Splunk Core + ES(SIEM) 소개

splunk> turn data into doing™

Who is Splunk?

- **글로벌 HQs:**

  -샌프란시스코(AMER)

  -런던(EMEA)

  -홍콩(APAC)
- **직원수 전세계 6,000+명**
- **연 매출 약 2조 4천억원 ($1,803 YoY +30%)**
- **나스닥 상장 : SPLK**

- **2003년 시작**
- **제품 구성:**

  -Splunk Enterprise

  -Splunk Cloud

  -Premium Solutions
  - Enterprise Security(SIEM)
  - SOAR, UBA, TruStar(TIP)
  - Observability
  - IT Service Intelligence

- **고객사 (전체): 16,000+**
- **국가기준: 110개국+**
- **Fortune 100대 기업: 92+**
- **고객사 (한국): 400+**

  -중소기업, 대기업, 그룹 계열사
- **최대 라이센스: 10+ PB/일**

splunk>

turn data into doing™

"**머신데이터**를 아무런 **제약 없이 수집>저장>분석>시각화** 할 수 있는 **실시간 분산 플랫폼**"

머신데이터
(Machine Data)

- 서버/NW 로그
- 각종 설비 데이터
- 애플리케이션 로그
- 기타 **모든 텍스트 형태의 데이터**

제약 없음
(No Limits)

- 비정형/반정형/정형 데이터
- 데이터 **포맷 무관**
- 데이터 **용량 무관**
- 데이터 **속도 무관**
- **제약 없이 수용**

엔드 투 엔드
(End-to-End)

- 데이터의 생성부터 가치 획득까지 하나의 솔루션에서 처리
- 별도의 외부 솔루션 불필요
- 복잡한 코딩 및 SI 개발이 필요 없음

실시간 및 분산
(Real-time)

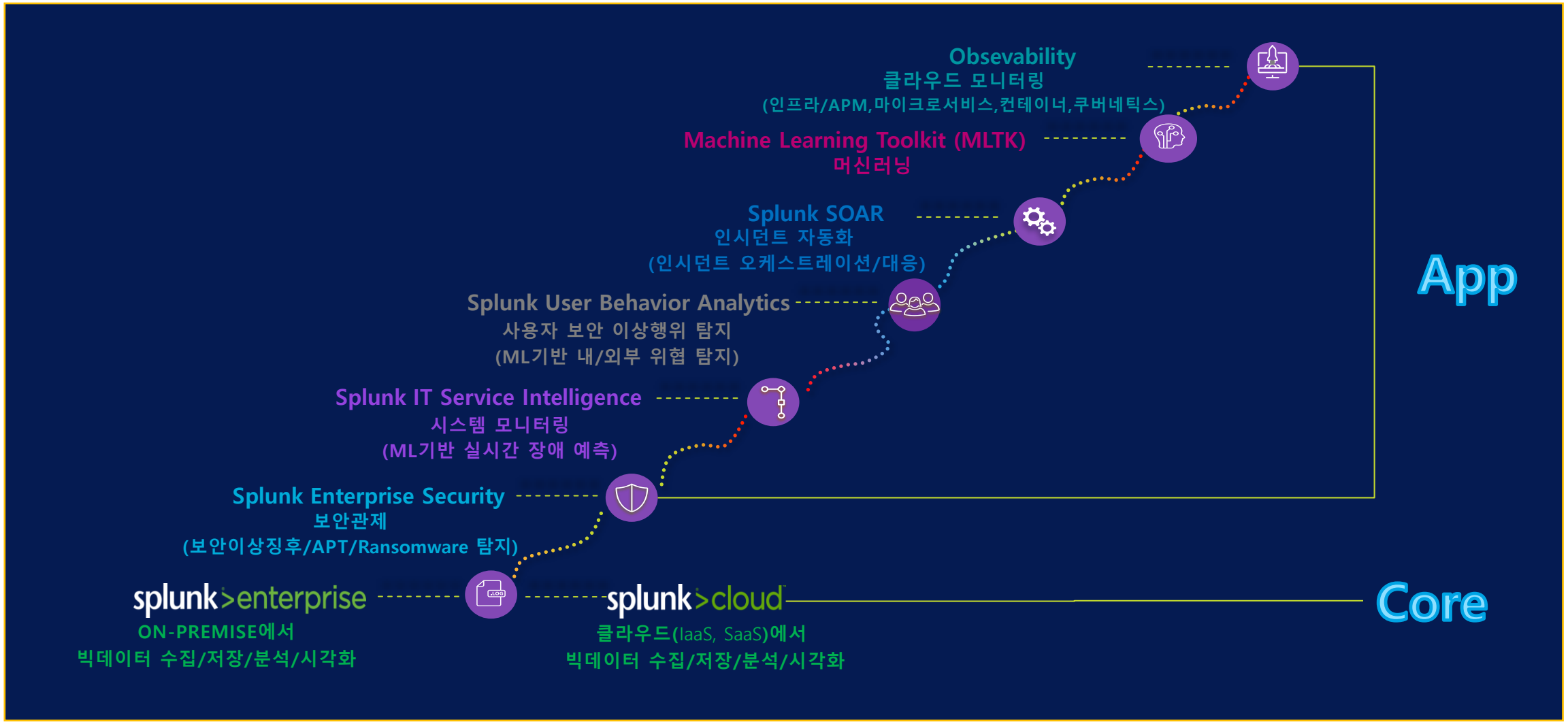
- 모든 데이터 실시간
- 처리, 즉시 결과 확인
- 분산 저장, 분산 검색
- HA 기본 제공
- 성능 및 용량의 선형 확장 (scale-out)

플랫폼
(Platform)

- 커스터마이징 용이
- 외부 시스템과 손쉬운 연동
- **2500+ 무료 앱**을 통한 기능 확장

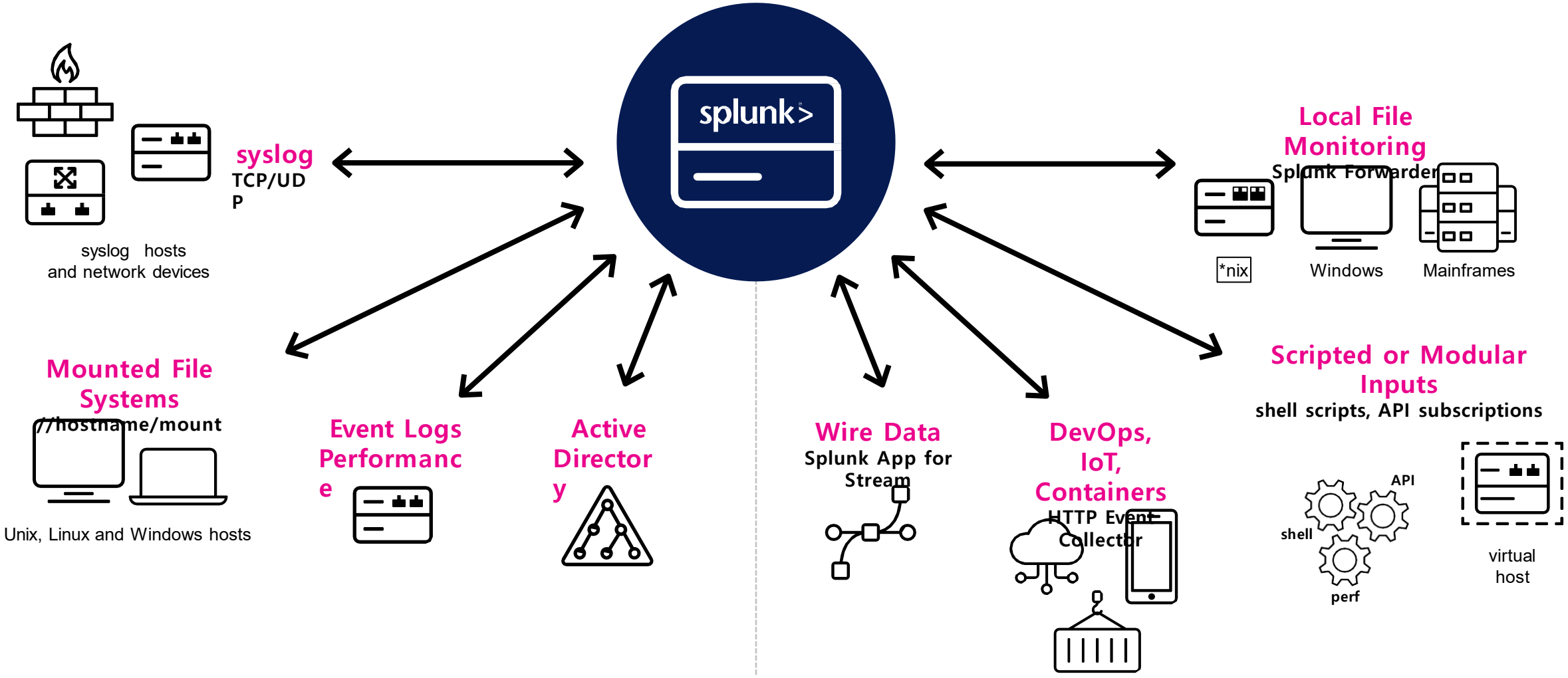
Splunk 솔루션 라인업

ITOps(IT운영), DevOps(개발운영), SecOps(보안운영) 및 AIOps(인공지능운영)를 위한 유일한 플랫폼



1. 다양한 이기종 데이터 소스로부터 제약 없는 수집

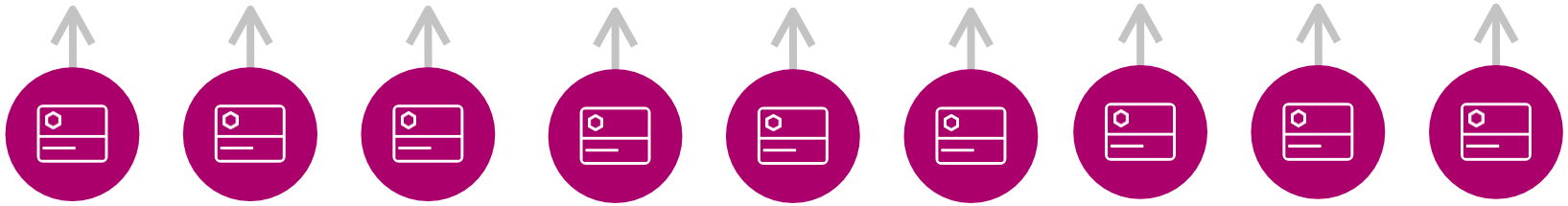
에이전트/에이전트리스 방식 제공으로 유연성과 최적화된 수집 기능 제공



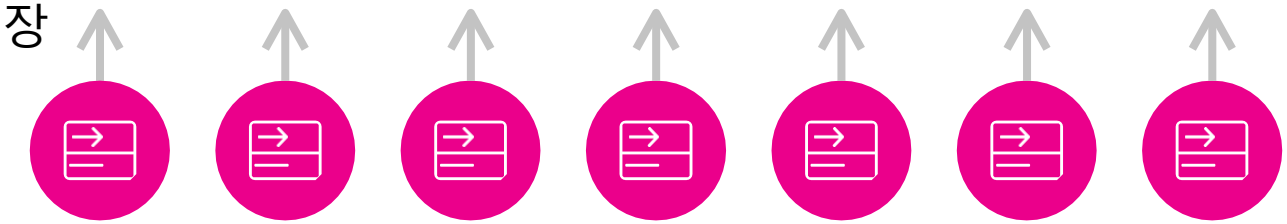
2. 하루 수백 TB 수집까지 확장

엔터프라이즈급 확장성(Scale out), 장애 복구(HA, Clustering) 및 통합성 제공

Search head로 검색, 분석, 시각화, 관리 수행



Splunk Indexer로 자동 부하분산하여 균등하게 데이터 압축 저장

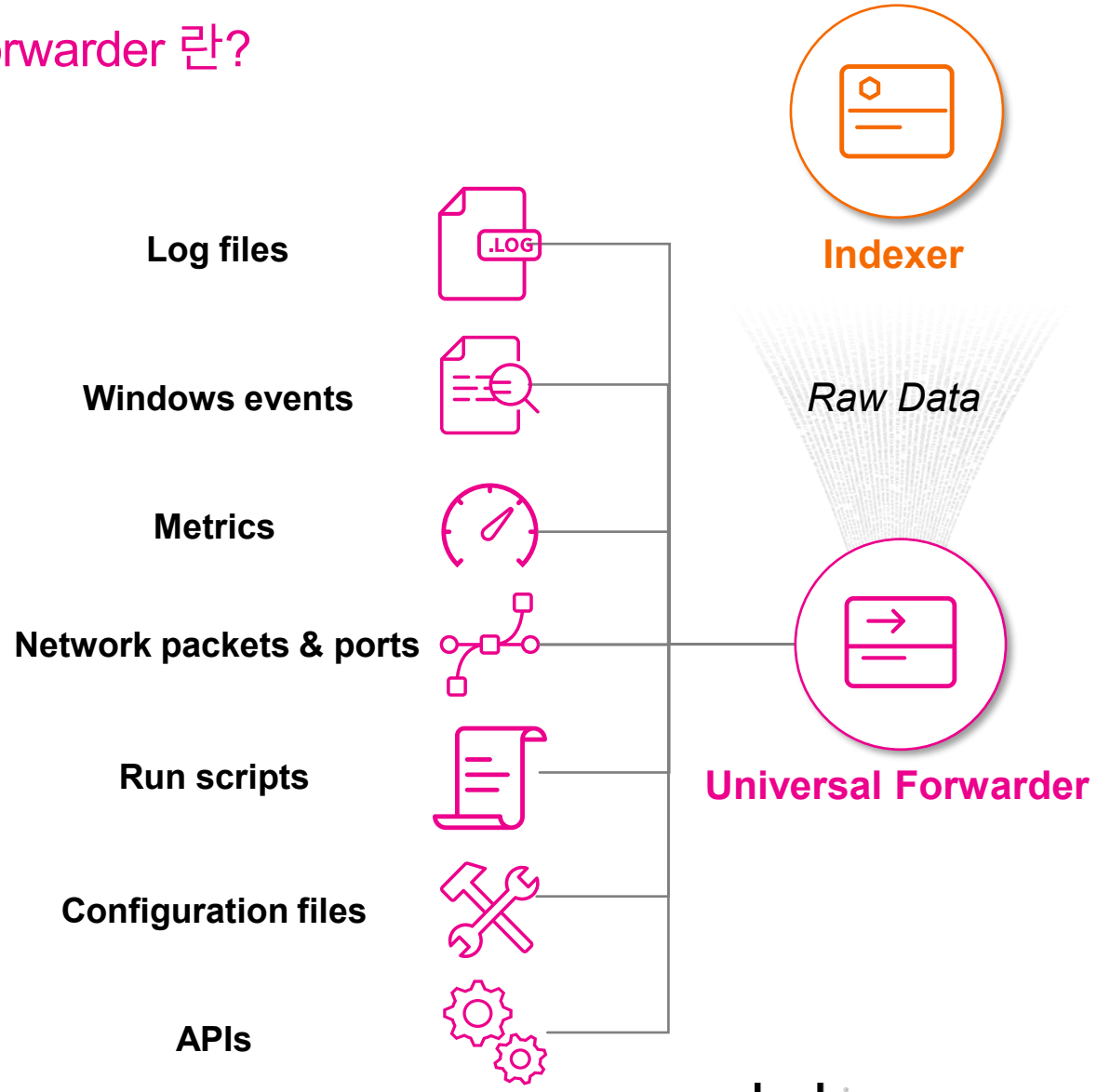


Splunk Forwarder를 통해 수천대 서버에서 데이터를 전송

2. 하루 수백 TB 수집까지 확장

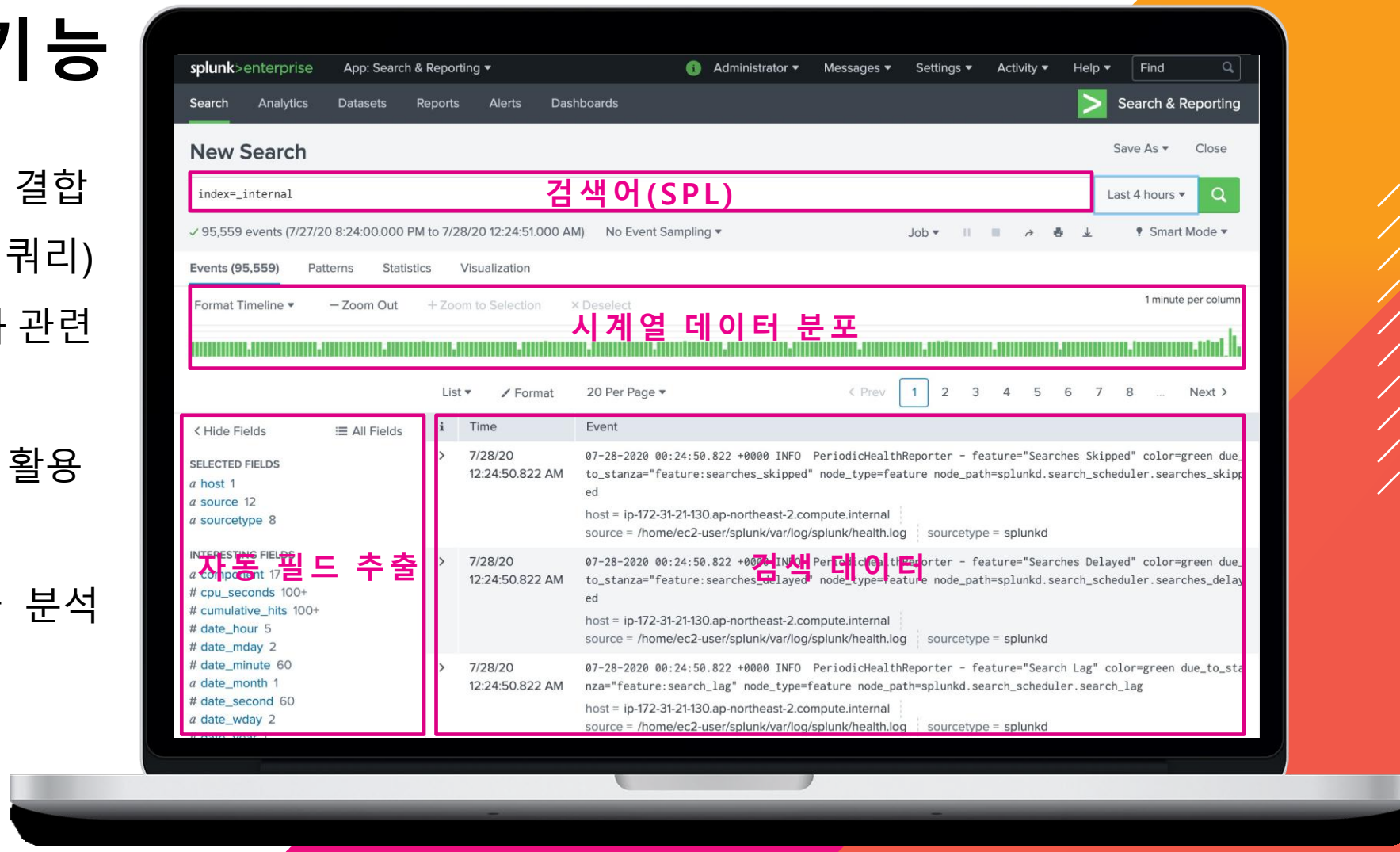
Universal Forwarder 란?

