Splunk for Security

박순섭 / 최대수 매니저

December 11, 2019

splunk>Forum

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

What's New in .conf2019

2019년 스플렁크의 새로운 기술 포트폴리오

Platform

Splunk Enterprise
Connected Experiences
Splunk Machine Learning Toolkit
Splunk Cloud FedRAMP
Data Fabric Search
Data Stream Processor

IT Operations

Splunk IT Service Intelligence
Splunk App for Infrastructure
Splunk Business Flow
VictorOps
SignalFX

DevOps

SignalFX
Splunk Investigate
VictorOps
Splunk Developer Cloud

Security

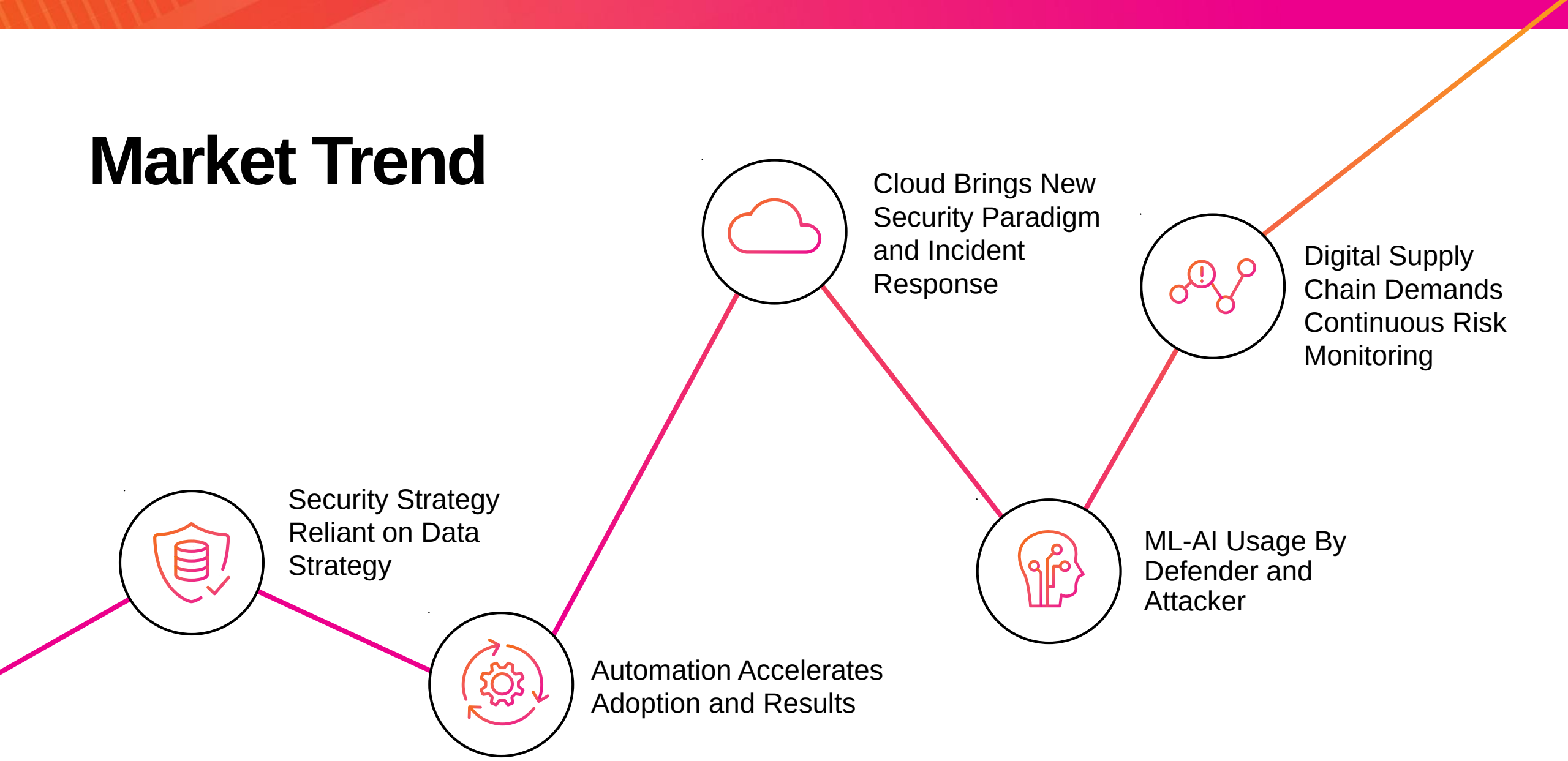
Splunk Enterprise Security
Splunk User Behavior Analytics
Splunk Phantom
Splunk Mission Control

splunk> turn data into doing™

Splunk Security Operations Suite

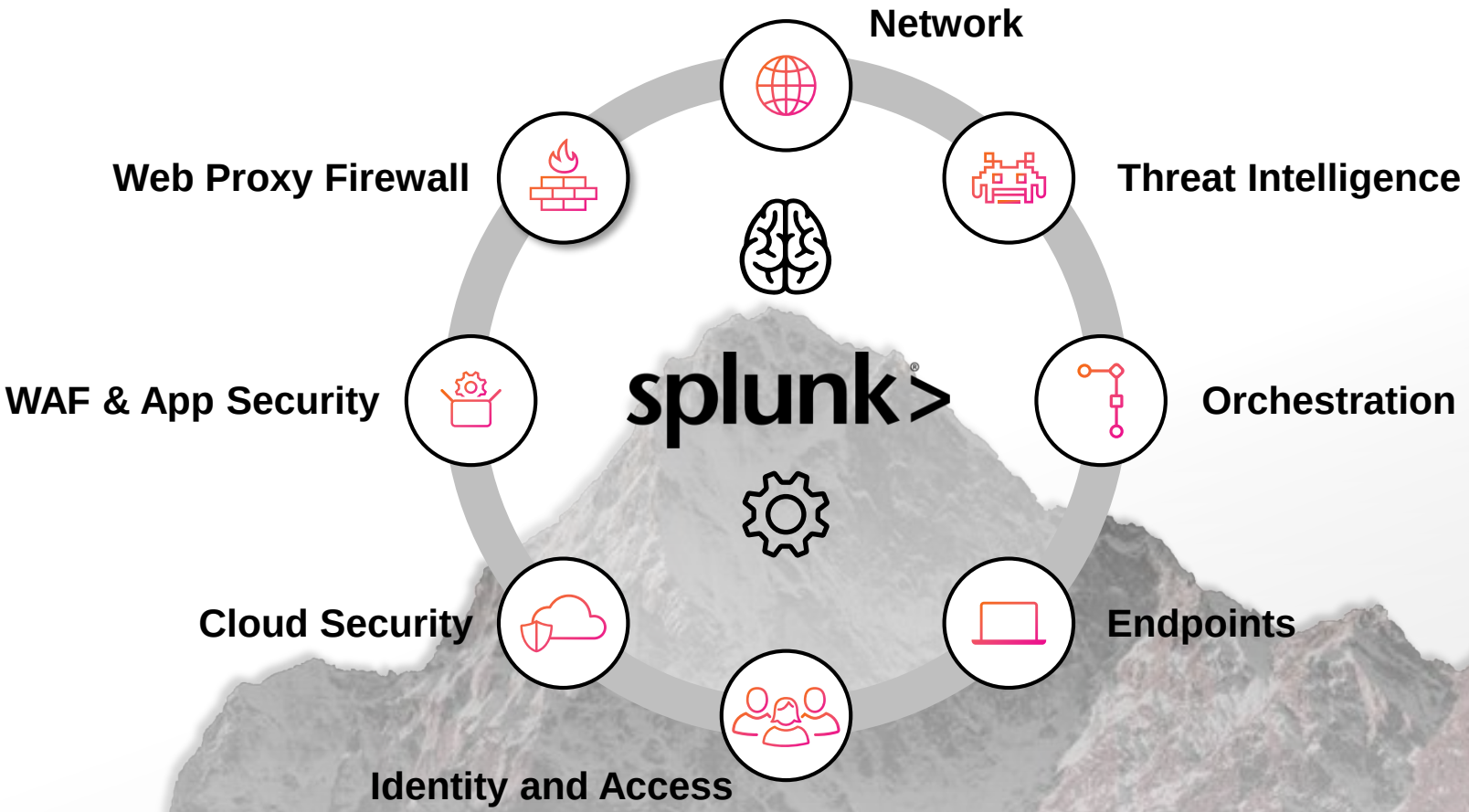
Innovations

Market Trend



Splunk as the Security Nerve Center

Optimize People, Process and Technology



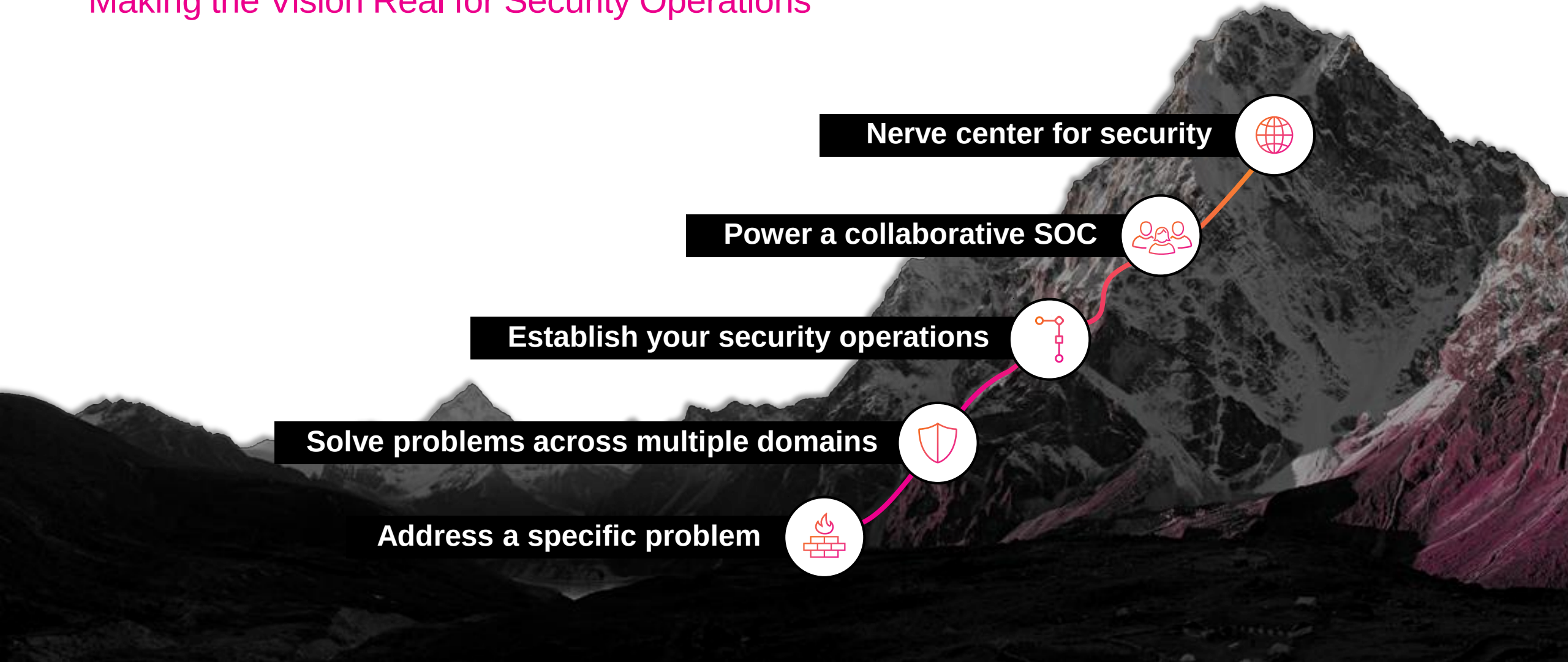
Operations

Analytics

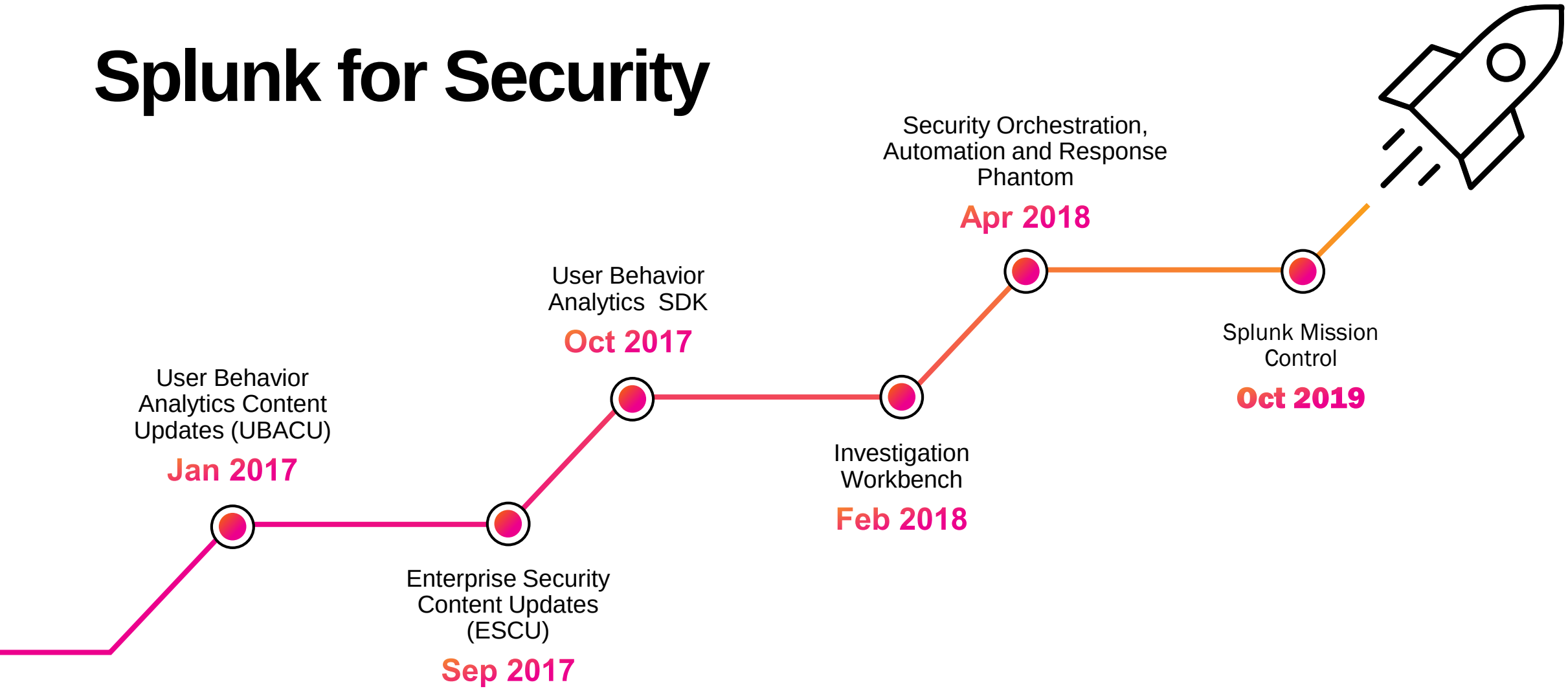
Data Platform

Journey to the Nerve Center

Making the Vision Real for Security Operations



Splunk for Security



ANNOUNCING

Mission Control *Beta*

splunk> turn data into doing

State of Security Operations

What is our Objective?

