cisco Engage

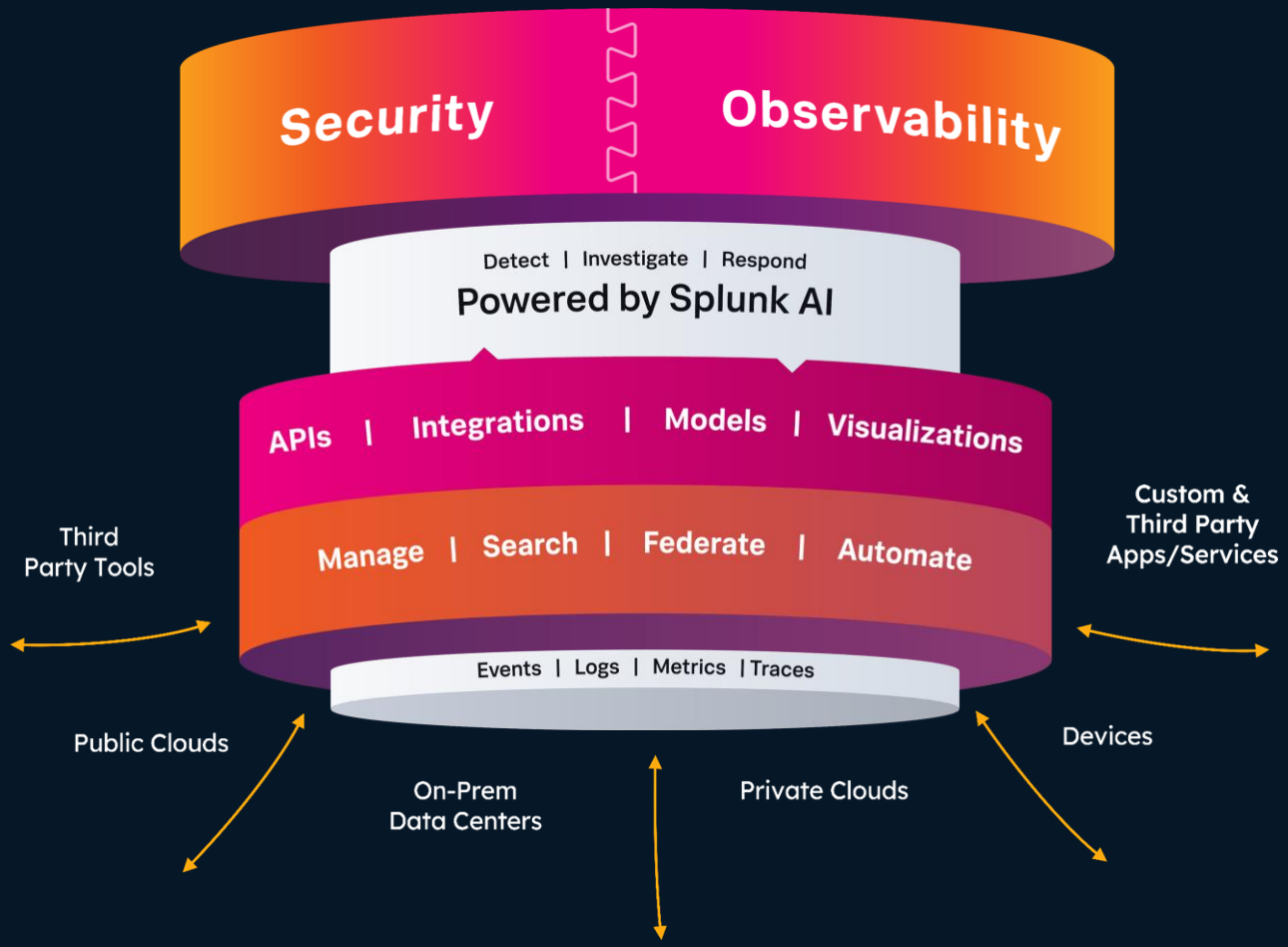
GO BEYOND
Cisco Engage GBA

Driving the Next Generation of AI-Enabled Security and Observability

Cheuk Fong Wai
Cisco Senior Solutions Engineer

Agenda

- Splunk Overview
- ML Use-cases for Observability
- ML Use-cases for Security



Digital Resilience

The Unified Security and Observability Platform

Access the Right **Data**

Apply the Right **Analytics**

Accelerate the Right **Actions**

cisco Engage

Cisco's UCS solution for Splunk

GO **BEYOND**
Cisco Engage GBA

Cisco's goal is to provide you the right infrastructure for all of your workloads, including Splunk, that can be deployed in a consistent and thoughtful manner mindful of your full landscape. CVDs provide you both your blueprints and a lab tested proof point ensuring a best in class experience for you Splunk workloads.