- 원격에서 안정적인 데이터 수집
- 다양한 데이터 소스에서 수집하는 방법을 포함
- 가볍고 단순하지만 많은 장점을 갖추고 있음:
  - ✓ 버퍼링 / 전송 보장
  - ✓ 암호화
  - ✓ 압축
  - ✓ 부하 분산
  - ✓ 그외 다양한 기능들!
- 매우 작은 설치 공간
- 단순한 설정

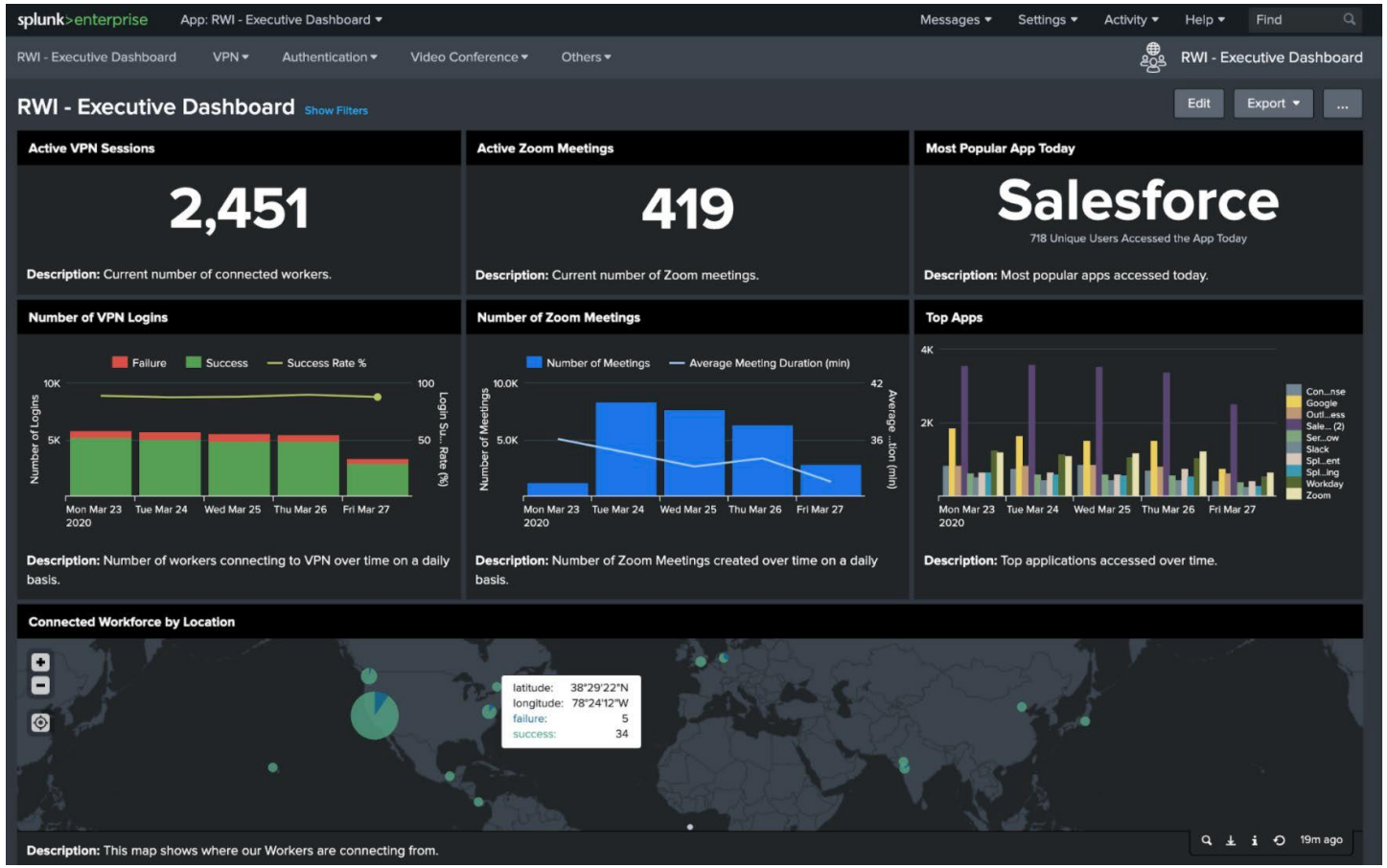


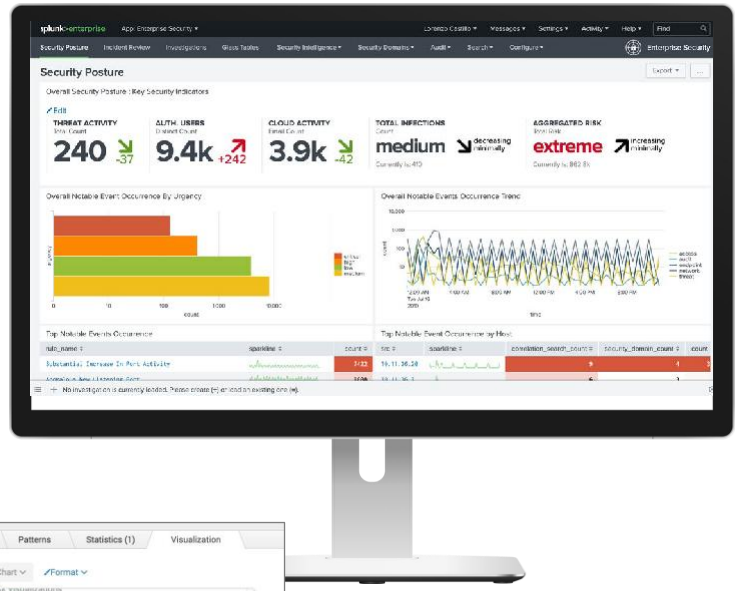
3. 강력한 검색 기능

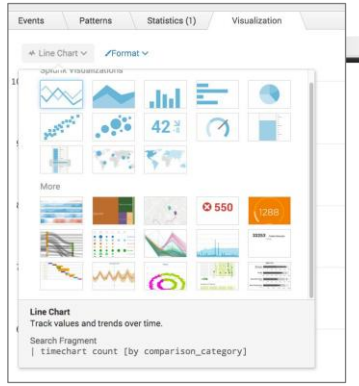
- SQL과 Unix 파이프라인 구문이 결합된 최적의 검색 언어 SPL(검색 쿼리)
- 검색, 상호 연관, 분석 및 시각화 관련된 160개 이상의 명령어
- 통계, 그래프, 각종 연산 함수를 활용한 분석
- 신속하게 필요한 데이터를 찾아 분석하여 사고의 근본 원인을 파악



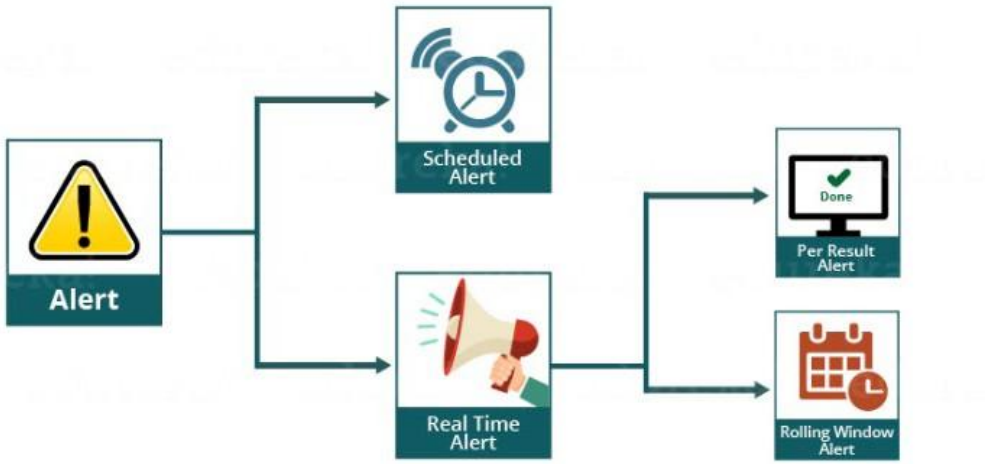
4. SPL을 알면 내장 UI 컴포넌트를 활용하여 빠른 대시보드/레포트/경고 제작



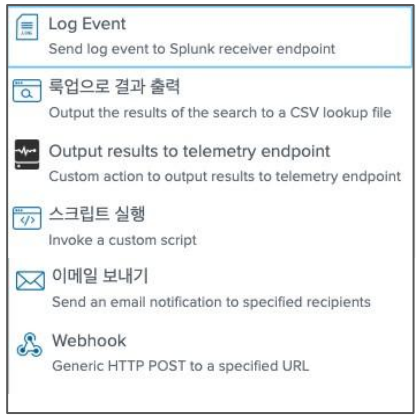




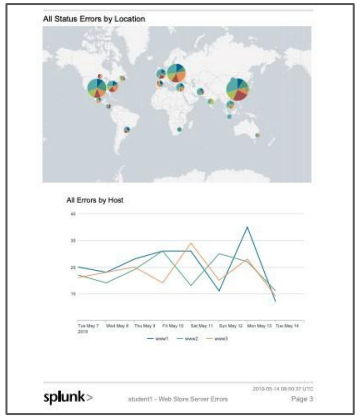
5. 실시간 감시 및 알람(경고)



경고 트리거 옵션



PDF 예약 전송



- 실시간 모니터링 및 알람 등록
- 검색 쿼리(SPL) 저장 후 실시간/주기적인 실행을 통한 모니터링
- 자동 대응을 위한 각종 프로그램/스크립트 실행
- Email/SMS 통지 및 Jira/NMS/SNS 연동
- PDF 스케줄 전송 기능을 통한 보고서 이메일 발송

6. Machine Learning 기반 분석 지원

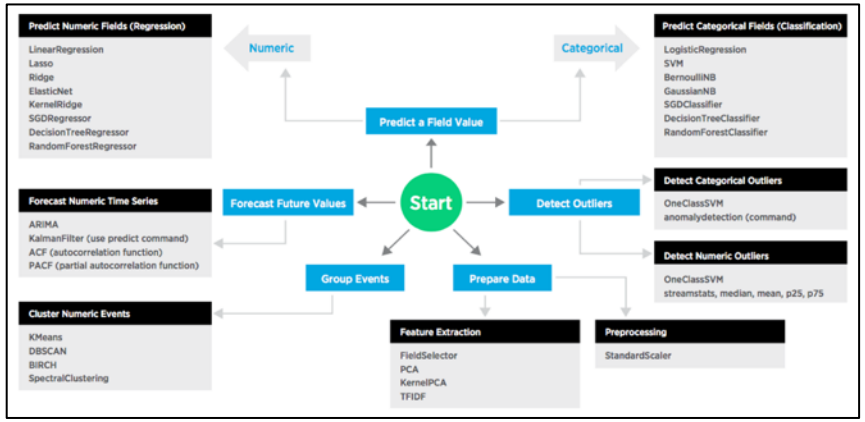
MLTK(Machine Learning Toolkit) 앱을 통해, 위협 및 이상행위 탐지를 위한 머신러닝 모델 생성 및 검증/운영을 손쉽게 구현하기 위한 다양한 기능을 제공하여, 단순 메트릭 이상치 검출 뿐 아니라 다양한 예측 모델을 적용하여 보안 사고 방지에 활용

항목	내용
기본 ML 알고리즘 탑재 + 오픈소스 라이브러리 활용	• 30+ 기본 알고리즘 모델 탑재 • 지도학습: Logistic & Linear Regr., SVM, Random Forest 등 • 비지도학습: K-means, DBSCAN, Spectral Clustering 등 • API 제공으로 SciPy의 300+ 오픈소스 라이브러리 탑재 가능
머신러닝 쇼케이스 & 어시스턴트	• 44개 보안, IT등 머신러닝 적용분야에 대한 예시 제공으로 고객 데이터셋을 가지고 빠르고 쉽게 ML적용 후 검증 가능
모델링 지원	• 알고리즘 선택 옵션 설정, fit 설정 후 가이드 모델 구축, 유효성 검사 및 시각화, 모델 정확도 검증 기능 탑재로 ML모델링 고도화 지원
다양한 보안 고객의 머신러닝 적용 사례	• 전세계 고객이 사용 중 • 검증된 유즈케이스 및 고객 레퍼런스 확보로 적용 위험성 최소화

다양한 ML 예제 어시스턴트

보안 예제

- Predict VPN Usage
- Predict the Presence of Malware
- Detect Outliers in Number of Logins
- Detect Outliers in Bitcoin Transactions
- Forecast the Number of Employee Logins



30+ 다양한 알고리즘 기본 탑재

6. 스플렁크 플랫폼에서의 커스텀 ML

앱 에코시스템

MLTK

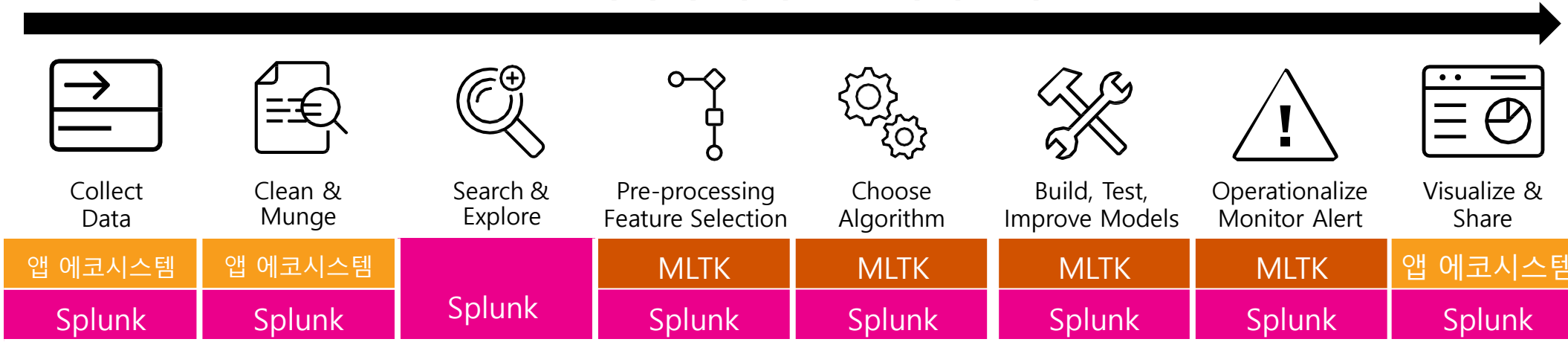
Splunk

Splunk의 App Ecosystem에는 데이터를 가져오고, 구조를 적용하며 ,데이터를 시각화하여, 가치 창출 시간을 단축 할 수있는 1000 가지의 무료 애드온이 포함되어 있습니다.

Machine Learning Toolkit은 다양한 ML 개념을 탐색하기위한 새로운 SPL 명령, 커스텀 시각화, 어시스턴스 및 예제를 제공합니다.

Splunk Enterprise는 머신 데이터의 인덱스 생성, 검색, 분석, 경고 및 시각화를 위한 미션 크리티컬 플랫폼입니다.

