Splunk Forum

Breakout Session 2 (Security)

Splunk Korea
황원섭(Bob Hwang) | Senior Sales Engineer

splunk> turn data into doing™

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> turn data into doing™


92
of the
Fortune 100
Trust Splunk
splunk> turn data into doing

Splunk는 조사 액션(Investigation Action) 및 대규모 환경을 위한 유일한 플랫폼입니다.

3B

Searches in the Last Month

918K

Monthly Active Users

85%

Growth in cloud data sources

2,400+

Unique Splunkbase Apps

A Leader

8 Consecutive Years

Gartner® SIEM Magic Quadrant™ 2021

#1

Market Share in SIEM & ITOM

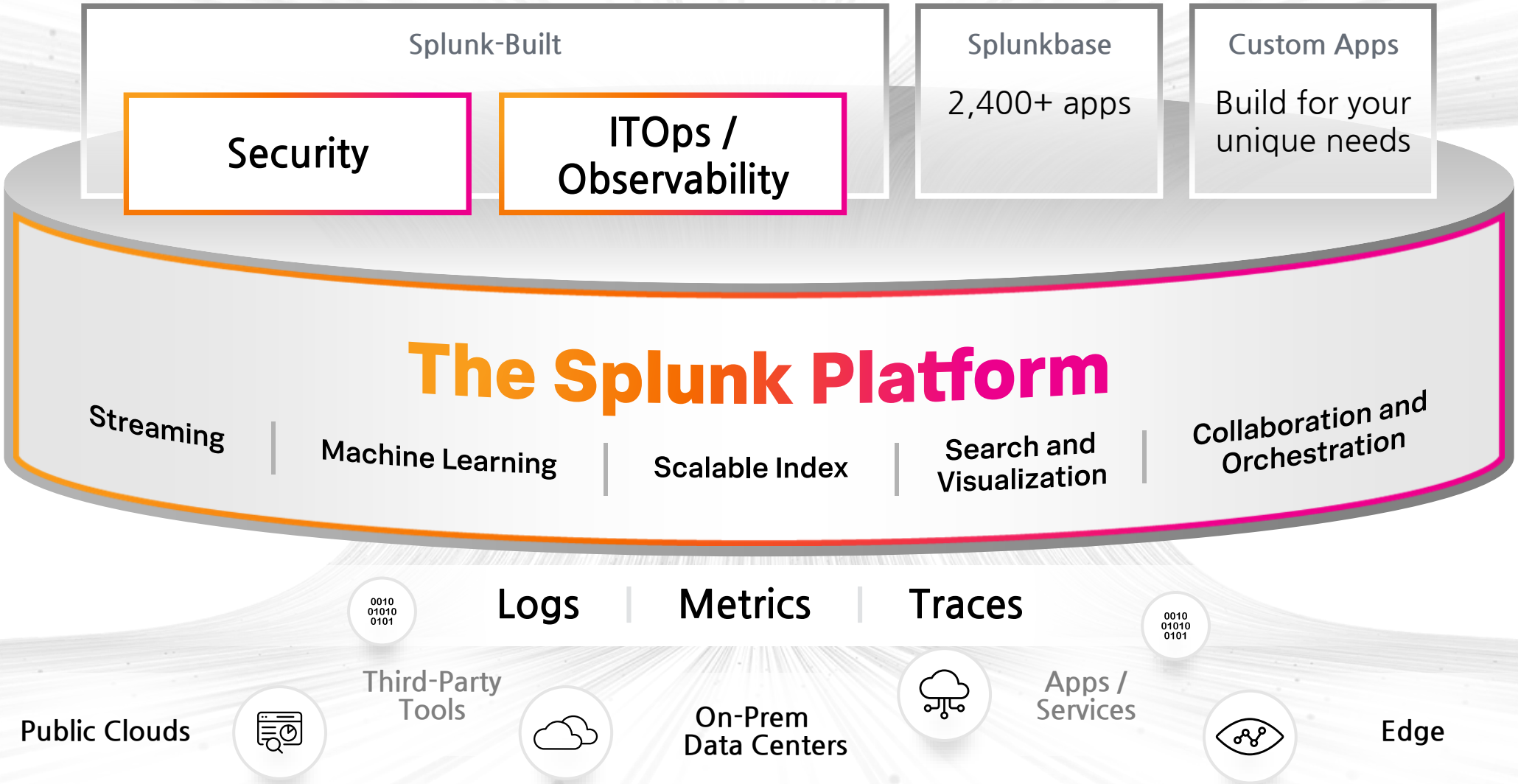
Gartner, Market Share 2020

Leader and Only "Outperformer"

GigaOm for Cloud Observability, 2021

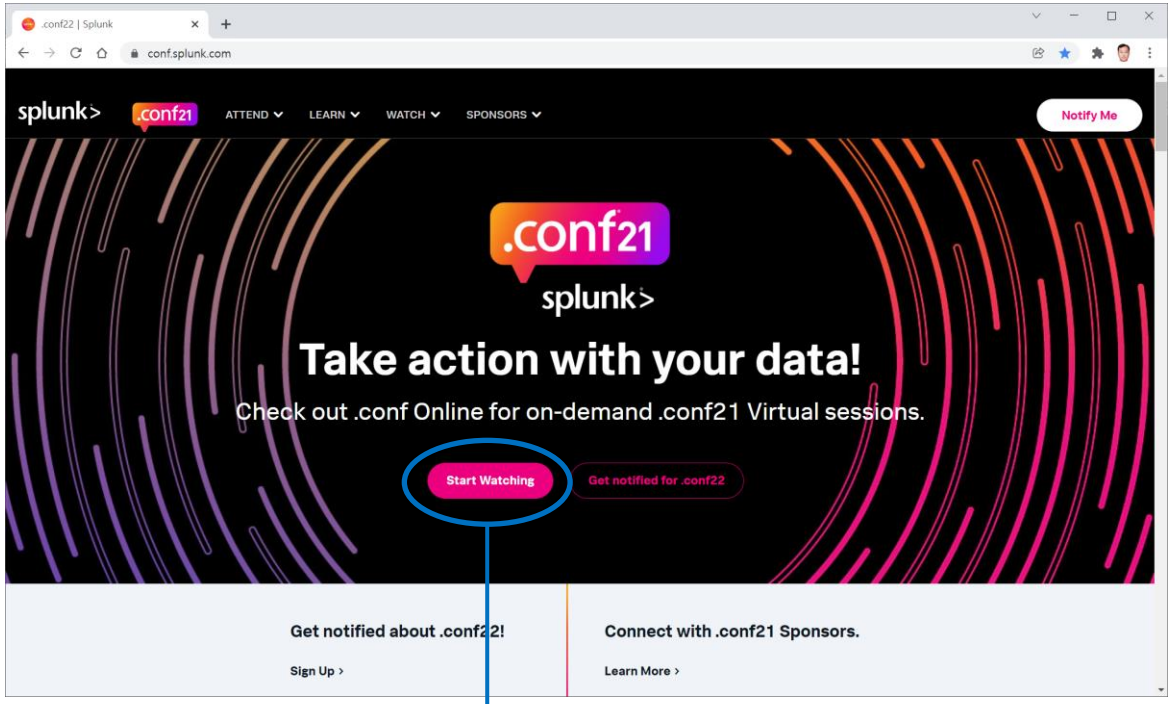
Gartner, Magic Quadrant for Security Information and Event Management, Kelly Kavanagh, Toby Bussa and John Collins, 29 June 2021.
Full report available at https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.html.
Gartner, Inc., Market Share: All Software Markets, Worldwide 2020; Neha Gupta et al; 14 April 2021
GigaOm, Radar for Cloud Observability, 2021, David Linthicum and Andy Thurai, 26 February 2021