Turnkey infrastructure

CVD program ensures a lab tested architecture and outcome

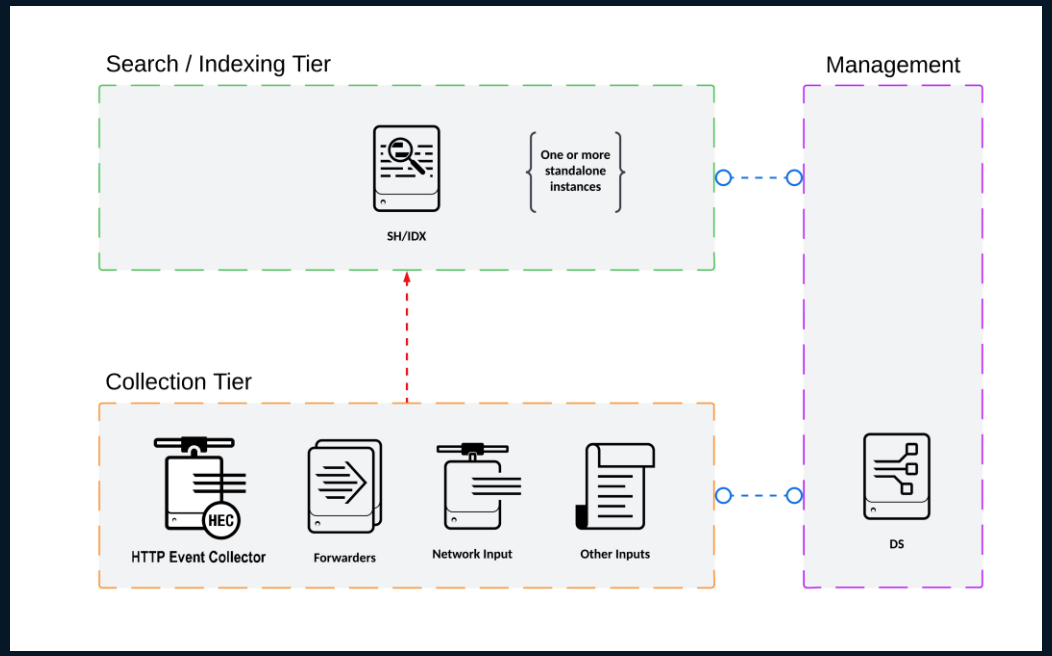
Operational simplicity

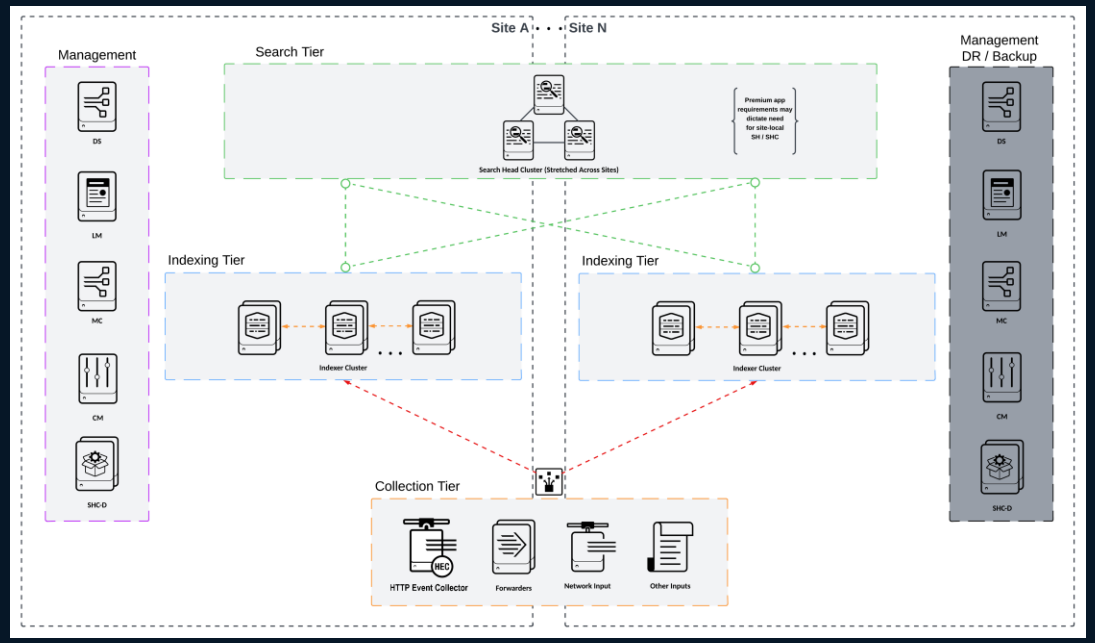
Intersight provides second to none management of resources

Scalable solution for tomorrow

Easily add resources for growth or longer retention

Architectural Options

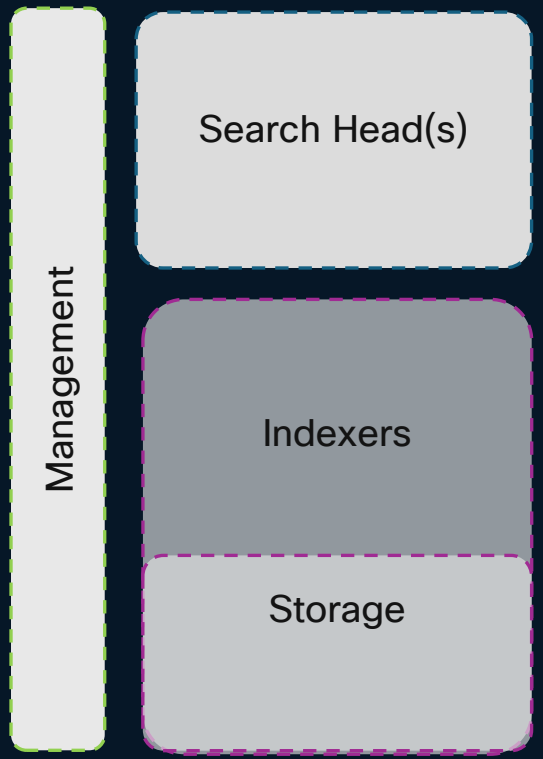




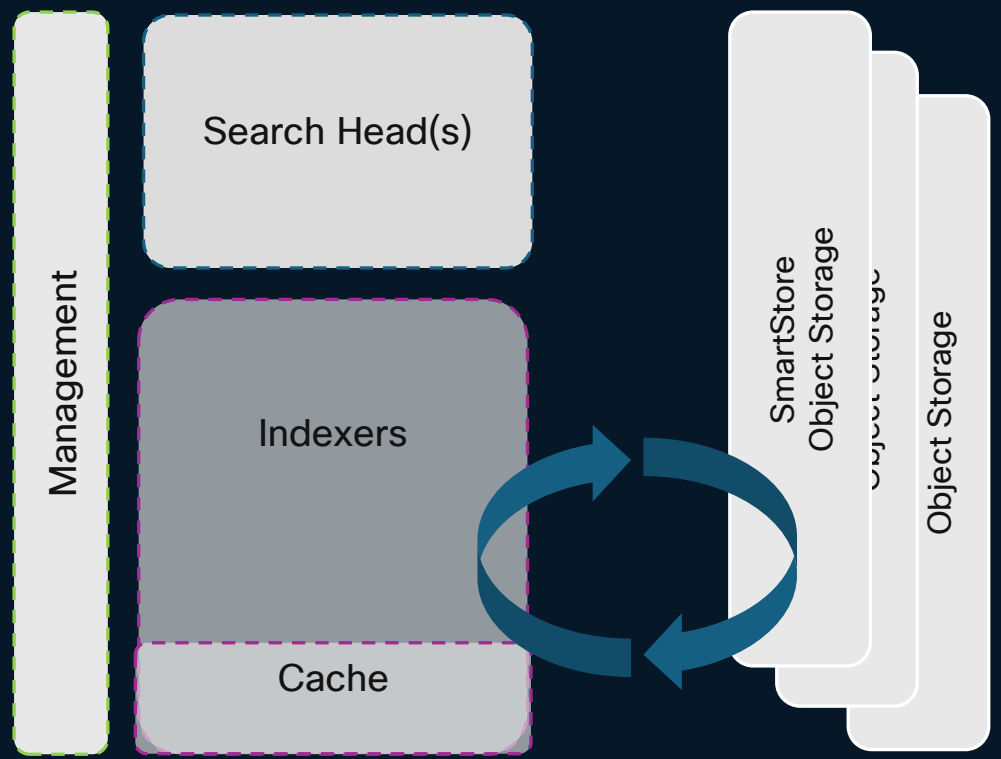
Single Server ← → Single Site Clustered ← → Multi Site

Splunk Validated Architectures support distinct use cases and requirements. Cisco Compute supports them all!

