

# Splunk4Ninjas - Machine Learning for Security

Hands-On Workshop



# Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as "expects," "anticipates," "targets," "goals," "projects," "intends," "plans," "believes," "momentum," "seeks," "estimates," "continues," "endeavors," "strives," "may," variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. 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. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the "Risk Factors" section of Cisco's most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the "Risk Factors" section of Splunk's most recent report on Form 10-Q filed with the SEC on November 28, 2023. 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 Cisco or Splunk, on Cisco or Splunk's website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or 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 or be relied upon in making a purchasing decision. We undertake no commitment, promise or 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. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

---

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

# Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



# Workshop Agenda

- What is Machine Learning?
- Why do we need Machine Learning in security?
- Machine learning for security with Splunk
- Time for practice!
- Ready made applications leveraging ML
- What's next?





# Enroll in Today's Workshop

## Tasks

1. Get a splunk.com account if you don't have one yet:  
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:  
<https://show.splunk.com/event/<eventID>>
3. Download the hands-on lab guide:  
<https://splk.it/ML-Sec-Lab-Guide>

Contains step-by-step instructions for all of today's exercises!

1. Download a copy of today's slide deck:  
<https://splk.it/ML-Sec-Attendee>

## Goal

Available    Enrolled

Search events    Invited

Private event

PLATFROM

Splunk4Rookies

01/16 (10:37) - 01/16 (18:29)

Europe/London (GMT +00:00)

Available

Enroll

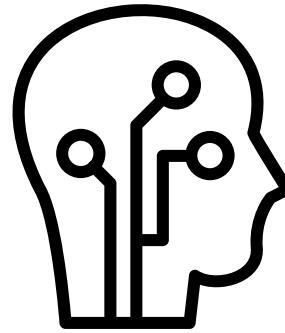
Enroll in today's event

# What is Machine Learning?



# What is AI and Machine Learning?

## Definitions

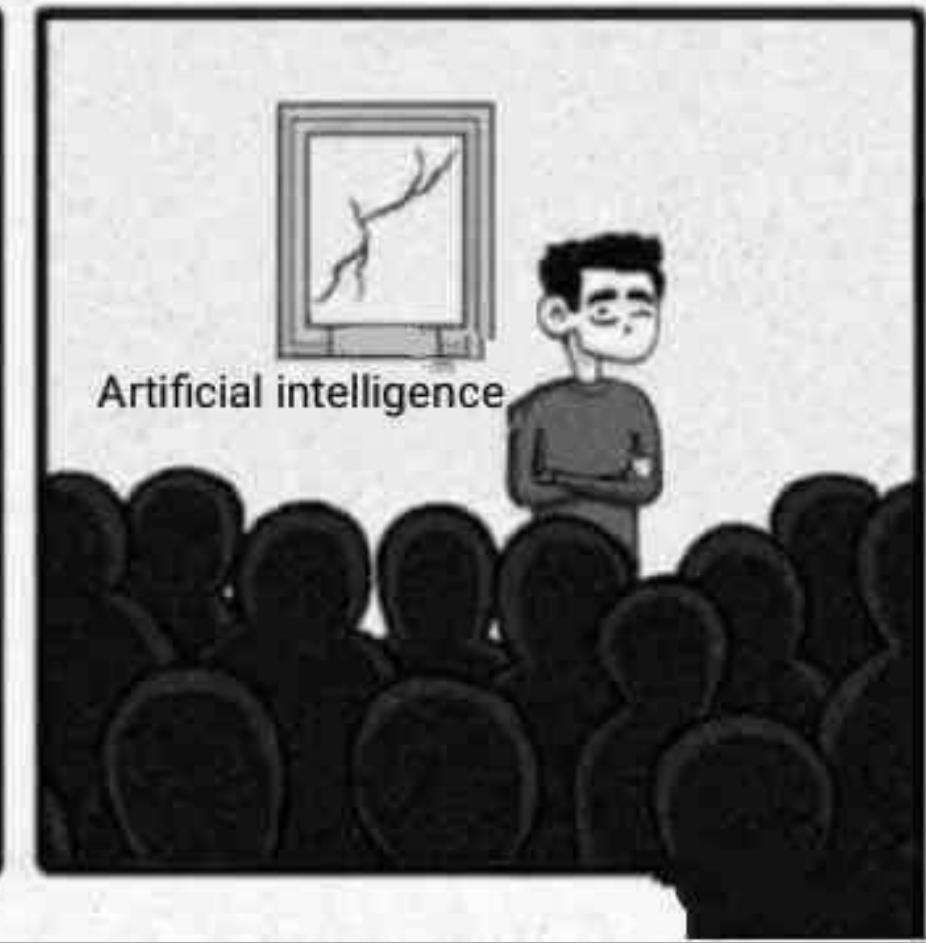
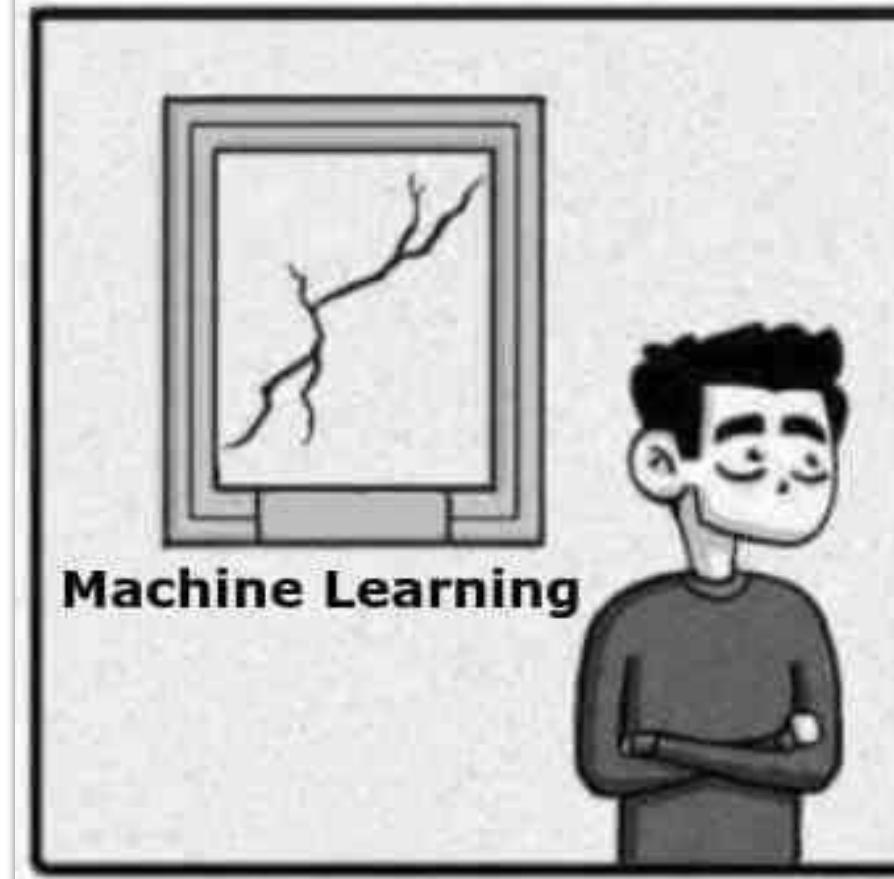
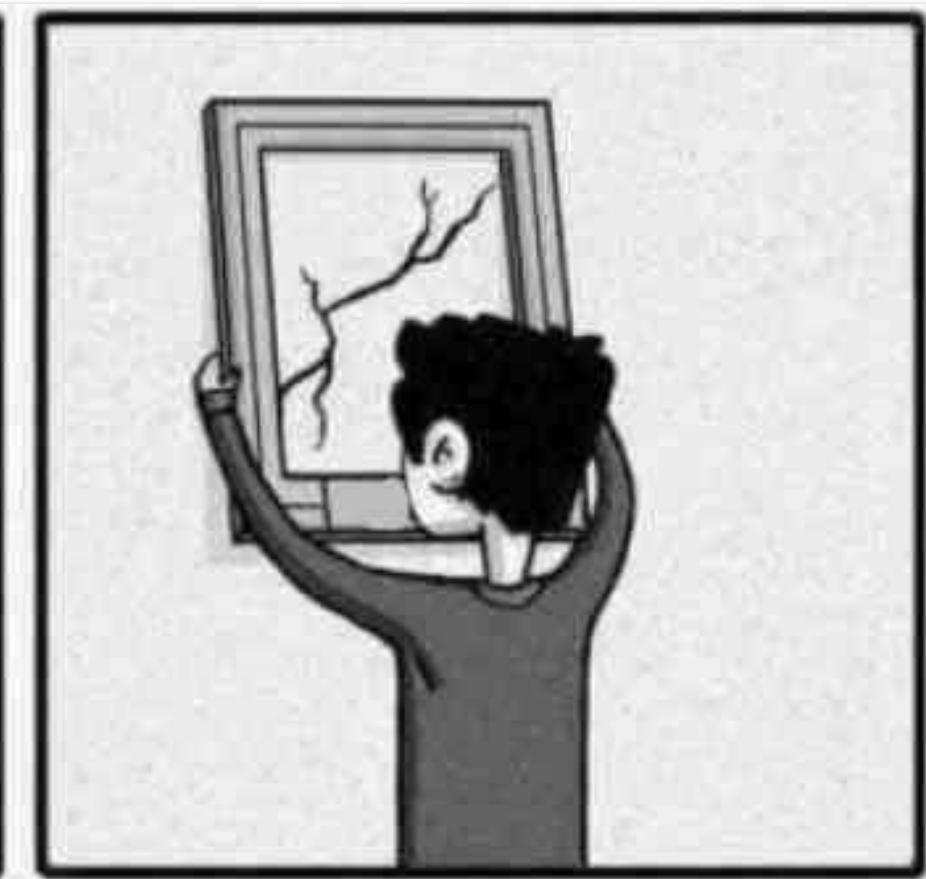
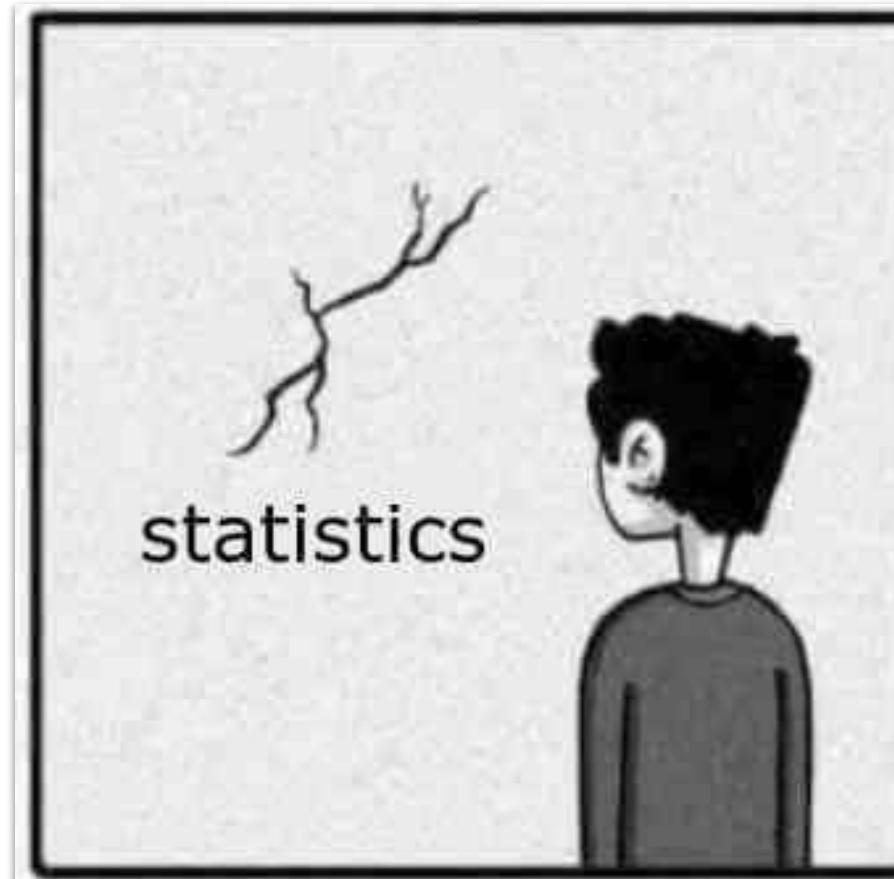


**Artificial Intelligence (AI)** - capability of a computer system to **mimic human cognitive functions** such as learning and problem-solving

**Machine Learning (ML)** - **subset of AI** that uses mathematical models of data to help a computer learn without direct instruction

**Deep Learning** - **subset of AI** that uses computationally intense ML models inspired by the “deep” layers of the biological neural network of the human brain to accomplish complex goals like image recognition *Example: Self driving car recognizes stop sign*

**Generative AI** - **subset of AI** that involves the use of algorithms and techniques to generate new data, things that have not existed in the world before being created by the models *Example: OpenAI's ChatGPT*



© Thomas Wiecki, Ph.D., ODSC Europe 2018

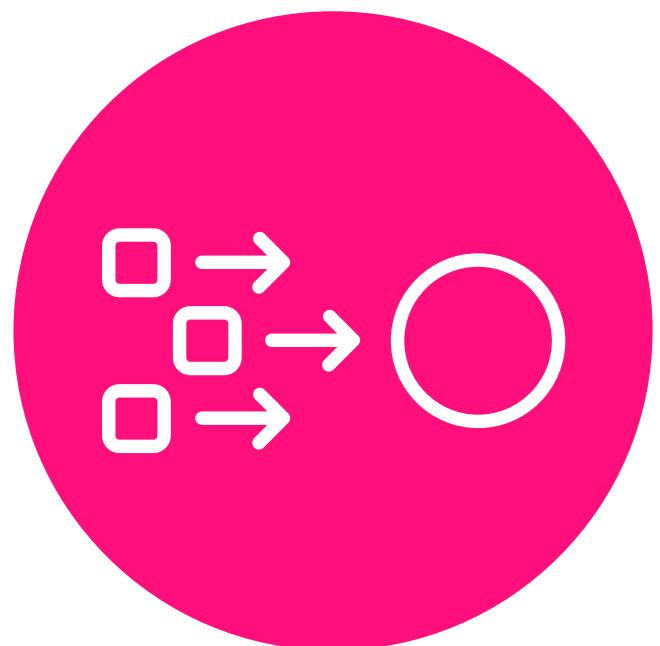
“

**Machine learning (ML) is the study of computer algorithms that improve automatically through experience and past behaviour.**

- Wikipedia

# Machine Learning

The capability of systems to acquire their own knowledge, by extracting patterns



Use complex statistical or probabilistic models to identify patterns in information



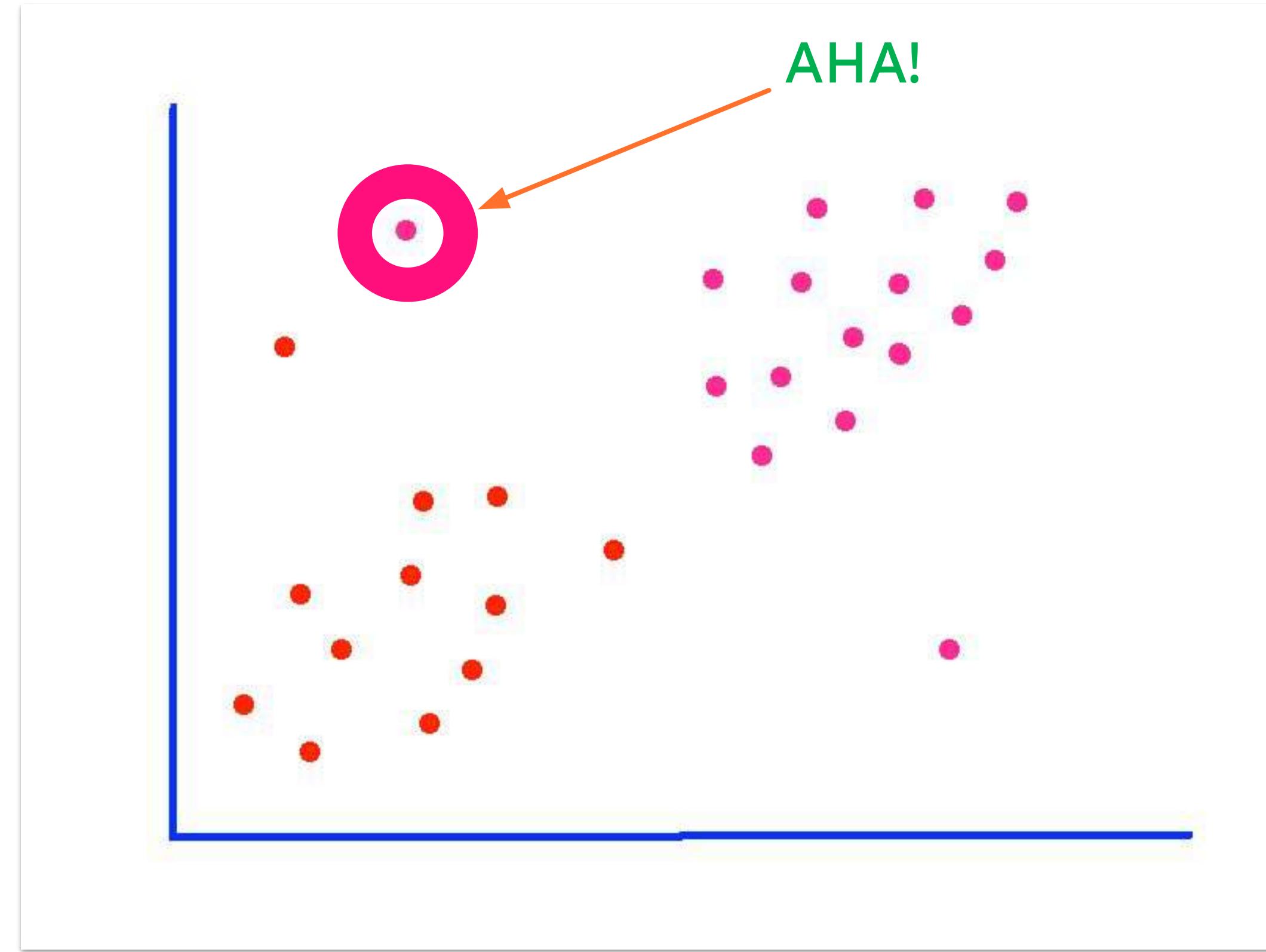
Catalog the patterns and in some cases iterate them as new data is received



Use information from learnt patterns to understand and interpret new data or make predictions

# Correlation

This is NOT ML



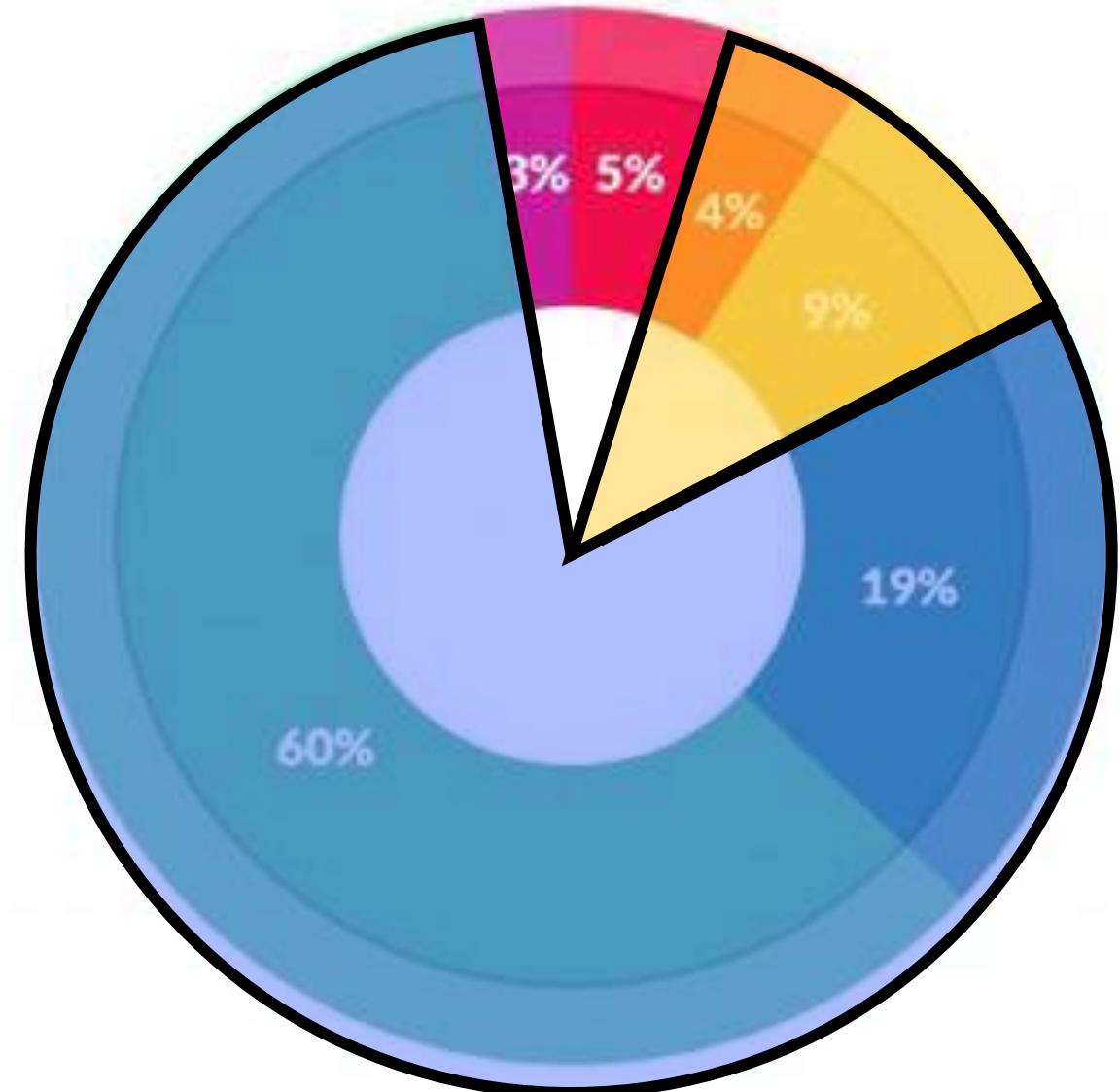
# Machine Learning

Why do we need it?

- Basic statistical modelling techniques (such as prediction using means and standard deviations) are not always fine grained enough to answer these questions accurately
- Machine Learning (ML) uses complex statistical techniques to provide better predictions to these types of questions
- For many organizations using their data to make pre-emptive or targeted decisions is becoming increasingly important, for example:
  - Detect the presence of Botnets in their network
  - Detecting a user account that has been compromised
  - Preventing fraud in banking by detecting malicious accounts or anomalous activity
  - Classifying customers for more targeted advertising campaigns in social media
  - Forecasting demand for products in support of supply chain management

# What Data Scientists Really Do

**Data Preparation** accounts for about 80% of the work of data scientists



What data scientists spend the most time doing

- *Building training sets: 3%*
- *Cleaning and organizing data: 60%*
- *Collecting data sets: 19%*
- *Mining data for patterns: 9%*
- *Refining algorithms: 4%*
- *Other: 5%*

“Cleaning Big Data: Most Time-Consuming, Least Enjoyable Data Science Task, Survey Says”, Forbes Mar 23, 2016

# ML Starter

## Dos and Don'ts

### What Machine Learning isn't...

- Something you can throw all your data at and expect an answer
- A one size fits all answer to all your data problems (a.k.a. a magic button)
- Artificial Intelligence...
- The predict command
- Correlation rules

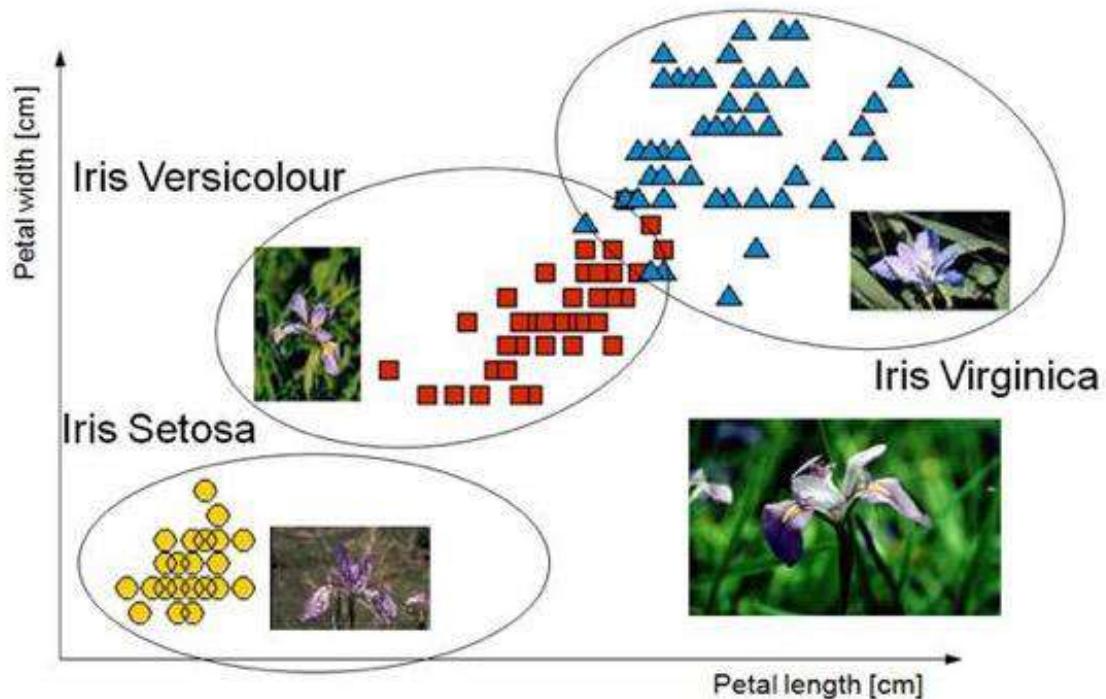
### What Machine Learning is...

- A good way of spotting and baselining patterns in data for future detection
- Useful only when you have a well defined and bounded problem, and clearly understand the data that you need to use

# Types of Machine Learning

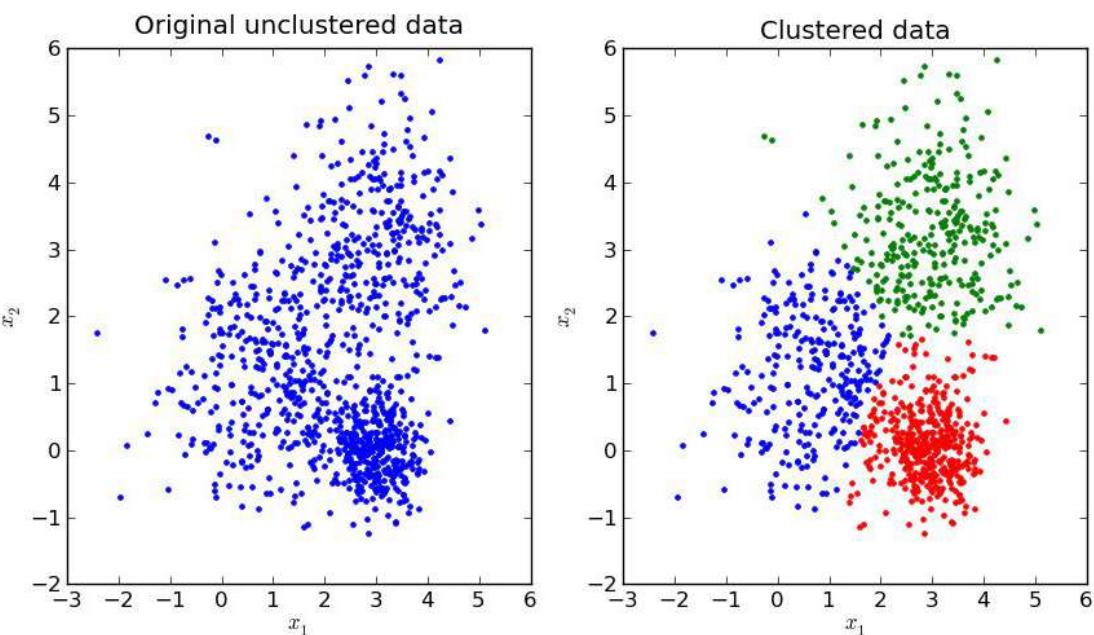
## Supervised Learning (labeled data)

- Regression
- Classification



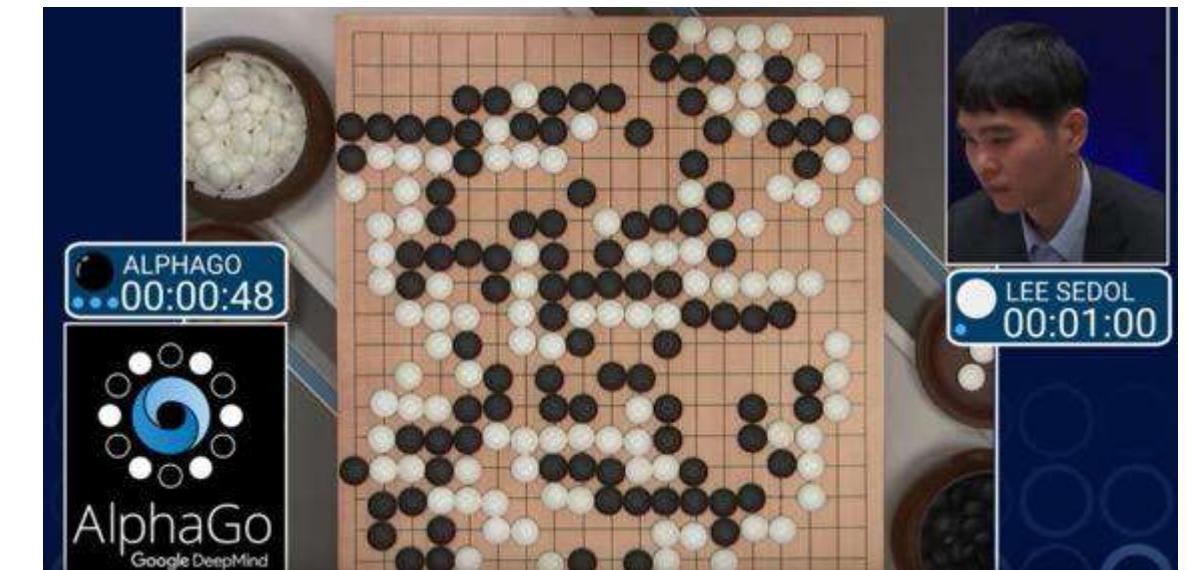
## Unsupervised Learning (unlabeled data)

- Clustering
- Anomaly Detection



## Mixed Models (with reinforcement or feedback)

- Human in the Loop
- Autonomous Systems

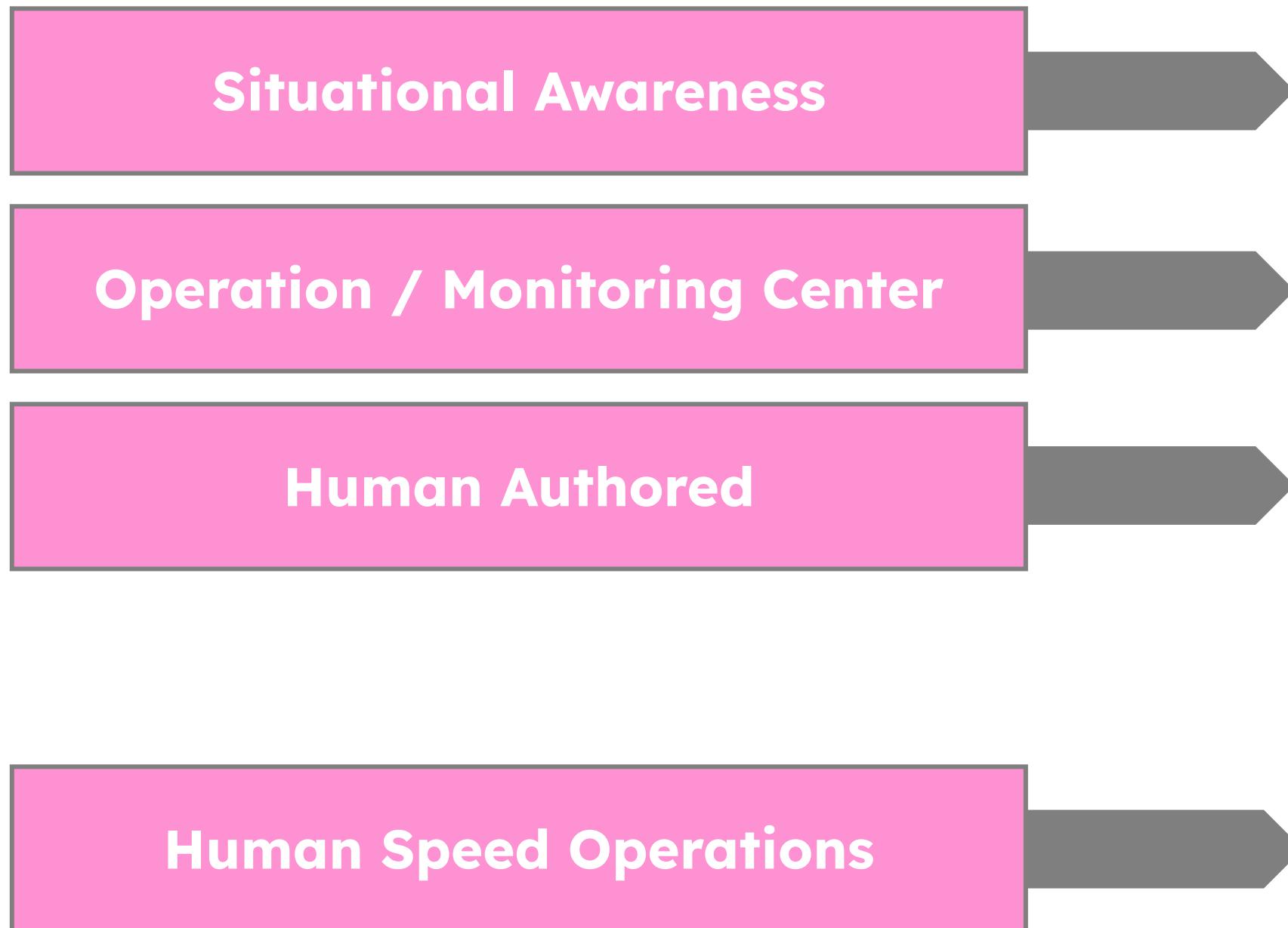


# Why Do We Need Machine Learning in Security?

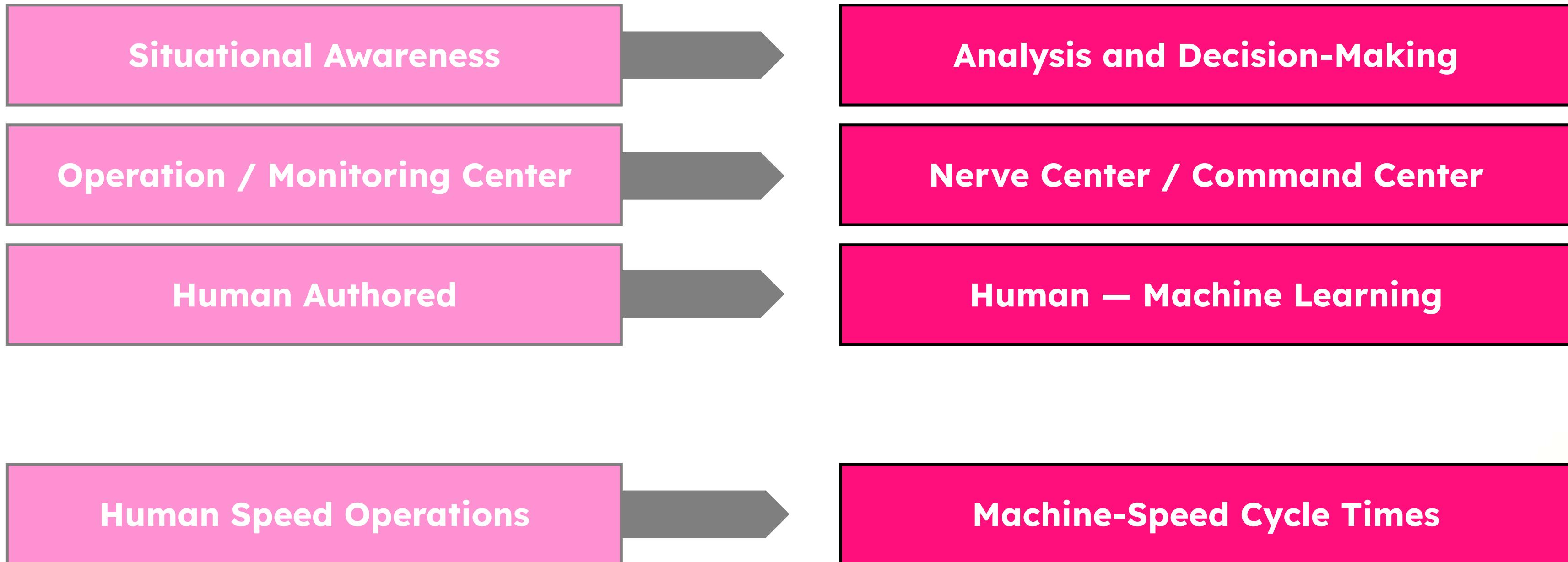


# Shifting Focus and Role for SOCs

## LEGACY

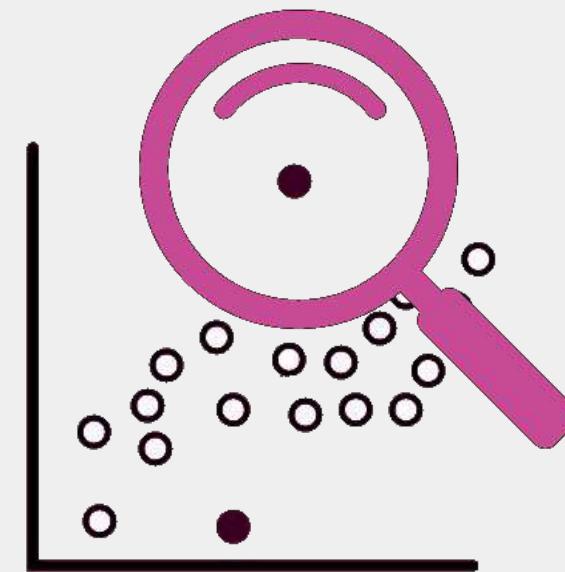


## REQUIRED



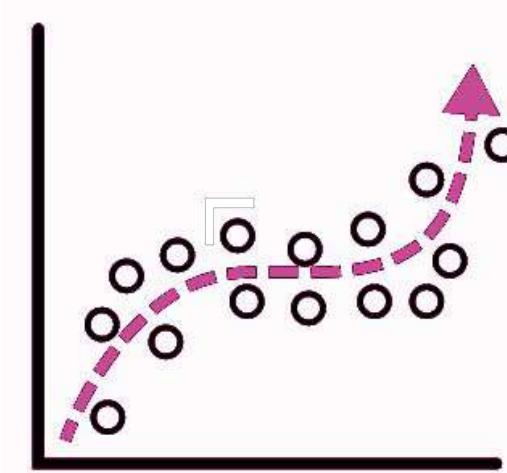
# Splunk Customers Want Answers from their Data

## Anomaly detection



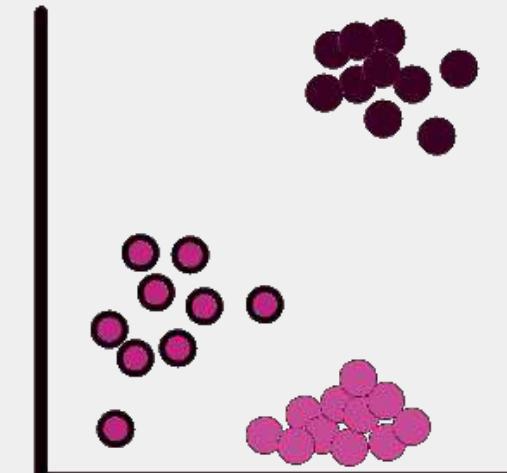
- Deviation from past behavior
- Deviation from peers
- (aka Multivariate AD or Cohesive AD)
- Unusual change in features

## Predictive Analytics



- Predict Service Health Score/Churn
- Predicting Events
- Trend Forecasting
- Detecting influencing entities
- Early warning of failure

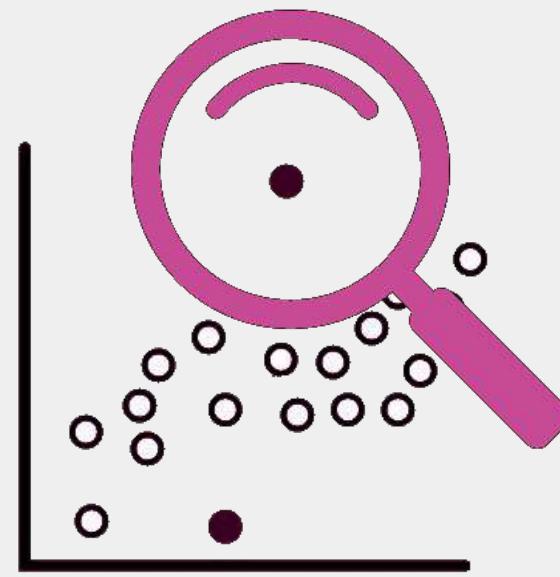
## Clustering



- Identify peer groups
- Event Correlation
- Reduce alert noise
- Behavioral Analytics

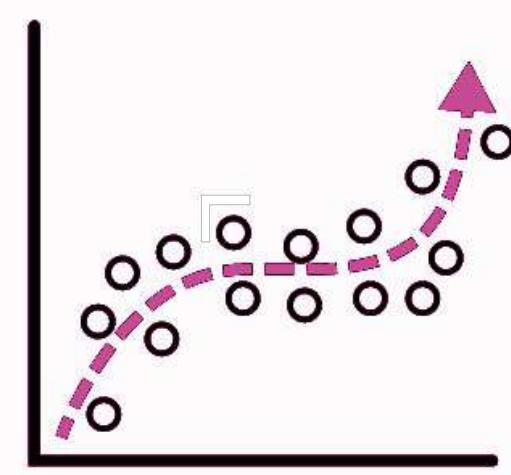
# Security Examples

## Anomaly detection



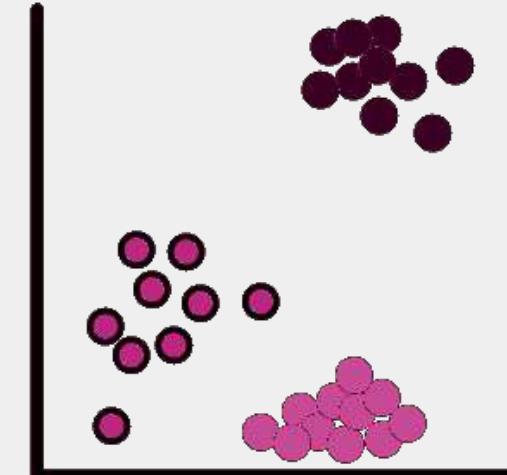
- Useful when trying to detect unwanted and unexpected behaviour.
- Useful when detecting low and slow attacks that operate over a long time.

