



Workshop

Using Splunk
10.- 11. September 2019

Inhaltsverzeichnis

1	Leistungsbeschreibung	2
2	Zielgruppe und Voraussetzungen.....	3
3	Agenda.....	3
4	Hotelinformation.....	5
5	Information zum Veranstaltungsort.....	6

Anhang 1: Anmeldeformular

This Document is classified as Internal.

SPP Handelsges.m.b.H.
Vienna Twin Tower
Wienerbergstrasse 11
1100 Wien, Österreich

T +43 1 597 33 40 – 0
F +43 1 597 33 40 – 40
office@spp.at
www.spp.at

FN 89331w
Handelsgericht Wien
UID ATU 37465907
Steuer Nr 059/0549

Raiffeisenbank NÖ-Wien
Konto Nr 2.378.891, BLZ 32000
IBAN AT55 3200 0000 0237 8891
BIC RLNWATWW

1 Leistungsbeschreibung

Logmanagementsysteme bieten die Möglichkeit, einen zentralen Überblick über alle kritischen Systeme innerhalb eines Unternehmens zu bieten. Dies erhöht die allgemeine Sicherheit und reduziert den Rechercheaufwand bei Security Incidents.

Die Arbeit mit Splunk ist jedoch nicht trivial, das Durchsuchen und Visualisieren von Daten kann schnell unübersichtlich werden.

Aus diesem Grund bieten wir einen 2 Tages Workshop für Splunk an.

Workshop - Fakten

Termin	10. bis 11. September 2019
Dauer	Von 09.00 Uhr bis 16.00 Uhr
Ort	SPC – Gschwandtner Seminare Projekte Consulting GmbH Nordbahnstraße 36, 1020 Wien
Trainer	Zoran Cukic
Teilnehmer Anzahl	Max. 10 Personen
Kosten	Gesamtpreis für die zweitägige Veranstaltung inkl. Mittagessen und Schulungsunterlagen 1.260,- € pro Teilnehmer. Der Preis versteht sich exklusive USt. und Übernachtungskosten.
Sprache	Deutsch

Bitte teilen Sie uns auch mit, wenn Sie grundsätzlich Interesse an einer solchen Schulung haben, aber aus terminlichen Gründen nicht teilnehmen können. Bei entsprechender Nachfrage werden wir weitere Termine anbieten.

Wir möchten Sie darauf hinweisen, dass der genannte Workshop-Termin nur zustande kommt, wenn die Mindestteilnehmeranzahl von 3 Personen erreicht wird. Aus diesem Grund können wir eine fixe Terminzusage erst zum Anmeldeschluss, 1 Woche vor dem Workshop, machen. Sollte der Termin wider Erwarten nicht zustande kommen, werden Sie von uns proaktiv verständigt. Wenn Sie zwecks Flug- oder Hotelbuchung eine frühzeitige Information benötigen, nehmen Sie bitte mit uns Kontakt auf.

2 Zielgruppe und Voraussetzungen

Dieser Workshop richtet sich vor allem an diejenigen Mitarbeiter Ihres Unternehmens, die mit Splunk nur wenig in Berührung gekommen sind, aber das Produkt gerne mehr nutzen würden, oder das Wissen bezüglich der Nutzung von Splunk festigen möchten. Das Ziel des Workshops ist die Vermittlung von Kenntnissen, die für das eigenständige, effiziente Durchsuchen von Daten, das Erstellen von Reports und Alerts sowie die tägliche Arbeit in der Splunk Weboberfläche notwendig sind. Lernen sie außerdem wie man Datenmodelle mittels CIM (Common Information Model) erstellt und wie man bereits indizierte Daten beschleunigt.

Anmeldung / Rückfragen

Das Anmeldeformular bitte ausfüllen und per Fax oder E-Mail an:

- Fax: +43/1/597 33 40 40
- Email: e.froemmel@spp.at

3 Agenda

Änderungen vorbehalten!