UCS Solutions for Splunk



Traditional Deployment



SmartStore Deployment

AI Readiness

80%

Of CIOs and tech leaders plan full Gen AI adoption within 3 years[1]

13%

IT organizations with infrastructure prepared for AI today[2]

36.2%

IT staff /skill recruitment and training is highest priority to support Gen AI[1]

1. IGartner: **Infrastructure and Operations Summit** November 2023
2. Cisco Global AI Readiness Index, December 2023

Cisco AI ecosystem stack

GO **BEYOND**
Cisco Engage GBA

Simplified operations

Security

Firewall | Secure workload | Robust Intelligence | Splunk

splunk>

AI frameworks	NVIDIA NGC, intel Developer Cloud
AI management tools	NVIDIA, PyTorch
Virtualization and Kubernetes	OPENSHIFT
Infrastructure management	Nexus Dashboard, Intersight
AI Infrastructure	Nexus® Series | Nexus Dashboard; UCS Series | Intersight®; NVIDIA, intel, AMD, COHESITY, FlashStack, FlexPod, NUTANIX

Observability

Observability platform | Splunk

splunk>

Sustainability

Data center | Edge | Colocation | Public cloud

AI and ML capabilities across our portfolio accelerate detection, investigation, and response.

Our approach

Domain and Splunk specific

Human-in-the-loop and trusted

Open and extensible

What we offer

Generative AI

Make sense of the signal to improve user productivity and outcomes

Foundational AI

Find the signal from the noise in vast amounts of data

Powered by Splunk AI

SECURITY

- Enterprise Security with Enterprise Security Content Updates (ESCU)
- User Behavior Analytics
- AI Assistant

OBSERVABILITY

- IT Service Intelligence
- Application Performance Monitoring
- Infrastructure Monitoring
- AI Assistant

Included Embedded AI/ML Capabilities

Assistive Intelligence Experiences

- AI Assistant for SPL
- Anomaly Detection

Customizable ML

- Machine Learning Toolkit
- Data Science and Deep Learning

Free Assistive and Customizable Apps & Tools

THE SPLUNK PLATFORM

- Splunk Cloud Platform
- Splunk Enterprise

Domain-Specific Use Cases

Security

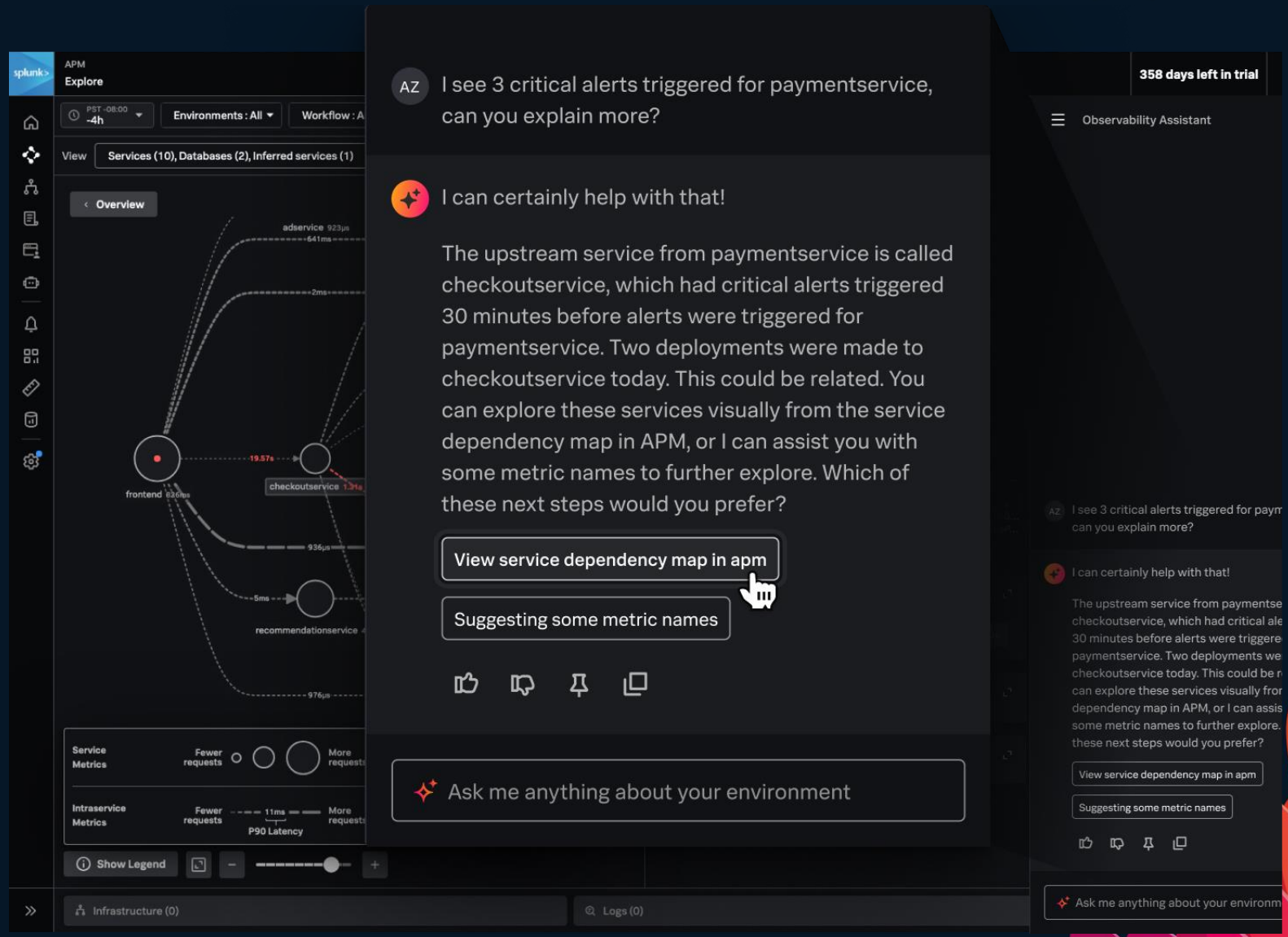
- Simplify workflows
- Guided response actions
- Event correlation and alert noise reduction
- ML powered detections
- Risk based alerting
- Predictive analytics
- Anomaly detection
- Clustering

Observability

- Probable root cause analysis
- Assisted remediation
- Suggested responders
- Proactive outage prevention assistance
- Alert correlation and prioritization
- Anomaly and outlier detection
- Adaptive thresholding