데이터 사이언스 파이프라인



splunk> 운영 인텔리전스를 위한 플랫폼

7. 다양한 App 생태계 및 커뮤니티

앱 생태계를 활용하여 최소의 리소스로 빠르게 요구사항을 구현

splunkbase.com **2500+** 개 이상의 다양한 앱

Answers.splunk.com **9만건**의 Q&A

전세계 **85**개 user groups

400 여개의 partners

7. 다양한 App 생태계 및 커뮤니티

App & Add-on

- Splunk, 기술 협력 파트너 또는 사용자 커뮤니티에서 개발
- Splunk 플랫폼을 확장하는데 도움을 주는 사전 빌드 된 패키지
- 특정 기술, 목적 또는 사용 사례에 대한 콘텐츠 및 기능(예 : 보고서, 대시 보드 및 통합)을 제공하고 필요에 따라 유연하게 커스터마이징 해서 사용
- Splunkbase 에서 2500개 이상의 무료 App 과 Add-on 다운로드 가능
  https://splunkbase.splunk.com/

Apps

✓ 사전 구축된 대시보드, 보고서, 경고, 시각화 및 워크플로우를 포함하여 Splunk의 데이터에서 가치 창출 시간을 단축하도록 설계된 콘텐츠

Add-ons

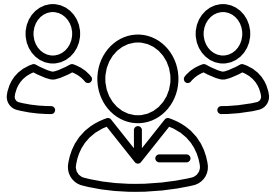
✓ 데이터 가져오기, 데이터 매핑 또는 저장된 검색(saved searches) 및 매크로 제공과 같은 특정 기능을 Splunk에 제공

8. Splunk as a Service

가장 빠른 가치 창출 시간, 최소한의 인프라, 최대 가치

간단한 3단계 :

1. 온보드 데이터
2. 온보드 사용자
3. 데이터에서 가치 얻기



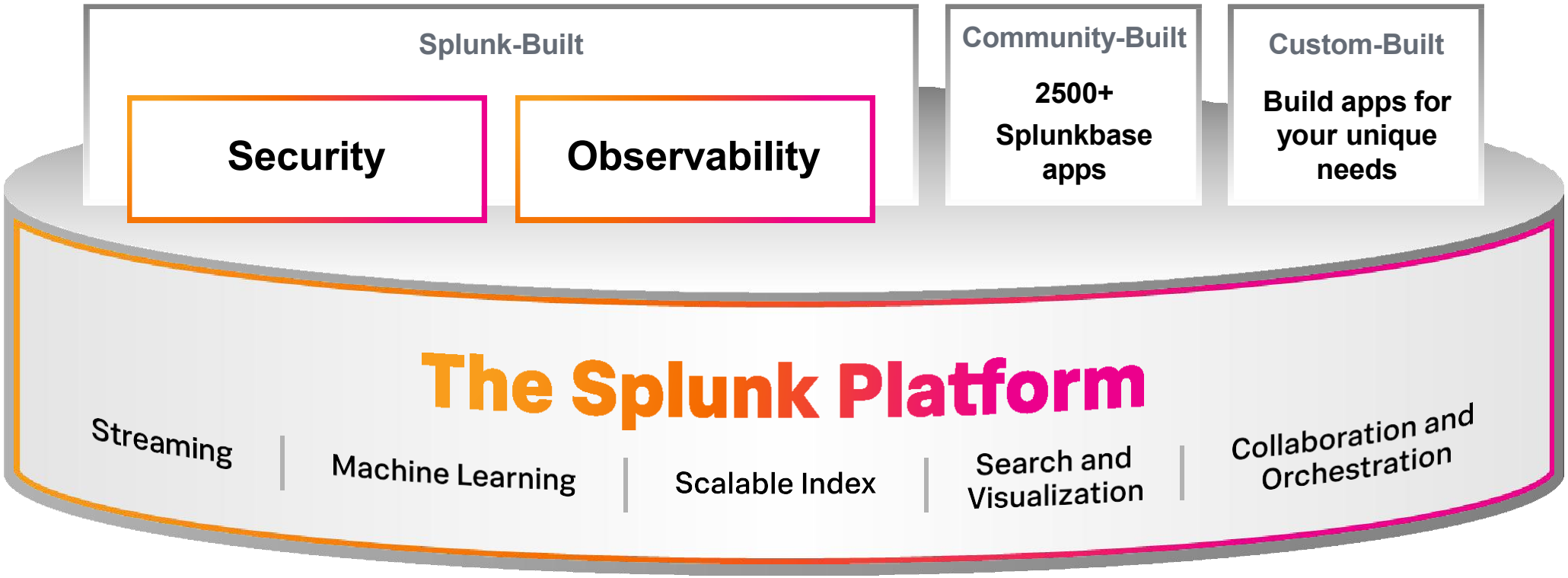
splunk>cloud™

데이터 수집

- ✓ **Software as a service (SaaS)**
- ✓ **보안** - ISO27001, SOC2 Type 2, PCI, HIPAA, FedRAMP
- ✓ **전송 중 암호화** - optional encryption-at-rest
- ✓ **탄력적인 인프라**
- ✓ **100% uptime(가동시간) 보장**
- ✓ **24/7 NOC/SOC 지원팀**

> **Splunk Cloud Service Description:** https://bit.ly/SplunkCloudServDesc

9. Splunk 란



0010
01010
0101
Events | **Logs** | **Metrics** | **Traces**

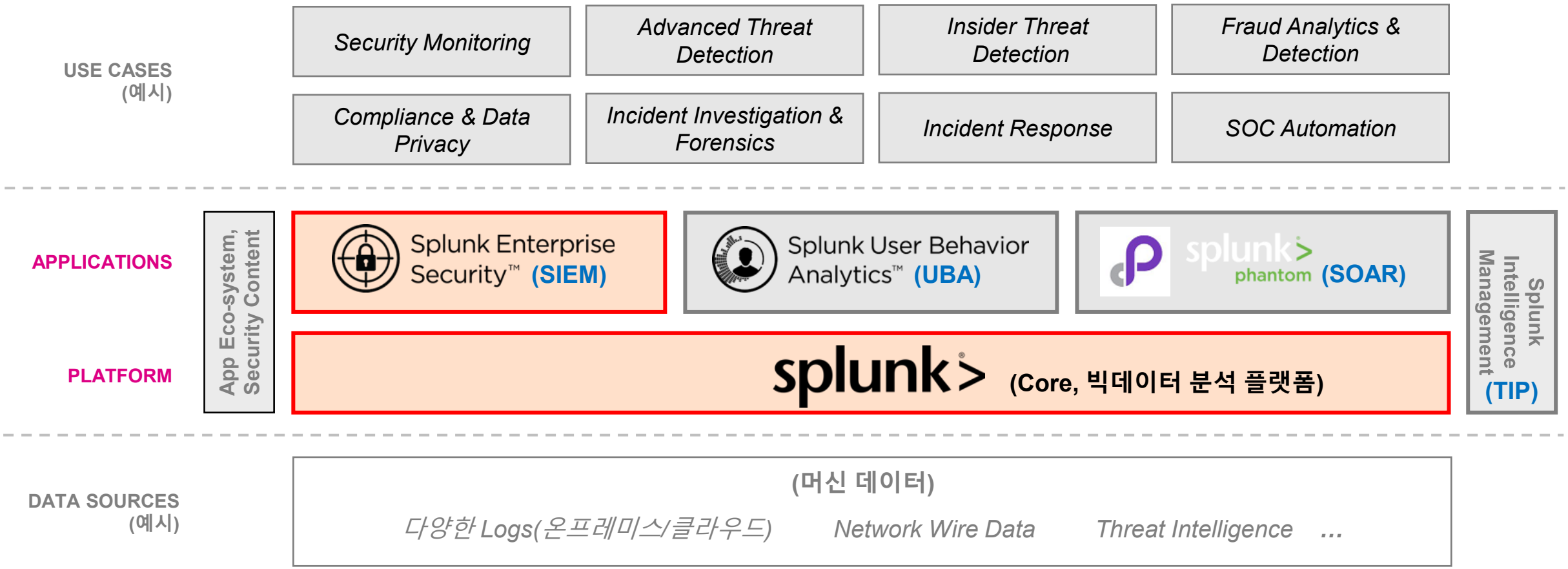
Public Clouds **Third-Party Tools** **On-Prem Data Centers** **Apps / Services** **Edge**

ta into doing

Splunk ES(SIEM) 소개

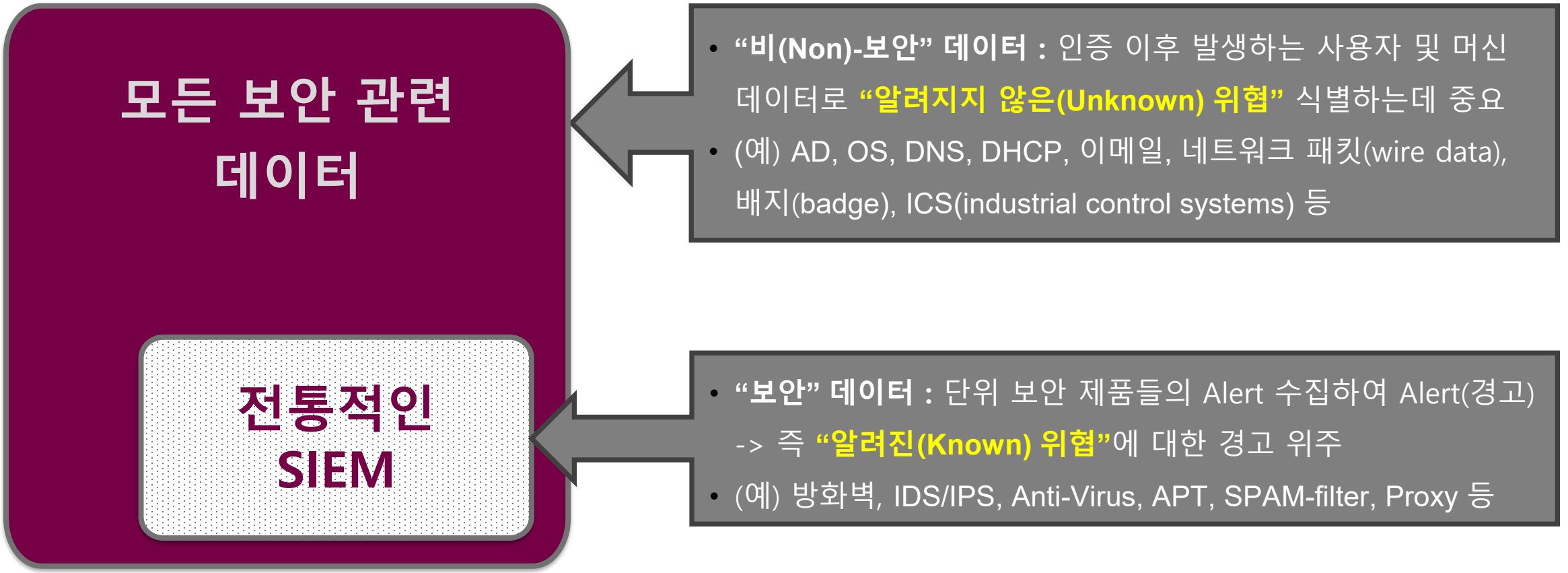
차세대 SOC 솔루션 도입 시 고려사항

분석 기반의 보안 운영을 통해 주요 보안 사용 사례(Use Cases) 해결



무엇을 모니터링(식별, 분석) 할 것인가?

모든 데이터가 보안과 관련됨 => 빅데이터 분석 플랫폼 필요



Splunk ES: Analytics-Driven(분석기반) SIEM

주요 기능

모니터링 | 탐지 | 조사 | 대응

프로세스

1 검토 (Review) → 2 위협 식별 (Determine) → 3 조사/결정 (Decide) → 4 실행 & 적용 (Act & Adapt)

필요 사항

인시던트 우선순위 지정

후속 조치 또는 조사해야 할 가장 중요한 사항 결정

적시에 조사

가능한 한 적은 인원으로 각 단계를 최대한 빠르게 수행

분석 및 대응

각 데이터 비트는 컨텍스트와 다른 모든 데이터와의 관계가 필요

Splunk ES: Analytics-Driven(분석기반) SIEM

주요 기능


모니터링


탐지


조사


대응

프로세스

1 검토 (Review) → 2 위협 식별 (Determine) → 3 조사/결정 (Decide) → 4 실행 & 적용 (Act & Adapt)

주요 기능

Splunk Enterprise Security™

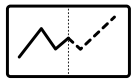
보안경고, 조사, 워크플로우 Notable Events	**이벤트 상관 관계 분석** Correlation Search	**보안 컨텍스트 강화** Asset, Identity, Others
위협 인텔리전스 Threat Info Management	**위험 기반 분석** Risk Scoring Framework	**기본 제공 보안 컨텐츠** Views / Reports / Rules

splunk> enterprise


Collect


Store


Ad hoc Search

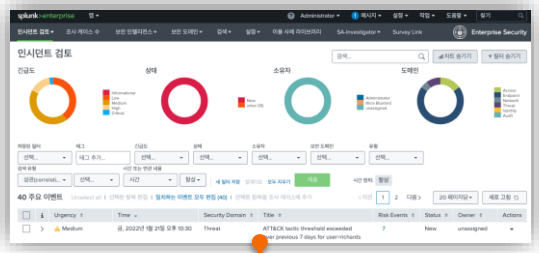

Analyze

Report

Splunk ES - 주요 기능 요약

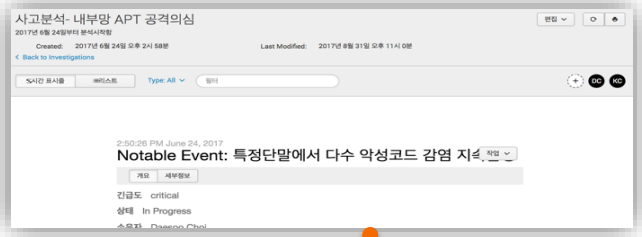
위협 탐지 및 분류

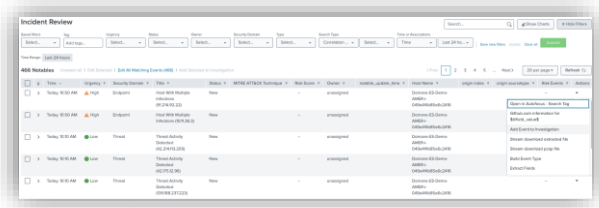
인시던트 검토 및 분석
긴급도에 따른 인시던트 분류(triage)



침해사고 조사케이스 등록

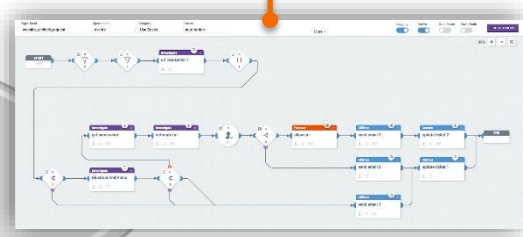
위협 인텔리전스 및 장기간 분석 필요한 조사 등록
핵심보안지표기반 심층분석이 필요한 항목 등록





즉각적 대응

단위보안솔루션에 조회, 차단,
블랙리스트 등록 등 대응 기능 수행
(Adaptive Response)

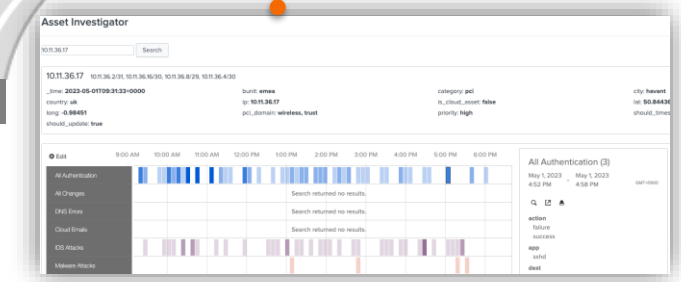


보안 업무 자동화(SOAR 필요)

워크플로우에 대한 플레이북 생성을
통한 반복적인 업무에 대한 보안 업무
자동화(Automation) 수행

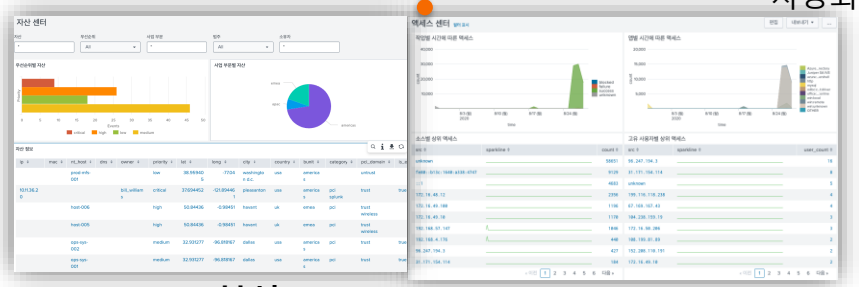
시작

보안관제센터의
보안 워크플로우



자산 위협 시각화

자산기반 위협 탐지
시간별 이상패턴 탐지



Deep-Dive 분석

조사 대상 (예, 랜섬웨어, 웹공격탐지 등) 보안 컨텐츠와
관련된 대시보드를 결합하여 심층분석 업무 수행

splunk> turn data into doing

인시던트 분류

인시던트의 빠른 분류(triage)는 보안관제운영(SIEM)의 첫 번째 프로세스

MEDICLINIC

UNDERSTANDING TRIAGE

분류(triage) 시스템은 **응급 센터**에서 **치료의 우선 순위**를 정하는 보편적으로 인정되고 객관적인 방법

환자가 응급 센터에 도착하면 어떻게 처리하나요?