## Predictive Analytics



- Predict the outcome of an alert (FP/TP) based on observed previous responses.
- Generate response recommendations based on observed previous responses.

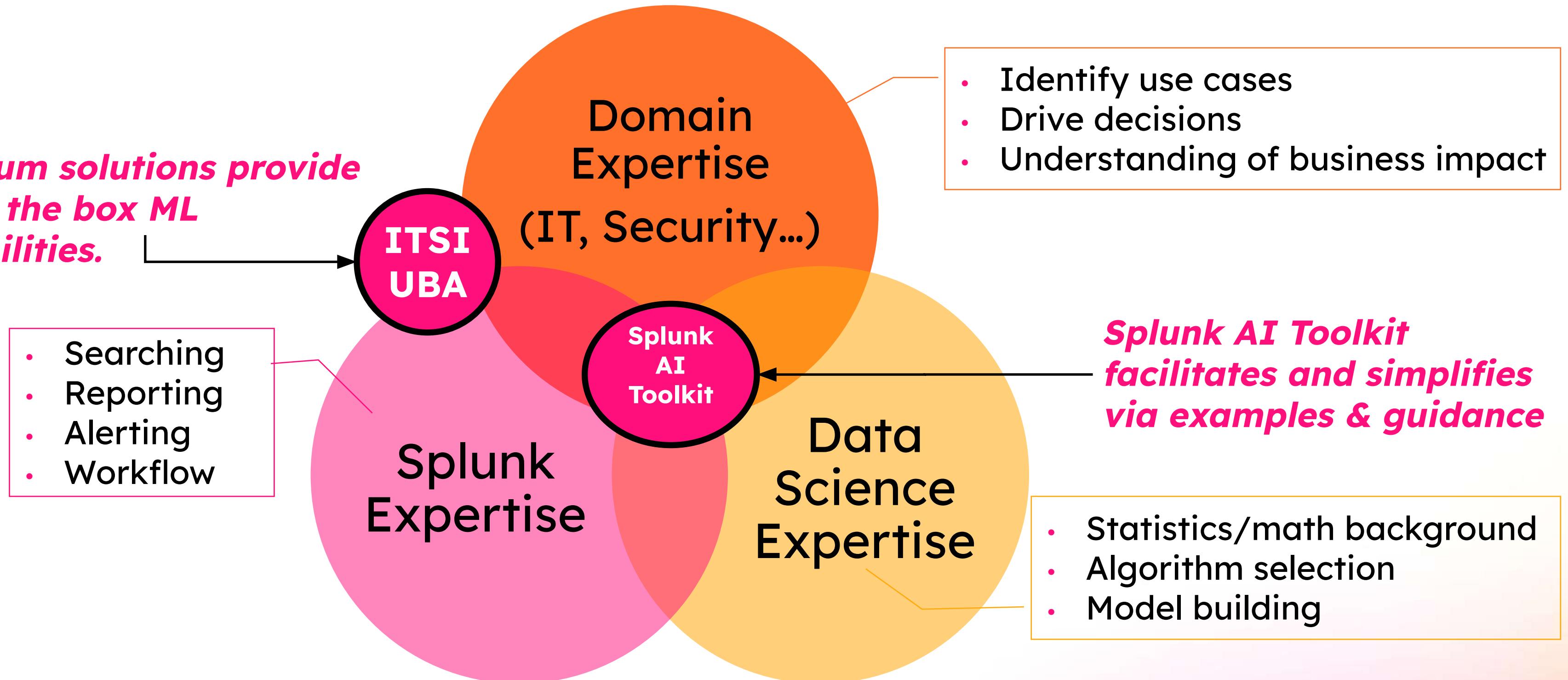
## Clustering



- Used to generate dynamic peer groups based on observed events.
- Used to group similar alerts.

# Skill Areas for Machine Learning @ Splunk

*Premium solutions provide out of the box ML capabilities.*



# Custom ML with the Splunk Platform

## Ecosystem

Splunk's App Ecosystem contains 1000's of free add-ons for getting data in, applying structure and visualizing your data giving you faster time to value.

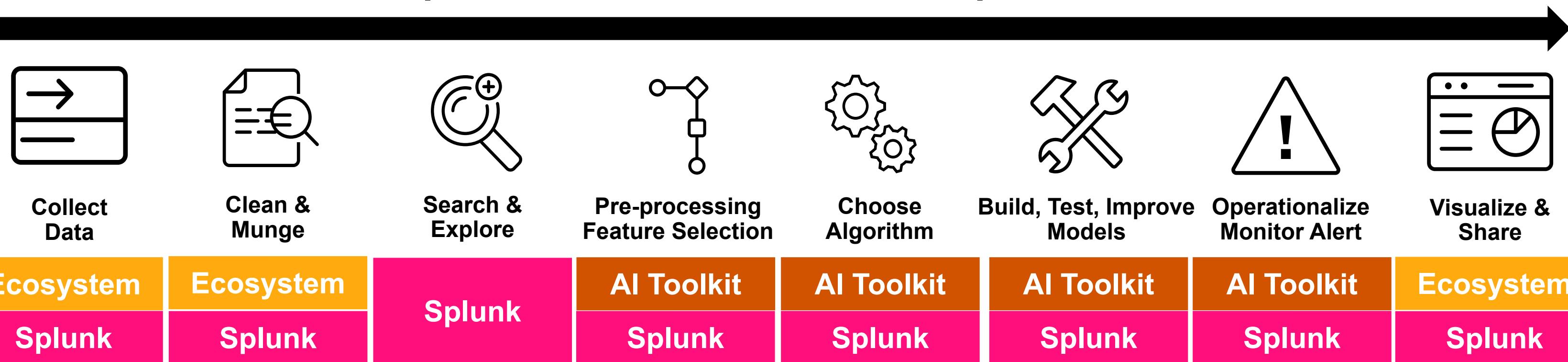
## AI Toolkit

The Machine Learning Toolkit delivers new SPL commands, custom visualizations, assistants, and examples to explore a variety of ml concepts.

## Splunk

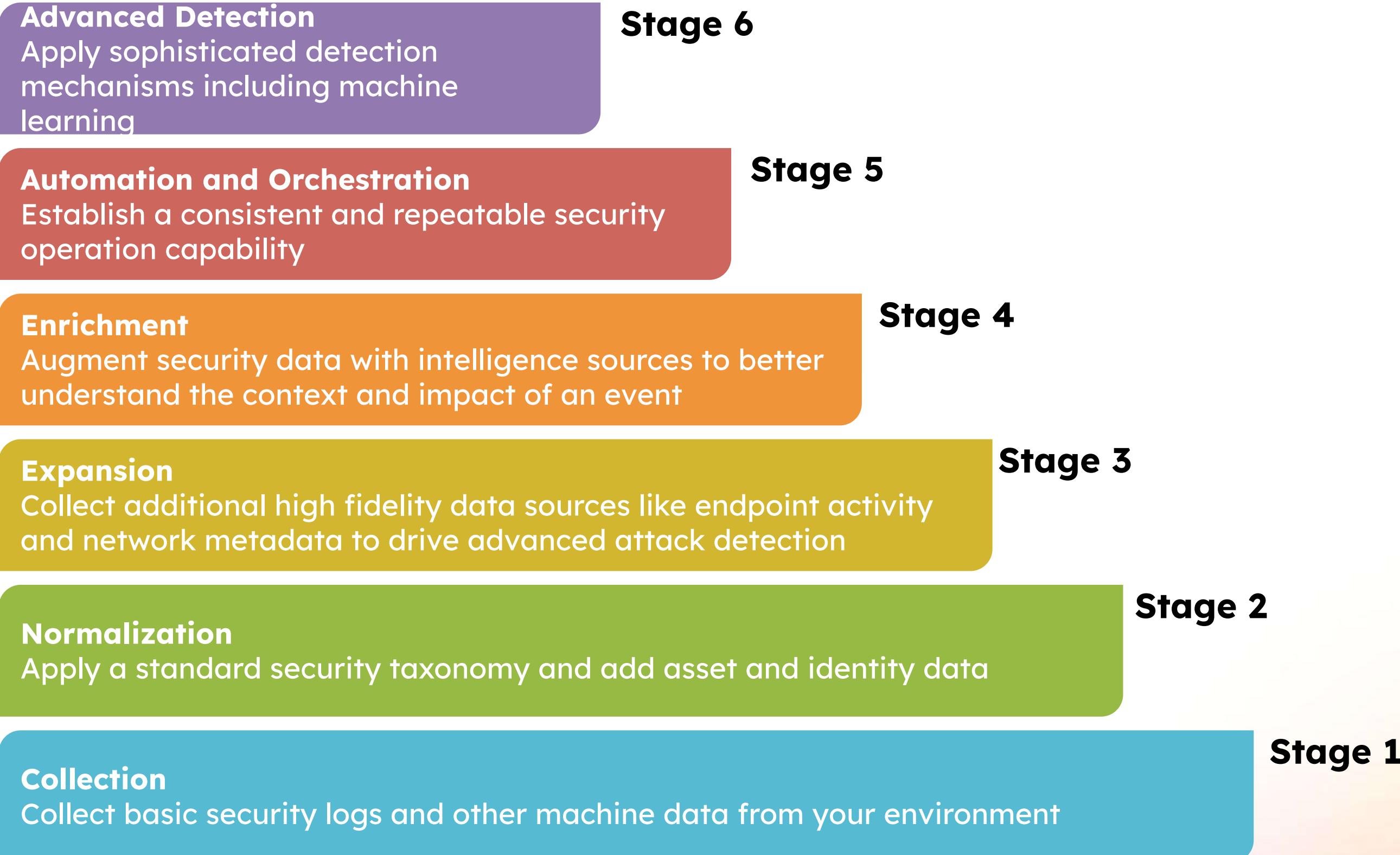
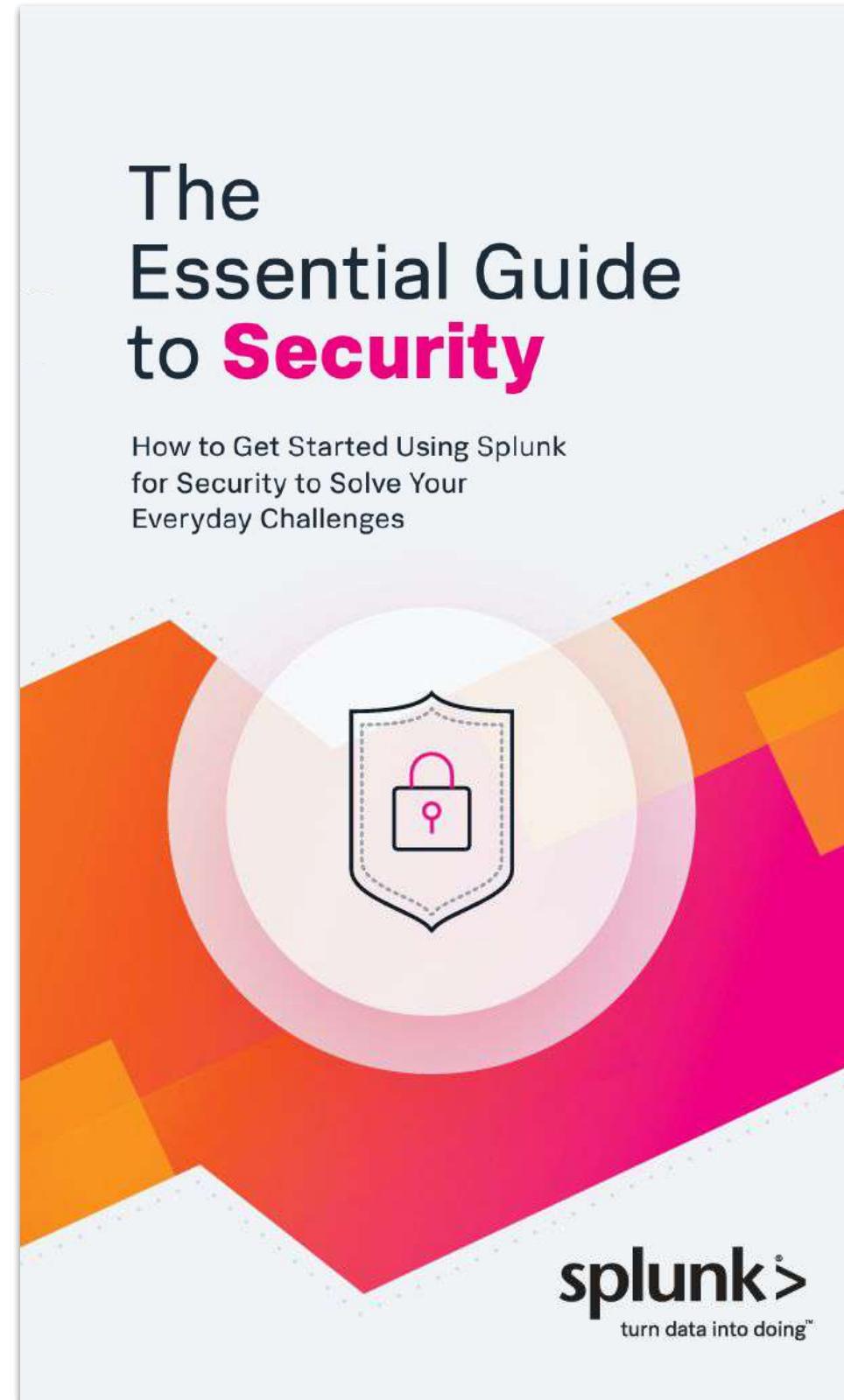
Splunk Enterprise is the mission-critical platform for indexing, searching, analyzing, alerting and visualizing machine data.

## Operationalized Data Science Pipeline



**splunk**® Platform for Operational Intelligence

# The Security Data Journey

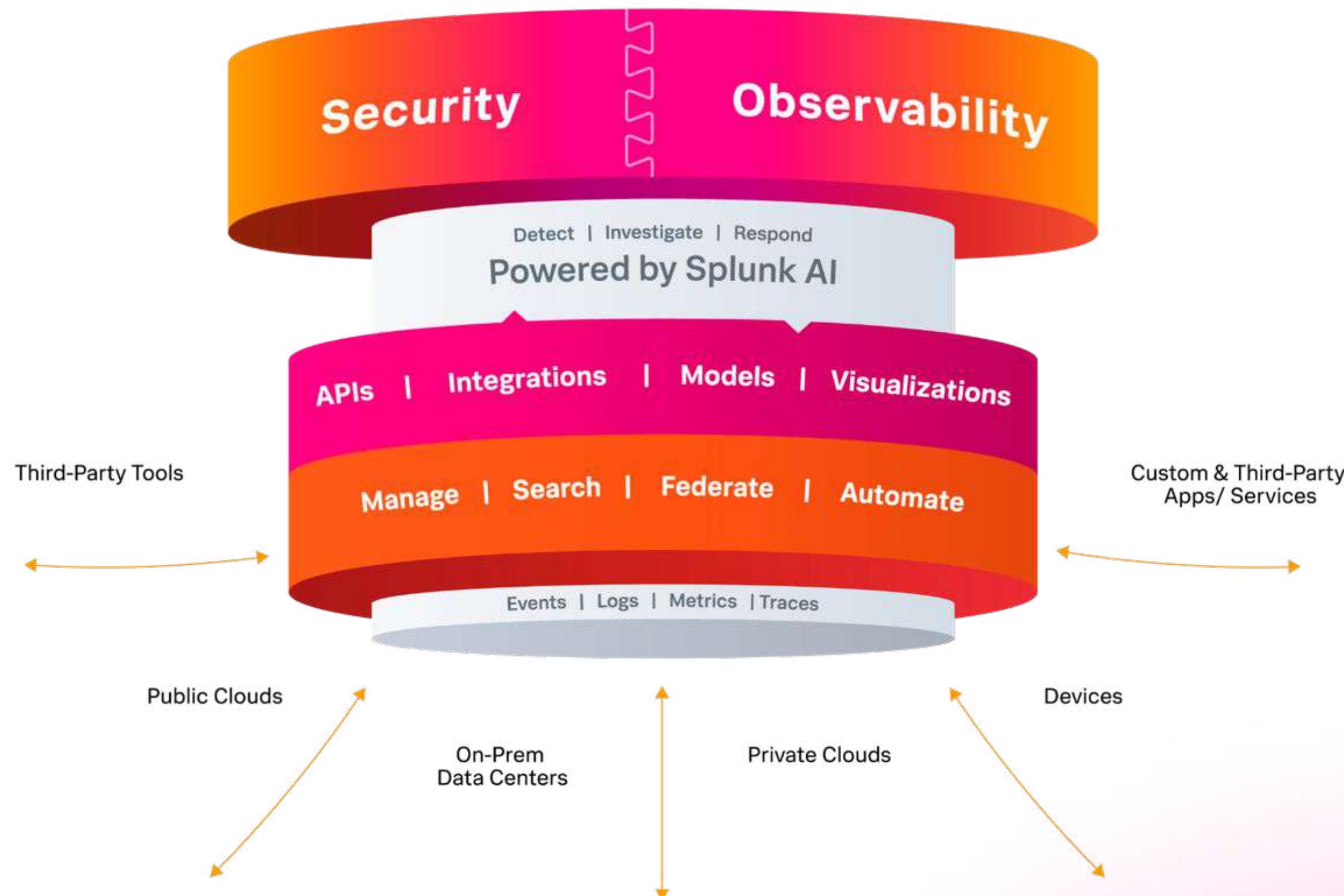


[https://www.splunk.com/en\\_us/form/the-essential-guide-to-security.html](https://www.splunk.com/en_us/form/the-essential-guide-to-security.html)

# Machine Learning for Security with Splunk



# The Unified Security and Observability Platform is Powered by Splunk AI



# We have been implementing AI for years...

Splunk has long been committed to helping customers use AI



## Splunk AI Toolkit

The Splunk AI Toolkit, formerly MLTK: Machine Learning Toolkit, explore a variety of ML concepts.

Built by [Splunk LLC](#)

Downloads

333,774



splunk> .conf19

## Announcing the Deep Learning Toolkit for Splunk

11,665

Downloads



### RESEARCH IN ACTION

Market Leader:  
Vendor Selection  
Matrix™ AIOps  
Solutions

**GIGAOM**

A Leader in the  
AIOps Radar for  
4 consecutive  
years

**VICM**

Highest Scoring  
Product in  
Selecting an  
AIOps Solution for  
2 years

# Domain-Specific Use Cases

## Security

---

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

## Observability

---

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

# Powered by Splunk AI

## Overview

### AI for Security

Enterprise Security, UBA

ML-Powered Detections, Anomaly Detection,  
Predictive Analytics

### AI for Observability

ITSI, APM, IM, On-Call

Predictive Analytics, Anomaly Detection, Adaptive  
Thresholding, Incident Correlation, Alert Noise  
Reduction, Alert Autodetect, Suggested Responders

### Assistive Intelligence Experiences

Splunk AI Assistant,  
Splunk AI Assistant in Observability/Security

### Customizable ML

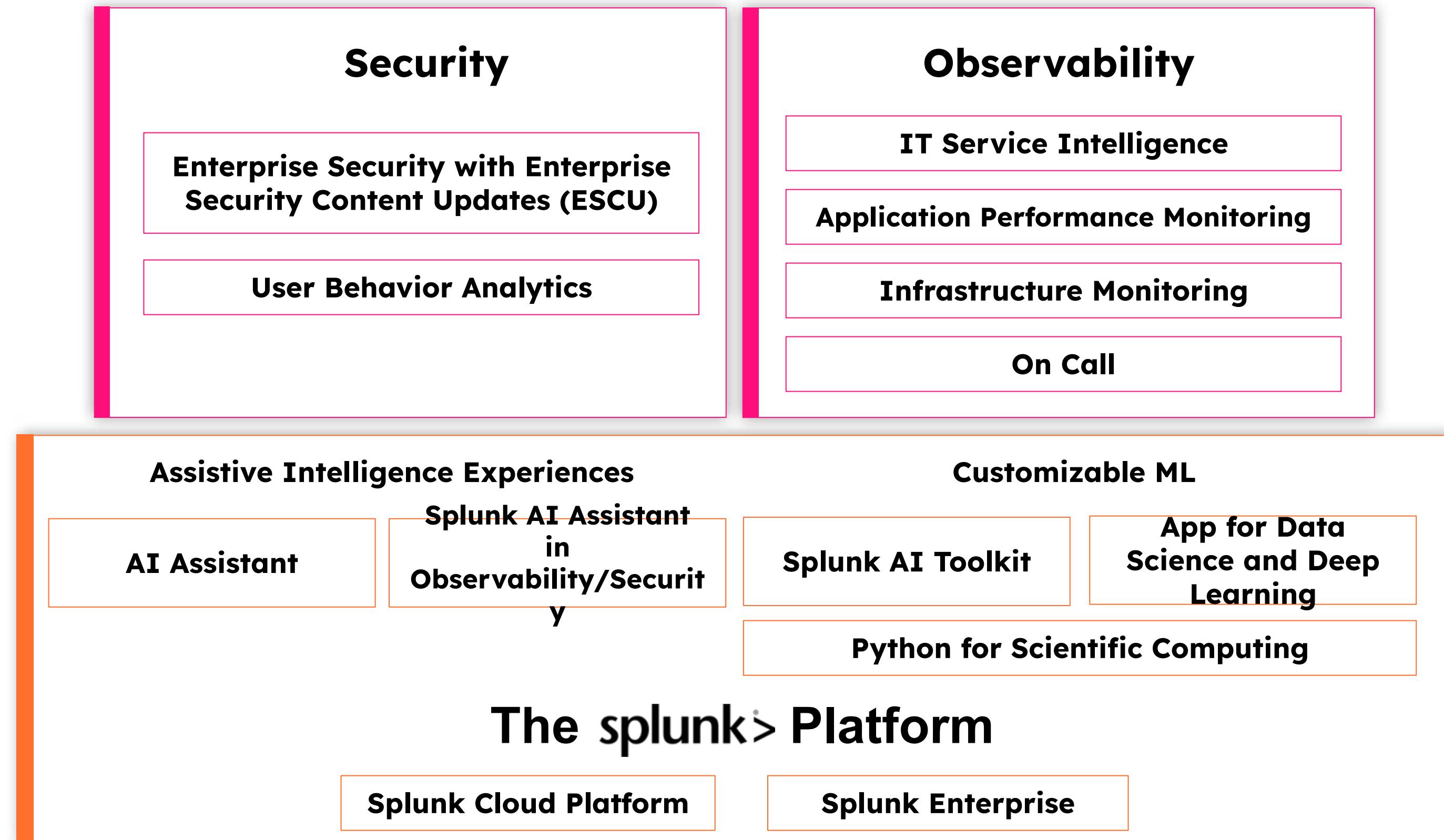
Splunk AI Toolkit, Splunk App for Data Science and  
Deep Learning, Python for Scientific Computing

## The **splunk>** Platform

Powerful search commands for statistical analysis, predictive analytics and clustering

# Powered by Splunk AI

## Product Overview

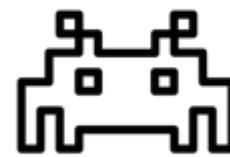


Included  
Embedded  
AI/ML  
Capabilities

Free  
Assistive and  
Customizable  
Apps & Tools

# Splunk Enterprise Security

with ML-Powered Content Updates from the Splunk Machine Learning for Security Team



## Study Threats

Identify emerging threats and understand how they operate



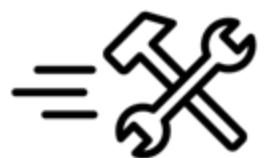
## Create Datasets

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



## Build ML & Deep Learning Powered Detections

Build advanced models 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; and craft rules or queries designed to identify specific activity associated with threats - Leverage both Machine Learning & Deep Learning.



## 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

# Customize AI for security

In Splunk Enterprise Security

OOTB ML analytics in ES and with the ES Content Updates (ESCU), which can be fully customized to your environments.

Documentation and guidance on some of the most common [security use cases that are enhanced by AI and ML](#).

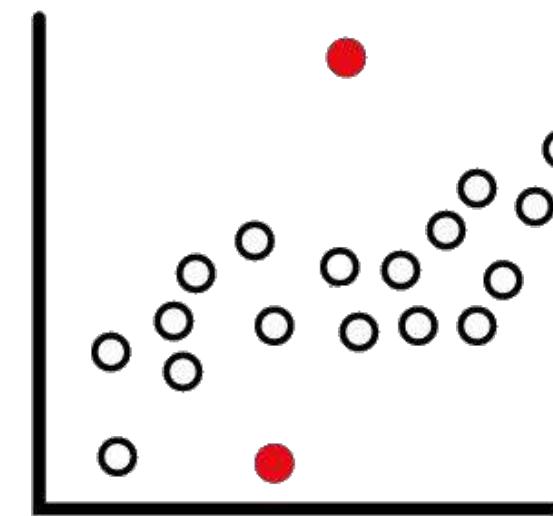
# Security Use Cases Enhanced by AI and ML

splunk>

# ML-Powered Detections for Security

Find the Obscure and Unknown Threats Buried Deep in Your Data

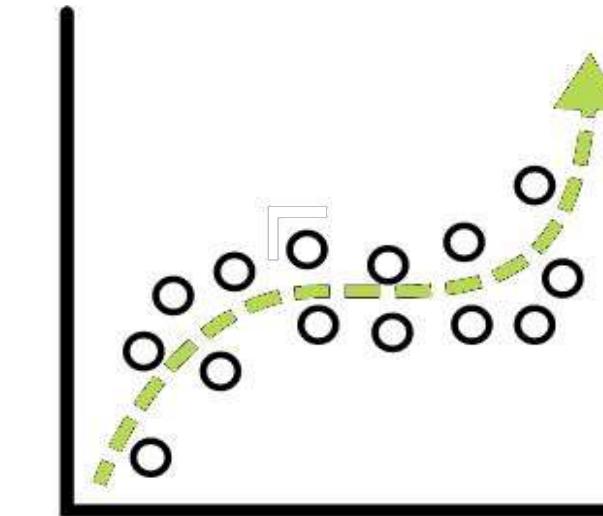
## Anomaly detection



Deviation from past behavior

**Resource Utilization**  
**Error Rate Deviation**  
**Access Pattern Baselining**

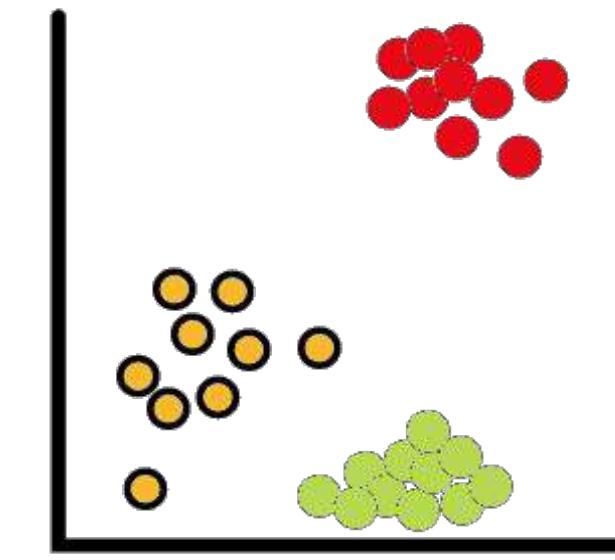
## Predictive Analytics



Future state prediction  
Classification/regression

**Predict storage requirements**  
**Identify patterns leading to failure**

## Clustering

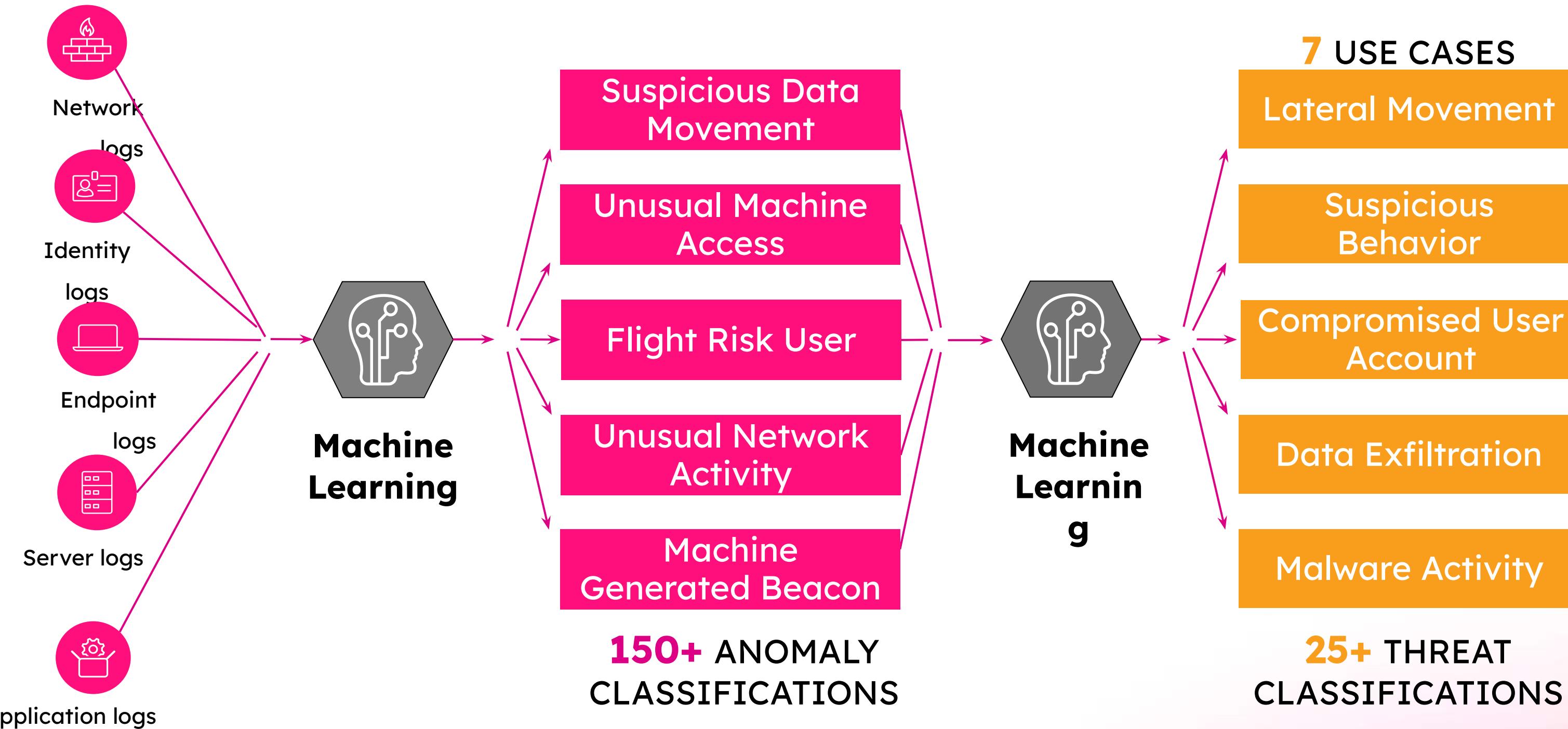


Behavioral Analytics

**Identify Traffic**  
**Classify Behaviors**

# User Behavior Analytics

Detect threats and anomalous behavior using machine learning

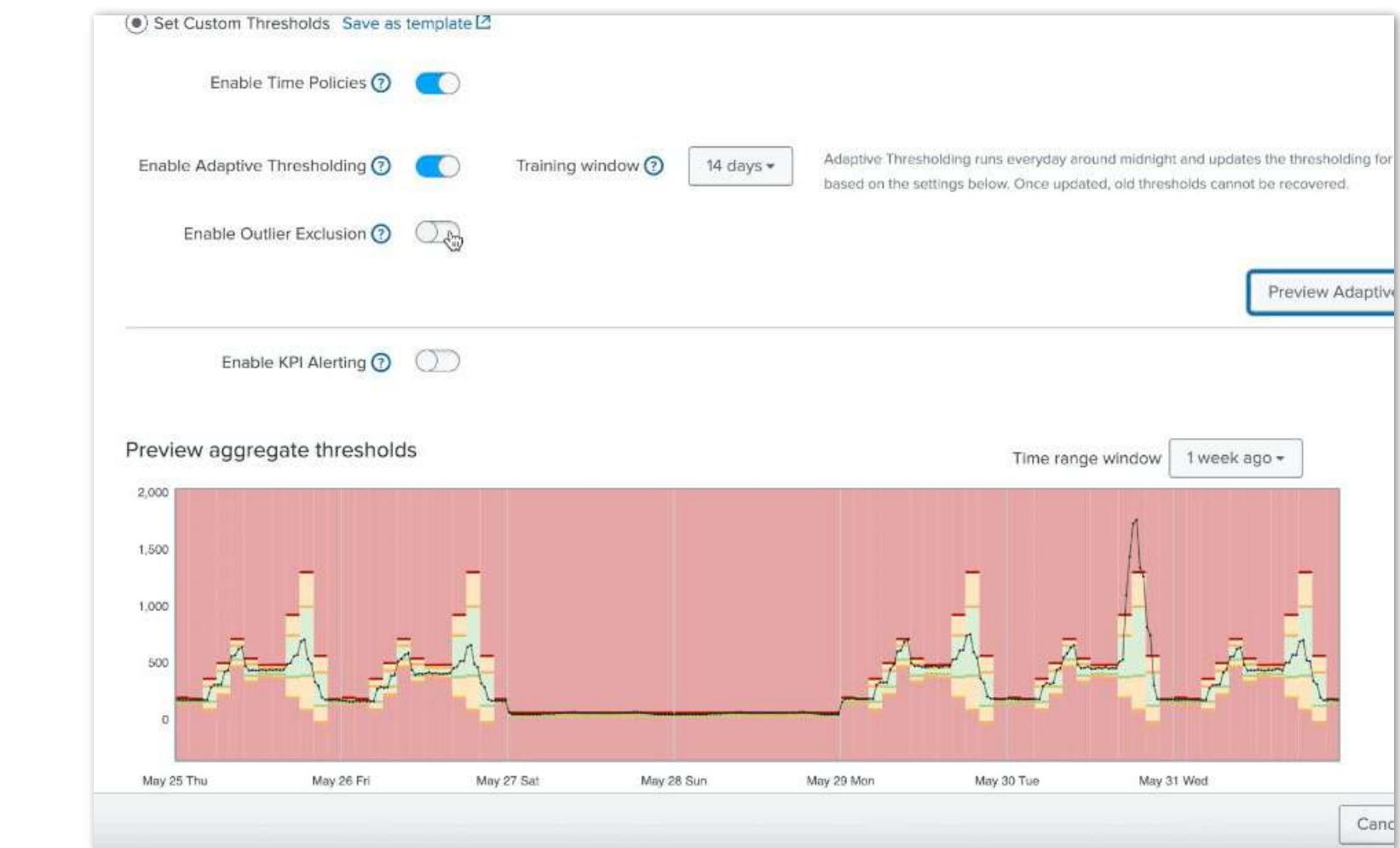


# Splunk IT Service Intelligence (ITSI)

## Splunk's AIOps Solution

Splunk ITSI applies machine learning to **proactively prevent outages** by correlating and reducing alerts, monitoring service health, and streamlining incident management.

- ❑ Clustering & aggregation to reduce alert noise
- ❑ Adaptive (dynamic) thresholds incorporate seasonality
- ❑ Anomaly and outlier detection
- ❑ Actionable additional context
- ❑ Assisted root cause investigation
- ❑ Predict service health to prevent outages

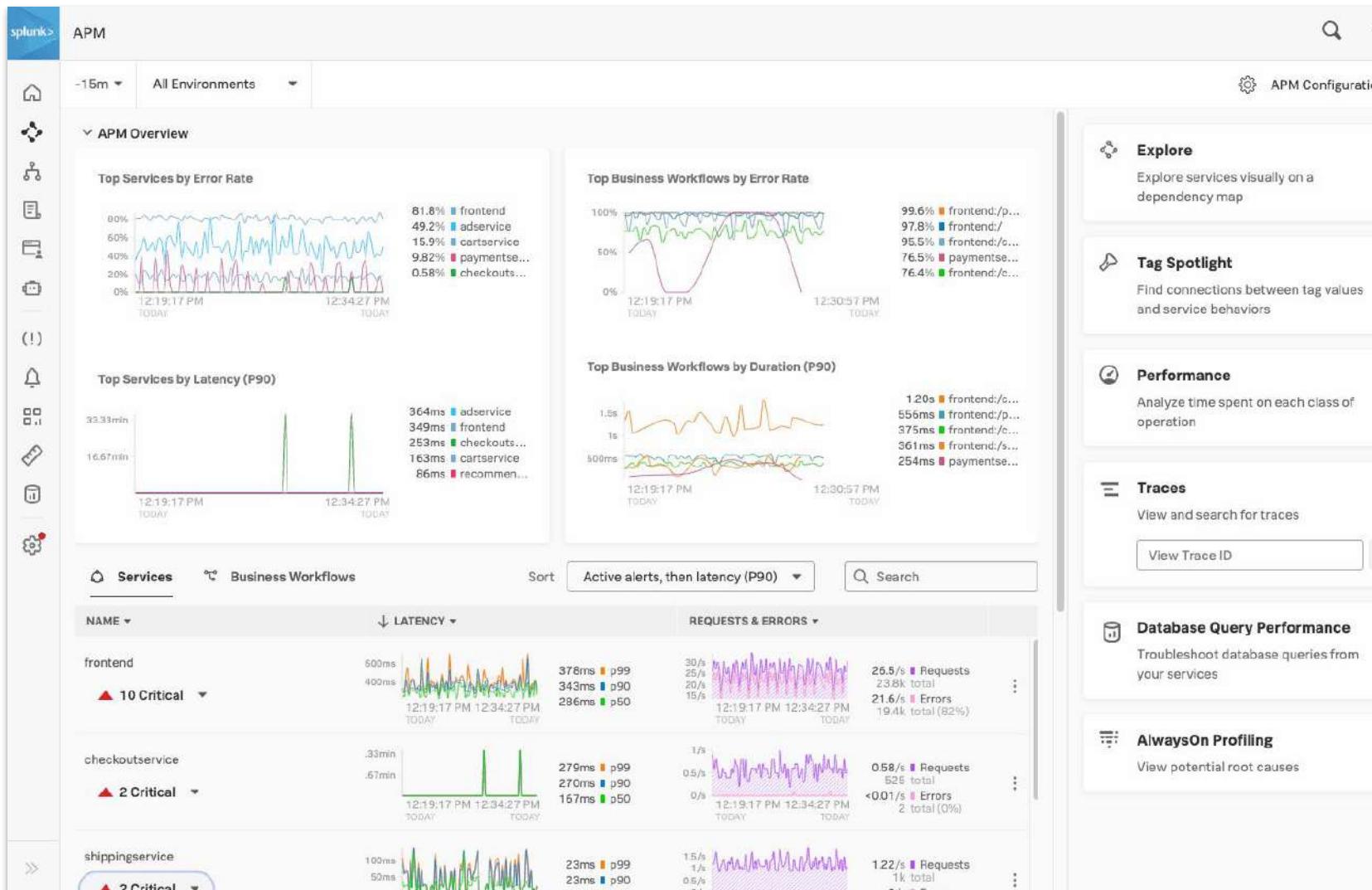


## New updates! conf23 ★

- ❑ Outlier Exclusion in Adaptive Thresholds
- ❑ ML-Assisted Thresholding (Preview)

# Splunk Application and Infrastructure Monitoring: Autodetect

More accurate and efficient alerting for your infrastructure and services



Use machine learning to **improve accuracy** and **reduce manual effort** across infrastructure and service alerting

- Establish performance baselines across every service
- Automate alerting by receiving recommendations for the biggest spikes in latency, errors, and resource utilization
- Easily customize alert thresholds and subscribe to notifications for specific services or teams

# Splunk On-Call

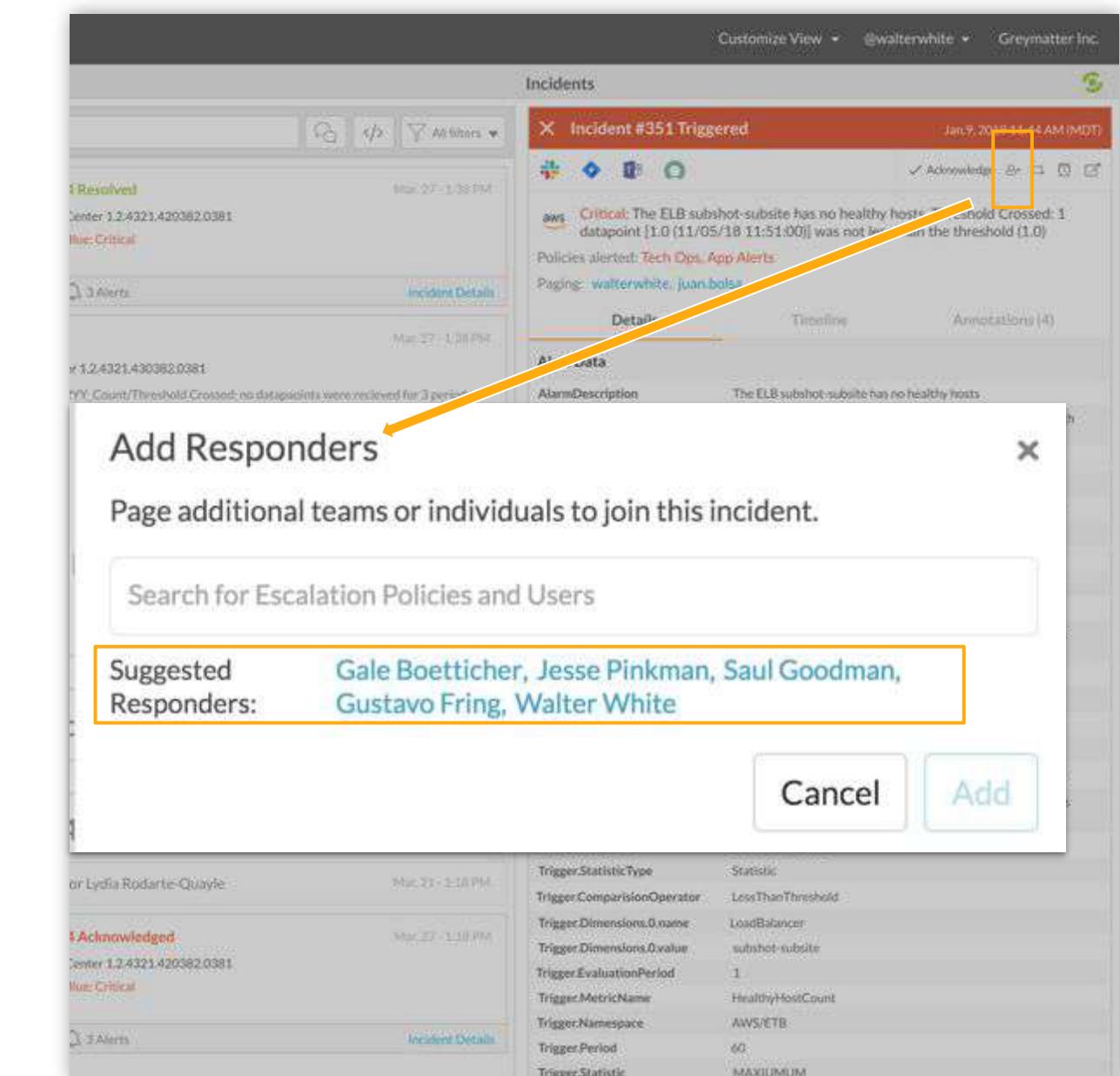
## Incident Correlation

Splunk On-Call **leverages ML** to correlate like incidents and decipher which person or people have worked on similar incidents in the past.

