

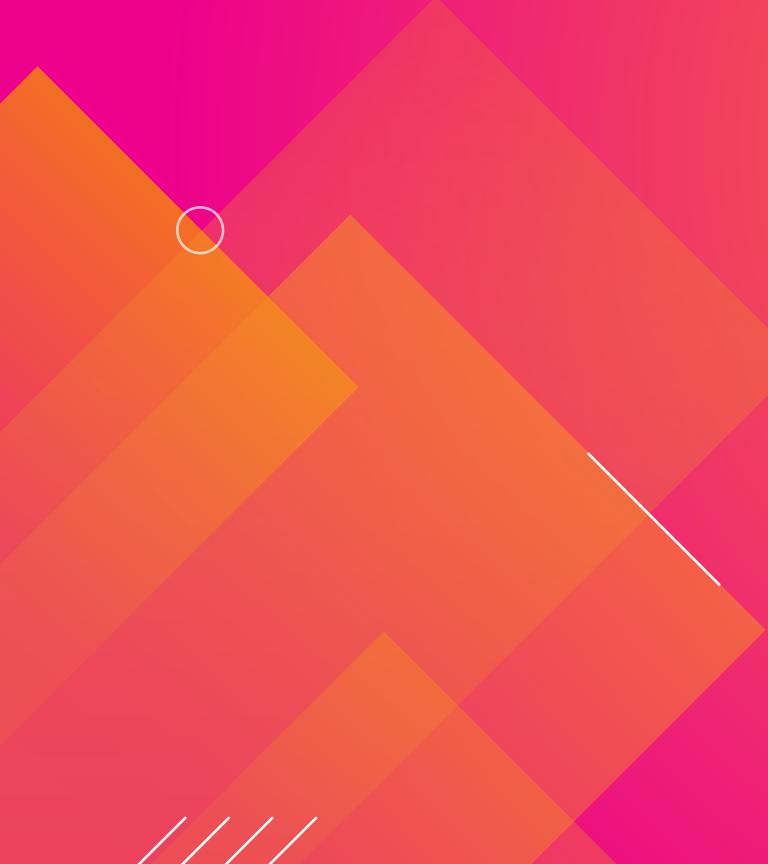
Splunk for Security

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 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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

What's New in .conf2019

2019년 스플렁크의 새로운 기술 포트폴리오

Platform



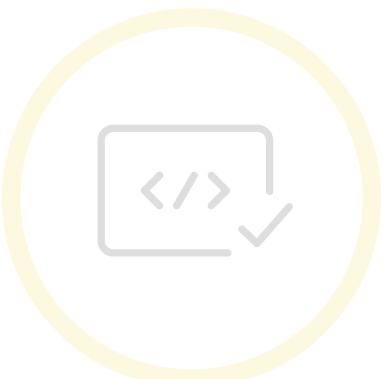
Splunk Enterprise
Connected Experiences
Splunk Machine Learning Toolkit
Splunk Cloud FedRAMP
Data Fabric Search
Data Stream Processor

IT Operations



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

DevOps



SignalFX
Splunk Investigate
VictorOps
Splunk Developer Cloud

Security



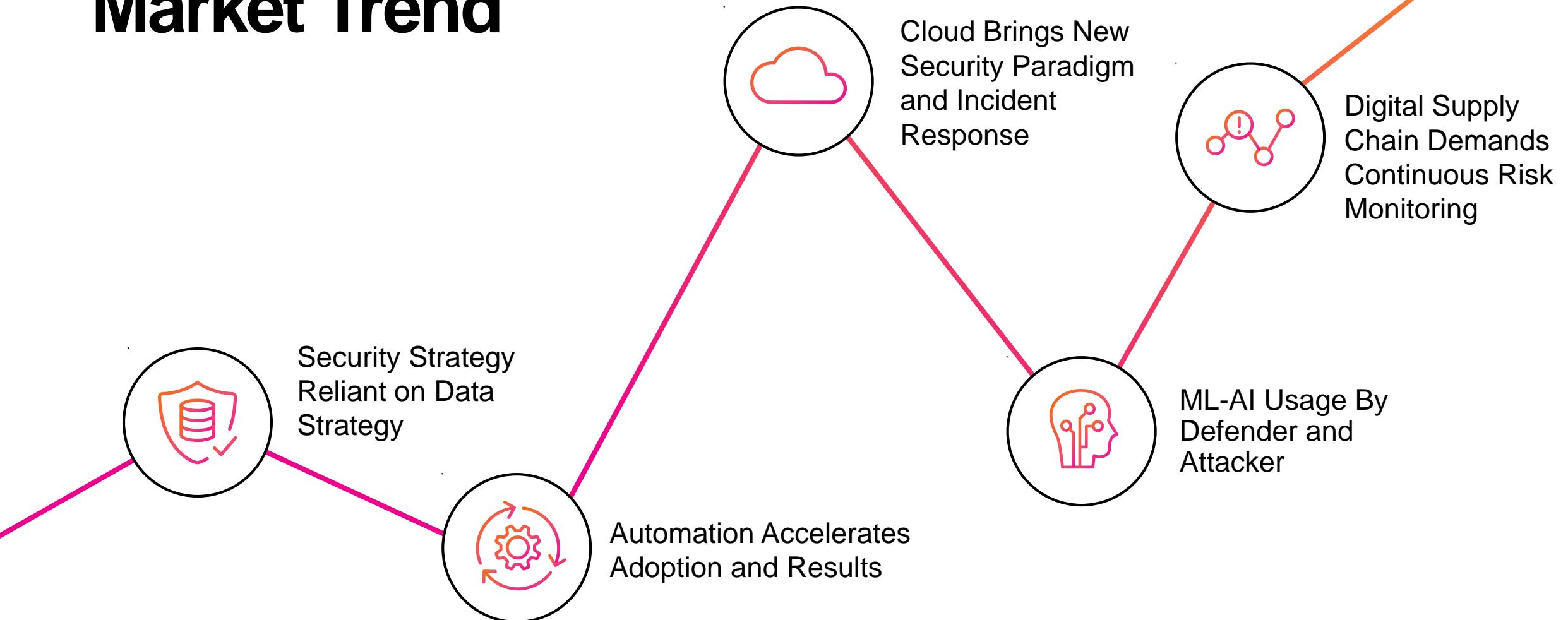
Splunk Enterprise Security
Splunk User Behavior Analytics
Splunk Phantom
Splunk Mission Control