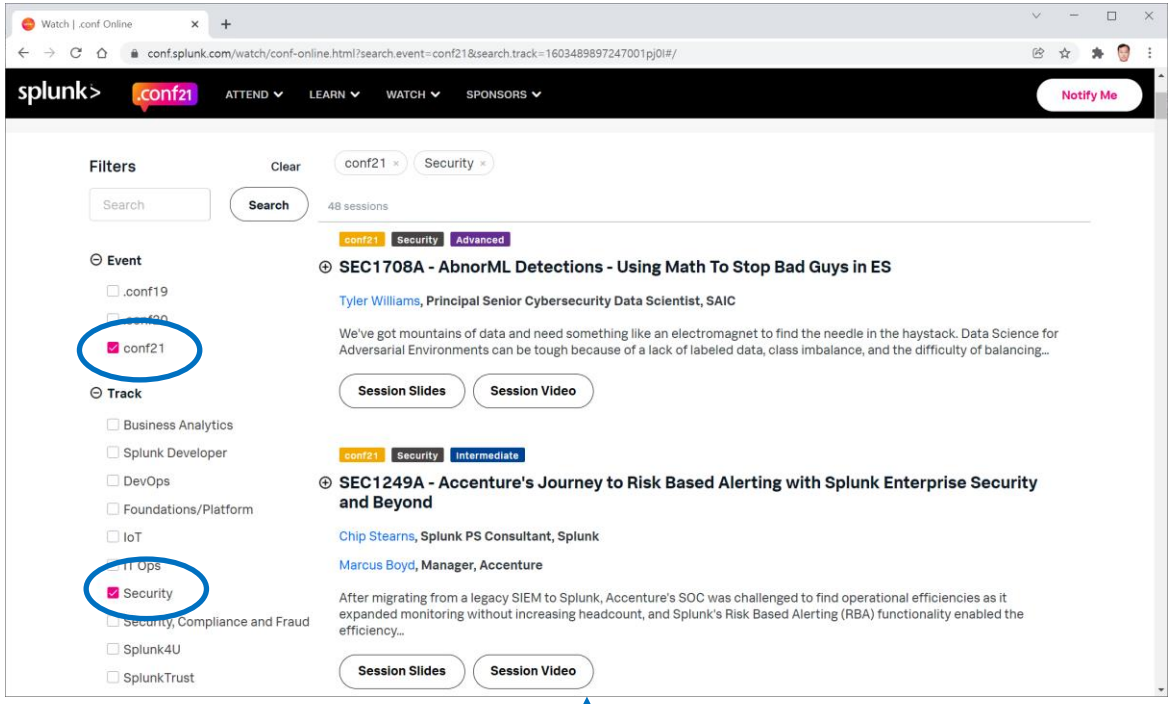
The Foundation of Hybrid World



conf.splunk.com

Conf 행사 사이트에서 세션 슬라이드 및 비디오(녹화영상) 공개 (splunk.com 계정 로그인)



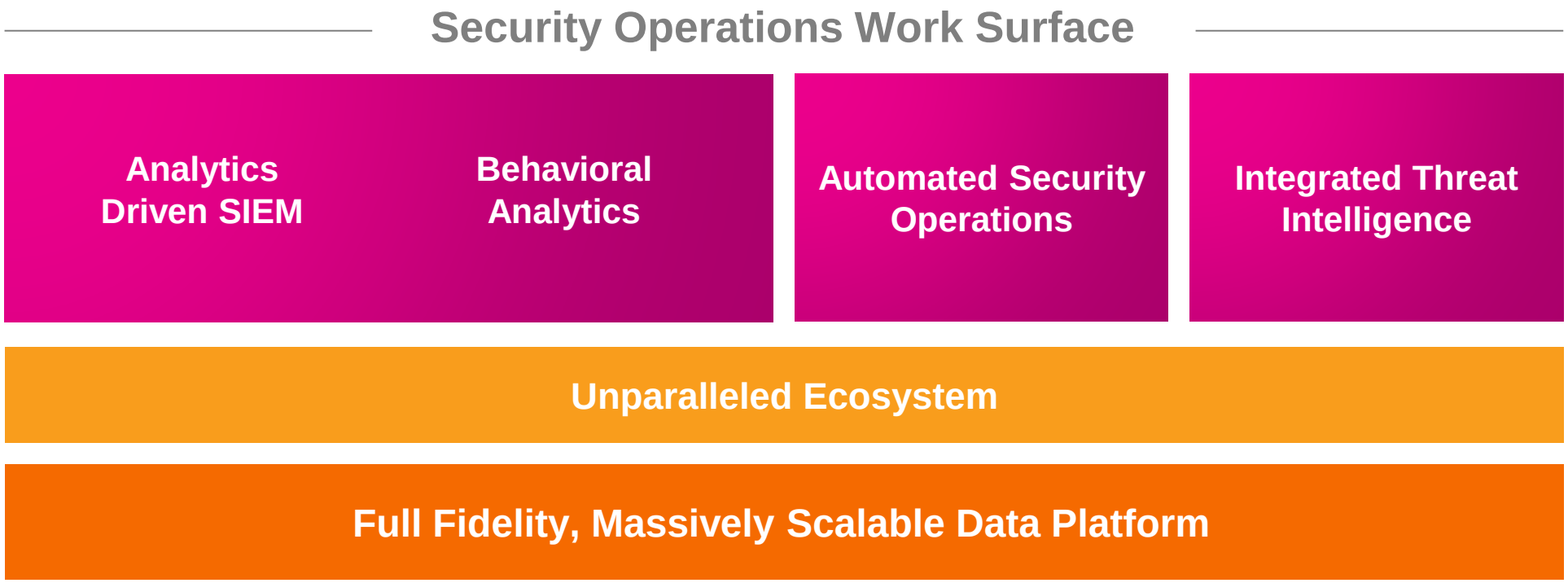


Splunk Security 미래 전략

splunk> turn data into doing™

Splunk for Security

Splunk's vision for a Modern SOC Platform



Splunk Security Portfolio

Splunk's Modern SOC Platform

Splunk Mission Control

Security Operations Work Surface

Splunk Security Operations Suite

Splunk Enterprise Security
On-Prem / Hybrid

Splunk User Behavior Analytics
On-Prem

Splunk SOAR
On-Prem / Hybrid

Splunk Security Cloud

Splunk Enterprise Security
Cloud-Delivered / Hybrid

Behavioral Analytics
(In Preview)
Cloud-Delivered / Hybrid

Splunk SOAR
Cloud-Delivered / Hybrid

TruStar
Cloud-Delivered

Unparalleled Ecosystem
(Apps, TAs, Connectors, Partner, Community)

Splunk Cloud Platform
Full-Fidelity | Real-Time Streaming | Massively Scalable | AI/ML-driven Analytics

