Call for **Speakers Track Guidance**

To learn more about the .conf23 Call for Speakers, visit:

conf.splunk.com

Hello Splunk Enthusiast!

Call for Speakers for .conf23 is now open! **You have until March 2, 2023 @ 11:59 PM PT to submit.**

This year .conf will be live, in-person in Las Vegas! .conf23 will have all the fun, information and education that's made our conference a favorite among data champions. To help you with an amazing submission for .conf23, we have included a list of topics specific to each of this year's tracks — *Observability, Platform, Security and Splunk Developer.*

Submission Tips

Follow these tips to optimize your submission. Also, be sure to **reference our other Call for Speakers assets on conf.splunk.com.**

TIP #1 Keep your abstract short, specific and enticing.

With dozens of concurrent sessions and activities to choose from at any given time, the .conf23 agenda promises to be jam-packed! Short and enticing abstracts will increase your chances of having .conf23 attendees choose your session—not to mention our Review Committees, who will read all your submissions! Our favorite abstracts usually average 100 words (and should not exceed 500 characters with spaces).

TIP #2 Get creative, differentiate yourself from other speakers.

Why are you the best person to tell this story? Maybe it is because you experienced the challenge firsthand and addressed it with Splunk. Or did it differently. Maybe you've used Splunk for a long time and have become a wiz. Or maybe you've been in your industry and role for longer than you've owned your favorite T-shirt. Whichever it is, let us know!

TIP #3 There's an audience for everything.

You can submit your abstract as *Novice, Intermediate* or *Advanced*. Run your topic by a few colleagues and ask them how they would rate its level of difficulty. Think your submission may be too advanced for the audience? Think again! Advanced sessions perform well at .conf and usually draw larger than expected audiences. Breakout sessions will be 30 minutes in length, with 15 minutes for Q&A. Interactive sessions may be 60, 90 or 120 minutes long.

TIP #4 If your submission is industry-specific, focus on key industries.

We have zero doubt that your submission on cybersecurity use cases for beekeepers would make an interesting session. Unfortunately, it may not attract the sizeable audience of fellow beekeeping cybersecurity specialists that you're hoping for. Focus instead on industries and sectors like high tech, financial services and insurance, healthcare and pharma, manufacturing, retail and public sector. Otherwise, think about how your topic could be generalized to apply to industries and sectors outside of yours.

TIP #5 CFS is NOT a numbers game.

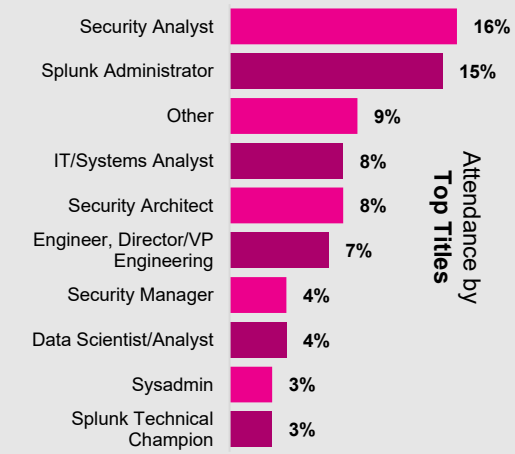
Each year, a few overzealous speakers submit multiple abstracts hoping to get one of them chosen. Unfortunately, this only increases both your and our work and review cycles, but it doesn't increase your chances of getting selected. Focus on your best topics or storylines you want to share and write amazing abstracts for those.

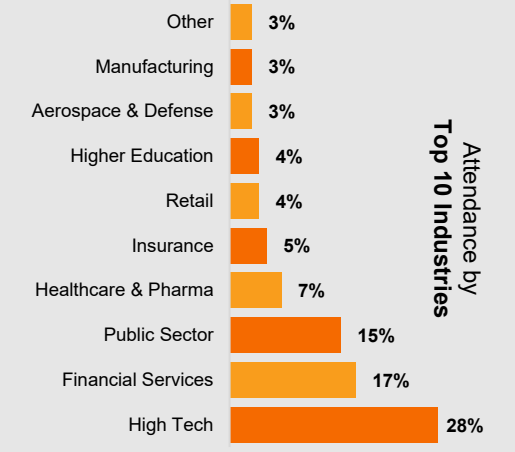
.conf22 by the Numbers

10,000 Attendees from…

72 Countries with…

370+ Customer, Partner and Splunk speakers





splunk> .conf23

Splunk Observability (ITOps+DevOps) Track

Sub-Tracks, Themes and Storylines

In the Observability track, we'll show you how to gain complete visibility and context across the full stack of infrastructure, applications, and the digital customer experience. Build better experiences, ship software faster. This track includes deep dives from Splunk experts, customers, and practitioners who will share pragmatic advice and help you level up your DevOps and ITOps practices.

