SPLUNK ADMIN SERVICES

BRIGHT

THE SPLUNK ADMIN SERVICE PROVIDES YOU WITH A TECHNICAL PARTNER TO OPERATE YOUR SPLUNK ENVIRONMENT.

Leverage one of Europe's most trusted and capable Splunk teams to get the most out of Splunk.

OVERVIEW

The Splunk Admin Service is a monthly subscription service that allows you direct access to Splunk technical consultants who can administer and manage your Splunk environment so you have free time to focus on your business use cases.

These consultants provide a variety of remote technical services to assist with the overall success of the Splunk development. The service allows you to choose from a predefined service catalogue with offerings within areas of expertise such as Splunk Core, Enterprise security, SOAR, ITSI, Cloud and more.

AREAS OF EXPERTISE

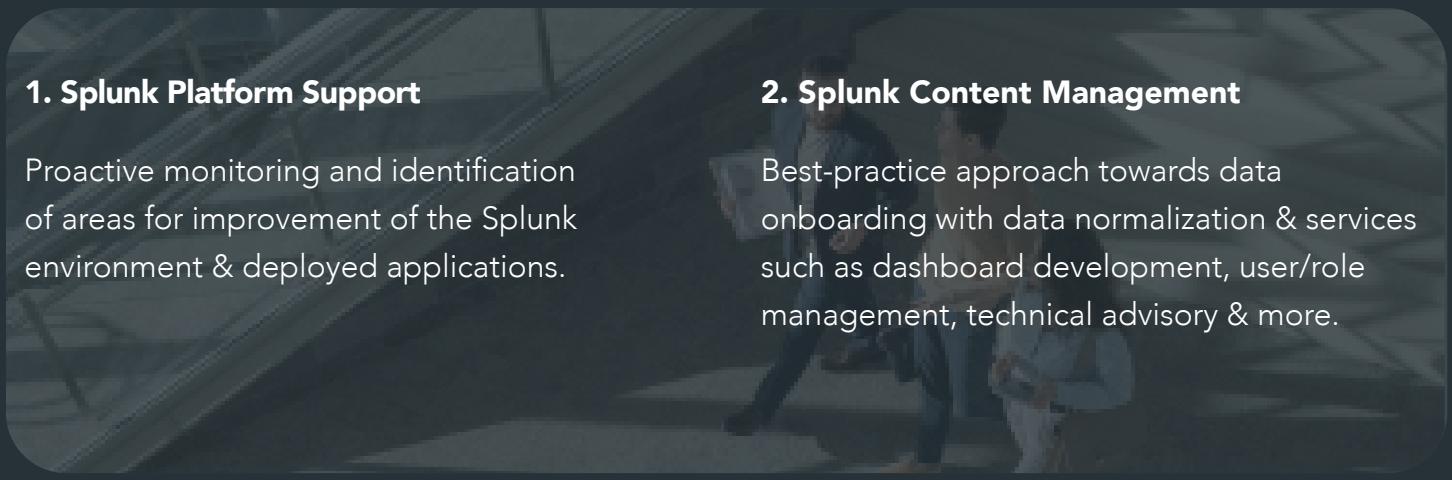
- Splunk Enterprise Security
- Splunk Observability
- Splunk ITSI
- Splunk SOAR
- Splunk UBA
- Splunk Enterprise
- Splunk Cloud
- Splunk Dashboard Studio
- Splunk Supported Apps

BRIGHT

SCOPE OF THE OFFERING

splunk>

The scope of the Splunk admin service includes the following areas:



1. Splunk Platform Support

Proactive monitoring and identification of areas for improvement of the Splunk environment & deployed applications.

2. Splunk Content Management

Best-practice approach towards data onboarding with data normalization & services such as dashboard development, user/role management, technical advisory & more.