Change the way SecOps are managed

Prioritize the analyst experience first

Optimize for hybrid environments

Unify and simplify

Improve security effectiveness

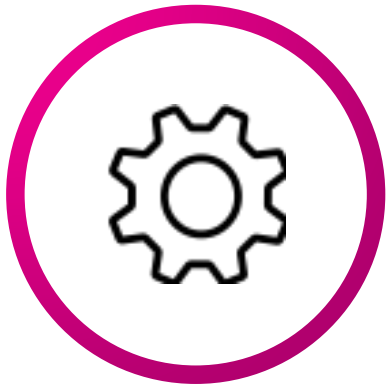
Splunk Mission Control

- Cloud-native SaaS
- Common SOC work surface
- Data, Analytics, and Automation

splunk> turn data into doing

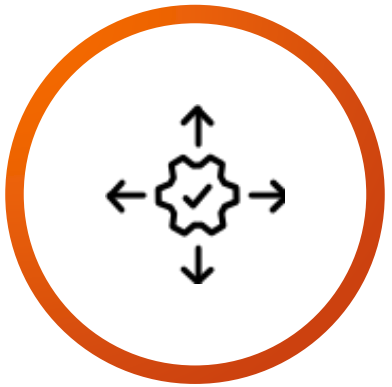
Benefits of Splunk Mission Control

Recover Time Spent



- 통합된 자동화
- 컴퓨팅 속도로 플레이북 실행

Improve Response

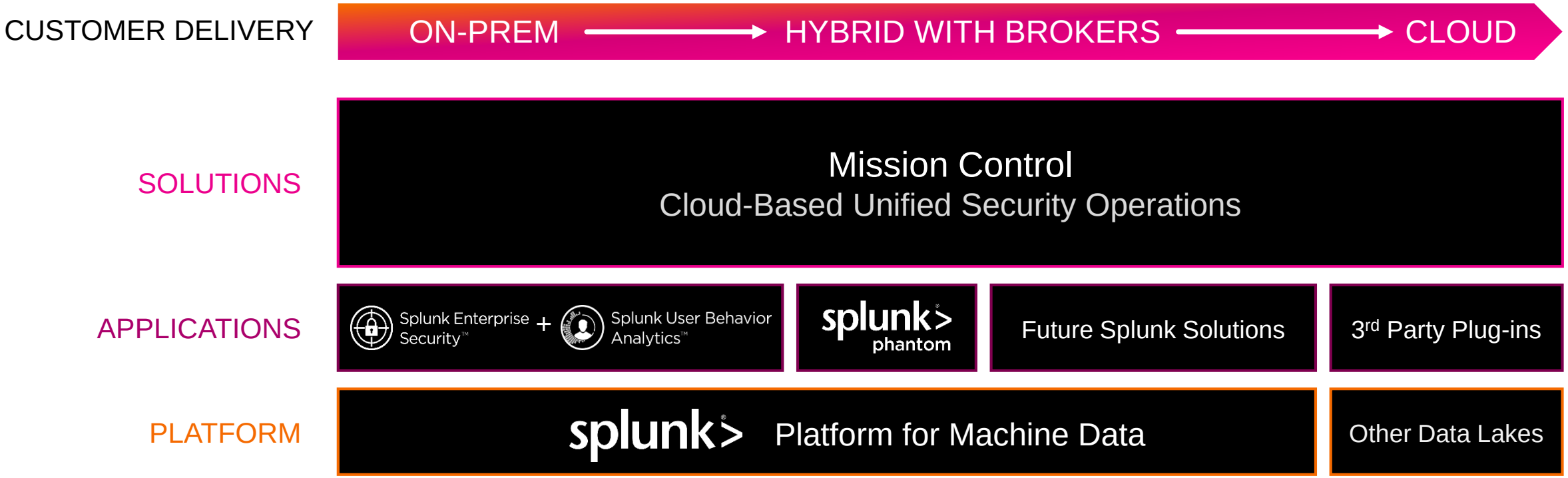


- 보안 대응 계획 모델링
- 대규모 보안 운영 감사

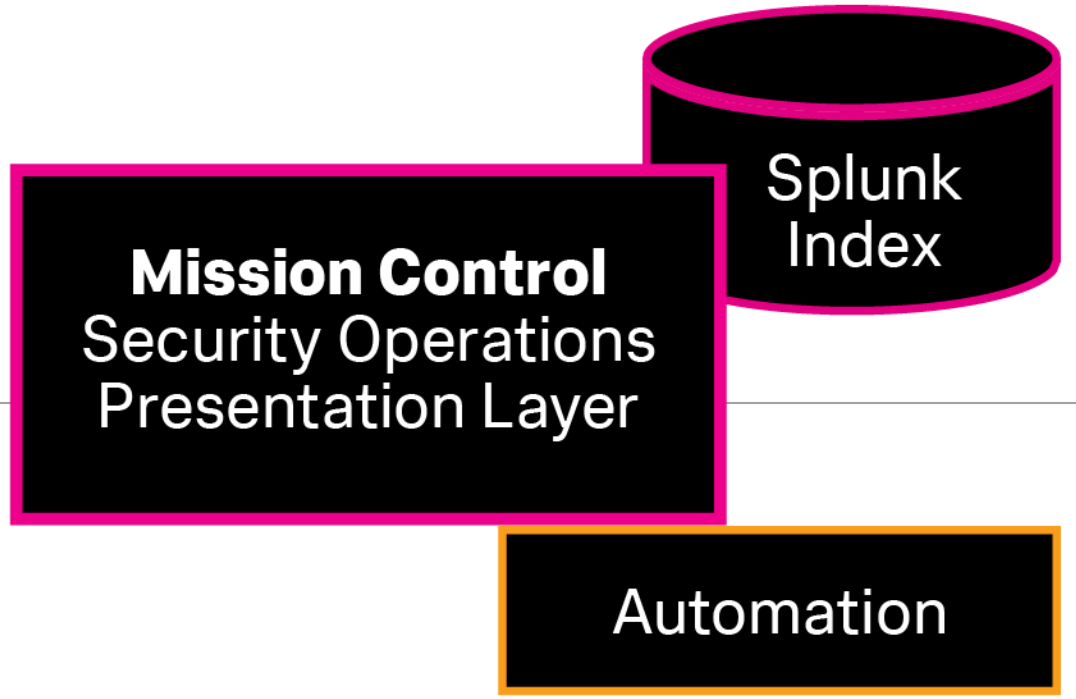
Optimize SOC

- 하나의 작업 영역에서 위협 탐지 및 조사

Security Operations Suite Architecture

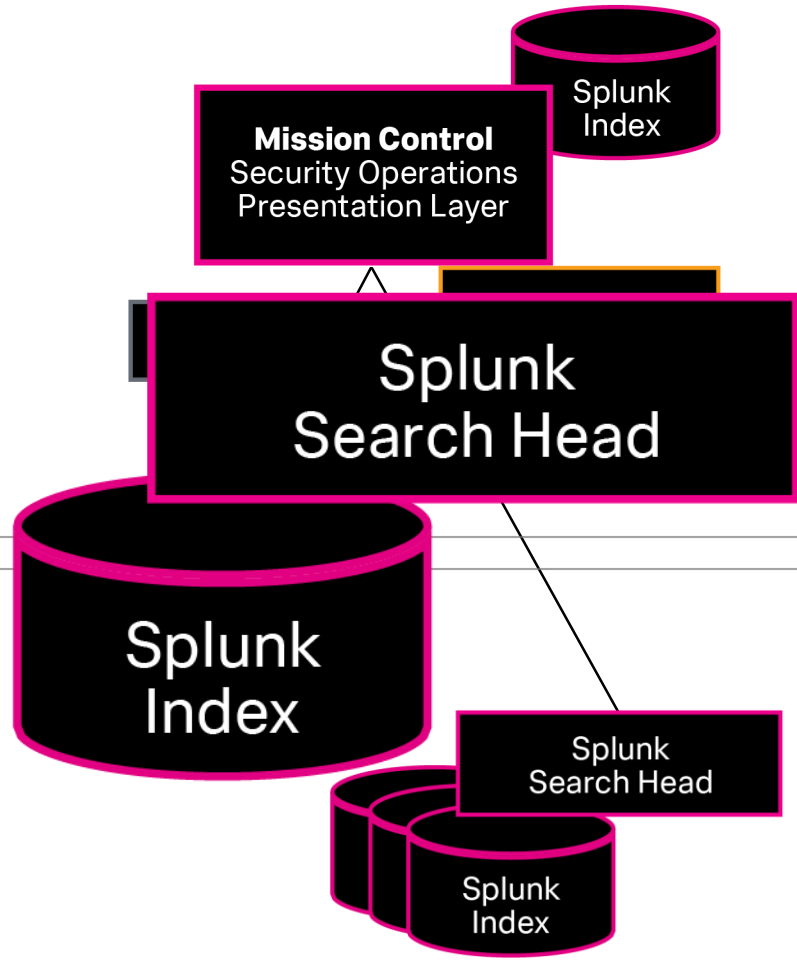


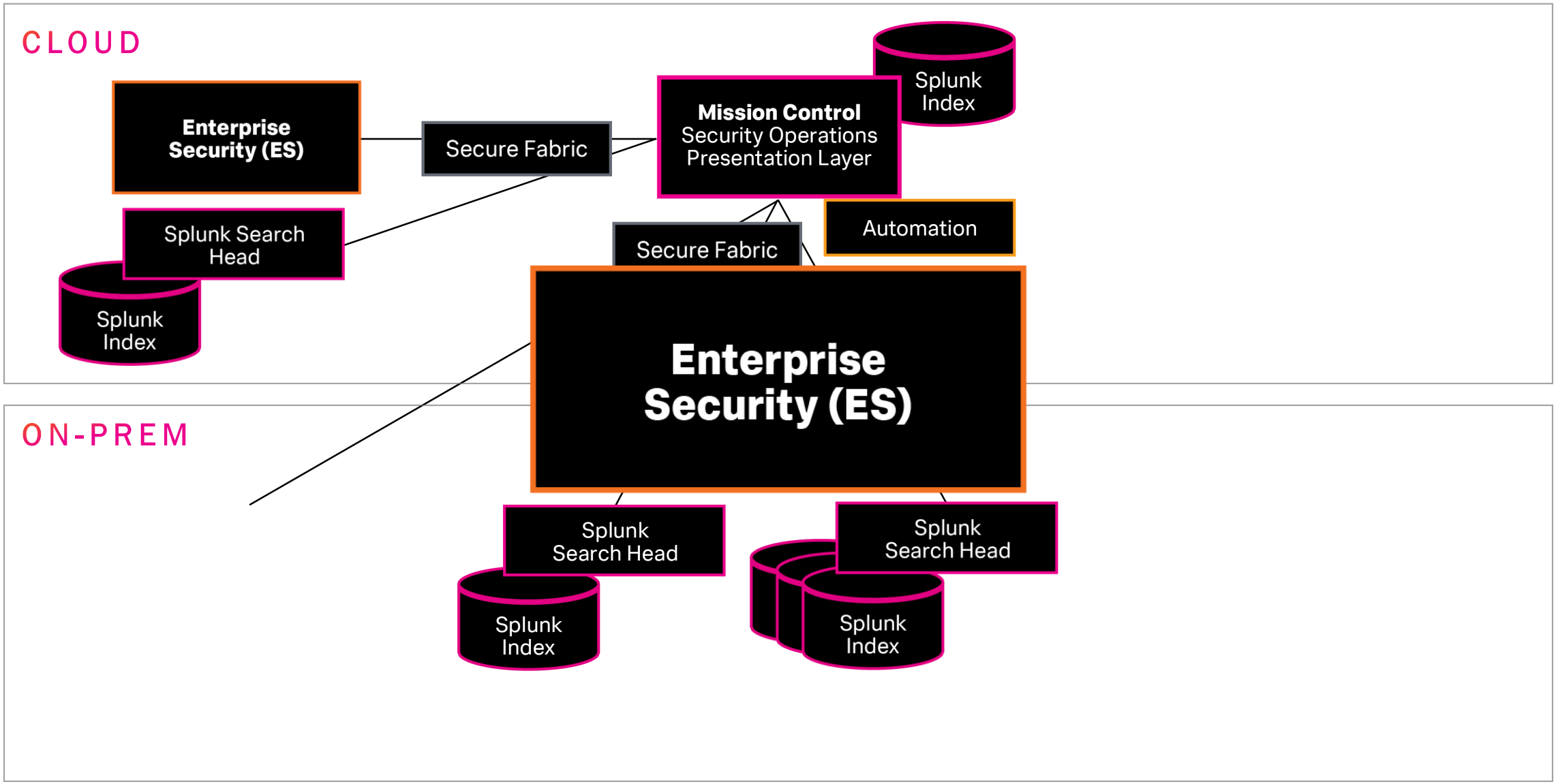
CLOUD

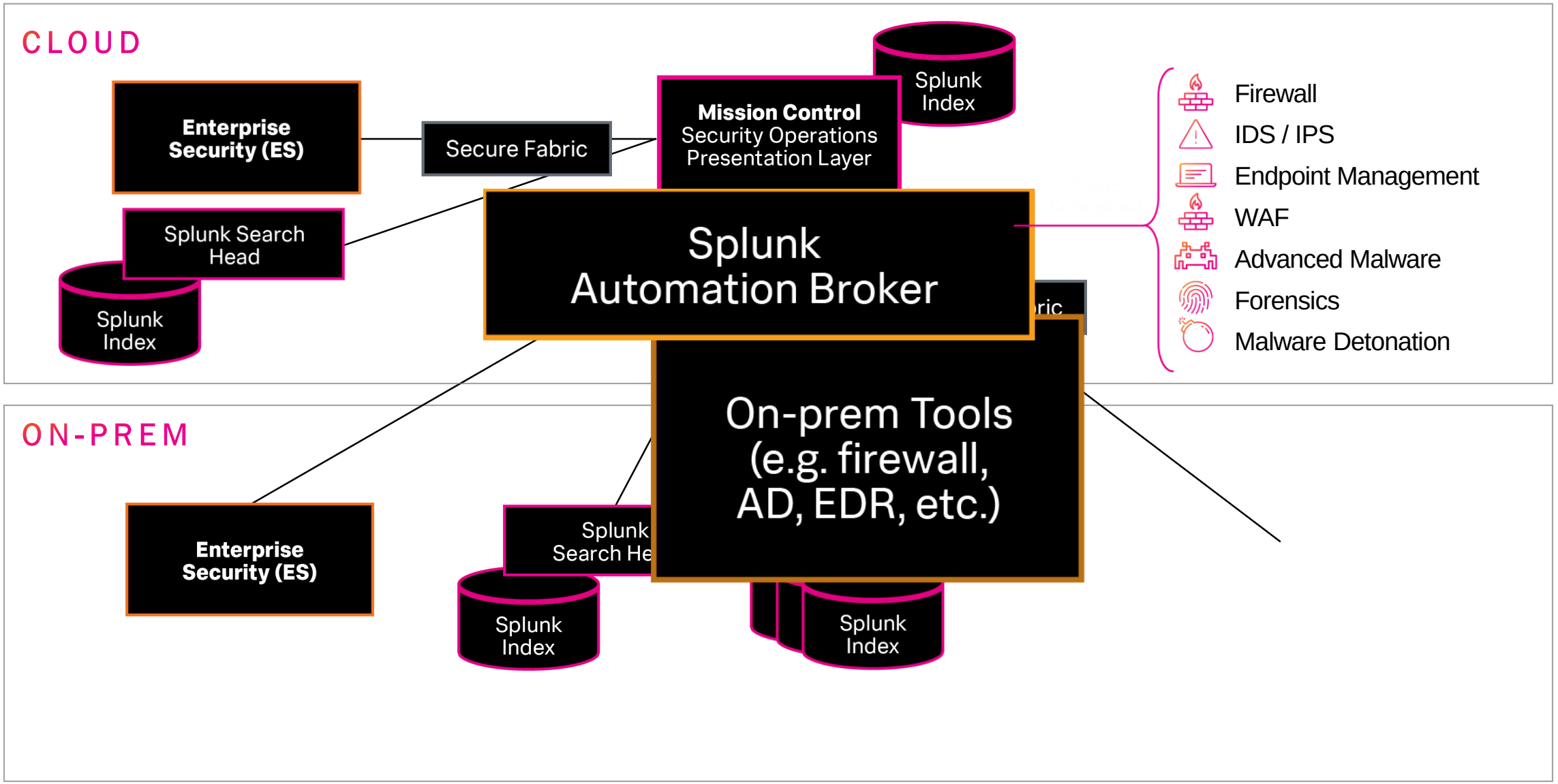

Splunk
Index
Mission Control
Security Operations
Presentation Layer
Automation

CLOUD

ON-PREM



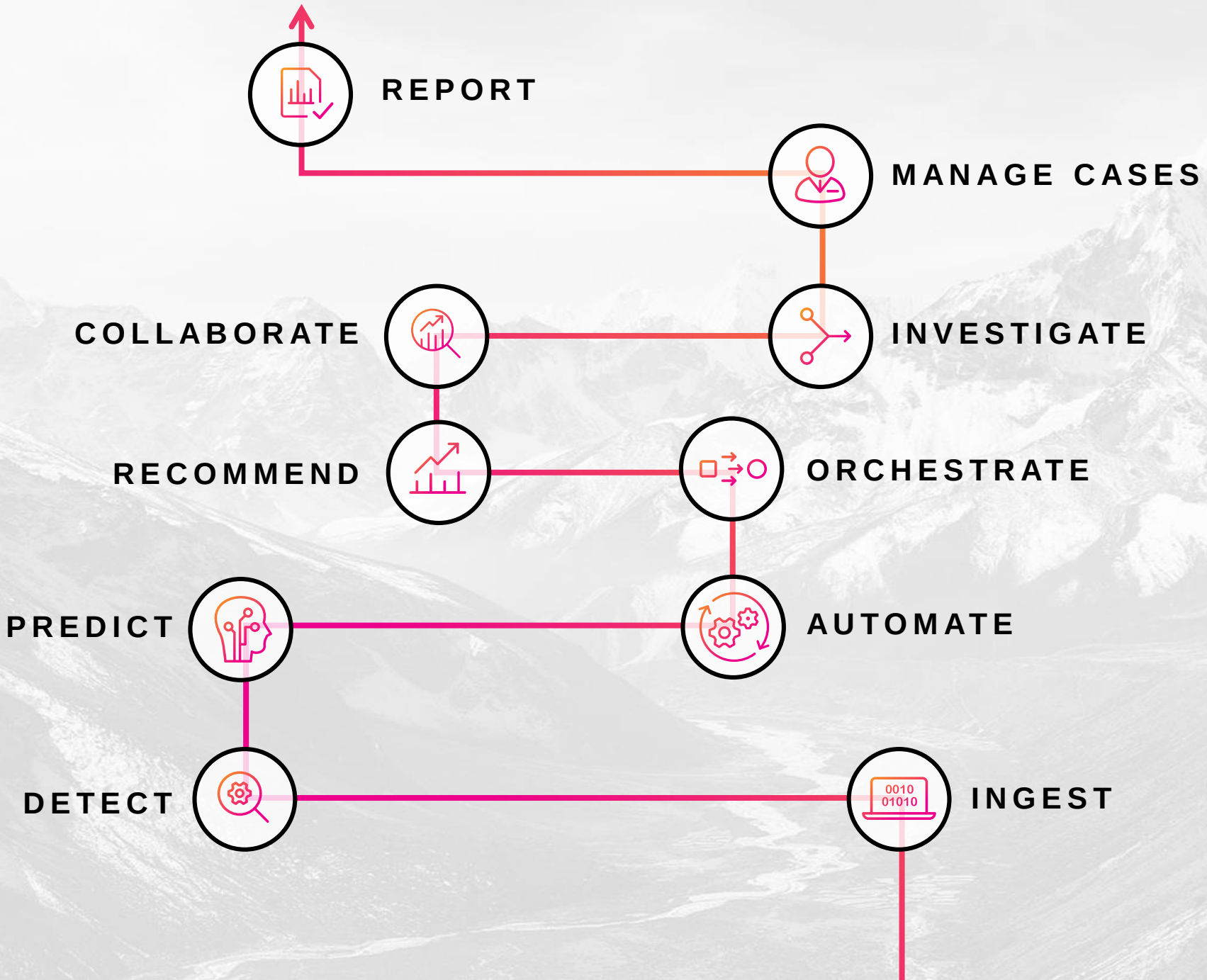

CLOUD
Enterprise Security (ES)
Secure Fabric
Mission Control
Security Operations
Presentation Layer
Splunk Index
Splunk Search Head
Splunk Index
Secure Fabric