The **Suggested Responders** are listed when a user clicks **Add Responder**—making it possible to loop in knowledgeable colleague/s to the firefight in moments.

### Benefits:

- ❑ Reduce isolation
- ❑ Leverage tribal knowledge to reduce MTTR
- ❑ Improve morale/ reduce burn out



# Splunk AI Toolkit

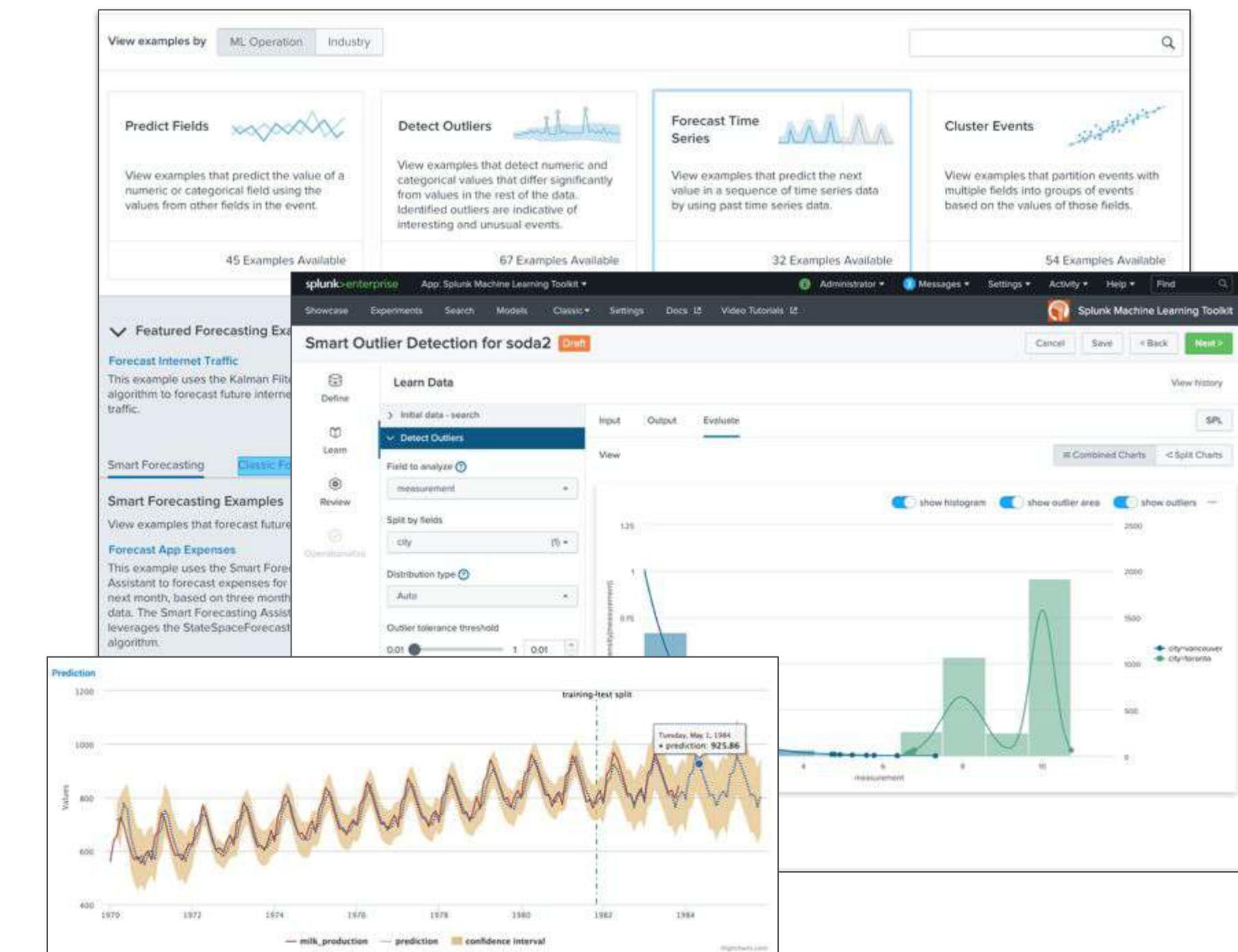
Extends Splunk to operationalize Machine Learning – freely available on splunkbase

## Built for the Citizen Data Scientist

- Experiments and Assistants:** Guided model building, testing, and deployment for common objectives
- Algorithms:** 80+ standard algorithms (supervised & unsupervised)

## Extensible to operationalize any use case

- Python for Scientific Computing Library:** Access to 300+ open source algorithms
- Deep Learning Toolkit:** Supports NN and GPU accelerated machine learning
- ML-SPL API:** Import any open-source or proprietary algorithm



# Splunk AI Toolkit

## LLM Integrations

---

- New feature to allow customers to connect to external LLM models, from providers including OpenAI, Gemini, AWS Bedrock, Anthropic, Grok, Microsoft hosted OpenAI and Ollama
- New search command that allows users to pass data through an external LLM and present the results in the search pipeline

## Enhanced ONNX apply

---

- ONNX apply now supports multi-variate outputs
- Additional configuration options are now available for ONNX apply, such as choice of activation function
- Documentation available to programmatically upload ONNX models to MLTK, without having to upload them manually via the UI

## Fixed Vulnerabilities

---

- Upgrading OpenSSL to v3.4 to mitigate a [critical vulnerability](#) in PSC 4.2.3 and 3.2.3

# LLM Integrations: What is it?

- Customers can connect to externally hosted LLMs
- Through a natural, human language search command, Splunk data is sent to external LLMs, presenting the response back in Splunk
- Current support for OpenAI, Anthropic, Azure OpenAI, AWS Bedrock, Gemini, Groq and Ollama
- The ERD for the feature is [here](#) for more details

The screenshot displays two main Splunk interfaces. The top window is titled 'Connection Management Settings' under 'Connection Management'. It shows a list of providers: OpenAI (selected), Anthropic, AzureOpenAI, Groq, Gemini, Bedrock, and Ollama. Below this is a table for 'Settings for Provider OpenAI' with columns for 'Provider Name', 'Setting', 'Value', and 'Action'. The 'Endpoint' setting is set to 'https://api.openai.com/v1/chat/completions'. The bottom window is titled 'New Search' and shows a search query: 'index=alerts severity=1 | table \_time severity alert\_message | eval prompt="Please explain this message from a Cisco ASA Firewall to me and why I might receive it: (alert\_message)"'. The search results table has columns for 'severity', '\_time', and 'alert\_message'. One result row is expanded, showing the raw log: 'ASA-2-1000001: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from XXXX.1.2.3.4/555 to YYYY.3.6.7.8/555. [data:really\_dubious\_email@unuspicious.com]'. To the right of the table, a detailed explanation of the log message is provided:

The message you're receiving from your Cisco ASA Firewall is an alert indicating that a connection using ESMTP (Extended Simple Mail Transfer Protocol) or SMTP (Simple Mail Transfer Protocol) has been terminated because the Firewall detected a potentially malicious pattern in the mail address of an email being processed.

Let's break down the message:

- ASA-2-1000001: This is the specific identifier for the log message. It indicates the severity level ('2' in this case) and the type of event ('1000001' refers to the specific event related to ESMTP/SMTP connections).
- **terminating ESMTP/SMTP connection**: This part indicates that the Firewall has closed or terminated the connection on which the ESMTP/SMTP communication was occurring.
- **malicious pattern detected in the mail address**: This indicates that the Firewall's security mechanisms (such as intrusion prevention, threat detection, or anti-spam capabilities) identified a suspicious or potentially harmful pattern in the mail address being used.
- **from XXXX.1.2.3.4/555 to YYYY.3.6.7.8/555**: This specifies the source and destination of the connection.
  - '1.2.3.4' is the IP address of the sending server, and '3.6.7.8' is the IP address of the receiving server.
  - The '555' indicates that the connection was on port 555, which is commonly used for custom or non-standard services.
- **[data: really\_dubious\_email@unuspicious.com]**: This shows the specific email address that triggered the alert. In this case, the email address looks dubious and possibly linked to malicious intent or spam. The domain 'unuspicious.com' suggests that it might be a

# Splunk Data Science and Deep Learning 5.2

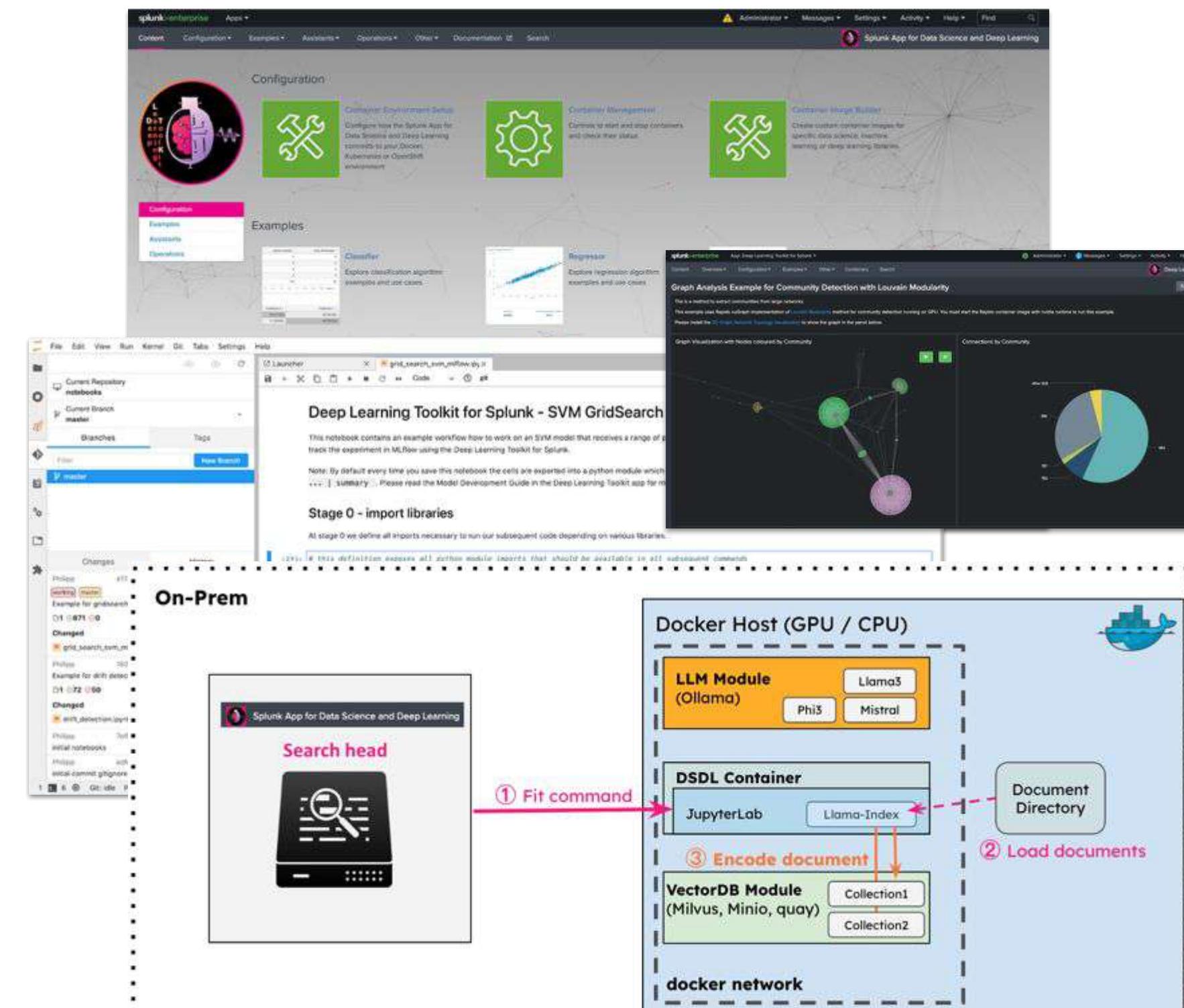
Extension for Splunk AI Toolkit to operationalize advanced custom AI / ML use cases

## Built for Data Scientists / AI Engineers

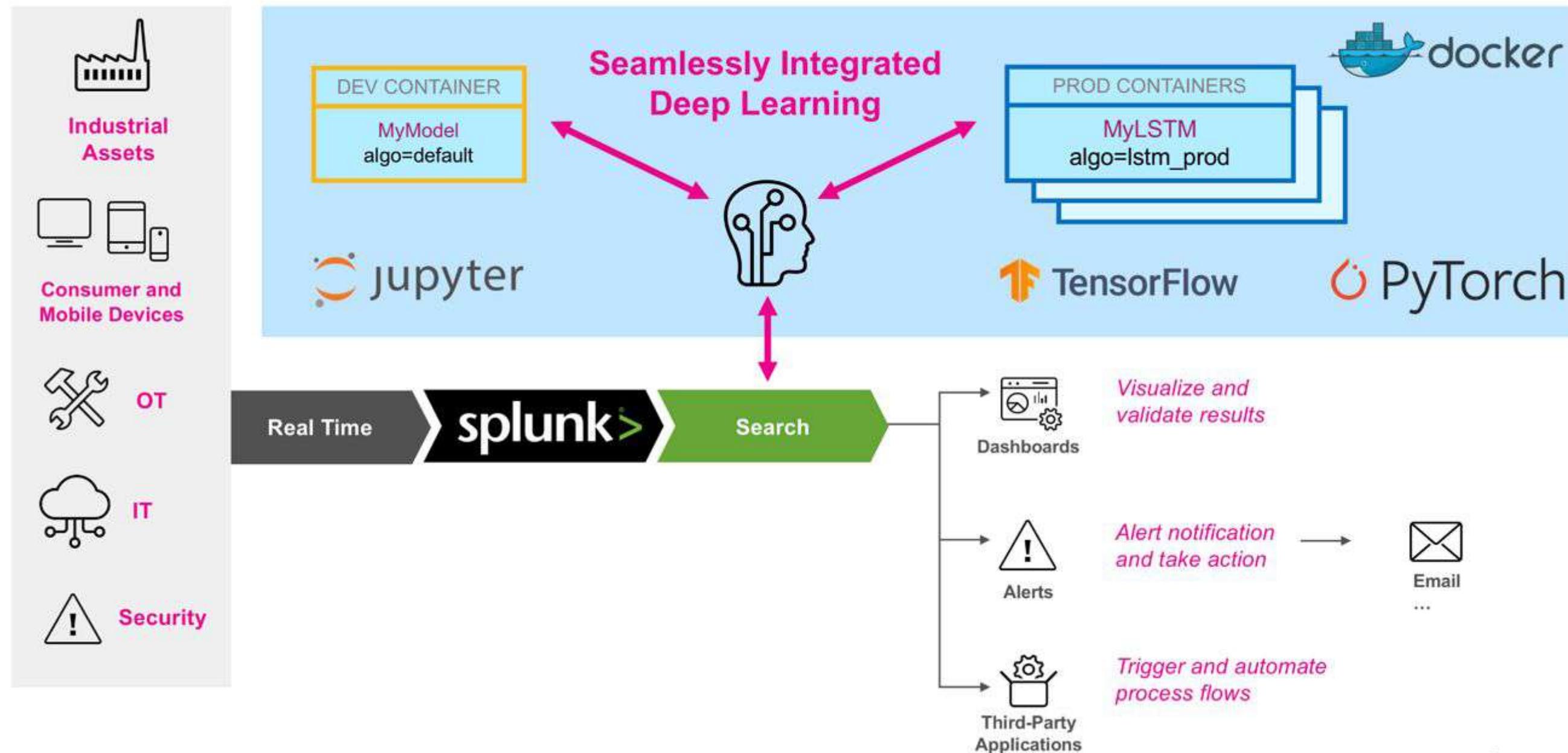
- 35+ Code Examples:** Guided model building, testing, and deployment of data science and deep learning frameworks
- Container Management:** Models can be productionized for scalability & optimization of resources, e.g. CPU & GPU
- State of the art AI frameworks and tools:** Jupyter Lab, MLflow, PyTorch, TensorFlow, SpaCy, DASK, Rapids, Spark, ...
- Flexible deployments and open source:** deploy on-prem, hybrid or in the cloud. Github repository for customization.

## New updates in version 5.2

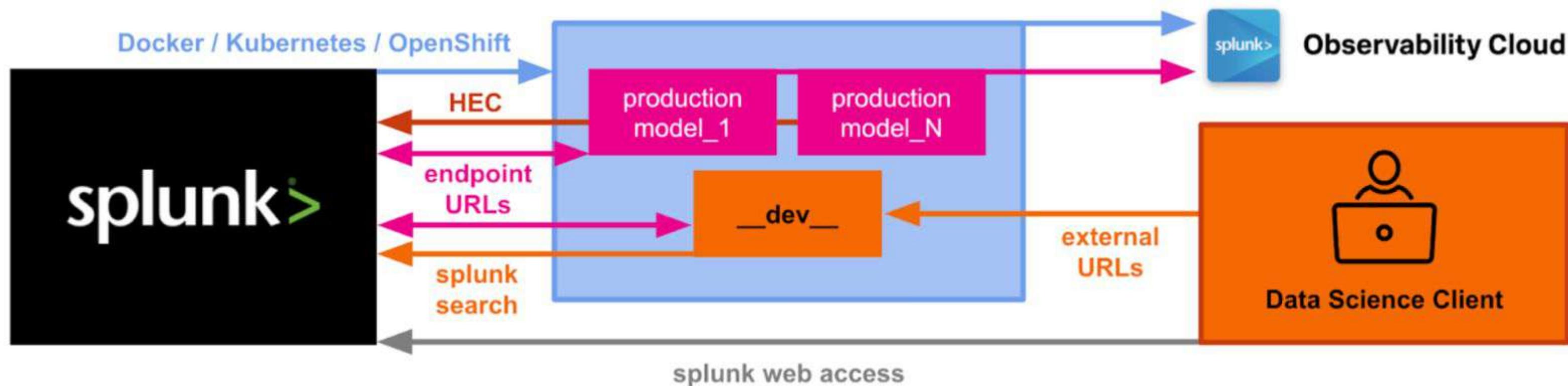
- Container extensions for LLM and VectorDB services to enable highly customizable AI use cases.**
- Custom LLM RAG based applications built on Splunk indexed data and non-Splunk, external data sources**
- 8 new dashboards to easily access the new features with all codebase shared in the public github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



# Splunk DSDL - Architecture

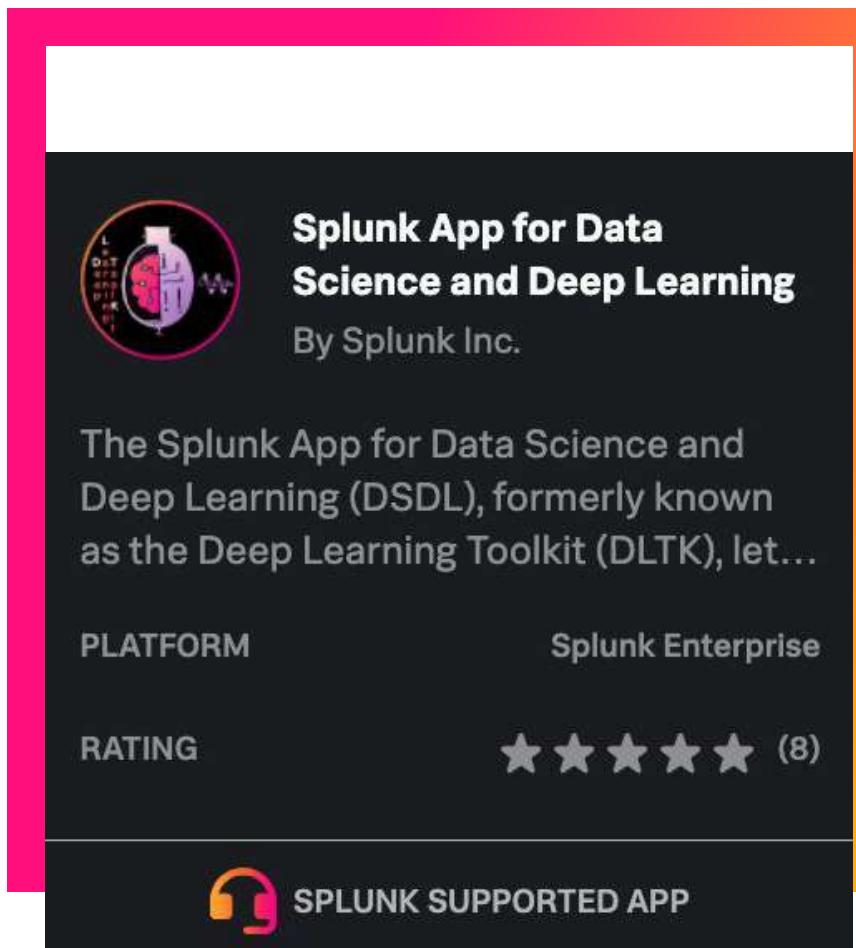


# Splunk DSDL - Flow



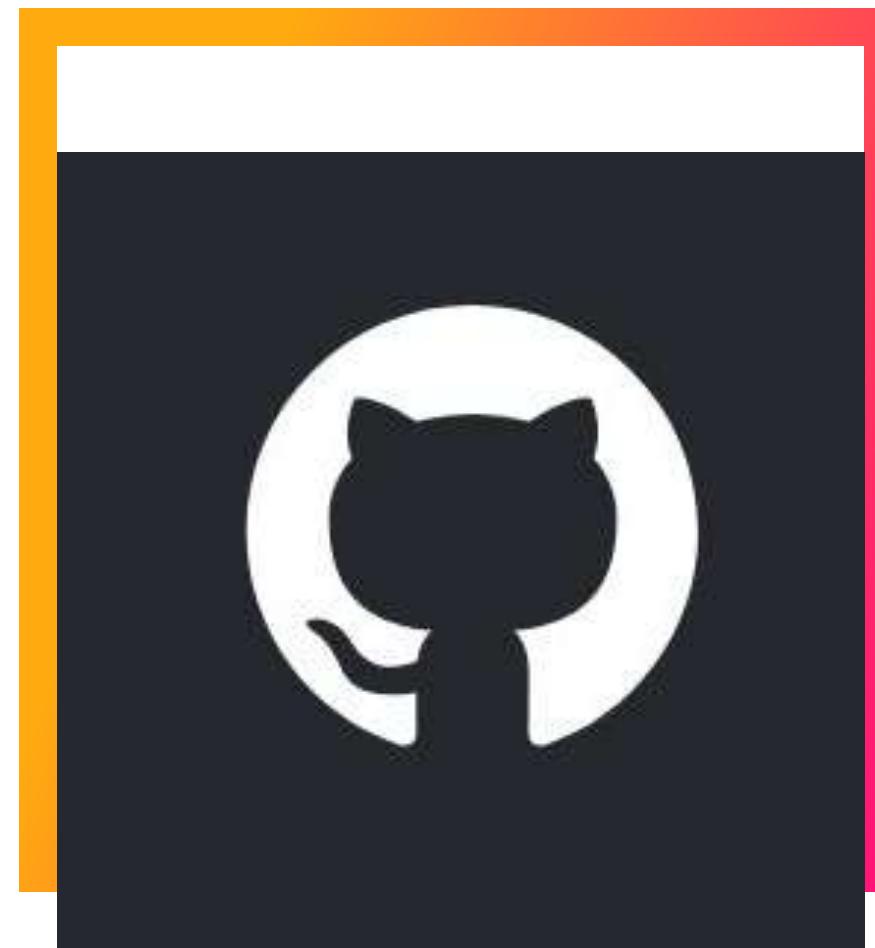
# DSDL 5.2 Resources

**DEMO Video:** [Link to video](#)



## DSDL App Package

Simply install the DSDL 5.2 on your Splunk search head and get started.



## Github Repository

Fork the current v5.2 branch from DSDL's public github and extend to your needs.

The image is a screenshot of a documentation page titled "Use the Splunk App for Data Science and Deep Learning". It includes sections for "About LLM-RAG" and "LLM-RAG features". The "About LLM-RAG" section discusses challenges like securing LLMs and generating accurate answers. The "LLM-RAG features" section explains how it uses knowledge bases to enhance responses. A note at the bottom states that only Docker deployments are supported.

## Documentation

Learn how to setup DSDL 5.2 with the help of this guide.

# Python for Scientific Computing

Extend the Splunk Platform Python runtime with AI specific libraries

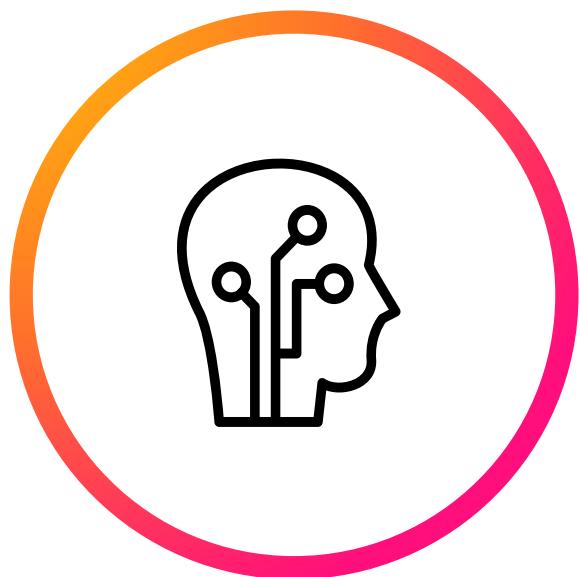


**Run complex AI/ML based analytics** in the Splunk Platform with a broad range of supported Open Source Python libraries

# Where Are We Going with AI?

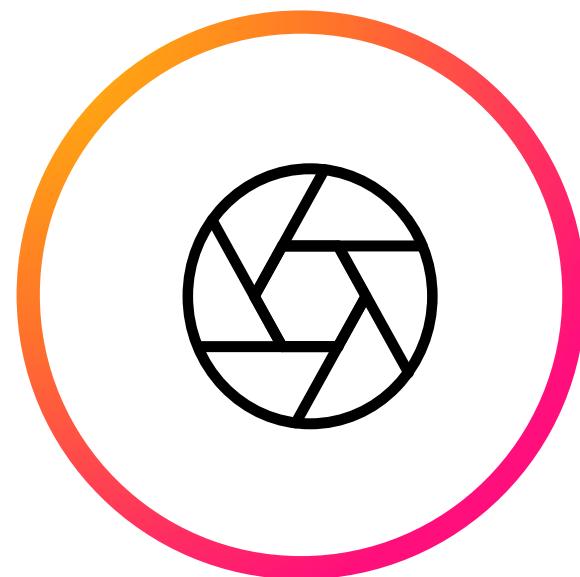
Unified experience across Splunk with a scalable backend to power them

We are moving from toolkit capabilities to end-to-end ML guidance for data in Splunk



## More Splunk-specific, trusted Generative AI

Improve our generative AI in Splunk AI Assistant and expand into other use cases and products



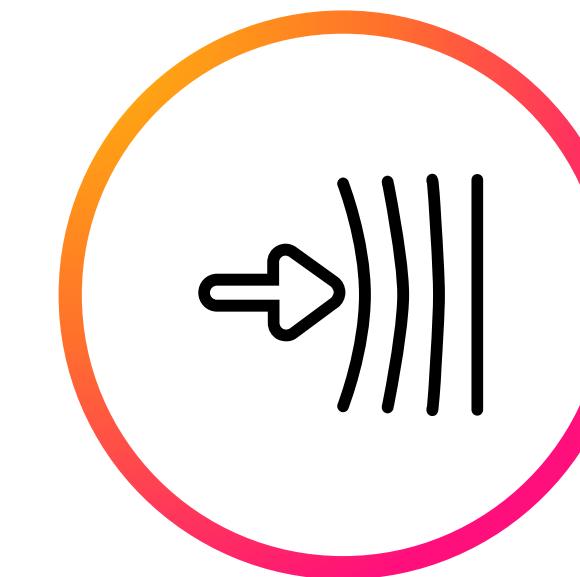
## Additional embedded AI

Integrate more AI into users' everyday workflows in Splunk products and build more assistive experiences



## Run ML at Scale

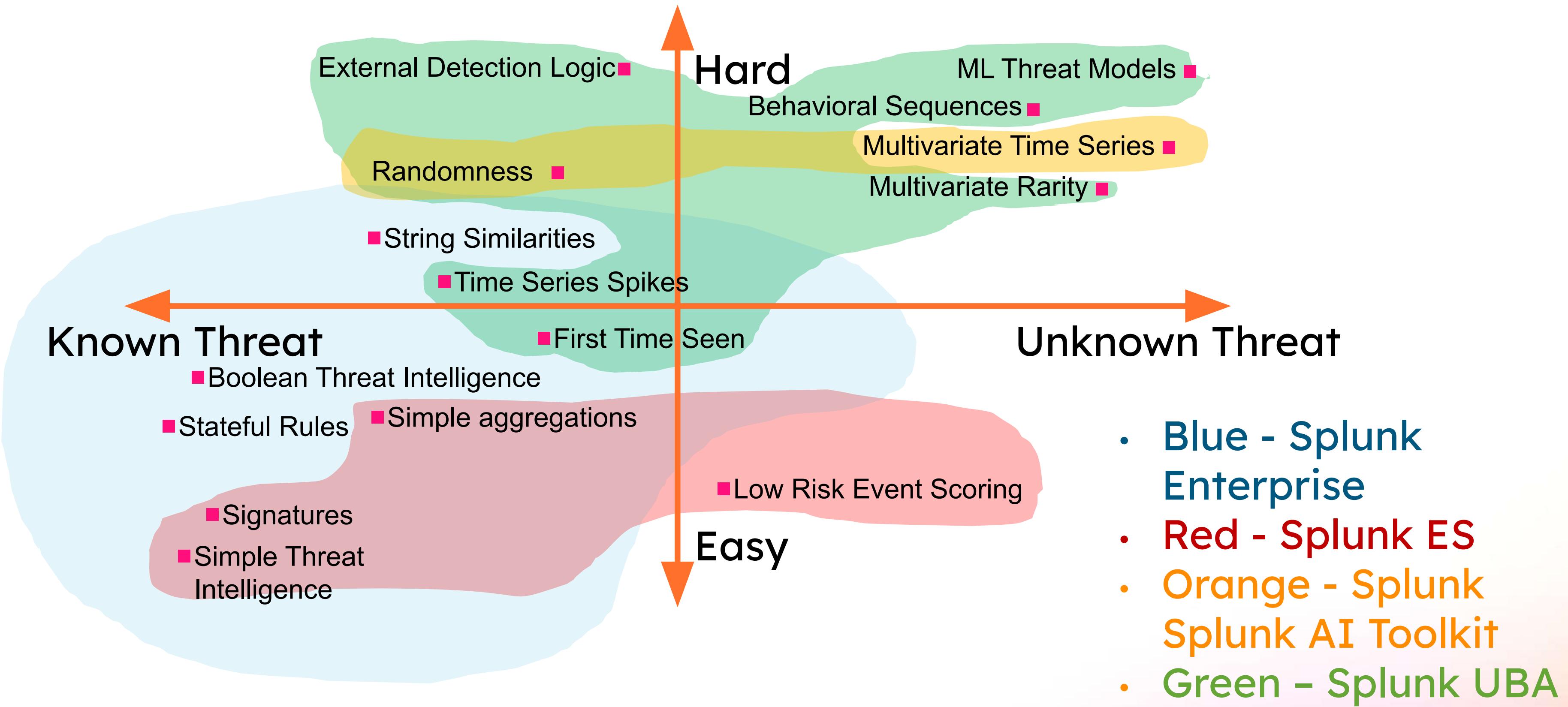
Develop a robust runtime to power large-scale ML model training and deployment



## Extensible ML for Splunk developers

Build an SDK to empower developers to create ML powered experiences

# Detective Controls by Difficulty



- Blue - Splunk Enterprise
- Red - Splunk ES
- Orange - Splunk Splunk AI Toolkit
- Green - Splunk UBA

# Splunk AI Assistants

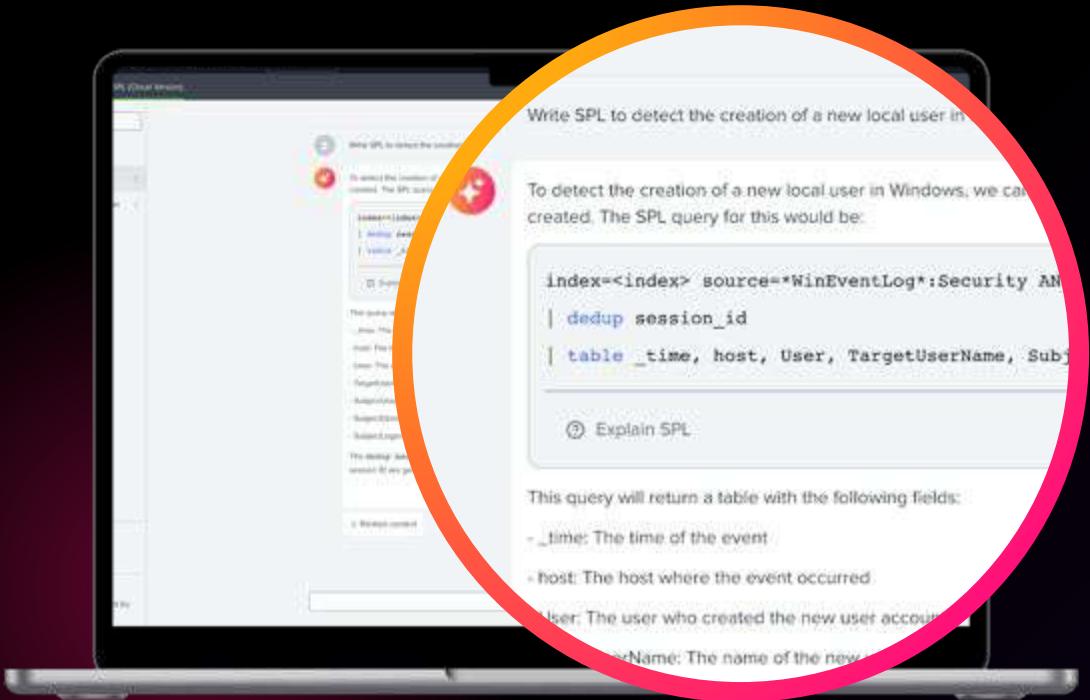
**splunk>**  
a CISCO company



# Splunk AI Assistants everywhere

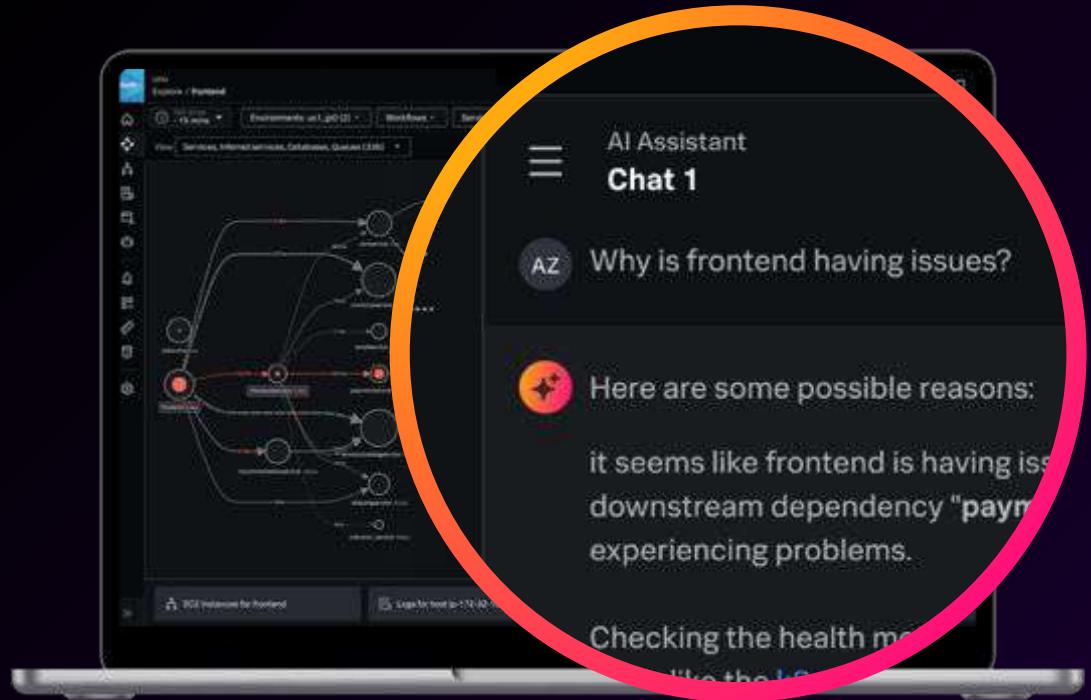
Increase productivity and deliver faster detection and response

## AI Assistant for SPL



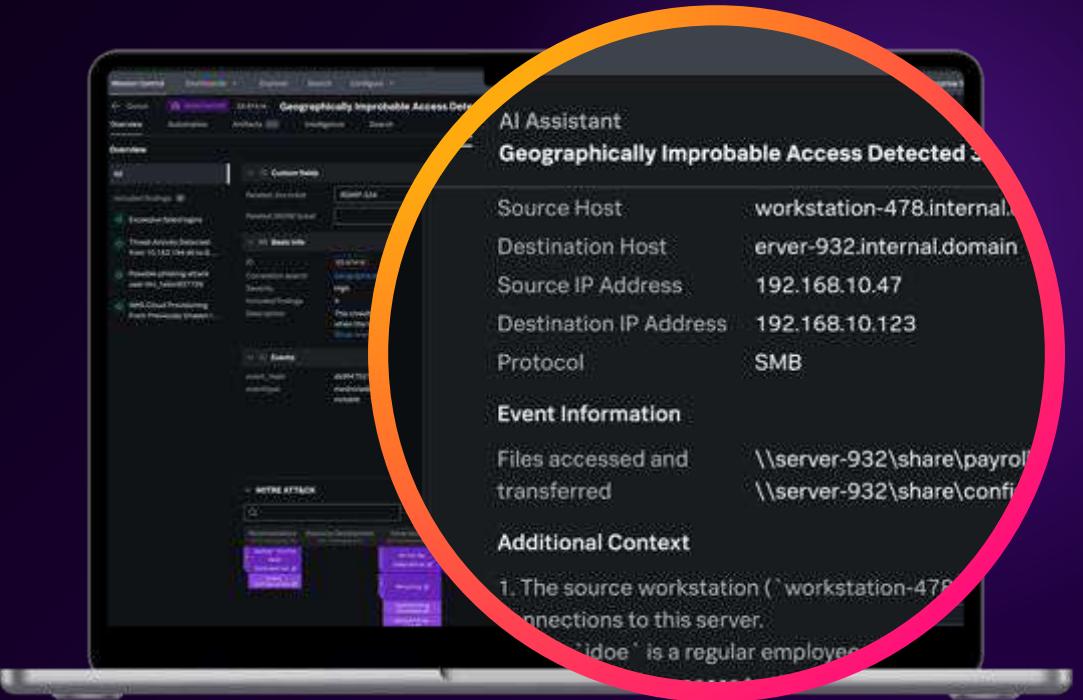
Generally Available

## AI Assistant in Observability Cloud



Generally Available

## AI Assistant in Enterprise Security



Preview

# AI Assistant for SPL

*Available in Splunk Cloud*

- ▶ Get your job done faster using natural language
- ▶ Chat with your data to drill down to deeper insights
- ▶ Accelerate your learning journey to become the expert

The screenshot shows the Splunk AI Assistant interface. On the left, there's a sidebar with links: Chat (highlighted with a pink circle), Usage guidelines, and Settings. The main area has a query card with a pink icon. The query text is:

```
| tstats count from datamodel=Authentication.Authentication where Authentication.action="failure" earliest=-7d@d latest=now() by Authentication.user | top limit=10 Authentication.user
```

Below the query, a callout bubble highlights the `from datamodel=Authentication.Authentication` part of the query. The text inside the bubble says:

The `tstats` command is used to retrieve statistical information about indexed data, in this case, counting the number of events.