1. SPLUNK APPLICATION SUPPORT

SPLUNK ENVIRONMENT HEALTH MONITORING

- Search performance
- Index performance
- Operating system resource usage
- App key-value strore performance
- Search head and indexer clustering
- Index & volume usage
- Forwarder connections, TCP performance
- HTTP Event Collector performance
- License usage

PATCHING & UPGRADES

- Splunk Enterpsie platform updates & upgrades
- Splunk supported applications updates & upgrades

DEPLOYMENT OF SPLUNK ENTERPRISE APPS

- Installation & configuration pf standard Splunk Enterprise apps

LICENSE MANAGEMENT

- Proactive monitoring of license usage
- Advise & configure log collection to optimize license consumption

COMPLEX DISTRIBUTED DEPLOYMENT ADMINISTRATION

- Handling of incidents
- Tackling requests for enhancements and scaling of Splunk Enterprise Environment
- Execute change requests regarding Splunk Enterprise Environment
- Capacity monitoring and planning

BRIGHT

2. SPLUNK CONTENT MANAGEMENT

splunk>

ONBOARDING & NORMALIZATION OF NEW DATA SOURCES TO SPLUNK ENTERPRISE PLATFORM

- Network devices/ infrastructure
- Servers (OS Level)
- DB Servers
- Application servers
- On-Prem applications
- Cloud applications & platforms
- Maintaining the relevant log-source on-boarding documentation

REPORTING SERVICES

- Configuration of alerts & reports
- Configuration of correlative searches
- Customization of "Out of the box" reports
- Analytics tuning & optimization
- Optimization to reduce false positives
- Data Validation
- Data models & development
- Maintaining reports & dashboards documentation / runbooks

DEVELOPMENT

- Development of custom applications
- Development of custom REST/API/DB and other connectors

USER MANAGEMENT

- Creation of groups (accounts)
- Configure access to specific data sets

USE CASE LIFECYCLE MANAGEMENT

- Use case identification
- Log soruces identification
- Development of correlation rules & analytics
- Deploy & retire use case within SE platform
- Documenting of developed use cases

BRIGHT

OUR SPLUNK EXPERTISE IN NUMBERS

splunk>

17+
Years of experience

30+
Splunk Consultants

140+
Splunk certifications completed

190+
Successful projects completed

OUR TEAM

Our team of 30+ Splunk-Certified Consultants will work side by side with you to enable you to unlock the full value of Splunk. Benefit from the expertise of BRIGHT's:

- ✓ Splunk-Certified Core Consultants
- ✓ Splunk-Certified Architects
- ✓ Splunk-Certified Data Admins
- ✓ Splunk Senior Engineers
- ✓ Splunk Cyber Security Consultants
- ✓ Senior Solution Consultants
- ✓ Splunk Security Architect
- ✓ Splunk Security Implementation Managers
- ✓ Splunk Technical Implementation Manager

Our Splunk team won the EMEA Professional Services Partner of 2023 award - a recognition of exceptional performance and our proficiency in professional services implementation.

BRIGHT

OUR TEAM IS HERE TO HELP BRING FASTER INNOVATION & MAXIMIZE YOUR SPLUNK INVESTMENT.

As the 2023 Splunk Professional Services Partner for EMEA, we have enabled multinational enterprises like Mondelez, Paysafe, and A1 Telekom Austria Group to tackle their most pressing business challenges.
Whether you need help finding the right solution, you are just getting started, or you are looking for a partner to support your existing implementation, our team is here to make Splunk work for you.

TRUSTED BY 140+ TOP COMPANIES

A1 Telekom Austria Group · Mondelēz International · Paysafe: · TYVYL · CatalystPay

INTERESTED IN WORKING WITH US?

Contact us at info@bright.consulting and our Splunk team will be happy to get in touch & discuss your needs.

BRIGHT

CONTACT US

London, UK

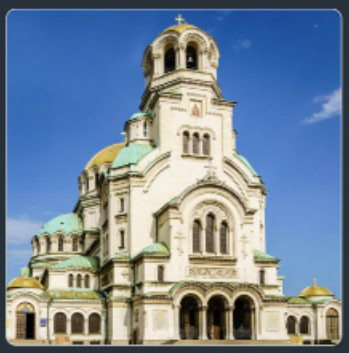
Impact Hub King's Cross
34b York Way, King's Cross
London, N1 9AB

sales@bright.consulting
+44 20 8078 0586

Warsaw, Poland

4 Inflancka str.
00-189, Warsaw,
Poland

sales@bright.consulting
+ 359 29711117



Sofia, Bulgaria

2B Srebarna str.
Mobi Art Building, floor 6
1407 Sofia, Bulgaria

sales@bright.consulting
+ 359 29711117

www.bright.consulting

BRIGHT