The following Sub-Tracks, Themes and Storylines are key for the Observability Track in 2023:

Sub-Tracks

- AIOps & Incident Management
- APM (Application Performance Monitoring)
- Infrastructure/Cloud/Metrics Monitoring
- OpenTelemetry
- User Experience Monitoring (RUM, Synthetics, DEM)

Themes

- AIOps
- Alert & Incident Management
- Application, Infrastructure and IT Service Monitoring
- Application Performance Monitoring (APM)
- Infrastructure Monitoring
- Observability Best Practices
- OpenTelemetry
- Starting an Observability Practice
- User Experience Monitoring (RUM, Synthetics, DEM)

Storylines	Details
Understanding Observability	What is observability and why do you need it? Learn how to improve the digital customer experience and find and fix problems faster by understanding your infrastructure health and application performance.
Building your Observability strategy and best practices	Are you looking to improve customer experience, or empower your developers to innovate faster, and run services with greater resilience, scale, and efficiency but don't know how/where to start? If "yes," learn the foundations you need to build an end-to-end observability strategy to get better visibility across your infrastructure, applications, and business services to help you achieve your business goals.
Moving beyond traditional monitoring	You need metrics, logs, and traces to monitor cloud-native applications and infrastructure, but how can you tackle problems before customers are affected if this data is siloed in different systems? Learn how you can eliminate fragmented telemetry data, anticipate emerging problems before customers notice, and know where to look when a problem does occur.
Removing the complexity of moving to the cloud	Moving to the cloud has its advantages. But greater scale creates more complexity, and with more complexity comes more problems. Learn how full-stack observability can help you understand the behavior of your hybrid infrastructure to accurately find, fix, and prevent service outages quickly before it impacts your business.
Simple troubleshooting	Finding the root cause of a service failure becomes complicated and time-consuming when teams have to deal with disparate, inaccurate alerts that are slow to detect problems and offer no business context to the impact of each change. Learn how to leverage Splunk to proactively detect, alert, and easily resolve problems before they impact the business.
Building a complete Observability practice starting with logs	Whether you're an existing Splunk customer or new to Splunk, for many practitioners, logs are the most familiar pillar of Observability. But for new cloud-native environments and microservices-based applications, logs alone are not enough. For complete visibility into customer experience and system health, teams need to leverage metrics and trace data in context with log data to troubleshoot issues quickly. Learn how to build an end-to-end observability strategy starting with log monitoring to detect the root cause of problems faster across your applications and infrastructure.
Improve your digital user experience	Digital businesses increasingly rely on cloud technologies and DevOps processes to accelerate time-to-market and deliver high-quality digital experiences that win customers. Learn how to proactively eliminate customer-facing issues and optimize web and API performance by incorporating predictive issue detection into your development cycles, collecting immediate customer experience feedback on new code releases, and continuously prioritizing performance across web and mobile.
Better monitoring for cloud-native applications with APM	You know that building cloud-native applications can increase speed and scale. You also know that it adds complexity. Learn how APM solves problems faster in monoliths and microservices by immediately detecting problems from new deployments, confidently troubleshooting the source of an issue, and optimizing service performance.
OpenTelemetry: the standard for Observability	OpenTelemetry is an open standard for the collection of metrics, traces, and logs that can be ingested by almost every vendor. Learn why OpenTelemetry is the most flexible solution for getting observability data from an application into an observability system, and how you can have complete control over your data regardless of your observability tooling.
Modernize your IT operations with predictive business insights and AIOps	Are you looking to optimize your business services, while reducing complexity, and improve visibility, resiliency, and operational efficiency? Learn how ITOps teams can prevent unplanned downtime, deliver reliable services, and improve operational efficiency with end-to-end visibility, predictive analytics, and automated incident response.
Integrating your monitoring and incident management	Learn how to connect monitoring data, incident response workflow, and even your ITSM and chat tools into one seamless workflow and system.
Responding to IT incidents quickly	Cutting the lag time between receiving alerts and resolving issues is crucial for any company deploying mission-critical applications. Learn how to quickly identify the problem, engage the right people, and fix issues before they impact your customers and stakeholders.