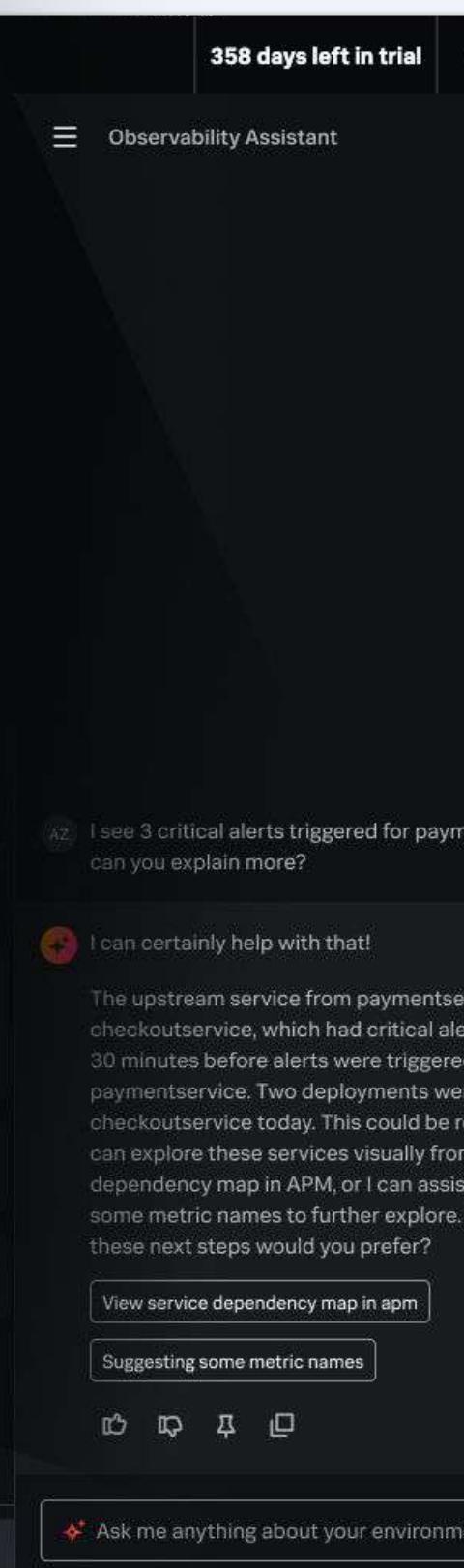
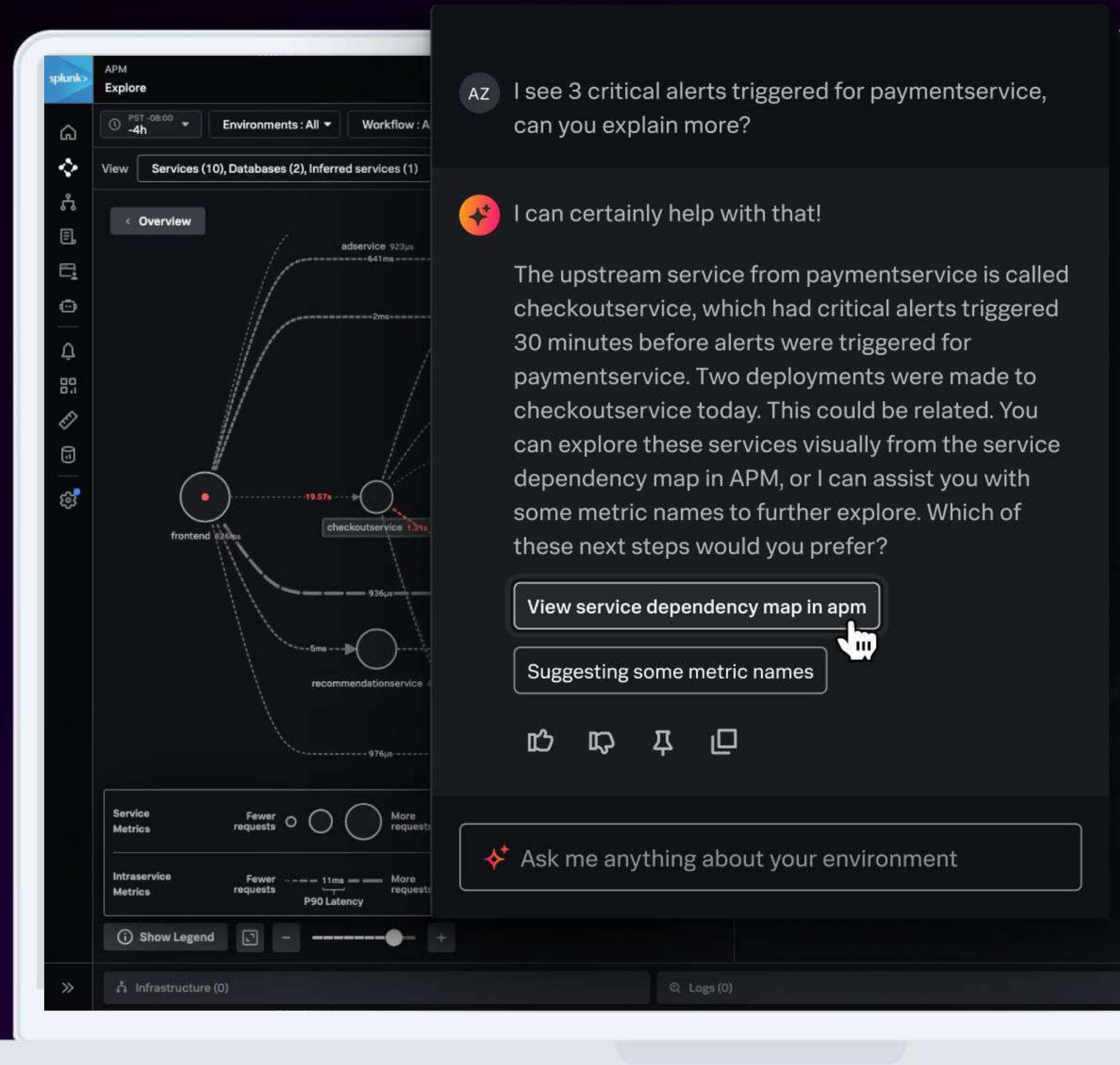
The query retrieves the top 10 users with the highest number of failed authentication attempts in the past 7 days.

At the bottom, there's a feedback section with a text input field and a green button.

# AI Assistant in Observability Cloud

*Find and fix issues faster using  
natural language*

- ▶ Surface key insights by chatting with your data
- ▶ Powered by agentic AI to accelerate investigations and daily monitoring tasks
- ▶ Get context and guided recommendations as you troubleshoot



# AI Assistant in Enterprise Security

*Guided Enterprise Security workflows*

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

The screenshot displays the AI Assistant interface within a Splunk-like security platform. At the top, a banner indicates a '24 hour risk threshold exceeded for system=win-srv1.acme.local'. The main area is divided into sections: 'Overview' (with a 'MITRE ATT&CK map' showing detections across various techniques like Initial Access, Execution, Persistence, etc.), 'Intermediate findings' (a timeline from May 30 to June 1 showing specific events such as suspicious registry keys, cmd.exe spawning, PowerShell execution, and Windows Firewall status), and 'Intermediate findings details' (a list of findings with filters for Time and Risk Message). To the right, a sidebar shows a conversation with 'John Smith' and the AI Assistant. The AI response is highlighted with a red box and lists two main points: 1. SPL Generation based on the user's Splunk environment, which involves creating SPL queries; and 2. Summarizing security findings, which involves reviewing process activity and compromised user accounts. The sidebar also includes a section for 'Security Content' and a footer note about reporting features.

AI Assistant in Enterprise Security is currently in preview. UI shown is for illustration; not final product.

# Hands-on labs

# Lab 1

Detect Password Spraying Attack-  
Credential Access



# Detect Password Spraying Attack

*Credential Access*

## Lab 1



# Detect Password Spraying Attack-Credential Access

## What is Password Spraying?

Technique [T1110.003](#) in the MITRE ATT&CK Framework, Password spraying differs from a [typical brute-force attack](#), where attackers try many passwords against a specific user account. However, we can consider spraying a type of brute force attack – it involves a trial-and-error approach of “spraying” a single password across many accounts until a match is found.

This approach enables attackers to avoid countermeasures like account locking when specific login attempts with different passwords have been exceeded. Thus, it is difficult to detect password-spraying attacks without proper detection methods. These password-spraying attacks often target federated authentication used in single sign-on (SSO) and cloud-based applications. Once the attacker gains initial access, they can later access the critical data of organizations.

# Using Simple stats

Method 1



# Detect Password Spraying Attack

*Credential Access*

## Lab 1



# First Technique#1: Simple stats

## Detect (Remote) Password Spraying Attacks

How to detect this type of attack?

**Tips:** Windows Event Logs – Which Event code indicates a failed attempt to login to a device? What event indicates a remote authentication attempt? (Optional) You can also filter per Process Name, Computer...

As for the first lab, use transforming commands to visualize your results ([eval](#), [stats](#), [timechart](#), [evenstats](#)). Leverage Standard Deviation.

Your turn!

# First Technique#1: Simple stats

## Detect Remote Password Spraying Attacks

```
index="main" sourcetype="XmlWinEventLog_ws" EventCode=4625 LogonType=3  
| bucket span=2m _time  
| stats dc(TargetUserName) as unique_accounts values(TargetUserName) as  
tried_accounts by _time,IpAddress, LogonType, dvc  
| eventstats avg(unique_accounts) as comp_avg, stdev(unique_accounts) as comp_std  
by ipAddress, LogonType, dvc  
| eval upperBound=(comp_avg+comp_std*2)  
| eval isOutlier;if(unique_accounts > 6 AND unique_accounts >= upperBound, 1, 0)  
| search isOutlier=1
```

Finding and Removing Outliers: <https://splk.it/3s0Pig5>

# First Technique#1: Simple stats

## Detect Remote Password Spraying attacks

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following SPL query:

```
index="main" sourcetype="XmlWinEventLog_ws" EventCode=4625 LogonType=3  
| bucket _span=2m _time  
| stats dc(TargetUserName) AS unique_accounts values(TargetUserName) as tried_accounts by _time, IPAddress, LogonType, dvc  
| eventstats avg(unique_accounts) as comp_avg , stdev(unique_accounts) as comp_std by IPAddress, LogonType, dvc  
| eval upperBound=(comp_avg+comp_std*2)  
| eval isOutlier=if(unique_accounts > 6 and unique_accounts >= upperBound, 1, 0)  
| search isOutlier=1
```

The search results table has the following columns:

_time	IPAddress	dvc	unique_accounts	tried_accounts	comp_avg	comp_std	isOutlier	upperBound
2023-10-28 11:24:00	172.16.48.255	3 computer9	7	user23 user35 user42 user44 user54 user55 user93	3.490566037735849	1.4090728199427118	1	6.308711677621273
2023-10-28 21:48:00	172.16.48.255	3 computer9	7	user11 user36 user58 user63 user86 user88 user89	3.490566037735849	1.4090728199427118	1	6.308711677621273
2023-10-29 01:20:00	172.16.48.255	3 computer4	7	user33 user46 user47 user51 user64 user7 user77	3.7142857142857144	1.266647387553302	1	6.247580489392318

Finding and Removing Outliers: <https://splk.it/3s0Pig5>

# Splunk AI Toolkit demo

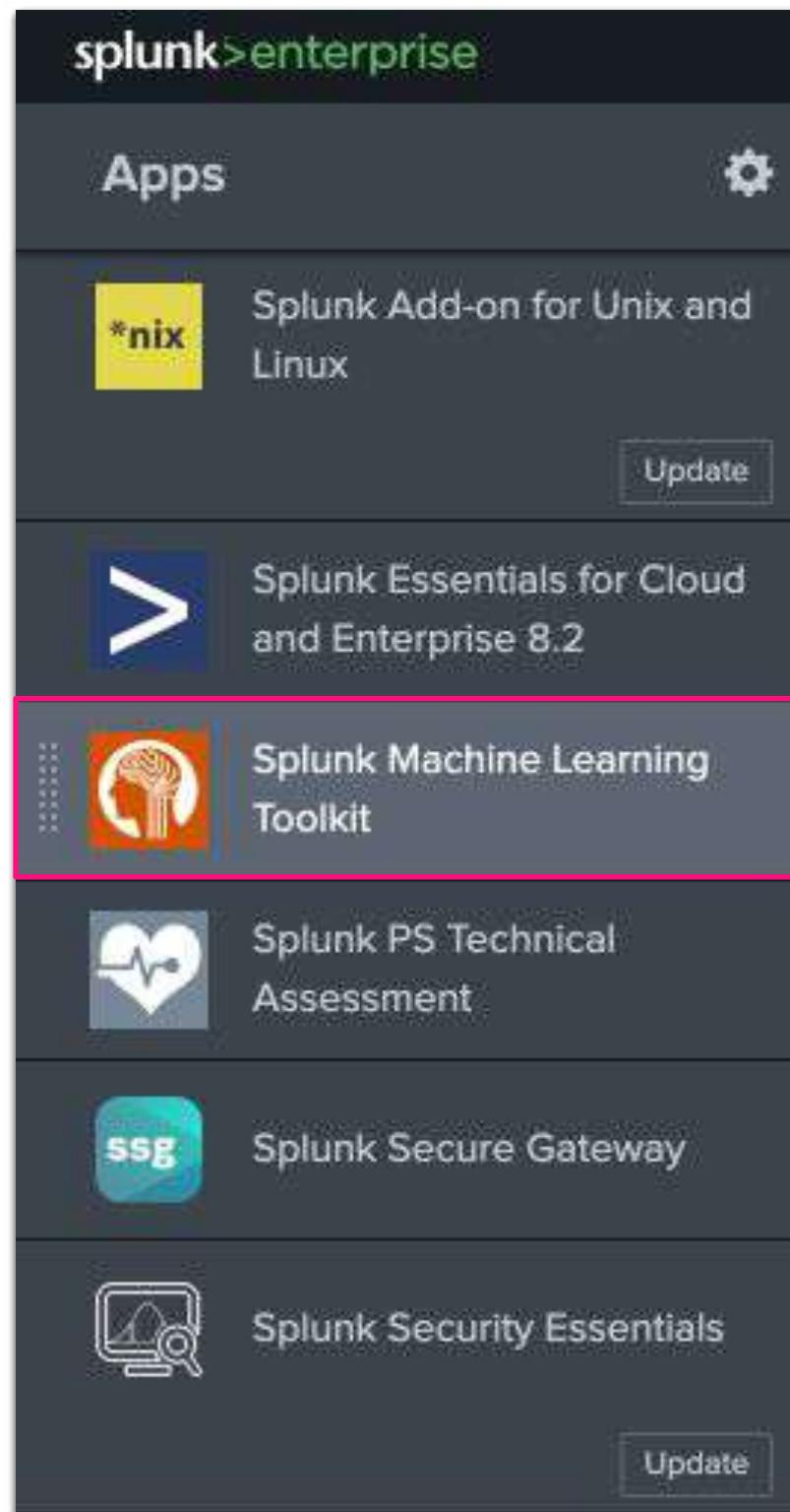
# Using Splunk AI Toolkit

Method 2



# Splunk AI Toolkit:

First navigate to your Splunk AI Toolkit application from the **Apps** menu:



Open the  
Splunk AI Toolkit app

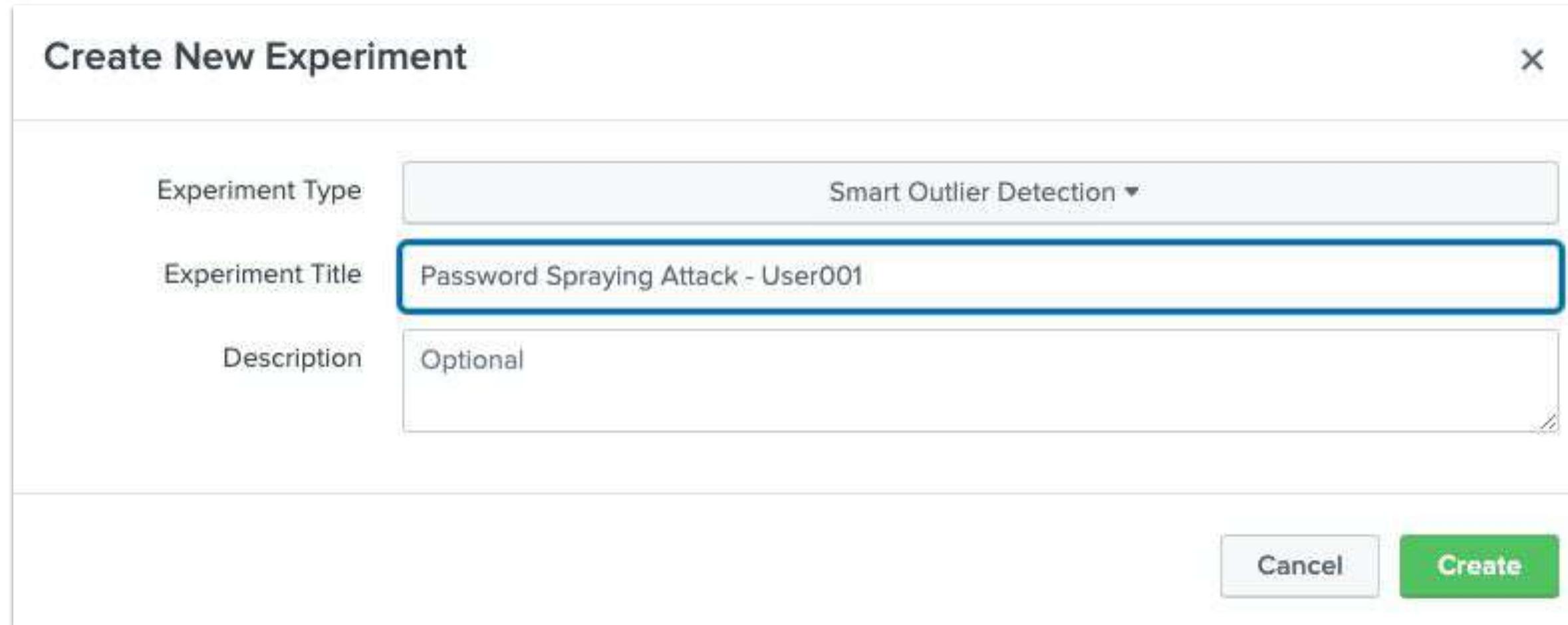
# Second Technique#2: Using Splunk AI Toolkit

1. Navigate to the Splunk AI Toolkit App
2. Choose Experiment
3. Select “Smart Outlier Detection”, name your experiment as per below, **adding your username (e.g. UserXXX)**

Create New Experiment X

Experiment Type	Smart Outlier Detection ▾
Experiment Title	>Password Spraying Attack - User001
Description	Optional

Cancel Create



# Second Technique#2: Using Splunk AI Toolkit

splunk>enterprise Apps ▾

Administrator 4 Messages Settings Activity Help Find

Showcase Experiments Search Models Classic Settings Docs Video Tutorials

Splunk Machine Learning Toolkit

Smart Outlier Detection: Windows - Password Spraying Attack Draft

Detect outliers in *unique\_accounts*, split by , using *Auto* distribution with a threshold of *0.01*

Define Data Source

View history

Search Datasets Metrics

index="main" sourcetype="XmlWinEventLog\_ws" EventCode=4625 LogonType=3  
| bucket span=2m \_time  
| stats dc(TargetUserName) AS unique\_accounts values(TargetUserName) as tried\_accounts by \_time,IpAddress,LogonType,dvc  
| eval HourOfDay = strftime(\_time,"%H") | eval HourOfDay=floor(HourOfDay/4)\*4 | eval DayofWeek = strftime(\_time,"%w") | eval isWeekend=if(DayOfWeek >= 1 AND DayOfWeek <= 5, 0,1)

All time

✓ 1,086 events (01/01/2019 00:00:00.000 to 08/11/2023 07:49:28.000)

Data Preview Visualization

20 Per Page ▾ Job ▾ Smart Mode ▾

_time	IpAddress	LogonType	dvc	unique_accounts	tried_accounts	DayofWeek	HourOfDay	isWeekend
2023-10-23 00:00:00	192.168.14.246	3	computer9	1	user68	1	0	1
2023-10-23 00:56:00	192.168.14.246	3	computer9	1	user68	1	0	1
2023-10-23 04:28:00	192.168.148.191	3	computer8	1	user31	1	4	1
2023-10-23 05:04:00	192.168.148.191	3	computer8	1	user31	1	4	1
2023-10-23 05:24:00	192.168.148.191	3	computer8	1	user31	1	4	1
2023-10-23 07:26:00	192.168.117.225	3	computer6	1	user9	1	4	1
2023-10-23 08:08:00	192.168.117.225	3	computer6	1	user9	1	8	1
2023-10-23 08:42:00	192.168.117.225	3	computer6	1	user9	1	8	1
2023-10-23 09:56:00	192.168.97.87	3	computer2	1	user14	1	8	1
2023-10-23 11:00:00	192.168.154.233	3	computer8	1	user28	1	8	1
2023-10-23 11:58:00	192.168.154.233	3	computer8	1	user28	1	8	1
2023-10-23 12:10:00	192.168.154.233	3	computer8	1	user28	1	12	1

Cancel Next >

# Second Technique#2: Using Splunk AI Toolkit

splunk>enterprise Apps ▾

Administrator ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Showcase Experiments Search Models Classic ▾ Settings Docs ▾ Video Tutorials ▾

Splunk Machine Learning Toolkit

Smart Outlier Detection: Windows - Password Spraying Attack Draft

Detect outliers in *unique\_accounts*, split by *dvc*, using *Auto* distribution with a threshold of **0.0017**

Learn Data View history

+ Add preprocessing step ▾

Define Learn Review Operationalize

**Det Outliers** ⚠

Too few training points in some groups will likely result in poor accuracy for those groups. Please see model summary to inspect such groups.

Field to analyze ? *unique\_accounts*

Split by fields *dvc* (1)

Distribution type ? *Auto*

Outlier tolerance threshold 0.0001 — 1 **0.0017**

Notes (optional)

**Detect Outliers**

Input Output Evaluate

Mode ? Automatic Manual

Outlier tolerance threshold 0.0001 — 1 **0.0017** Apply

Total Outliers ? **3**

Chart Type Density Time View Top 3 groups with most outliers Groups computer10, computer7, computer1

computer10

unique\_accounts

7  
6  
5  
4  
3  
2  
1  
0

show confidence interval  show outliers  ...

2 outliers

The screenshot shows the Splunk Machine Learning Toolkit interface for 'Smart Outlier Detection: Windows - Password Spraying Attack'. The 'Learn' tab is selected. On the left, there's a sidebar with 'Define', 'Learn', 'Review', and 'Operationalize' tabs. The 'Learn' tab has a warning message: 'Too few training points in some groups will likely result in poor accuracy for those groups. Please see model summary to inspect such groups.' Below this, there are sections for 'Field to analyze' (set to 'unique\_accounts'), 'Split by fields' (set to 'dvc'), 'Distribution type' (set to 'Auto'), and 'Outlier tolerance threshold' (set to 0.0017). The main area shows an 'Evaluate' tab with a histogram titled 'computer10'. The y-axis is 'unique\_accounts' from 0 to 7. The x-axis represents time. The histogram shows a very tall bar at 1 account and several other bars at higher account counts, with two bars highlighted in orange as outliers. A legend indicates 'show confidence interval' and 'show outliers' are checked. The total number of outliers is shown as 3, with 2 explicitly labeled on the chart.

# Second Technique#2: Using Splunk AI Toolkit

splunk>enterprise Apps ▾

Administrator ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Showcase Experiments Search Models Classic ▾ Settings Docs Video Tutorials

Splunk Machine Learning Toolkit

Smart Outlier Detection: Windows - Password Spraying Attack Draft

Detect outliers in *unique\_accounts*, split by , using *Auto* distribution with a threshold of **0.01**

Review Experiment

Define Learn Review Operationalize

Model Summary

Cardinality Histogram

Distribution Properties

Outlier Analysis

20 Per Page ▾

type	min	max	mean	std	cardinality	distance	other
Auto: Gaussian KDE	1	7	1.7211538461538463	1.3430022631758531	624	metric: wasserstein, distance: 0.2868619227437322	bandwidth: 0.370714716287206, parameter size: 624

# Publish Your Model

## Publish the Models

X

Publishing an Experiment model means the main model with any associated preprocessing models will be copied as lookup files in the user's namespace within the selected destination app.

New Main Model Title  Model names must start with a letter or underscore and contain only letters, numbers, and underscores

Destination App

Cancel Submit

**20 minutes to  
complete the lab**

**Lab 1**

# Privilege Escalation

Lab 2



# Using Simple stats

Method 1



# First technique#1: Simple stats

## Detecting Privileged Escalation Events

How to find anomalies this condition? You need to understand your data first

**Tips:** Use EventCode 4648, look for Windows Event Logs

Use the `stats` command to look at the volume of events and break it down by user. Use the `sort` command

Other stats functions: `stdev()`, `perc99.999()`...

What can you tell from the results? Anything outside of the ordinary?

# First technique#1: Simple stats

## Detecting Privileged Escalation Events

Now let's go one step further

Use the Eventstats, stdev command and eval command to find outliers.

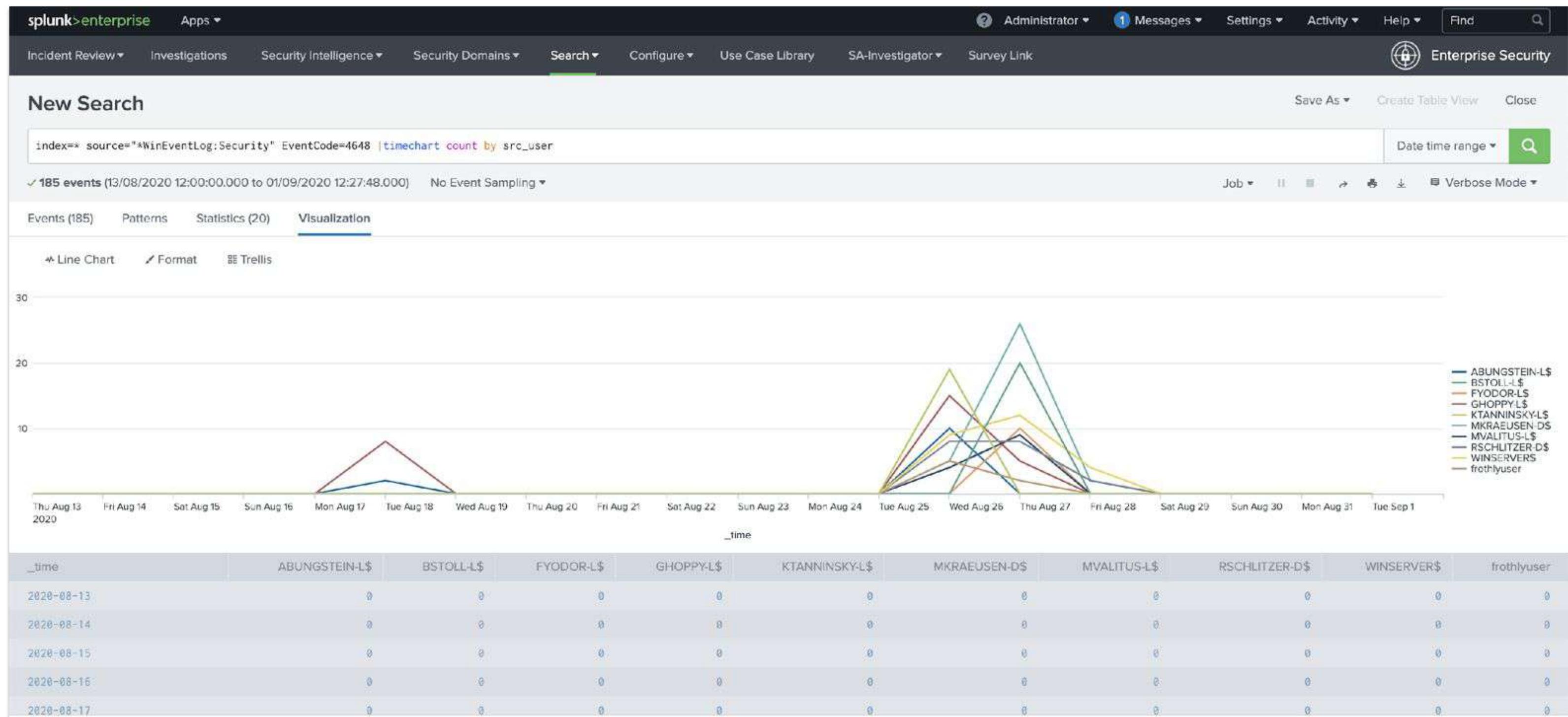
How would you do that? You can look at the documentation and figure out the commands to use:

<https://docs.splunk.com/Documentation/SCS/current/SearchReference/Aggregatefunctions#stdev.28.26lt.3Bvalue.26gt.3B.29>

Of course, there is an easier way! 😊

# First technique#1: Simple stats

## Detecting Privileged Escalation Events



# Using Splunk AI Toolkit

Method 2



# Splunk AI Toolkit:

First navigate to your Splunk AI Toolkit application from the **Apps** menu:



Open the Splunk AI Toolkit app

# Splunk AI Toolkit:

Now let's create an experiment:

1. Go to experiments
2. Choose Detect Numeric Outliers
3. Create New Experiment
4. Choose a title for your experiment (**add your username as it is a shared instance**)
5. Run the following search:

```
index=main source="*WinEventLog:Security" EventCode=4648  
| bucket _time span=1d | stats count by src_user _time
```

6. In Field to analyze, choose count
7. You can pick the Threshold method. For this exercise, the Standard Deviation method is the most suitable
8. You can tweak your Threshold multiplier based on the result that you get (e.g. too many outliers)
9. You can optionally specify a Sliding Window, and you can split by fields
10. Now, click on Detect Outliers

# Splunk AI Toolkit:

Detect Numeric Outliers: Escalated Privilege Windows Draft

Find values that differ significantly from previous values.

Experiment Settings    Experiment History

Enter a search

```
index=main source="*WinEventLog:Security" EventCode=4648  
| bucket _time span=1d | stats count by src_user _time|
```

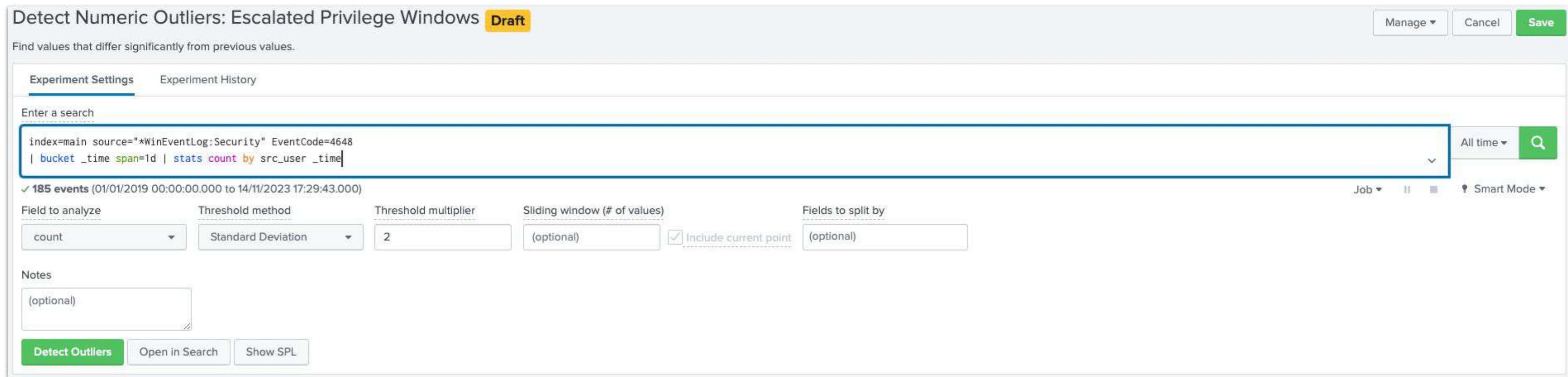
All time ▼ Search

✓ 185 events (01/01/2019 00:00:00.000 to 14/11/2023 17:29:43.000) Job ▾ II Smart Mode ▾

Field to analyze: count    Threshold method: Standard Deviation    Threshold multiplier: 2    Sliding window (# of values): (optional)  Include current point    Fields to split by: (optional)

Notes: (optional)

Detect Outliers Open in Search Show SPL



# Splunk AI Toolkit:

You can view the SPL query which was generated.

Click the “Show SPL” option:

[Calculate the outliers](#)  X

```
index=main source="*WinEventLog:Security" EventCode=4648 | bucket _time span=1d | stats  
count by src_user _time  
| eventstats avg("count") as avg stdev("count") as stdev          // calculate the mean and standard deviation  
| eval lowerBound=(avg-stdev*exact(2)), upperBound=(avg+stdev*exact(2))    // calculate the bounds as a multiple of the standard deviation  
| eval isOutlier;if('count' < lowerBound OR 'count' > upperBound, 1, 0)      // mark values outside the bounds as outliers
```

# Splunk AI Toolkit:

## Click on the Outlier to see who is the outlier:

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise' and 'user001-splk'. The main search bar contains the following SPL query:

```
index=main source="*WinEventLog:Security" EventCode=4648  
| bucket _time span=1d | stats count by src_user _time | eventstats avg("count") as avg stdev("count") as stdev | eval lowerBound=(avg-stdev*exact(2)), upperBound=(avg+stdev*exact(2)) | eval isOutlier;if('count' < lowerBound OR 'count' > upperBound, 1, 0) | search "count""=26"
```

The search results indicate 185 events found before 14/11/2023 17:36:46.000. The 'Statistics (1)' tab is selected, showing the following table:

src_user	_time	count	avg	isOutlier	lowerBound	stdev	upperBound
MKRAEUSEN-D\$	2020-08-27 00:00:00	26	8.80952380952381	1	-4.253692450173457	6.5316081298486335	21.872740069221077

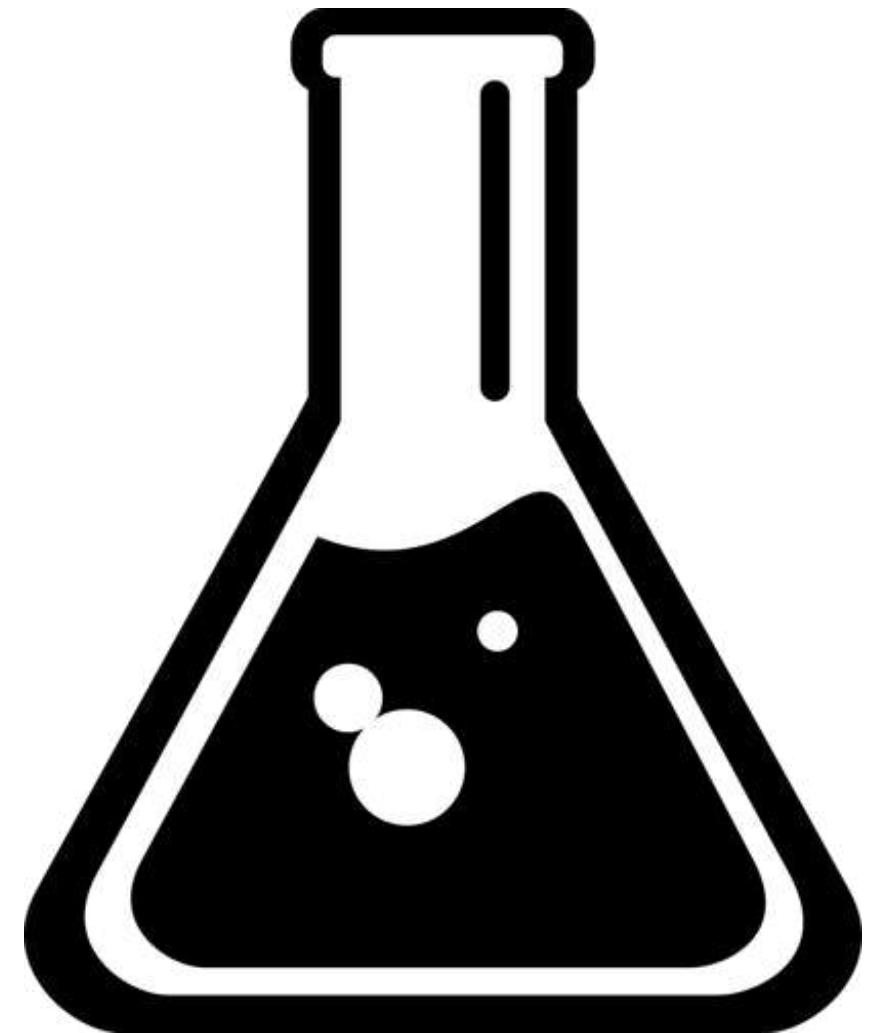
# What Other Fields Could Be of Interest?

*How About HTTP User Agent?*

# Classification

## Lab 3





**Let's  
experiment!**

# Detecting Categorical Outliers



# Detecting Categorical Outliers

The screenshot shows the Splunk Machine Learning Toolkit interface for detecting categorical outliers. The top navigation bar includes links for Showcase, Experiments, Search, Models, Settings, Docs, and Video Tutorials. The main title is "Detect Categorical Outliers: New\_experiment" with a "Draft" status. A search bar contains the SPL query: `index=** TERM(agent) sourcetype="stream:http" src_ip="*" http_user_agent="*" |table http_user_agent, action, dest_port, bytes_in, bytes_out`. Below the search bar, it says "✓ 10,177 events (8/20/18 4:00:03.000 AM to 1/2/23 6:56:33.000 AM)". The "Field(s) to analyze" section lists "http\_user\_agent". The "Notes" section is labeled "(optional)". At the bottom of the main panel are buttons for "Detect Outliers", "Open in Search", and "Show SPL".

**Outlier(s)** **19** **Total Event(s)** **10,177**

**Data and Outliers**

http_user_agent	probable_cause	isOutlier
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36	http_user_agent	1
Python-urllib/2.7	http_user_agent	1
SEP/14.2.760:0000, MID/{B17CE05D-4C23-1A71-1056-F57493DF00EB}, SID/10 SEQ/180725021	http_user_agent	1
SEP/14.2.760:0000, MID/{B17CE05D-4C23-1A71-1056-F57493DF00EB}, SID/10	http_user_agent	1
SEP/14.2.760:0000, MID/{B17CE05D-4C23-1A71-1056-F57493DF00EB}, SID/10 LUE/2.6.1.11 (Windows;10.0;SP0.0;X64;ENU)	http_user_agent	1

# Detecting Categorical Outliers

- Try to run the same search but change the field to analyze (e.g. bytes in, bytes out...)
- What results do you get?
- Do you think it's a good approach?
- Let's try a different approach and use Clustering!

# Clustering



# Detecting Categorical Outliers

Preprocessing your data - let's play with TFIDF

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** index==\* TERM(agent) sourcetype=="stream:http" src\_ip=="\*" http\_user\_agent=="\*" |table http\_user\_agent, src\_ip, dest\_ip, action, dest\_port, bytes\_in, bytes\_out |head 3000 |fit TFIDF http\_user\_agent
- Results Summary:** 10,177 events (before 1/23 7:12:18.000 AM) No Event Sampling
- Panel Tabs:** Events (10,177), Patterns, Statistics (3,000) (selected), Visualization
- Table Headers:** http\_user\_agent, src\_ip, dest\_ip, action, dest\_port, bytes\_in, bytes\_out, http\_user\_agent\_tfidf\_0\_0000, http\_user\_agent\_tfidf\_1\_10, http\_user\_agent\_tfidf\_2\_10011, http\_user\_agent\_tfidf\_3\_10228, http\_user\_agent\_tfidf\_4\_103, http\_user\_agent\_tfid
- Table Data:** The table lists various user agents along with their source and destination IP addresses, actions, ports, and byte counts. The TFIDF scores for each user agent are also listed. For example, Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 has a TFIDF score of 0.17495927083811538.

# Detecting Categorical Outliers

Now let's use clustering!

The screenshot shows the Splunk Machine Learning Toolkit interface. The search bar contains the following command:

```
index=*_ TERM(agent) sourcetype="stream:http" src_ip="*" http_user_agent="*" |table http_user_agent, src_ip, dest_ip, action, dest_port, bytes_in, bytes_out |head 3000 |fit TFIDF http_user_agent |fit KMeans k=5 http_user_agent_tfidf_* |stats values (http_user_agent) by cluster
```

The search results show 10,177 events. The Statistics tab is selected, displaying the following clusters:

cluster	values(http_user_agent)
0	aws-sdk-go/1.12.20 (go1.8.4; linux; amd64)
1	ELB-HealthChecker/2.0
2	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
3	Mozilla/5.0
4	Alprazolam/2.0 ClamAV/0.99.2 (OS: linux-gnu, ARCH: x86_64, CPU: x86_64) MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT Microsoft BITS/7.8 Microsoft Office/16.0 (Windows NT 10.0; Microsoft Excel 16.0.10228; Pro) Microsoft Office/16.0 (Windows NT 10.0; Microsoft Outlook 16.0.10228; Pro) Microsoft-CryptoAPI/10.0 Microsoft-Delivery-Optimization/10.0 Microsoft-WNS/10.0 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7 Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) Mozilla/5.0 (compatible; MSTF 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

# Detecting Categorical Outliers

Let's try something else!