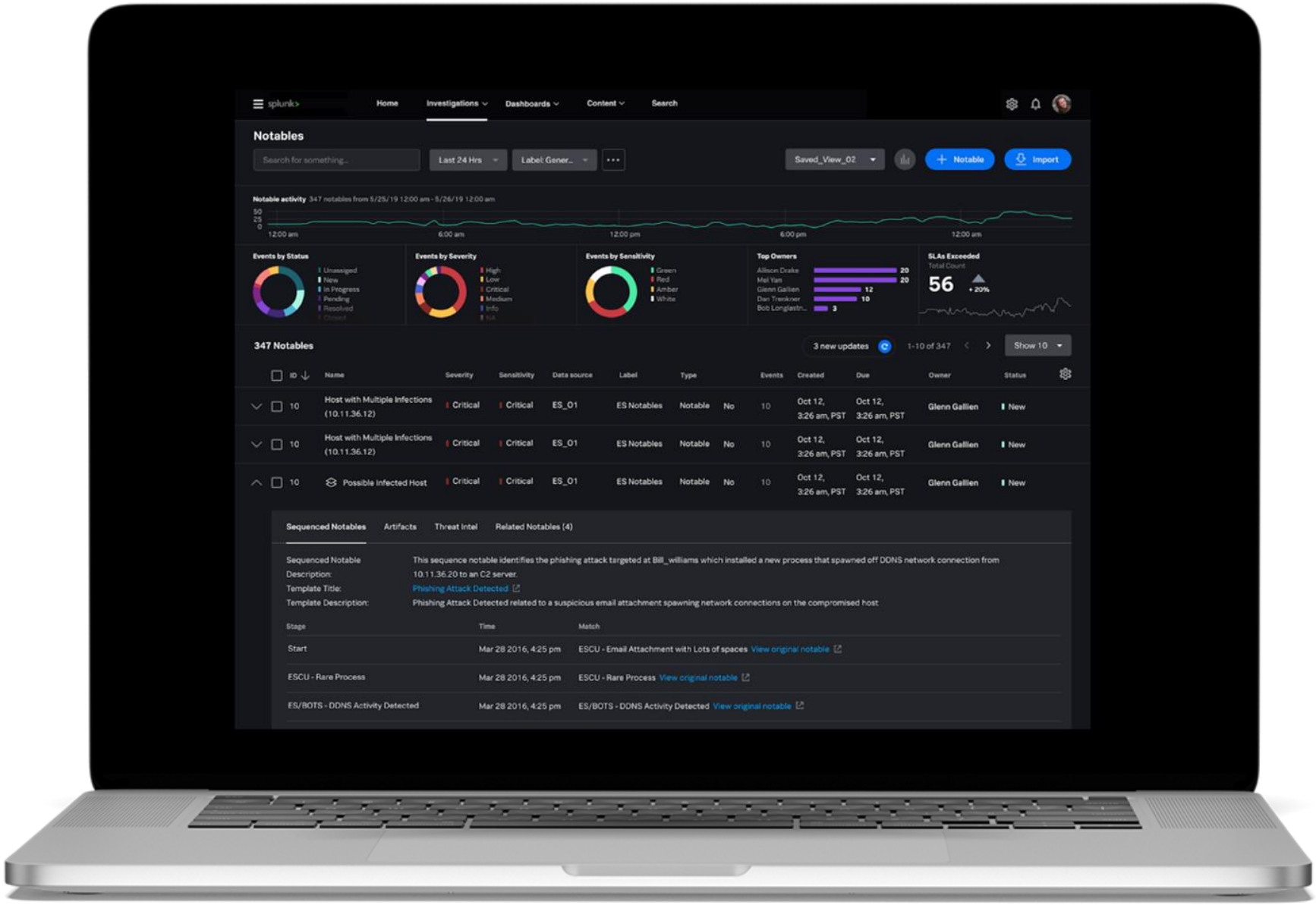
Splunk .conf21 Security Innovations

Outcomes	Capabilities	Offerings
Faster Time to Detect, Investigate, and Respond	**Advanced Security Analytics** **Automated Security Operations** **Integrated Threat Intelligence** **Unparalleled Ecosystem**	**Splunk Security Cloud**
Faster Time to Detect	SURGe Security Research In-Product Content Updates Integrated Threat Intelligence	Splunk Enterprise Security Splunk Intelligence Management
Faster Time to Investigate	Risk-Based Alerting reduces Alert Volume Behavior Analytics (Preview)	Splunk Enterprise Security
Faster Time to Respond	Visual Playbook Editor Integrated Threat Intelligence	Splunk SOAR (new in Cloud) Splunk Intelligence Management
Reduce Burden of Disparate Tools	New integrations: Mandiant, Zscaler, DTEX Deeper integrations: CGP, AWS, Azure, Onedrive, Sharepoint, Box.net, GDrive for holistic Cloud Security Monitoring	Splunkbase w/ 2,400+ Integrations Splunk Enterprise Security Splunk SOAR (new in Cloud)

Splunk Security Cloud

보안 이벤트 라이프사이클 전반에 걸친 가시성 및 제어

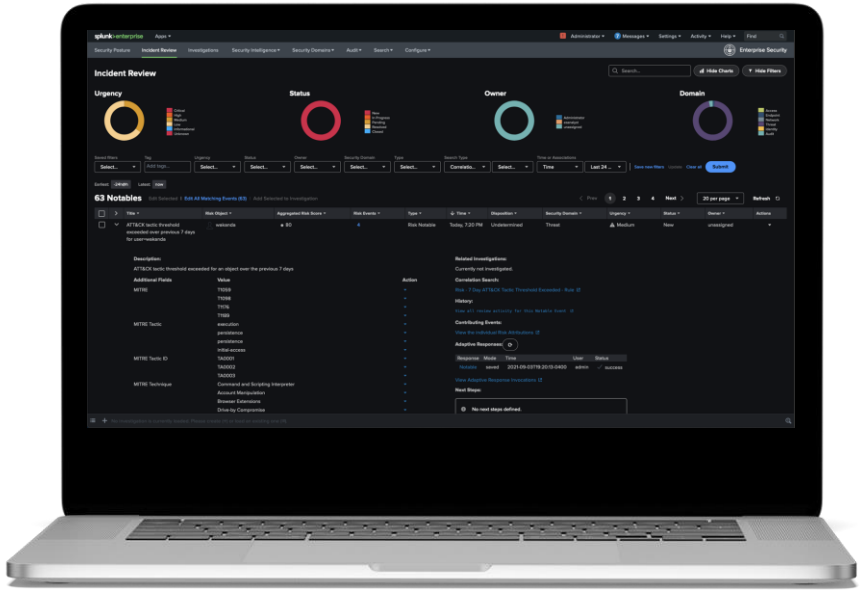
- 고급 보안 분석 (Advanced Security Analytics)
- 자동화된 보안 운영 (Automated Security Operations)
- 통합 위협 인텔리전스 (Integrated Threat Intelligence)
- 세계 최고의 에코시스템 (Unparalleled Ecosystem)