Automation
Enterprise Security (ES)
ON-PREM
Splunk Search Head
Splunk Index
Splunk Search Head
Splunk Index


CLOUD
Enterprise Security (ES)
Secure Fabric
Mission Control
Security Operations
Presentation Layer
Splunk Index
Splunk Search Head
Splunk Index
Splunk Automation Broker
Firewall
IDS / IPS
Endpoint Management
WAF
Advanced Malware
Forensics
Malware Detonation
ON-PREM
On-prem Tools
(e.g. firewall,
AD, EDR, etc.)
Enterprise Security (ES)
Splunk Index
Splunk Index

ANNOUNCING

Enterprise Security 6.0

splunk> turn data into doing



Artificial Intelligence

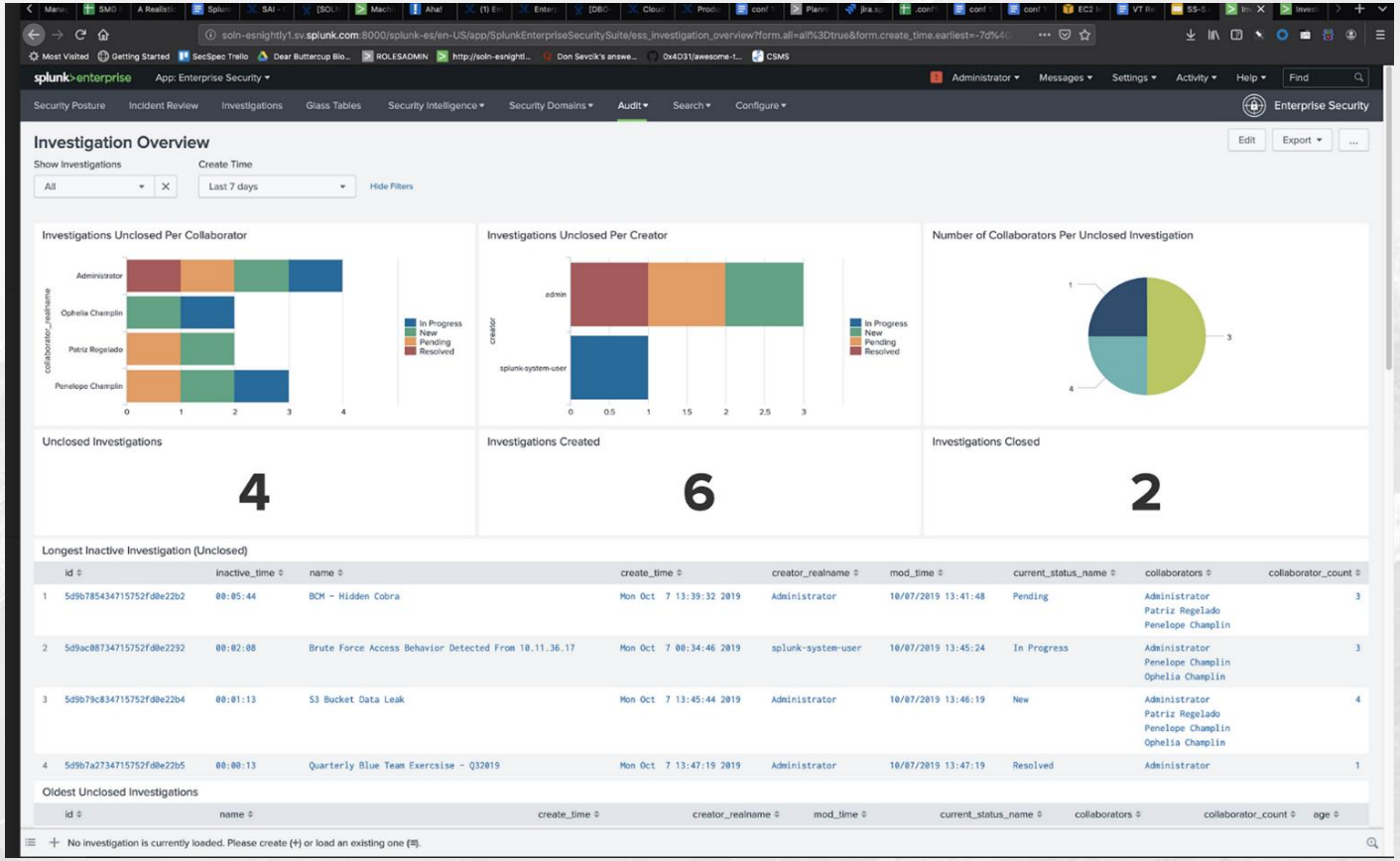
Machine Learning

Content

splunk> turn data into doing

Splunk Enterprise Security

- Detect advanced threats
- Enrich with Analytics
- Analyze & investigate threats
- Enterprise-wide coordination & response



INGEST

DETECT

INVESTIGATE

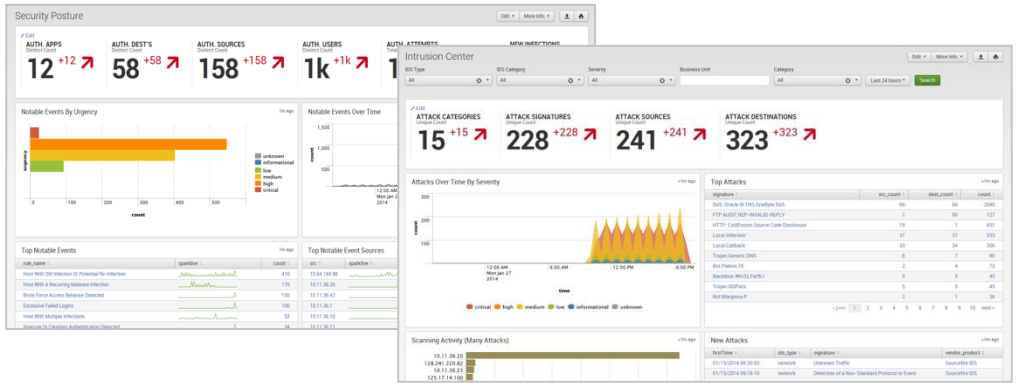
COLLABORATE

REPORT

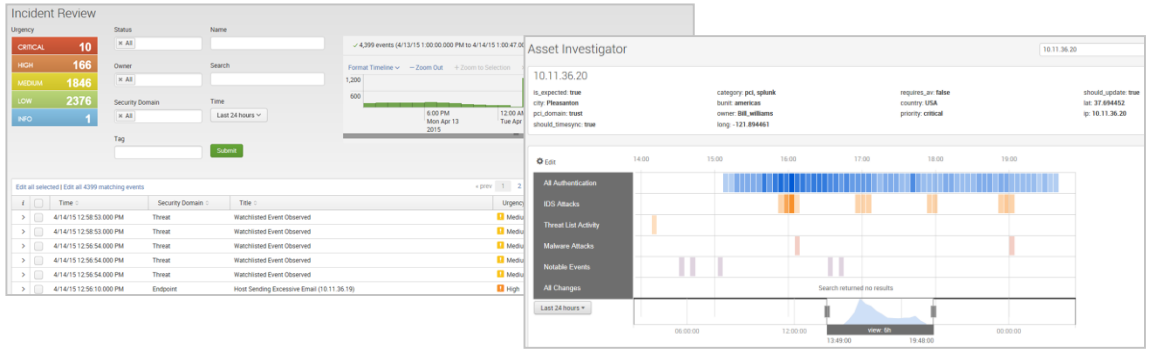
splunk> turn data into doing

Splunk Enterprise Security

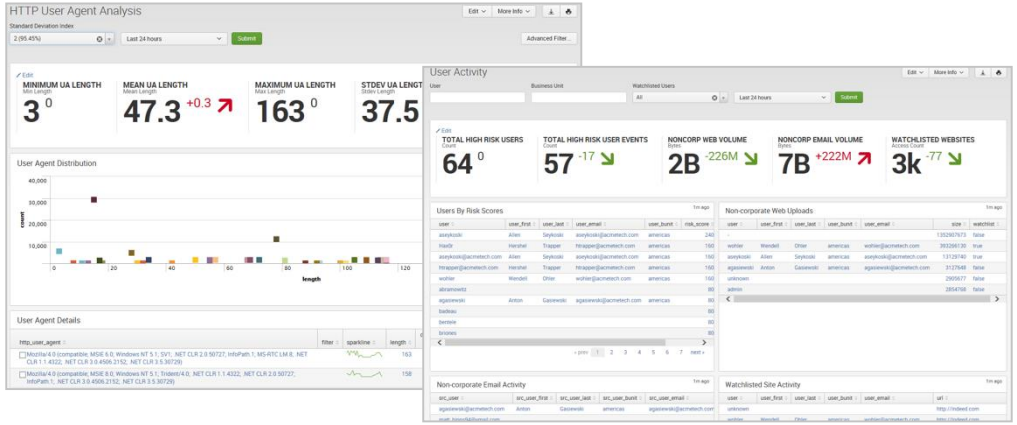
기본 탑재된 검색, 경고, 리포트, 대시보드, 인시던트 워크플로우, 위협 피드