Splunk Security Operations Suite

Innovations

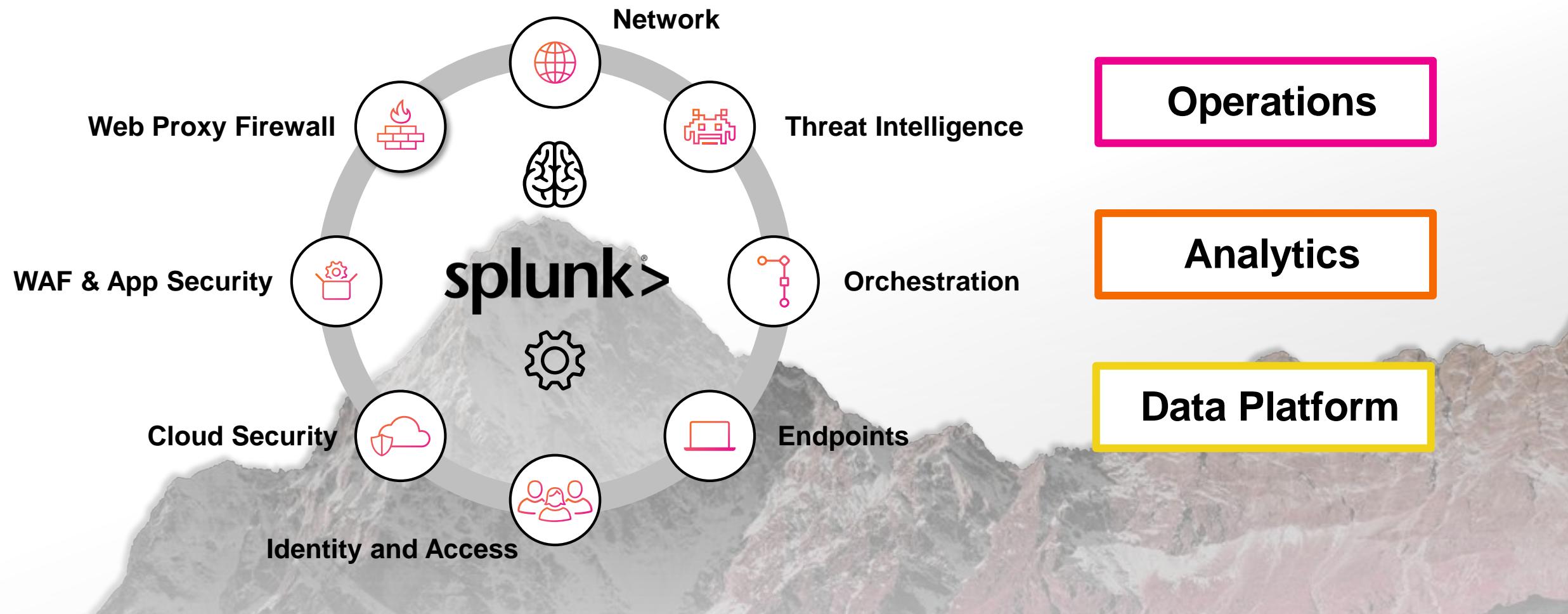


Market Trend



Splunk as the Security Nerve Center

Optimize People, Process and Technology



Journey to the Nerve Center

Making the Vision Real for Security Operations

Nerve center for security



Power a collaborative SOC



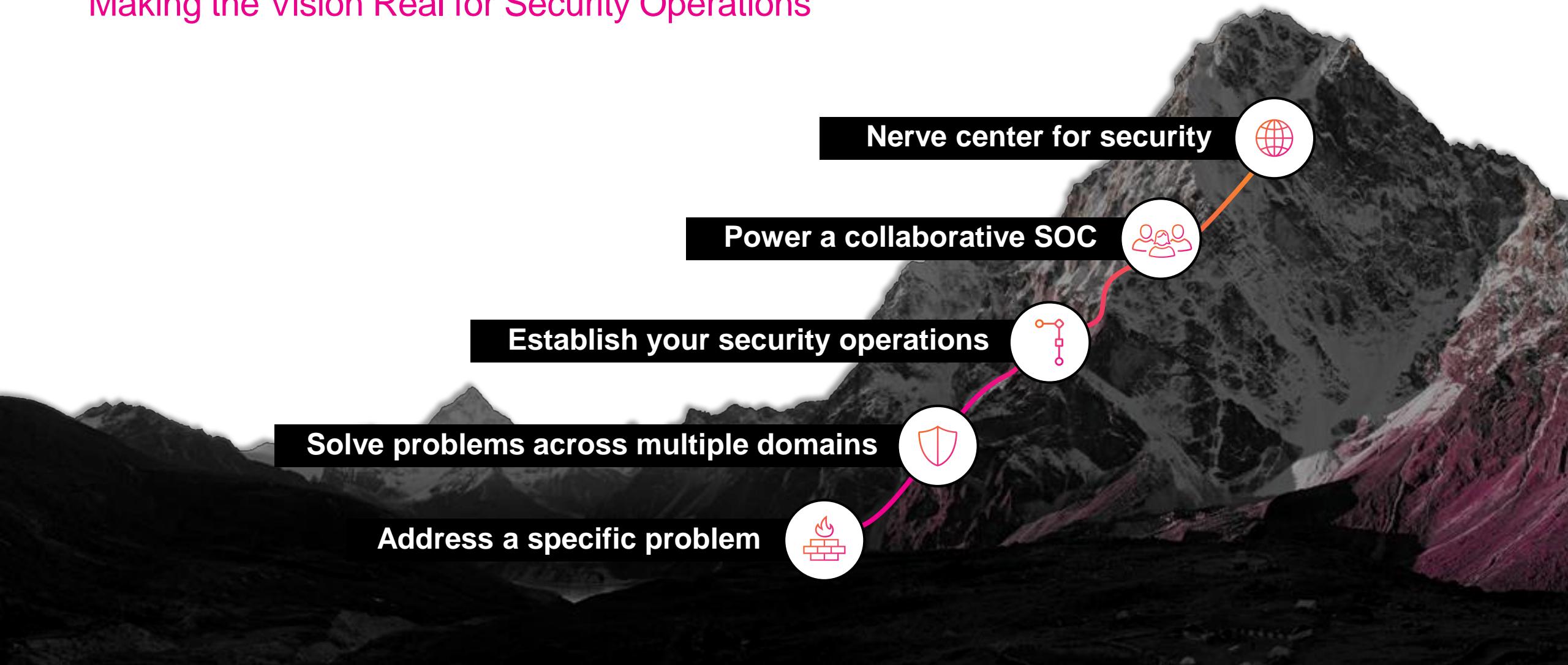
Establish your security operations



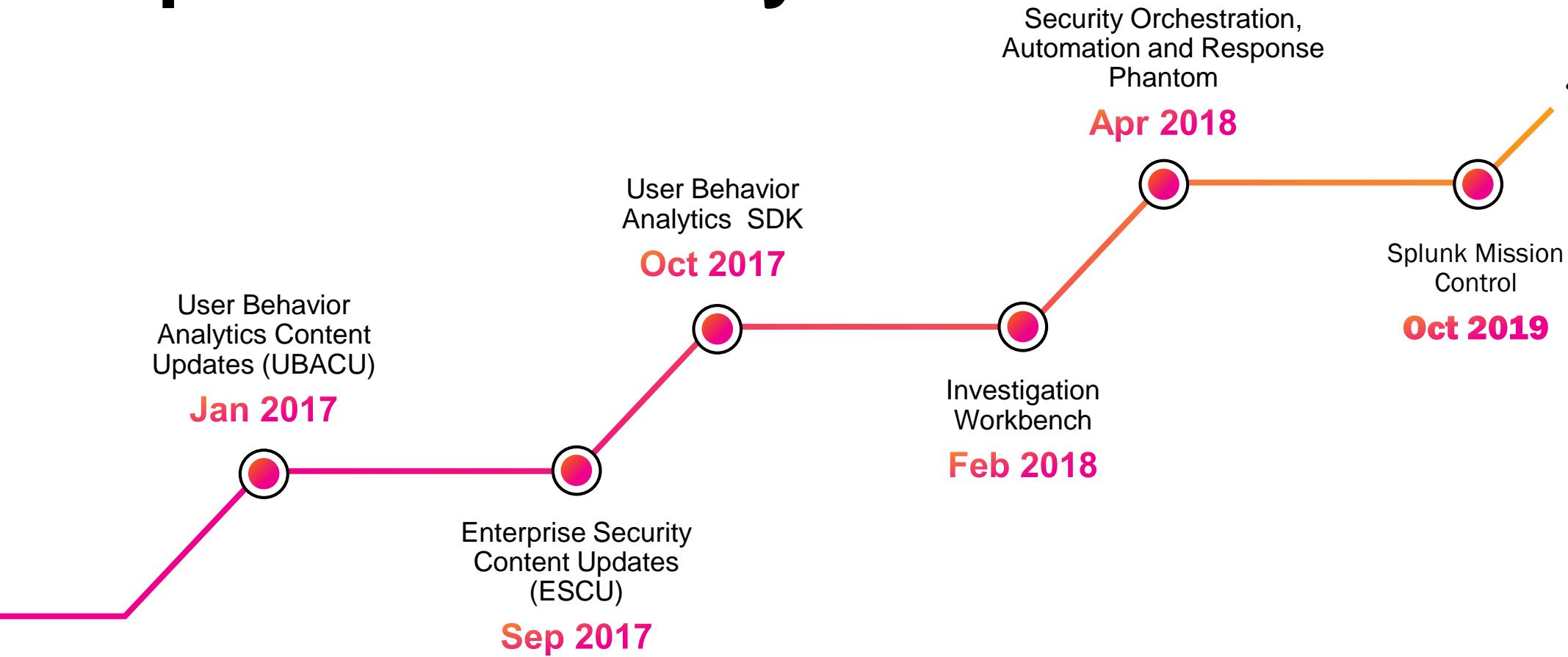
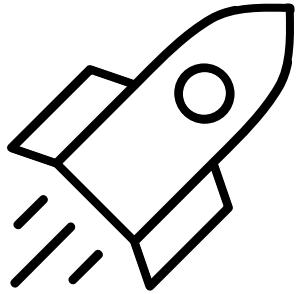
Solve problems across multiple domains



Address a specific problem



Splunk for Security





ANNOUNCING

Mission Control *Beta*

State of Security Operations



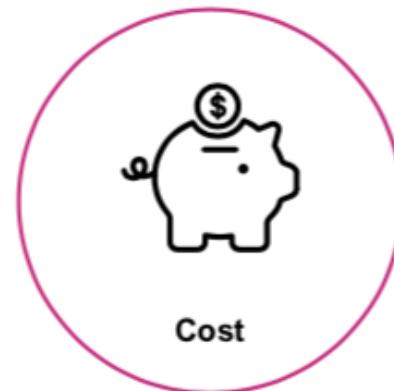
Tools



Alerts



Hiring



Cost



Education



Adversaries



Techniques



Users & Devices

What is our Objective?