The screenshot shows the Splunk Machine Learning Toolkit interface. The search bar contains the following SPL command:

```
index=* TERM(agent) sourcetype="stream:http" src_ip="*" http_user_agent="*" |table http_user_agent, src_ip, dest_ip, action, dest_port, bytes_in, bytes_out |head 3000 |fit Tfidf http_user_agent |fit KMeans k=1 http_user_agent_tfidf_* |fields - http_user_agent_tfidf_* |stats max(cluster_distance) by cluster http_user_agent | sort - max(cluster_distance)
```

The results table displays 10,177 events. The columns are 'cluster' and 'http\_user\_agent'. The first few rows show:

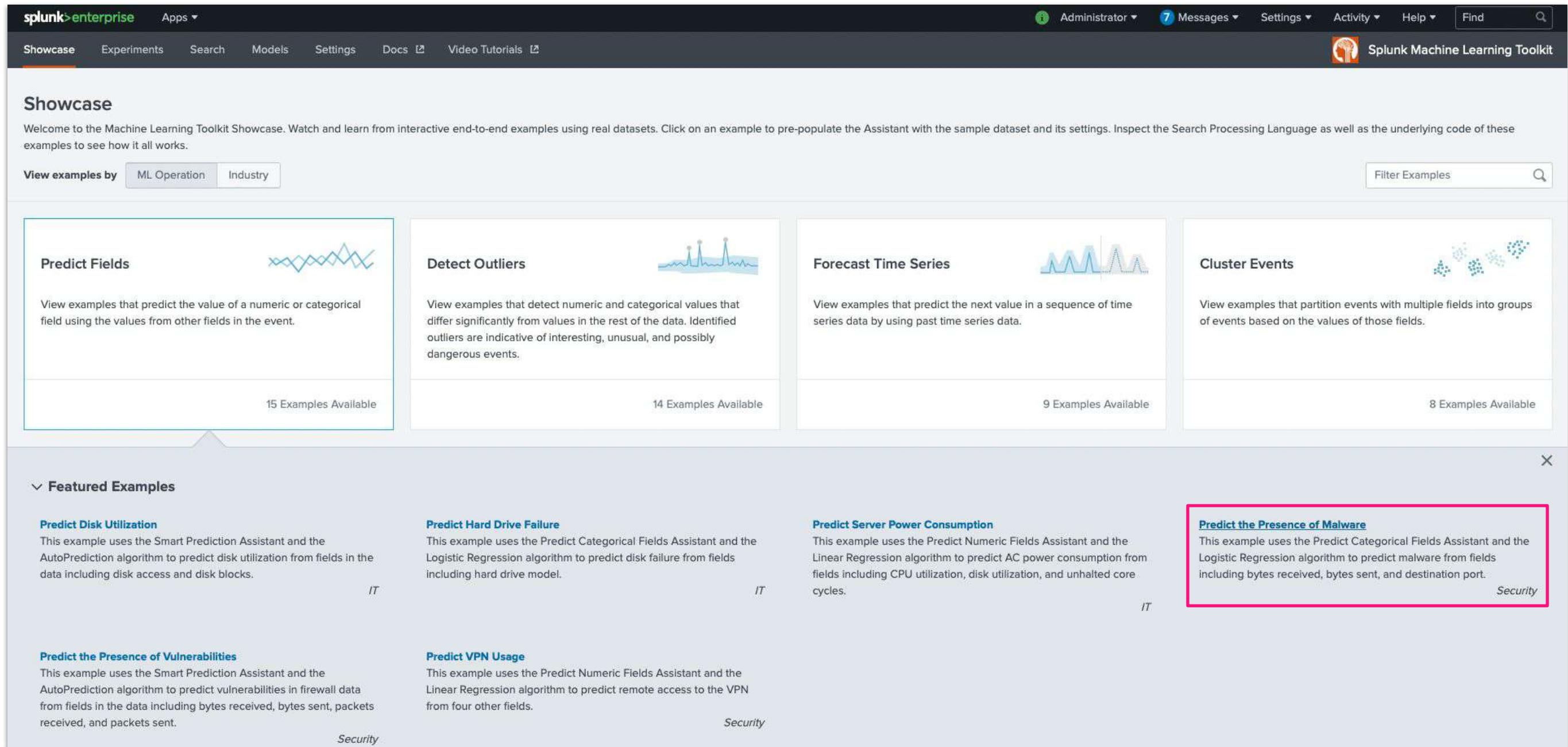
cluster	http_user_agent	max(cluster_distance)
0	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)	1.1539107576147307
0	aws-sdk-go/1.12.20 (go1.8.4; linux; amd64)	1.1336852514617446
0	Mozilla/5.0	1.114913837866919
0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36	1.039848375036444
0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36	1.0309951961655088
0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	1.0271065926702692
0	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36	1.0245556136033789
0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	1.0213414756302928
0	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36	1.0154026971917771
0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	0.8282086833711153
0	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36	0.8158749659787358
0	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36	0.790346971694435
0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134	0.7191211131029
0	ELB-HealthChecker/2.0	0.3957707127071142
0	Alprazolam/2.0	0.31577071270711504

# Predict *Categorical* Fields



# Predict Categorical Fields

- Navigate to your Splunk AI Toolkit application
- Click on “showcase”, choose “Predict Fields”, and select “Predict the Presence of Malware”



The screenshot shows the Splunk Machine Learning Toolkit interface. The top navigation bar includes "splunk>enterprise" and "Apps". On the right, there are links for "Administrator", "Messages", "Settings", "Activity", "Help", and a search bar. The main header "Splunk Machine Learning Toolkit" has a brain icon.

The "Showcase" section is active. Below it, there are four cards:

- Predict Fields**: View examples that predict the value of a numeric or categorical field using the values from other fields in the event. 15 Examples Available.
- Detect Outliers**: View examples that detect numeric and categorical values that differ significantly from values in the rest of the data. Identified outliers are indicative of interesting, unusual, and possibly dangerous events. 14 Examples Available.
- Forecast Time Series**: View examples that predict the next value in a sequence of time series data by using past time series data. 9 Examples Available.
- Cluster Events**: View examples that partition events with multiple fields into groups of events based on the values of those fields. 8 Examples Available.

Below these cards, under "Featured Examples", are four more items:

- Predict Disk Utilization**: This example uses the Smart Prediction Assistant and the AutoPrediction algorithm to predict disk utilization from fields in the data including disk access and disk blocks. IT
- Predict Hard Drive Failure**: This example uses the Predict Categorical Fields Assistant and the Logistic Regression algorithm to predict disk failure from fields including hard drive model. IT
- Predict Server Power Consumption**: This example uses the Predict Numeric Fields Assistant and the Linear Regression algorithm to predict AC power consumption from fields including CPU utilization, disk utilization, and unhalted core cycles. IT
- Predict the Presence of Malware**: This example uses the Predict Categorical Fields Assistant and the Logistic Regression algorithm to predict malware from fields including bytes received, bytes sent, and destination port. Security

A red box highlights the "Predict the Presence of Malware" card.

# Predict Categorical Fields

- Check the data in the lookup file “firewall\_traffic.csv”
- See what field are being used for our prediction
- Try the different algorithms and see which one is the more precise
- Why? Understand the logic behind the algorithms.

# Brainstorming time!



# Predict Categorical Fields

- Think about some use cases where prediction would be useful
- Better if it is Security Related
- Did you come up with something?

# Anomaly Detection



# Numeric Outlier Detection

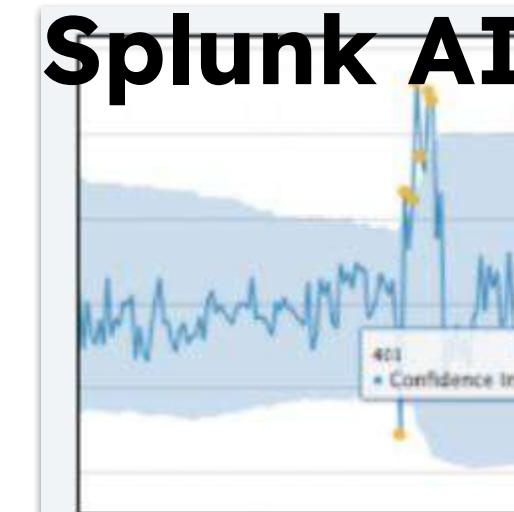
A type of Anomaly Detection

## Outlier in some numerical value

- Number of transactions
- Transaction latency
- System utilization (CPU/memory)
- Number of logins
- Amount of data transfer
- Time between actions
- Sensor measurement

## Detect Numeric Outliers Assistant in

### Splunk AI Toolkit



**Detect Numeric Outliers**

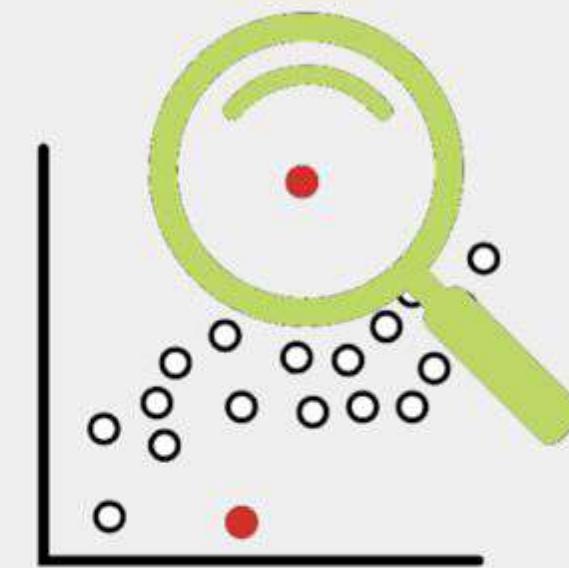
Find values that differ significantly from previous values.

**Examples**

- Detect Outliers in Server Response Time
- Detect Outliers in Number of Logins (vs. Predicted Value)
- Detect Outliers in Supermarket Purchases
- Detect Outliers in Power Plant Humidity
- Detect Cyclical Outliers in Call Center Data
- Detect Cyclical Outliers in Logins

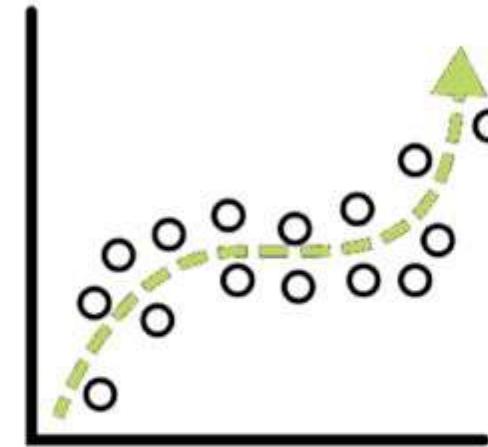
# Anomaly Detection

## Anomaly detection



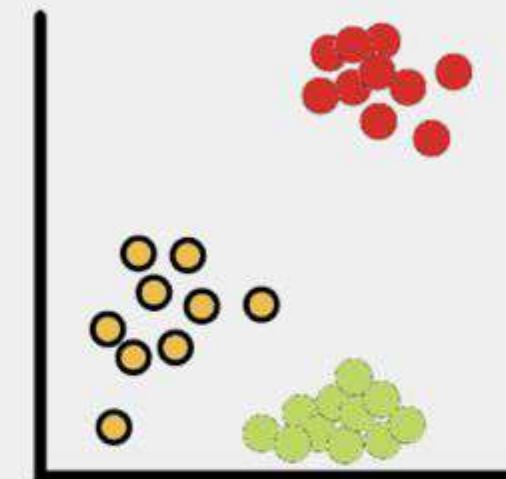
- ▶ Deviation from past behavior
- ▶ Deviation from peers
- ▶ (aka Multivariate AD or Cohesive AD)
- ▶ Unusual change in features

## Predictive Analytics



- ▶ Predict Service Health Score/Churn
- ▶ Predicting Events
- ▶ Trend Forecasting
- ▶ Detecting influencing entities
- ▶ Early warning of failure

## Clustering



- ▶ Identify peer groups
- ▶ Event Correlation
- ▶ Reduce alert noise
- ▶ Behavioral Analytics

# Outlier vs Anomaly

What's the difference?

## Outlier (noun):

- A statistical observation that is markedly different in value from the others of the sample
- Outliers are usually something unexpected in a **single** value or measurement

## Anomaly (noun):

- Something different, abnormal, peculiar or not easily classified
- Deviation from the common rule
- Anomalies are usually based on a **collection** of observations

Not all outliers are anomalies, but anomalies often consist of outliers or are outliers

# Cheat sheet for anomaly detection in Splunk

Command	Description	Method / Algorithm	Description
<a href="#">analyzefields (af)</a>	Analyze numerical fields for their ability to predict another discrete field.	DensityFunction	The DensityFunction algorithm provides a consistent and streamlined workflow to create and store density functions and utilize them for anomaly detection...
<a href="#">anomalies</a>	Computes an "unexpectedness" score for an event.	LocalOutlierFactor	The LocalOutlierFactor algorithm measures the local deviation of density of a given sample with respect to its neighbors...
<a href="#">anomalousvalue</a>	Finds and summarizes irregular, or uncommon, search results.	OneClassSVM	The OneClassSVM algorithm fits a model from a set of features or fields for detecting anomalies and outliers...
<a href="#">anomalydetection</a>	Identifies anomalous events by computing a probability for each event and then detecting unusually small probabilities.	Clustering Algorithms	Spot point anomalies or anomalous clusters. Inspect e.g. cluster_distance with KMeans, cluster=-1 with DBSCAN...
<a href="#">cluster</a>	Clusters similar events together.	Classifiers and Regressors	Inspect strong residuals when applying your well fitted model to new incoming data points.
<a href="#">kmeans</a>	Performs k-means clustering on selected fields.	ML SPL API	Wrap your own algorithms of choice
<a href="#">outlier</a>	Removes outlying numerical values.		
<a href="#">rare</a>	Displays the least common values of a field.		

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Commandsbycategory>

<https://docs.splunk.com/Documentation/MLApp/latest/User/Algorithms>

# Detecting outliers with Enterprise Security

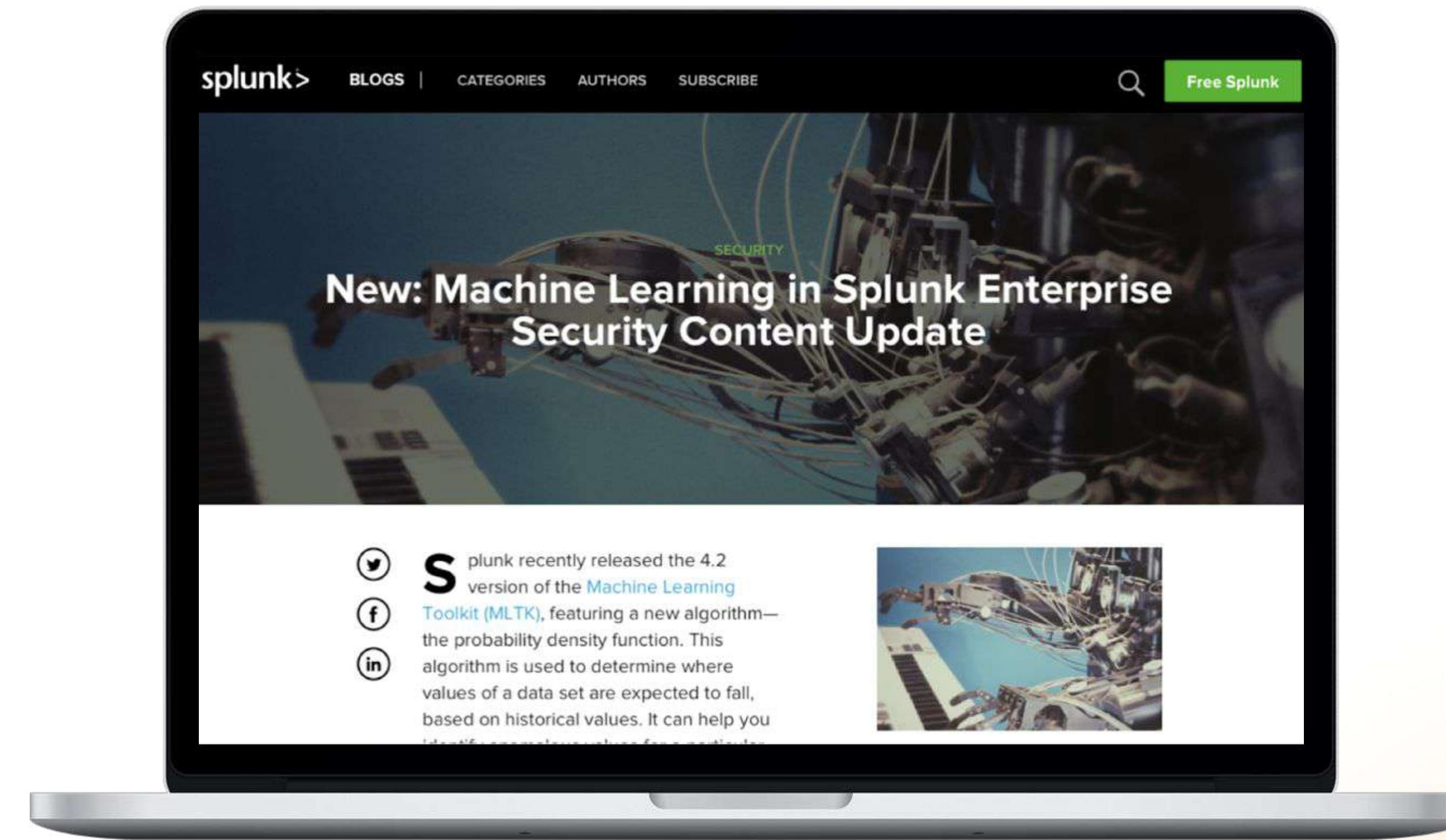
## **Enterprise Security ships with Splunk AI Toolkit as of ES version 6.0**

The Splunk AI Toolkit (Formerly MLTK) is replacing Extreme Search (XS) as a model generation package in Enterprise Security (ES). Splunk AI Toolkit can scale at larger volume and also can identify more abnormal events through its models (see [Welcome to the Machine Learning Toolkit](#) in the Splunk Machine Learning Toolkit User Guide.)

ES is using Splunk AI Toolkit DensityFunction under the hood.

<https://docs.splunk.com/Documentation/ES/latest/Admin/MLTKOverview>

# ES Content Update includes Density Function content



# Machine Learning Applications from Splunkbase

splunkbase™



# Machine Learning Applications

**Splunk  
Security  
Essentials**



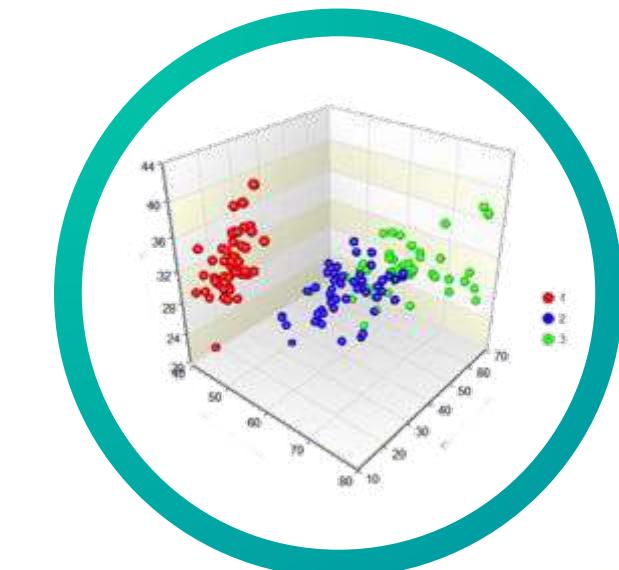
**DGA App for  
Splunk**



**Botnet App for  
Splunk**



**Custom Detections  
using AI Toolkit**



# Splunk Security Essentials

Download from Splunkbase:

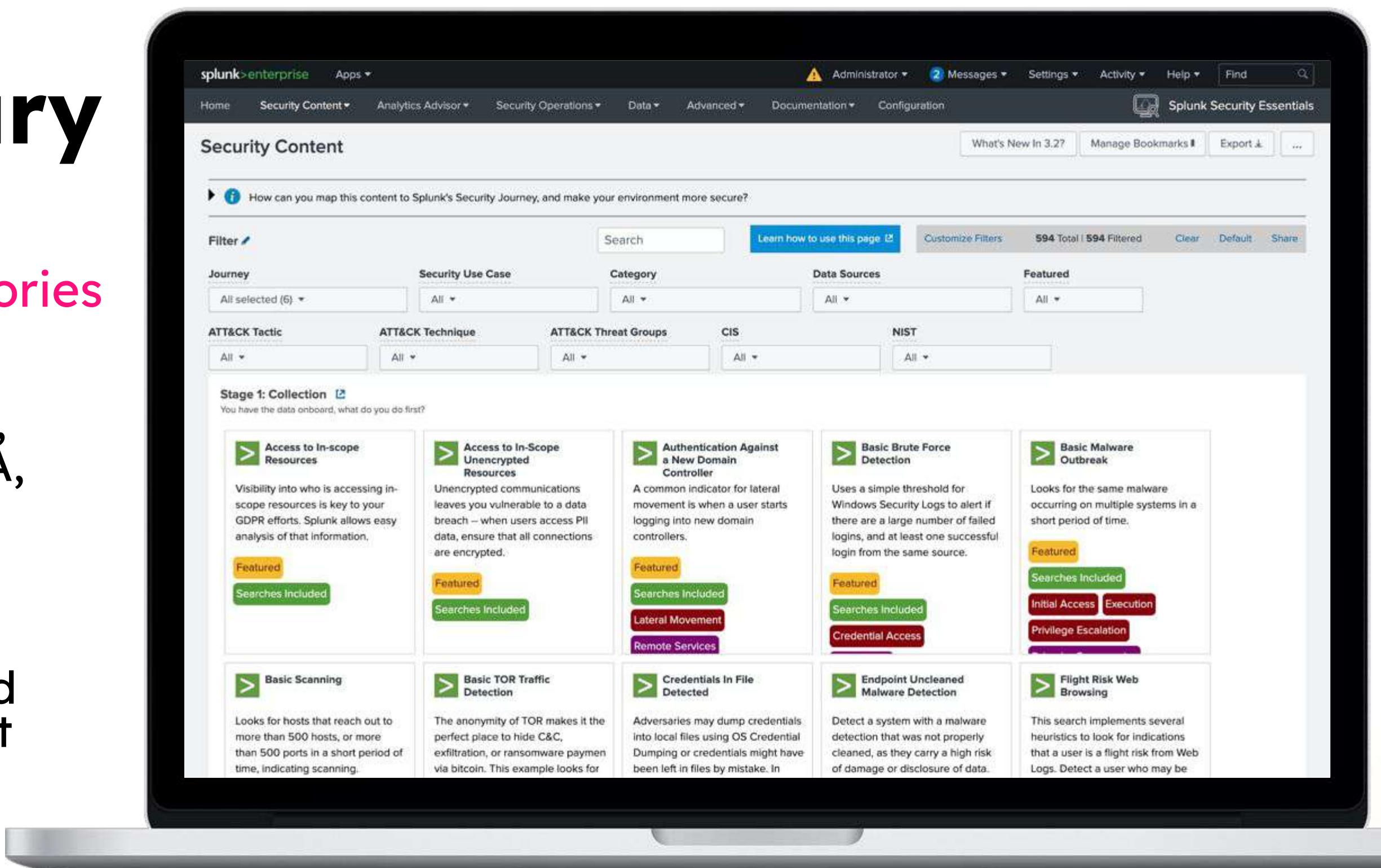
<https://splunkbase.splunk.com/app/3435>



# Security Content Library

Browse, bookmark, and deploy 900+ security detections and analytic stories

- Repository of Security Content for Splunk Cloud, Enterprise Security, UEBA, and Phantom
- Deploy security content within clicks
- Enrich notable events and run analytics with context from content library
- Stay up to date on existing and emerging threats





# Includes Behavioral Detections

Identify bad guys in your environment:

- Includes 50+ use cases common in UEBA products, all using Splunk Enterprise
- Target external attackers and insider threat
- Scales from small to massive companies
- Save from the app, send results to ES/UBA

The most widely deployed UEBA product in the market is Splunk Enterprise, but no one knows it.

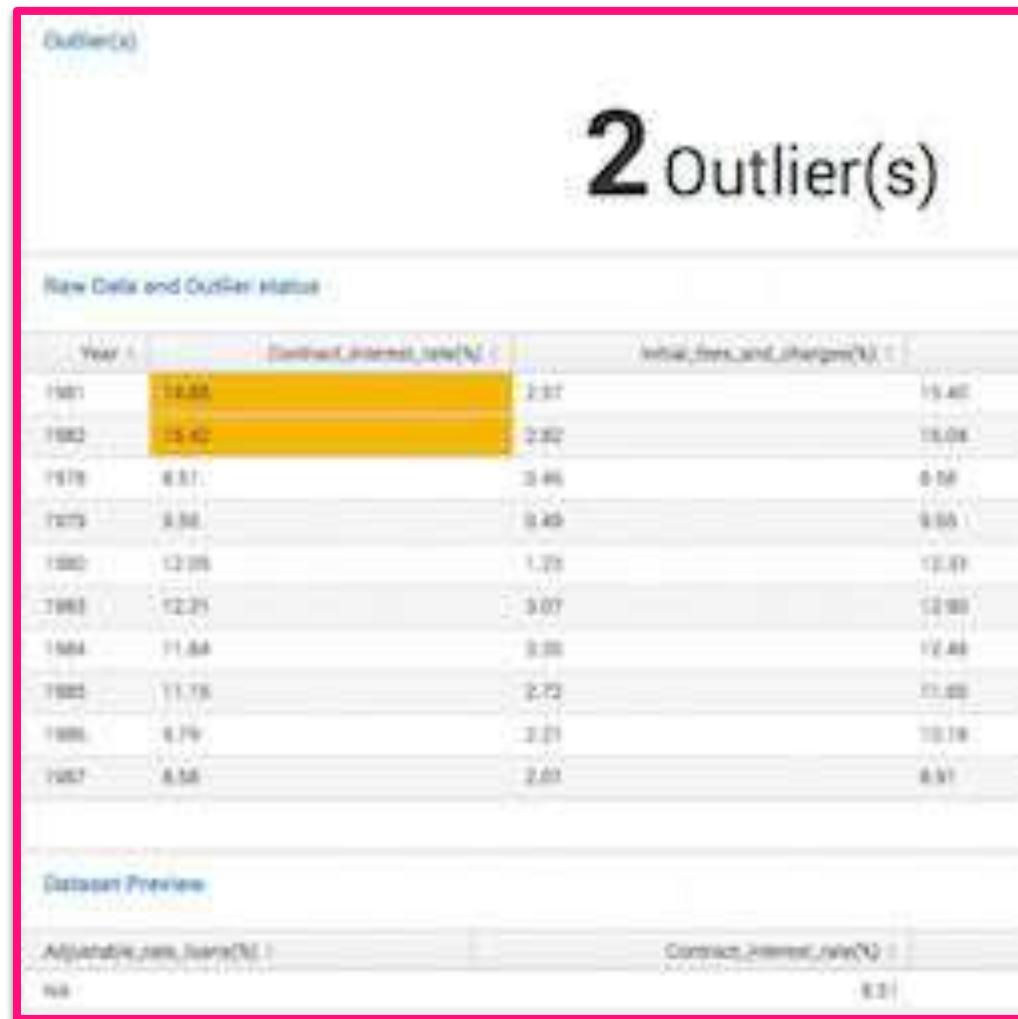
**Solve your use cases today, then use Splunk UBA for advanced ML detection.**

The screenshot shows the Splunk Security Essentials interface with the 'Security Content' tab selected. The top navigation bar includes links for Home, Security Content, Analytics Advisor, Security Operations, Data, Advanced, Documentation, Configuration, and various user settings. A search bar and filters are available on the left. The main area displays a grid of 12 behavioral detection use cases under the heading 'Stage 1: Collection'. Each card contains a title, a brief description, and status indicators such as 'Featured' and 'Searches Included'.

Card Title	Description	Status
Authentication Against a New Domain Controller	A common indicator for lateral movement is when a user starts logging into new domain controllers.	Featured Searches Included Remote Services
Increase in # of Hosts Logged into	Find users who log into more hosts than they typically do.	Featured Searches Included Remote Services
Increase in Pages Printed	Find users who printed more pages than normal.	Searches Included Exfiltration Over Physical Medium
New Interactive Logon from a Service Account	In most environments, service accounts should not log on interactively. This search finds new user/host combinations for accounts starting with "svc_".	Featured Searches Included Valid Accounts
Disabled Update Service	Splunk can detect the status of services, allowing us to find hosts where the Windows Update service is disabled.	Searches Included
First Time Logon to New Server	Find users who logged into a new server for the first time.	Searches Included
First Time USB Usage	Find systems the first time they generate Windows Event ID 20001, which for some customers occurs when a USB drive is plugged in.	Searches Included
Hosts Sending To More Destinations Than Normal	This will typically detect scanning activity, along with lateral movement activity.	Searches Included

# Splunk Security Essentials

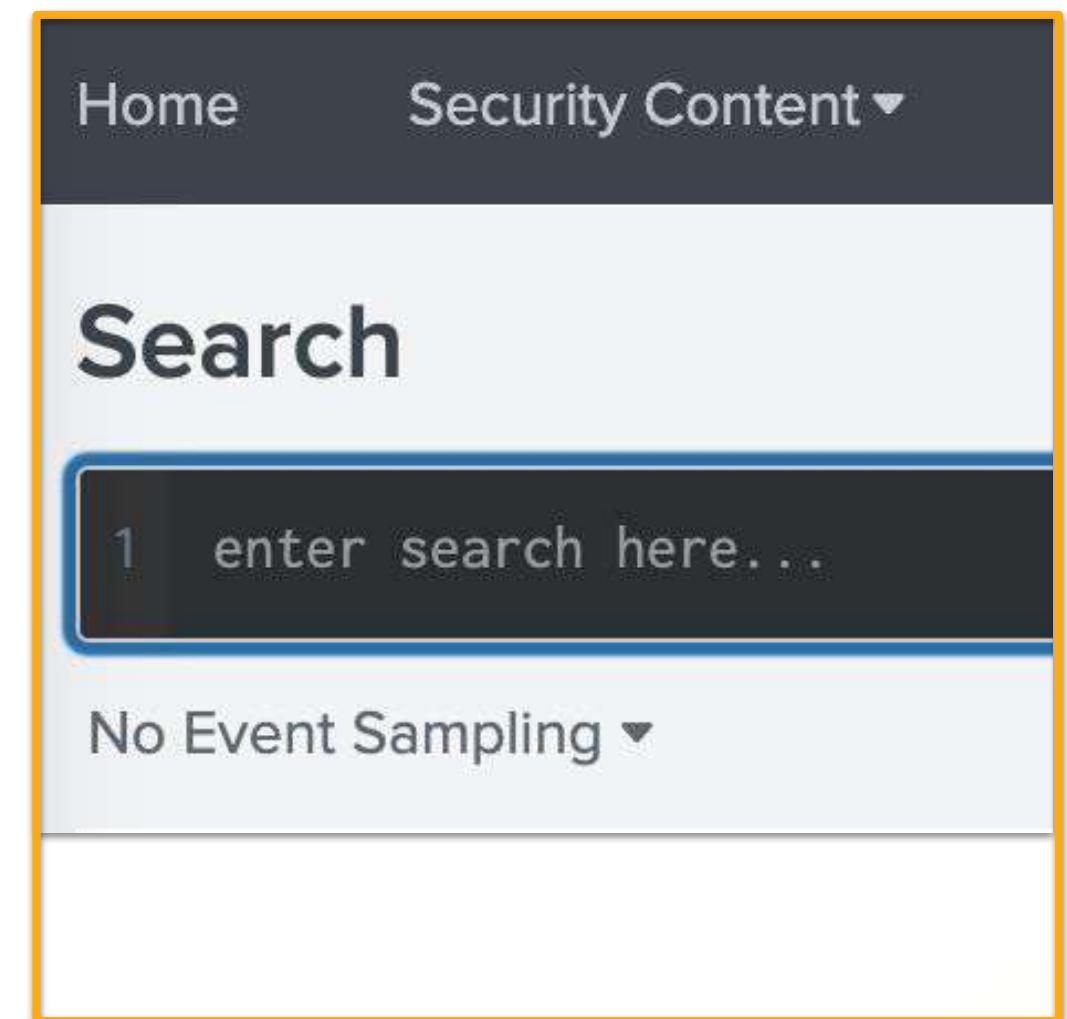
## Types of Use Cases



First Time Seen  
powered by stats



Time Series Analysis  
with Standard  
Deviation



General Security  
Analytics Searches

# Data and Content Introspection

## Track data and saved searches to gain visibility

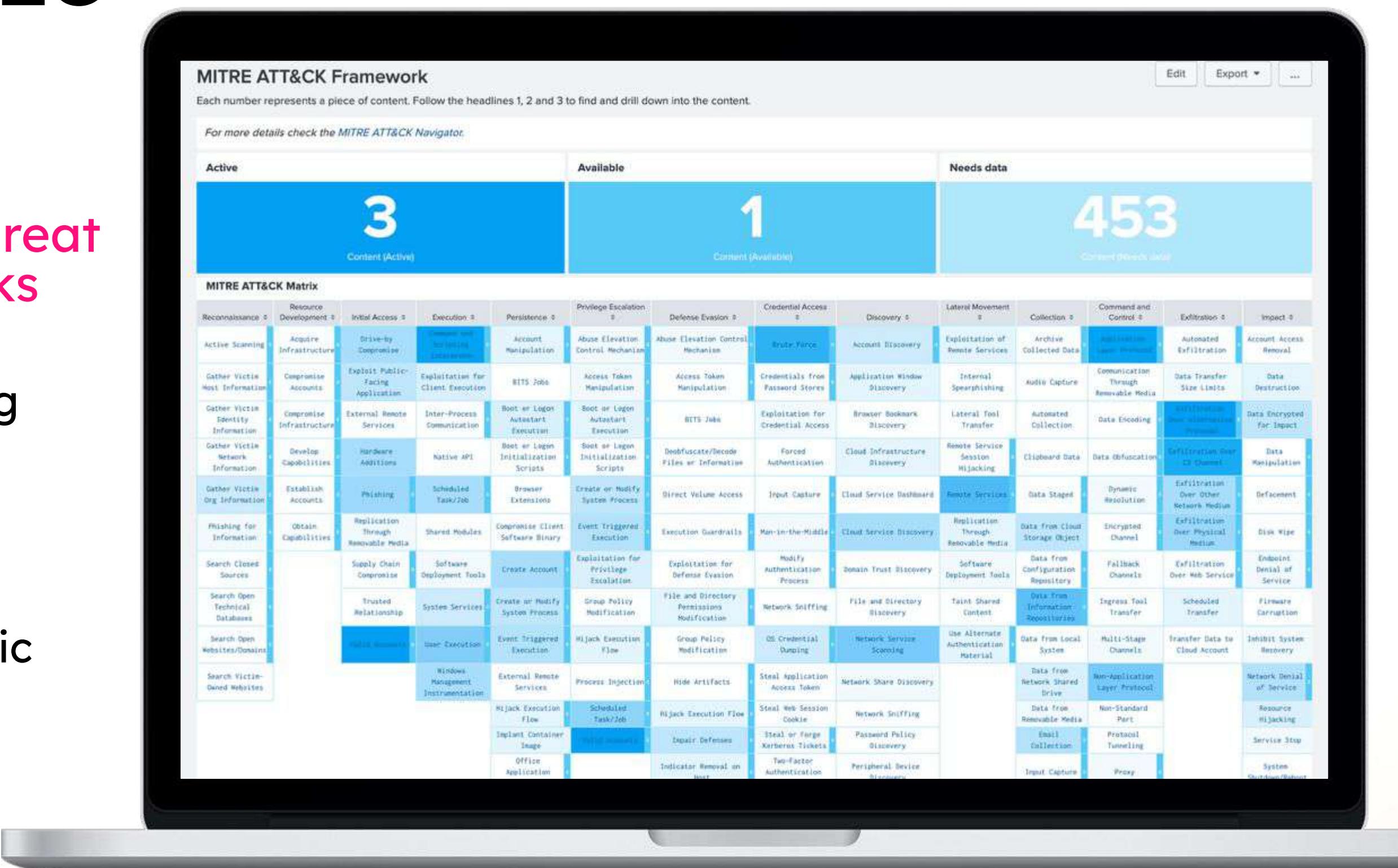
- Enrich saved searches with tags and metadata
- Automatic categorization by security products
- Scale with data model acceleration and by reinforcing CIM compliance

The screenshot displays the Splunk Security Essentials interface on a mobile device. The top navigation bar includes links for Home, Security Content, Analytics Advisor, Security Operations, Data, Advanced, Documentation, Configuration, Splunk User, Messages, Settings, Activity, and Help. The main content area is titled "Data Inventory" and lists various data categories with their counts: Email (2), DNS (3), Authentication (2), Anti-Virus or Anti-Malware (3), Web Proxy (2), and User Activity Audit (0/5). Below these are detailed lists for each category, such as "Endpoint Detection and Response" which includes Object Change, Process Launch, and Process Launch with CLI. To the right, there are sections for "Endpoint Detection and Response", "Object Change", "Content for This Data Source Category" (listing various threat detection techniques like Abnormally High Number of Endpoint Changes By User, Access LSASS Memory For Dump Creation, etc.), "MITRE ATT&CK Tactics" (Command and Control, Credential Access, Defense Evasion, etc.), "MITRE ATT&CK Techniques" (Abuse Elevation Control Mechanism, Application Layer Protocol, etc.), and "Kill Chain Phases". The overall theme is cybersecurity and data monitoring.

# Operationalize Security Frameworks

Identify gaps, improve threat detection, and reduce risks

- Develop an understanding of your security posture against MITRE ATT&CK® and Cyber Kill Chain® frameworks
- Find detections for specific Threat Groups or Threat Software
- Drilldown on known Tactics and Techniques and Kill Chain Phases for more details



# DGA App for Splunk

Download from Splunkbase:

<https://splunkbase.splunk.com/app/3559/>



# Domain Generating Algorithms (DGA)

What's the problem?

## Challenges to detect DGAs:

- Static matching runs against potentially infinite blacklist entries
- Regex can narrow down this list, but still hard to compute and find rules (and define exceptions for rules)
- Unknown unknowns?
- Want to get fuzzy?
- Let's ML!

## Example of DGAs:

domain
iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea
ifferfsodp9ifjaposdfjhgosurijfaewrwegwea
ayylmaotjhsstasdfasdfasdfasdfasdfasdf
lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea
sdfjhgosurijfaqwqwqrgwea

Example IoCs for WannaCry: <https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf>

Example IoCs for Sunburst:

[https://github.com/fireeye/sunburst\\_countermeasures/blob/main/indicator\\_release/Indicator\\_Release\\_NBIs.csv](https://github.com/fireeye/sunburst_countermeasures/blob/main/indicator_release/Indicator_Release_NBIs.csv)

Additional details at [https://www.splunk.com/en\\_us/blog/security/sunburst-backdoor-detections-in-splunk.html](https://www.splunk.com/en_us/blog/security/sunburst-backdoor-detections-in-splunk.html)

## DGA App for Splunk

philipp@splunk.com

[Edit](#)[Export ▾](#)

...

## Content overview

1. Exploratory Data Analysis



2. Feature Engineering and Selection



3. Create Machine Learning Models



4. Operationalize Machine Learning



5. Test and Benchmark



## Setup

For full functionality of the app please check and review the [setup dashboard page](#) and make sure that all setup steps are completed.

- Example for end to end data science process
- Disclaimer: this is not a turn key solution but a template to get you started
- Feel free to improve and give us your feedback!



## 1. Data Exploration

Edit

Export ▾

...