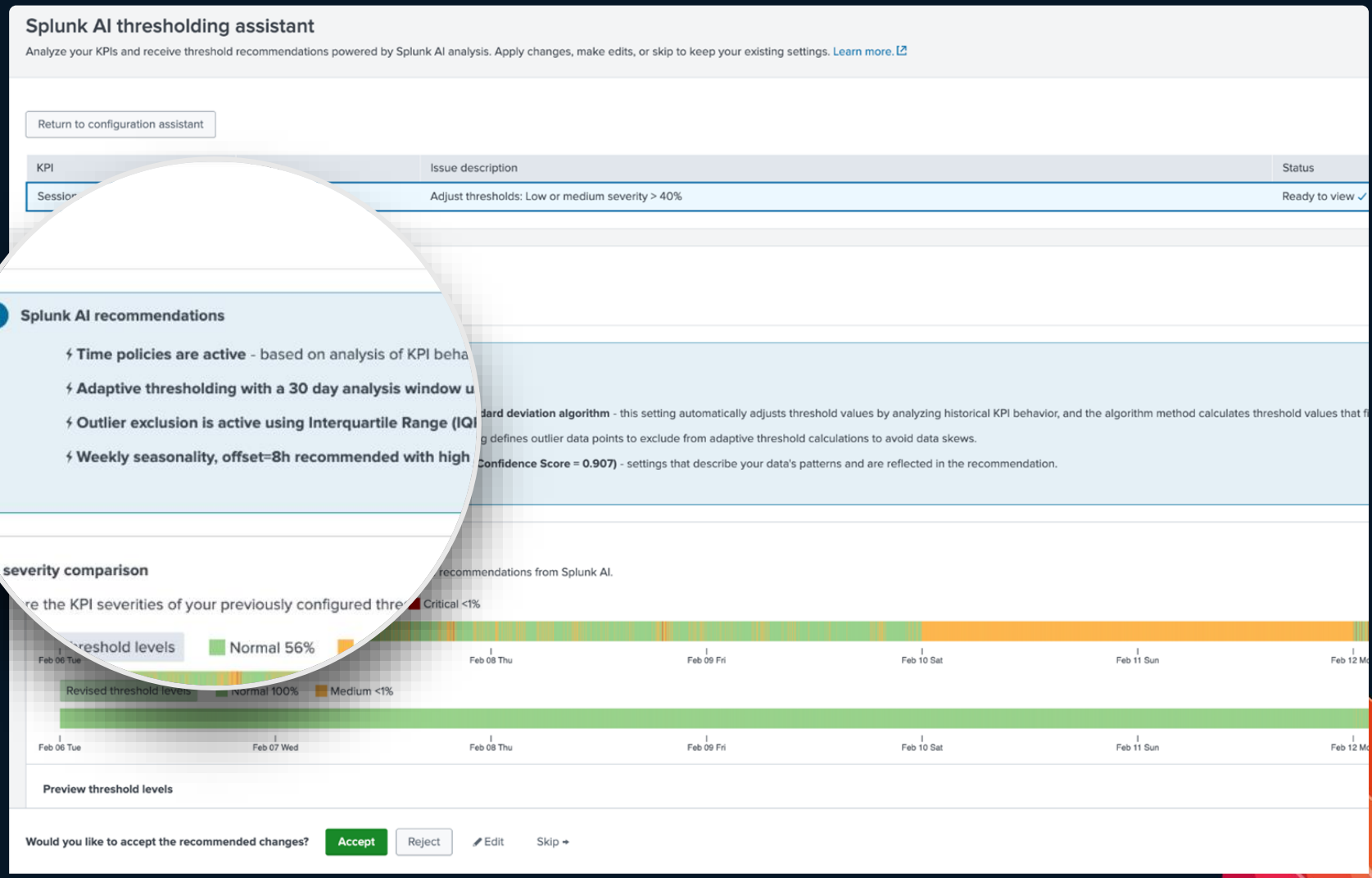
New AI Assistant for Observability

- Find and fix issues faster using natural language in Splunk Observability Cloud
- Accelerate investigations and day-to-day monitoring tasks
- Get context and support as you troubleshoot



New Foundational AI for ITSI

- Analyze IT service health in context
- Reduce alert noise with intelligent alert correlation to resolve issues faster
- Prevent outages with embedded AI and machine learning
- Align IT and the Business with service monitoring