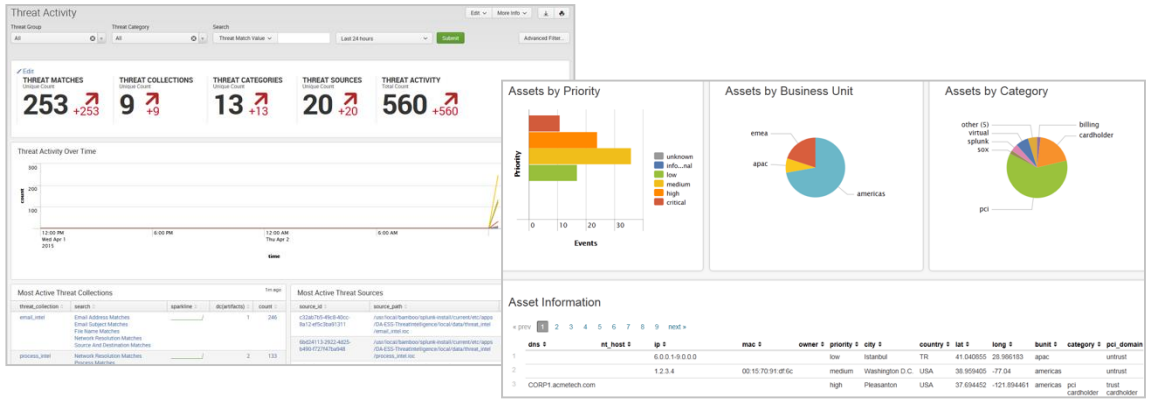
경고 & 대시보드 & 리포트



사고 조사 및 관리



통계적 이상치 & 위험 점수 & 사용자 활동

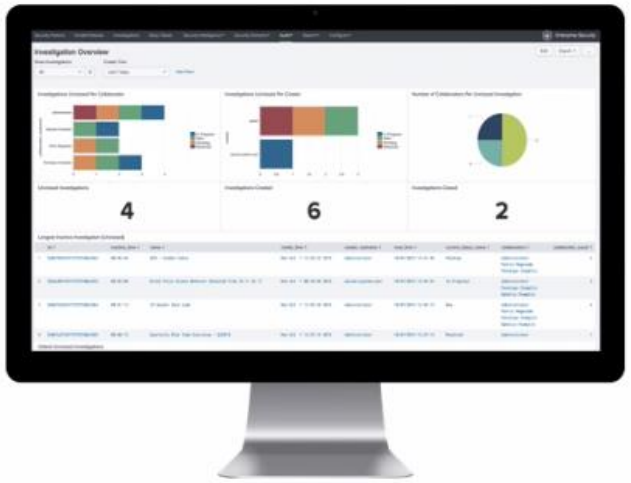


위협 인텔리전스 & 자산 & 신원정보 통합

Splunk Enterprise Security 6.0

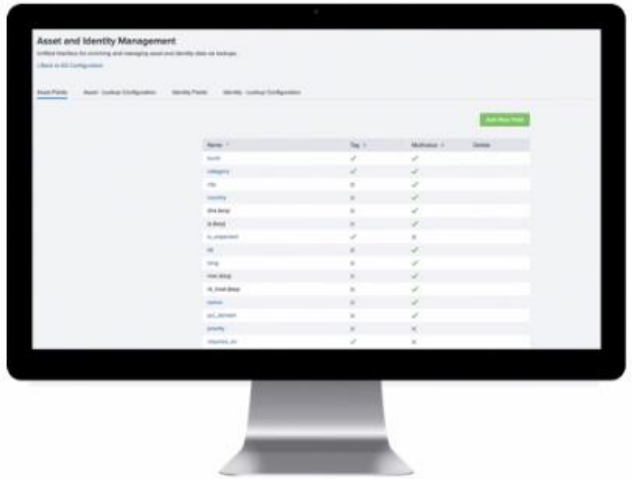
Key Enhancements

Analytics Reporting on Investigations



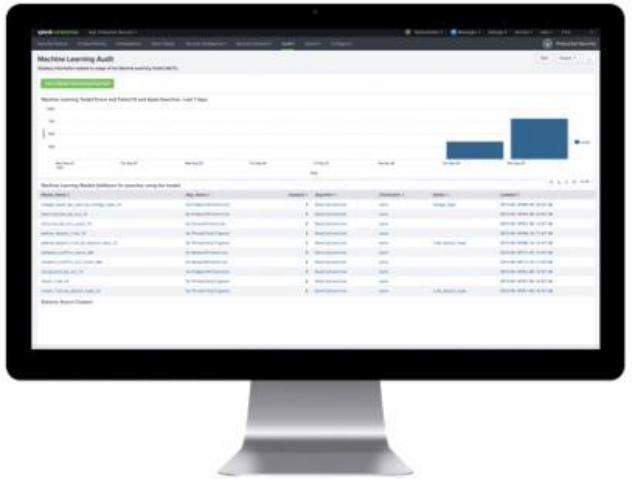
- 조사 활동에 대한 보고서 기능 추가
- SOC의 요구 사항에 따른 커스텀 가능 (SPL 지원)

Asset and Identity Framework Enhancements



- 데이터 수집 성능 증가
- 3x 스케일 확장으로 2백만 이상의 엔트리 수용

Splunk Machine Learning Tool Kit (MLTK) Integration

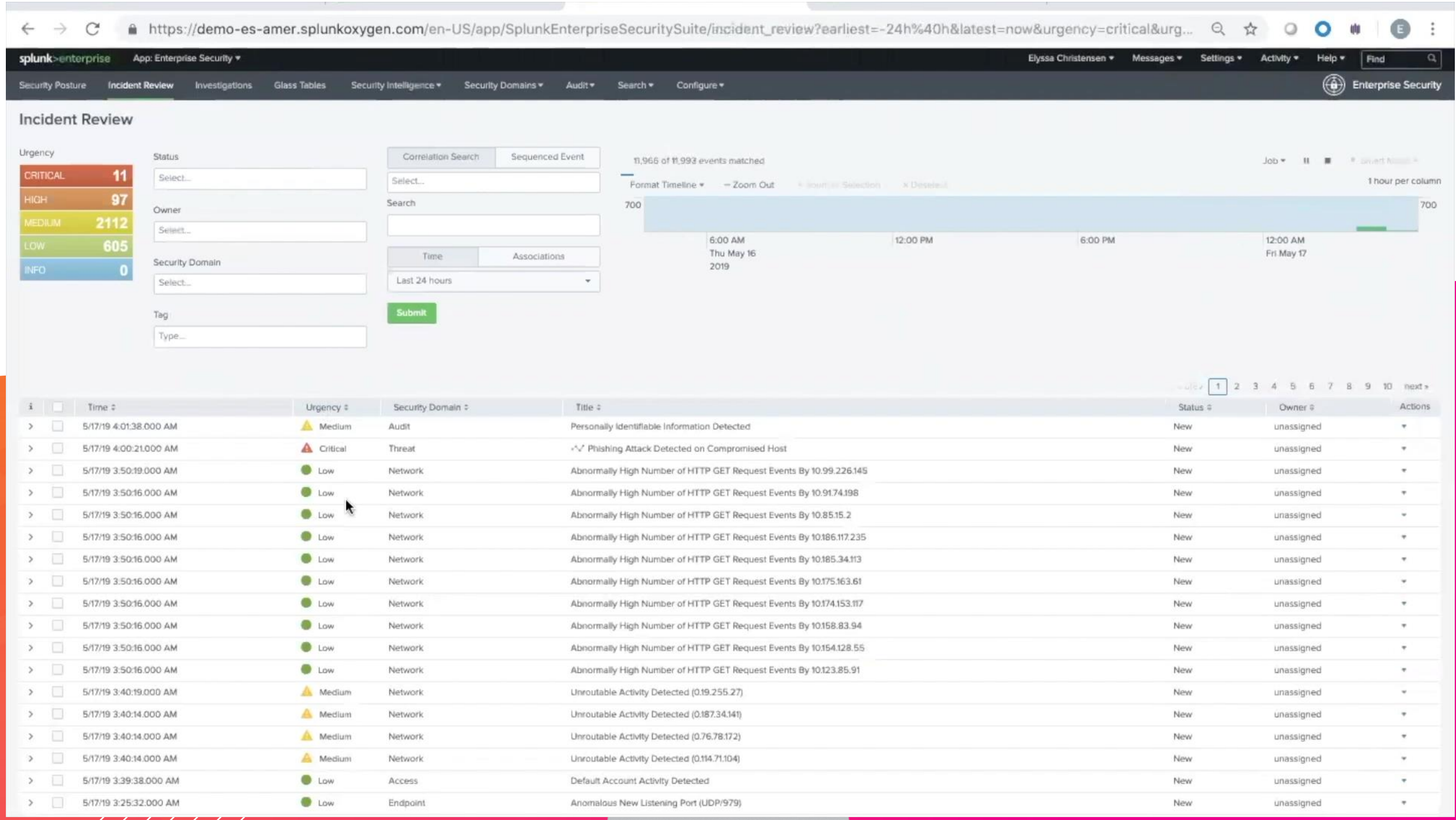


- 40% 처리 속도 증가
- 20% CPU 리소스 절감

Demo

Enterprise Security

splunk> turn data into doing


https://demo-es-amer.splunkoxygen.com/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=-24h%40h&latest=now&urgency=critical&urg...
splunk>enterprise
App: Enterprise Security
Elyssa Christensen
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Investigations
Glass Tables
Security Intelligence
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 11
HIGH 97
MEDIUM 2112
LOW 605
INFO 0
Status
Select...
Owner
Select...
Security Domain
Select...
Tag
Type...
Correlation Search
Sequenced Event
Select...
Search
Time
Associations
Last 24 hours
Submit
11,966 of 11,993 events matched
Job
Format Timeline
Zoom Out
1 hour per column
700
700
6:00 AM
Thu May 16
2019
12:00 PM
6:00 PM
12:00 AM
Fri May 17
1 2 3 4 5 6 7 8 9 10 next »
Time
Urgency
Security Domain
Title
Status
Owner
Actions
5/17/19 4:01:38.000 AM Medium Audit Personally Identifiable Information Detected New unassigned
5/17/19 4:00:21.000 AM Critical Threat Phishing Attack Detected on Compromised Host New unassigned
5/17/19 3:50:19.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.99.226.145 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.91.74.198 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.85.15.2 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.186.117.235 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.185.34.113 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.175.163.61 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.174.153.117 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.158.83.94 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.154.128.55 New unassigned
5/17/19 3:50:16.000 AM Low Network Abnormally High Number of HTTP GET Request Events By 10.123.85.91 New unassigned
5/17/19 3:40:19.000 AM Medium Network Unroutable Activity Detected (0.19.255.27) New unassigned
5/17/19 3:40:14.000 AM Medium Network Unroutable Activity Detected (0.187.34.141) New unassigned
5/17/19 3:40:14.000 AM Medium Network Unroutable Activity Detected (0.76.78.172) New unassigned
5/17/19 3:40:14.000 AM Medium Network Unroutable Activity Detected (0.114.71.104) New unassigned
5/17/19 3:39:38.000 AM Low Access Default Account Activity Detected New unassigned
5/17/19 3:25:32.000 AM Low Endpoint Anomalous New Listening Port (UDP/979) New unassigned

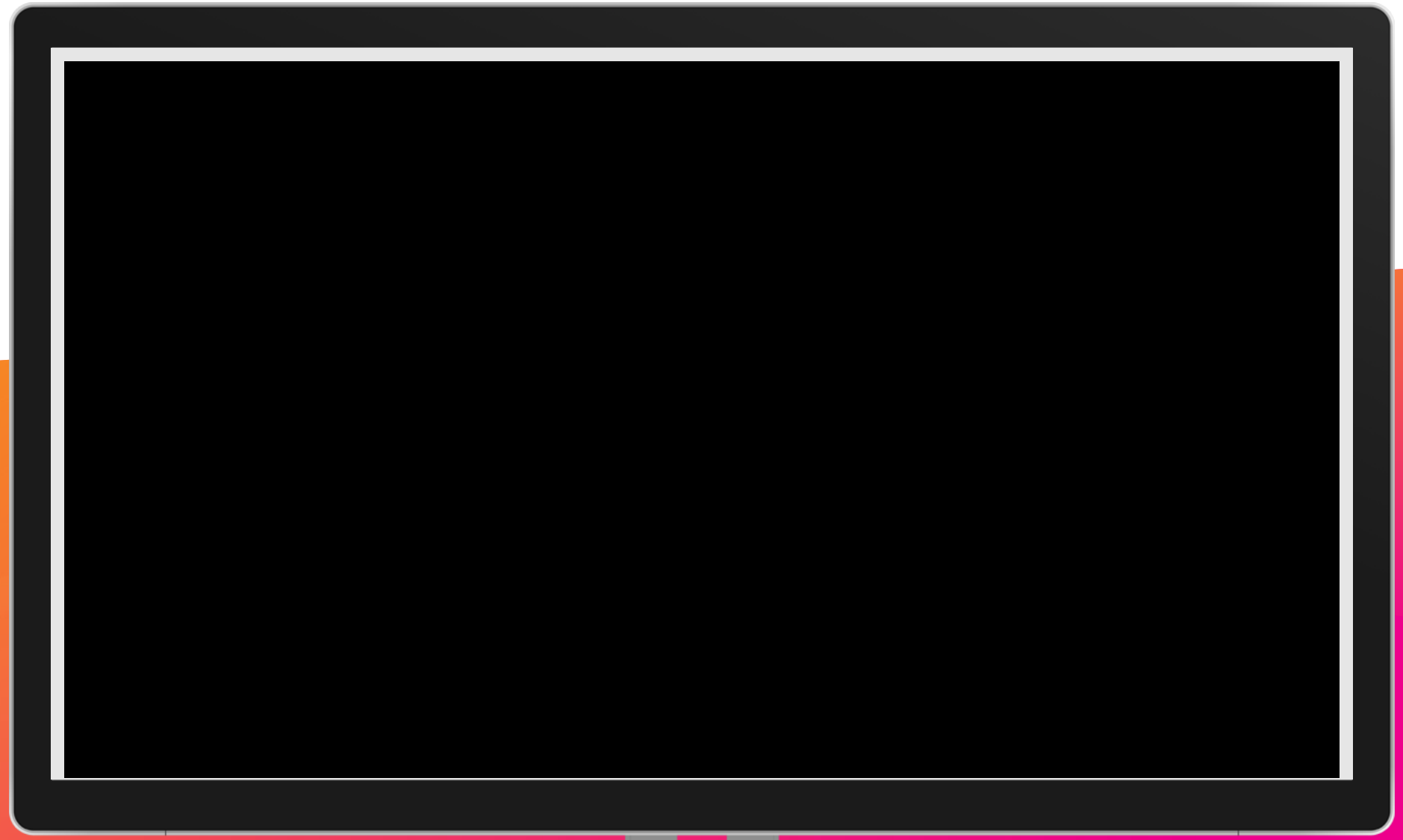
Splunk Phantom 4.6

Security Orchestration, Automation and Response

splunk> turn data into doing™

귀사의 SOC에서 가장 큰 과제는 무엇인가요?