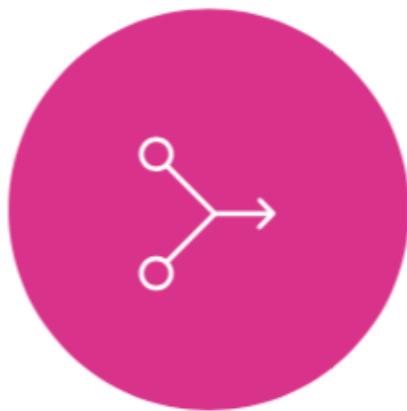
Change the
way SecOps are
managed



Prioritize the
analyst
experience first



Optimize for
hybrid
environments



Unify and
simplify



Improve
security
effectiveness

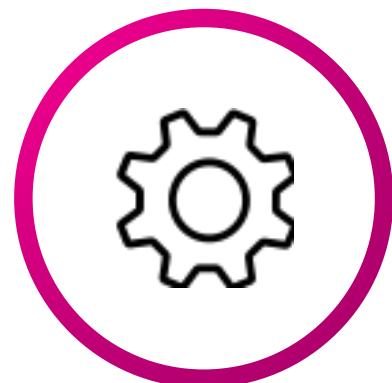
Splunk Mission Control

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



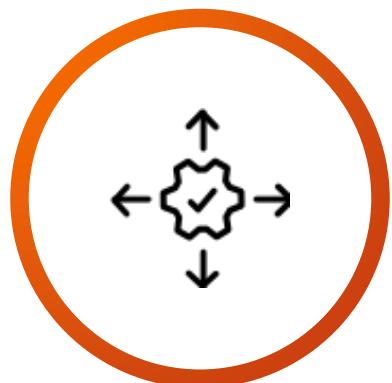
Benefits of Splunk Mission Control

Recover Time Spent



- 통합된 자동화
- 컴퓨팅 속도로 플레이
- 북 실행

Improve Response



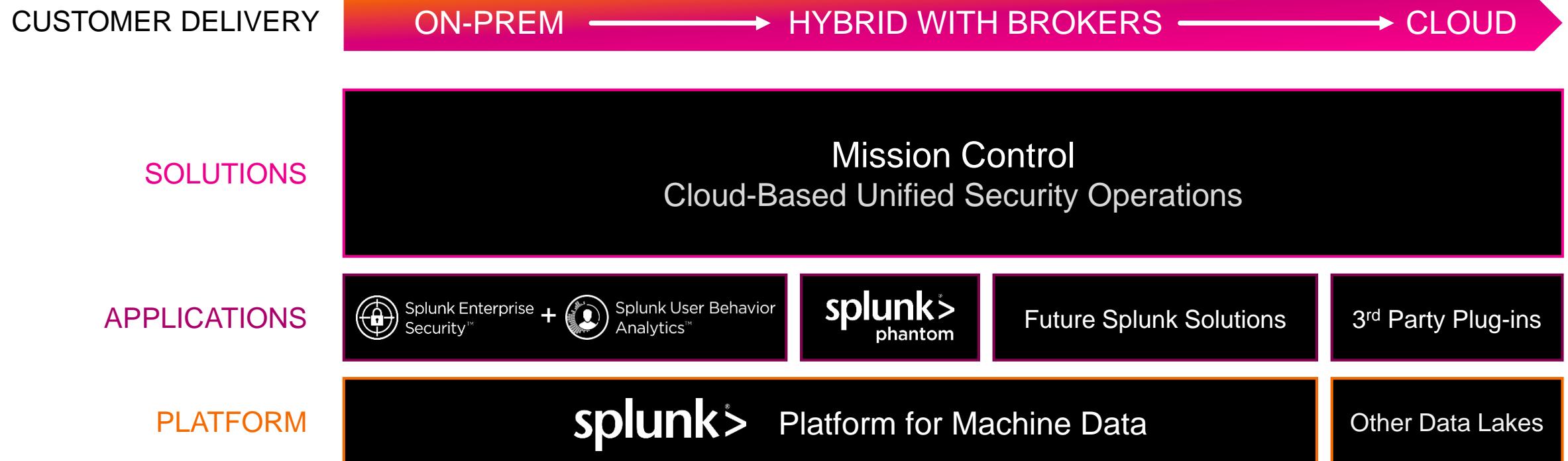
- 보안 대응 계획 모델링
- 대규모 보안 운영 감사

Optimize SOC

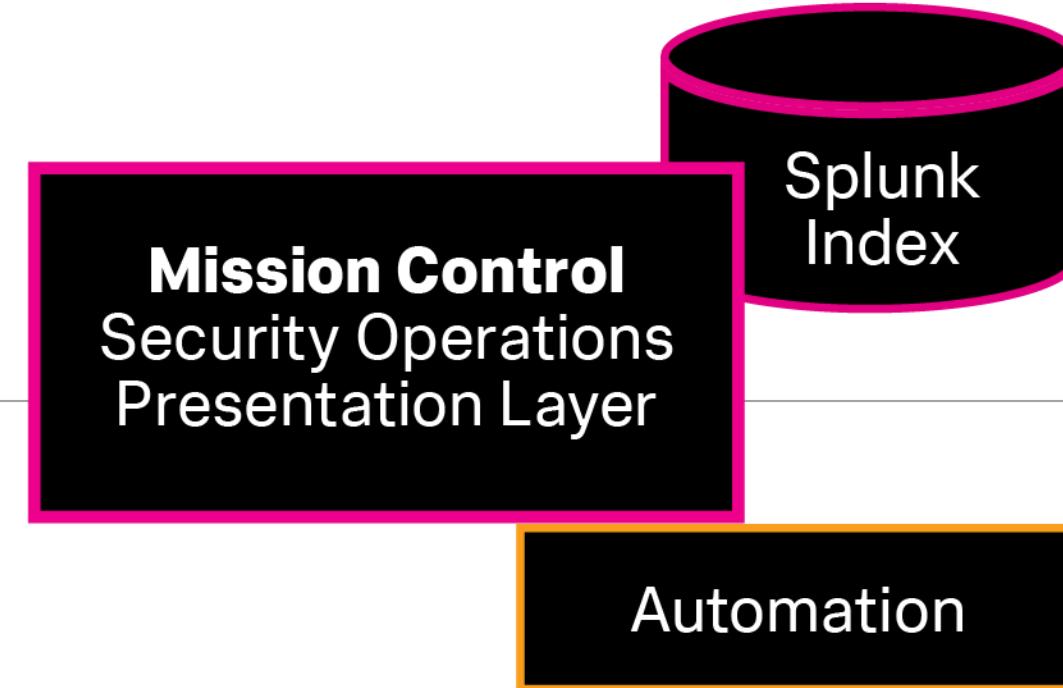


- 하나의 작업 영역에서
- 위협 탐지 및 조사

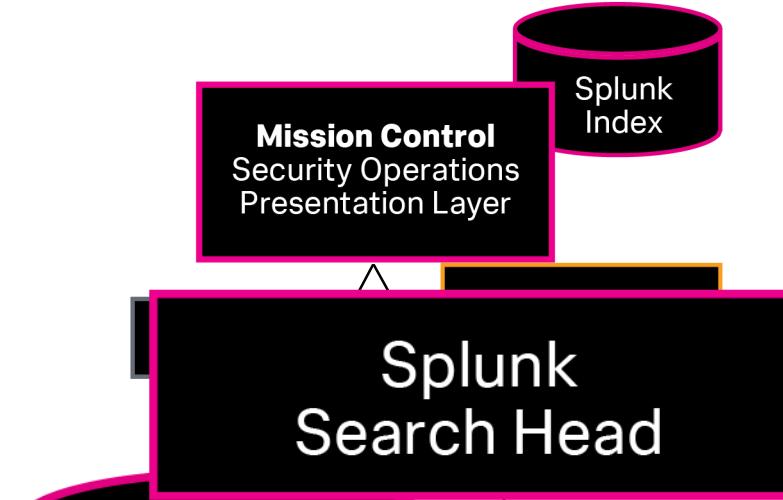
Security Operations Suite Architecture



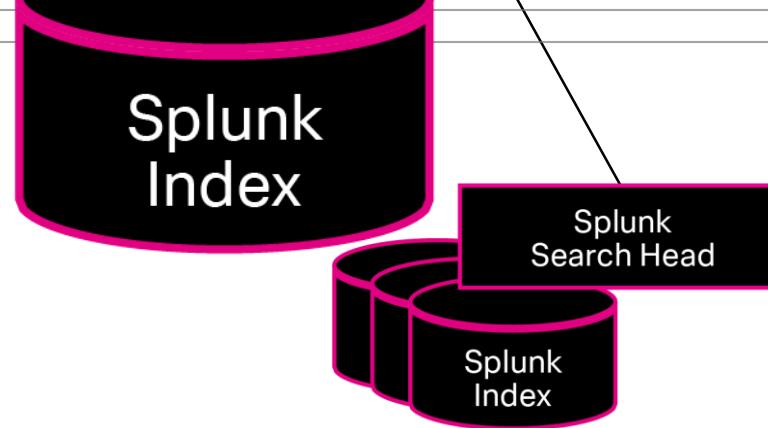
CLOUD



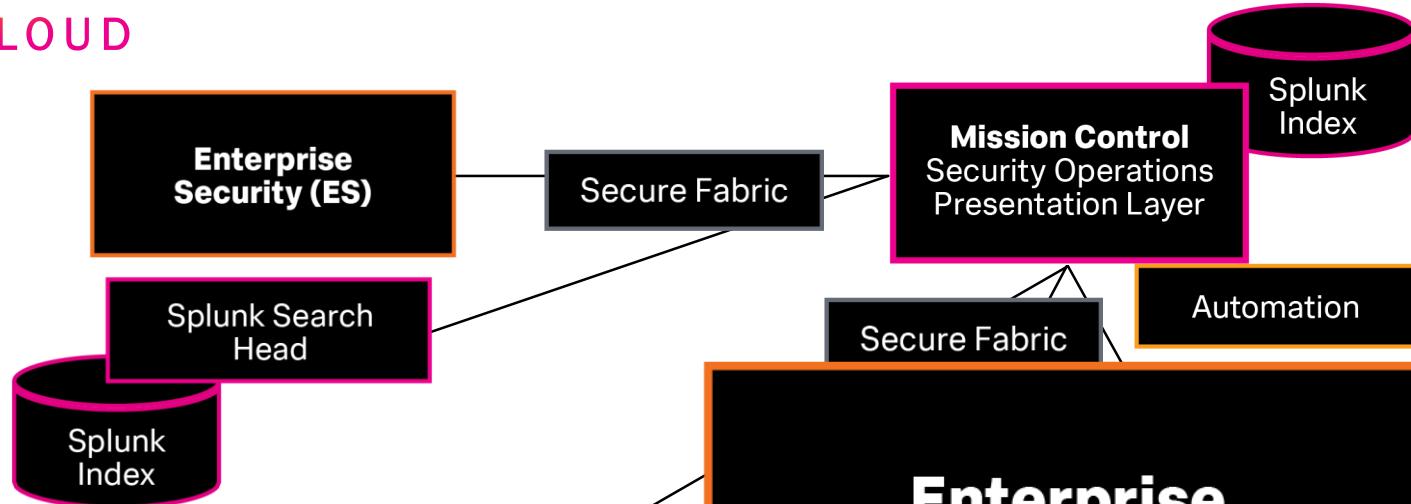
