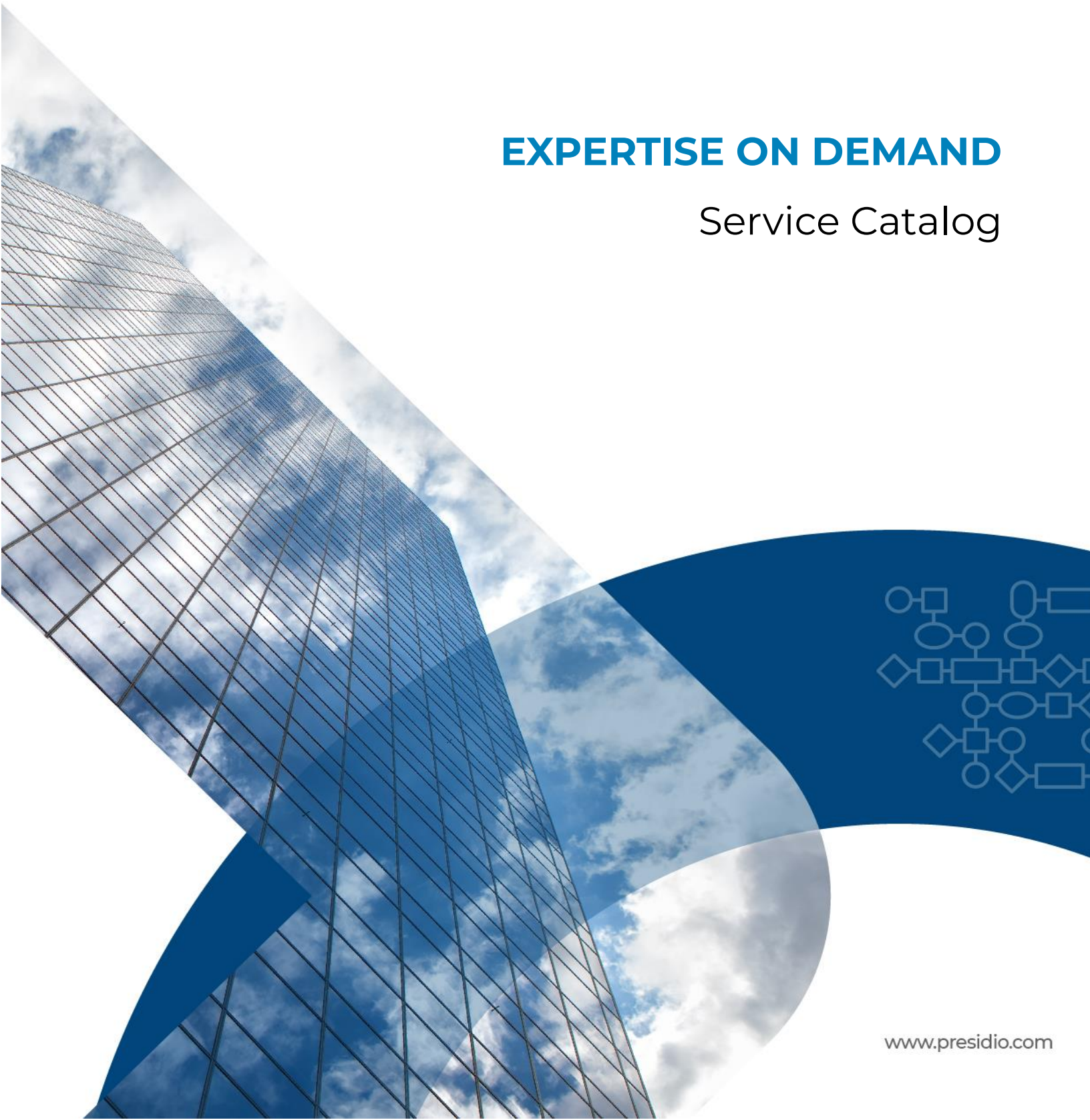
PRESIDIO®

EXPERTISE ON DEMAND

Service Catalog



www.presidio.com

Table of Contents

Searching & Dashboarding

Schedule a call with our team to cover common content-focused tasks in the Splunk Web interface, including searching, dashboarding, and tuning search-supporting configurations.