splunk> .conf23

Splunk Platform Track

Sub-Tracks, Themes and Storylines

Learn how to jump start your data use cases with Splunk Cloud Platform and Splunk Enterprise or get up to speed on more advanced techniques. We will review how Splunk can super charge your hybrid cloud transformations with exciting platform innovations like AI & ML, Edge Hub, Edge Processing, Streaming, Federated Search and Connected Experiences.

The following Sub-Tracks, Themes and Storylines are key for the Platform Track in 2023:

Sub-Tracks

- Admins: Managing an Efficient Splunk Deployment
- Emerging Capabilities for Data Lifecycle Management
- Hybrid Cloud: Managing Complex Processes and Growing Threat Surfaces
- Users: Getting Started with Security and Observability Use Cases

Themes

- Advanced Architectures
- Alerting
- Artificial Intelligence and Machine Learning
- Cloud and Hybrid Transformation
- Connected Experiences (Mobile/AR)
- Dashboards and Analytics
- Edge, Streaming, Routing and Getting Data In
- Getting Started with Splunk Use Cases
- Innovative Storage Techniques
- SPL, Search & Federated Search

Storylines	Details
Jumpstart with Splunk	Admin best practices for starting with Splunk - spark your curiosity around what is possible and find specific guidance on how to configure Splunk
Getting started with basic Security and Observability use cases	Build and extend on the Splunk platform to expand into new use cases
Discover what's new	Get the most out of the newest Splunk platform products, services and features
Mastering Splunk	Explore mastery level use cases around platform innovations including the latest in SPL, dashboards, and architecture
Investigating federated search	Dive into advanced tactics using federated search
Scaling your Splunk Architecture	Advanced designs for architecting an optimized Splunk at scale
Best practices for cloud and hybrid transformations	Learn how Splunk can help you migrate your data workloads to the cloud, or manage your hybrid and multi-cloud environment
Integrating with your favorite cloud provider's ecosystem	Explore Splunk's integrations with leading cloud providers
Operationalizing artificial Intelligence and machine learning	Learn about Splunk's latest innovations in artificial intelligence and machine learning and how to implement these in your environments
Discovering streaming data analytics	Find out how streaming data analytics allow you to identify potential business opportunities as well as detect and resolve organizational threats
Engaging your full workforce	Expanding access to data to every user through innovations like mobile, augmented reality, and natural language processing
Data optimization	Strategically filter, route and store your growing data sources to get the most value from Splunk search

splunk> .conf23

Splunk Security Track

Sub-Tracks, Themes and Storylines

The Security Track will cover a wide range of contemporary security topics across security monitoring, compliance, detection, response and more. Experts from Splunk, our customers and partners will share their experiences and best practices to help improve your security skills.

The following Sub-Tracks, Themes and Storylines are key for the Security Track in 2023:

Sub-Tracks

- Security Analytics (SIEM, UBA and Threat Intelligence)
- Security Automation (SOAR)
- Security Foundations: Get started with Splunk for security use cases, including Fraud, OT security, cloud security and compliance
- Unified Security Operations (Security Portfolio)

Themes

- Advanced Threat Detection (Insider & External, Risk-Based Alerting, Fraud)
- Cloud Security
- Compliance
- Incident Investigation and Forensics
- Security Monitoring
- SOC Automation & Orchestration (Workflows)
- Threat Hunting