CLOUD



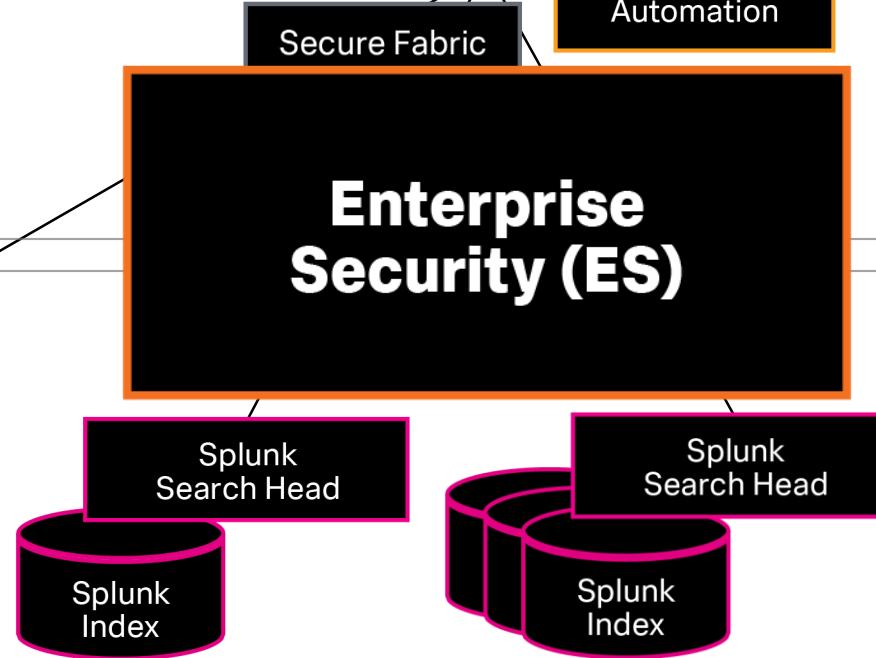
ON-PREM



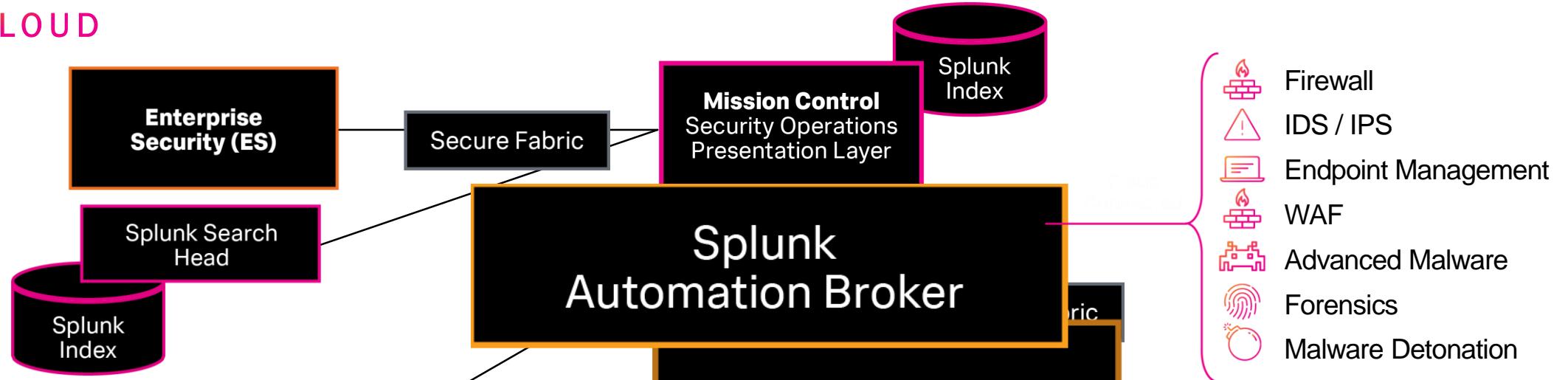
CLOUD



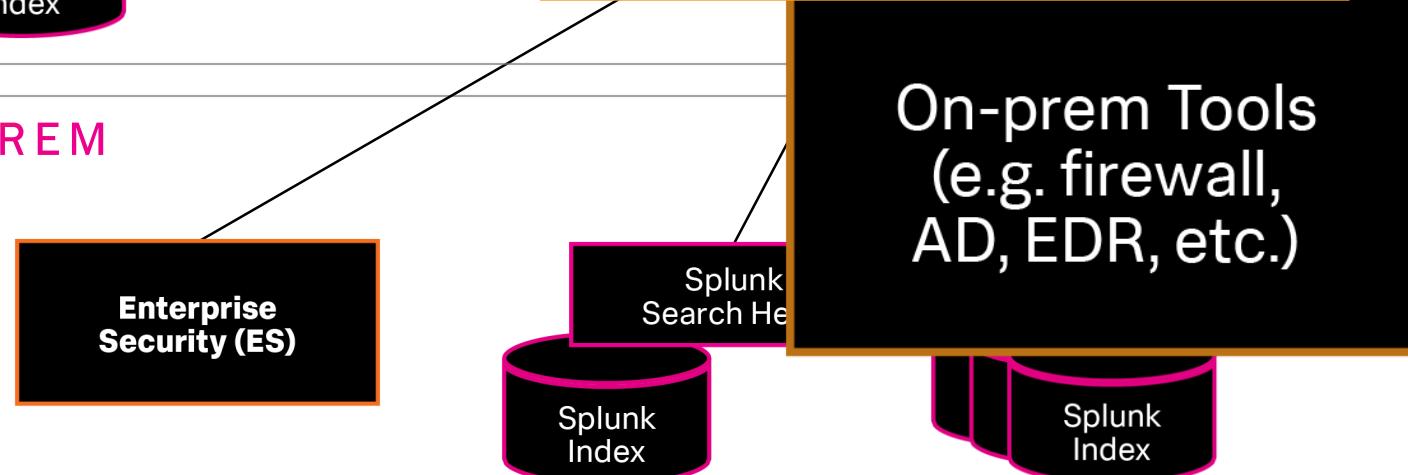
ON-PREM



CLOUD

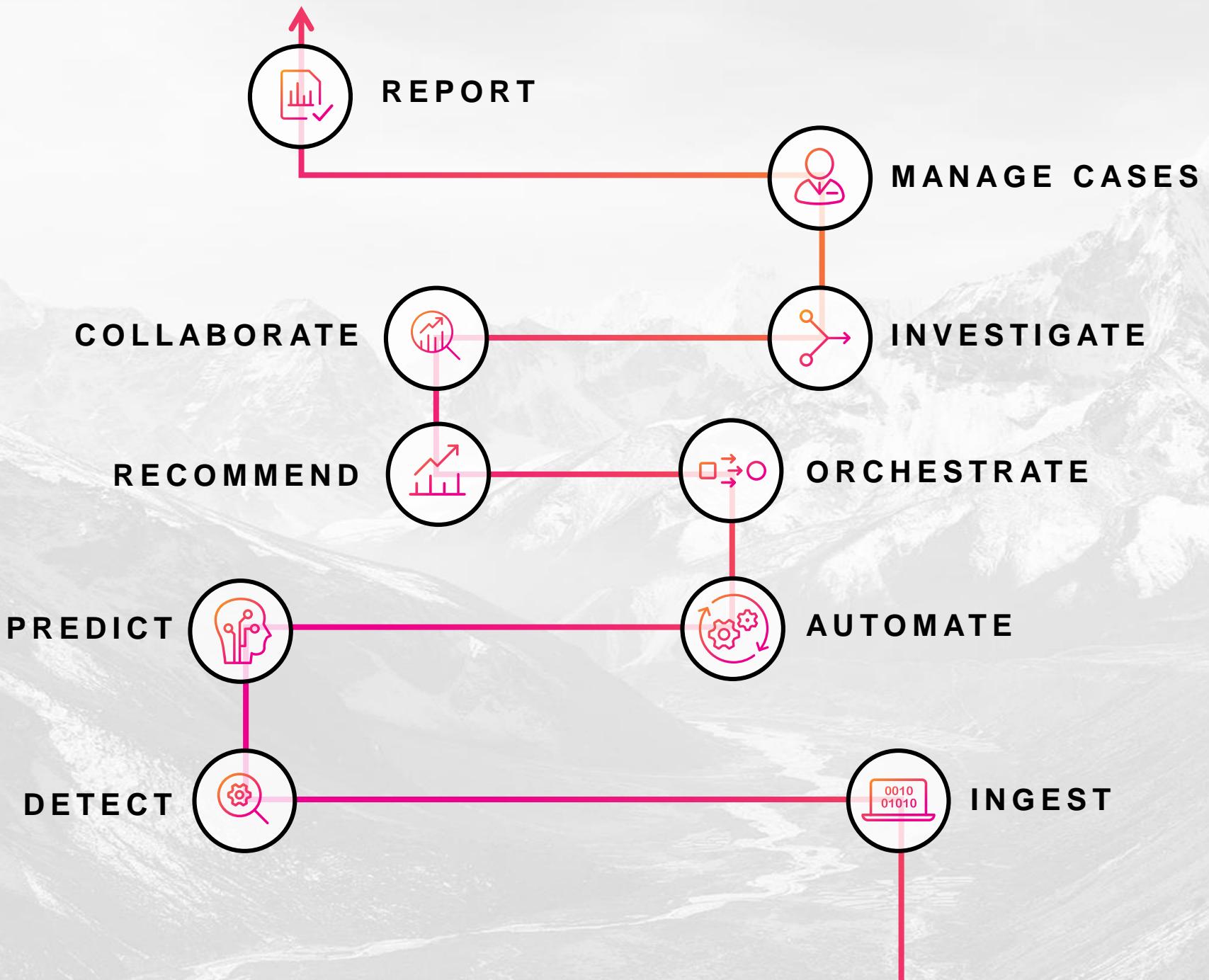


ON-PREM





ANNOUNCING Enterprise Security 6.0



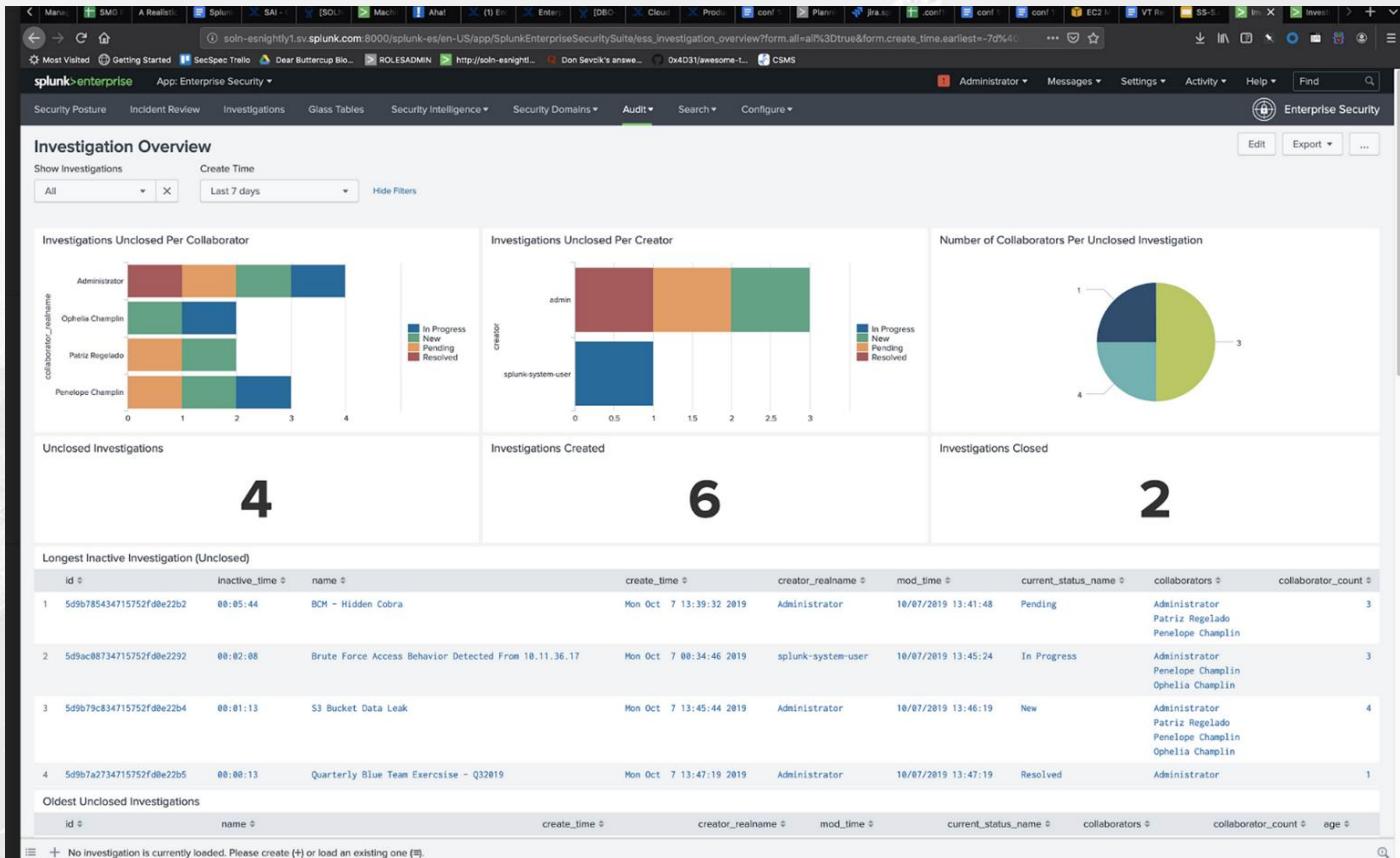
Artificial
Intelligence

Machine
Learning

Content

Splunk Enterprise Security

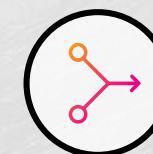
- Detect advanced threats
- Enrich with Analytics
- Analyze & investigate threats
- Enterprise-wide coordination & response



INGEST



DETECT



INVESTIGATE



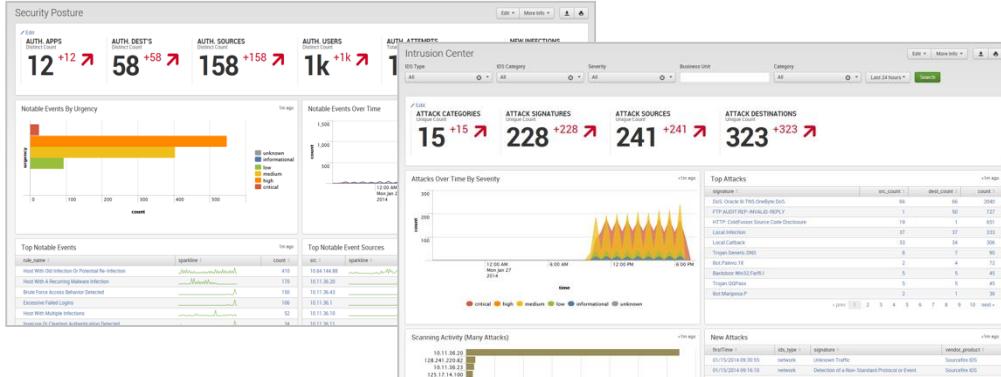
COLLABORATE



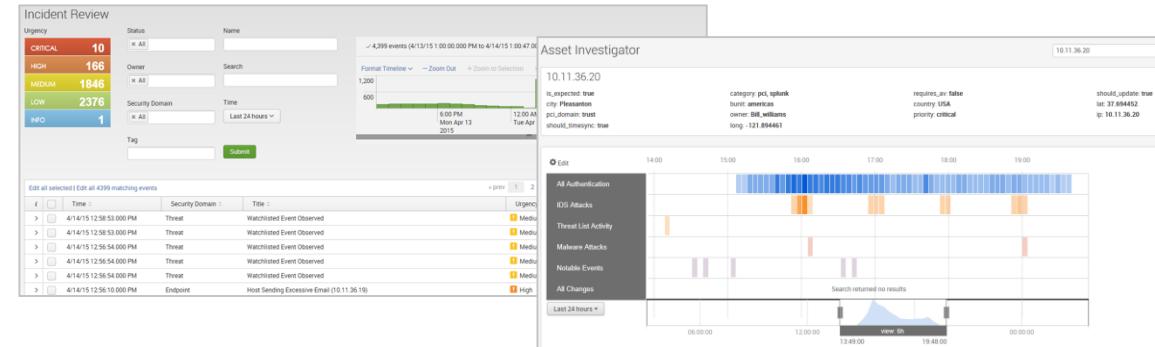
REPORT

Splunk Enterprise Security

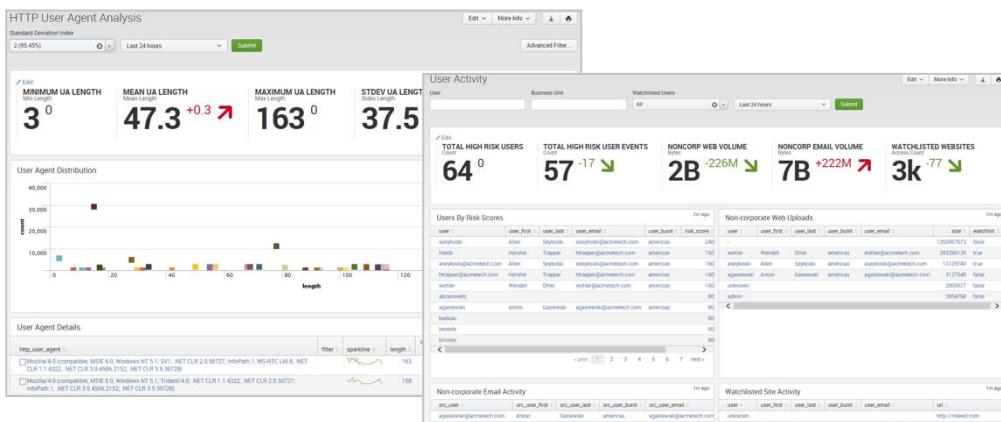
기본 탑재된 검색, 경고, 리포트, 대시보드, 인시던트 워크플로우, 위협 피드