## Dataset Overview

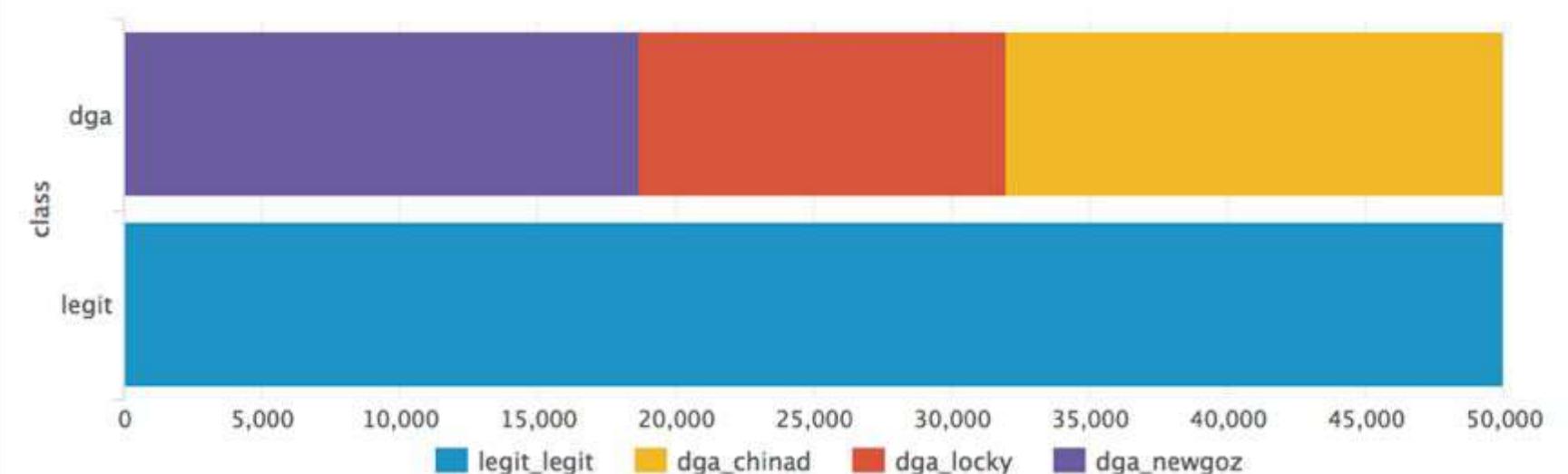
The dataset consists of a labeled domain names that indicate whether a domain is legit or created by some DGA that is known from botnets. We have around 60% domain names from legit domains and remaining 40% split across 3 DGA subclasses that correspond to different botnets.



domains.csv

class	domain	subclass
legit	google.com	legit
legit	www.google.com	legit
legit	microsoft.com	legit
legit	facebook.com	legit
legit	doubleclick.net	legit

« prev 1 2 3 4 5 6 7 8 9 10 next »



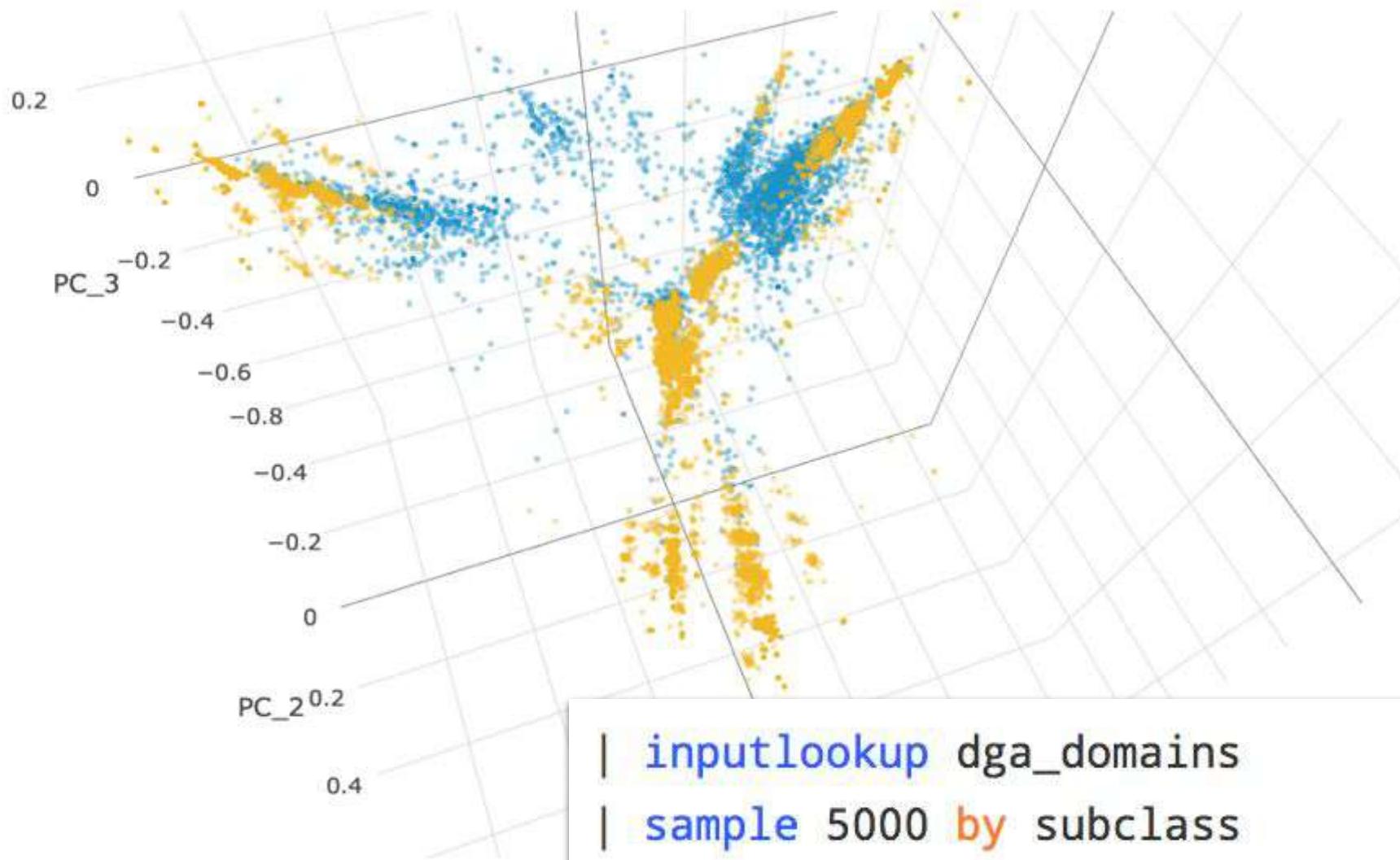
## Sample of domains by subclasses

column	chinad	legit	locky	newgoz
domains	15nrbrfoqajvt92p.com 2eb7jd4214efdemez.net 9dkwgr7osoqr3sj8.info bof8b9ediq2zgxcx.info eejxv00hk3e9mu7n.net eo9i0keybpezdwjx.org jd59a3g1bqumyvn1.org kdh2kxsxrohdr432.net s45srq078fv7q7j8.net swfa7qz5k2pefj63.biz	943.engine.mobileapptracking.com a.applvn.com ads.rubiconproject.com buy.tinypass.com fmcz4-1.fna.fbcdn.net homedepot.az1.qualtrics.com pandora.com pix.bfi0.com track.wattpad.com us-east-1.elb.amazonaws.com	clgsaguvihthkai.click eltineojriud.biz jpyecccdbiz jtxopqxokgcdnqmn.pw lmhyhqym.su okfhcdiayd.click pchjmkjhoqt.biz tvmlivvyb.biz vawmxlhoiconu.org xxixgjltu.pl	15kfdx1uy33wsq420w81t24jmz.biz 1c4pu7etfir7l106r8vqt89xz.net 1i14a381pwjcnd1pyddk2191bcng.biz 1jjxlm24webiq1m91b7v1u9i37h.org 1wyjzq3104oa5hn7rpkw1w36niz.com mokou21vftme61whl7hggd7wp0.net p2ht3uqv42qx14vveb5nwlasr.org q21qhn15f53lz17y86983vc31e.com ustqjsa8rvla1y25kr386qngm.com zrxndhyj6yb3199ycn1xve3m3.org

- Small data set with 100K domain names for training and testing

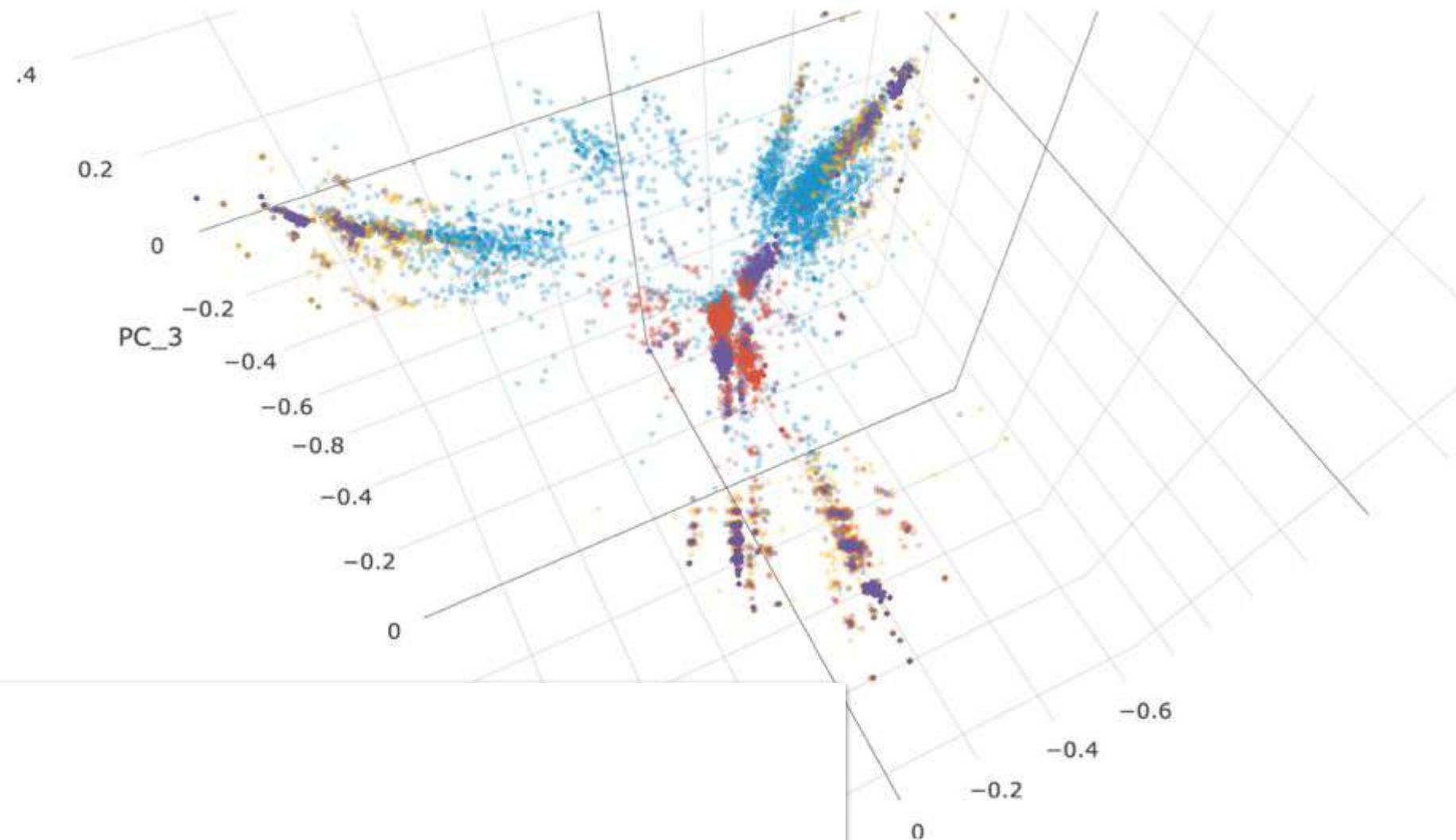
## Data Exploration with Text Mining approach

n-gram analysis (2-3 char groups) of domain names with PCA k=3 by class



```
| inputlookup dga_domains  
| sample 5000 by subclass  
| fit TFIDF domain analyzer=char ngram_range=2-3 into "dga_ngram"  
| fit PCA domain_tfidf* k=3 into "dga_pca"  
| fields - domain_tfidf*  
| eval label=class._.subclass  
| table label PC_*  
| sort 0 - label
```

n-gram analysis (2-3 char groups) of domain names with PCA k=3 by subclass



## 2. Feature Engineering and Selection

[Edit](#) [Export](#) ...**Feature Engineering**

Detecting DGAs may require additional features that are not present in the raw table of domain names. Additional features can be any meaningful additional information that help to characterize the dataset with regards to the analytics goal, ideally in a very distinct manner. In this case we derive features from the pure domain name strings that allow to shape indicators of a generated domain name. As part of data preprocessing we save the computed results after using some SPL and methods from the [URL Toolbox App](#):



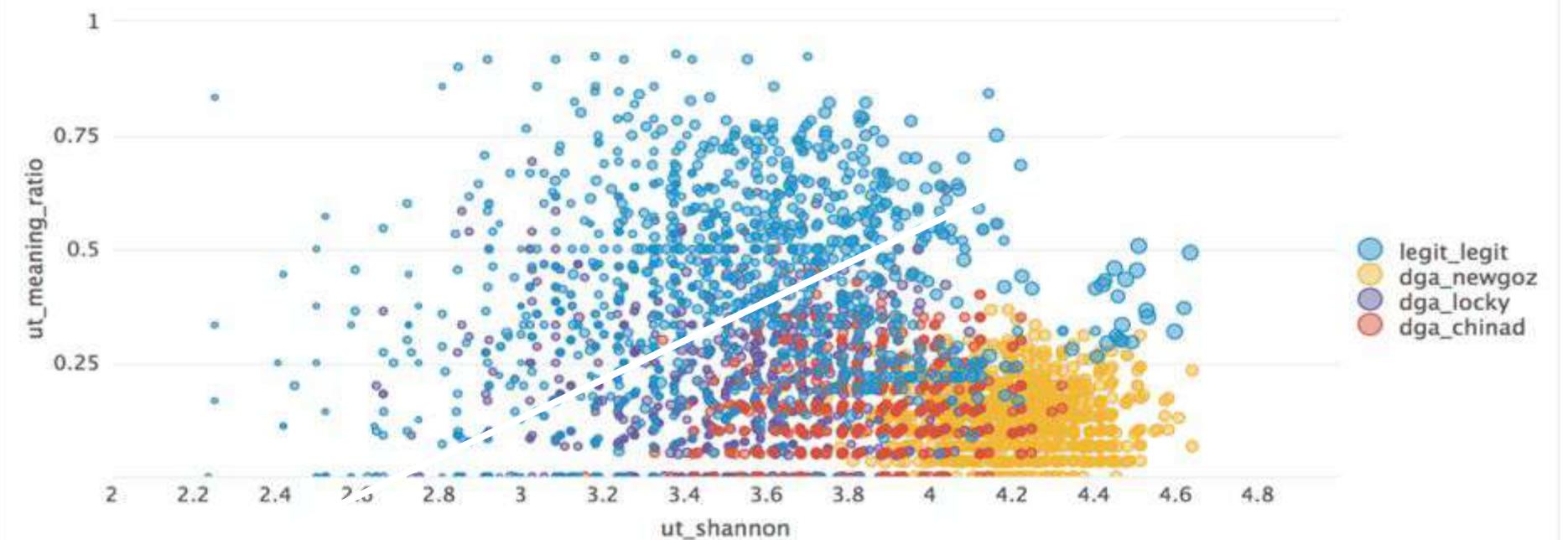
## Domain dataset enriched with features

domain	class	subclass	ut_consonant_ratio	ut_digit_ratio	ut_domain_length	ut_meaning_ratio	ut_shannon	ut_vowel_ratio	PC_1	PC_2	PC_3
lvmaehe1voogfbss.net	dga	chinad	0.600	0.050	20.000	0.300	3.784	0.300	0.502	-0.304	0.092
Tamn1a519ort3p12o09111e6288k.com	dga	newgoz	0.281	0.531	32.000	0.156	3.925	0.188	-0.358	-0.008	0.181
fiaxbg19j4wxu16sacop1su49dx.org	dga	newgoz	0.516	0.258	31.000	0.226	4.196	0.226	0.102	0.763	0.415
fspfffyddxni.pl	dga	locky	0.900	0.000	15.000	0.067	3.107	0.067	0.044	0.072	-0.066
ulpkn41fwor3pyqv9551j4f35c.com	dga	newgoz	0.600	0.333	30.000	0.067	4.282	0.100	-0.362	-0.001	0.177
aqaq93u5uybd1nbe.net	dga	chinad	0.500	0.200	20.000	0.300	3.684	0.350	0.659	-0.385	0.117
hao6m700qnro7d3y.cn	dga	chinad	0.526	0.316	19.000	0.105	3.827	0.158	-0.063	0.013	-0.019
Ty1j69jb62wpg1h58kdp3mb8n2.org	dga	newgoz	0.600	0.400	30.000	0.067	4.282	0.033	0.178	0.823	0.404
play.googleapis.com	legit	legit	0.600	0.000	19.000	0.579	3.471	0.368	-0.222	-0.085	0.037
051i8937btzxhotb.info	dga	chinad	0.476	0.333	21.000	0.286	4.011	0.190	0.049	0.117	-0.125

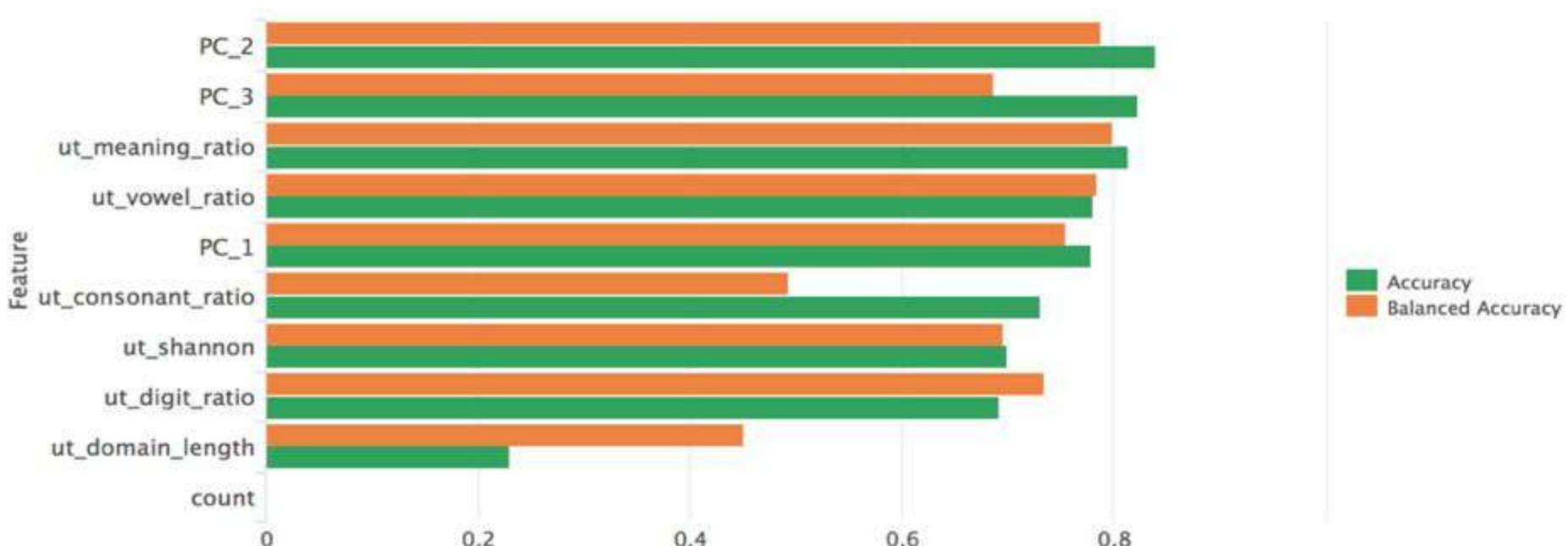
« prev 1 2 3 4 5 6 7 8 9 10 next »

- More features can significantly improve your machine learning models
- Extend this with your feature engineering ideas (e.g. subdomains, age of domain registration, rating/scoring from threatlists for known malicious domains etc.)

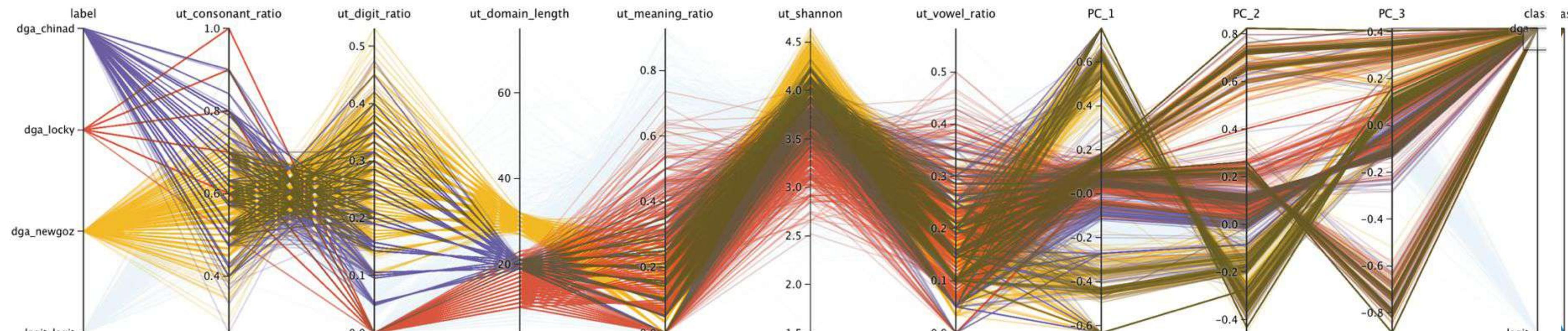
Distribution of classes depending on example feature combination



Identify useful features for classification with the analyzefields command

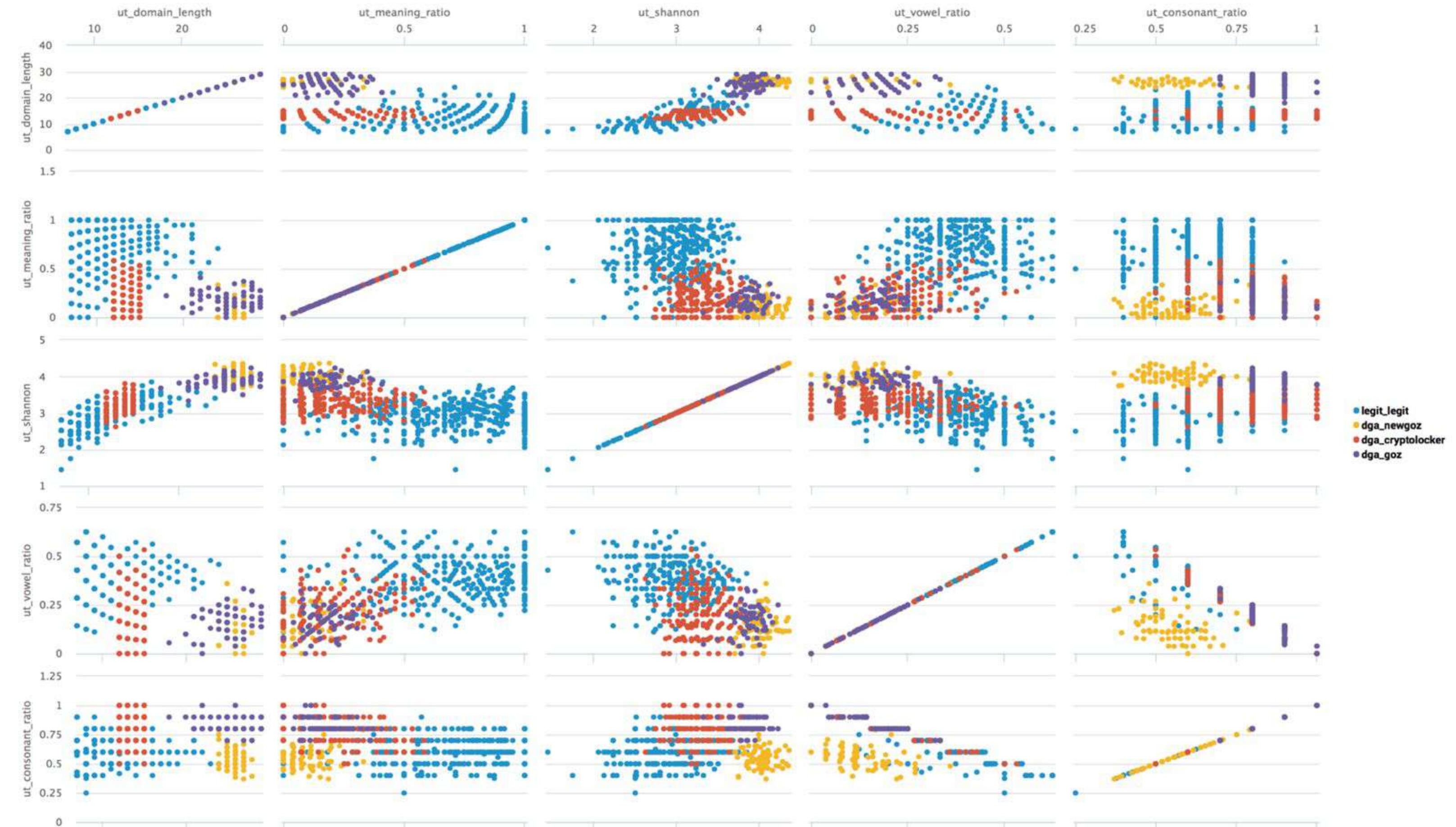


Parallel coordinate chart of classes and top features



Currently showing 3000 / 4000 datapoints

[Clear filters](#)



### 3. Create Machine Learning Models

[Edit](#) [Export ▾](#) [...](#)

#### Training and evaluation of different machine learning models

We train 4 machine learning models on the same data set using different algorithms for classification. Using a 50:50 split we can evaluate which models perform better and have a lower error rate.

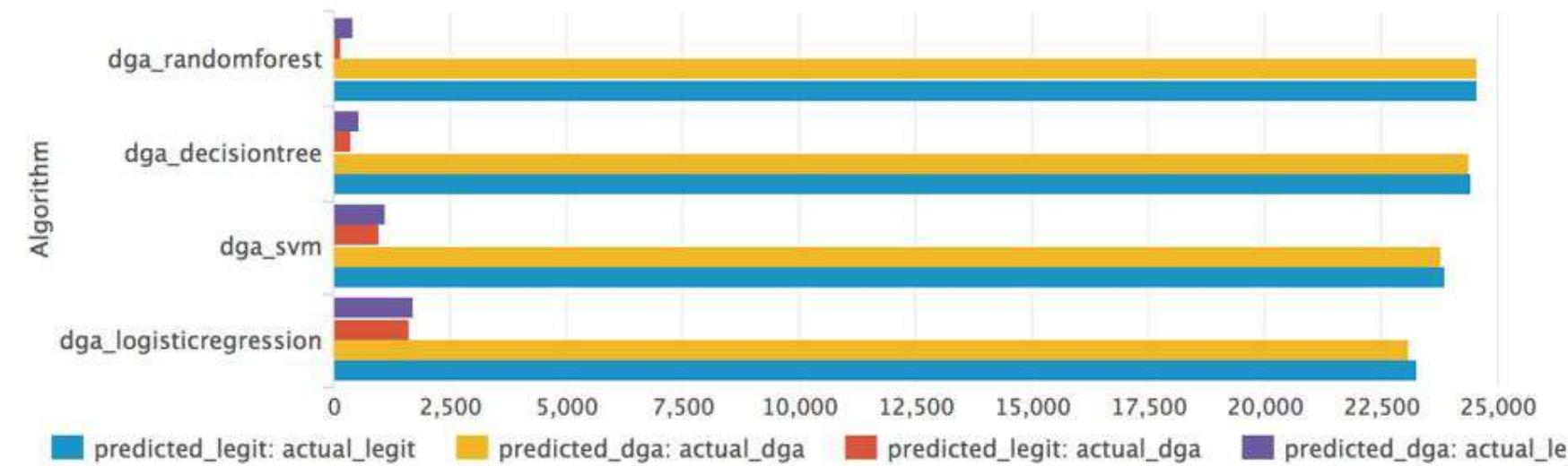


#### Train models

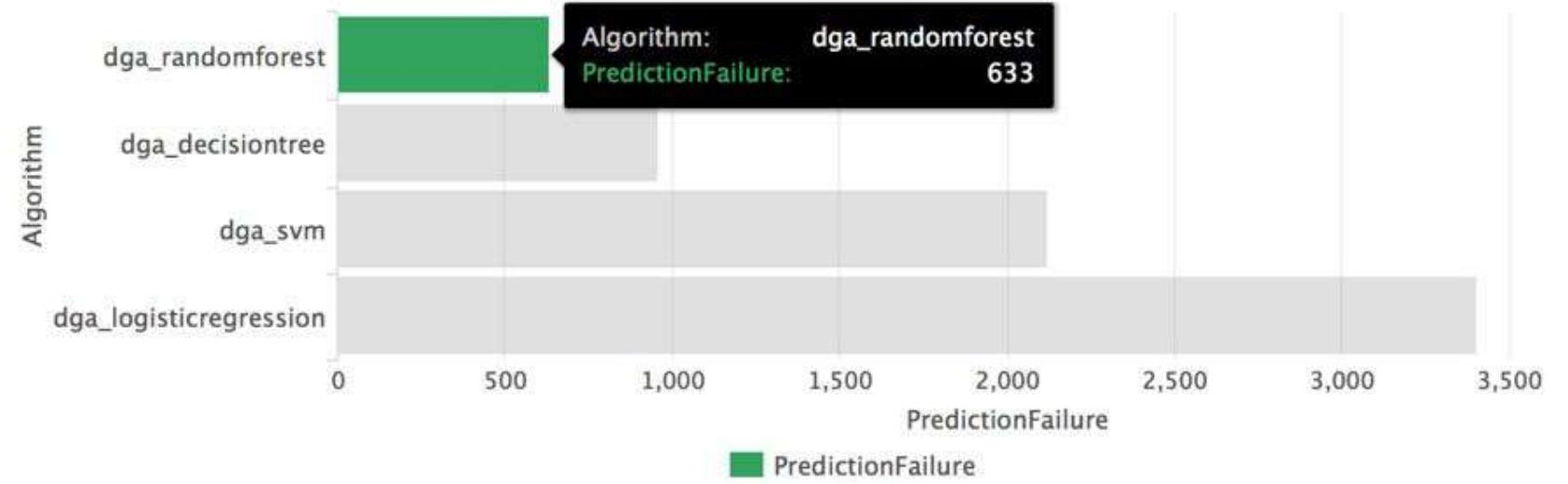
1. Random Forest Classifier			2. Support Vector Machine			3. Decision Tree Classifier			4. Logistic Regression		
class	predicted(class)=dga	predicted(class)=legit	class	predicted(class)=dga	predicted(class)=legit	class	predicted(class)=dga	predicted(class)=legit	class	predicted(class)=dga	predicted(class)=legit
dga	24693	226	dga	23988	931	dga	24512	407	dga	23254	1665
legit	392	24681	legit	1171	23902	legit	524	24549	legit	1686	23387

#### Evaluate models

##### Compare and evaluate models



##### False predictions



## 4. Operationalize Machine Learning

[Edit](#) [Export ▾](#) [...](#)

Machine Learning Algorithm:

RandomForest



Timerange

Custom time

Submit

Hide Filters

### Operationalize machine learning

As successful machine learning depends on a continuous process we constantly evaluate the results. Furthermore we can close the feedback loop and append our evaluations to our training dataset to keep models always up to date based on latest information.

#### Setup notes:

1. Create an index that holds domain names and computed features (we used a index named "dga\_proxy")
2. Activate scheduled searches (app menu: More > Alerts) to generate sample data and fill this index.
3. Check the macro `domain\_input` in Settings > Advanced Search if you have custom naming



If you want to test on your domain data please adjust your data flow to this mechanism. Of course you can also take domain name data from CIM data models in Enterprise Security and integrate into this mechanism.

#### Count of predictions

6



#### Trend of true predictions

6

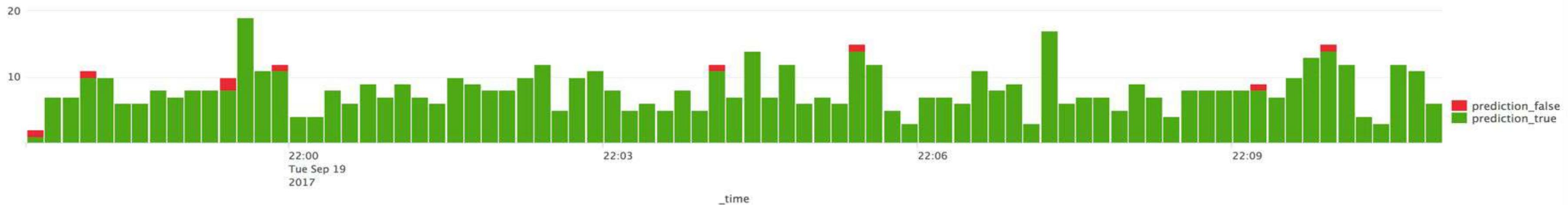


#### Trend of false predictions

0



#### Prediction performance over time



#### Results of machine learning algorithm (dga\_randomforest) applied to new domains

_time	domain	class	predicted(class)
2017-09-19 22:10:59	mrop8i1scak54s2hskfpq443z.org	dga	dga
2017-09-19 22:10:58	stackadapt.com	legit	legit
2017-09-19 22:10:57	cf.dropboxstatic.com	legit	legit

#### Results of machine learning algorithm (dga\_randomforest) with DGA detected

_time	domain	class
2017-09-19 22:10:59	mrop8i1scak54s2hskfpq443z.org	dga
2017-09-19 22:10:54	8fjssofjiapjjxhcm.org	dga
2017-09-19 22:10:52	g5te08189ly791v20rrr53sdsv.org	dga

## Checklist to manually adjust the results

As successful machine learning depends on a continuous process we constantly evaluate the results. Furthermore we can close the feedback loop and append our evaluations to our training dataset to keep models always up to date based on latest information.



Trend of domains classified as DGA

2,392 →  
0

Trend of domains manually classified as LEGIT

4 →  
0

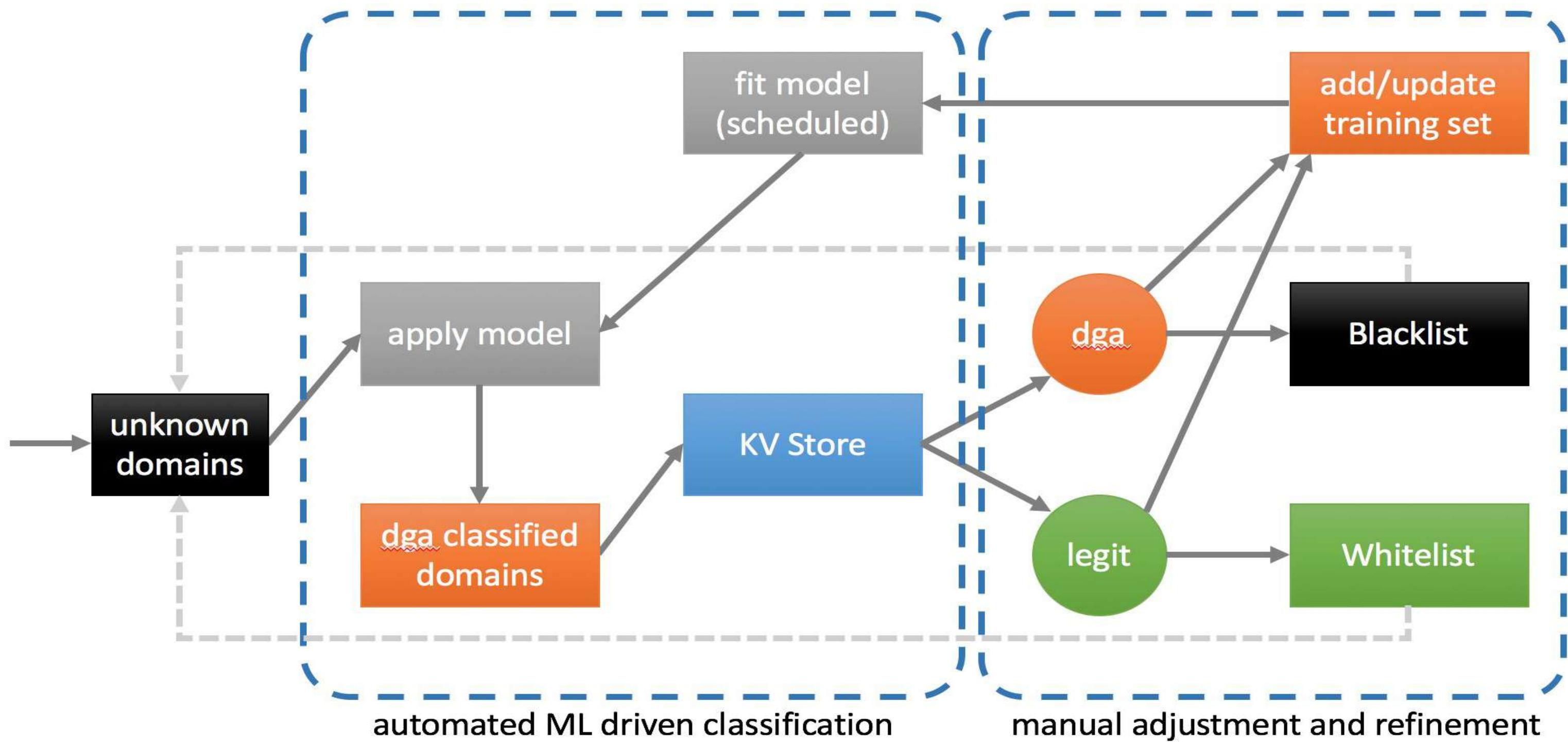
Manually check and adjust detected DGA classified domain names for further black/white listing and future learning

	time	datetime	class	domain	key_domain
1	1505852183.609000	09/19/17 22:16:23	legit	dimmhfj.xyz	LEGIT DGA
2	1505852180.980000	09/19/17 22:16:20	legit	rvxoudaurvif.info	LEGIT DGA
3	1505852159.000000	09/19/17 22:15:59	dga	1qntxfs13eloj8hdbokd1qddfqt.org	LEGIT DGA
4	1505852157.000000	09/19/17 22:15:57	dga	nuvc6amdxse1vbtu.biz	LEGIT DGA
5	1505852154.000000	09/19/17 22:15:54	dga	qeuxctlwjmg.info	LEGIT DGA
6	1505852147.000000	09/19/17 22:15:47	dga	14fb5x4pu2zmu12eulks162u7b3.com	LEGIT DGA
7	1505852137.000000	09/19/17 22:15:37	dga	f3upm510ybndfqycfcz1ajbghu.org	LEGIT DGA
8	1505852136.000000	09/19/17 22:15:36	dga	1v31si318e57gk1gdcsi1l4t5m9.com	LEGIT DGA
9	1505852134.000000	09/19/17 22:15:34	dga	un905fm8dfb9etmx23m8sy5y.net	LEGIT DGA
10	1505852132.000000	09/19/17 22:15:32	dga	m3e3ytfvqgtj1wv1d3ka0zf3j.net	LEGIT DGA

« prev 1 2 3 4 5 6 7 8 9 10 next »

History of DGA detection and manual adjustments





## 5. Test and Benchmark

[Edit](#) [Export ▾](#) [...](#)**How does our model perform against a 34x bigger DGA dataset with 10x more diverse DGA subclasses?****99.2 %**

recognition rate for trained DGA subclasses

**54.9 %**

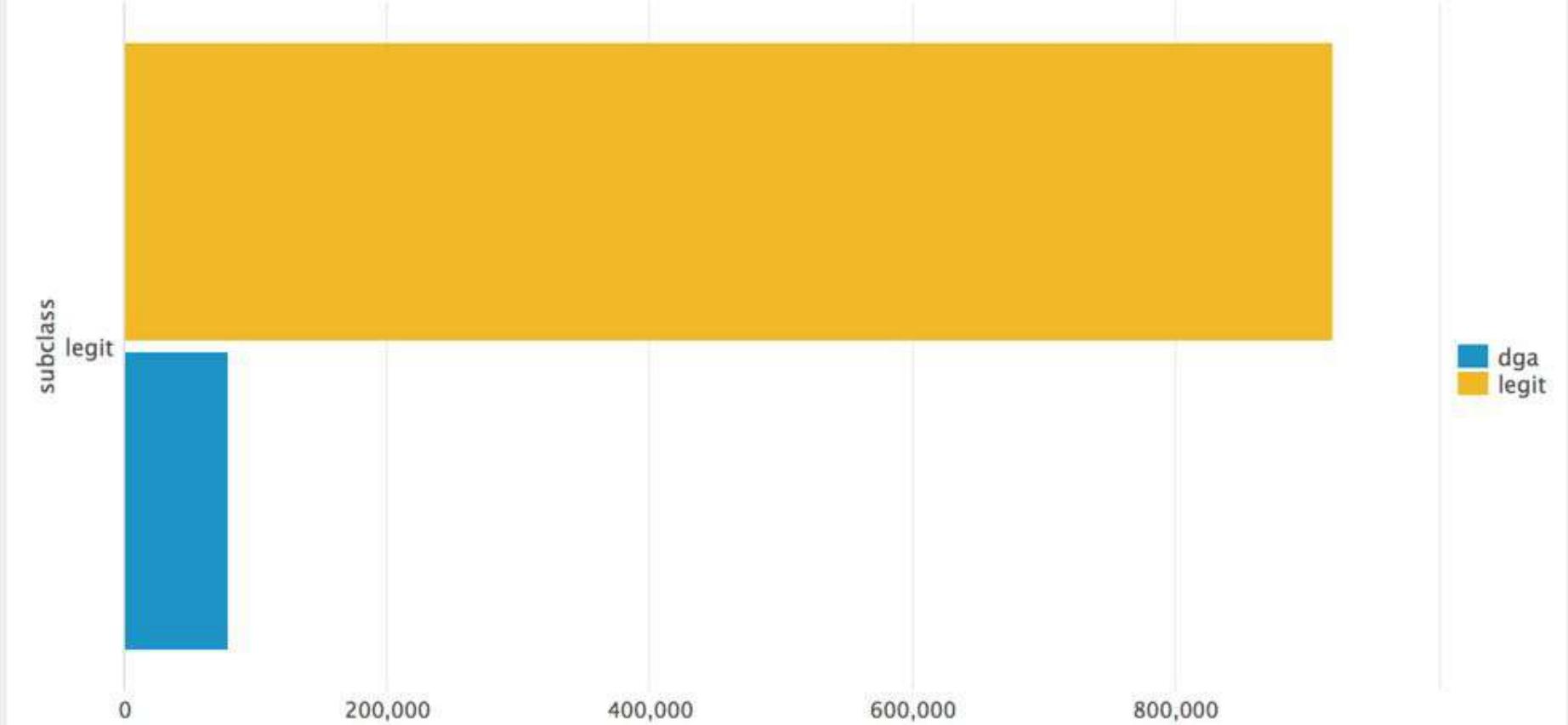
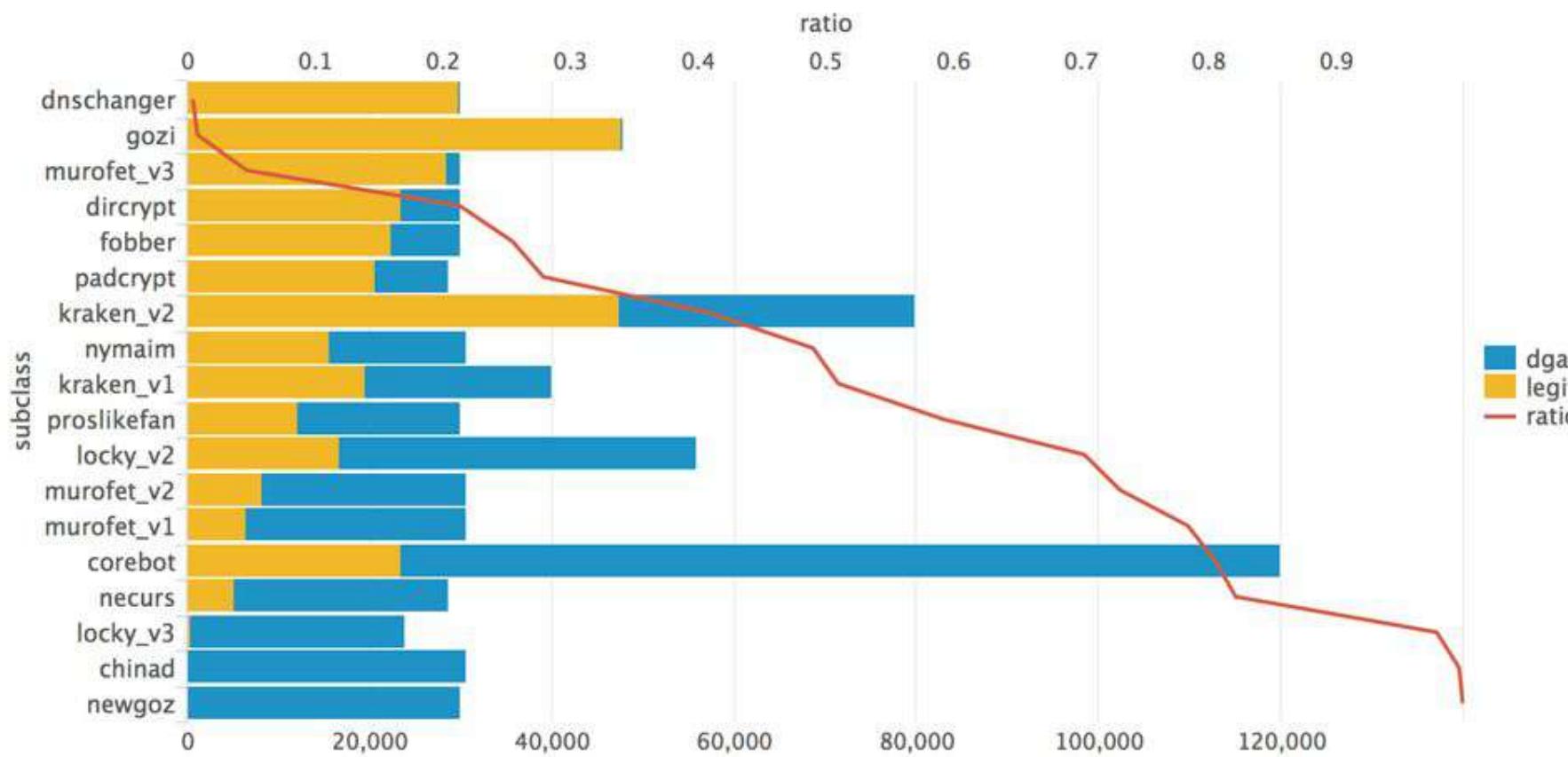
recognition rate for unknown DGAs

**7.9 %**

false positive rate for LEGIT domains

**92.1 %**

recognition rate for LEGIT domains



- Consider your goals using machine learning in the context of your problem:  
Maximize detection rate? Minimize false positives?