Searching	Create searches to extract insights from indexed data. Learn new search commands and syntax for growing search capabilities.
Field Extractions	Make new fields available for use in search activities.
Lookup Files, Collections, and Definitions	Create and modify lookup reference tables for enriching or filtering data.
Tags, Event Types, and Macros	Support searching across datasets and alignment with datamodels using tags and event types. Leverage modular SPL operations with search macros.
Data Models	Configure acceleration and leverage datamodels in searching to improve performance of queries. (Splunk Common Information Model datamodels only)
Alert Actions	Modify the automated outcomes of searches meeting alerting criteria. (Default alert actions only)
Dashboard Configuration	Visualize data for executive reporting, detailed investigations, and simplified consumption of complex data. (Classic, Dashboard Studio)
Navigation Menus	Ensure applications promote productive user workflows through view navigation.

System Administration

Expand your admin team by using EOD to handle everyday Splunk administration tasks. Discuss and establish workflows and capabilities to simplify maintenance.

User Account Management and RBAC	Create/modify user accounts and configure permissions for role-based access control supporting customer-specific requirements.
Splunk Add-ons	Install, configure, and update Splunk add-on knowledge objects and permissions to ensure the right users are getting the most out of data in Splunk.
Authentication Methods	Configure Splunk's native authentication methods to meet organizational policies and support account management strategies.
Distributed Monitoring Console	Configure a single console for observing and investigating performance of distributed Splunk servers.
Splunk Version Upgrade	Upgrade environment to leverage the latest features of Splunk Enterprise. **This task requires scoping to ensure enough service hours are available for completion of the upgrade, particularly in distributed environments.**

Data Administration

Make the most of the data in your environment by ingesting data for alerting, dashboarding, and investigations. Get assistance with best-practice configurations for forwarders.

Data Onboarding	Get new data in, configuring inputs for new data feeds through standard Splunk inputs or documented Splunk add-ons. **Custom scripting is not supported.**
Input Configuration Tuning	Handle requirements for parsing unique data sources to ensure usability of indexed data.
Index Configuration	Create/modify indexes supporting access control and data retention requirements.
Deployment Server Management	Create serverclasses to organize forwarders. Remotely manage configuration of forwarders within the Splunk environment.
Forwarder Configuration	Get assistance with new forwarder setup and guidance for common management practices.
Ingest Actions (Splunk v9.x+)	Create Splunk Ingest Actions to filter or manipulate events before ingestion.

Enterprise Security

Ensure supporting configurations are tuned for enabling your use of Splunk Enterprise Security. Explore opportunities to expand detection and investigation capabilities.

Correlation Search Creation, Modification	Tune correlation searches for performance and coverage of targeted security data.
Incident Management Configuration	Modify notable statuses and Incident Review presentation of notable events to support analyst productivity.
Data Model Review	Configure CIM datamodels to support detection needs, defining indexes for optimal performance and tuning of acceleration summary ranges.
Asset & Identity Configuration	Assist with configuration of lookups storing data for assets and identities.

General Troubleshooting

Splunk is complex. If you're experiencing an unexpected behavior that doesn't seem to fall under the listed service categories, you can share information to help us help you.

Diagnostic Testing	Run a Splunk diag to review potential misconfigurations.
Health Check	Run a comprehensive Health Check to get a wholistic view of environmental health with actionable recommendations for remediation and improvement.
Report an Error	Share observations of an issue so the EOD team can assist in identifying the problem.

User Education

We're Splunkers, just like you. We'd love to share our experiences relevant for your Splunk use cases.

Monthly Lunch & Learn Webinar	Get information on the next monthly "Lunch & Learn" webinar, open to all Atlas customers.
Custom Lunch & Learn Session	If you'd like to learn about a specific topic, we can create custom content to meet your needs.