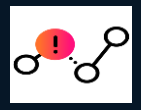
The problems we are solving using AI/ML

Predictive Analytics

Forecast the future behavior of services

Adaptive Thresholding

Automatically adjusts KPI thresholds based on historical trends

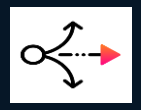


Anomaly Detection

Automatically identify unusual patters or deviations in KPI behavior

ML Assisted Thresholding

Automatically recommend optimal thresholds for KPIs



Drift Detection

Identifies when a KPI's trend changes

AI Assisted Alert Correlation

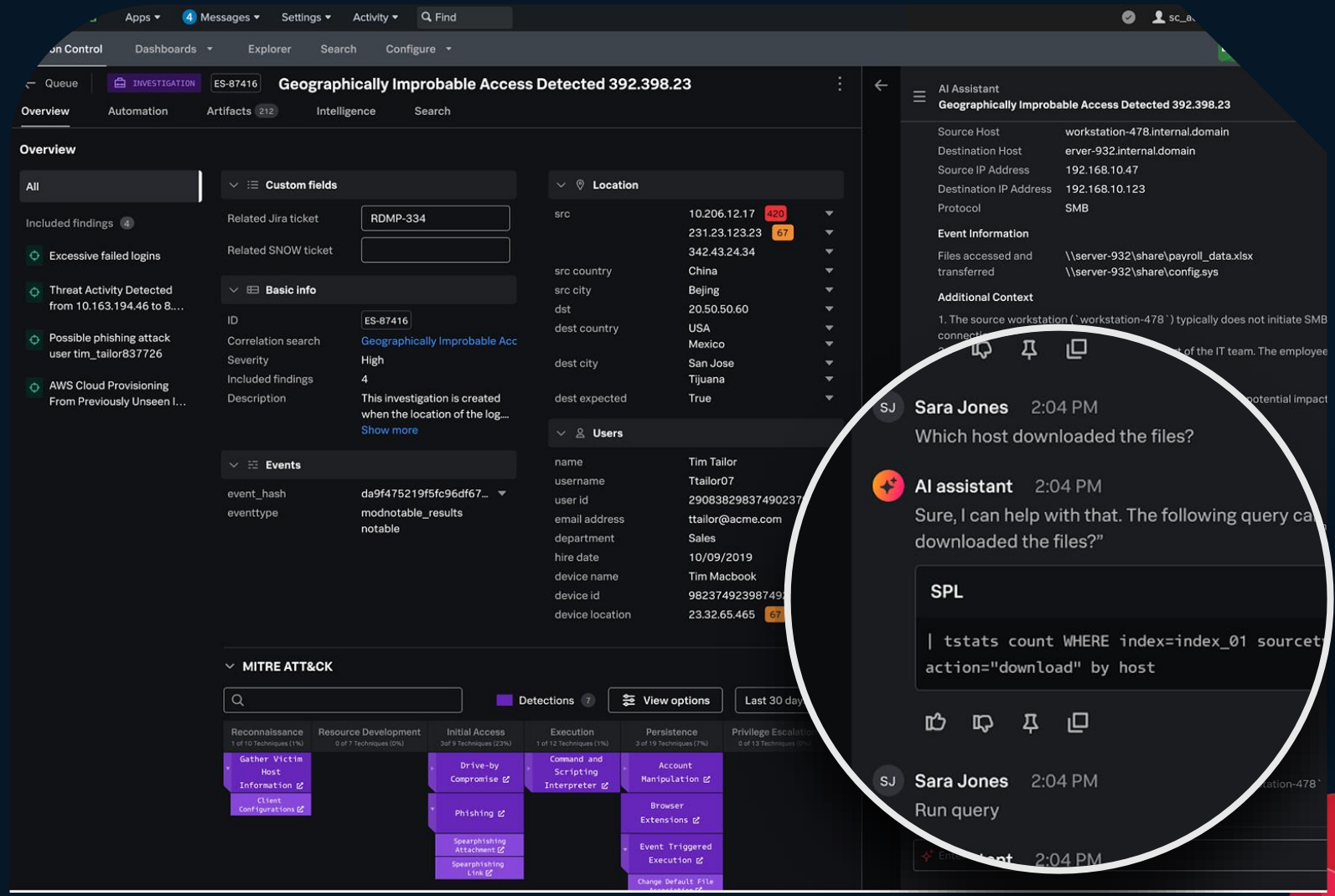
AI-driven alert correlation in to uncover patterns in your alert data

New AI Assistant for SPL

- Upskill new and advanced Splunk users quickly.
- Translate bi-directionally between natural language and SPL.
- Help security analysts that are new to Splunk to catch up in no time.

New AI Assistant for Security

- Answer analyst questions to speed up daily workflows.
- Use natural language queries to investigate more quickly.
- Save time while addressing threats more rapidly.



Accelerate Detections with ML in Splunk Enterprise Security (ESCU)

GO **BEYOND**
Cisco Engage GBA

Study Threats

Identify emerging threats and understand how they operate

Create Datasets

Collect data and use Splunk to parse the data and identify patterns that can be used to detect the threat

Build ML-Powered Detections

Build a model based on data in order to make predictions or decisions; enable systems to learn from data, identify patterns, and make decisions with minimal human intervention

Test Detections

Run queries against a dataset that simulates attacker behavior to improve accuracy and reduce false positives

Release

Package detections to deliver timely and effective protections against emerging threats to Splunk customers

Domain Generation Algorithms

DGAs are algorithms to generate random domain names used by malware families.

Domains are usually based on the date and are difficult to block because there are so many (e.g., 100k/day).

Traditional DGA

fmeajblnlqgyijlfqswfevokbkj[.]ru
i0rxagnbyd4a1jug4qb1uwd6np[.]org
y9qd1f1hhcb7f1fr5mgqw5ypq[.]net

Dictionary DGA

marketexpresspicturereport[.]com
destroyready[.]net
vacuum-exclusion[.]net

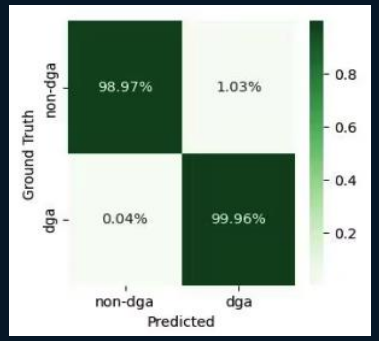
Dictionary DGA Detection (D3)

Dictionary DGA:

- Composed of actual words, dictionary DGAs look more plausible to both humans and algorithms and are more difficult to detect.

Detection model:

- Pre-trained LSTM model for DGA detection provided by Splunk.
- Detection rule provided on ESCU.
- Inference using Splunk DSDL app.



Stage 3: Expansion
You're ingesting advanced data sources and running better investigations.

Detect Dga Domains Using Pretrained Model In Dsdl

The following analytic uses a pre trained deep learning model to detect Domain Generation Algorithm (DGA) generated domains. The model is trained independently and is then made available for download. One of the prominent indicators of a domain being DGA generated is if the domain name consists of unusual character sequences or concatenated dictionary words.

MITRE ATT&CK Techniques (Click for Detail)

Dynamic Resolution | Domain Generation Algorithms

Data Sources

DNS

Data Model

Network_Resolution

Asset Type

Endpoint

References

https://attack.mitre.org/techniques/T1568/002/
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
https://en.wikipedia.org/wiki/Domain_generation_algorithm

https://research.splunk.com/network/92e24f32-9b9a-4060-bba2-2a0eb31f3493/

Detect suspicious DNS TXT records

DNS TXT records detection:

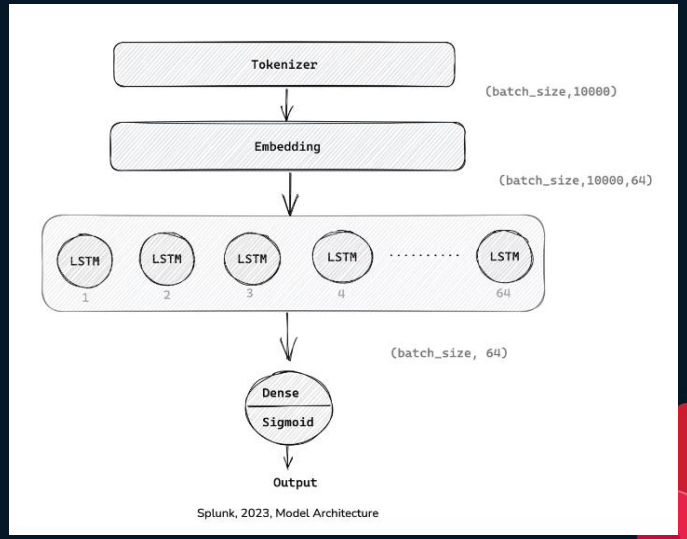
- DNS TXT records are frequently used for malicious purposes to create DNS amplification attacks, injection of malware and exfiltrate data from the victim's machine.
- The freedom of unstructured text poses a huge security threat and makes it hard to detect.

Detection model:

- Pre-trained LSTM model for DNS TXT records provided by Splunk Threat Research.
- Detection rule provided on ESCU.
- Inference using Splunk DSDL app.