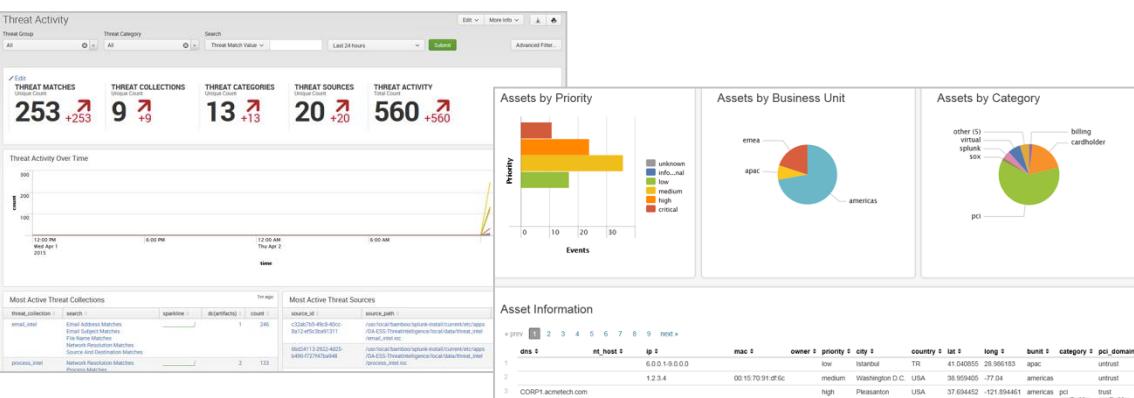
경고 & 대시보드 & 리포트



사고 조사 및 관리



통계적 이상치 & 위험 점수 & 사용자 활동



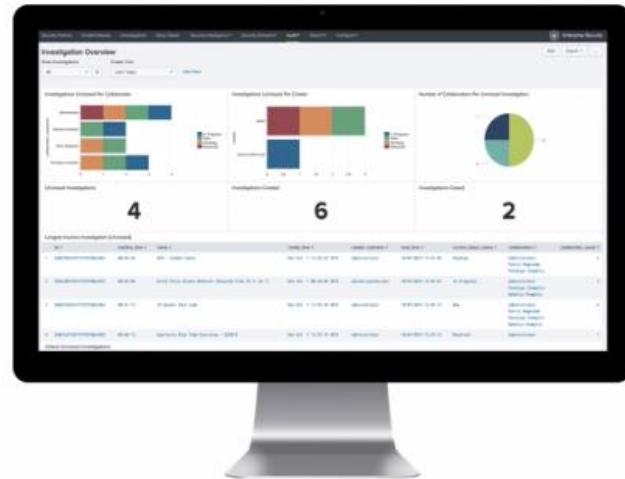
위협 인텔리전스 & 자산 & 신원정보 통합

splunk > turn data into doing

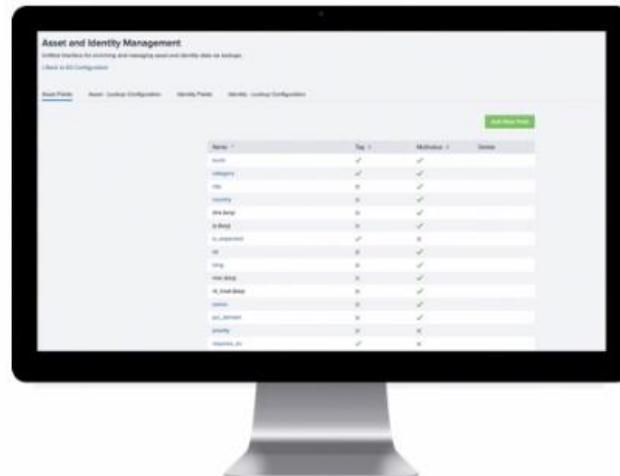
Splunk Enterprise Security 6.0

Key Enhancements

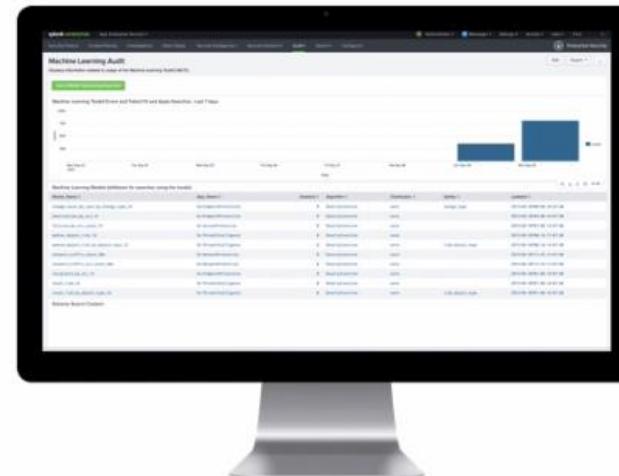
Analytics Reporting on Investigations



Asset and Identity Framework Enhancements



Splunk Machine Learning Tool Kit (MLTK) Integration



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

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

- 40% 처리 속도 증가
- 20% CPU 리소스 절감

Demo

Enterprise Security

Incident Review

Urgency	Status	Correlation Search	Sequenced Event
CRITICAL	11	Select...	Select...
HIGH	97		
MEDIUM	2112		
LOW	605		
INFO	0		
Owner		Search	
Select...			
Security Domain		Time	Associations
Select...		Last 24 hours	
Tag		<input type="button" value="Submit"/>	
Type...			



i	<input type="checkbox"/>	Time	Urgency	Security Domain	Title	Status	Owner	Actions
>	<input type="checkbox"/>	5/17/19 4:01:38.000 AM	⚠ Medium	Audit	Personally Identifiable Information Detected	New	unassigned	▼
>	<input type="checkbox"/>	5/17/19 4:00:21.000 AM	⚠ Critical	Threat	“^v” Phishing Attack Detected on Compromised Host	New	unassigned	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	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	▼
>	<input type="checkbox"/>	5/17/19 3:40:19.000 AM	⚠ Medium	Network	Unroutable Activity Detected (0.19.255.27)	New	unassigned	▼
>	<input type="checkbox"/>	5/17/19 3:40:14.000 AM	⚠ Medium	Network	Unroutable Activity Detected (0.187.34.141)	New	unassigned	▼
>	<input type="checkbox"/>	5/17/19 3:40:14.000 AM	⚠ Medium	Network	Unroutable Activity Detected (0.76.78.172)	New	unassigned	▼
>	<input type="checkbox"/>	5/17/19 3:40:14.000 AM	⚠ Medium	Network	Unroutable Activity Detected (0.114.71.104)	New	unassigned	▼
>	<input type="checkbox"/>	5/17/19 3:39:38.000 AM	🟢 Low	Access	Default Account Activity Detected	New	unassigned	▼
>	<input type="checkbox"/>	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?