숙련된 staff가 **환자**가 도착 시 긴급도를 **평가**

진료를 **기다릴 수 있는 사람**과 **기다릴 수 없는 사람**을 평가하기 위해 **분류 시스템**을 사용

임상적 긴급도에 **점수**와 해당 **색상**이 부여됨

RED	EMERGENCY	A **life-threatening** medical condition. Expect to **receive immediate attention**.
ORANGE	VERY URGENT	A **serious** medical condition. Expect attention **after red patients have been stabilised**.
YELLOW	URGENT	Expect attention **after red and orange patients have been stabilised**.
GREEN	ROUTINE	You **can function without immediate care** and will be attended to **as soon as possible**.

WHY ARE WE WAITING?

The triage system can be distressing, especially for parents with a sick child. But it's necessary in order to treat each patient fairly.

International standard of practice in emergency medicine

인시던트 분류

인시던트의 빠른 분류(triage)는 보안관제운영(SIEM)의 첫 번째 프로세스

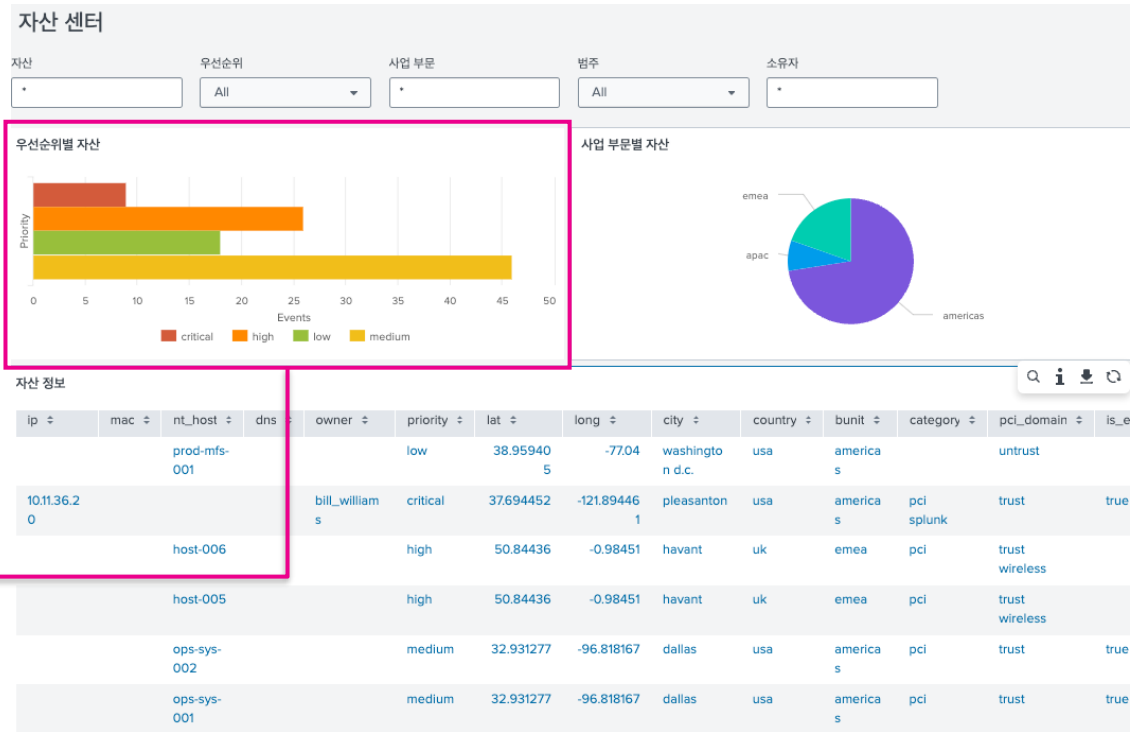
	Urgency	Time	Security Domain	Title	Risk Events
>	Medium	금, 2022년 1월 21일 오후 10:30	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	7
>	Low	금, 2020년 9월 25일 오후 6:58	Threat	Threat Activity Detected (31.171.154.114)	--
>	Critical	금, 2020년 8월 28일 오전 2:00	Access	Geographically Improbable Access Detected For richards	--

Corelation Search의 탐지로 발생되는 인시던트의 빠른 분류(triage)를 위한 긴급도가 반드시 필요

긴급도: 인시던트 이벤트의 우선 순위를 정하기 위함
긴급도 = 자산 우선순위 + 이벤트 심각도

자산 우선순위 / 이벤트 심각도

자산 우선순위 \ 이벤트 심각도	Informational	Unknown	Low	Medium	High	Critical
Unknown	Informational	Low	Low	Low	Medium	High
Low	Informational	Low	Low	Low	Medium	High
Medium	Informational	Low	Low	Medium	High	Critical
High	Informational	Medium	Medium	Medium	High	Critical
Critical	Informational	Medium	Medium	High	Critical	Critical

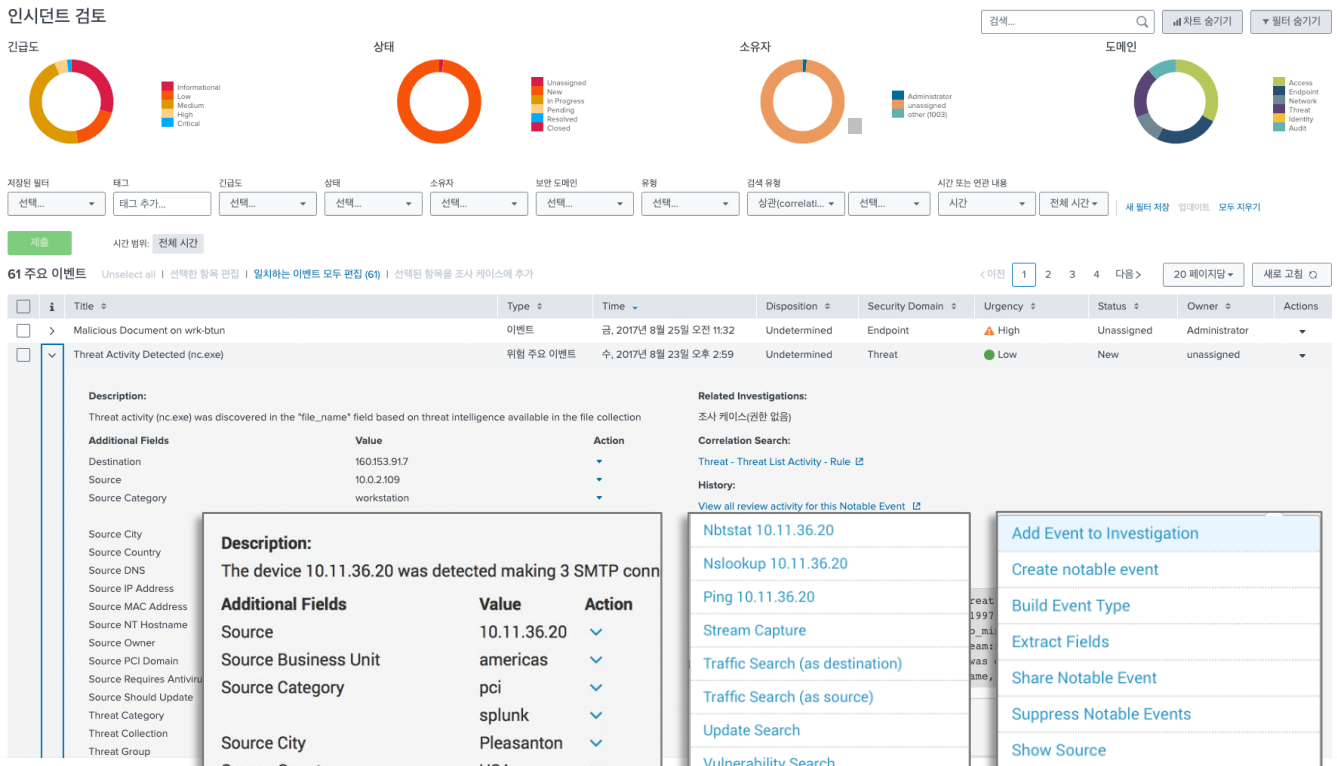


우선순위: 자산에 대해서 보안 담당자가 설정
심각도: 상관 검색 룰에서 설정

인시던트 검토

- **인시던트 관리 프로세스 간소화**
  - 통합 인시던트 관리를 통해 보안 인시던트의 효과적인 라이프사이클 관리가 가능
- **신속한 의사결정 지원**
  - 신속한 인시던트 검증을 위해 모든 보안 컨텍스트를 자동으로 매핑하고 사전 정의된 분석 경로를 제공
- **보안 관리 프로세스 개선**
  - 복잡한 프로세스 통합 요구사항을 지원하기 위한 조사 관리 및 분석/대응 지원

인시던트 검토:
통합 인시던트 관리



인시던트 상세 설명:
보안 컨텍스트 자동 매핑

인시던트 워크플로 액션: 조사 관리 및 분석/대응 지원

splunk> turn data into doing

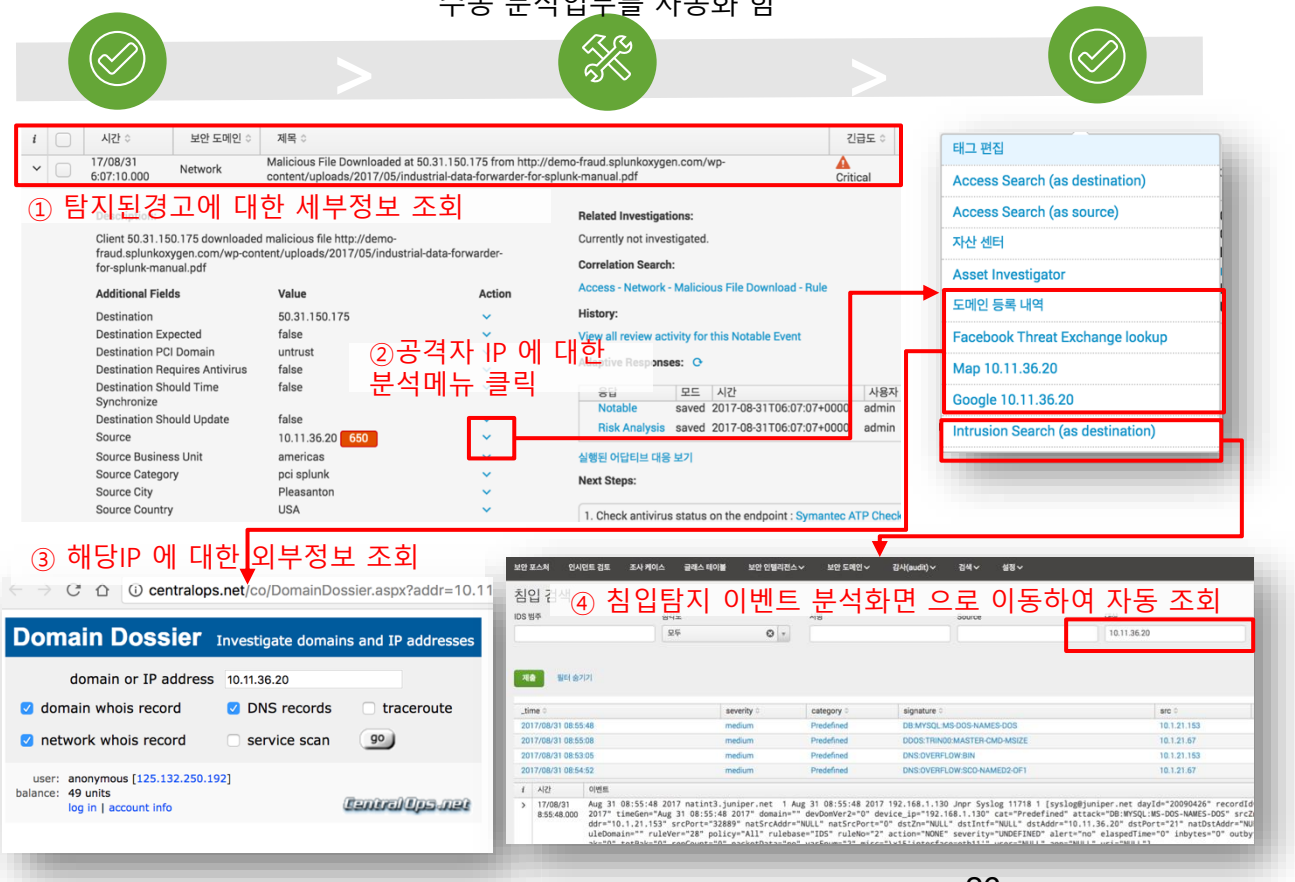
인시던트 상세 분석 기능

Splunk의 대시보드와 정보 조회를 위한 Workflow Action 기능을 활용하고 Splunk ES의 다양한 위협 분석 대시보드를 활용하여 빠르게 분석업무를 수행할 수 있는 기반을 제공

위협탐지
(예시)IDS 유형

공격정보 분석 (외부 연계)
도메인/IP 정보, 위협인텔리전스 정보
수동 분석업무를 자동화 함

인텔리전스 기반 분석
자동반복 패턴 등 분석



기능개요

- 공격징후를 탐지한 이후 근본원인을 찾기 위해 연관이 높은 데이터까지 빠르게 찾아갈수 있는 기능 구성
  - Drill-Down, Workflow Action

효과

- 상관분석에 의한 공격징후 탐지 이후, 근본원인 파악을 빠르게 클릭으로 드릴다운하여 찾아갈수 있도록 구성 제공

기타

- 데이터에 대한 CIM 매핑확인

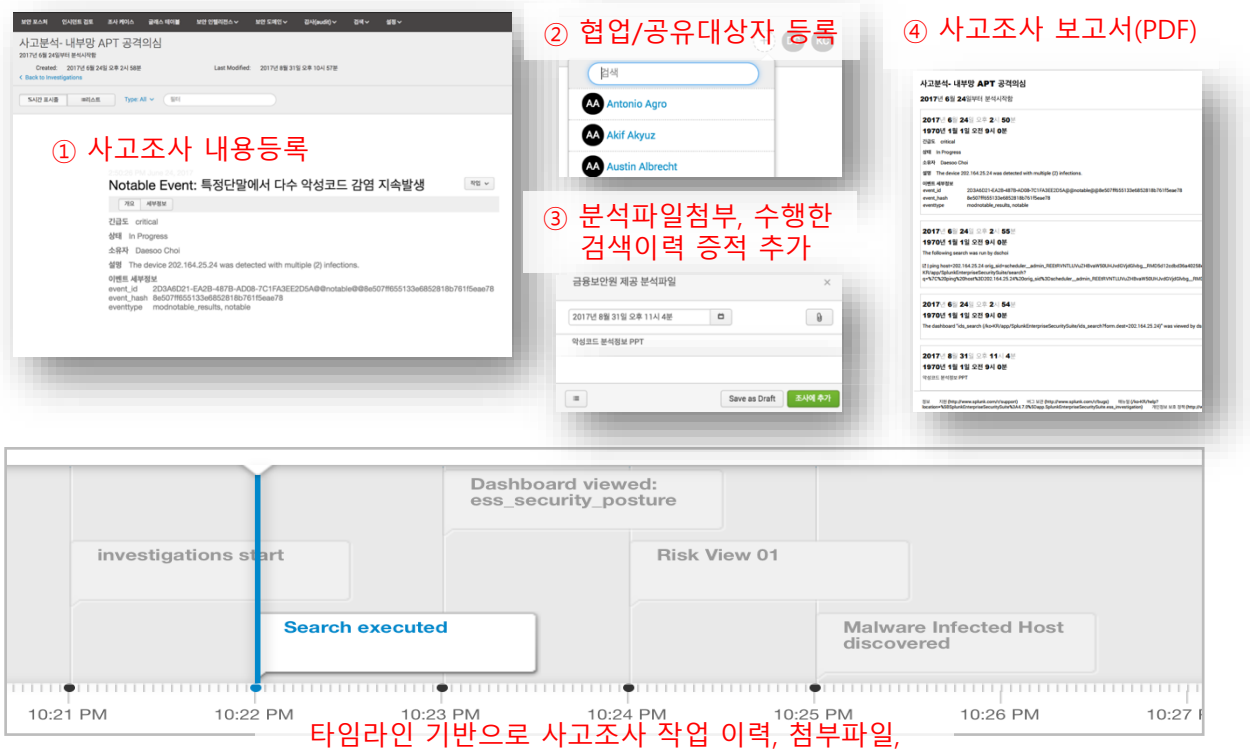
조사 케이스(Investigation) 관리

조사 케이스 관리 기능은 일련의 사고조사 및 분석업무를 쉽게 관리하고 추적할 수 있는 기능으로 보안분석가들 간의 공유와 협업으로 분석 업무 효율성을 높임

상관경고 탐지/ 첨보내용 등록

대응 작업/협업 수행
타임라인 기반 조사 이력관리
고급분석 관리 간소화

보고서 생성



타임라인 기반으로 사고조사 작업 이력, 첨부파일, 주석 등 추적관리 용이

기능 개요

- 사고조사 활동을 타임라인 기반으로 관리하여 고급위협 조사 프로세스 간소화함
- 예, 금융권 사고 첩보 발생시, 사고정보 등록후 은행내 조사 수행, 추적,협업 관리