Detect Suspicious DNS Txt Records Using Pretrai...

The following analytic uses a pre trained deep learning model to detect suspicious DNS TXT records. The model is trained independently and is then made available for download. The DNS TXT records are categorized into commonly identified types like email, verification, http using regular expressions https://www.tide-project.nl/blog/wtmc2020/. The TXT



Splunk, 2023, Model Architecture

https://www.splunk.com/en_us/blog/security/ml-in-security-detect-suspicious-txt-records-using-deep-learning.html

Common PowerShell obfuscations

GO BEYOND
Cisco Engage GBA

Just a few of the available techniques

Base64

The PowerShell `-encodedcommand` parameter accepts a base64 string that can be used to hide commands

```
powershell -encodedcommand ENCODING
```

There are many variations, including `-e`, `-enc`, `-ec`, `-encodedc`, etc.

XOR

Another common encoding scheme is PowerShell's bitwise XOR operator, `-bxor`

String concatenation (+, –, “, ‘)

```
New-Object
$("Sys"+"tem.Refl"+"ection.Ass"+"embl"+"yNa
me")
```

Escaping (^)

```
powershell.exe –^e^n^c^ ENCODING
```

Mixed Upper / Lower case

```
(nEw-oBjecT Net.WeBclIENt)
```

Whitespaces

```
DownloadString(“ https://bit.ly/3dV6cFr ”)
```

What if these are combined?!?!

Detect Powershell Suspicious Script

Why attackers choose powershell?

- Installed by default, Execute payloads from memory, Encryption, Easy to obfuscate, Easy access of malicious script.

Detection model:

- BERT model fine-tuned on classification for decoded powershell scripts.
- Delivered in ONNX format through Splunk DSDL app.
- To be shipped as an ESCU detection rule.

Machine Learning Toolkit 5.5

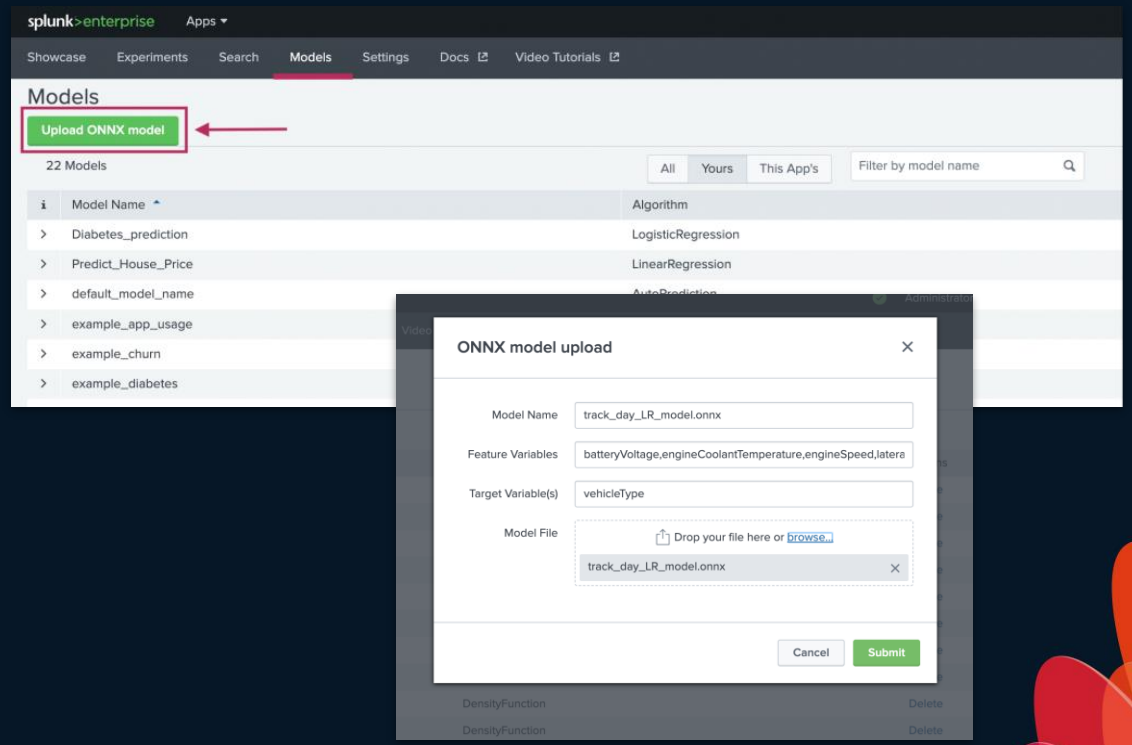
Extend Splunk to Operationalize Machine Learning Use Cases Within Search

Designed for Splunk users at all levels

- ML-Powered Splunk Searches
  - Apply techniques like anomaly detection and predictions
- Showcase and Experiments
  - Simple low-code experience to guide model building, testing, and deployment
- Extensible out of the box
  - 80+ built-in scikit-learn algorithms, and API support to plug in new runtimes

New updates!

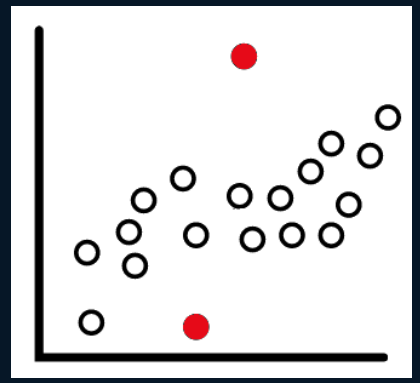
- Ability to upload externally pre-trained ONNX models with a simple UI and then use the model with your Splunk data with no modification to your existing workflows
- Extended user anomaly detection capabilities with a new algorithm for multivariate outlier detection