splunk> turn data into doing™

Announcing

Splunk ES(Enterprise Security) Cloud



Executive Summary and SecOps Dashboards

- 주요 SOC 수치(지표)에 대한 모니터링/보고서

Cloud Security Monitoring Dashboards

- Cloud에 대한 보안 가시성 및 탐지 기능 향상

Automated Real-time Content Updates

- 새로운(최신) 위협에 대한 신속한 탐지 지원

Now: Splunk Intelligence Management

포트폴리오 전반에 걸친 통합된 인텔리전스 기능을 통해 가시성, 탐지, 조사 및 대응 속도 향상

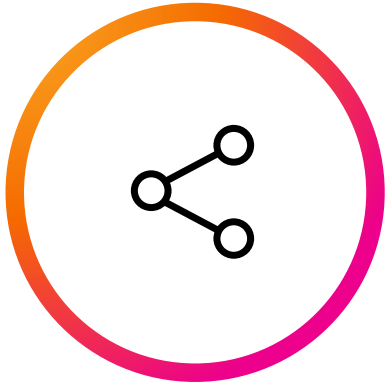
Splunk Enterprise

보유한 모든 인텔리전스 소스와 매칭하여 모니터링

Splunk Enterprise Security

자동 이벤트 풍부화 및 Notable 이벤트의 우선순위 지정에 활용

Splunk SOAR



인텔리전스 기반 플레이북

Splunk Intelligence Management Enclaves

ISACs, ISAOs와 정보 공유

Announcing

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

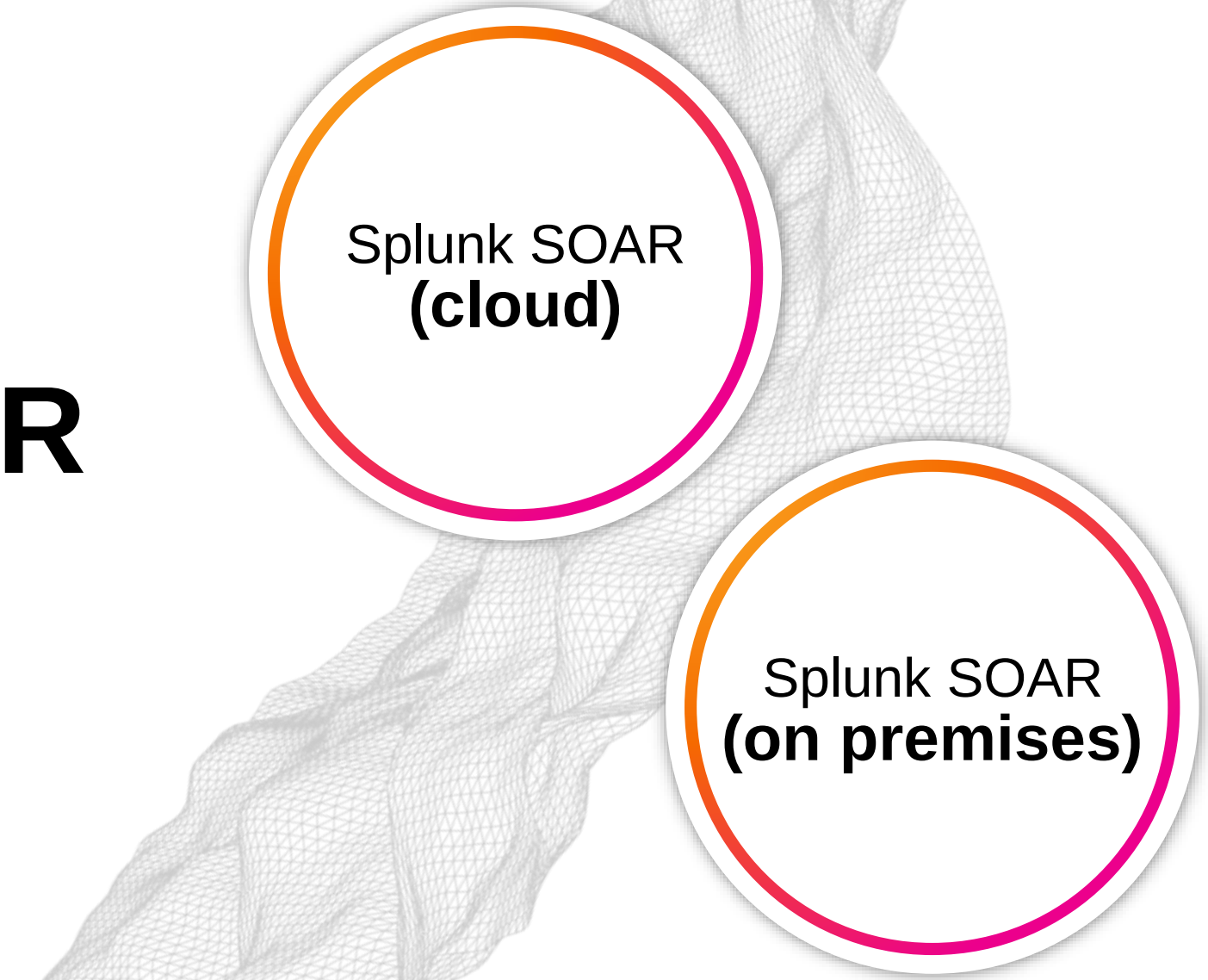
Sign up for alerts: splunk.com/surge

Risk-Based Alerting to the Rescue

- 경보 품질 향상
- 탐지 정확도 향상
- 조사 업무의 간소화

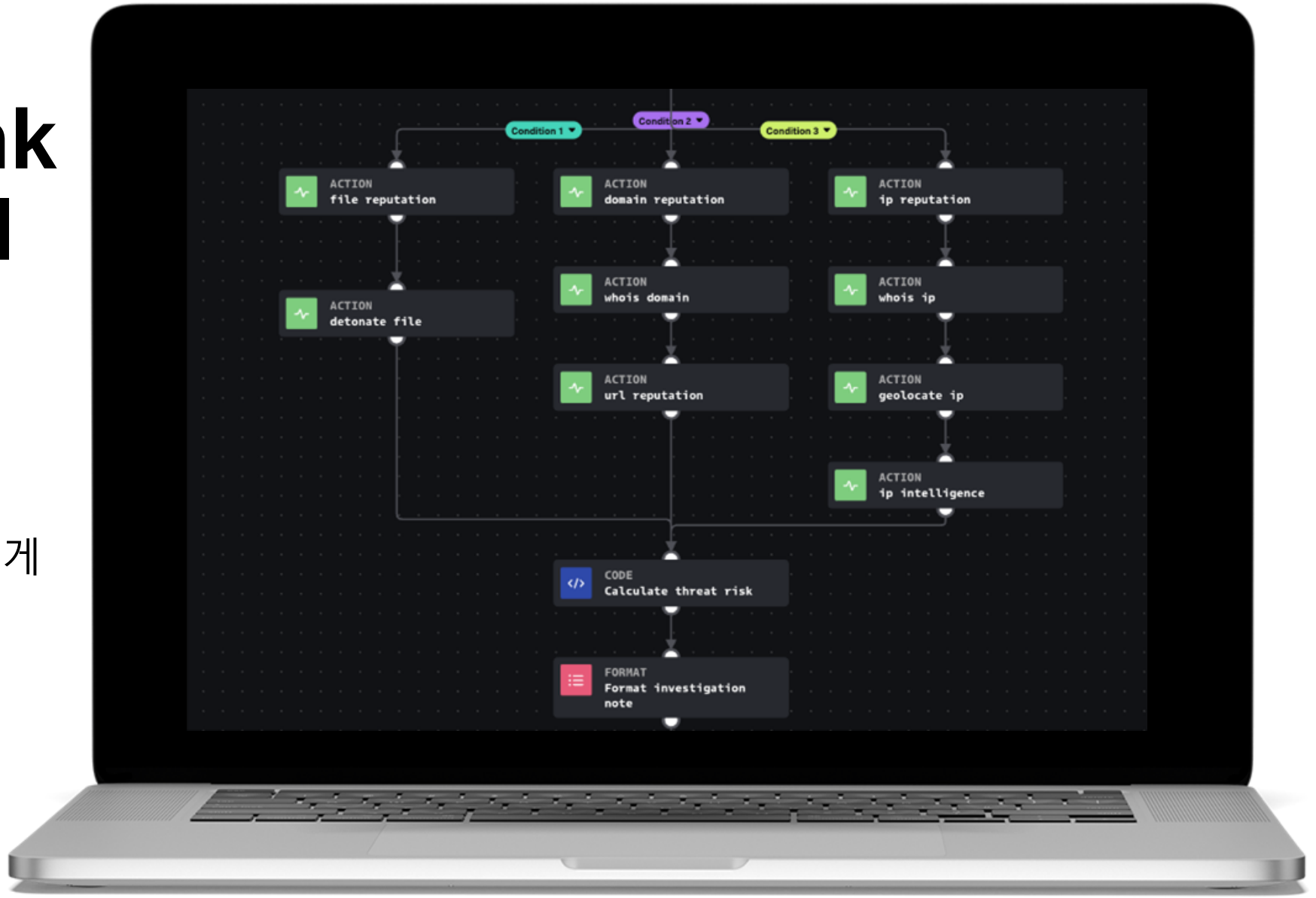
Splunk SOAR

Two Deployment Options

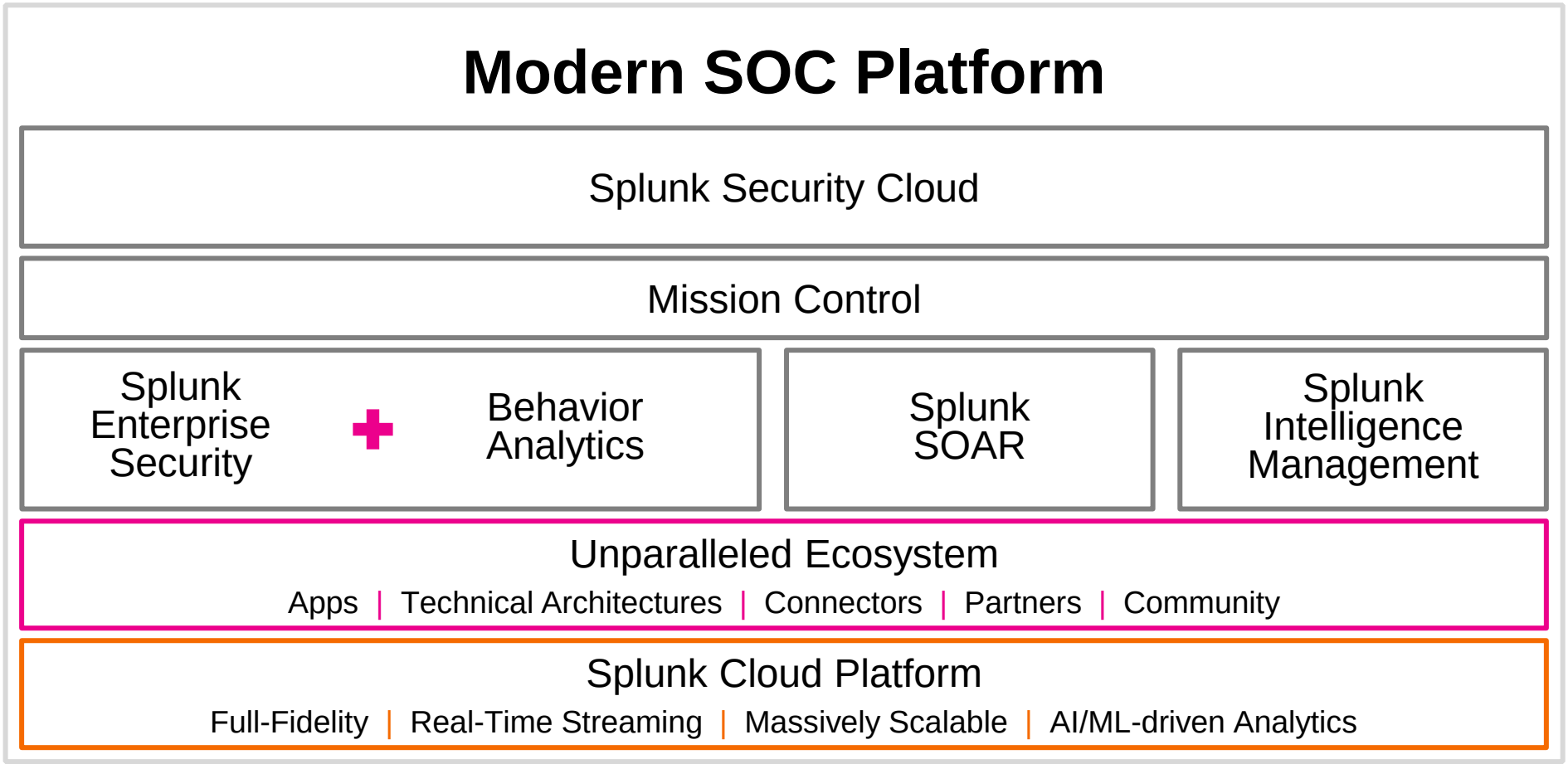


새로운 Splunk SOAR Visual Playbook Editor 출시

- 더 많은 유즈케이스를 빠르게 자동화 확장