가장 많은 시간을 보내는 업무는?



보안 운영 문제

자원

보안 전문가의 자원 부족

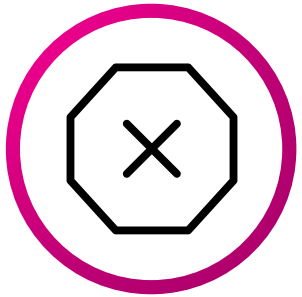
제품

단위 보안 제품들의 끊임없는 연동

경보

대량 보안 경보의 에스컬레이션

정적



오케스트레이션 없이 정적이고 독립적인 통제

속도

탐지, 우선순위 구분 및 대응 시간의 속도가 향상되어야 함

비용

비용은 계속 증가

이러한 문제를 누가 다루는가?

운영

Tier 1
보안 분석가

Tier 2
위협 대응

Tier 3
위협 대응

피싱 이메일 조사

위협 사냥

위협 인텔리전스

말웨어 조사

이벤트 선별

내부자 위협 분석팀

관리

SOC 팀장

CISO

팀 성과

프로세스 & 운영

메트릭 & 리포팅

보안운영을 위한 SOAR

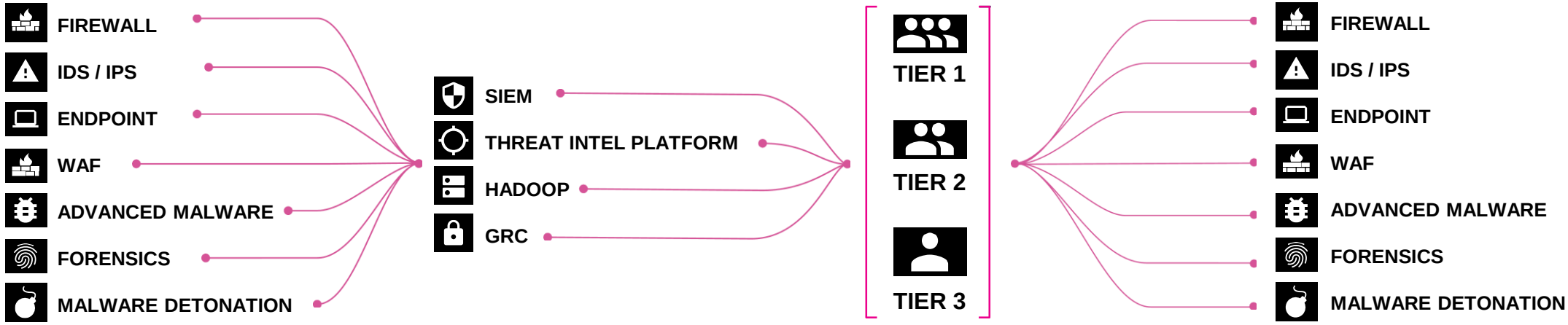
OODA 루프를 통한 빠른 실행으로 보안 향상

Observe
Point Products

Orient
Analytics

Decision Making

Acting

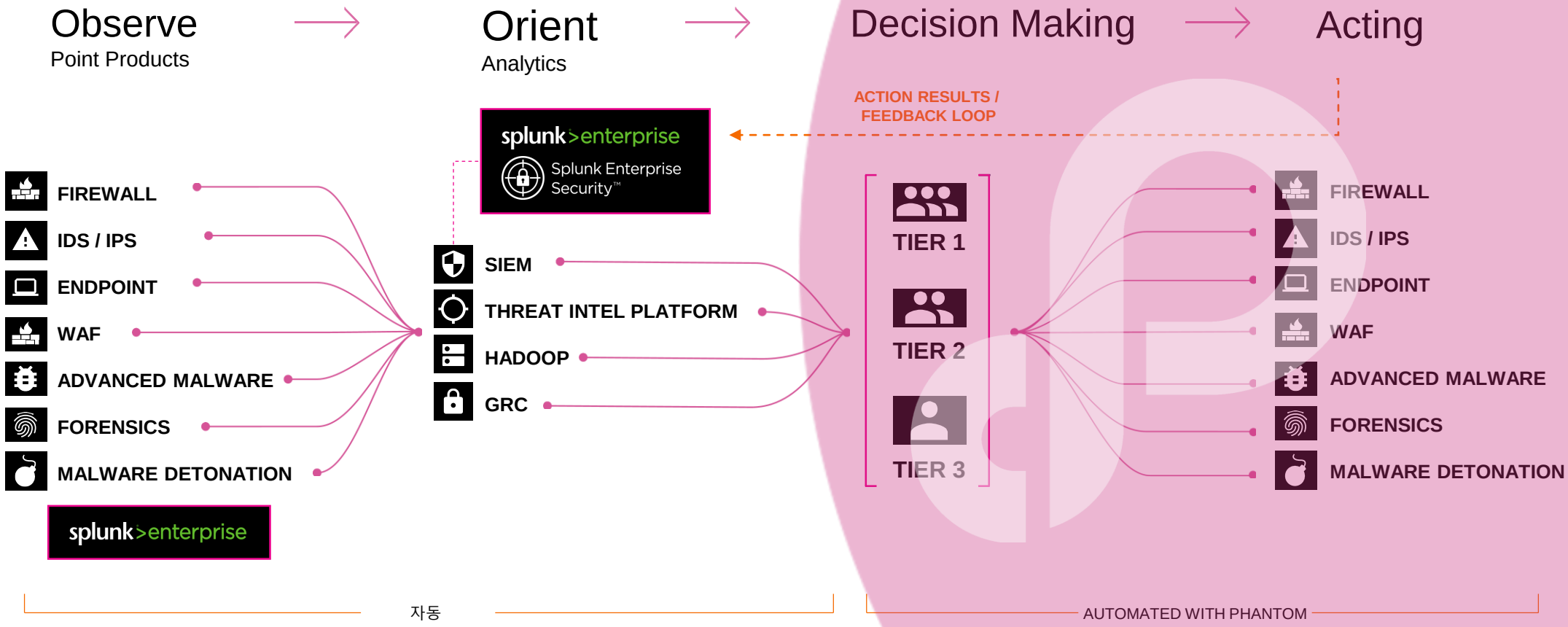


자동

수동 (현재)

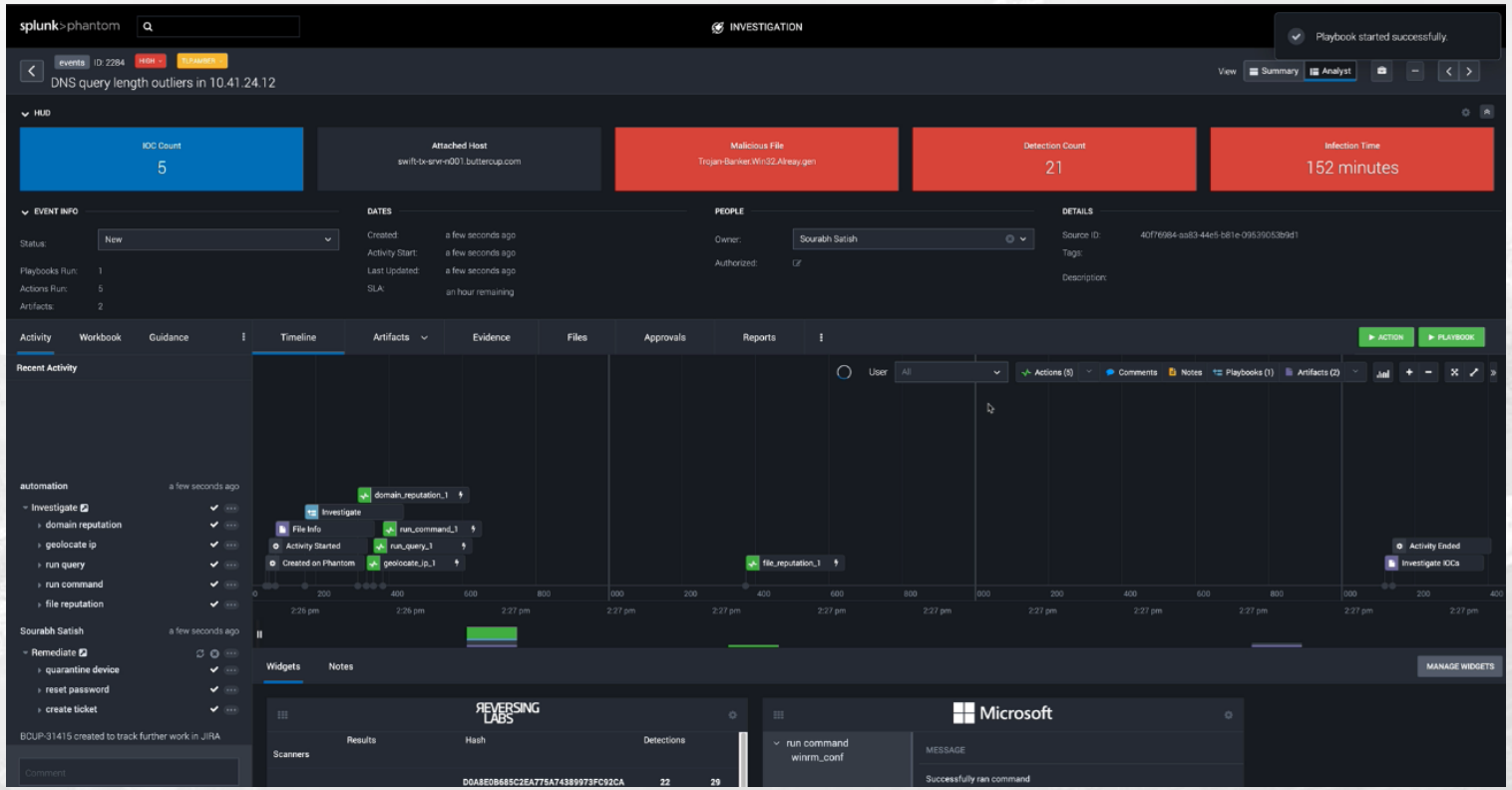
보안운영을 위한 SOAR

OODA 루프를 통한 빠른 실행으로 보안 향상



Splunk Phantom 4.6

1) Phantom 모바일
2) AWS에 환경에 유연하게 구성
3) SHC 검색 지원
4) ITSI 모니터링



자동화

오케스트레이션 (조정, 편성)

권장 (추천)

협업 (공동작업)

케이스 관리

Splunk Phantom 4.6

가장 큰 SOC

100
분석가

이벤트 처리

1
백만 / 일

확장되는 에코시스템

300 앱
1,900+ 액션

Phantom 앱 오픈 소스


AWS Athena


AWS CloudTrail


AWS IAM


AWS Lambda


AWS Security Hub

Carbon Black.

cuckoo

DARKPOINT

DOMAINTOOLS

endace

FORCEPOINT

';--have i been pwned?

INTEZER

ipinfo.io

Jira

mimecast

Nessus

NetBIOS

netskope

PASSIVE TOTAL

proofpoint.

