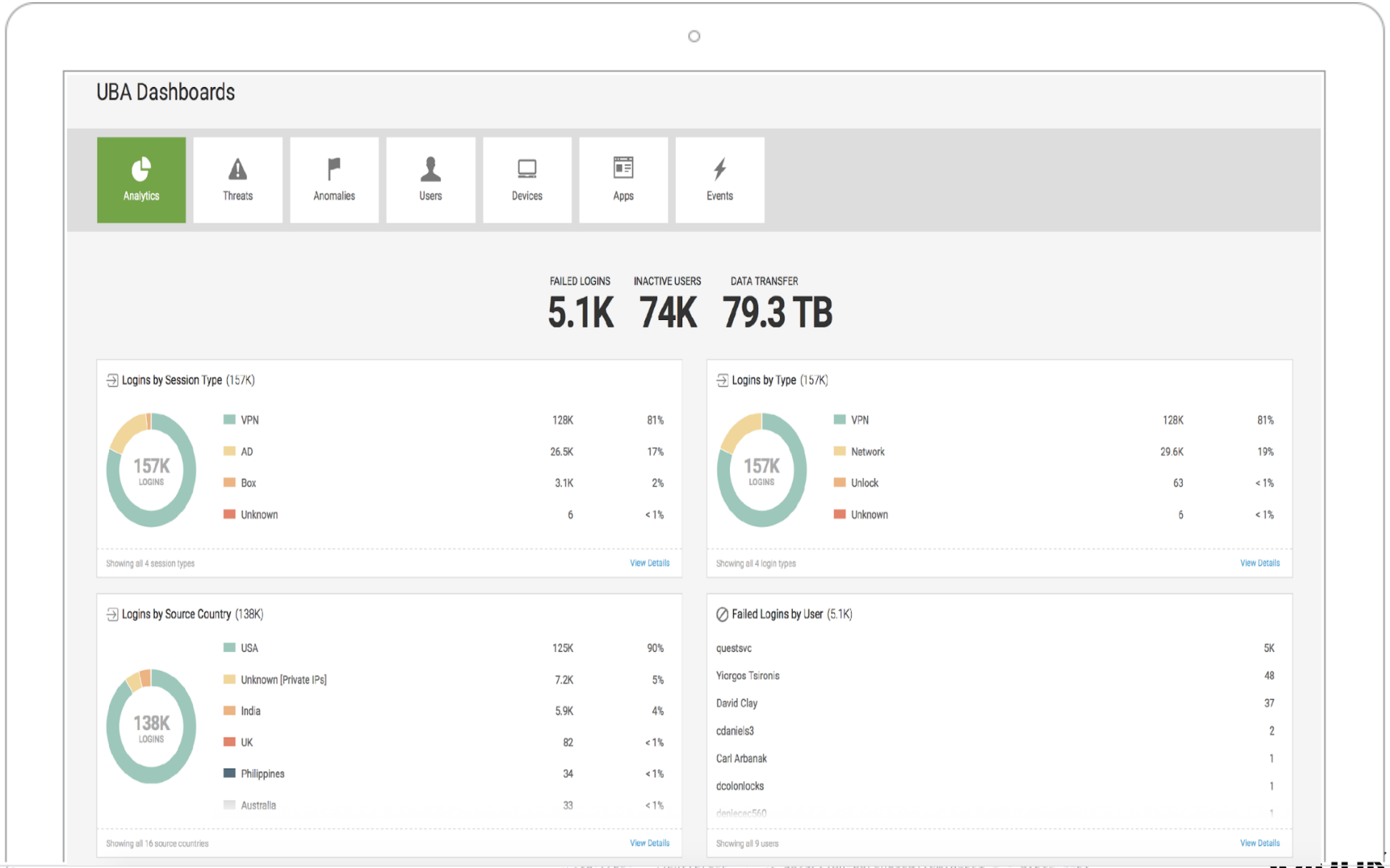
splunk> turn data into doing

Thank You

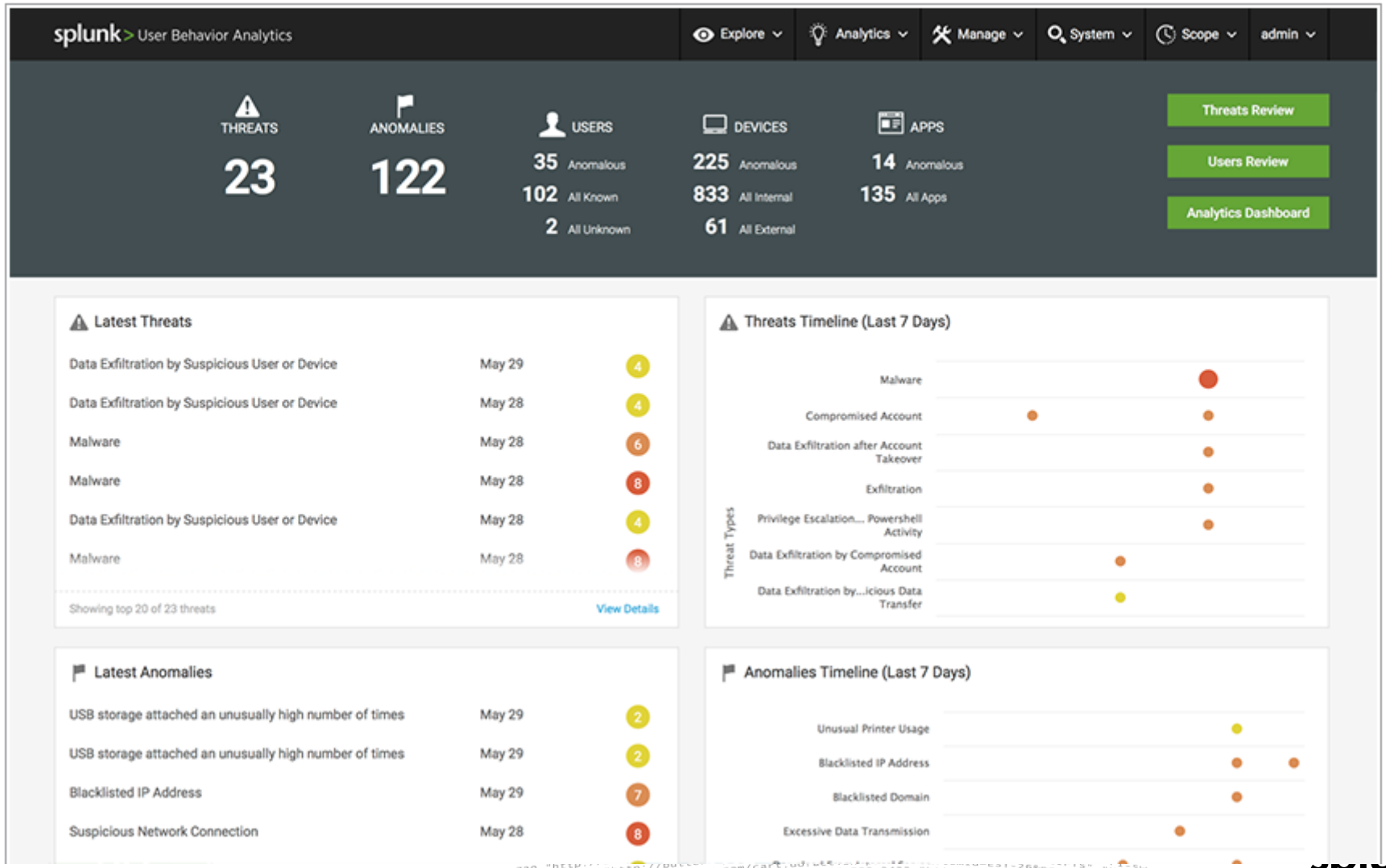
splunk> turn data into doing™

별첨. Splunk UBA 화면

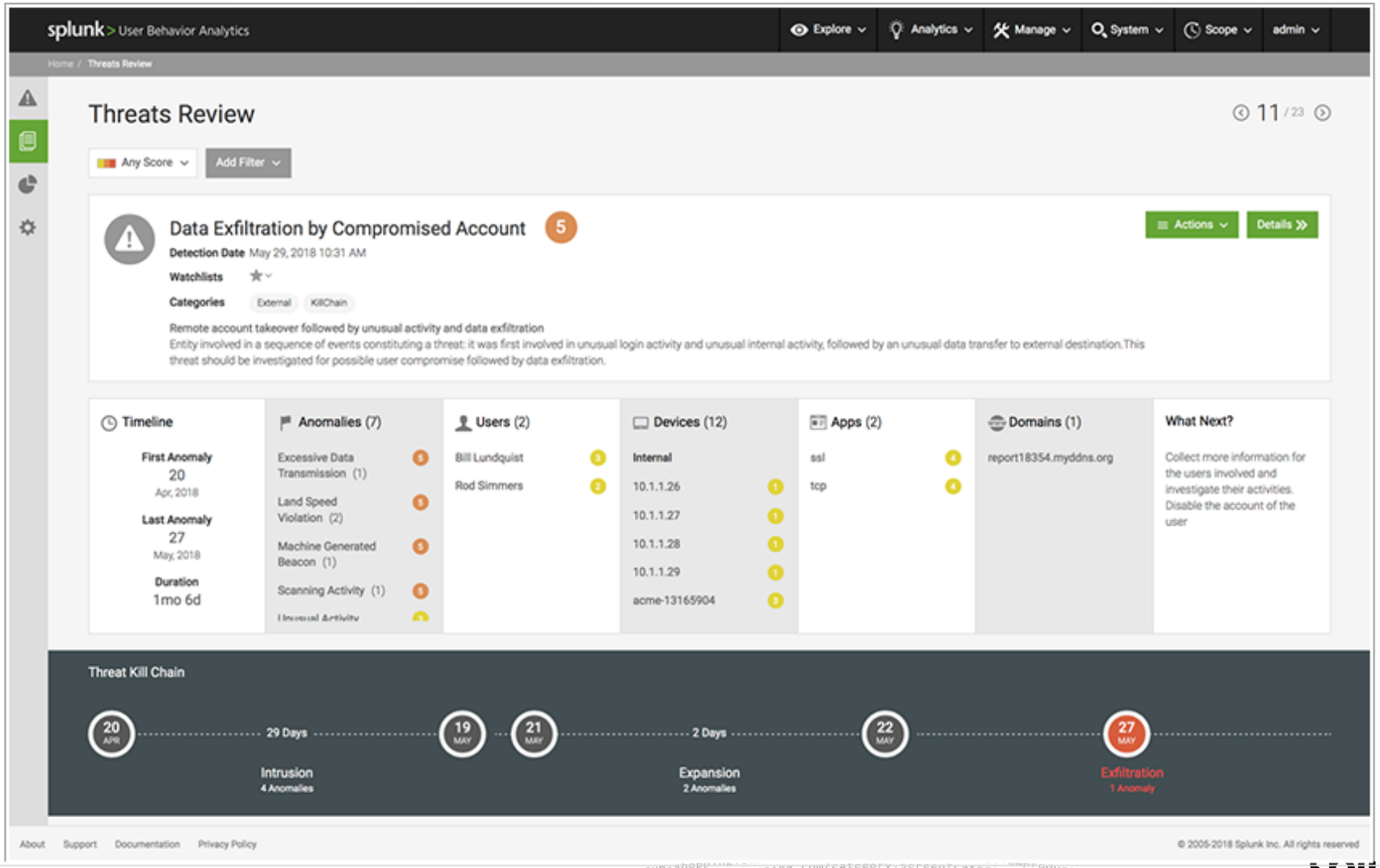
UBA 대시보드


UBA Dashboards
Analytics
Threats
Anomalies
Users
Devices
Apps
Events
FAILED LOGINS
5.1K
INACTIVE USERS
74K
DATA TRANSFER
79.3 TB
Logins by Session Type (157K)
157K
LOGINS
VPN 128K 81%
AD 26.5K 17%
Box 3.1K 2%
Unknown 6 < 1%
Showing all 4 session types
View Details
Logins by Type (157K)
157K
LOGINS
VPN 128K 81%
Network 29.6K 19%
Unlock 63 < 1%
Unknown 6 < 1%
Showing all 4 login types
View Details
Logins by Source Country (138K)
138K
LOGINS
USA 125K 90%
Unknown [Private IPs] 7.2K 5%
India 5.9K 4%
UK 82 < 1%
Philippines 34 < 1%
Australia 33 < 1%
Showing all 16 source countries
View Details
Failed Logins by User (5.1K)
questsvc 5K
Yiorgos Tsironis 48
David Clay 37
cdaniels3 2
Carl Arbanak 1
dcolonlocks 1
Showing all 9 users
View Details