효과

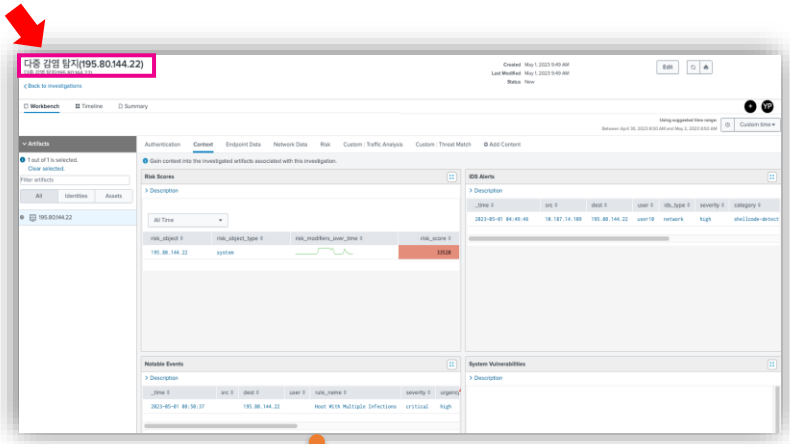
- 타임라인 기반으로 사고조사에 대한 작업, 주석기록 등 체계화로 공격 세부사항에 대한 이해 강화 와 타임라인 시각화 전달
- 고급 위협조사에 대한 분석을 간소화 하고 협업 기능 제공

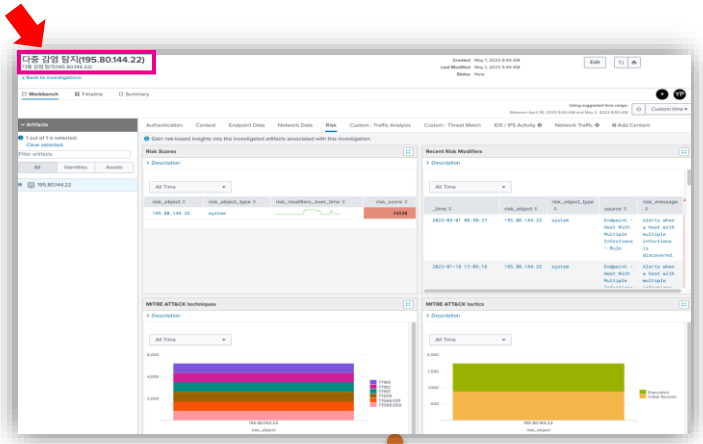
기타

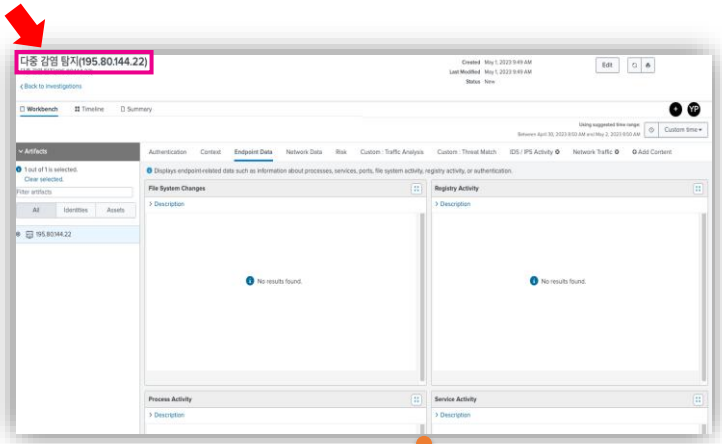
- 사용자에게 Investigation Read/Write 권한부여

자산 위협 시각화

IP 자산을 이용하여 여러 위협에 대해서 신속한 탐지 및 보안 가시성 제공







Investigation Workbench (다중 감염 탐지 – 자산: 195.80.144.22)

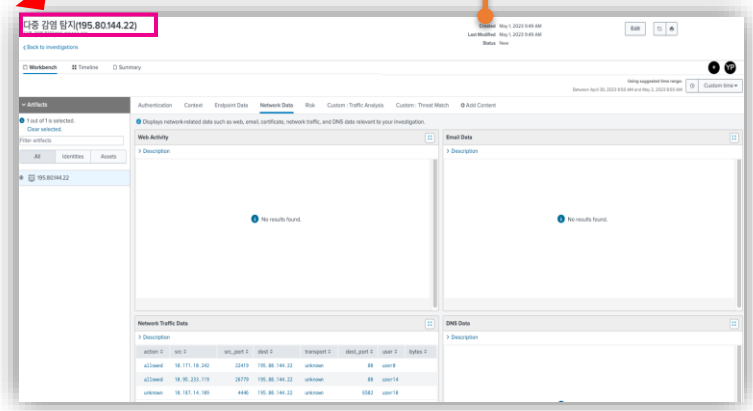
컨텍스트

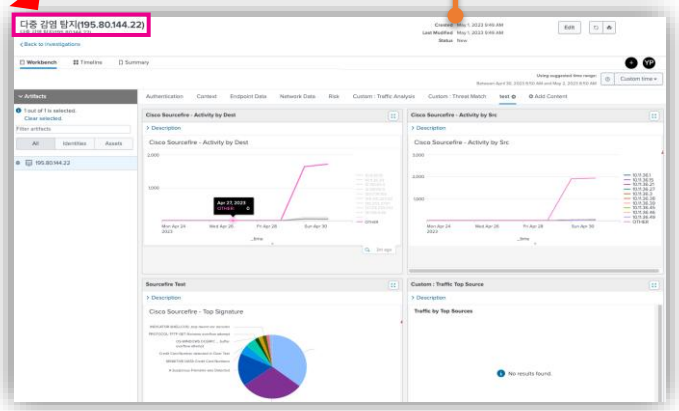
네트워크 데이터

위험

IDS/IPS 액티비티

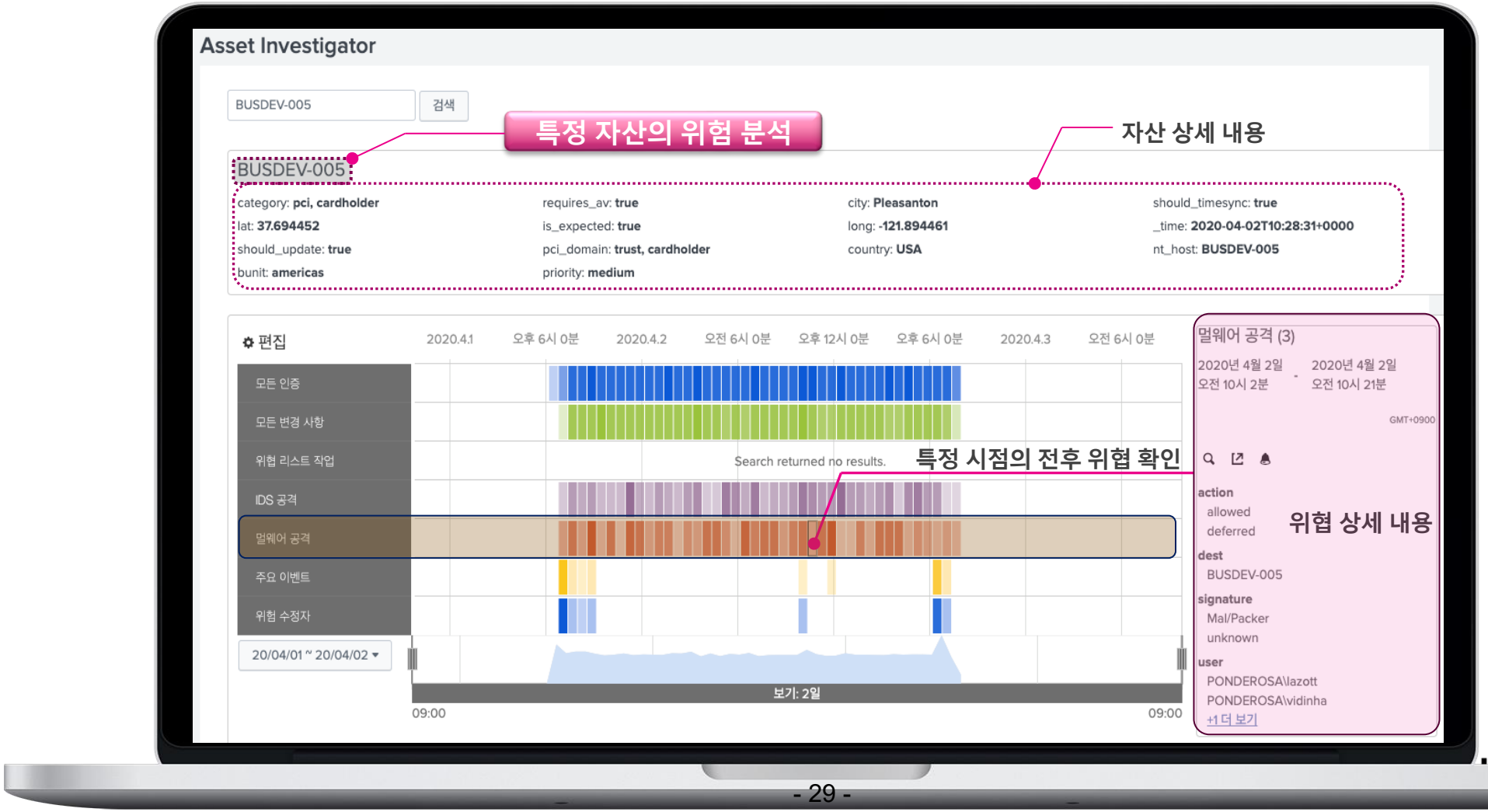
엔드포인트 액티비티





보안 인텔리전스(사용자 인텔리전스->Asset Investigator)

자산에 대해서 보안 이상징후를 시각적인 방법으로 요소간의 관계를 파악할 수 있습니다. 보안 이상징후를 시각적으로 정돈하여 파악이 수월합니다. **인증, 위협 활동, IDS 공격, 멀웨어 공격**, **이상행위 관련 주요 이벤트 추이**를 확인할 수 있습니다.

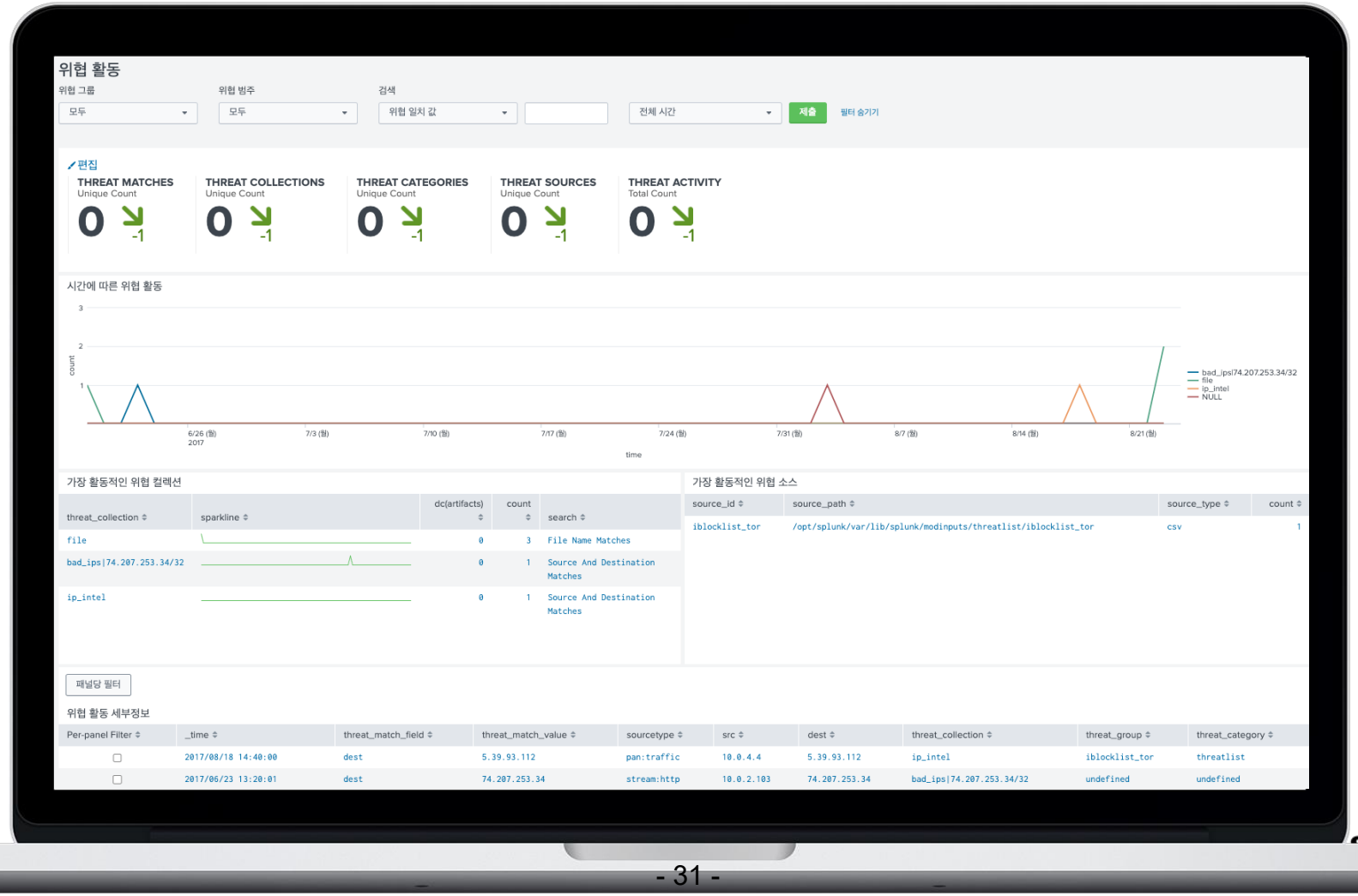


보안 인텔리전스(프로토콜 인텔리전스->프로토콜 센터)

네트워크 패킷 데이터를 이용해서 프로토콜과 사용자 프로파일링을 쉽게 할 수 있습니다. 여기서 제공되는 화면은 보편적인 프로토콜에 포함된 중요한 속성들은 표시할 수 있습니다. 네트워크 패킷 데이터는 전반적인 보안 현황과 위협 및 위반 사항을 조사하는데 핵심 요소입니다.

보안 인텔리전스(위협 인텔리전스->위협 활동)

위협 인텔리전스 소스 컨텐츠(SRC IP, DST IP, Email Address, File Hash, File Name, Process 등)와 일치하는 위협 활동 정보를 제공합니다.



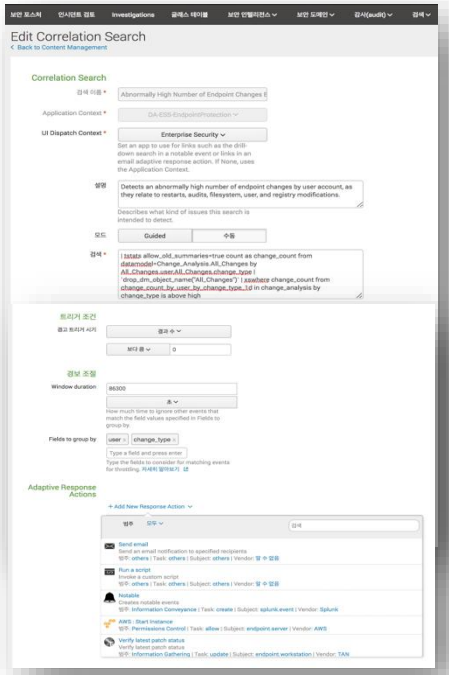
어댑티브 대응(Adaptive Response)

탐지 룰 설정 시 사전에 지정된 대응프로세스에 따라 시스템적으로 자동 알람/차단/격리 조치 기능

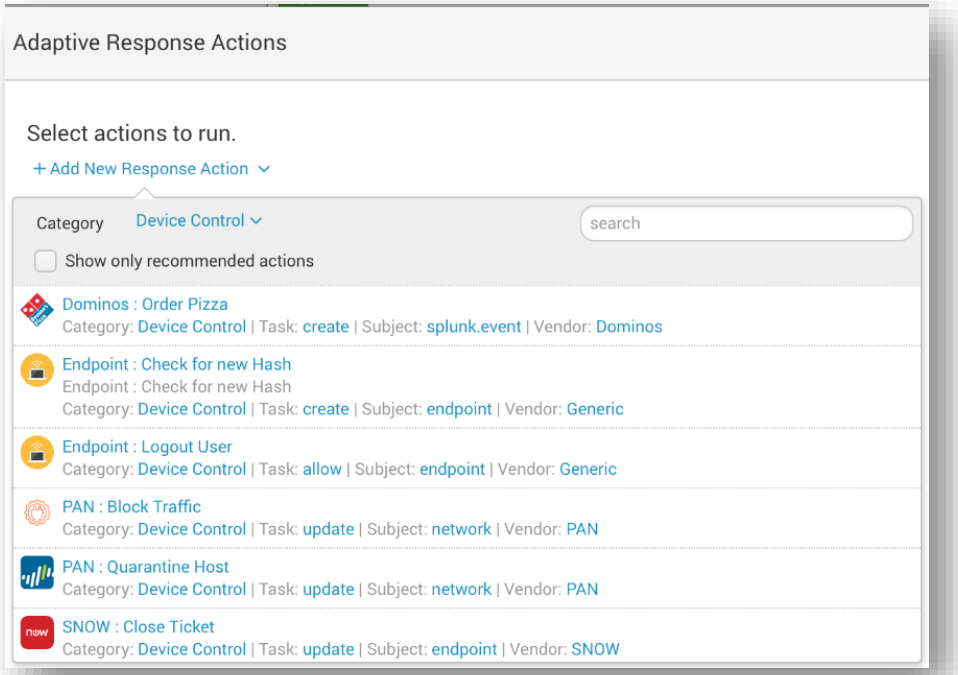
적응형 응답(Adaptive Response)기능을 제공하여 탐지 룰에 의해 경고 발생시, 문자, 이메일 등 알림을 보내거나, 보안장비에 대하여 차단 정책을 반영하는 등의 대응 조치 기능을 제공합니다.