- SOAR를 통해 빠르게 가치 실현(제공)



Splunk for Security



Catch these Sessions on-demand at .conf Online

Security Solutions

Security Modernization

SEC1108C: Securing the Software Factory with Splunk

SEC1745C: Hunting the Known Unknown: Supply Chain Attacks

SEC1397A: Fighting Fraud with Splunk

SEC1800A: Implementing Zero Trust

Security Analytics (SIEM)

SEC1271: What's New in Splunk Enterprise Security?

SEC1163: RBA and Vmware

SEC1249: RBA and Accenture

SEC1162: RBA and Chevron

SEC1546A: Reduce Noise From Intel Sources with TruSTAR + ES

SOAR

SEC1209A: Automated Vulnerability Detection

SEC1590C: Automated Incident Response

SEC1194: Uber and Splunk SOAR

SEC1301C: SOAR Overview

Security Super Session:
Accelerate Threat Detection, Investigation, and Response

splunk> turn data into doing™

Splunk ES 업데이트

splunk> turn data into doing™

Recap of Enterprise Security 6.6

GA: June 30, 2021

In case you missed it!

splunk> turn data into doing™

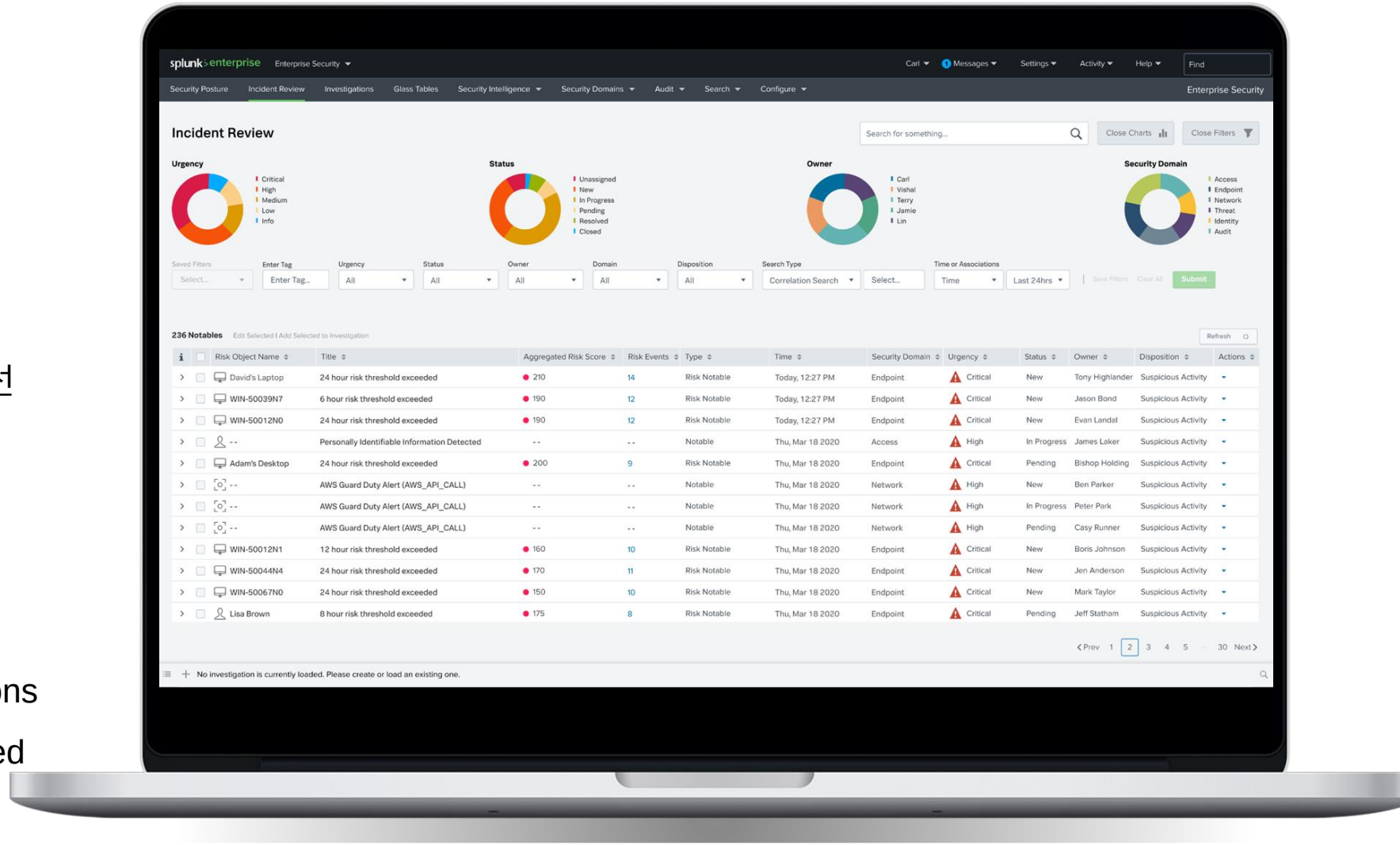
ES 6.6 Available Now

In case you missed it...