Storylines	Details
Modernize your security operations	Rapid threat detection, investigation and response (TDIR); comprehensive security visibility; increased analyst efficiency; security automation; breach prevention
Develop a strategic security mindset	Better alignment to, and execution against, the organization's overall business mission and executive vision. Leveraging security as a revenue enabler and as a business differentiator
Prevent breaches	Stop breaches before they happen. Empower your security team with resources and technology to be more proactive rather than reactive so they can stay one step ahead of attackers
Achieve comprehensive security visibility	See threats across disparate data silos to achieve comprehensive and contextual security visibility across your infrastructure
Detect accurately and reduce business risk	Use Splunk Enterprise Security, the market-leading SIEM with Risk-Based Alerting (RBA), integrated behavioral analytics and threat intelligence to rapidly detect advanced threats like polymorphic malware, file-less and zero-day attacks
Transform and curate data to make it actionable for your SOC	Use Splunk Intelligence Management to make detection workflows more accurate by reducing false positives. Leverage internal/external intelligence sources to identify malicious vs. safe items
Clear a vast majority of security alerts and tasks with no human interaction	Use Splunk SOAR to automate repetitive security tasks, alert triage and response. By automating this workload, your team can eliminate analyst grunt work and free up time to focus on more mission critical tasks.
Reduce mean time to respond to threats	Use security automation from Splunk SOAR to accelerate investigations, response and remediation. Automate security tasks in a matter of seconds, versus minutes or hours if performed manually, resulting in a reduced mean time to respond (MTTR) to threats
Increase SOC efficiency	Use Splunk Mission Control for a unified security operations experience, enabling the SOC to detect, investigate, and respond to threats from one common work surface; simplify security workflows and harmonize your existing security stack
Solve compliance challenges	Achieve compliance at scale (e.g. harmonize multiple privacy standards, major reduction in overhead/compliance cost)
Reduce losses from fraud	Positive financial outcomes and reduced risk via improved fraud detection—especially within a vertical such as retail, financial services or healthcare
Scale security operations	Maintain consistent results, even as the organization goes through hyper-growth
Execute a use case rollout plan	Design and implement a phased security strategy that tackles your biggest challenges
Use nontraditional data sources	Leverage data sources such as ICS, OT, IoMT or industry-specific audit logs within the Security Operations Center
Accelerate your journey to cloud	Achieve faster time to value with more efficient installation, configuration and sizing of cloud-delivered security. Cloud software updates are continuous and automatic, which allows your team to spend more time securing the business instead of managing infrastructure

splunk> .conf23

Splunk Developer Track

Themes and Storylines

The Developer Track will cover building extensions to Splunk from basic to advanced. Learn how to build apps and add-ons, custom commands, and more to bring new data into Splunk, search and analyze, and display in beautiful visualizations to drive actions and meaningful outcomes for users.

The following Themes and Storylines are key for the Splunk Developer Track in 2023:

Themes

- AddOn Builder and Getting Data In
- APIs
- App Inspect/Cloud Vetting
- App Publishing and Splunkbase
- Best Practices
- Building Splunk Apps
- Custom Commands
- SDKs
- Splunk Apps and Add Ons
- Tooling and CI/CD

Storylines	Details
How to create a custom command for Splunk	Learn how to extend the Splunk command set with your own custom commands
Building an app with Splunk UI and React Visualizations	Walk through the process of creating a highly customized application experience using React and Splunk's UI and visualization libraries
Optimizing your SPL	Learn best practices for writing better SPL and how to debug your searches
Getting started building apps for Splunk	Don't think you can build a Splunk app? It's easier than you think, and we'll tell you how!
Best practices for logging data from your app into Splunk	You may have logging about your app, but you should also be logging from your app for full visibility!
Integrating Splunk's new Dashboard Framework	Learn how to build advanced dashboards and take full advantage of new UI features
Applying best practices to get your app into Splunk Cloud Platform	Your customers want to use your app in Splunk Cloud Platform—learn how to make it available to them
Publishing your app in Splunkbase	Want to share your app with the whole Splunk community? Get tips and best practices for releasing your app in Splunkbase
Generating sample data for your app testing and demos	Discover tools to use for testing your app with realistic large data sets of simulated data
Mastering app management with Visual Studio Code	Get hands-on using Visual Studio Code for Splunk app management
Integrating AppInspect into your app release process	See how you can add AppInspect automation into your app delivery and release process to ship better apps faster

Thank You!

To learn more about the .conf23 Call for Speakers, visit:

conf.splunk.com