❏ 상관경고 설정에서 적응형 대응(Adaptive Response) 메뉴에서 대응할 설정을 입력합니다.
Nbtstat, Ping, Nslookup 등의 조회 / Email 로경고 발송, Webhook, 등 Notice 기능을 제공합니다.

❏ 상관분석 룰 설정



❏ 자동 대응 항목 설정



어댑티브 대응(Adaptive Response) 활용

상관분석 룰에 의한 위협탐지 이후 신속하고 체계화된 대응을 위하여, 운영자가 단위 보안시스템에 직접 접속하지 않고, ES 에서 직접 연계된 보안시스템에 대응 업무를 수행함 (예, IPS 장비에 블랙리스트 등록)

기능 개요

- 상관경고 룰에 탐지된 이벤트에 대하여 대응 업무를 수행을 중앙에서 수행하고, 필요시 자동화 하고 수행결과를 확인 함

효과

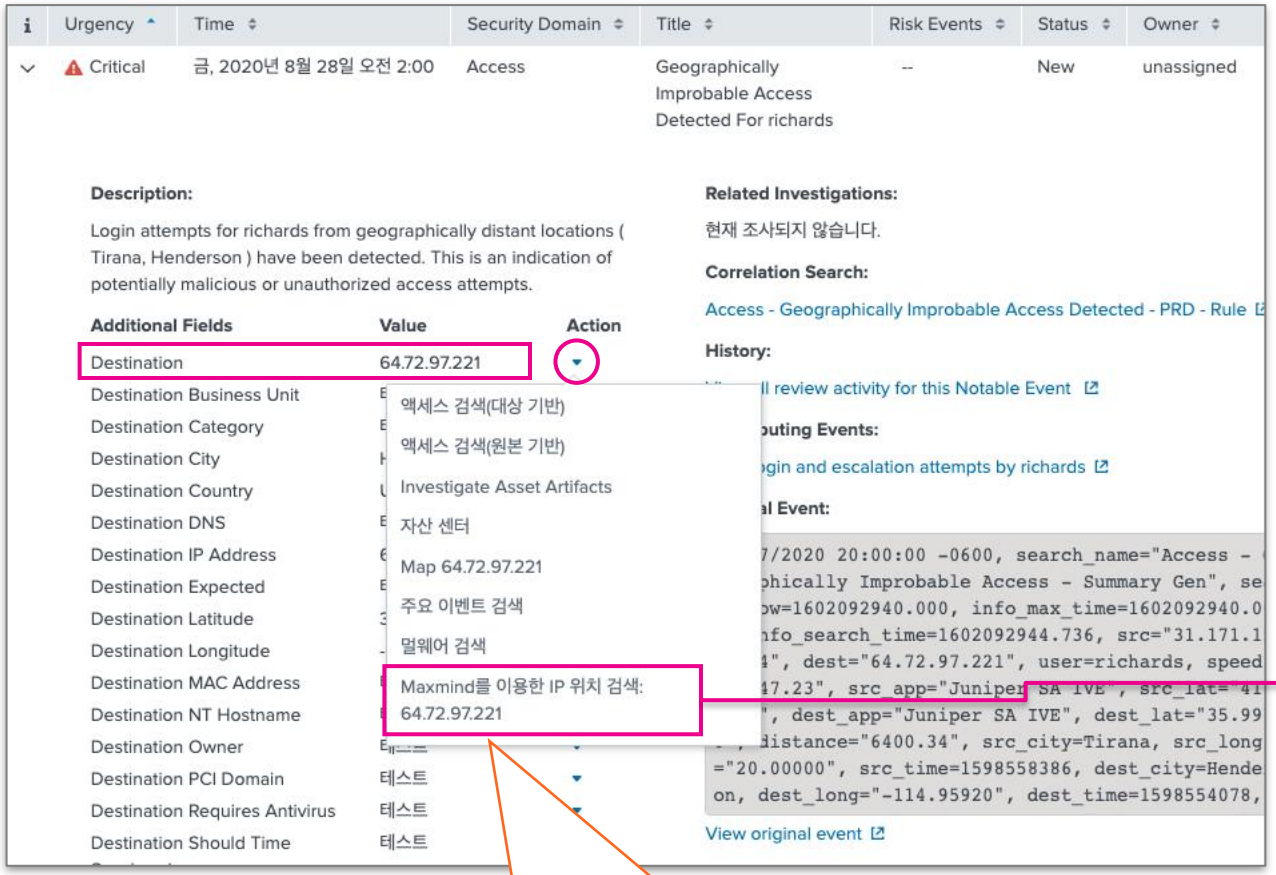
- 보안관제 업무에서 대응작업을 중앙에서 자동화하여 대응 업무시간 단축 (검색, 공유업무 포함)
- 자동화되고 사전 정의된 워크플로우 기반으로 운영 효율성 향상

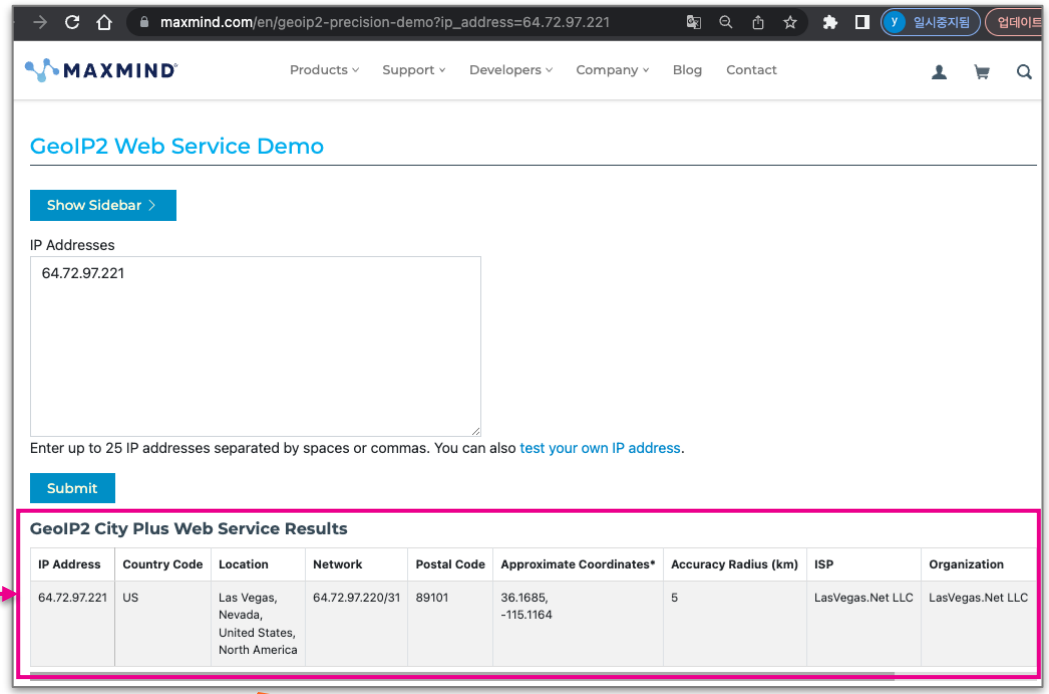
기타

- 대상 솔루션 벤더와 사전 연동 작업 필요
  ※ Adaptive Response Partner 사는 add-on 설치로 즉시 사용가능

OSINT(외부평판조회) 활용

OSINT(Open Source Intelligence)란? 언론미디어, 구글검색, 블로그/SNS 등 누구에게나 공개된 정보



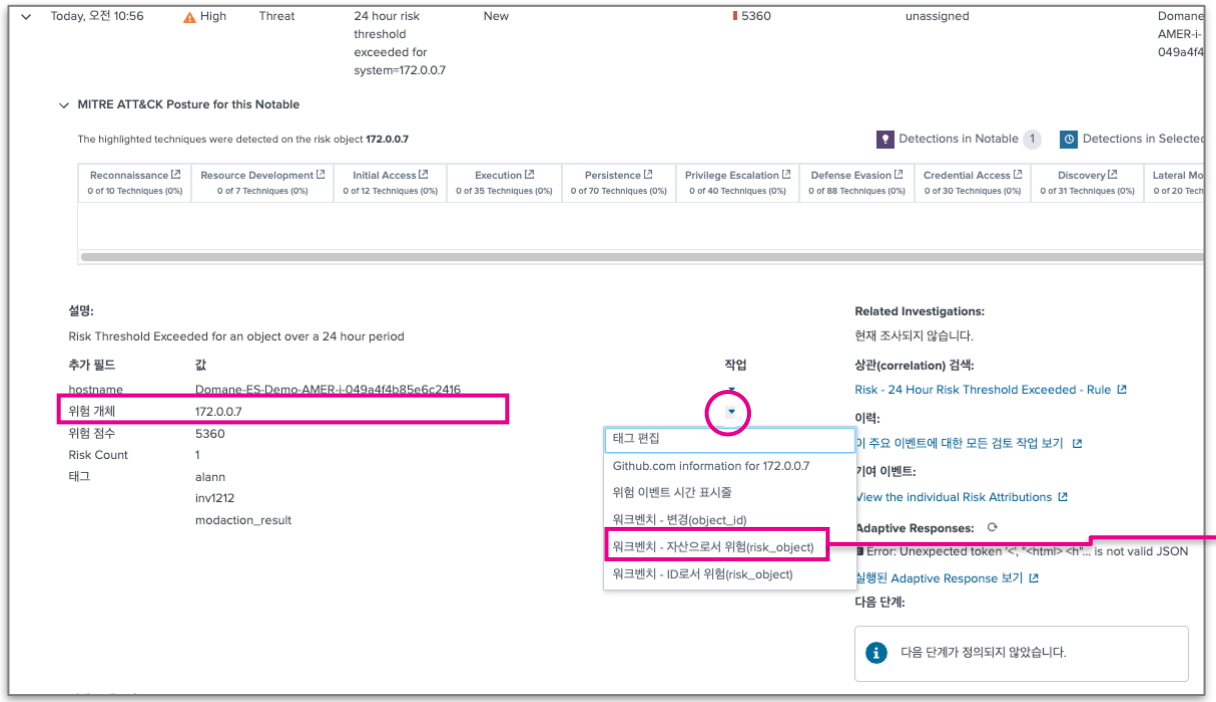


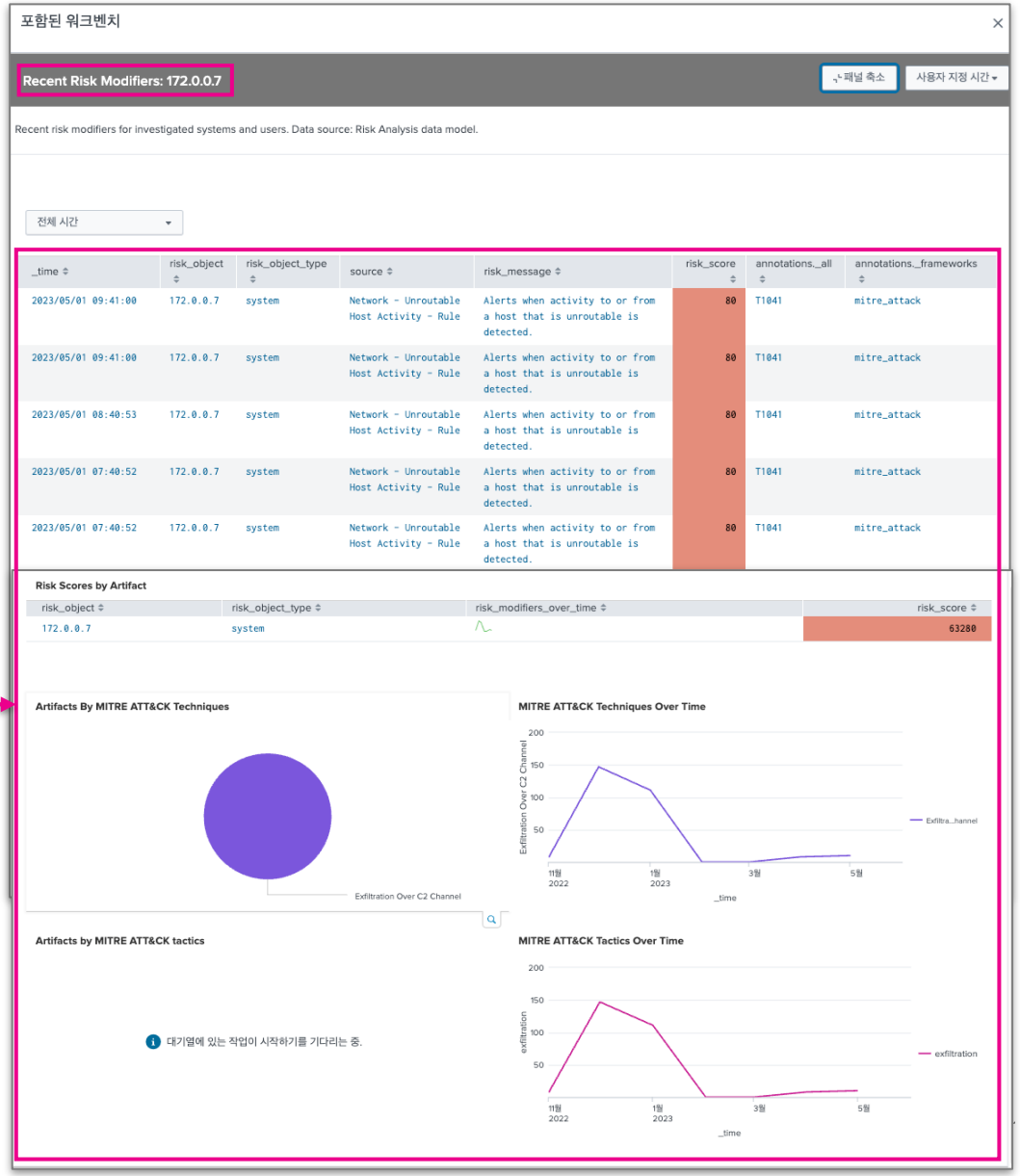
외부 자산에 대해서 OSINT를 활용하여 신속하게 평판 서비스 이용

인시던트의 유효성, 범위 및 심각도를 결정하는데 도움이 되는 자산 정보 필드값에 워크플로우 액션 기능을 이용하여 OSINT를 활용

위험 점수 활용

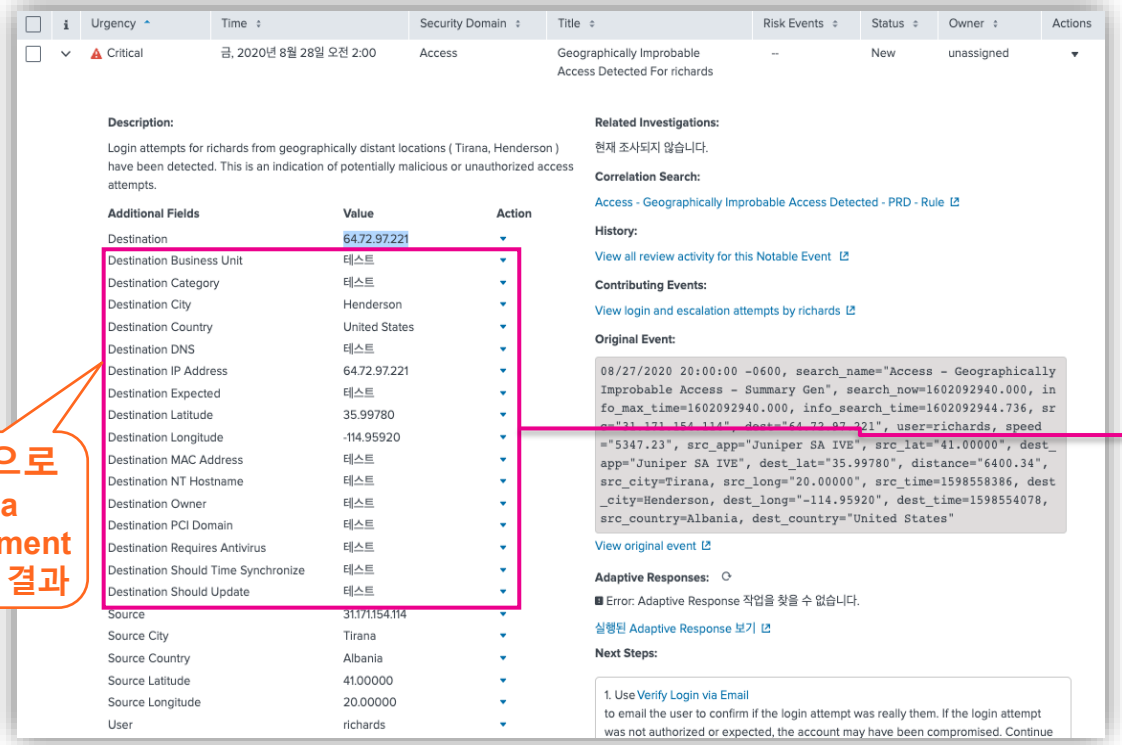
자산 별 위험 점수(risk score) 활용하여 위험기반 탐지 가능





보안 인시던트의 데이터 강화

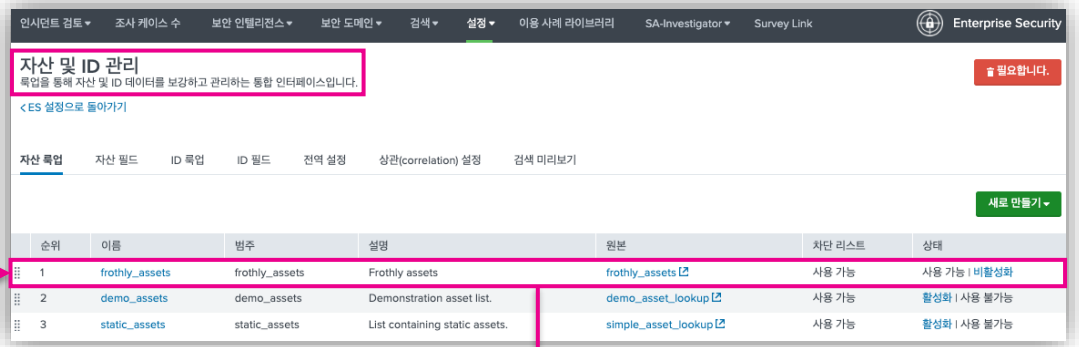
Original event에 자동으로 자산/ID 정보를 추가할 수 있는 data enrichment 기능 제공