Enterprise Security 6.6

June 30, 2021

- Incident Review Dashboard 개선
  - Saved Filters
  - More Screen Real-Estate
  - RBA Details
  - Dispositions(배치)
- RBA Event Timeline visualizations
- Cloud Security Monitoring shared storage datasets



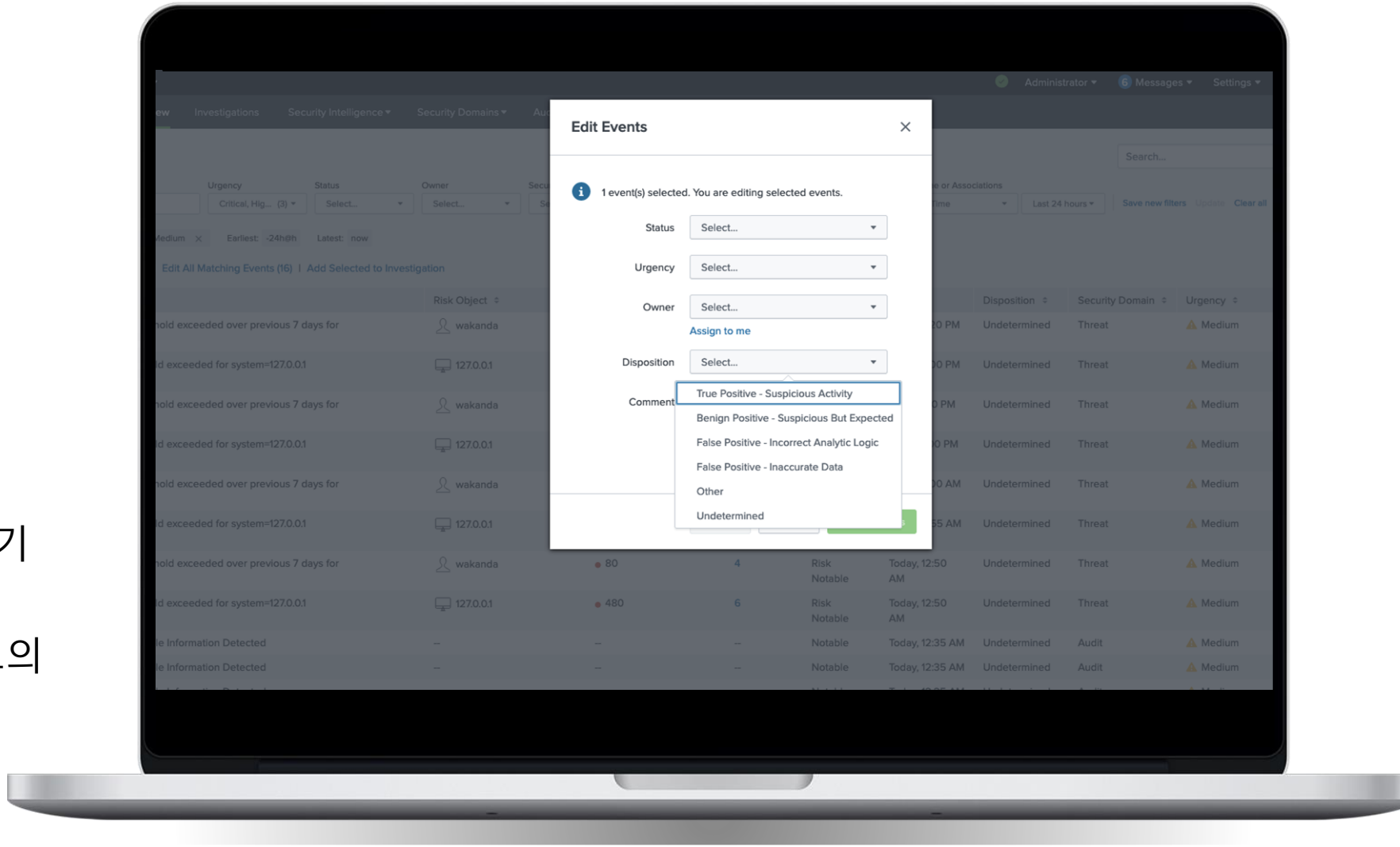
Tune into the ES 6.6 Tech Talk On-Demand

splunk> turn data into doing™

ES 6.6
Available Now

Incident Review Dashboard 개선

- Notable 이벤트를 신속하게 분류하는 새로운 방법
- 필터와 태그로 위협을 쉽게 식별
- Notable 이벤트를 그룹화하기 위한 저장 필터 기능
- 오탐에 대한 Notable 이벤트의 배치(Dispositions) 분류



ES 6.6
Available Now

Cloud Security Monitoring

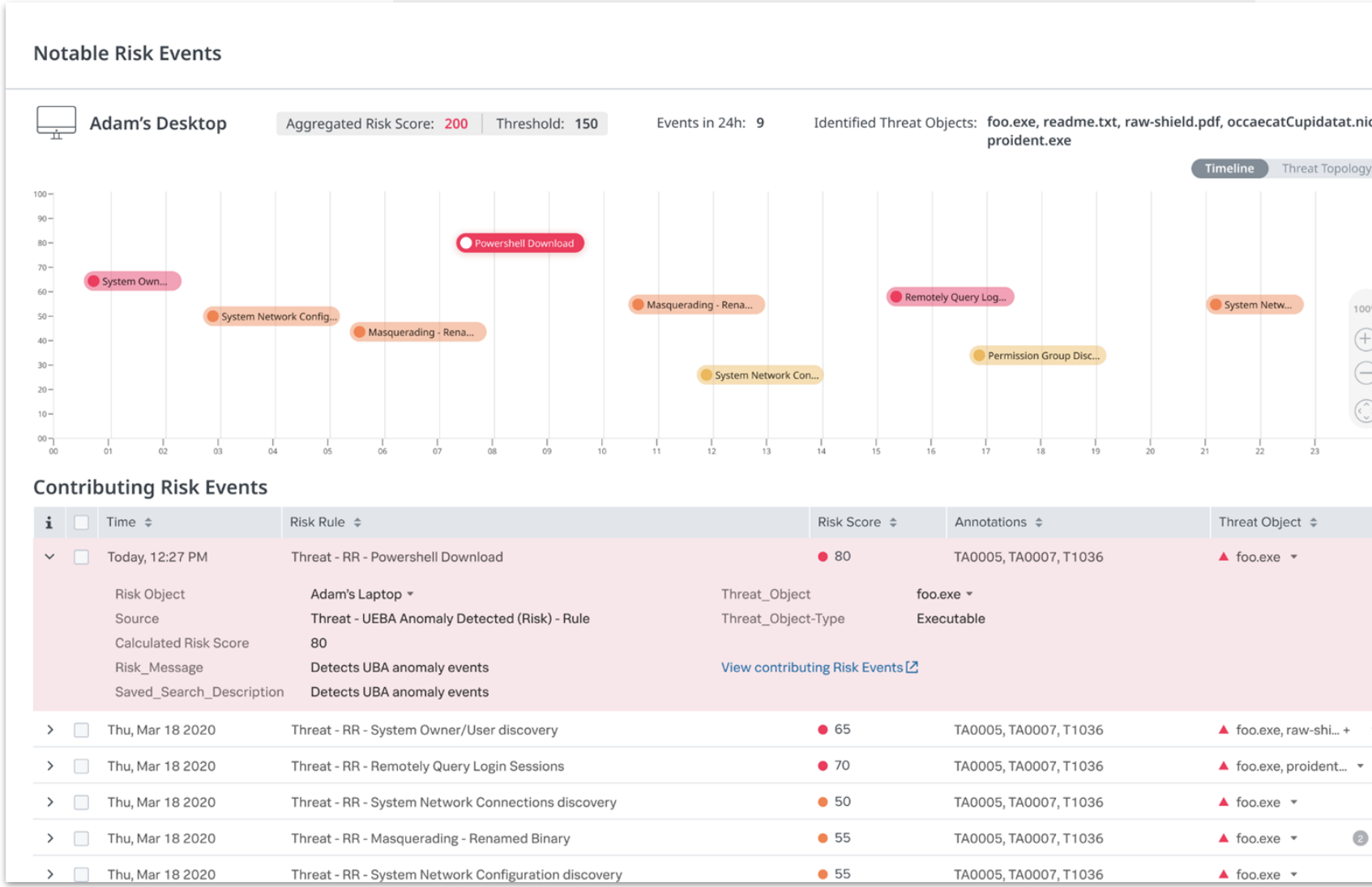
- Box, Google Drive, SharePoint, OneDrive와 같은 공유 클라우드 스토리지 서비스에 대한 데이터 모델 및 정규화 지원
- AWS, GCP, Microsoft Azure와 같은 하이브리드 및 멀티클라우드 환경에서 데이터 운용
- 통합 클라우드 보안 포스쳐(security posture) 구축 및 강화