ML-Powered Detections for Security & Observability

Find the Obscure and Unknown Threats Buried Deep in Your Data

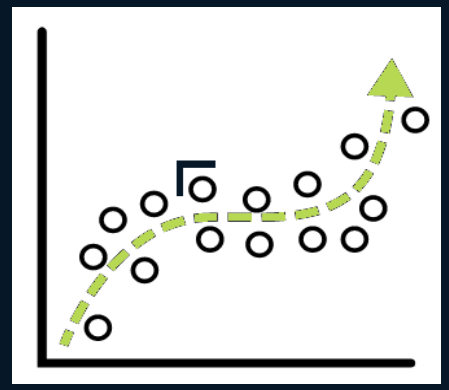
Anomaly detection



Deviation from past behavior

Resource Utilization
Error Rate Deviation
Access Pattern Baselining

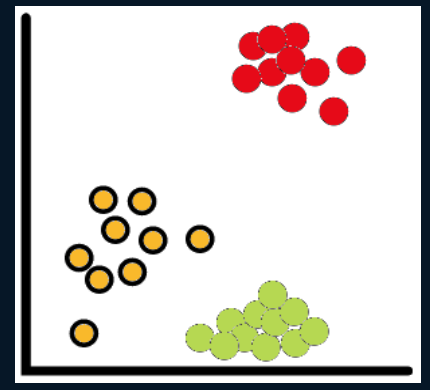
Predictive Analytics



Future state prediction
Classification/regression

Predict storage requirements
Identify patterns leading to failure

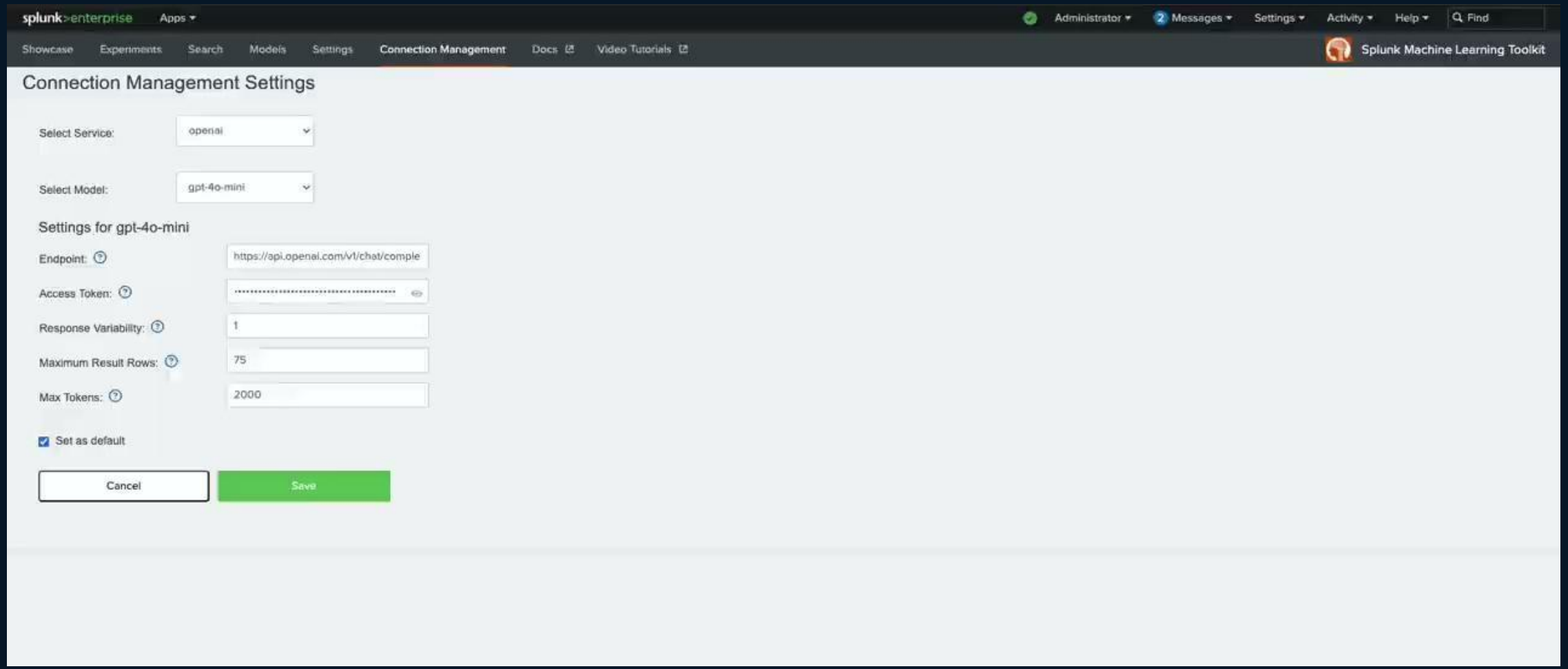
Clustering



Behavioral Analytics

Identify Traffic
Classify Behaviors

Coming next in MLTK 5.6 – AI Commander

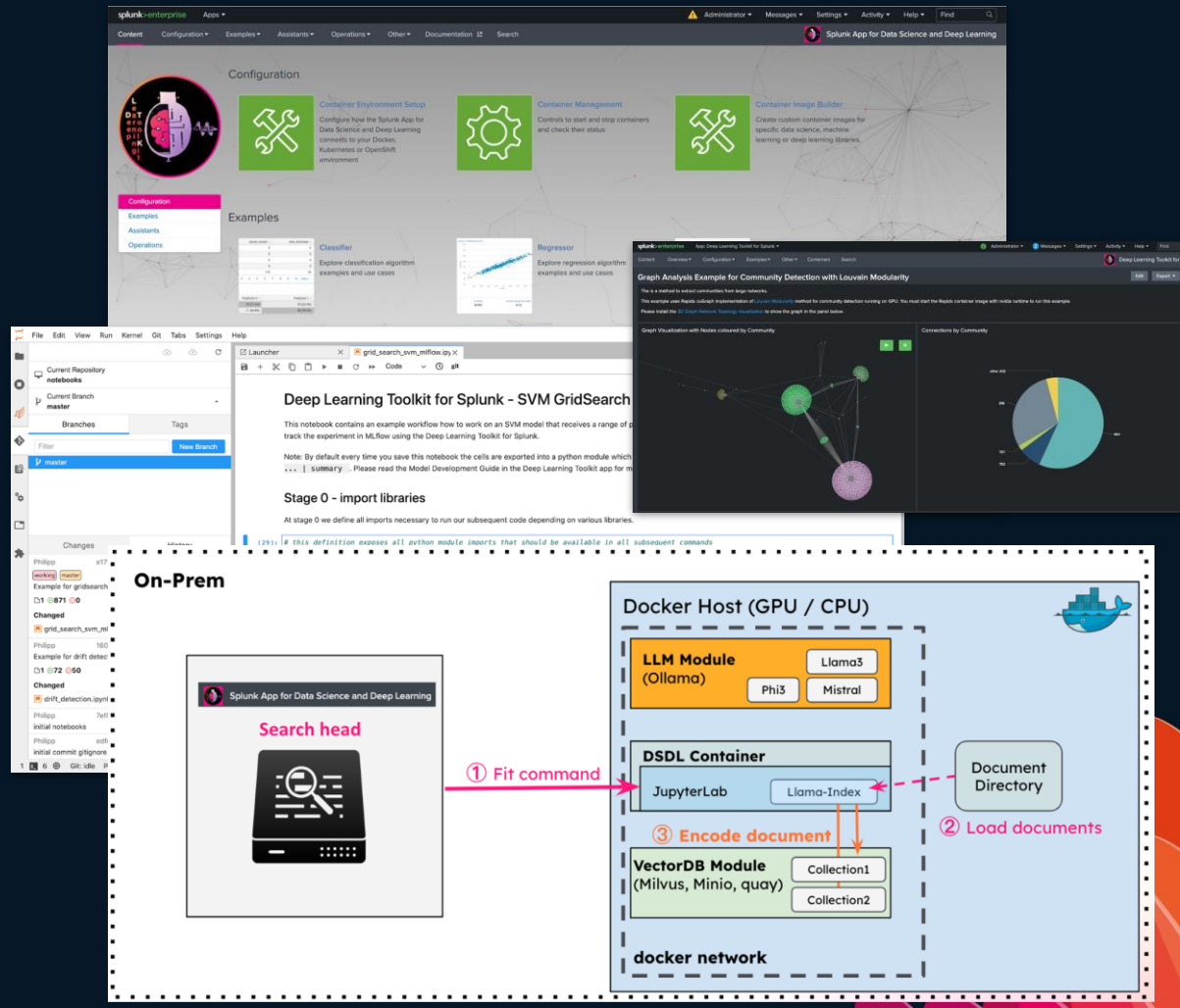


Splunk Data Science and Deep Learning 5.2

Extension for MLTK to operationalize advanced custom AI / ML use cases

Built for Data Scientists / AI Engineers

- Guided models and code examples
- Container Management: Models can be productionized on CPU & GPU
- Extension to LLMs and VectorDB
- State of the art AI frameworks and tools - Jupyter Lab, MLflow, PyTorch, TensorFlow, SpaCy, DASK, Rapids, Spark, ...
- Flexible deployments: deploy on-prem, hybrid or in the cloud.

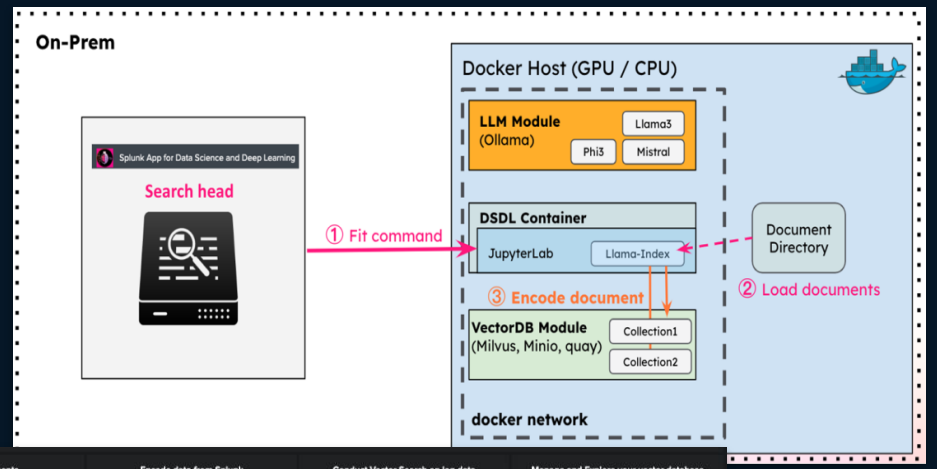


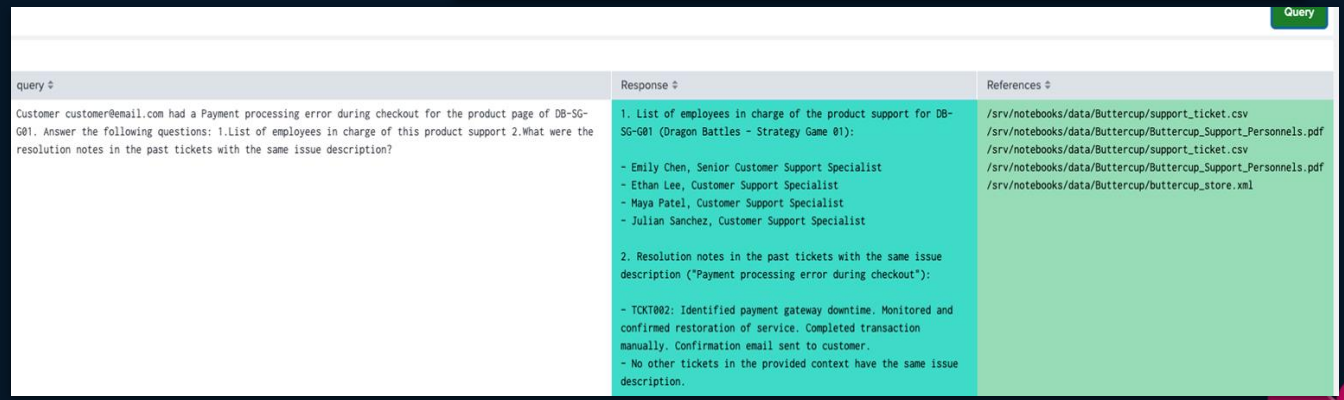
Splunk Data Science and Deep Learning 5.2

Extension for MLTK to operationalize advanced custom AI / ML use cases

New updates in version 5.2*!

- Container extensions for LLM and VectorDB services to enable highly customizable AI use cases.
- Custom LLM RAG based applications built on Splunk indexed data and non-Splunk, external data sources
- New dashboards to easily access the new features