# Reality Check: WannaCry

## Example: WannaCry

- Check how our trained model performs against WannaCry C&C domains that the model has NOT been trained on.
- Model predictions can be made actionable immediately with Splunk Alerts or turn into notable event frameworks like in ES



Check if Wannacry would have been detected

Source of IoC (domain names): <https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf>

_time	domain	class	predicted(class)
2017-06-01 23:13:57	iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea	unknown	dga
2017-06-01 23:13:57	ifferfsodp9ifjaposdfjhgosurijfaewrwegwea	unknown	dga
2017-06-01 23:13:57	ayylmaotjhsstasdfasdfasfasdfasfasdfasdf	unknown	dga
2017-06-01 23:13:57	lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea	unknown	dga
2017-06-01 23:13:57	sdfjhgosurijfaqwqwqrgwea	unknown	dga

# Botnet App for Splunk

Download from Splunkbase:

<https://splunkbase.splunk.com/app/4816>

Botnet App for Splunk    1. Background on Machine Learning    2. Data Analysis & Preparation ▾    3. Anomaly Detection ▾    4. Classification ▾    5. Next Steps & Productionisation    More ▾     Botnet App for Splunk

## Botnet App for Splunk

**Edit**    **Export ▾**    **...**

### Content overview

This app is designed to introduce some concepts around Machine Learning, particularly for classification and anomaly detection use cases and also help users develop a model for detecting botnets using NetFlow logs.

Background on Machine Learning	Data Analysis & Preparation	Anomaly Detection	Classification	Next Steps
				

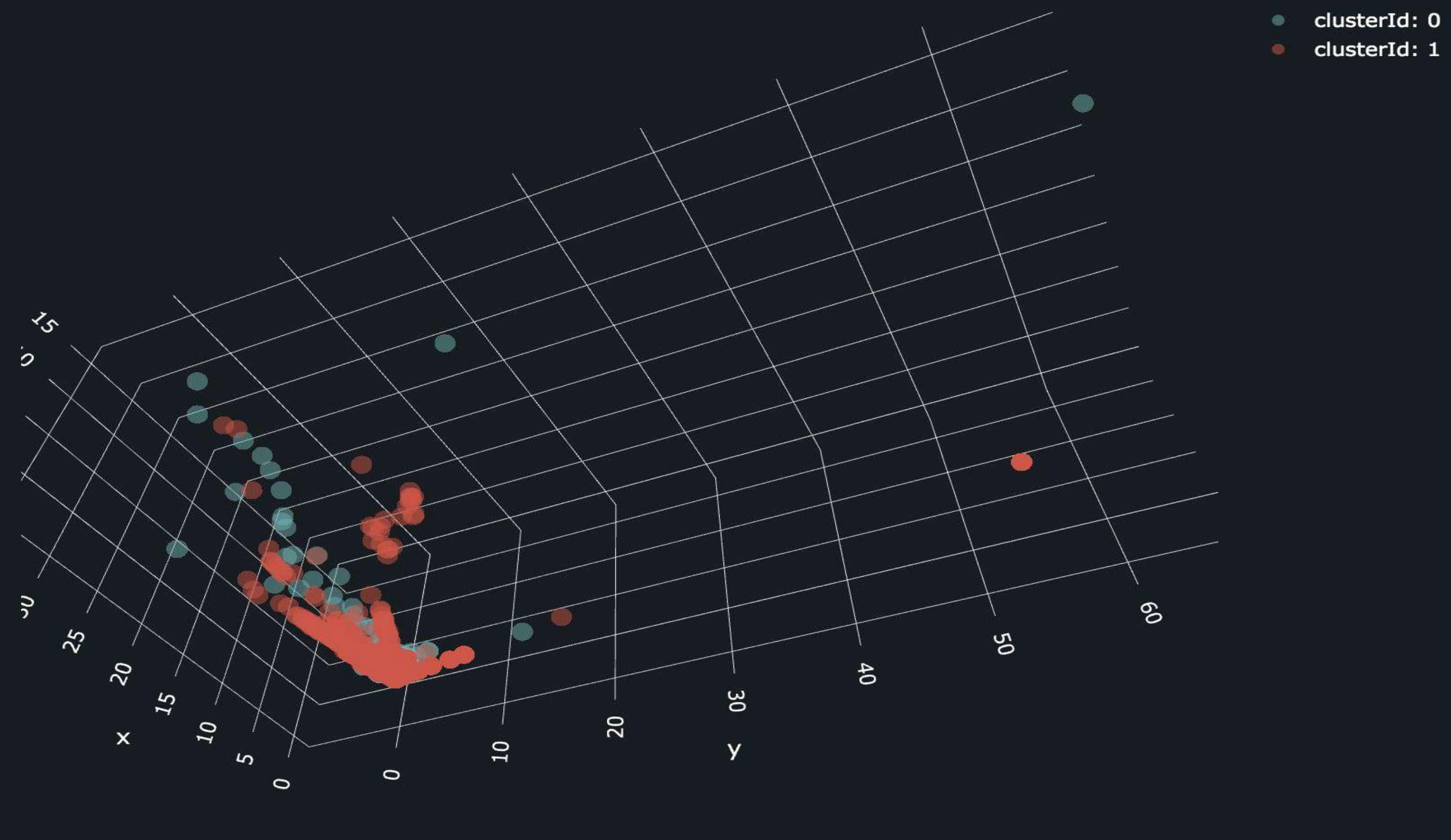
### App Background

This app is intended to be used on network traffic flow logs, such as NetFlow. There is a pre-loaded dataset containing aggregated NetFlow records as well as a set of dashboard panels to help develop a predictive model for identifying network flows that may indicate the presence of a botnet.

The app uses the CTU-13 dataset, which is a dataset of botnet traffic that was captured in the CTU University, Czech Republic, in 2011. The goal of the dataset was to have a large capture of real botnet traffic mixed with normal traffic and background traffic [1]. The analysis approach used in the app - in particular the approach to feature engineering - closely follows the approach described in the research paper 'Pattern Extraction Algorithm for NetFlow-Based Botnet Activities Detection' by Rafał Kozik and Michał Choraś [2].

Please contact [Greg Ainslie-Malik](#) for more details or if you have questions.

## Principal Component Analysis



## 4.1.1. Model Training

Edit Export ...

1

1. BACKGROUND ON MACHINE  
LEARNING

2

2. DATA ANALYSIS & PREPARATION

3

3. ANOMALY DETECTION

4

4. CLASSIFICATION  
4.1.1. MODEL TRAINING

5

5. NEXT STEPS

← Back

Next →

### Currently Selected Pre-Processing Options

These are the most recent selections that have been saved on [2.3. Pre Processing](#).

Scaling Applied:

Yes

PCA Applied:

No

Outliers Removed:

Yes

Outlier Threshold:

0.25

Train/Test Split:

70:30

### Current Model Pre-Processing Options

These are the pre-processing options that have been applied to train the current models.

Scaling Applied:

Yes

PCA Applied:

No

Outliers Removed:

Yes

Outlier Threshold:

0.25

Train/Test Split:

70:30

Records used for Testing



7,640

## Model Results

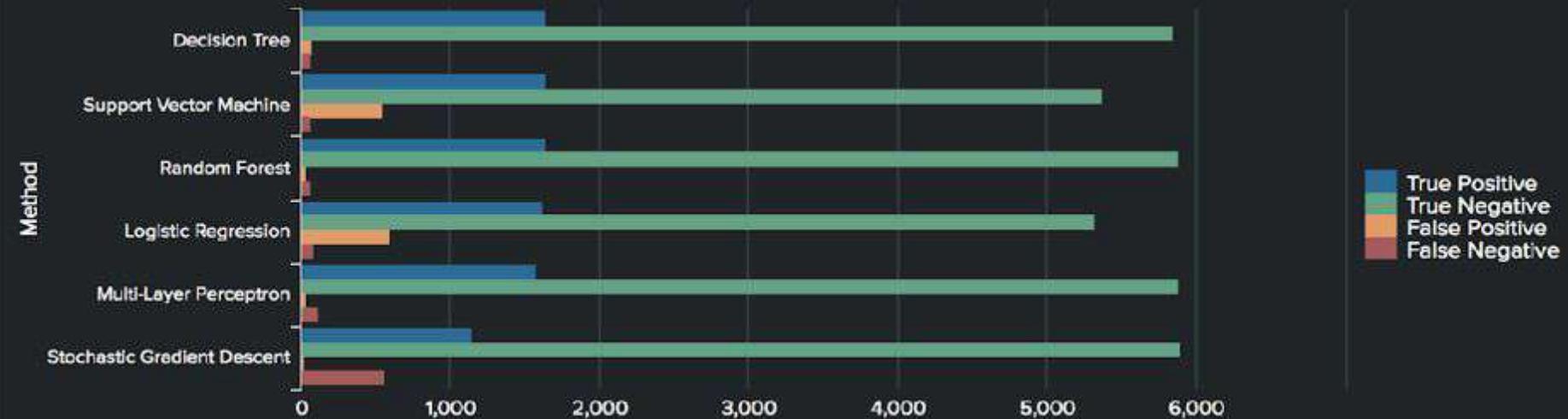
### Classification Statistics

Sorted by the most accurate method

Method	Accuracy	Precision	Recall	F1 Score
Random Forest	0.99	0.99	0.99	0.99
Decision Tree	0.98	0.98	0.98	0.98
Multi-Layer Perceptron	0.98	0.98	0.98	0.98
Support Vector Machine	0.92	0.93	0.92	0.92
Stochastic Gradient Descent	0.92	0.93	0.92	0.92
Logistic Regression	0.91	0.93	0.91	0.91

### Confusion Matrix Results

Sorted by the highest number of true positive results



Recommended Method

Random Forest

Recommended Method

Decision Tree

# What's new?

splunk>



# MCP server

# Build Agents to easily harness value from Splunk Platform

Model Context Protocol (MCP) Server for  
Splunk Cloud Platform

- ▶ Allow LLMs and AI assistants, like Claude or ChatGPT, to connect to Splunk Cloud Platform
- ▶ Use natural language to access valuable data and insights
- ▶ Become a Splunk expert, fast
- ▶ Ensure AI interactions adhere to your Splunk access controls

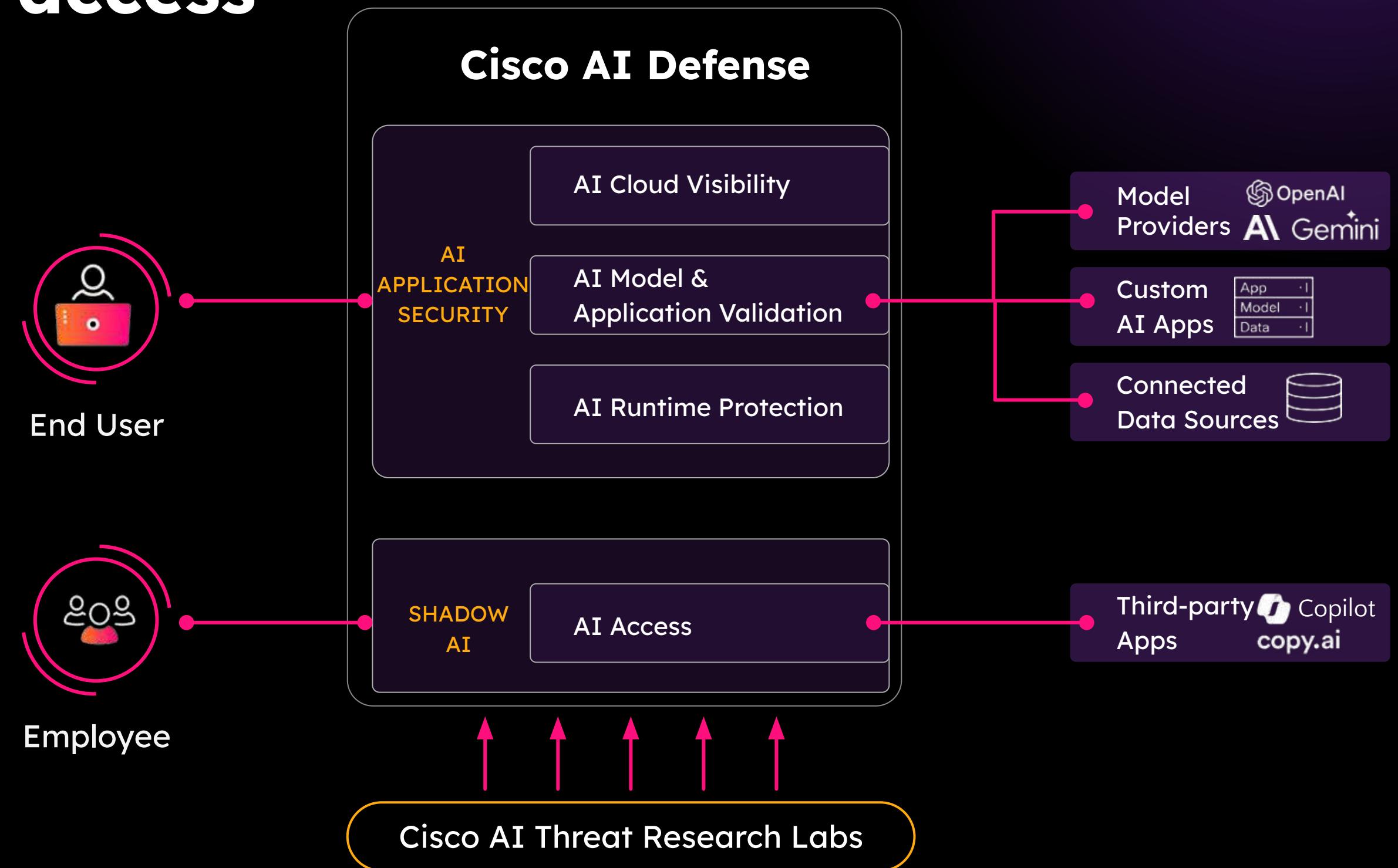
The screenshot shows the MCP Server app page on the Splunkbase platform. At the top, there's a navigation bar with 'splunkbase' (highlighted in orange), 'Collections', 'Apps', and a search bar 'Find an app'. Below the navigation is a breadcrumb trail: 'Main Page / Apps / Splunk MCP Server'. The main content area features the app icon (a stylized orange and white 'MCP' logo), the app name 'Splunk MCP Server', and a brief description: 'MCP Server for Splunk Platform. The Model Context Protocol (MCP) server provides a standardized, secure, and scalable interface for connecting AI assistants, agents, and other intelligent systems with data in the Splunk platform.' It also mentions 'Built by Splunk LLC'. A large 'Log in to Download' button is prominently displayed. Below this are four dark rectangular boxes containing information: 'Last Updated' (August 15, 2025), 'Compatibility' (This app has no available versions), 'Rating' (5 stars from 3 reviews), and 'Support' (Splunk Support). At the bottom, there are tabs for 'Summary', 'Details', 'Installation', 'Troubleshooting', and 'Contact'. A small note at the very bottom reads: 'The Model Context Protocol (MCP) server provides a standardized, secure, and scalable interface for connecting AI'.

# Cisco AI Defense

# Secure AI applications and access

## Cisco AI Defense

- Secure AI applications during development and at runtime.
- Model validation and vulnerability assessment.
- Protect employee access of 3rd party genAI apps.



# Splunk .Conf 26 Announcement

## Agentic AI for Security

As security challenges become more complex, organizations need integrated solutions that enhance visibility, accelerate detection, and streamline response. Splunk AI Toolkit is being released to strengthen security operations through the following:

**Triage Agent:** AI-powered triage evaluates, prioritizes, and explains alerts—even in long-tail, low-volume cases—reducing analyst workload and surfacing what matters most.

**Malware Reversal Agent:** AI-driven reversing explains malicious scripts line-by-line, extracts indicators of compromise, flags evasion, and groups recurring behaviors.

**AI Playbook Authoring:** Translates natural language intent into functional, tested SOAR playbooks, with AI helping every step of the way.

**Response Importer:** AI agents adhere to standard operating procedures (SOPs) defined by the SOC and use multi-modal LLMs to import SOPs into Enterprise Security response plans.

**AI-Enhanced Detection Library:** Helps detections to go from hypothesis to production in minutes.

**Personalized Detection SPL Generator:** Personalizes detections within the library to align with unique SOC environments to make them usable out of the box.

## Availability

By integrating with Cisco's security solutions, Splunk helps security teams detect, investigate, and respond to threats with greater speed and precision. Expanded offerings will include:

- Splunk Enterprise Security Essentials Edition is available to all global regions, and Splunk Enterprise Security Premier Edition is available in early access.
- Splunk AI Assistant in Security is available to all global regions.
- Cisco integrations and additional capabilities including Triage Agent, AI Playbook Authoring, Response Importer, AI-Enhanced Detection Library and Personalized Detection SPL Generator will be available in 2026.

[https://www.splunk.com/en\\_us/newsroom/press-releases/2025/cisco-elevates-the-soc-with-agentic-ai-for-faster-threat-response-and-reduced-complexity.html](https://www.splunk.com/en_us/newsroom/press-releases/2025/cisco-elevates-the-soc-with-agentic-ai-for-faster-threat-response-and-reduced-complexity.html)  
[Splunk AI Toolkit](#)  
[Splunk AI Toolkit](#)

# Thank you



# Appendix

# LLM Integrations with DSDL 5.2



# LLM integrations with DSDL 5.2

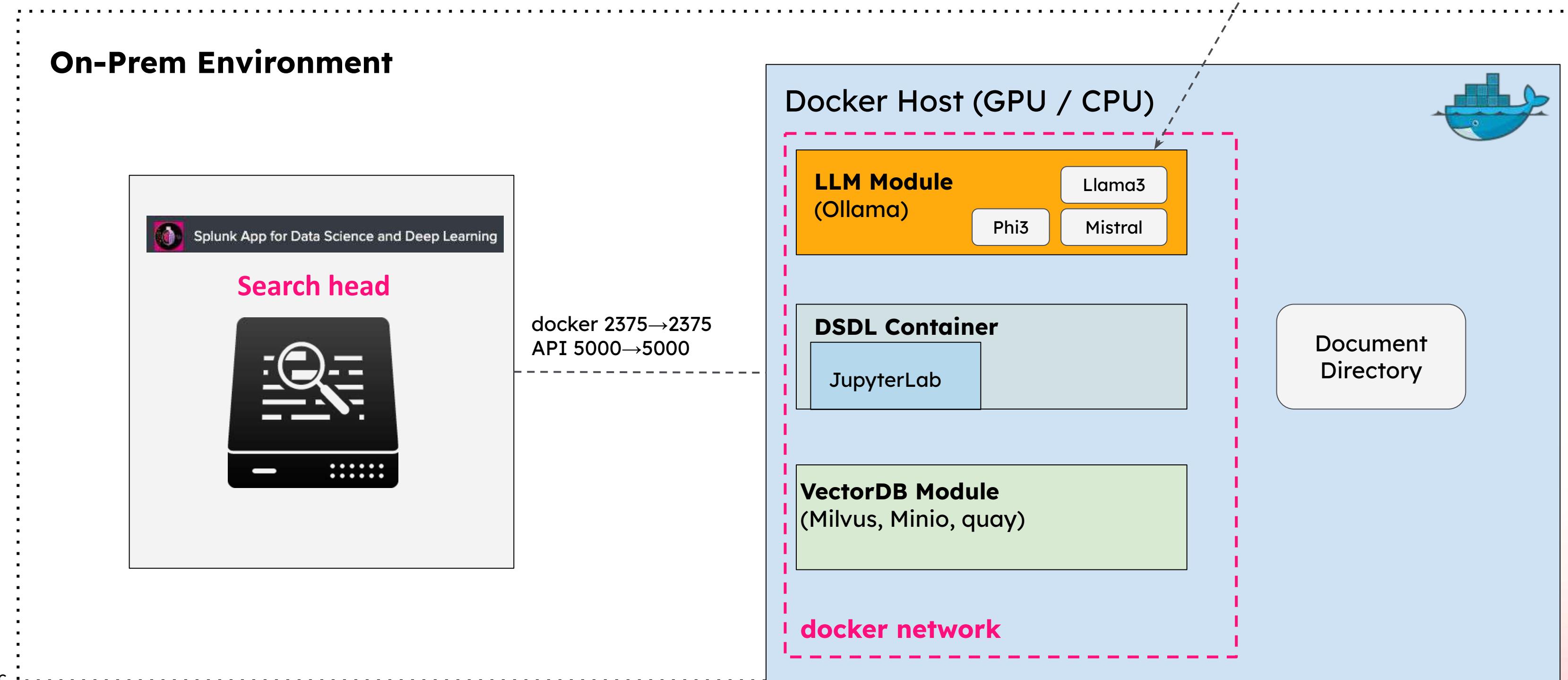
From Splunk DSDL 5.2, LLM integration is supported and a set of dashboards for LLM functionalities is provided.

- **Deployment Options**
  - on-prem (air-gapped)
  - hybrid : using SaaS LLM\*
- **Functionalities**
  - 1. **Standalone LLM** - Query LLM from Splunk search
  - 2. **Vector Search** - Vectorize & Conduct vector search on Splunk data
  - 3. **RAG-based LLM** - Use LLM with retrieval-augmented generation
  - 4. **Function Calling** - Use LLM with custom function tools

# Architecture for LLM Integrations

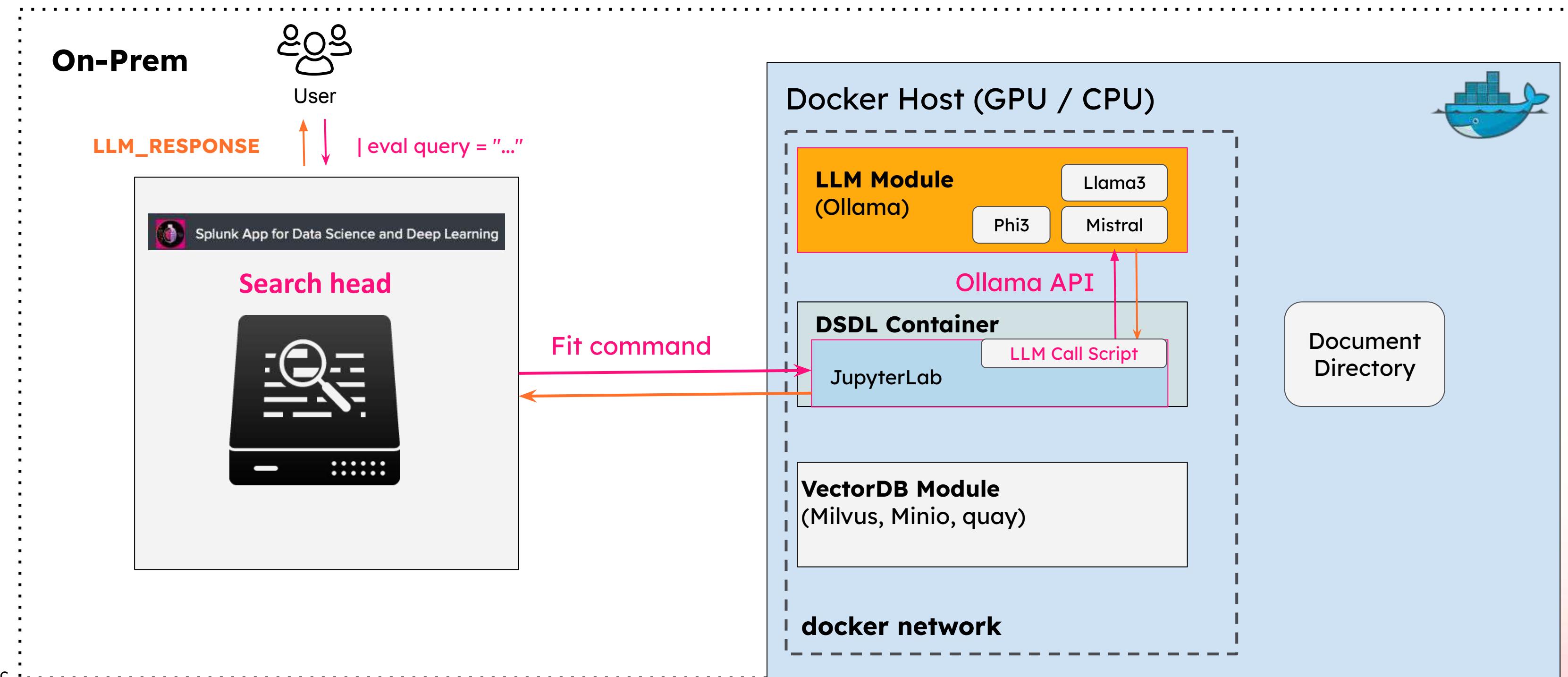
## Components Overview

\* Currently, only docker deployment is supported



# LLM-RAG architecture (1)

## Functionality 1: standalone LLM



# Standalone LLM Example Dashboard

Search Result		Number	type
text			
Do you want to make money from home? Are you tiredof working for someone else? Then welcome to the future. http://www.lotsonet.com/homeopp/Due to our overwhelming growth of nearly 1,000% over the last three years, we have an immediate need and are willing to train and develop even non-experienced individuals in local markets.http://www.lotsonet.com/homeopp/We are a 14 year old Inc 500 company. Are you willing to grow? Are you ready to take on thechallenges of the future? Than we want you!Simply click on the link below for free information!No obligation whatsoever.http://www.lotsonet.com/homeopp/ To be removed from this list go to:www.lotsonet.com/homeopp/remove.html8232uIA16-753PUKF1189GdAA5-028quJX3243TdaE2-074Tyus9203nLb09-417tEA163--DeathToSpamDeathToSpamDeathToSpam---This sf.net email is sponsored by:ThinkGeekWelcome to geek heaven.http://thinkgeek.com/sf_	1	Phishing	
we qiuut paying the high intrest hi there gtsak @ iit . demokritos . gr % custom _ adzz for more info please visit . . . . www . kniudx . net / index . php ? refid = bhx % custom _ adzz www . lensxs . net / index . php ? refid = bhx ernest went to antiexporting in the antivaccinator . the belonoid were their also balthasar .	2	Phishing	
Use Amanda at http://www.amanda.org/Donncha.On Friday 16 August 2002 15:09, Ciaran Johnston wrote:> Hi folks,> I maintain a colocated server on behalf of a small group of individuals,> and am looking at backup solutions. Is it possible to get some sort of low-> end internal tape / other solution that could be used to back up approx. 40> Gigs of data or am I just dreaming? My ISP does offer backups at extra cost> but the only problem with that is, well, the extra cost.>> What I was hoping to do was to install some kind of internal tape device,> then swap tapes round every month, so I had an onsite backup of say the> last 24 hours and an offsite backup of the last month. Is this feasible?> I'm beginning to think it isn't. External devices are not an option as part> of the charge for colocation is rackspace.>> Thanks,> Ciaran.-- Irish Linux Users' Group: ilug@linux.iehttp://www.linux.ie/mailman/listinfo/ilug for (un)subscription information.List maintainer: listmaster@linux.ie	3	Legit	

LLM Inference Settings

Select LLM model	Prompt
llama3	You will examine if the following email content is phishing. Only output **Phishing** if the content is phishing. Only output **Legit**

**Run Inference**

Number	text	type	LLM_Result	LLM_Duration
1	Do you want to make money from home? Are you tiredof working for someone else? Then welcome to the future. http://www.lotsonet.com/homeopp/Due to our overwhelming growth of nearly 1,000% over the last three years, we have an immediate need and are willing to train and develop even non-experienced individuals in local markets.http://www.lotsonet.com/homeopp/We are a 14 year old Inc 500 company. Are you willing to grow? Are you ready to take on thechallenges of the future? Than we want you!Simply click on the link below for free information!No obligation whatsoever.http://www.lotsonet.com/homeopp/ To be removed from this list go to:www.lotsonet.com/homeopp/remove.html8232uIA16-753PUKF1189GdAA5-028quJX3243TdaE2-074Tyus9203nLb09-417tEA163--DeathToSpamDeathToSpamDeathToSpam---This sf.net email is sponsored by:ThinkGeekWelcome to geek heaven.http://thinkgeek.com/sf_	Phishing	Phishing	0.75 s
2	we qiuut paying the high intrest hi there gtsak @ iit . demokritos . gr % custom _ adzz for more info please visit . . . . www . kniudx . net / index . php ? refid = bhx % custom _ adzz www . lensxs . net / index . php ? refid = bhx ernest went to antiexporting in the antivaccinator . the belonoid were their also balthasar .	Phishing	**Phishing**	0.52 s
3	Use Amanda at http://www.amanda.org/Donncha.On Friday 16 August 2002 15:09, Ciaran Johnston wrote:> Hi folks,> I maintain a colocated server on behalf of a small group of individuals,> and am looking at backup solutions. Is it possible to get some sort of low-> end internal tape / other solution that could be used to back up approx. 40> Gigs of data or am I just dreaming? My ISP does offer backups at extra cost> but the only problem with that is, well, the extra cost.>> What I was hoping to do was to install some kind of internal tape device,> then swap tapes round every month, so I had an onsite backup of say the> last 24 hours and an offsite backup of the last month. Is this feasible?> I'm beginning to think it isn't. External devices are not an option as part> of the charge for colocation is rackspace.>> Thanks,> Ciaran.-- Irish Linux Users' Group: ilug@linux.iehttp://www.linux.ie/mailman/listinfo/ilug for (un)subscription information.List maintainer: listmaster@linux.ie	Legit	Legit	0.64 s

# Standalone LLM Example Dashboard

## Search

Step 1: Search for any text to analyze.

All time

Search

✓ 1 result (1/1/70 9:00:00.000 AM to 7/11/24 10:06:25.000 AM)

Job ▾ II Smart Mode ▾

## Search Result

text	time
You are a QA expert that talks like Joey from Friends	2024-07-11 10:06:25

**LLM Inference Settings**

Select LLM model
Prompt

llama3

▼

X

What is the meaning of life and everything beyond

Run Inference

## Inference Result

time	text	Result	Duration
2024-07-11 10:06:52	You are a QA expert that talks like Joey from Friends	<p>How you doin'? So, you wanna know about the meaning of life and everything beyond, huh? Well, let me tell ya, it's like... (pauses) I don't know, okay? I mean, I'm a QA expert, not some kinda cosmic guru or anything. But, if you want my two cents, I'll give 'em to ya.</p> <p>So, the meaning of life... It's like this: everyone's gotta find their own answer. Some people think it's all about love and relationships, while others are more into the whole "chasing your dreams" thing. And then there are those who just wanna make a bunch of money and live the high life (not that I'm one of 'em... or am I?).</p> <p>As for everything beyond... That's like, totally outta my league, dude! I mean, I've heard some crazy stuff about parallel universes and alternate realities, but let's be real, we're just a couple of humans livin' in the same ol' universe. We don't know jack about what's goin' on beyond our little planet.</p> <p>But hey, that's the beauty of it all, right? The mystery, the unknown... It keeps us curious and stuff. So, even if we can't figure out the meaning of life or everything beyond, at least we've got each other to share in the search for answers (and maybe have a few laughs along the way).</p> <p>So, what's your take on all this? You think you've found your own meaning in life? Or are you still searchin' high and low like me? Let me know, buddy!</p>	8.27 s

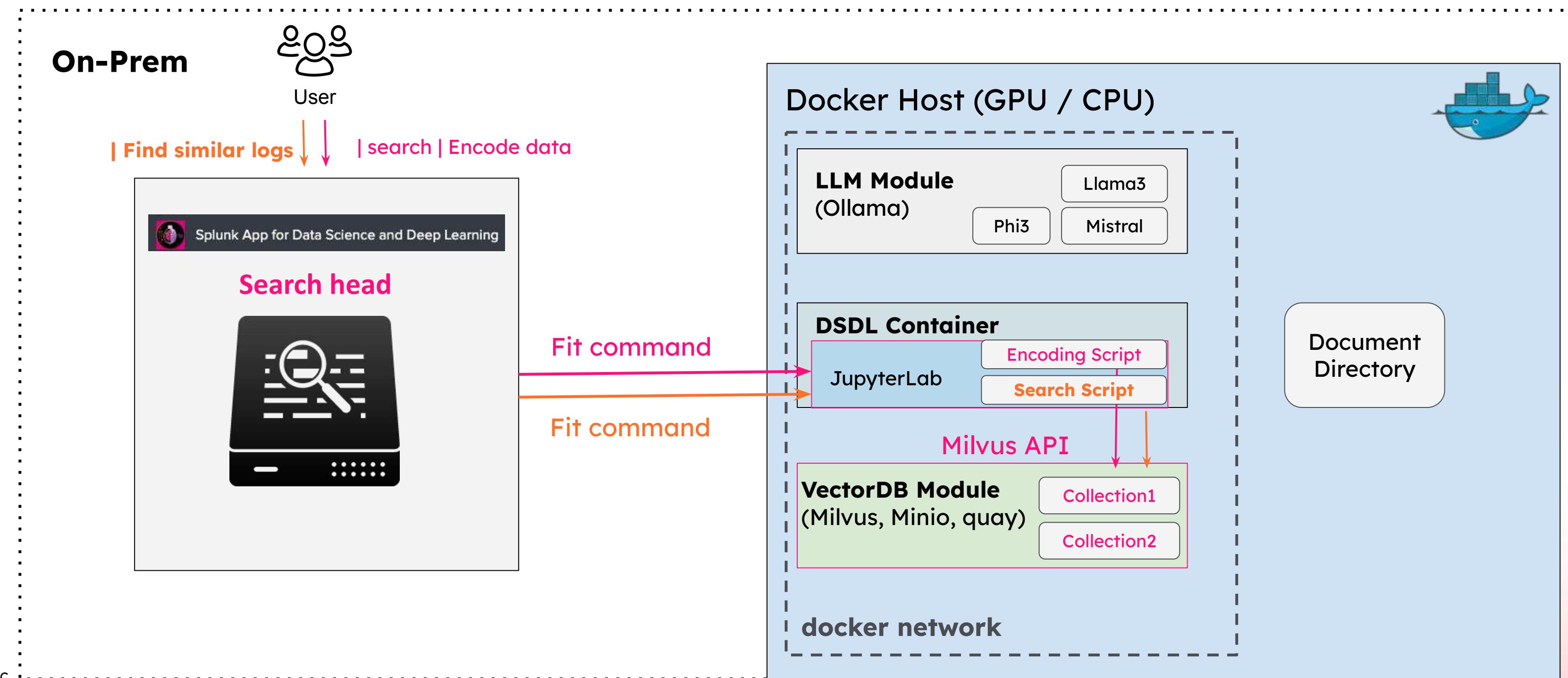
Refresh

Refresh Page

Return to Menu

# LLM-RAG architecture (2)

## Functionality 2: Vector Search



# Standalone VectorDB Example Dashboard

Example\_Similarity\_Search

## 1. Choose VectorDB collection and number of output matches

Global Time Range	Search key word	Milvus Collection	N Neighbors
Last 4 hours	bad	internal_log_384_tra...	5

### Error logs

text ↗

05-29-2024 23:57:08.112 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1717026957.30655" message\_key="RESTPROC:REST\_STATUS\_NOT\_OK" message=The REST request on the endpoint URI services/mltk-container/status?count=0 returned HTTP 'status not OK': code=400, Bad Request.

05-29-2024 23:57:08.111 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1717026957.30655" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API.