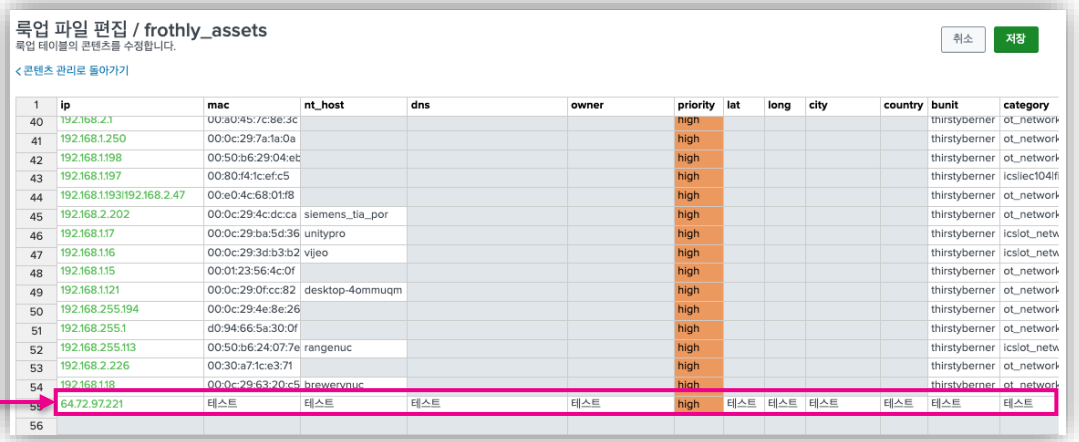


자동으로 data enrichment 수행된 결과

자산 관리 프레임워크

새 자산을 추가하거나 기존 값을 변경 가능
자산 상태를 비활성화하거나 활성화 가능
자산 우선순위 설정 가능





인시던트 리뷰 – 추가 필드(Additional Fields)

Original Event에 있는 Destination(목적지 IP주소)를 바탕으로 자산/ID 프레임워크에서 자동으로 자산 룩업을 통해 추가 필드에 관련된 ip, mac, nt_host, dns, owner, priority, lat, long, city, country, bunit, category, pci_domain, is_expected, should_timesync, should_update, requires_av, cim_entity_zone 정보들을 추가로 출력해줘 이벤트를 강화 가능

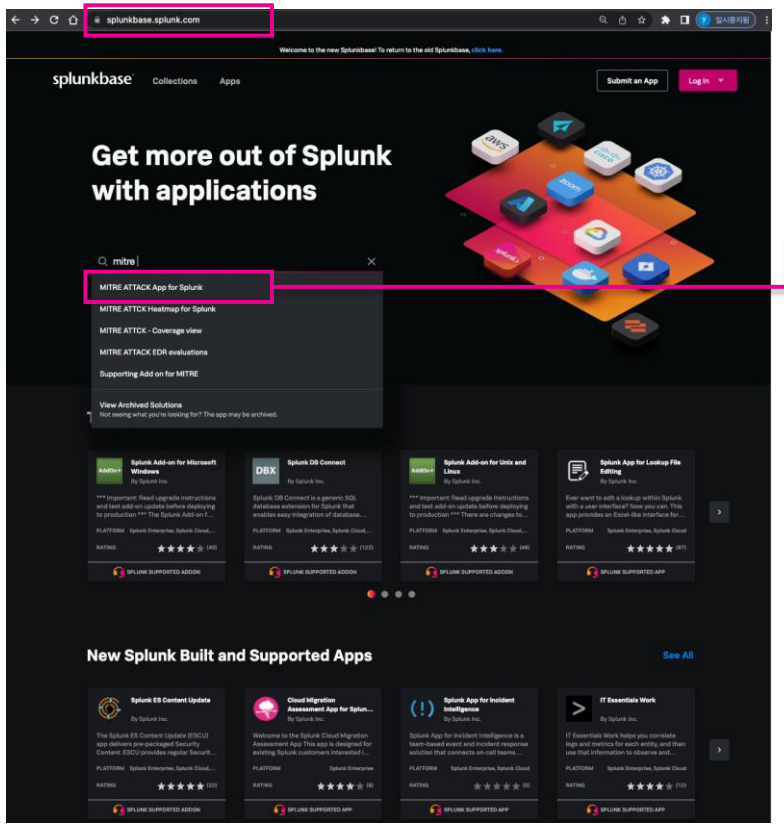
자산 KV Store

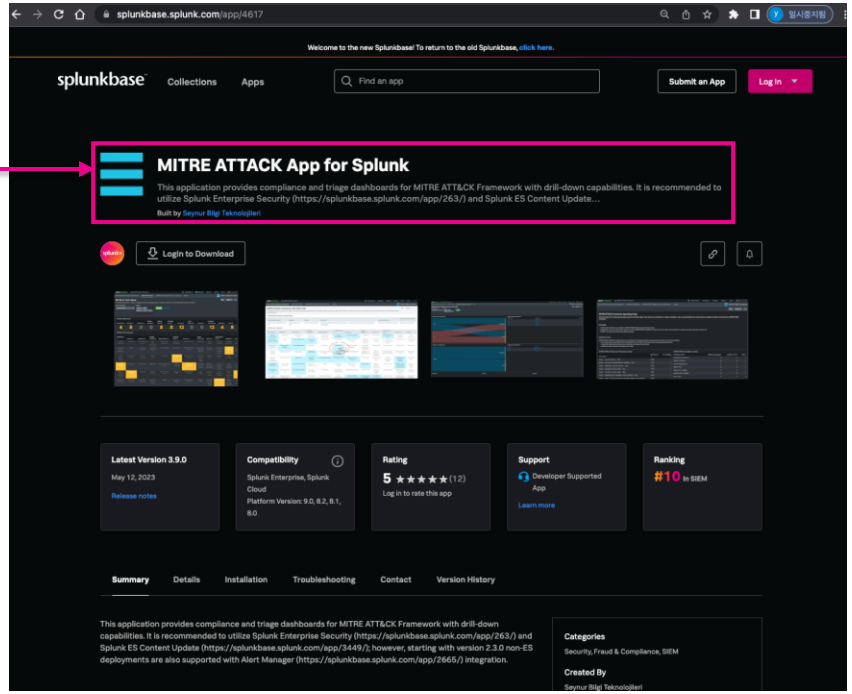
KV Store 에 저장된 자산은 언제라도 수동/자동으로 변경 가능 함

Splunk 차별점1 – 앱 마켓플레이스(Splunkbase)

https://splunkbase.splunk.com/

- 2500+ App / Add-on
- 특정 use case 와 technologies 를 위한 빌트인 검색, 리포트, 시각화, integration
- 앱 다운로드 후 요구사항에 따라 커스터마이징 가능
- 데이터를 활용한 신속한 time to value
- 나만의 앱 개발 및 다른 사용자와 공유

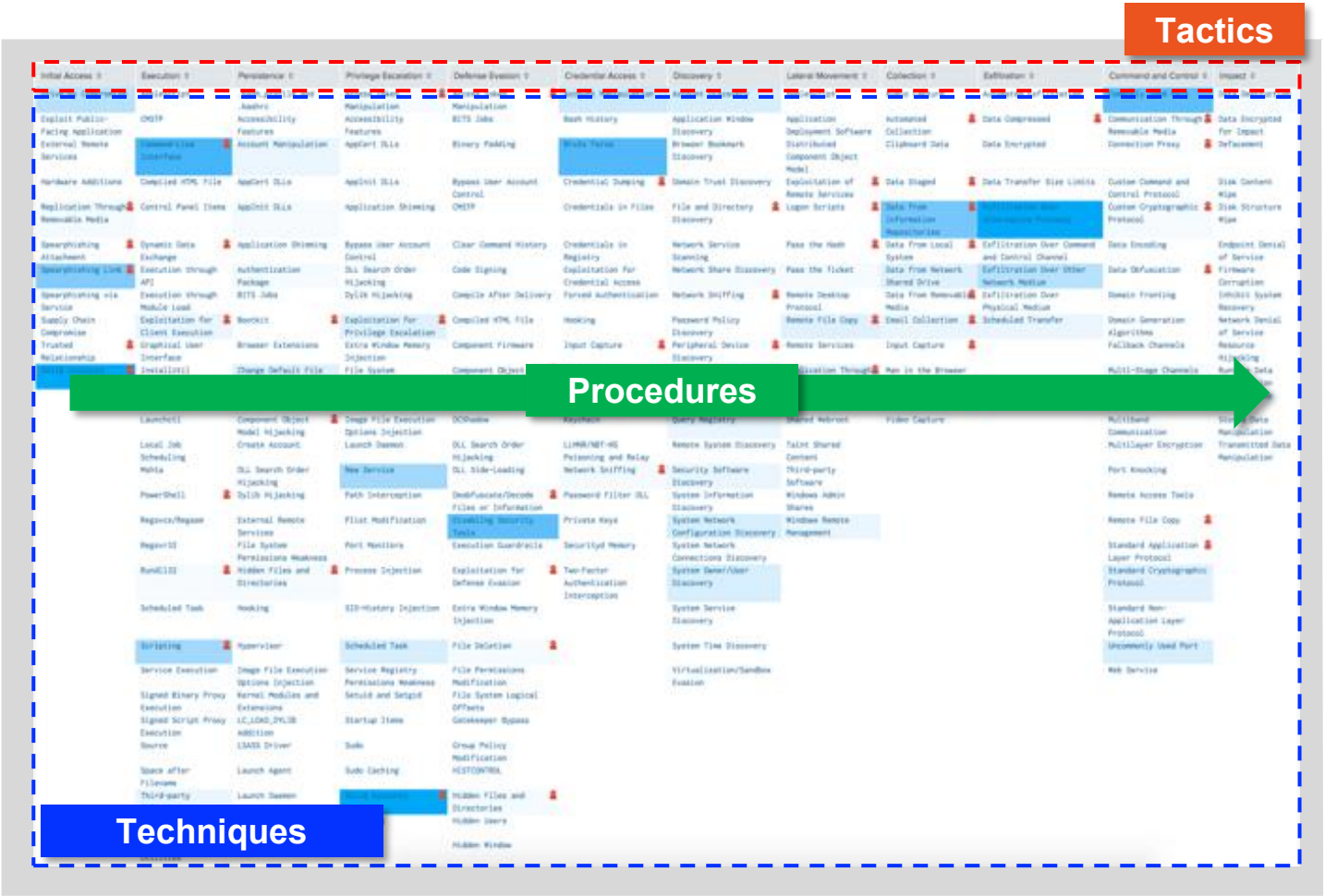




Splunk 차별점2 - MITRE ATT&CK(1/2)

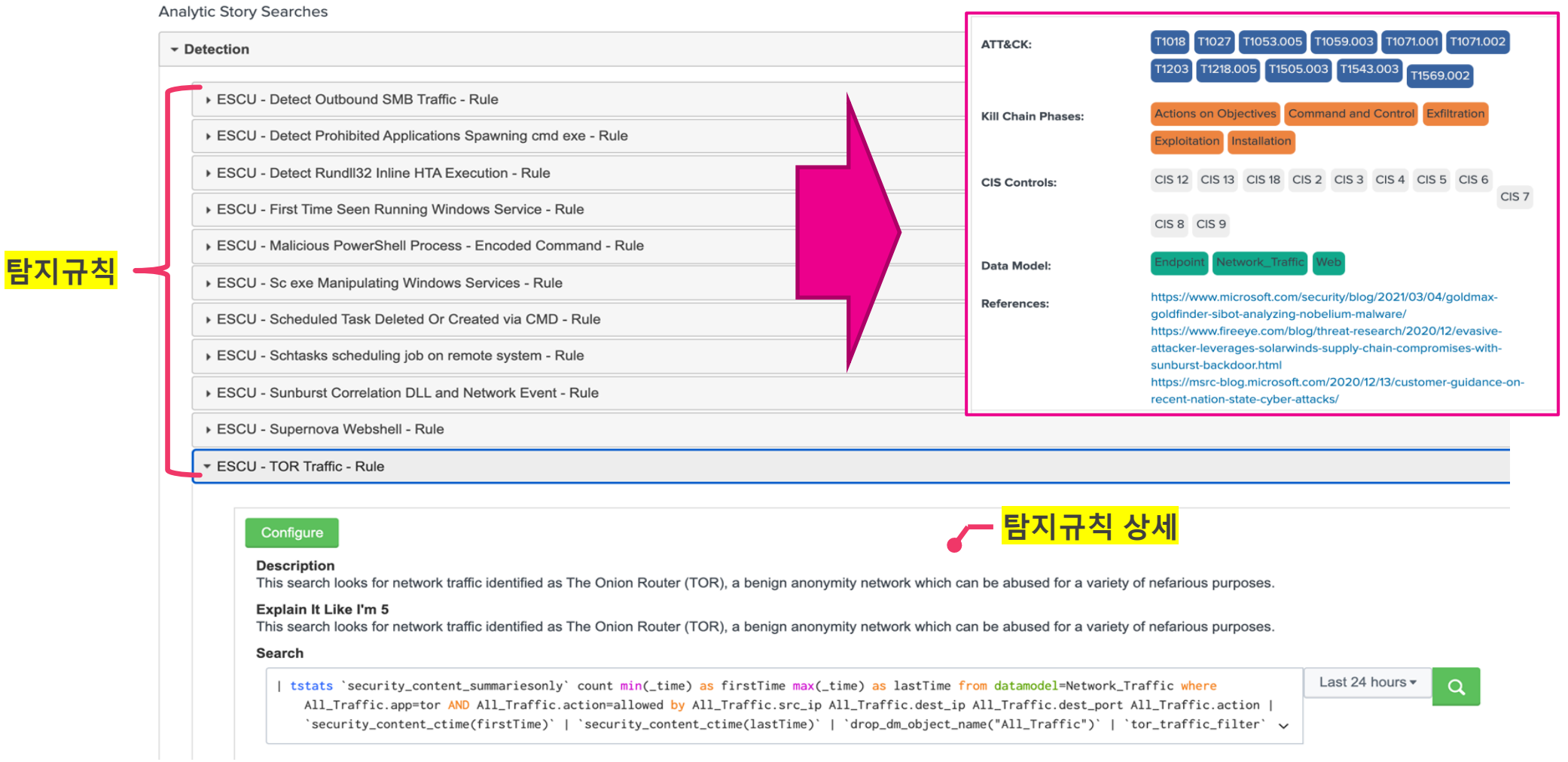
선진화된 보안 프레임워크(MITRE ATT&CK) 기반으로 보안 위협 식별(콘텐츠 제공)

- ATT&CK은 Adversarial Tactics, Techniques and Common Knowledge의 약어
- 사이버 공격자가 침투 이전 또는 이후 활동에 대한 사례 분석을 통해 공격자의 공격 전술(tactics, 단기적 목적), 침투기술(techniques, 전술을 달성하기 위한 방법), 침투기술을 실제 공격 그룹(예, APT5)이 침투 기술을 활용하는 절차(Procedure)를 프레임워크로 제안