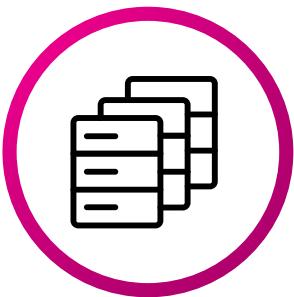
보안 운영 문제

자원



보안 전문가의
자원 부족

제품



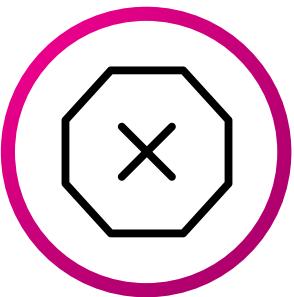
단위 보안
제품들의
끊임없는 연동

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



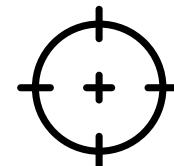
Tier 2
위협 대응



Tier 3
위협 대응



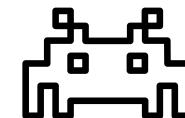
피싱 이메일
조사



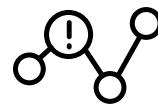
위협 사냥



위협
인텔리전스



말웨어
조사



이벤트
선별



내부자 위협
분석팀

관리



SOC 팀장



CISO



팀 성과



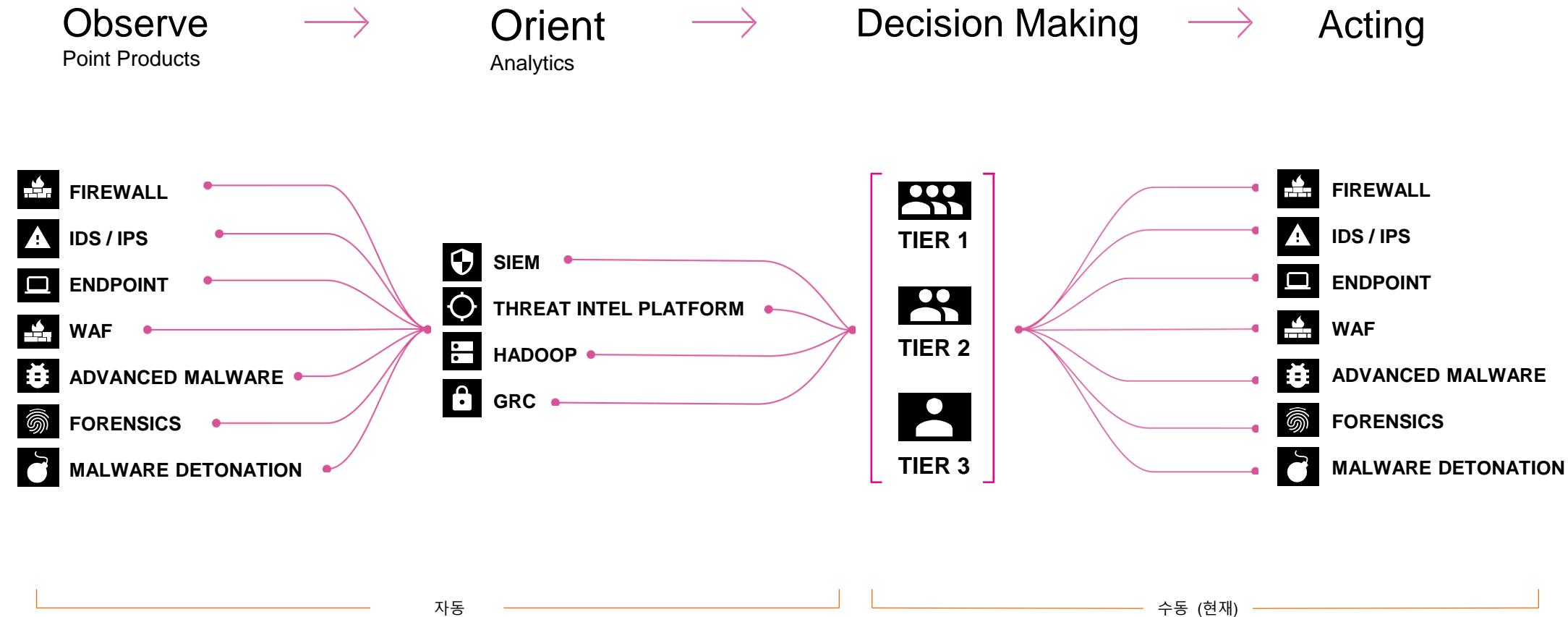
프로세스 & 운영



메트릭 & 리포팅

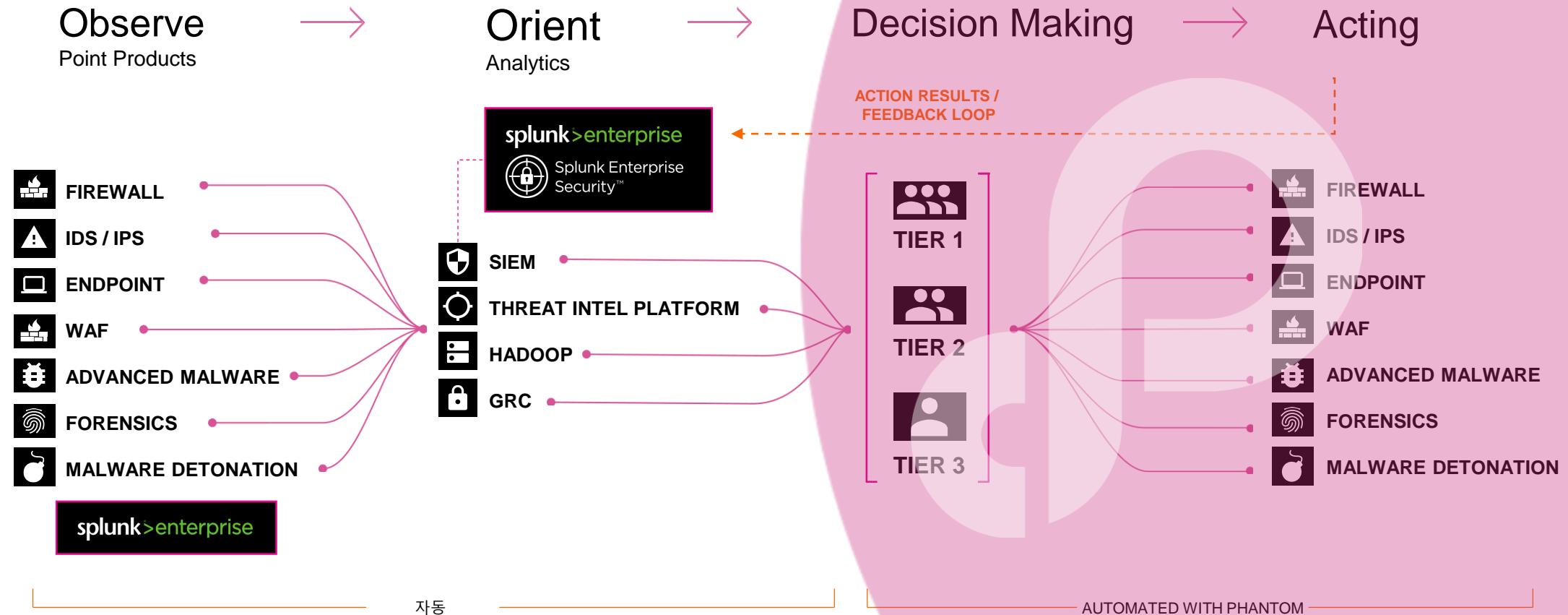
보안운영을 위한 SOAR

OODA 루프를 통한 빠른 실행으로 보안 향상



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

The screenshot shows the Splunk Phantom 4.6 investigation interface. At the top, there's a header with 'splunk>phantom' and a search bar. Below it, a banner displays 'events ID: 2284' with status indicators (red, yellow, green), followed by 'DNS query length outliers in 10.41.24.12'. The main area is titled 'INVESTIGATION' and contains several sections: 'HUB' with 'IOC Count 5', 'Attached Host swift-3x-srvv001.buttercup.com', 'Malicious File Trojan-Banker.Win32.Alazy.gen', 'Detection Count 21', and 'Infection Time 152 minutes'; 'EVENT INFO' with details like 'Status: New', 'Playbooks Run: 1', 'Actions Run: 5', 'Artifacts: 2', and 'Owner: Sourabh Satish'; 'DETAILS' with 'Source ID: 40ff7694-ac83-44c5-b81e-09539053b9d1', 'Tag: ', and 'Description: '; and a 'Timeline' section showing a sequence of events: 'automation' (a few seconds ago) with steps 'Investigate domain_reputation_1', 'File Info run_command_1', 'Activity Started', 'Created on Phantom run_query_1', and 'geolocate_ip geolocation_1'; and 'Sourabh Satish' (a few seconds ago) with steps 'quarantine device', 'reset password', and 'create ticket'. The bottom of the interface features 'Widgets' and 'Notes' sections, along with 'REVERSING LABS' and 'Microsoft' integration panels.



자동화



오페스트레이션
(조정, 편성)



권장
(추천)



협업
(공동작업)



케이스 관리

Splunk Phantom 4.6

가장 큰 SOC

100
분석가

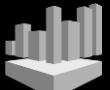
이벤트
처리

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.



DARKPOINT



NetBIOS



proofpoint



RSA Security Analytics

Screenshotmachine

Skype for Business

Symantec ATP



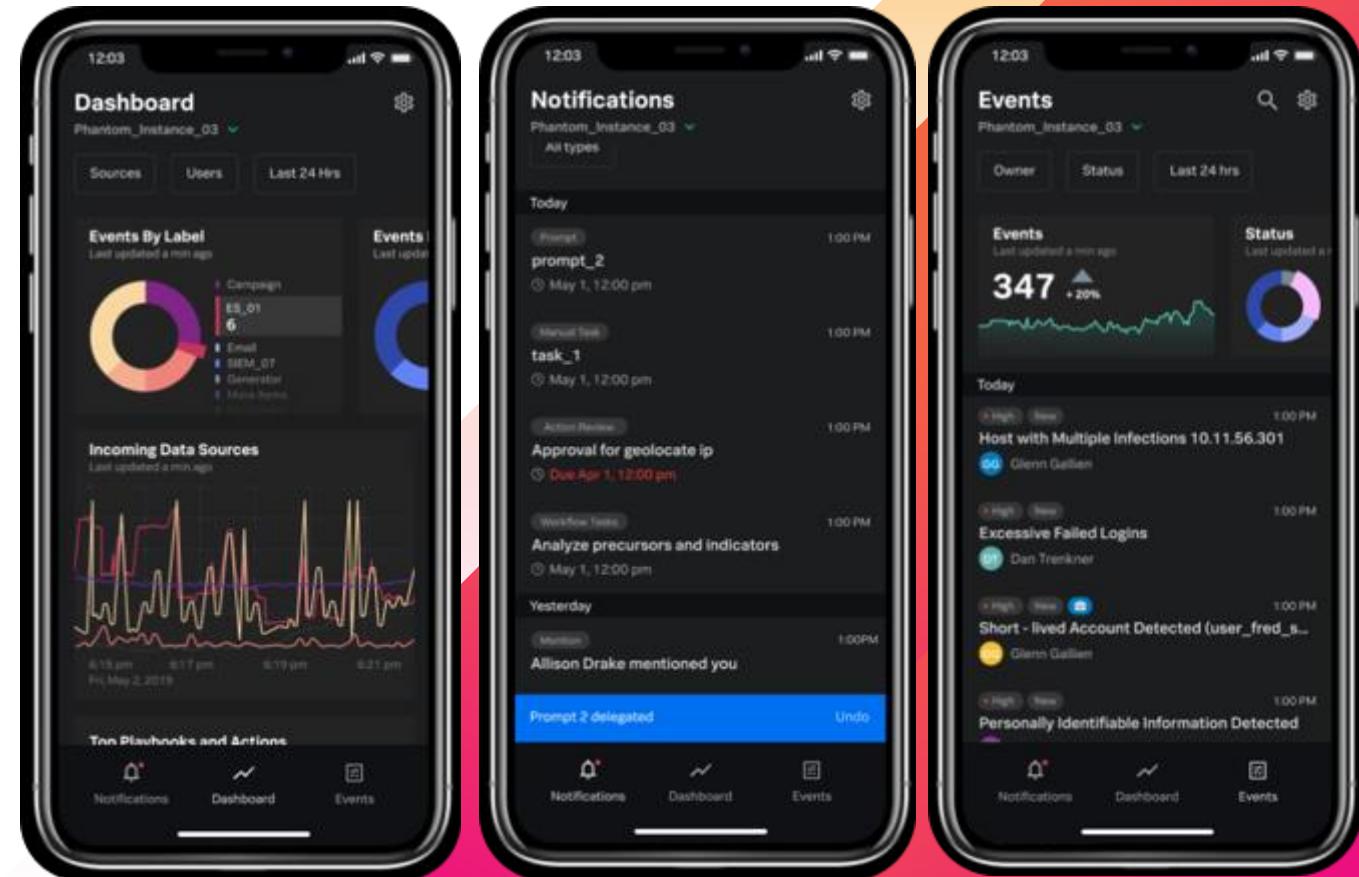
Windows Remote Management

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 Mobile App for Splunk Phantom(1/3)

설정방법

The screenshot shows the Splunk Phantom Administration interface. The top navigation bar includes the URL "splunk>phantom", a search bar, the version "version 4.6.19142", a notification icon with "0" notifications, and a user account "admin". The left sidebar has a "Administration" dropdown menu with options: Company Settings, Administration Settings, Product Settings, Event Settings, User Management, Mobile (which is selected and highlighted in blue), System Health, and About. A search bar labeled "Search settings" is also present in the sidebar. The main content area is titled "Mobile" and contains a section titled "Enable Mobile App" with a toggle switch set to "ON". Below this, a status message "All (0)" is displayed. A search bar labeled "Search devices" is located at the bottom of this section. A table header with columns "DEVICE NAME", "DEVICE TYPE", "OWNER", and "ACTION" is shown, followed by the message "No registered devices".