splunk> turn data into doing

ES 6.6 Available Now

Risk-Based Alerting Event Timeline

- 위험 이벤트 기여에 대한 타임라인을 빠르게 식별
- 단일 위험 기반 이벤트로 결합된 전체 위협 활동에 대한 포괄적인 뷰
- 위험 개체, 위험 속성, 위협 개체 및 탐지 타임라인 간의 가시성 향상
- MTTD 감소 및 MTTR SOC 메트릭 단축



splunk> turn data into doing

Coming Soon

Splunk Enterprise Security 7.0

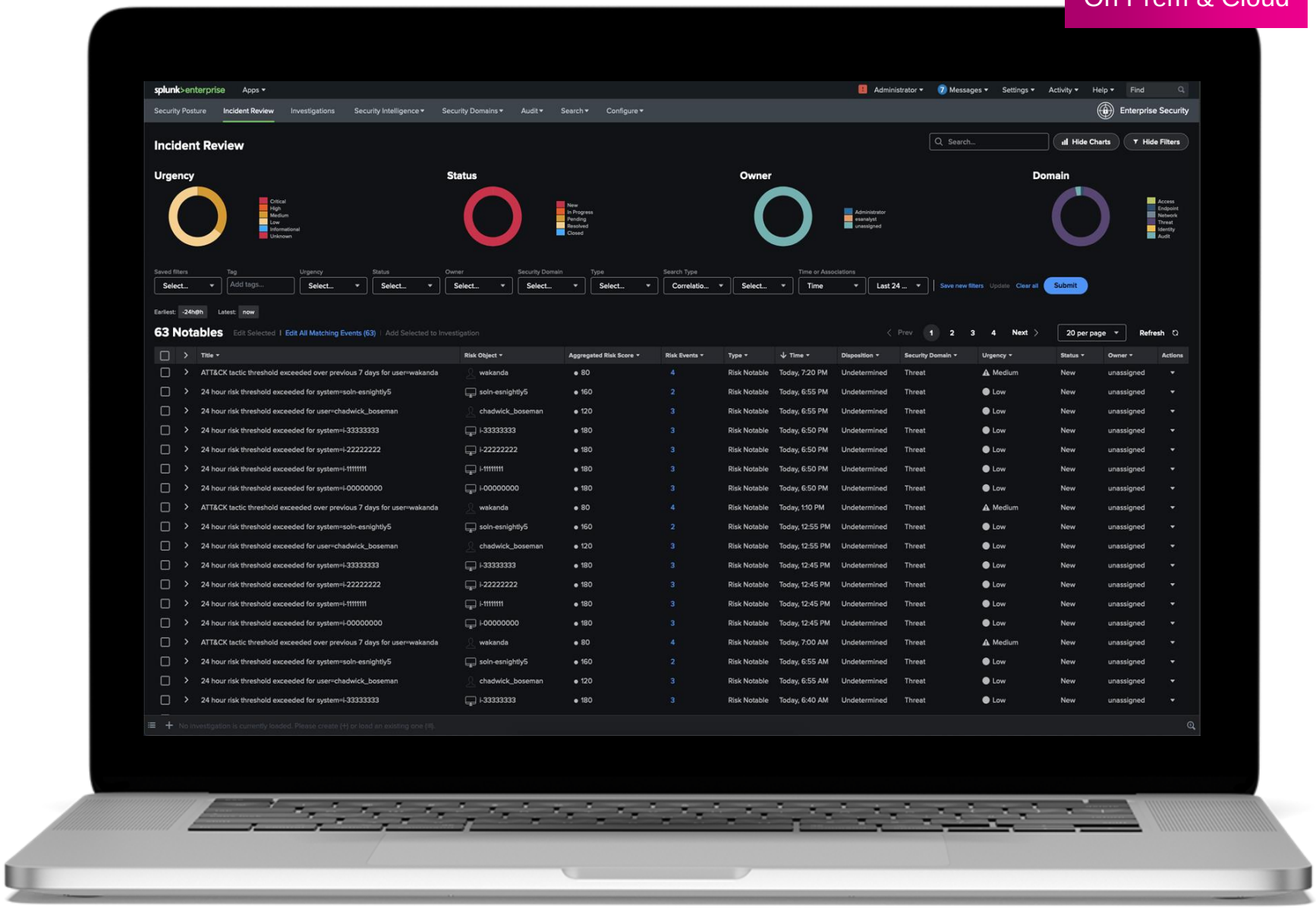
splunk> turn data into doing™

Coming Soon

On Prem & Cloud

What's New in Splunk Enterprise Security 7.0

- 요약 대시보드(Executive Summary Dashboard)
- 보안 운영 대시보드
- 클라우드 보안 모니터링 대시보드
- 실시간 콘텐츠 업데이트
- 다크 모드 사용자 UI



splunk> turn data into doing™

Coming Soon

Executive Summary Dashboard

시간 경과에 따른 트렌드가 포함된 경영진 수준 보안 인사이트 제공

- Key Insights
  - Mean Time to Triage
  - Mean Time to Respond
  - Investigations Created
  - Assigned Notables Over Time
  - Notable Event History Trends
  - Risk-Based Alerting Trends
  - Adaptive Response Action Trends