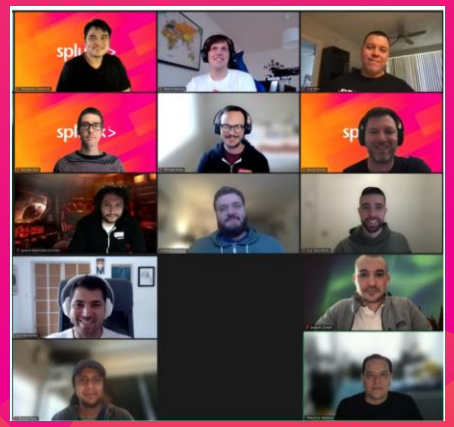
Splunk 차별점3 – 보안 콘텐츠 업데이트 지원

Splunk ES Content Update(ESCU) 앱을 통해 제조사 보안연구소에서 생성한 보안 콘텐츠를 제공



Splunk 차별점4 - 2개의 보안 연구 조직

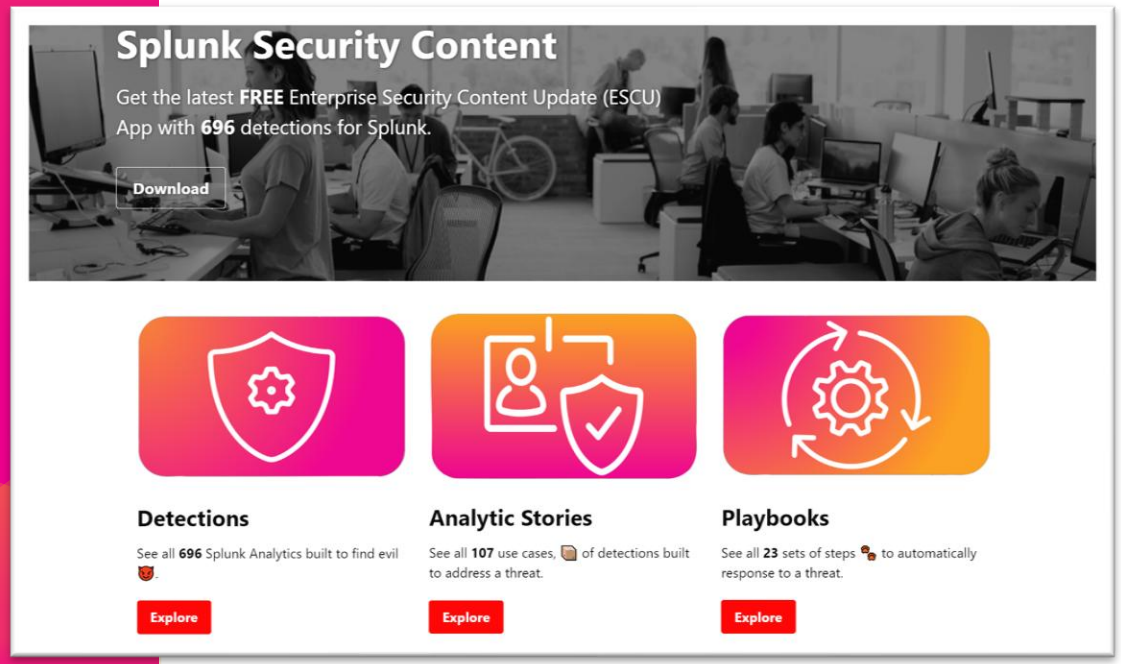
STRT
(Splunk Threat Research Team)



SURGe by Splunk

고객이 새로운(최신) 위협을 발견, 조사 및 대응할 수 있도록 지원하는
전문가 분석 및 인사이트를 제공하는 Security Research Team

Sign up for alerts: splunk.com/surge



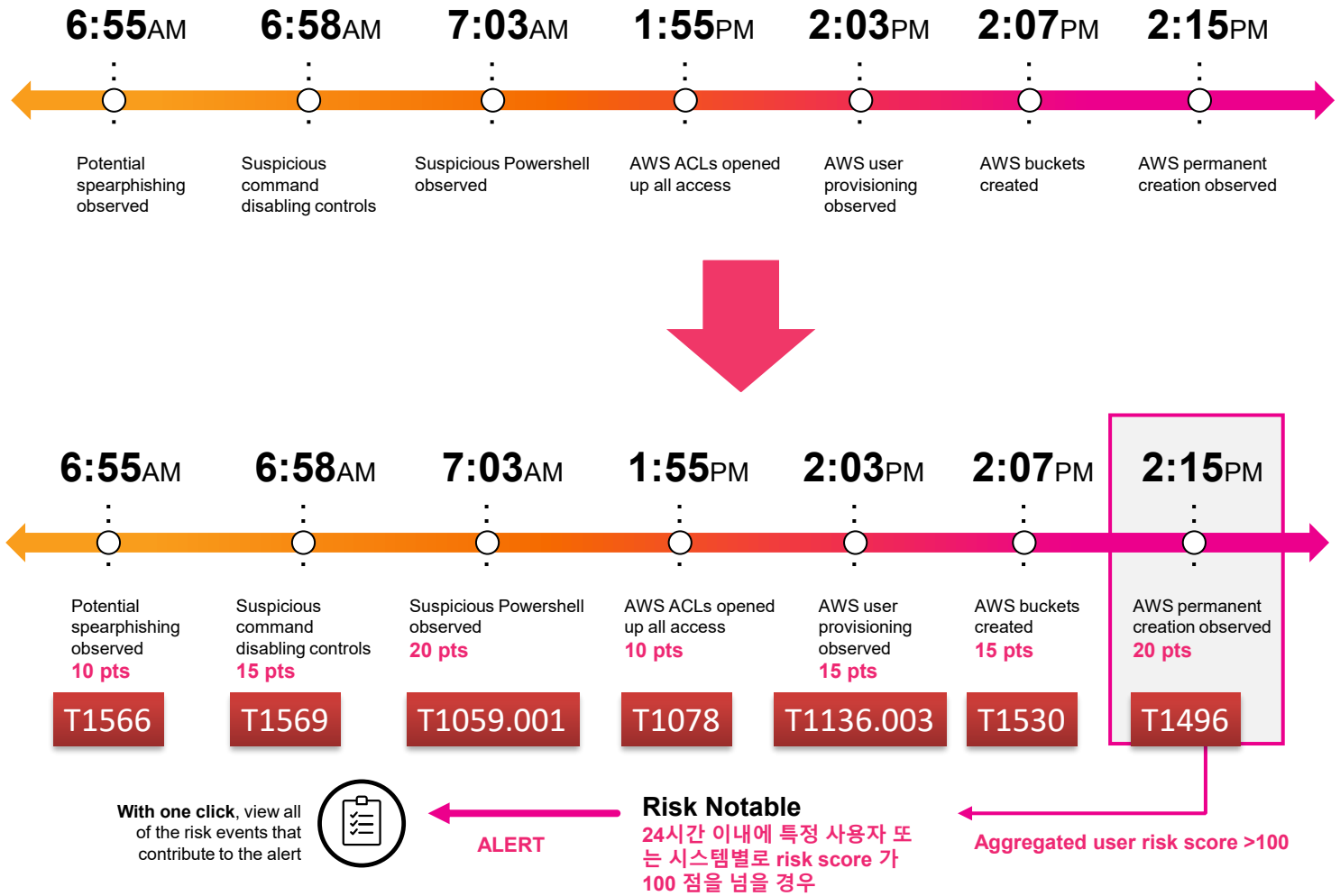
https://research.splunk.com/

https://github.com/splunk/security_content

splunk> turn data into doing

Splunk 차별점5 - RBA(Risk Based Alerting)(1/2)

- 각 event 별 risk index 를 지정 하고 특정 임계치의 합을 초과 하는 행위를 빠르게 식별
- 여러 event 를 묶어 하나의 context 로 제시



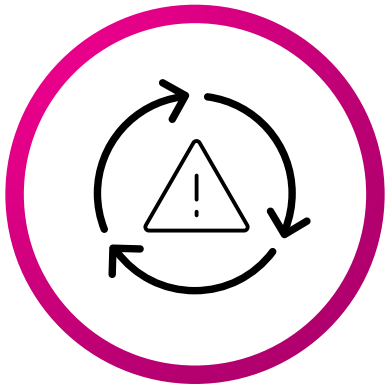
Splunk 차별점5 - RBA(Risk Based Alerting)(1/2)

- 각 event 별 risk index 를 지정 하고 특정 임계치의 합을 초과 하는 행위를 빠르게 식별
- 여러 event 를 묶어 하나의 context 로 제시

Splunk 차별점5 - RBA(Risk Based Alerting)(2/2)

RBA는 처음에경고 볼륨을 빠르게 감소시키며, 궁극적으로 전체 SOC 운영 효율화

경고 감소



- 경고 볼륨을 최대 80%까지 축소

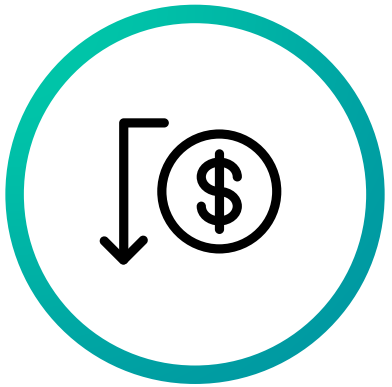
탐지 향상

- 오탐(false positives)을 최대 30%까지 축소

조사 시간 감소

- 원하는 시간 및 날짜에 대해서 조사 수행

SOC 운영 효율화



Splunk 차별점6 - 커스텀 ML 구현(1/2)

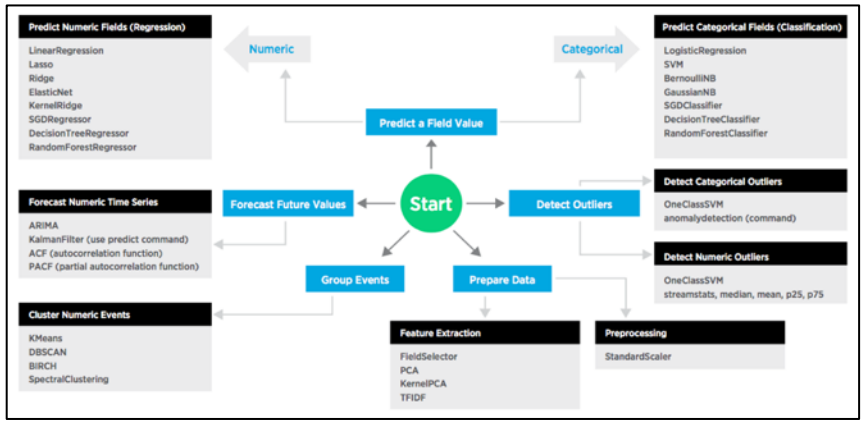
MLTK(Machine Learning Toolkit) 앱을 통해, 위협 및 이상행위 탐지를 위한 머신러닝 모델 생성 및 검증/운영을 손쉽게 구현하기 위한 다양한 기능을 제공하여, 단순 메트릭 이상치 검출 뿐 아니라 다양한 예측 모델을 적용하여 보안 사고 방지에 활용

항목	내용
기본 ML 알고리즘 탑재 + 오픈소스 라이브러리 활용	• 30+ 기본 알고리즘 모델 탑재 • 지도학습: Logistic & Linear Regr., SVM, Random Forest 등 • 비지도학습: K-means, DBSCAN, Spectral Clustering 등 • API 제공으로 SciPy의 300+ 오픈소스 라이브러리 탑재 가능
머신러닝 쇼케이스 & 어시스턴트	• 44개 보안, IT등 머신러닝 적용분야에 대한 예시 제공으로 고객 데이터셋을 가지고 빠르고 쉽게 ML적용 후 검증 가능
모델링 지원	• 알고리즘 선택 옵션 설정, fit 설정 후 가이드 모델 구축, 유효성 검사 및 시각화, 모델 정확도 검증 기능 탑재로 ML모델링 고도화 지원
다양한 보안 고객의 머신러닝 적용 사례	• 전세계 고객이 사용 중 • 검증된 유즈케이스 및 고객 레퍼런스 확보로 적용 위험성 최소화

다양한 ML 예제 어시스턴트

보안 예제

- Predict VPN Usage
- Predict the Presence of Malware
- Detect Outliers in Number of Logins
- Detect Outliers in Bitcoin Transactions
- Forecast the Number of Employee Logins



30+ 다양한 알고리즘 기본 탑재

Splunk 차별점6 - 커스텀 ML 구현(2/2)

앱 에코시스템

MLTK

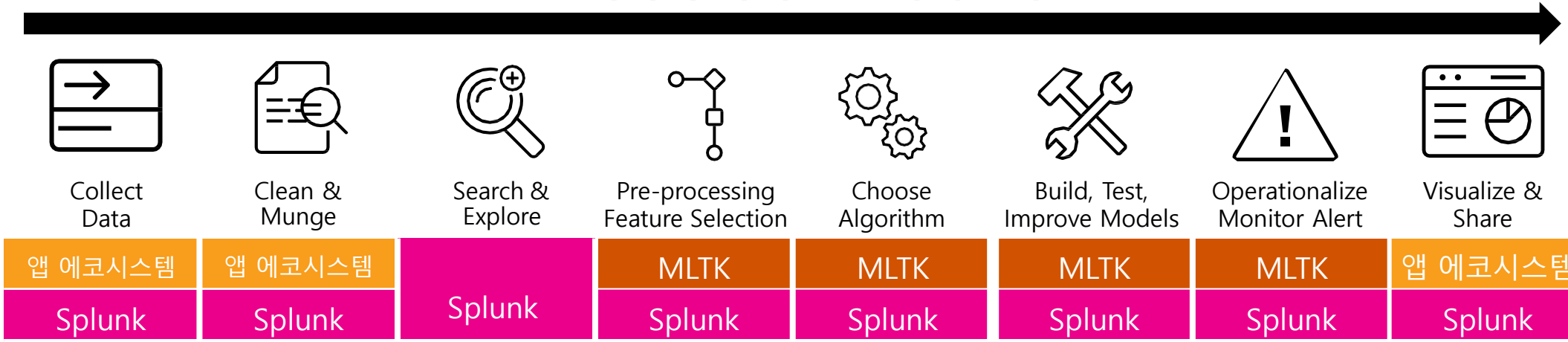
Splunk

Splunk의 App Ecosystem에는 데이터를 가져오고, 구조를 적용하며 ,데이터를 시각화하여, 가치 창출 시간을 단축 할 수있는 1000 가지의 무료 애드온이 포함되어 있습니다.

Machine Learning Toolkit은 다양한 ML 개념을 탐색하기위한 새로운 SPL 명령, 커스텀 시각화, 어시스턴스 및 예제를 제공합니다.

Splunk Enterprise는 머신 데이터의 인덱스 생성, 검색, 분석, 경고 및 시각화를 위한 미션 크리티컬 플랫폼입니다.

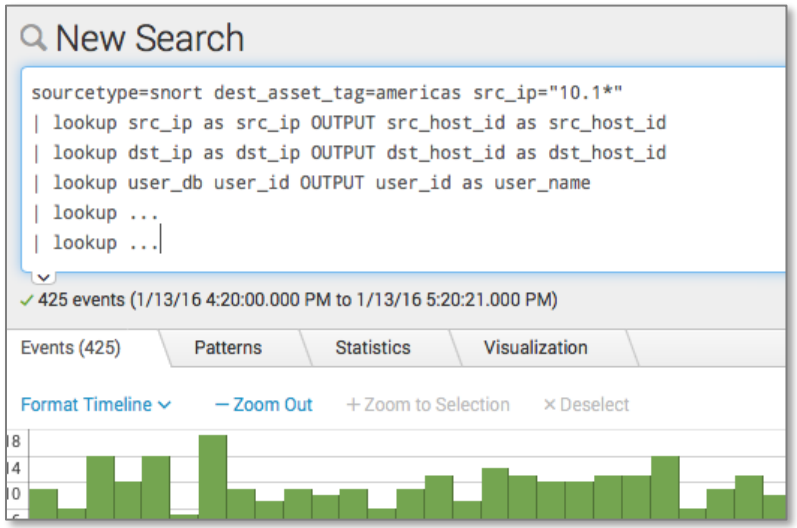
데이터 사이언스 파이프라인



splunk> 운영 인텔리전스를 위한 플랫폼

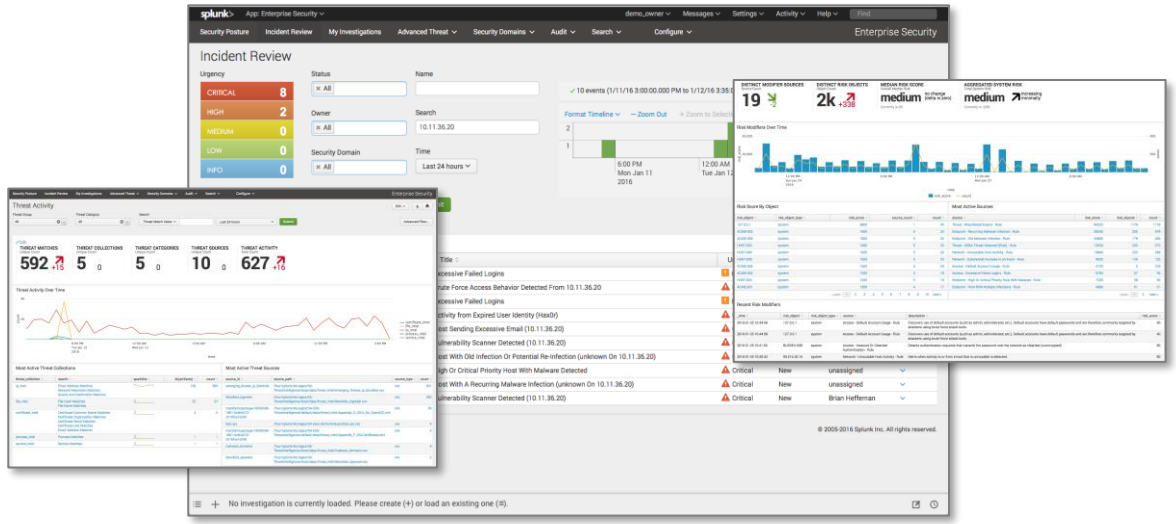
“Splunk 플랫폼” vs. “Splunk 플랫폼 + ES”

splunk>enterprise



- 여러 Lookup 테이블과 여러 필드에 대한 조인을 직접 정의
- 자산 및 계정 정보의 수동 매핑
- 위협 인텔리전스, 위험 점수 프레임워크와 같은 추가적인 확장된 컨텍스트 강화 기능을 자체 개발

Splunk Enterprise Security™ (ES)



- 보안 인시던트 탐지, 검증 및 분석과 관련된 모든 정보 연결
- 알려지지 않고 지능적 위협을 탐지하는 새로운 방법
- 위험 기반 보안 로드맵을 제공

감사합니다.

splunk> turn data into doing™