REDSEAL

REVERSING LABS

RSA Security Analytics

Screenshotmachine

Skype for Business

Symantec ATP

Symantec Management Center

ThreatMiner
Data Mining for Threat Intelligence

splunk> VictorOps

who.is

Windows Remote Management

Windows ATP

새로운 기능 : 모바일 장치의 Splunk Phantom

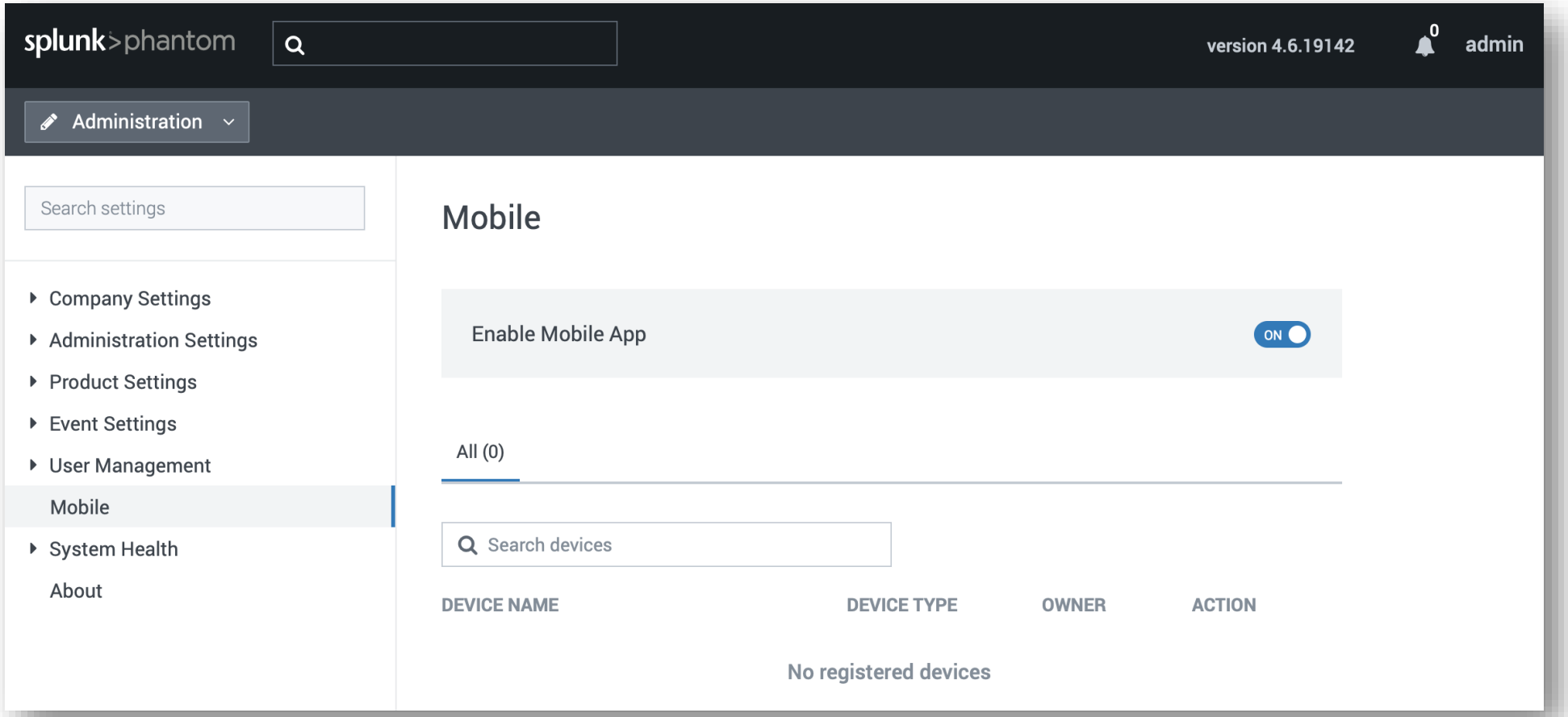
언제 어디서나 더 스마트하게 작업하고 더 빠르게 대응하며 방어를 강화

- Phantom on Splunk Mobile 은 Phantom 보안 오케스트레이션, 자동화 및 응답 (SOAR) 기능을 모바일에서 제공
  - 노트북을 열 필요가 없습니다. 손안에서 보안 작업을 조정하십시오.
  - 어느 곳에서나 연락 할 수 있으므로 그 어느 때보다 빠르게 응답합니다.
  - 어디에서나 플레이 북을 실행하고, 이벤트를 선별하고, 동료와 공동 작업을 수행하십시오.

splunk> turn data into doing

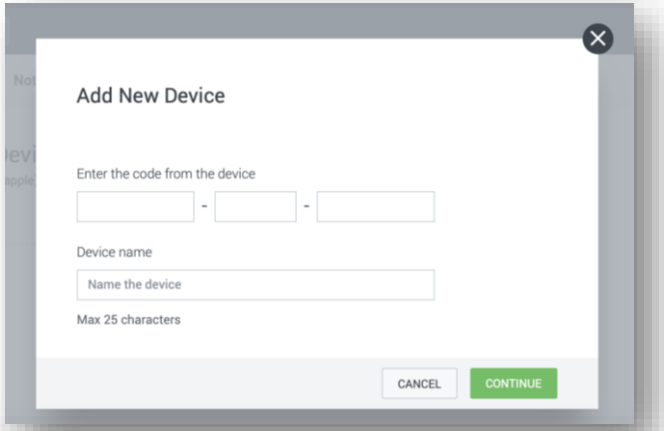
Splunk Mobile App for Splunk Phantom(1/3)

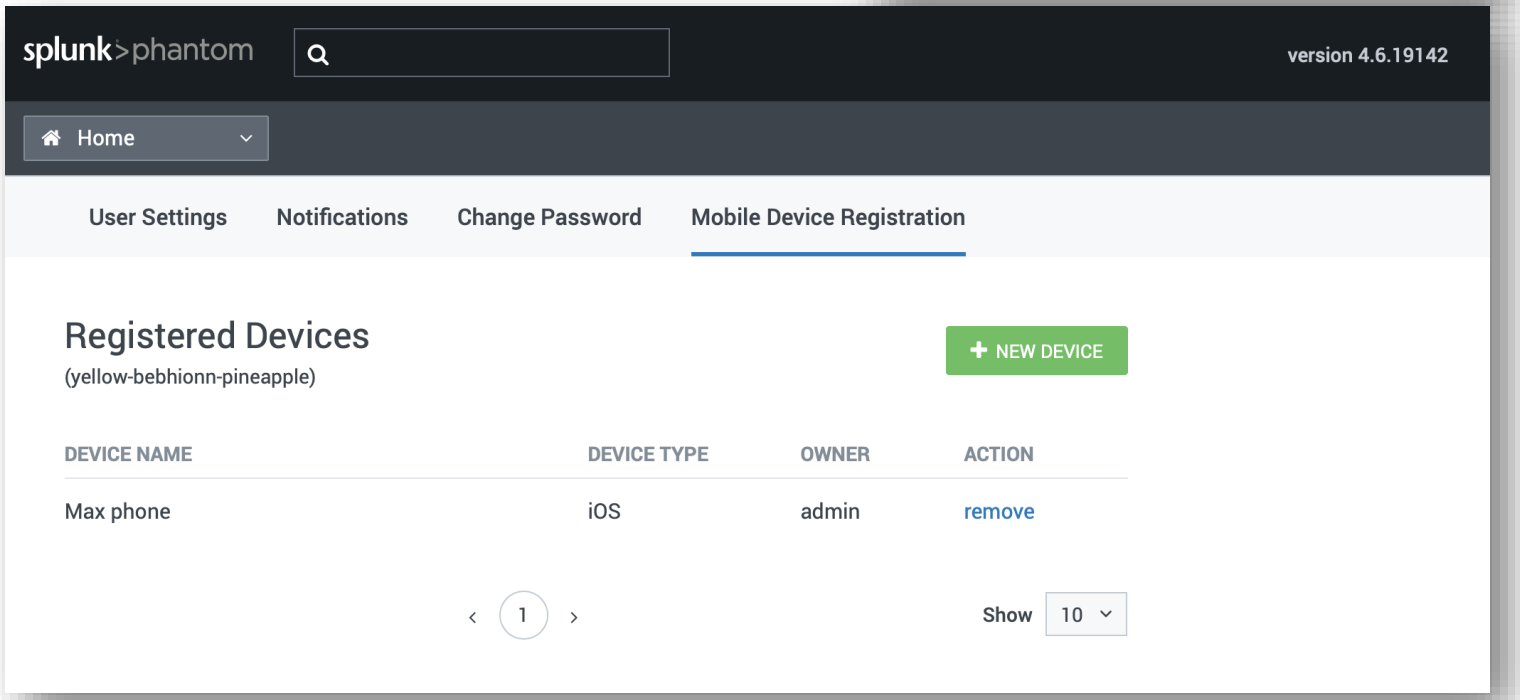
설정방법

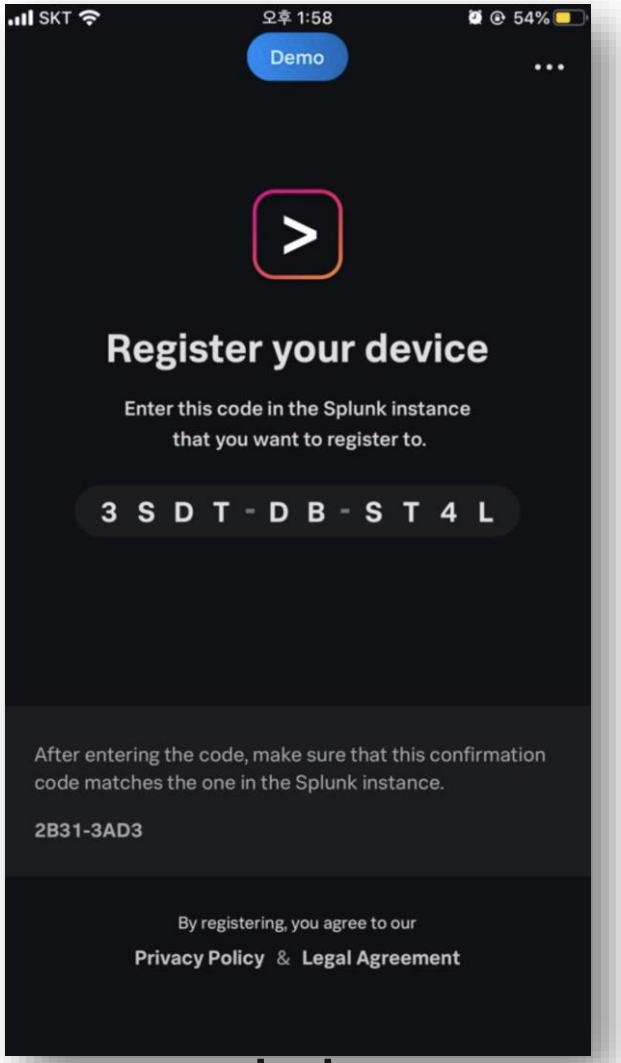


Splunk Mobile App for Splunk Phantom(2/3)