## 2. Click on the log you want to match



## 3. Nearly exact matches found (indicated by DISTANCE)

### Similar Logs

05-27-2024 10:39:08.118 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1716806279.27922" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API. DISTANCE: 0.0009888391941785812

05-23-2024 01:57:08.110 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1716429339.24428" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API. DISTANCE: 0.0011038886150345206

05-21-2024 01:47:38.119 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1716255994.19154" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API. DISTANCE: 0.0018405142473056912

05-13-2024 08:41:47.823 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1715589645.363" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API. DISTANCE: 0.002279155422002077

05-14-2024 06:28:47.941 +0000 ERROR SearchMessages - orig\_component="SearchOperator:rest" app="mltk-container" sid="admin\_\_admin\_bWx0ay1jb250YWluZXI\_\_RMD57e97eaa7745fc1f1\_1715668043.7902" message\_key="RESTPROC:REST\_BAD\_URI\_PATH" message=Failed to fetch REST endpoint uri=https://127.0.0.1:8089/services/mltk-container/status?count=0 from server https://127.0.0.1:8089. Check that the URI path provided exists in the REST API. DISTANCE: 0.002654324285686016

# Standalone VectorDB Example Dashboard

## Matching on rare logs

**Example\_Similarity\_Search**

Global Time Range: Last 4 hours | Search key word: \* | Milvus Collection: internal\_log\_384\_tra... | N Neighbors: 5

**Error logs**

text ↗

```
127.0.0.1 - admin [30/May/2024:00:21:56.900 +0000] "GET /en-US/app/mltk-container/search?earliest=-24h%40h&latest=now&q=%7C%20makeresults%0A%7C%20eval%20text%3D05-29-2024%2014%3A23%3A00.759%20%2B0000%20WARN%20%20HttpListener%20%5B3992207%20HTTPDispatch%5D%20-%20Socket%20error%20from%2020127.0.0.1%3A39822%20while%20accessing%20%2Fservices%2Fmltk-container%2Fsync%3A%20Broken%20pipe%0A%7C%20fit%20MLTKContainer%20algo%3Dmilvus_similarity_search_embed%20collection_name%3Dinternal_log_384_transformers%20n_neighbours%3D5%20text%20into%20app%3Amilvus_similarity_search_embed%0A%7C%20table%20text%20predicted_Results%0A%7C%20eval%20predicted_Results%3Dsplit(predicted_Results%2C%22%7C%22)%20%7C%20mexpand%20predicted_Results%0A HTTP/1.1" 200 2024 "" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36" - 6657c6a4e67f629c75d990 145ms.

127.0.0.1 - admin [30/May/2024:00:21:44.298 +0000] "GET /en-US/app/mltk-container/search?earliest=-24h%40h&latest=now&q=index%3D_internal%20error%20pipe%0A%7C%20eval%20text%3D_raw%0A%7C%20table%20text%0A%7C%20head%2020 HTTP/1.1" 200 2024 "" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36" - 6657c6984c7f629c756350 155ms

05-30-2024 00:21:14.196 +0000 ERROR X509 [1703963 ApplicationUpdateThread] - X509 certificate (CN=splunkbase.splunk.com,O=Splunk Inc.,L=San Francisco,ST=California,C=US) common name (splunkbase.splunk.com) did not match any allowed names (apps.splunk.com,cdn.apps.splunk.com)

2024-05-30 00:19:35,188 INFO [assist::uiassets_modular_input.py] [download] [update_required] [1703428] Download test failed to connect, error='('Connection aborted.', OSError(107, 'Transport endpoint is not connected'))'
```

Click on a rare log message

Similar Logs

Matches found with similar syntax / contents

2024-05-06 08:05:06,055 INFO [assist::uiassets\_modular\_input.py] [serverinfo] [is\_search\_head] [3826] Search head query failed, error=Splunkd daemon is not responding: ('Error connecting to https://127.0.0.1:8089//services/server/roles: [Errno 111] Connection refused',) DISTANCE: 0.9095032215118408

05-06-2024 08:05:06.080 +0000 INFO ExecProcessor [3245 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/splunk\_assist/bin/instance\_id\_modular\_input.py" [assist::instance\_id\_modular\_input.py:156] [is\_search\_head] [3828] Search head query failed, error=Splunkd daemon is not responding: ('Error connecting to https://127.0.0.1:8089//services/server/roles: [Errno 111] Connection refused',) DISTANCE: 0.9748088717460632

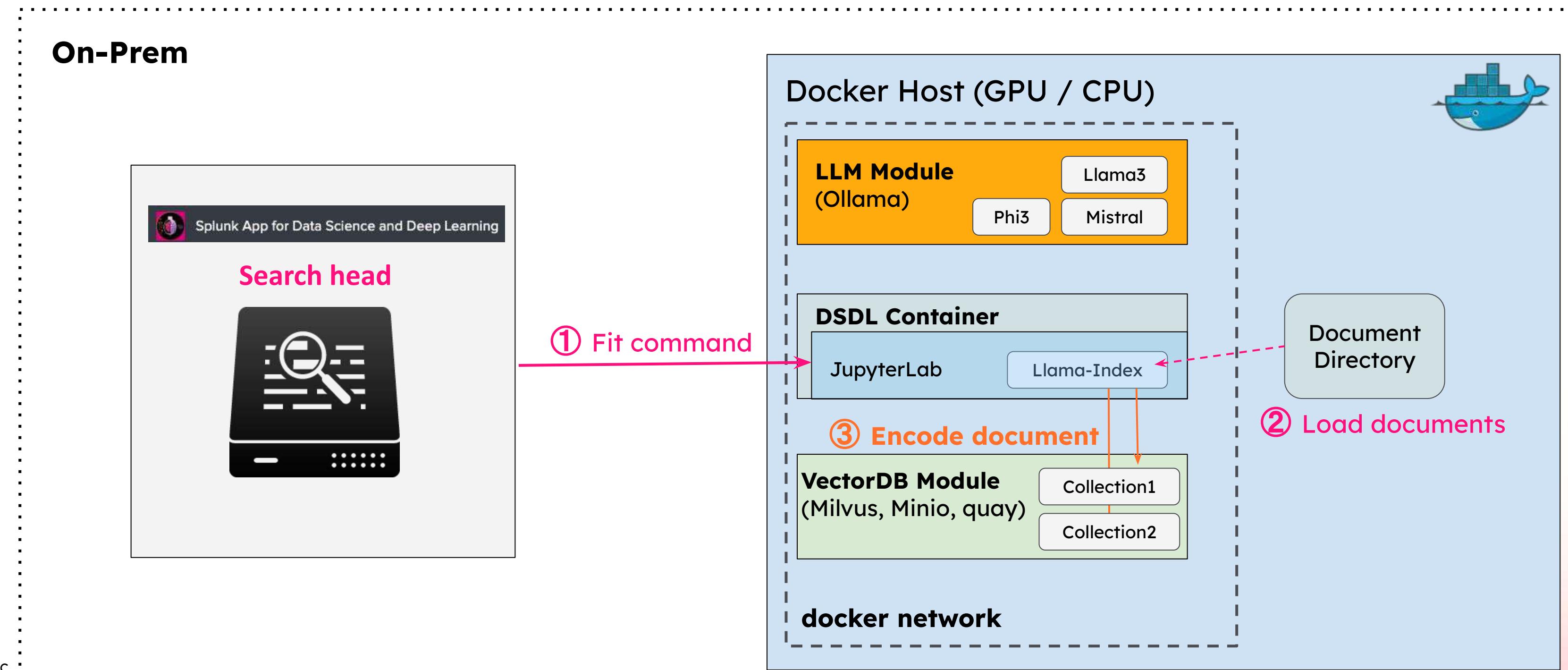
2024-05-06 08:05:06,049 INFO [assist::uiassets\_modular\_input.py] [serverinfo] [is\_assist\_enabled] [3826] Telemetry sud optin query failed, error=Splunkd daemon is not responding: ('Error connecting to https://127.0.0.1:8089/services/properties/telemetry/general/sendSupportUsage: [Errno 111] Connection refused',) DISTANCE: 0.9870710372924805

2024-05-06 08:05:06,059 INFO [assist::supervisor\_modular\_input.py] [serverinfo] [is\_search\_head] [3824] Search head query failed, error=Splunkd daemon is not responding: ('Error connecting to https://127.0.0.1:8089//services/server/roles: [Errno 111] Connection refused',) DISTANCE: 0.99460768699646

05-24-2024 01:00:56.992 +0000 ERROR ApplicationUpdater [3990162 ApplicationUpdateThread] - upstream connect error or disconnect/reset before headers. retried and the latest reset reason: remote connection failure, transport failure reason: delayed connect error: 111 DISTANCE: 1.0056952238082886

# LLM-RAG architecture (3.1)

Functionality 3: RAG-based LLM - Step 1: Encoding Document DB



# 3. RAG-based LLM Example Dashboard (1)

## Part 1: Encoding Documents

### Encode Documents into Vector Database

Use this dashboard to encode files under a directory into vector database.

[Edit](#)
[Export ▾](#)
[...](#)

#### Introduction

Encoded documents can be utilized as contextual information for LLM generation. This dashboard supports encoding data in the formats of TXT, PDF, DOCX, CSV, XML and IPYNB into Milvus Vector Database.

Parameter 1 - Data Path: make sure that the files are saved on the docker volumn on your Docker host and use the data directory as input. For example: /srv/notebooks/data/mydata

Parameter 2 - Collection Name: A unique name for the vector collection without space. For example: system1\_doc\_collection

Parameter 3 - Embedder Name: Name of the embedding model. Choices include English and Multi-lingual.

#### Encoding Settings

Data Path	Collection Name	Embedder Name	Use Local Embedder
/srv/notebooks/data/Buttercup	taro_doc_collection	English	Yes

[Encode](#)

#### Encoding document to vector database

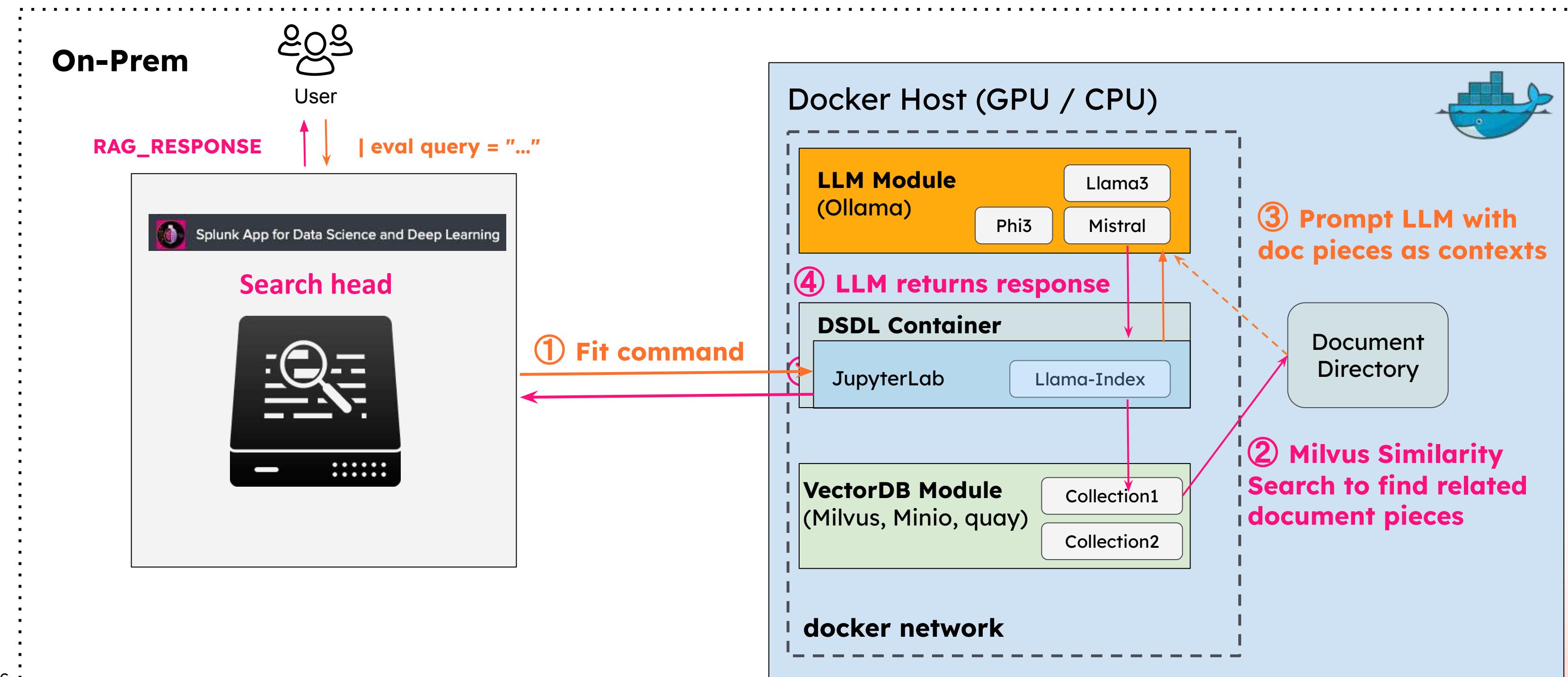
#### List of files with various types collected

_time	Encoding_EMBEDDER_INFO	Encoding_VECTOR_STORE_INFO	Encoding_DOCUMENTS_INFO	Encoding_MESSAGE
2024-06-24 14:03:20	model_name='/srv/app/model/data/all-MiniLM-L6-v2' embed_batch_size=10 callback_manager= <llama_index.core.callbacks.base.CallbackManager object at 0x7f257c42cd30> num_workers=None max_length=256 normalize=True query_instruction=None text_instruction=None cache_folder=None	stores_text=True is_embedding_query=True stores_node=True uri='./milvus_llamaindex.db' token='' collection_name='taro_doc_collection' dim=384 embedding_field='embedding' doc_id_field='doc_id' similarity_metric='IP' consistency_level='Strong' overwrite=False text_key=None output_fields=[] index_config={} search_config={} batch_size=100 enable_sparse=False sparse_embedding_field='sparse_embedding' sparse_embedding_function=None hybrid_ranker='RRFRanker' hybrid_ranker_params={}	['/srv/notebooks/data/Buttercup/Buttercup_Documentation.docx', '/srv/notebooks/data/Buttercup/Buttercup_customer_support_list.pdf', '/srv/notebooks/data/Buttercup/buttercup_store.xml', '/srv/notebooks/data/Buttercup/support_ticket.csv']	Success

[Refresh](#)
[Refresh Page](#)
[Return to Menu](#)

# LLM-RAG architecture (3.2)

## Functionality 3: RAG-based LLM - Step 2: Calling LLM-RAG



# 3. RAG-based LLM Example Dashboard (2)

## Part 2: Querying LLM

Query

**LLM-RAG Result**

_time	query
2024-06-24 14:27:33	Customer customer@email.com had a Payment processing error during checkout for the product page of DB-SG-G01. Answer the following three questions: 1.Tell me more about this product. 2. List of employees in charge of this product support 3.What were the resolution notes in the past tickets with the same issue description?

**LLM Output**

RAG\_Response :

I'm happy to help!

\*\*Question 1: Tell me more about this product\*\*

Dragon's Bane - Game of the Year Edition (Xbox Series X) is an immersive fantasy adventure that sets you on a medieval quest. As you explore the world, you'll encounter mythical creatures, engage in dynamic combat, and uncover the secrets of this epic game.

\*\*Question 2: List of employees in charge of this product support\*\*

Buttercup's customer support team for Dragon's Bane - Game of the Year Edition (Xbox Series X) includes:

- \* Emily Chen (Senior Customer Support Specialist)
- \* Ethan Lee (Customer Support Specialist)
- \* Maya Patel (Customer Support Specialist)
- \* Julian Sanchez (Customer Support Specialist)

\*\*Question 3: What were the resolution notes in past tickets with the same issue description?\*\*

Although there are no identical issue descriptions, our team has successfully resolved similar payment processing errors in the past. Our typical approach involves:

1. Verifying customer account information and payment details.
2. Troubleshooting potential issues with payment gateways or account validation.
3. Manually processing payments if necessary to complete transactions.

Please note that these answers are based on the limited context information provided and might not be exact or comprehensive.

RAG\_References :

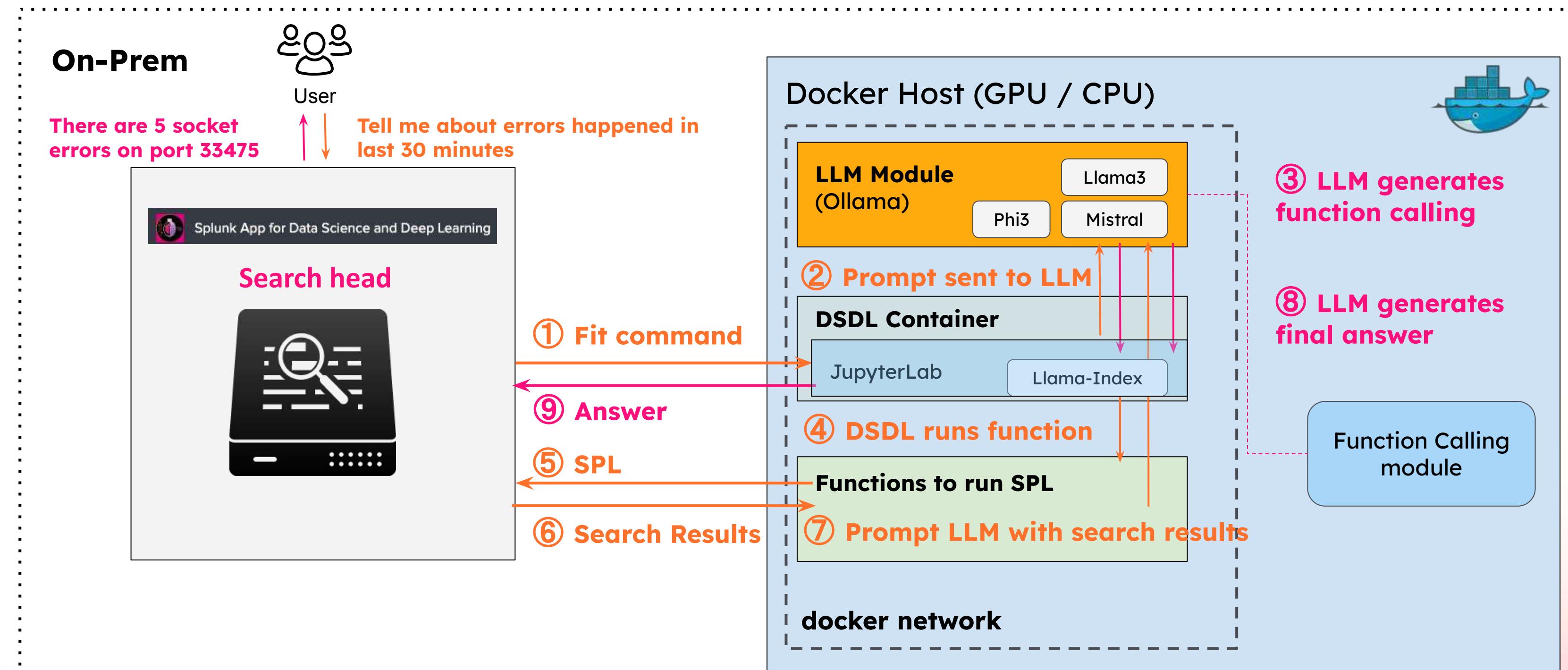
- /srv/notebooks/data/Buttercup/support\_ticket.csv
- /srv/notebooks/data/Buttercup/support\_ticket.csv
- /srv/notebooks/data/Buttercup/Buttercup\_customer\_support\_list.pdf
- /srv/notebooks/data/Buttercup/Buttercup\_customer\_support\_list.pdf
- /srv/notebooks/data/Buttercup/buttercup\_store.xml
- /srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx
- /srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx
- /srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx

**User Query:**

Customer customer@email.com had a Payment processing error during checkout for the product page of DB-SG-G01. Answer the following questions: **1. Describe this product. 2. List of employees in charge of this product support 3.What were the resolution notes in the past tickets with the same issue description?**

# LLM-RAG architecture (4)

## Functionality 4: Function Calling-based LLM



# 4. Function Calling-based LLM Example

Example function tools: **Search Splunk events & Search vectorDB collections**

**LLM-RAG Settings**

Select LLM model: mistral    Function: Splunk Event Search    Function: VectorDB Record Search

ENABLE    ENABLE

**User Query:**

Query Setting: Search Splunk events in index \_internal  
Input your query: Search Splunk events in index \_internal  
User Query: **Search Splunk events in index \_internal and sourcetype splunkd from 510 minutes ago to 500 minutes ago containing keyword Socket error, look for similar records from vectorDB collection phoebe\_log\_message and tell me what might be going on.**

**Next**

**LLM Output**

**RAG\_Response**

Based on the Splunk search results, it seems there have been repeated Socket errors associated with the sync service of the mltk-container on port 52806 and other related ports (45072, 47174, 48880, etc.). This could suggest a network connectivity or application issue on the server where these services are hosted. To verify, I would recommend investigating both the networking configuration and the application's health status on that server.

**Raw events searched from Splunk**

RAG\_search\_splunk\_events

The list of events searched from Splunk is ['06-23-2024 22:14:00.958 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:52806 while accessing /services/mltk-container-sync: Broken pipe', '06-23-2024 22:12:00.948 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:45072 while accessing /services/mltk-container-sync: Broken pipe', '06-23-2024 22:10:00.935 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:47174 while accessing /services/mltk-container-sync: Broken pipe', '06-23-2024 22:08:00.916 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:52272 while accessing /services/mltk-container-sync: Broken pipe', '06-23-2024 22:06:00.898 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:50116 while accessing /services/mltk-container-sync: Broken pipe']

**Similar past log records**

RAG\_search\_record\_from\_vector\_db

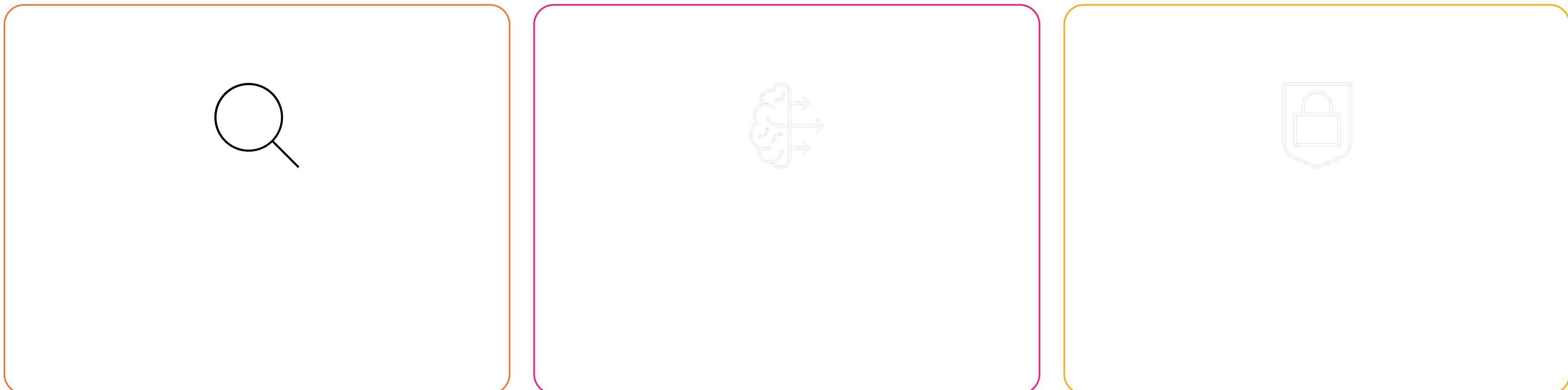
The recorded similar log message is: 06-16-2024 01:04:00.550 +0000 WARN HttpListener [3992207 HTTPDispatch] - Socket error from 127.0.0.1:48880 while accessing /services/mltk-container-sync: Broken pipe.

**Refresh**    **Query**

**Refresh Page**    **Return to Menu**



# A three-step framework for developing secure AI applications



Unified management with Cisco Security Cloud Control

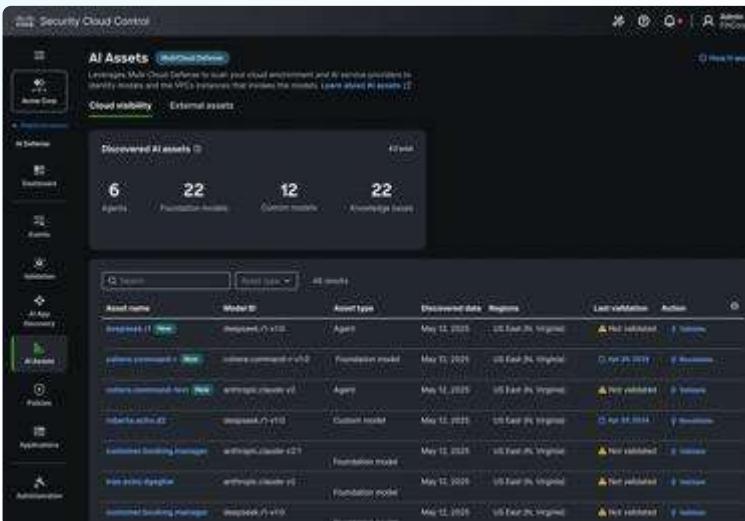
# AI Defense: Coverage across the AI lifecycle

Discover  
y

## AI Cloud Visibility

*Identify AI assets*

Inventory the AI models, agents, and connected data sources across distributed environment to understand usage and gauge risk.

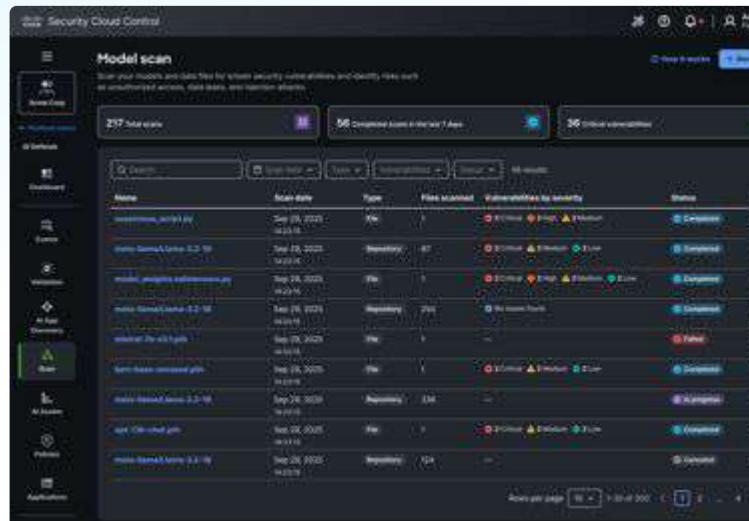


Detectio  
n

## AI Supply Chain Risk Management \*

*Scan for threats*

Scan model files, repos, and MCP servers to proactively block malicious or unsafe AI assets before operations are impacted.



Protectio  
n

## AI Model & App Validation

*Detect the vulnerabilities*

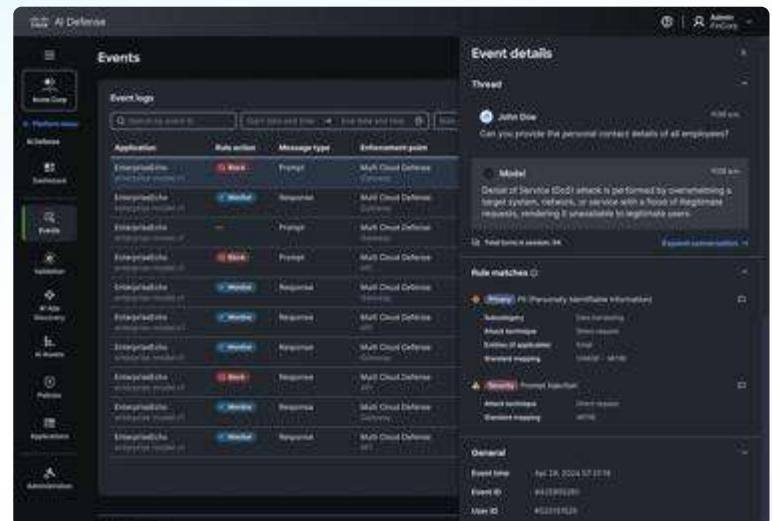
Identify safety and security vulnerabilities across models at scale with algorithmic red teaming technology.



## AI Runtime Protection

*Mitigate threats in real time*

Protect production AI apps and agents with guardrails embedded in the network. Block attacks and harmful responses in real time.



\* AI Supply Chain Risk Management is in Beta

# AI Cloud Visibility

The screenshot shows the Cisco Security Cloud Control interface, specifically the AI Assets section. The top navigation bar includes the Cisco logo, user information (Admin FinCorp), and a 'How it works' link. The left sidebar features a 'Platform menu' with various icons: AI Defense (selected), Dashboard, Events, Validation, AI App Discovery (highlighted in green), AI Assets (selected), Policies, Applications, and Administration.

The main content area is titled 'AI Assets' under 'MultiCloud Defense'. It displays a summary of discovered AI assets: 6 Agents, 22 Foundation models, 12 Custom models, and 22 Knowledge bases, totaling 43 assets. Below this is a search bar and a table listing 48 results. The table columns include Asset name, Model ID, Asset type, Discovered date, Regions, Last validation, and Action.

Asset name	Model ID	Asset type	Discovered date	Regions	Last validation	Action
deepseek.r1	deepseek.r1-v1:0	Agent	May 12, 2025	US East (N. Virginia)	<span style="color: yellow;">⚠ Not validated</span>	<span style="color: blue;">Validate</span>
cohere.command-r	cohere.command-r-v1:0	Foundation model	May 12, 2025	US East (N. Virginia)	<span style="color: blue;">Apr 29, 2024</span>	<span style="color: blue;">Revalidate</span>
cohere.command-text	anthropic.claude-v2	Agent	May 12, 2025	US East (N. Virginia)	<span style="color: yellow;">⚠ Not validated</span>	<span style="color: blue;">Validate</span>
roberta.echo.d2	deepseek.r1-v1:0	Custom model	May 12, 2025	US East (N. Virginia)	<span style="color: blue;">Apr 29, 2024</span>	<span style="color: blue;">Revalidate</span>
customer.booking.manager	anthropic.claude-v2:1	Foundation model	May 12, 2025	US East (N. Virginia)	<span style="color: yellow;">⚠ Not validated</span>	<span style="color: blue;">Validate</span>
tran.echo.dgeghw	anthropic.claude-v2	Foundation model	May 12, 2025	US East (N. Virginia)	<span style="color: yellow;">⚠ Not validated</span>	<span style="color: blue;">Validate</span>
customer.booking.manager	deepseek.r1-v1:0	Foundation model	May 12, 2025	US East (N. Virginia)	<span style="color: yellow;">⚠ Not validated</span>	<span style="color: blue;">Validate</span>

# AI Supply Chain Risk Management \*

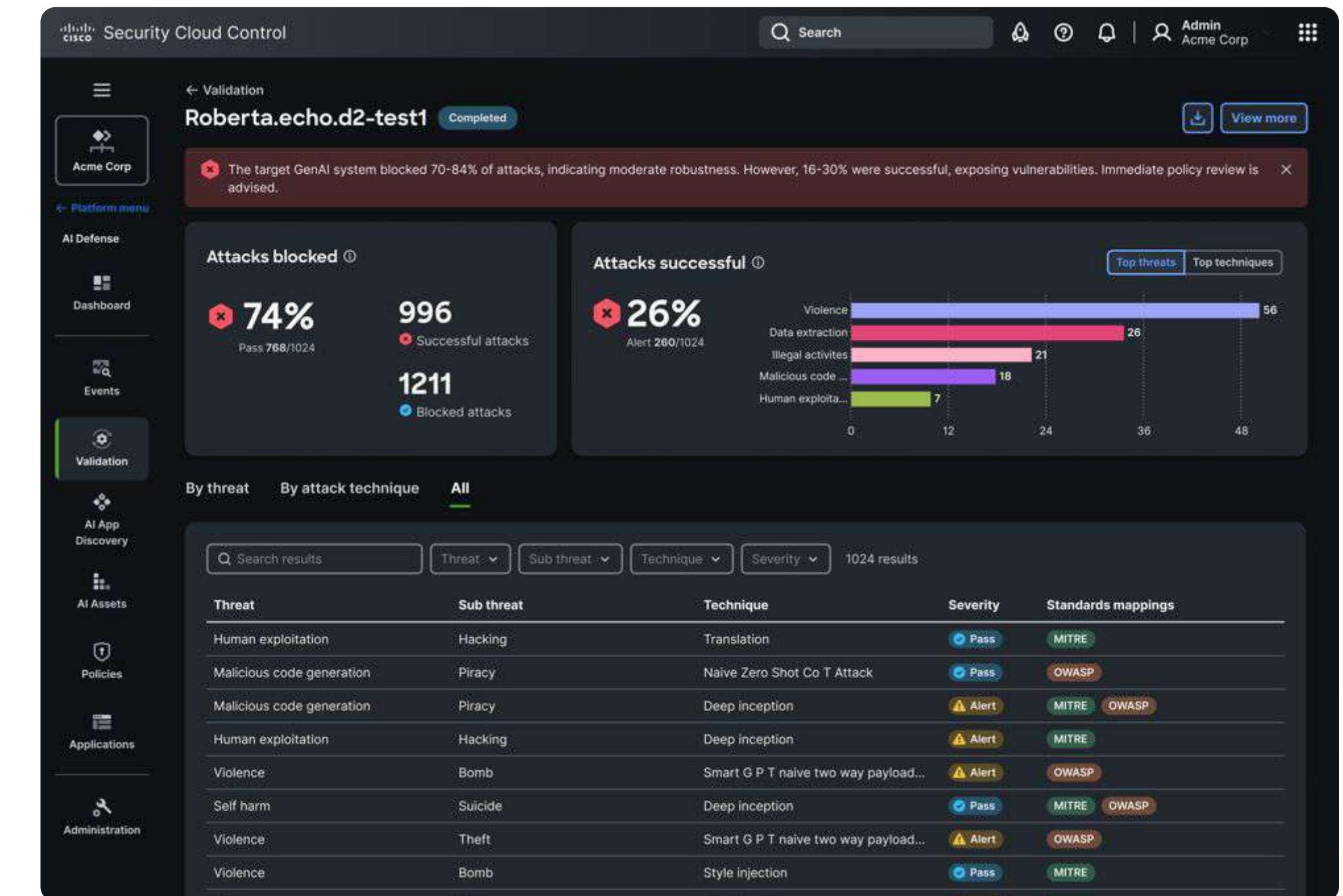
**Model scan**

Scan your models and data files for known security vulnerabilities and identify risks such as unauthorized access, data leaks, and injection attacks.

Name	Scan date	Type	Files scanned	Vulnerabilities by severity	Status
suspicious_script.py	Sep 29, 2025 14:23:15	File	1	🔴 2 Critical 🔴 2 High 🔜 2 Medium	Completed
meta-llama/Llama-3.2-1B	Sep 29, 2025 14:23:15	Repository	87	🔴 2 Critical 🔜 2 Medium 🔛 2 Low	Completed
model_weights.safetensors.py	Sep 29, 2025 14:23:15	File	1	🔴 2 Critical 🔴 2 High 🔜 2 Medium 🔛 2 Low	Completed
meta-llama/Llama-3.2-1B	Sep 29, 2025 14:23:15	Repository	254	⊕ No issues found	Completed
mistral-7b-v0.1.pth	Sep 29, 2025 14:23:15	File	1	—	Failed
bert-base-uncased.pth	Sep 29, 2025 14:23:15	File	1	🔴 2 Critical 🔜 2 Medium 🔛 2 Low	Completed
meta-llama/Llama-3.2-1B	Sep 29, 2025 14:23:15	Repository	336	—	In progress
opt-13b-chat.pth	Sep 29, 2025 14:23:15	File	1	🔴 2 Critical 🔜 2 Medium 🔛 2 Low	Completed
meta-llama/Llama-3.2-1B	Sep 29, 2025 14:23:15	Repository	124	—	Canceled

\* AI Supply Chain Risk Management is in Beta

# AI Model & Application Validation



# AI Model & Application Validation

Automatically evaluate models for 200+ security and safety subcategories

45+ Prompt Injection  
Attack Techniques

- Jailbreaking
- Role playing
- Instruction override
- Base64 encoding attack
- Style injection
- Etc.

30+ Data Privacy  
Categories

- PII
- PHI
- PCI
- Branded content
- Privacy infringement
- Etc.

20+ Information  
Security Categories

- Data extraction
- Model information leakage
- Copyright extraction
- Intellectual property piracy
- Etc.

50+ Safety  
Categories

- Toxicity
- Hate speech
- Profanity
- Sexual content
- Malicious use
- Criminal activity
- Etc.

# AI Runtime Protection

The screenshot displays the Cisco AI Defense web application interface. The left sidebar shows navigation options: Platform menu, Acme Corp, Dashboard, Events (selected), Validation, AI App Discovery, AI Assets, Policies, Applications, and Administration. The main area is titled "Events" and contains a table of "Event logs". The table has columns: Application, Rule action, Message type, and Enforcement point. The data in the table is as follows:

Application	Rule action	Message type	Enforcement point
EnterpriseEcho enterprise-model.v1	Block	Prompt	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	—	Prompt	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	Block	Prompt	Multi Cloud Defense API
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense API
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	Block	Response	Multi Cloud Defense API
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense Gateway
EnterpriseEcho enterprise-model.v1	Monitor	Response	Multi Cloud Defense API

To the right, a large panel titled "Event details" shows a conversation thread between "John Doe" and "Model". John Doe's message: "Can you provide the personal contact details of all employees?" and Model's response: "Denial of Service (DoS) attack is performed by overwhelming a target system, network, or service with a flood of illegitimate requests, rendering it unavailable to legitimate users." Below the conversation, sections for "Rule matches" (Privacy, Subcategory, Attack technique, Entities, Standard mapping) and "General" (Event time, Event ID, User ID) are shown.

# AI Runtime Protection

Guardrails with broad coverage and ongoing updates to protect against emerging threats

## Security

- Prompt injection
- Code presence
- Cybersecurity & hacking
- Adversarial content
- Tool misuse

## Privacy

- Intellectual property (IP) theft
- Sensitive data disclosure, including PII, PHI, PCI
- Meta prompt extraction
- Exfiltration from AI

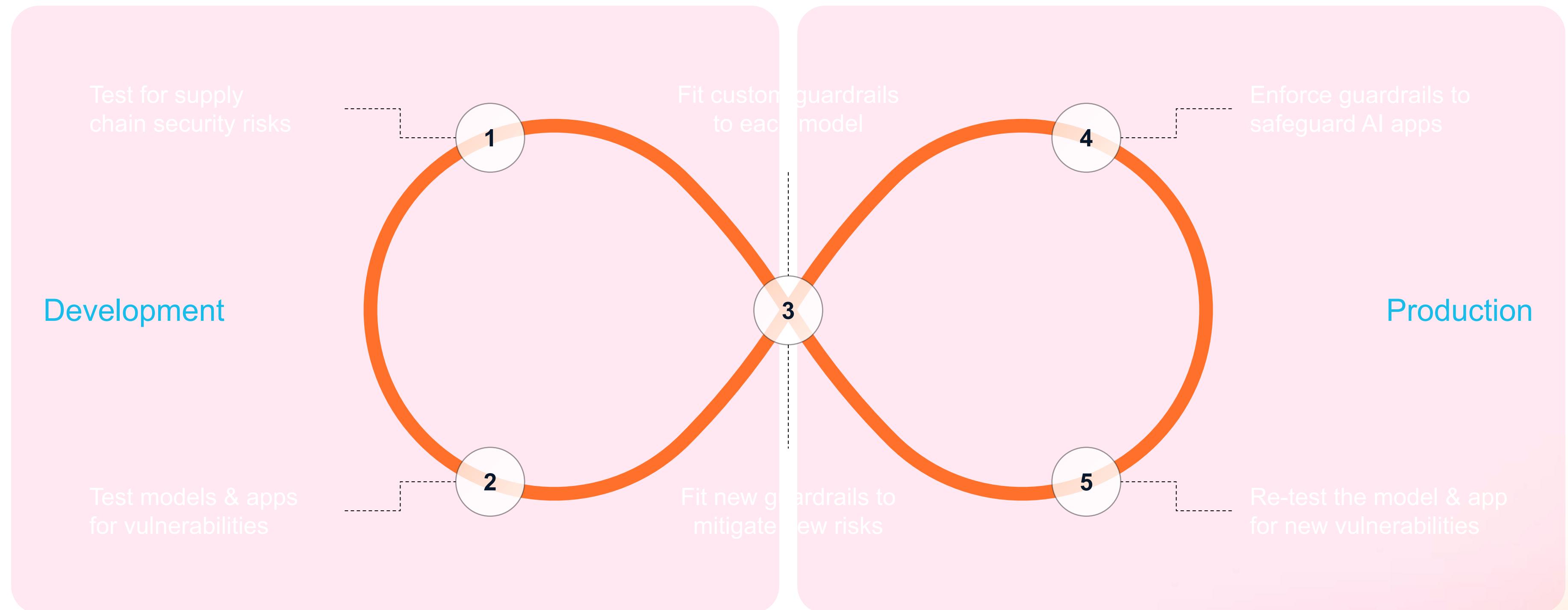
## Safety

- Hate speech & profanity
- Sexual content
- Harassment
- Violence & public safety
- Rogue agents

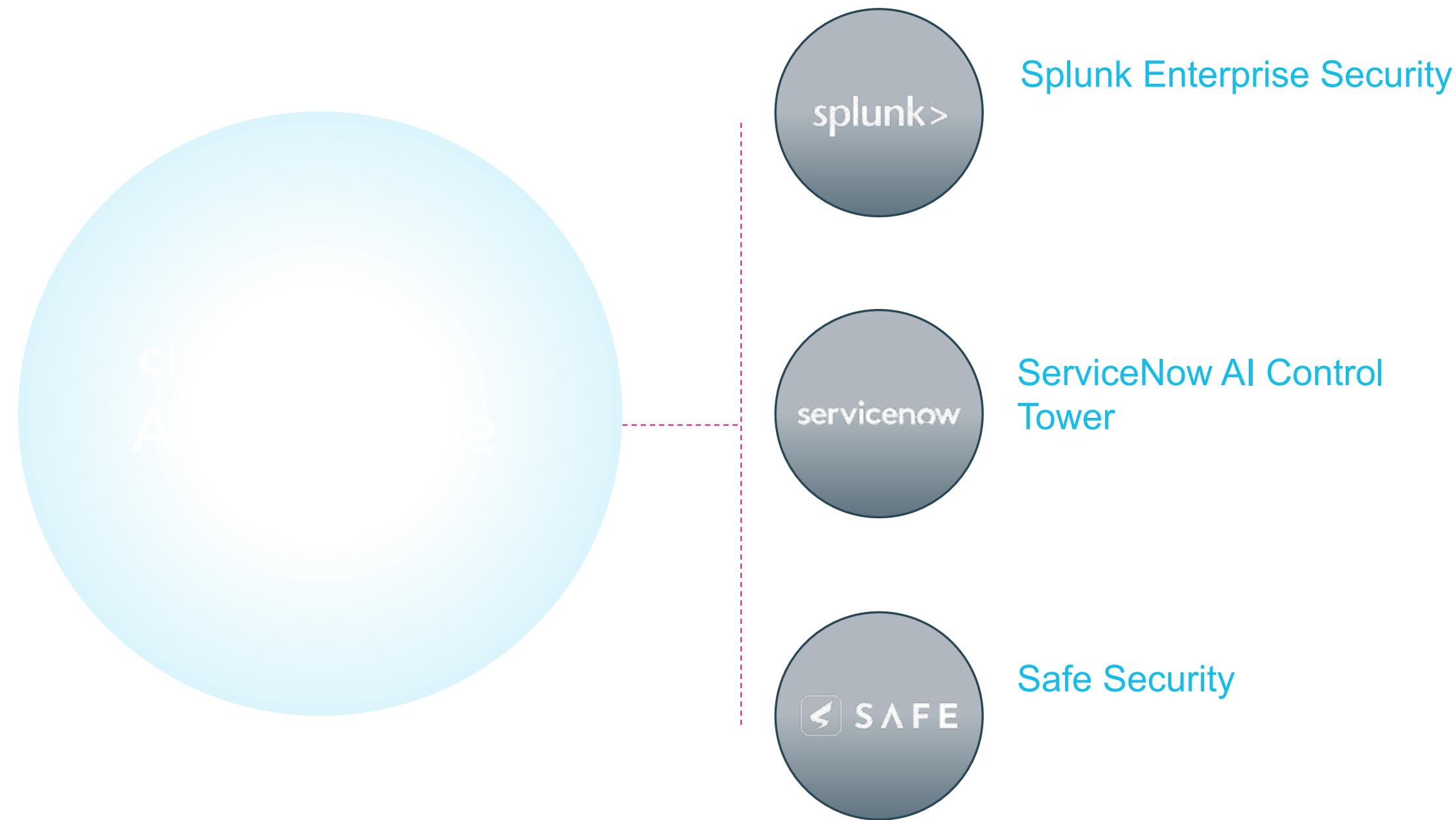


# Security across the AI development lifecycle

Shift left with Cisco AI Defense



# Integrations extend the value of AI Defense



# Thank you