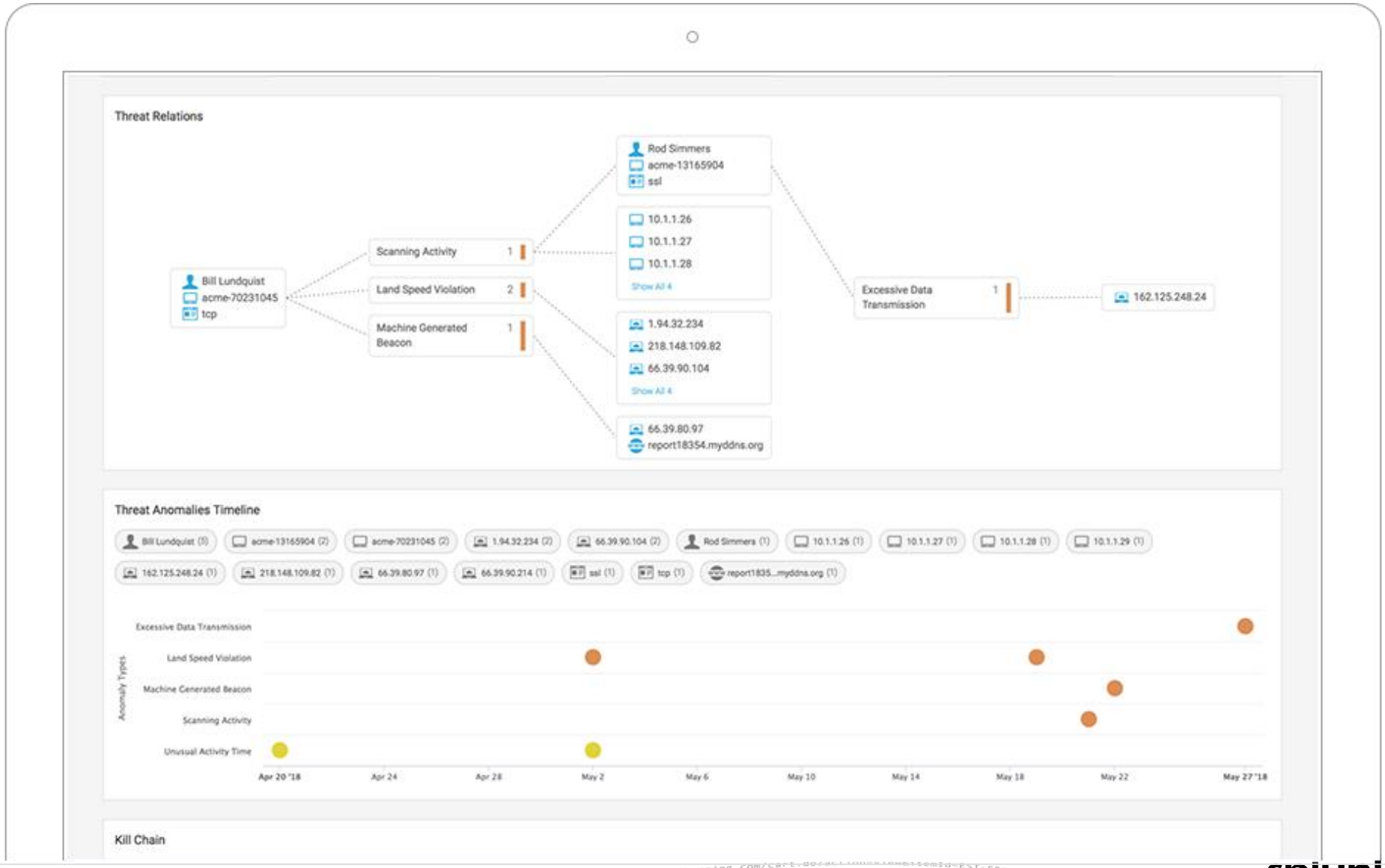
머신러닝을 사용하여 알려지지 않은 위협 및 비정상적인 동작 감지



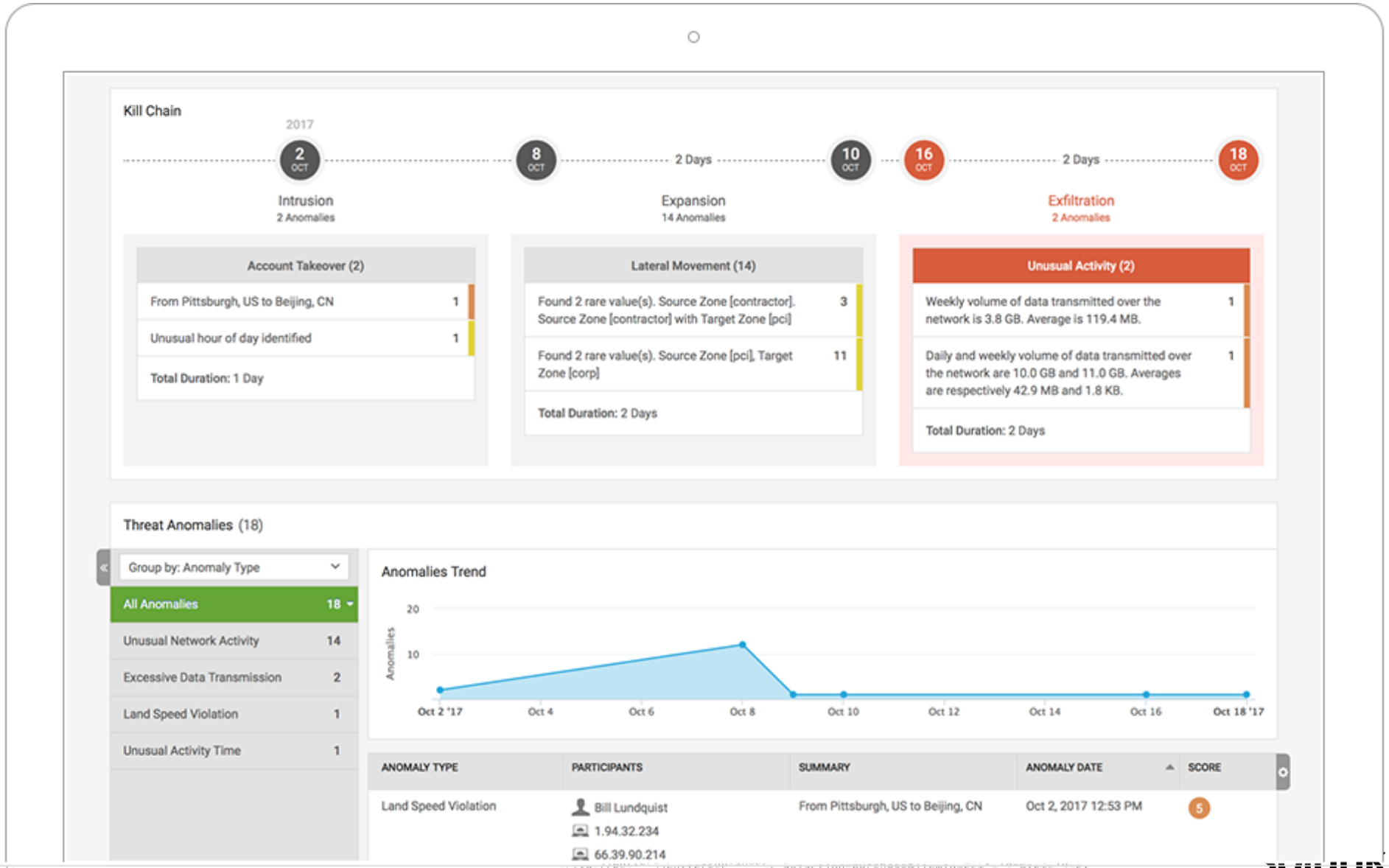
위협 탐지 신뢰도 및 정확성 향상



SOC 자원 증대



가시성 및 탐지 기능 향상



SCK

splunk> listen to your data

이상징후 탐지