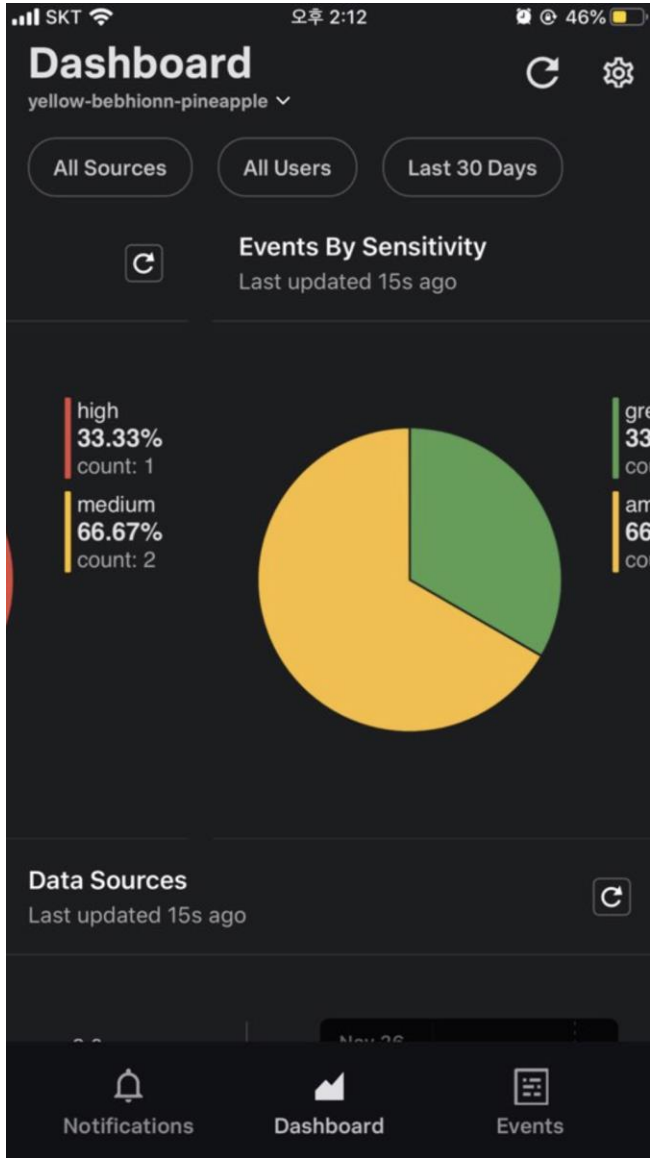
설정방법

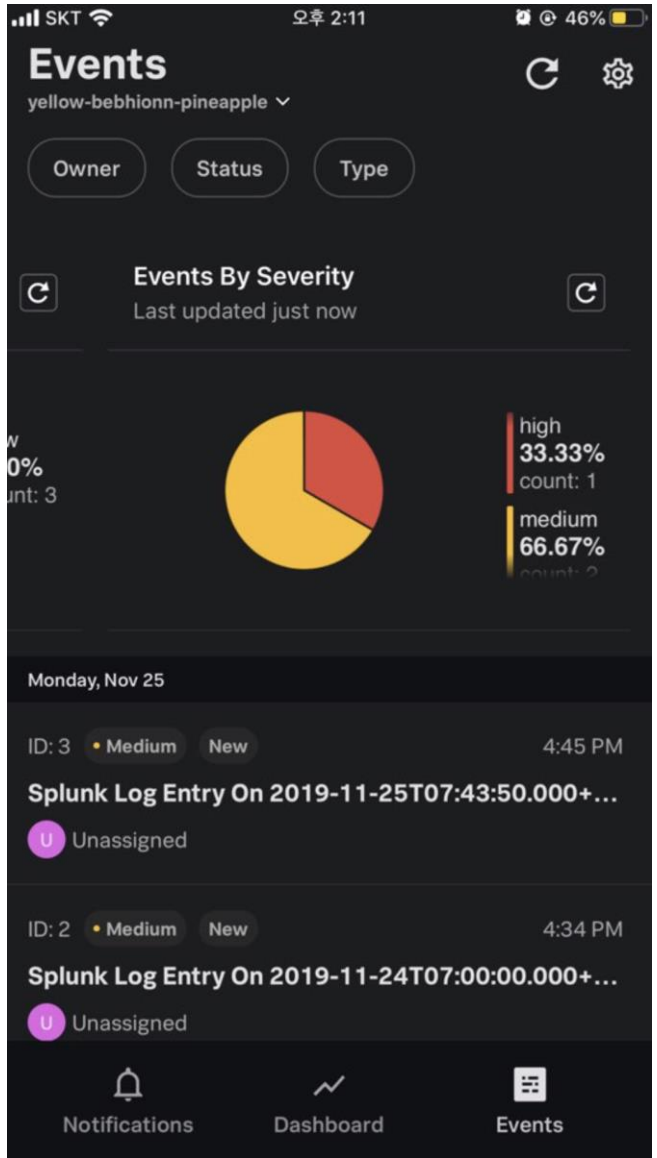


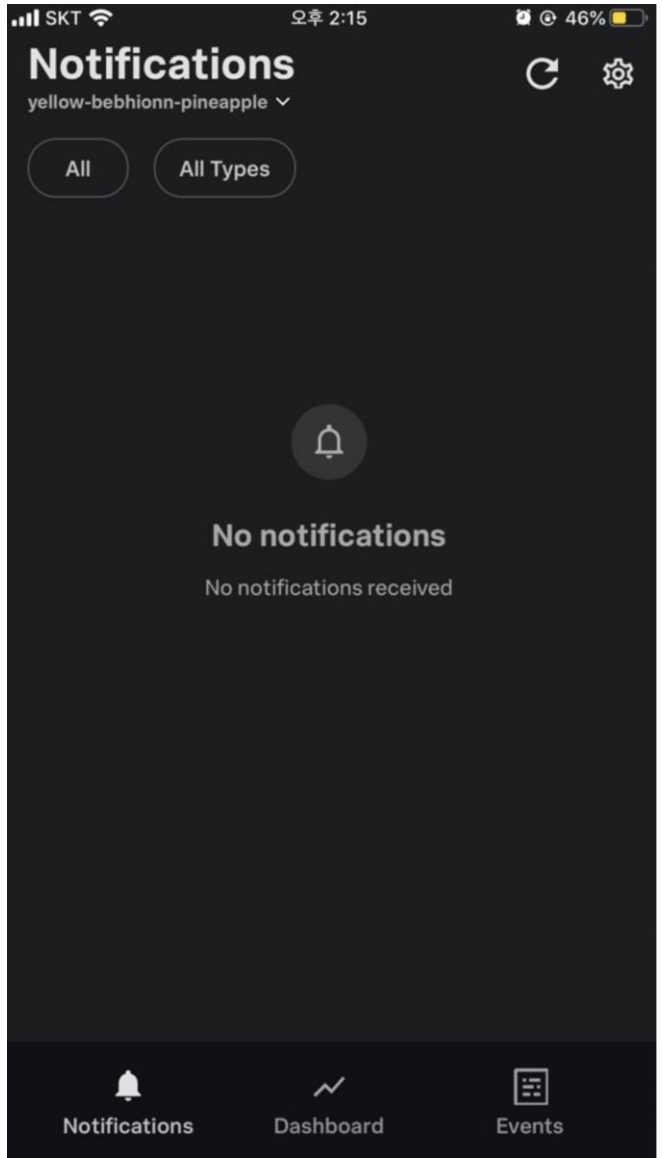




Splunk Mobile App for Splunk Phantom(3/3)

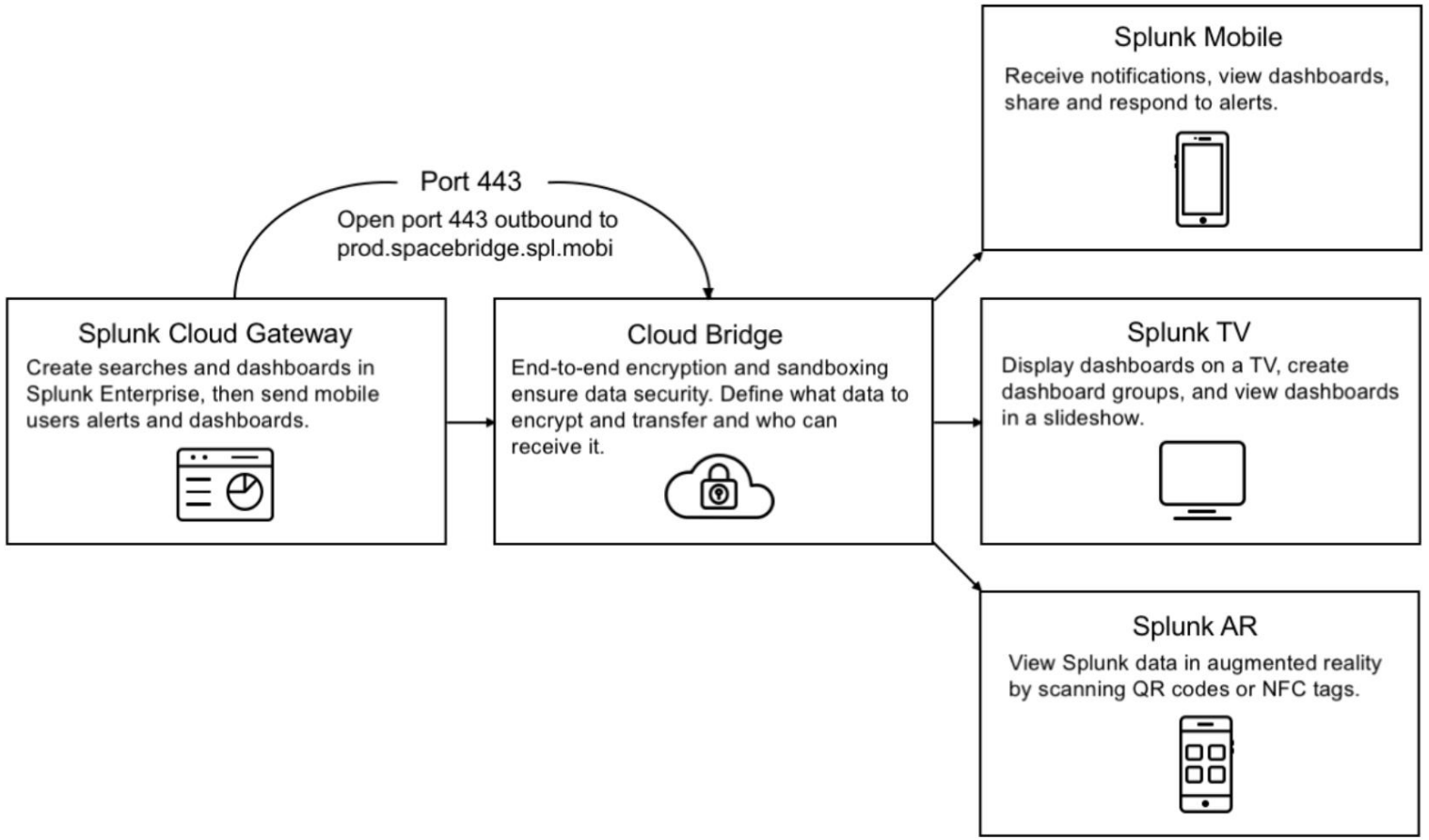






Splunk Mobile App for Splunk Phantom

Splunk Cloud Gateway는 모바일 장치가 Splunk Enterprise 인스턴스에 연결하기 위한 클라우드 기반 브리지입니다.



Splunk Mobile App for Splunk Phantom

These ports must be open on each Splunk Phantom node to enable mobile app registration.

Port	Purpose
TCP 15505	When the Enable Mobile App toggle is in the ON position, `ProxyD` connects to the Spacebridge / Automation Broker automatically at `grpc.prod1-cloudgateway.spl.mobi` to send the interprocess communication from Phantom to the proxy.
TCP 443	Spacebridge communication port. Outbound open
Others	See Prerequisites in the Install and Administer Splunk Cloud Gateway guide.

향상된 Splunk Enterprise Search

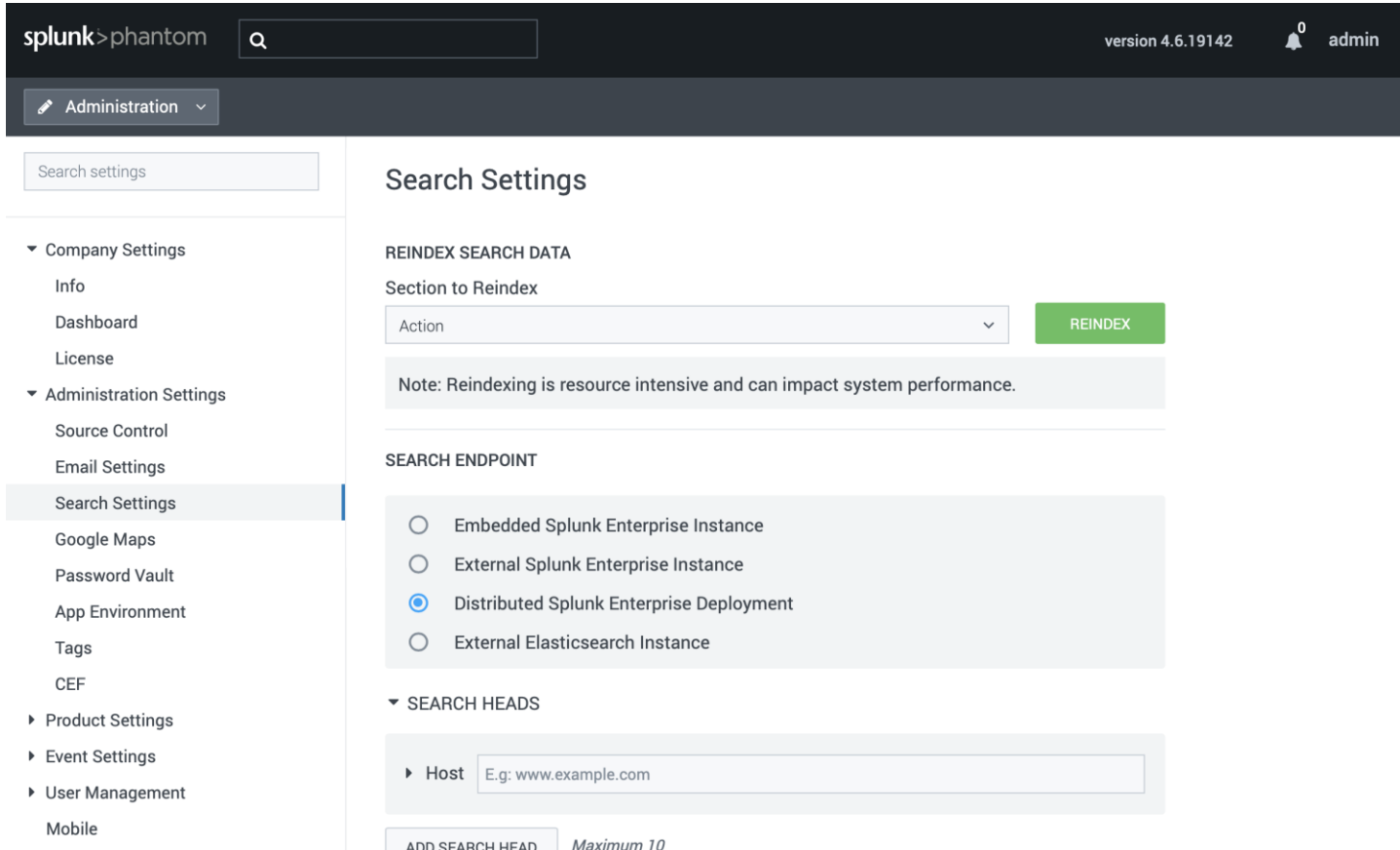
Splunk Phantom은 외부 Splunk Enterprise 인스턴스와 SHC 등 분산 환경을 지원합니다.

Configure search in

Main Menu > **Administration** >

Administration Settings >

Search Settings.



어떻게 동작하는가?

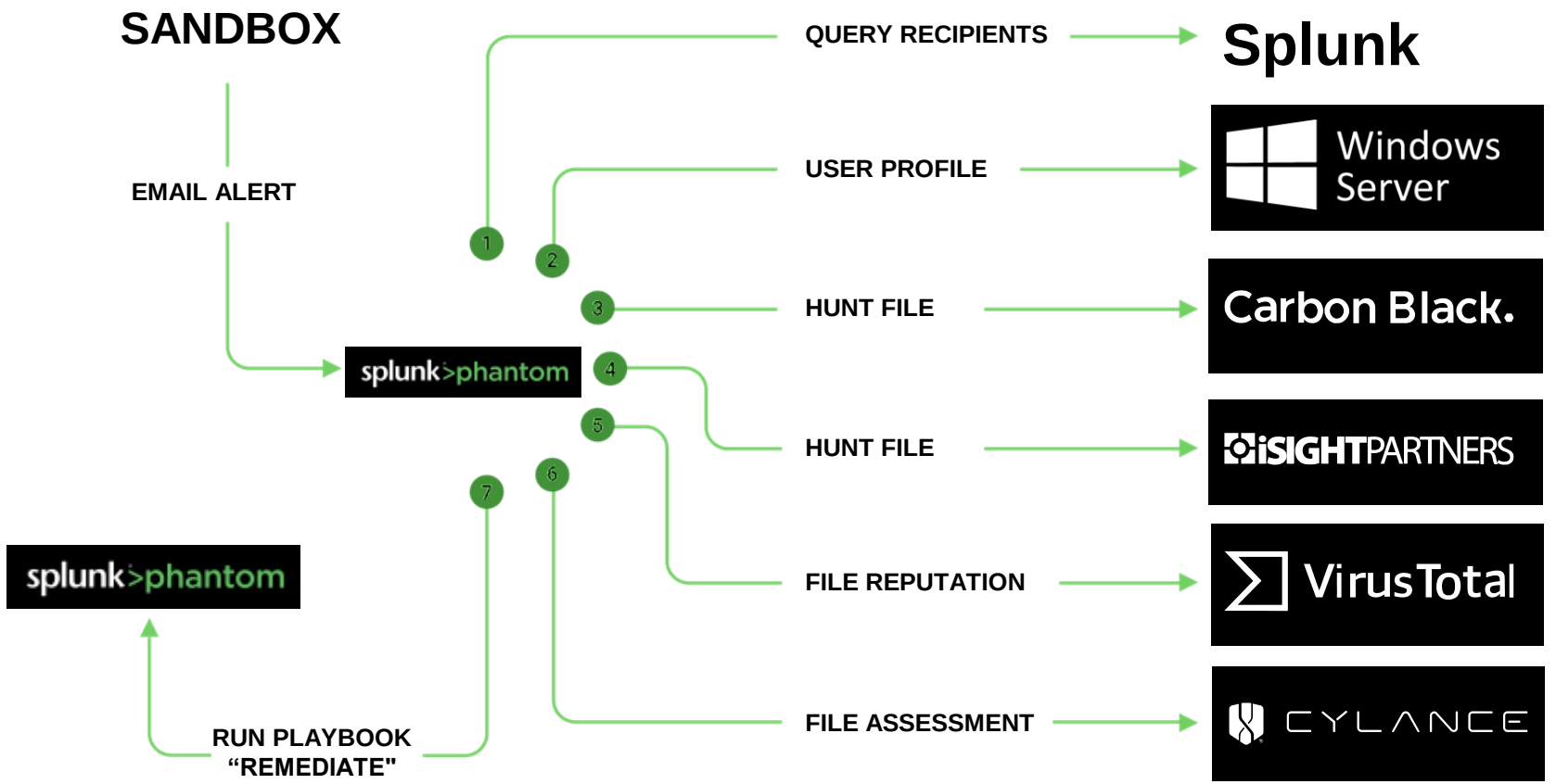
고객 팬텀 활용사례 : Blackstone

자동화된 말웨어 조사분석

"말웨어 이메일 경보를 팬텀으로 자동화하여 기존에 30분 이상 소요되던 작업을 40초로 단축하였다."