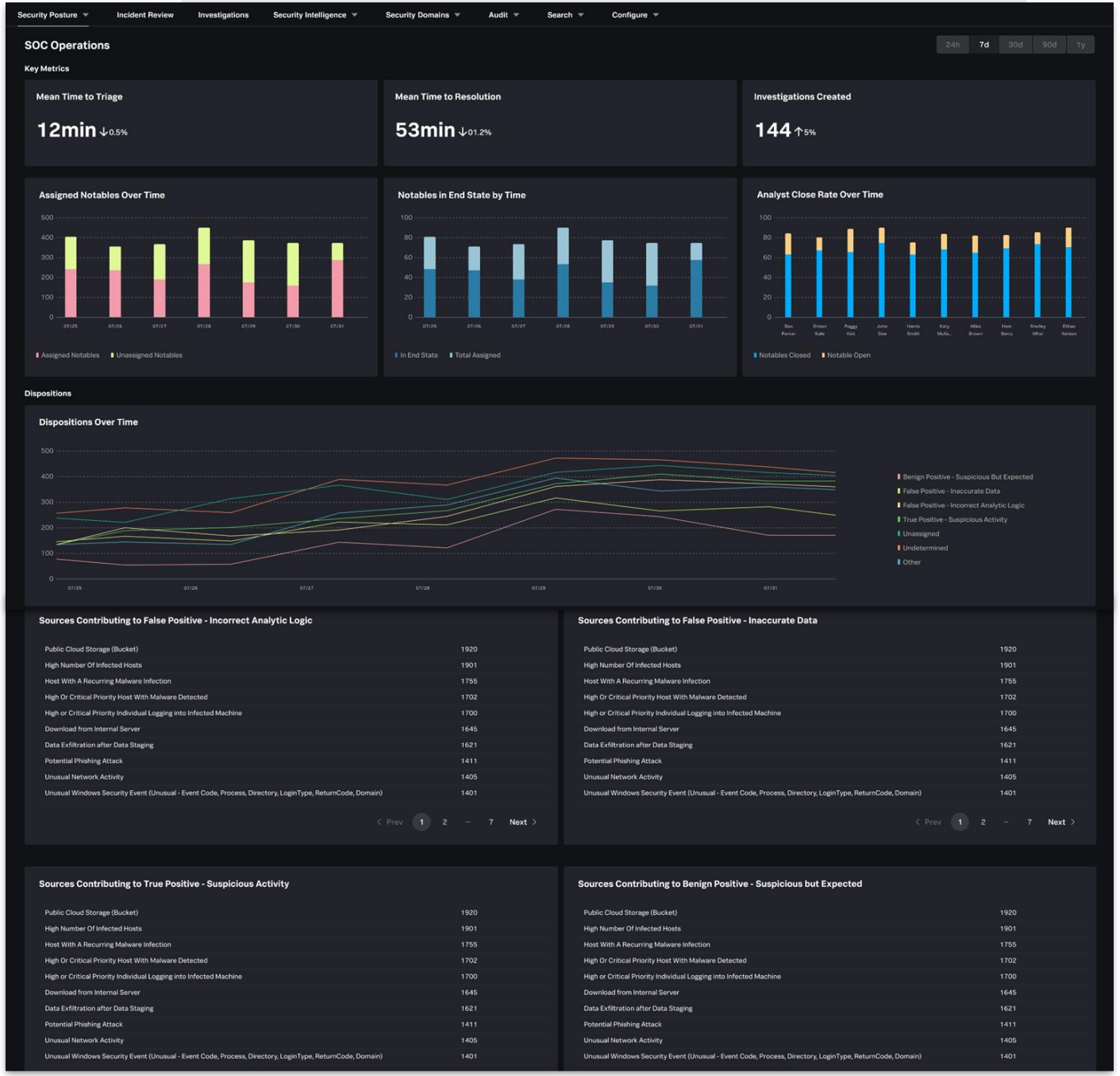
On Prem & Cloud

Coming Soon

Security Operations Dashboard

보안 운영 전반에 걸친 성능 및 효율성 통찰력

- Key Insights
  - Mean Time to Triage
  - Mean Time to Respond
  - Investigations Created
  - Notable Assignments
  - Notable and Analyst Close Rate
  - Notable Disposition
    - False Positives
    - True Positives
    - Benign Positives



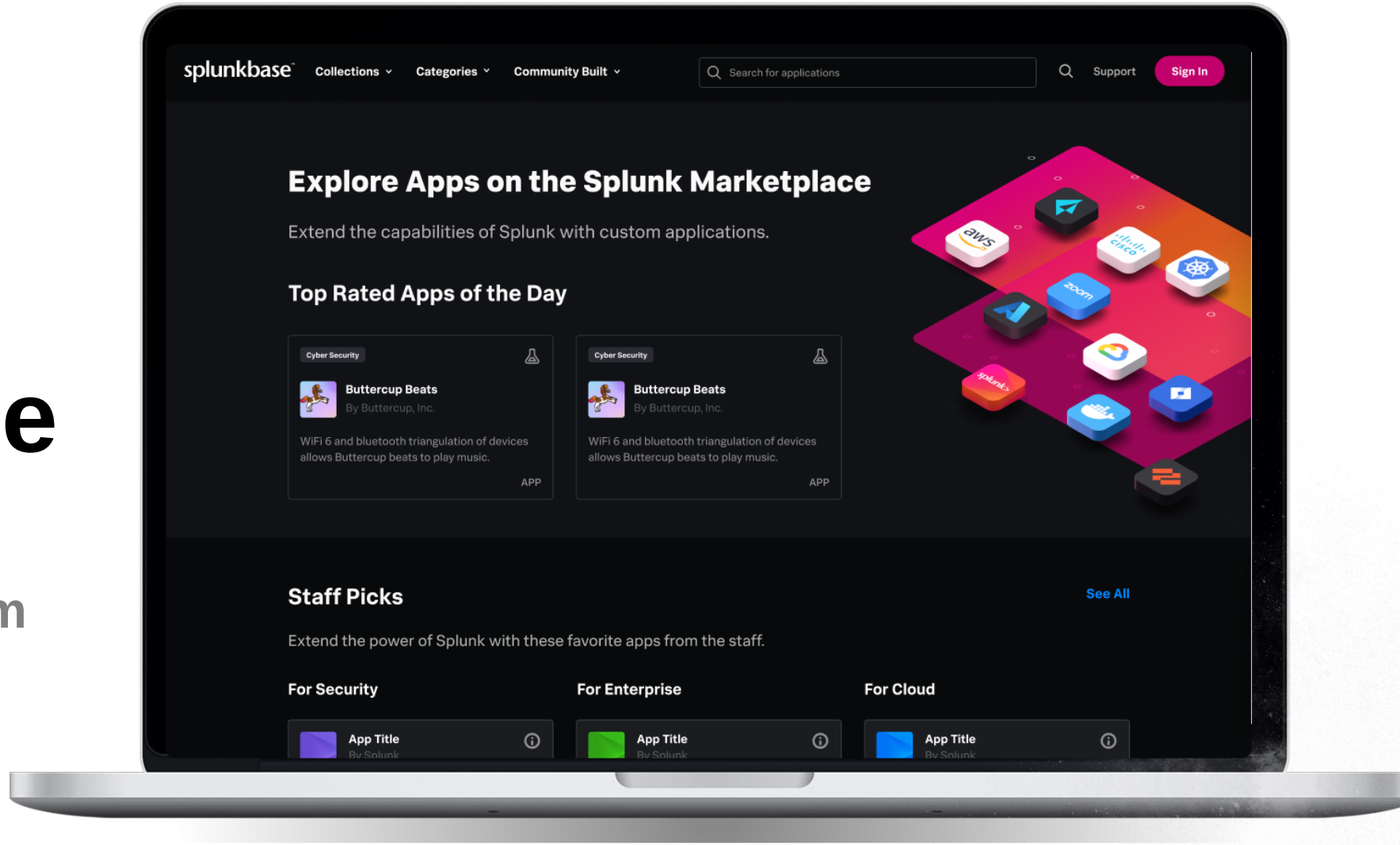
On Prem & Cloud

Splunkbase

splunk> turn data into doing™

Try New Splunkbase

http://splunkbase.com



Our partners help you
turn data into doing

Integrations

Enhanced SOC visibility

End-to-end zero trust

Insider threats

Thank You

splunk> turn data into doing™