Splunk Mobile App for Splunk Phantom(2/3)

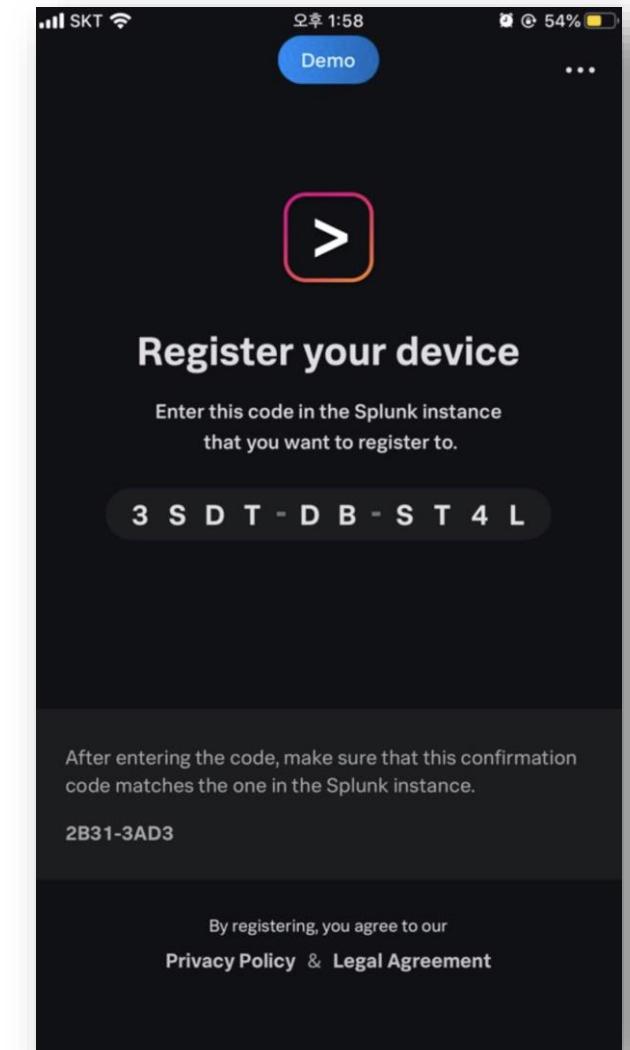
설정방법

The screenshot shows the Splunk Phantom web interface with the following details:

- Header:** splunk>phantom, version 4.6.19142
- Navigation:** Home, User Settings, Notifications, Change Password, Mobile Device Registration (highlighted)
- Section:** Registered Devices (yellow-bebhionn-pineapple)
- Table:**| DEVICE NAME | DEVICE TYPE | OWNER | ACTION |
| --- | --- | --- | --- |
| Max phone | iOS | admin | [remove](#) |

Add New Device Dialog:

- Enter the code from the device: - -
- Device name: Name the device
Max 25 characters
- Buttons: CANCEL, CONTINUE



Splunk Mobile App for Splunk Phantom(3/3)

Dashboard
yellow-bebhionn-pineapple

All Sources All Users Last 30 Days

Events By Sensitivity
Last updated 15s ago

high: 33.33% count: 1
medium: 66.67% count: 2

Data Sources
Last updated 15s ago

Notifications Dashboard Events

Events
yellow-bebhionn-pineapple

Owner Status Type

Events By Severity
Last updated just now

high: 33.33% count: 1
medium: 66.67% count: 2

Monday, Nov 25

ID: 3 • Medium New 4:45 PM
Splunk Log Entry On 2019-11-25T07:43:50.000+...

Unassigned

ID: 2 • Medium New 4:34 PM
Splunk Log Entry On 2019-11-24T07:00:00.000+...

Unassigned

Notifications Dashboard Events

Notifications
yellow-bebhionn-pineapple

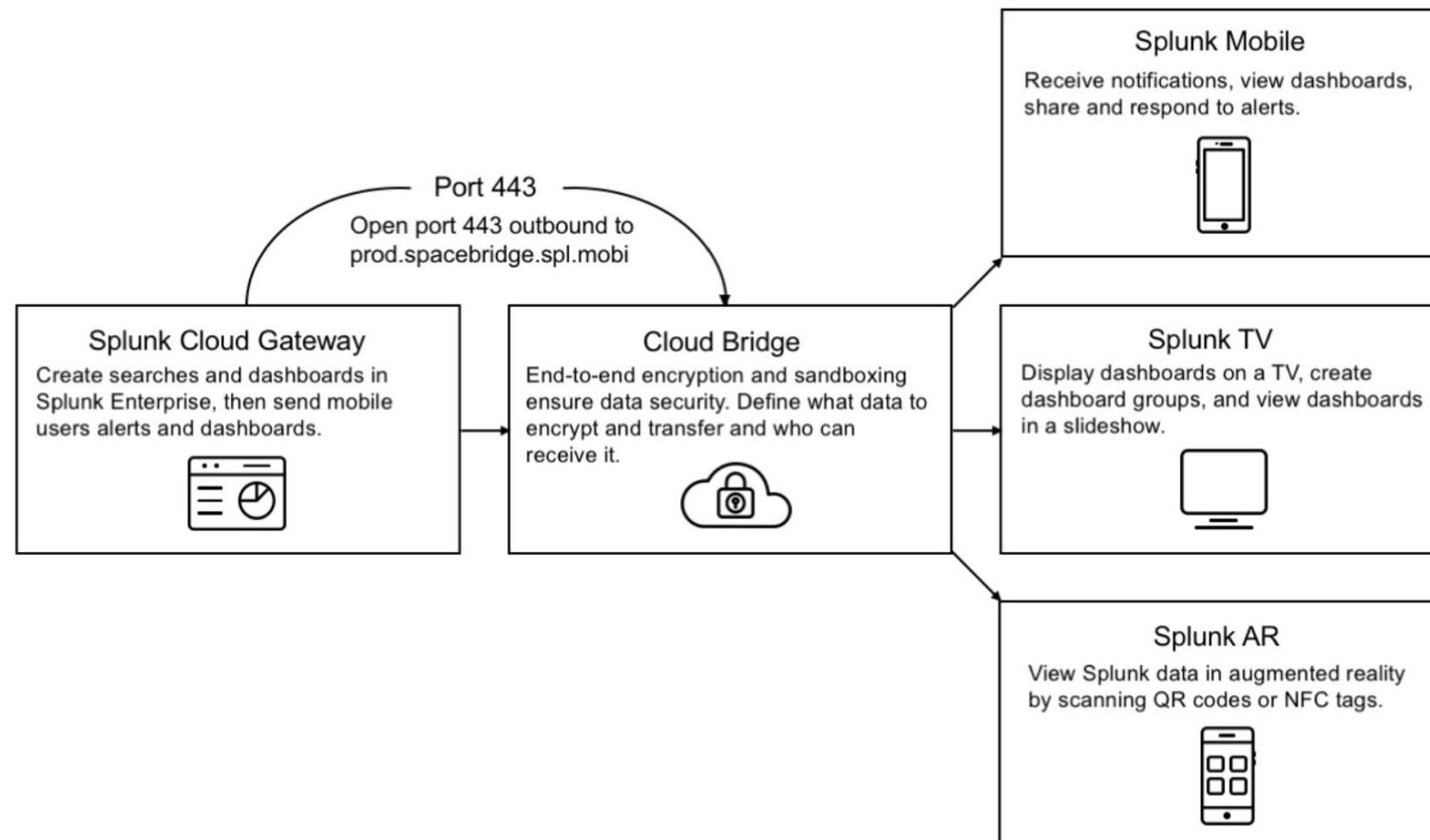
All All Types

No notifications
No notifications received

Notifications Dashboard Events

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 <code>grpc.prod1-cloudgateway.spl.mobi</code> 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.

The screenshot shows the Splunk Phantom administration interface. At the top, there is a header with the text "splunk>phantom" and a search bar. On the right side of the header, it says "version 4.6.19142" and "admin". Below the header, there is a navigation menu with "Administration" selected. The main content area is titled "Search Settings". It contains sections for "REINDEX SEARCH DATA" and "SEARCH ENDPOINT". In the "REINDEX SEARCH DATA" section, there is a dropdown menu labeled "Action" with a "REINDEX" button next to it. A note below says "Note: Reindexing is resource intensive and can impact system performance." In the "SEARCH ENDPOINT" section, there is a list of options: "Embedded Splunk Enterprise Instance", "External Splunk Enterprise Instance", "Distributed Splunk Enterprise Deployment" (which is selected), and "External Elasticsearch Instance". There is also a "SEARCH HEADS" section with a "Host" field containing "E.g: www.example.com". At the bottom, there are buttons for "ADD SEARCH HEAD" and "Maximum 10".

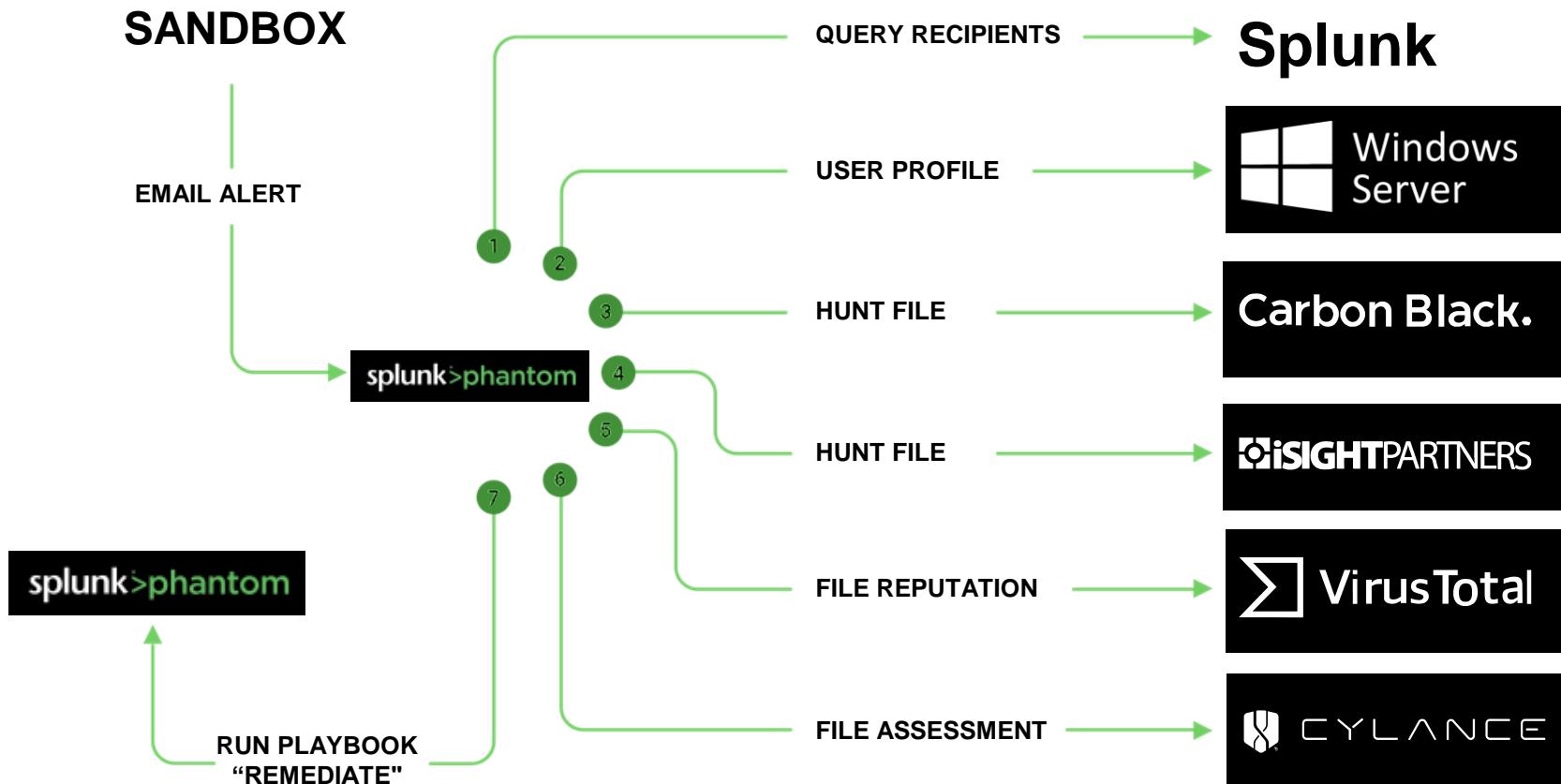
어떻게 동작하는가?