아담 플래처
CISO

Blackstone

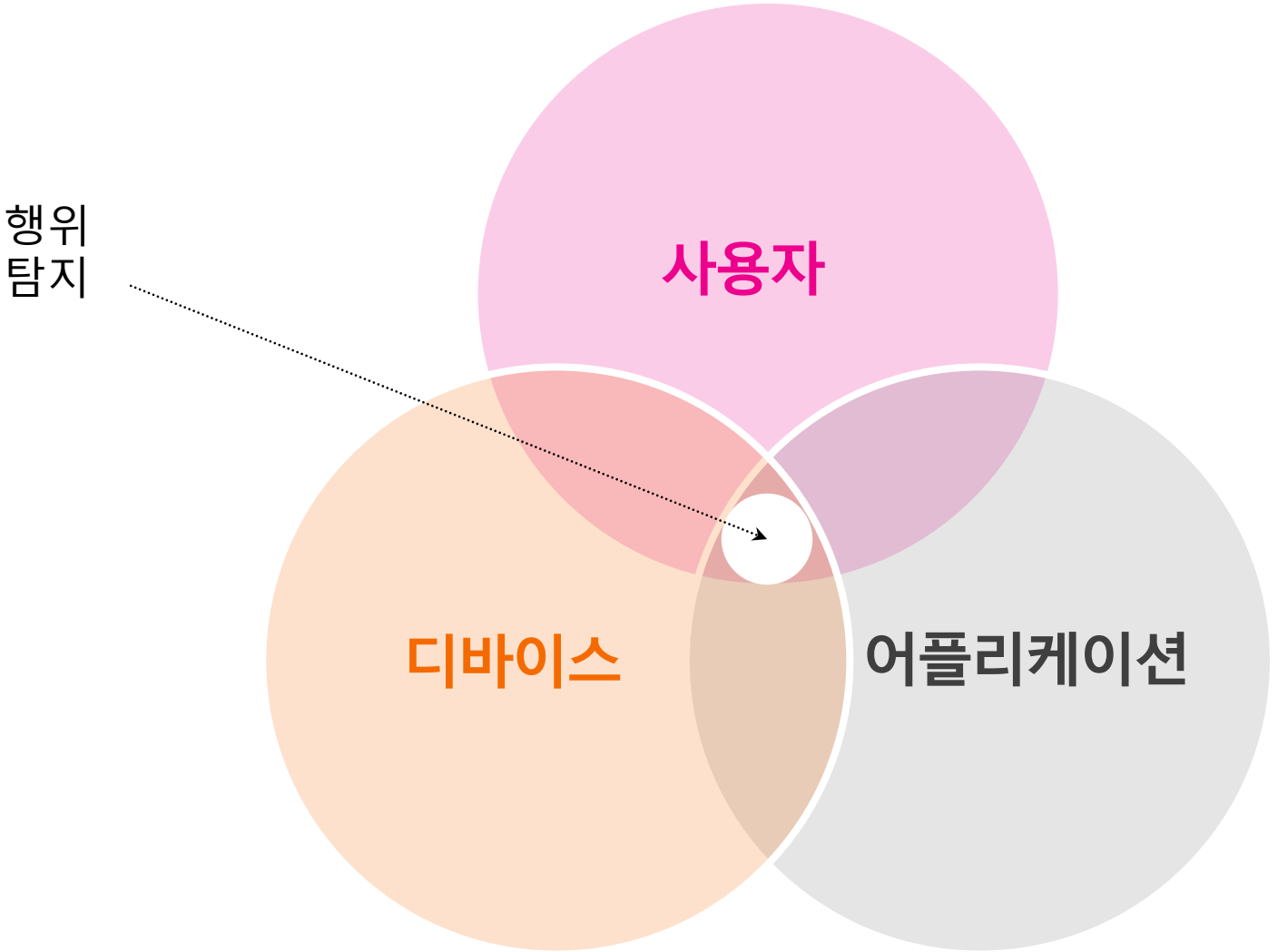


UBA 5.0

User Behavior Analytics

splunk> turn data into doing™

UBA는 단순히 사용자만을 의미하지 않습니다.



핵심 유즈케이스

A. 침해된 사용자 계정 탐지

B. 데이터 유출 탐지

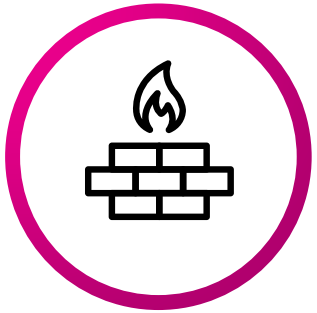
C. 침해된 엔드포인트 탐지

D. 권한 남용을 포함한 내부자의 접근 오남용

E. 조사를 위한 정보 제공

데이터 소스

네트워크



엔드포인트

서버

신원

클라우드 앱

어플리케이션

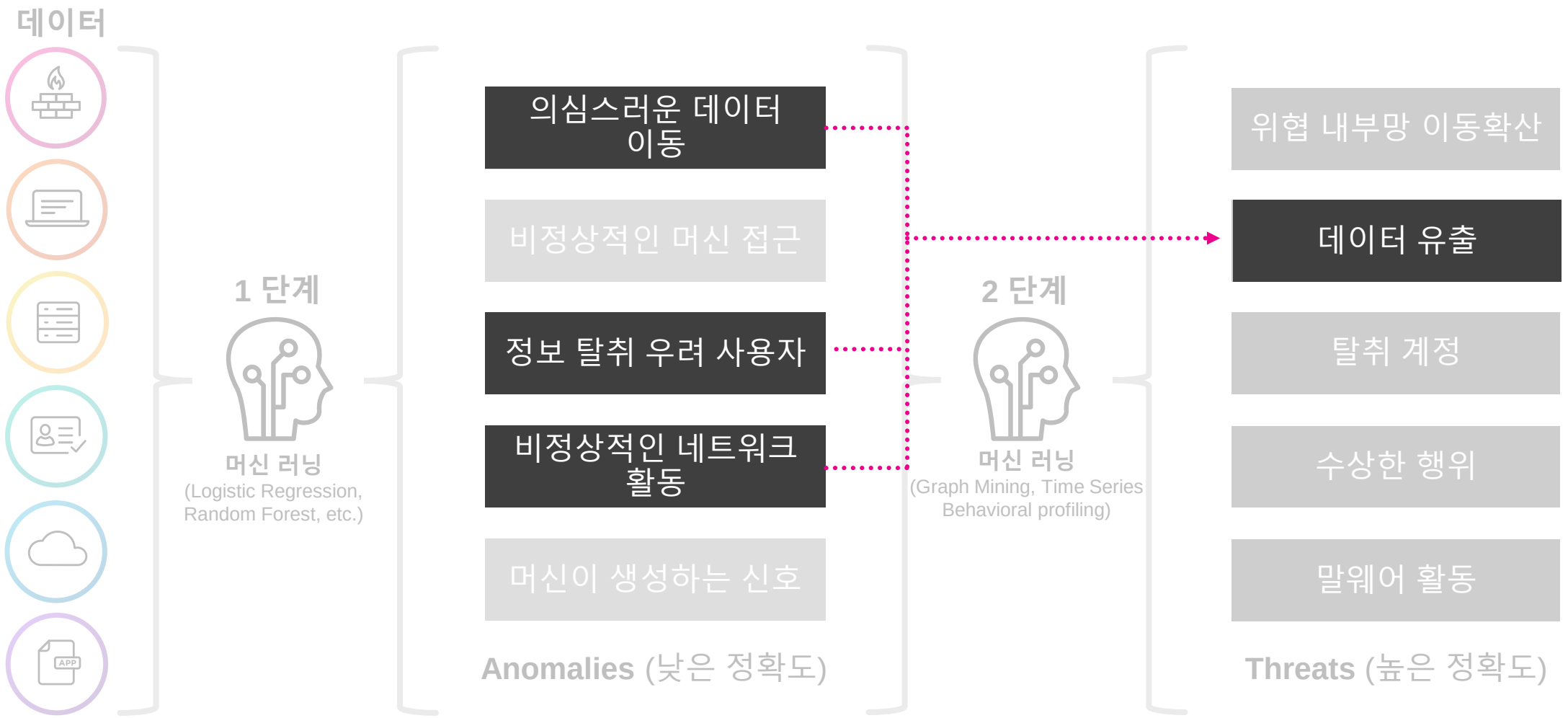
방법

임계치

통계

머신 러닝

왜 Splunk UBA 인가?



Splunk UBA 프로세스

무엇이 필요한가?

데이터 플랫폼

splunk>

Splunk Enterprise Security™

데이터 소스

- Active Directory
- DNS, DHCP
- Firewall
- Web Proxy

최소

- VPN
- Endpoint
- DLP

옵션

사양

CPU: 16 Cores

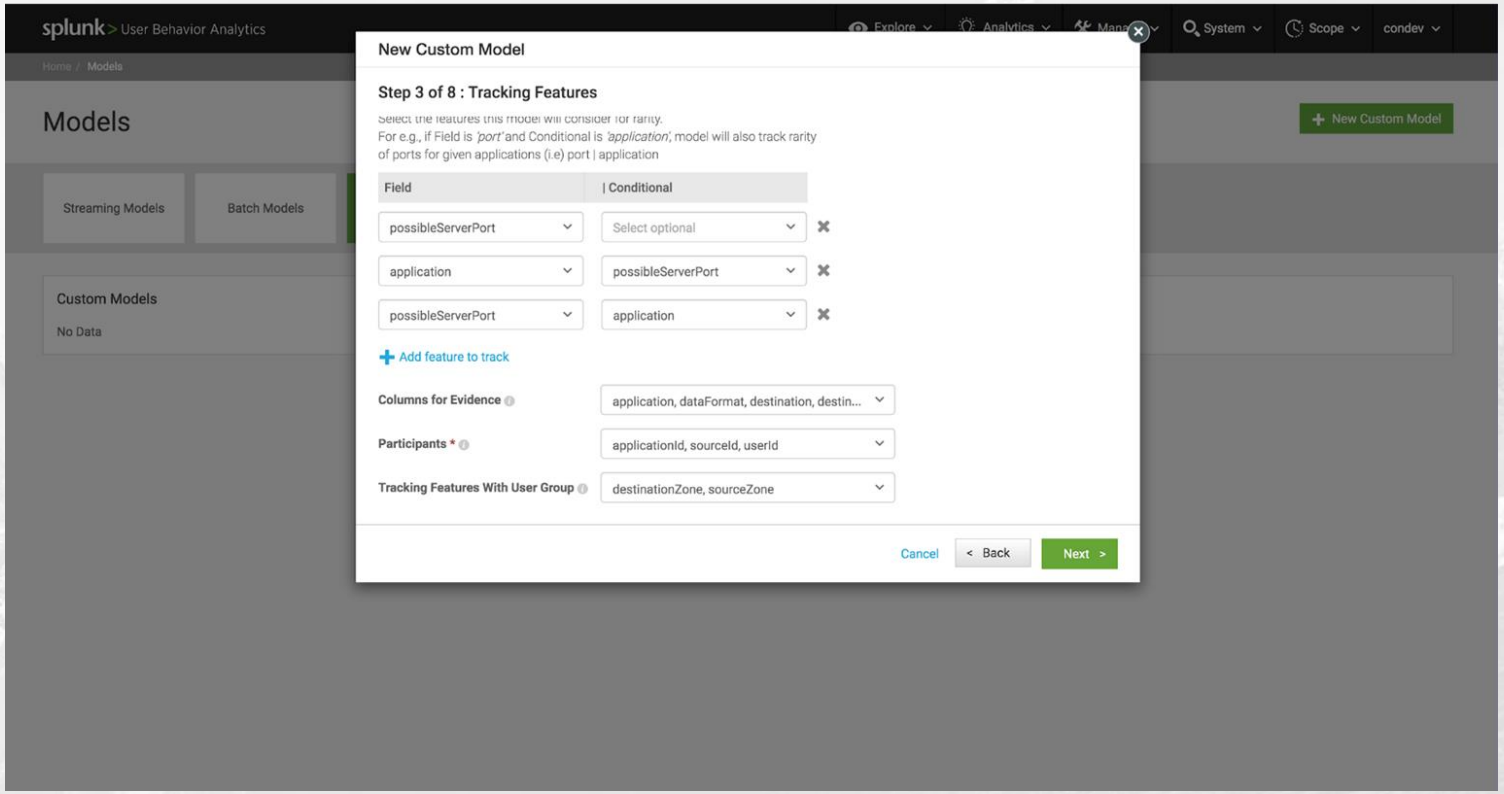
Memory: 64GB

Disk: 1200 IOPS

최소

Splunk User Behavior Analytics 5.0

1) 커스텀 ML 모델
2) HA/DR 웜 스텐바이
3) 향상된 디바이스 관리



탐지

예측

splunk> turn data into doing

Splunk User Behavior Analytics 5.0

데이터 카테고리 범위

4

신규

클라우드 파일 공유
(Onedrive, Sharepoint, Box)
데이터베이스, 물리적인 배지 접근,
프린터

HA/DR 웜 스탠바이

연속 백업

Splunk 보안 포트폴리오

Splunk + Phantom은 최신 SOC 구현을 위한, 세계 최고의 데이터, 분석 및 운영 플랫폼 제공

데이터

splunk>cloud™
splunk>enterprise

분석

splunk> Security Essentials

Splunk Enterprise Security™

ES CONTENT UPDATE

Splunk User Behavior Analytics™

Machine Learning Toolkit (MLTK)

운영

Phantom

Splunk Enterprise Security™

ADAPTIVE RESPONSE

협력적인 SOC로 강화

보안에 대한 중추신경센터

협력적인 SOC

보안 운영 수립

여러 도메인을 거쳐 해결함

특정 문제

상호 연결된 보안 스택

Splunk Enterprise Security™

ADAPTIVE RESPONSE

자동화 와 오케스트레이션

Phantom

AUTOMATION
ORCHESTRATION
COLLABORATION
EVENT MANAGEMENT
CASE MANAGEMENT
REPORTING & METRICS

인간의 기술을 향상 시키는 기계 학습

Splunk User Behavior Analytics™

Thank You

splunk> turn data into doing™