.conf23: Splunk Introduces New AI Offerings to Accelerate Detection, Investigation and Response Across Security and Observability

July 18, 2023

New generative AI app Splunk AI Assistant connects customers with faster answers through interactive chat experience

SAN FRANCISCO & LAS VEGAS--(BUSINESS WIRE)--Jul. 18, 2023-- Splunk Inc. (NASDAQ: SPLK), the cybersecurity and observability leader, today announced **Splunk AI**, a collection of new AI-powered offerings to enhance its unified security and observability platform. Launched at .conf23, Splunk AI combines automation with human-in-the-loop experiences, so organizations can drive faster detection, investigation and response while controlling how AI is applied to their data. Leaning into its lineage of data visibility and years of innovation in AI and machine learning (ML), Splunk continues to enrich the customer experience by delivering domain-specific insights through its AI capabilities for security and observability.

Splunk AI strengthens human decision-making and threat response through assistive experiences. The offerings empower SecOps, ITOps and engineering teams to automatically mine data, detect anomalies and prioritize critical decisions through intelligent assessment of risk, helping to minimize repetitive processes and human error. Splunk AI optimizes domain-specific large language models (LLMs) and ML algorithms built on security and observability data, so SecOps, ITOps and engineering teams are freed up for more strategic work - helping to accelerate productivity and lower costs. Looking forward, Splunk is committed to remaining open and extensible as it integrates AI into its platform, so organizations can extend Splunk AI models or use home-grown and third party tools.

“Splunk’s purpose is to build a safer, more resilient digital world, and this includes the transparent usage of AI,” said Min Wang, CTO at Splunk. “Looking forward, we believe AI and ML will bring enormous value to security and observability by empowering organizations to automatically detect anomalies and focus their attention where it’s needed most. Our Splunk AI innovations provide domain-specific security and observability insights to accelerate detection, investigation and response while ensuring customers remain in control of how AI uses their data.”

Generate faster outcomes through assisted intelligence

Splunk AI Assistant leverages generative AI to provide an interactive chat experience and helps users author Splunk Processing Language (SPL) using natural language. The app preview fosters an immersive experience where users can ask the AI chatbot to write or explain customized SPL queries to increase their Splunk knowledge. Splunk AI Assistant improves time-to-value and helps make SPL more accessible, further democratizing an organization’s access to, and insights from, its data.

Drive faster, more accurate alerting through new AIOps capabilities

The embedded AI offerings, highlighted below, enable organizations to drive more accurate alerting to build digital resilience:

- With a few clicks, **Splunk App for Anomaly Detection** provides SecOps, ITOps and engineering teams with a streamlined end-to-end operational workflow to simplify and automate anomaly detection within their environment.
- The IT Service Intelligence 4.17 features greater detection accuracy and faster time-to-value:
  - **Outlier Exclusion for Adaptive Thresholding** detects and omits abnormal data points or outliers (such as network disruptions or outage spikes) for more precise dynamic thresholds to drive accurate detection within one’s technology environment.
  - The new **ML-Assisted Thresholding** preview uses historical data and patterns to create dynamic thresholds with just one click, helping to provide more accurate alerting on the health of an organization's technology environment.

Execute insights-driven, effective anomaly detection through automation

The ML-powered foundational offerings provide organizations access to large, richer sets of information by extending solutions built on the Splunk platform, so they can drive data-driven decisions:

- The **Splunk Machine Learning Toolkit (MLTK) 5.4** provides guided access to ML technology to users of all levels and is one of the most downloaded Splunkbase apps, with over 200k downloads. Through leveraging techniques like forecasting and predictive analytics, SecOps, ITOps and engineering teams can unlock richer ML-powered insights. The new release builds on the open, extensible nature of Splunk AI by enabling customers to bring their externally trained models into Splunk.
- Now available on Splunkbase, **Splunk App for Data Science and Deep Learning (DSDL) 5.1** extends MLTK to provide access to additional data science tools to integrate advanced custom machine learning and deep learning systems with Splunk. This release includes two AI assistants that allow customers to leverage LLMs to build and train models with their domain specific data to support natural language processing.

Empower SecOps Teams with rapid detections

Over the past year, the Splunk Threat Research Team has added 6 ML-powered detections to Splunk Enterprise Security through the Splunk

Enterprise Security Content Updates (ESCU) to help security practitioners address ongoing time-sensitive security threats and attack methods.

Supporting Quotes:

"We leverage Splunk's Machine Learning Toolkit to detect anomalies in extensive datasets that may have otherwise remained undetected with traditional signature-based methods," said Matt Snyder, Program Lead - Advanced Security Analytics at VMWare. "By incorporating robust machine learning models within Splunk, we eliminate the need for a separate infrastructure for advanced analytics, saving us time and resources."

"With the growing complexity of tech infrastructure, coupled with the ongoing talent shortages, AI and AIOps capabilities are becoming essential to help organizations respond faster and more strategically to threats," said Steven Dickens, VP and Practice Leader at Futurum Group. "The new offerings within Splunk AI do just that - they enhance and accelerate human decision-making and response to threats, so organizations can ensure their digital systems remain secure and resilient."

Availability:

All new offerings within Splunk AI are now generally available, with the exception of Splunk AI Assistant and ML-Assisted Thresholding which are available in preview.

For more information on Splunk AI and its various offerings unveiled at .conf23, visit here.

For more details on all of Splunk's .conf23 announcements, please visit our newsroom.

About Splunk Inc.

Splunk helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

View source version on businesswire.com: https://www.businesswire.com/news/home/20230718305364/en/

Media Contact
Missy Somers
Splunk Inc.
press@splunk.com

Investor Contact
Investor Relations
Splunk Inc.
ir@splunk.com

Source: Splunk Inc.