고객 팬텀 활용사례 : Blackstone

자동화된 말웨어 조사분석

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

아담 플래처
CISO

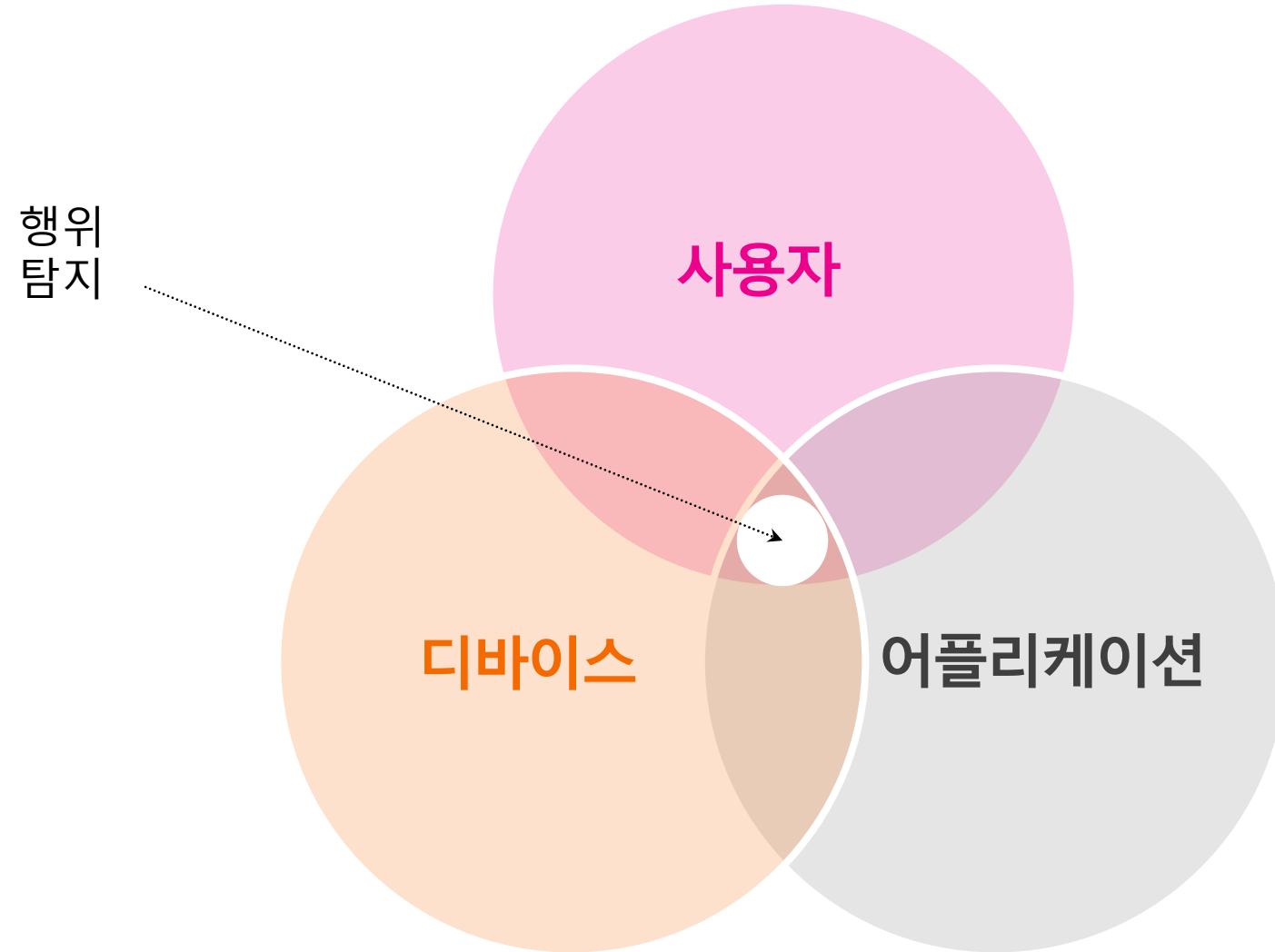


UBA 5.0

User Behavior Analytics

splunk> turn data into doing™

UBA는 단순히 사용자만을 의미하지 않습니다.

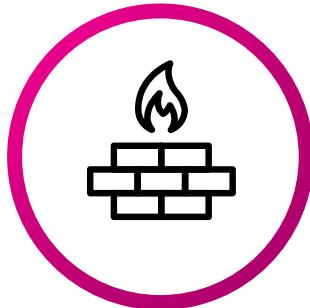


핵심 유즈케이스

- 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

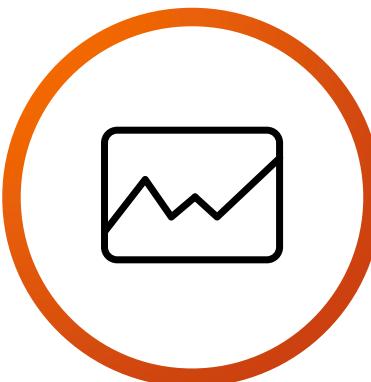


방법

임계치



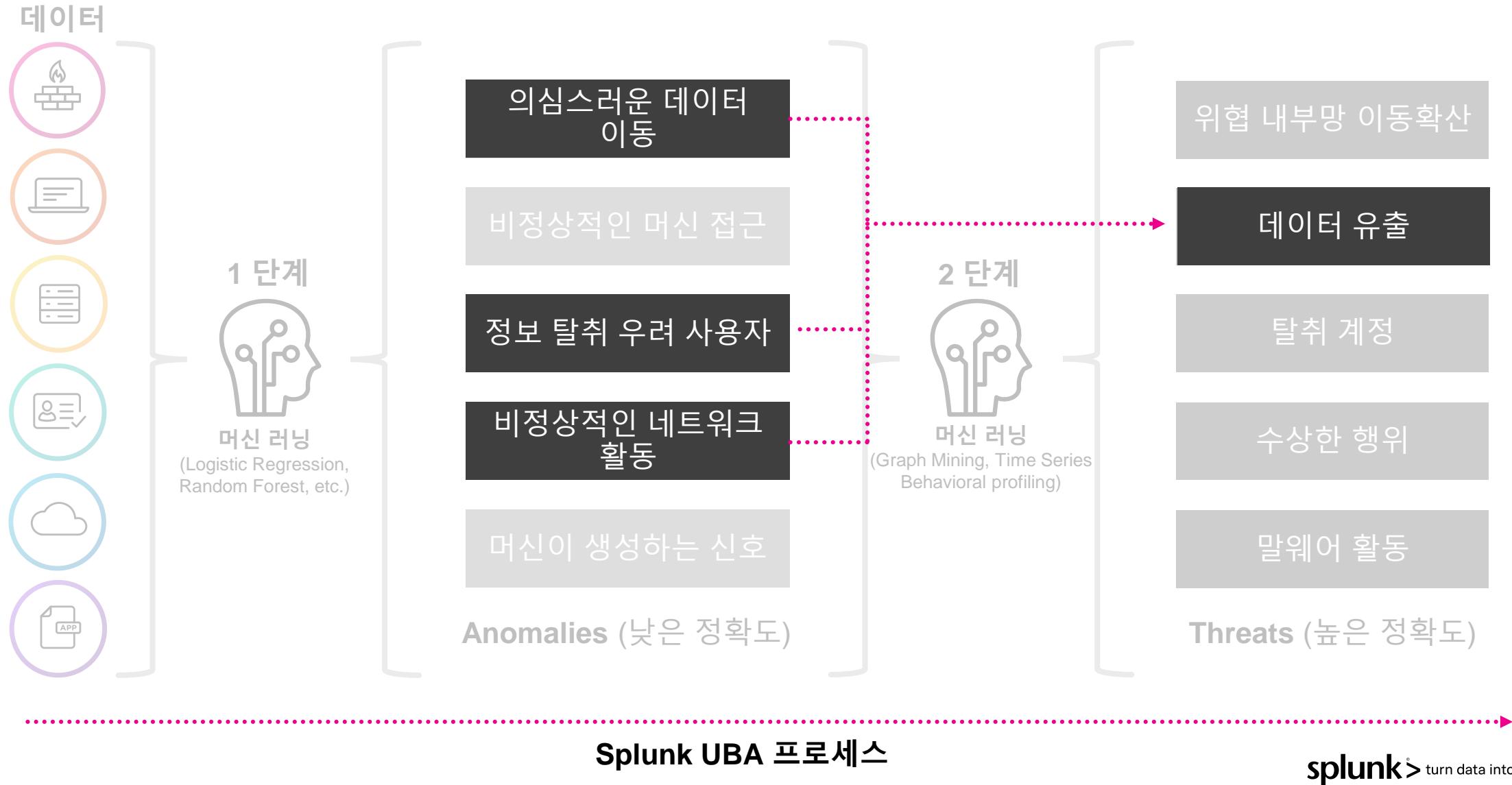
통계



머신 러닝



왜 Splunk UBA 인가?



무엇이 필요한가?

데이터 플랫폼

splunk®



Splunk Enterprise
Security™

데이터 소스

Active Directory

DNS, DHCP

Firewall

Web Proxy

VPN

Endpoint

DLP

최소

옵션

사양

CPU: 16 Cores

Memory: 64GB

Disk: 1200 IOPS

최소

Splunk User Behavior Analytics 5.0

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

The screenshot shows the Splunk User Behavior Analytics interface. On the left, there's a sidebar with 'splunk > User Behavior Analytics' at the top, followed by 'Home / Models', 'Models' (selected), 'Streaming Models', 'Batch Models', and 'Custom Models' which says 'No Data'. On the right, a modal window titled 'New Custom Model' is open, specifically 'Step 3 of 8 : Tracking Features'. It contains fields for 'Field' (with 'possibleServerPort' selected) and 'Conditional' (with 'Select optional'). Below that are three rows of 'Field' and 'Conditional' pairs: 'application' and 'possibleServerPort'; 'possibleServerPort' and 'application'; and another 'possibleServerPort' and 'application'. There's a '+ Add feature to track' button. Underneath these are sections for 'Columns for Evidence' (with 'application, dataFormat, destination, destin...' selected), 'Participants *' (with 'applicationId, sourceId, userId'), and 'Tracking Features With User Group' (with 'destinationZone, sourceZone'). At the bottom of the modal are 'Cancel', '< Back', and 'Next >' buttons.



탐지



예측

Splunk User Behavior Analytics 5.0

데이터 카테고리 범위

HA/DR 월
스탠바이

4
신규

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

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

자동화 와 오테스트레이션

인간의 기술을 향상 시키는 기계 학습



Splunk Enterprise
Security™



ADAPTIVE RESPONSE

 Phantom



Splunk User Behavior
Analytics™

Thank You

splunk[®] > turn data into doing[™]