- All codebase shared in the public github repo to start building own extensions or use cases.





Global Insurance Company

GO BEYOND
Cisco Engage GBA

Protect Application Security with Splunk ML

- Utilize Splunk AI to explore, model and deploy more easily
- WAF data to be alerted on anomalies and surface them in ticketing system
- Use Splunk's Machine Learning Toolkit for modeling
- DensityFunction to detect anomalies; model trained off hours
- Consult the SME to make sure findings are inline with business needs

2/3 ↓
Reduction in the Number of queries from 300+ detections to <100

40% ↓
Reduction in incidents generated

100+ hrs/month ↓
Reduction in time allocated to incident response & detection maintenance

A Top 3 Ivy School

GO **BEYOND**
Cisco Engage GBA

Deep Learning for Compromised Account Detection

- 5 people security team accountable for 40,000 active accounts
- Need to protect accounts against advanced threat actors
- Despite 2FA more account compromises in the last recent time
- Leverage DSDL for deep learning (LSTM model) to predict account compromise from complex time-series data obtained from Splunk SIEM

Unparalleled digital resilience.

+

Providing **end-to-end visibility** and insights across your entire digital footprint

Powering the **SOC of the future** with unified threat detection investigation and response, enhanced with network insights

Delivering **observability for the entire enterprise** to prevent unplanned downtime across all environments

Unified by a flexible platform that provides enterprise scale data management

cisco Engage

GO BEYOND
Cisco Engage GBA

Thank You!