1. Einführung
 - a. Überblick der Teststellung
 - b. Nutzen der Tutorialdaten
2. Grundlagen der Suche
 - a. Grundlagen der Suchsprache
 - b. Was ist während der Suche zu beachten?
 - c. Job Inspector
3. Kommandos / Visualisierung
 - a. Datenstruktur Voraussetzungen für Kommandos und Visualisierungen
 - b. Visualisierungstypen
 - c. Erstellen von Charts und Timecharts
4. Geo Map und Single Value Kommandos
 - a. iplocation Kommando
 - b. geostats Kommando
 - c. geom Kommando
 - d. addtotals/addcoltotals
5. Dashboards und Formulare
 - a. Erstellen eines Dashboards
 - b. Erstellen eines Formulare
 - c. Drilldown in Formalararen anpassen und konfigurieren
6. Manipulieren und Filtern
 - a. Manipulieren der Daten mittels eval Kommando
 - b. Wann verwendet man das search und where Kommando?
 - c. Verwenden des fillnull Kommandos

This Document is classified as Internal.

7. Korrelieren von Events
 - a. Was sind transactions?
 - b. Gruppieren von Events
 - c. Gruppieren von Events mit Feldern in einem bestimmten Zeitraum
 - d. Suche mit dem transaction Kommando
 - e. Reporting mit Transactions
8. Einführung in Wissensobjekte
 - a. Was sind Wissensobjekte?
 - b. Freigeben von Wissensobjekte
 - c. Verwalten der Wissensobjekte
9. Felder Extrahieren
 - a. Verwenden des Field Extractors
 - b. Verwenden des rex Kommandos um Felder zu extrahieren
10. Tags und Eventtypen
 - a. Was sind Tags und Event Types
 - b. Erstellen und verwenden von Tags und Event Types
11. Erstellen von Macros
 - a. Was sind Macros und wann verwende ich sie?
 - b. Erstellen von Macros
 - c. Argumente in Macros sinnvoll einsetzen
12. Workflows
 - a. Beschreibung der GET und POST Methode in Workflows
 - b. GET Methode in Workflows verwenden
 - c. POST Methode in Workflows verwenden
13. Erstellen von Datenmodellen
 - a. Was sind Datenmodelle und wie kann ich sie verwenden?
 - b. Erstellen eines Datenmodells
 - c. Erstellen einer Pivot Tabelle
 - d. Beschleunigung von Daten
14. Verwenden des CIM Addons
 - a. Was ist CIM?
 - b. Wissensobjekte um CIM
 - c. CIM richtig einsetzen

4 Hotelinformation

Hotel Ibis Wien Messe

Lassallestrasse 7a, 1020 Wien

Tel.: +43/1/217 700

14 Minuten Fußweg

<http://www.ibishotel.com/de/hotel-2736-ibis-wien-messe/>

Austria Trend Hotel Messe Wien

Messestraße 2, 1020 Wien

Tel.: +43/1/727 27 – 0

22 Minuten Fußweg

This Document is classified as Internal.

<http://www.austria-trend.at/Hotel-Messe-Wien/>

Hotel Nestroy Wien

Rotensterngasse 12, 1020 Wien

Tel.: +43/1/211 400

12 Minuten Fußweg

<http://www.imlauerhotels.com/nestroywien/>

City Hotel Tabor

Taborstraße 25, 1020 Wien

Tel.: +43/1/211 17 - 0

15 Minuten Fußweg

<http://www.city-hotels.at/>

5 Information zum Veranstaltungsort

Seminarort SPC – Gschwandtner Seminare Projekte Consulting GmbH
„Pharos Haus“, A – 1020 Wien; Nordbahnstraße 36, Stiege 1
(Eingang Nordbahnstrasse, Ecke Fugbachgasse)

This Document is classified as Internal.

Anfahrt



Parkplatzsituation

Ausreichende Parkmöglichkeiten sind auf der Straße verfügbar.

Wir möchten sie darauf hinweisen dass der Seminarort in einer Kurzparkzone liegt. Die maximale Parkdauer beträgt 2 Stunden. Kurzparkscheine liegen bei Bedarf an der Rezeption auf.

Der Zeitablauf des Workshops ist so gestaltet, dass das Wechseln der Parkscheine berücksichtigt ist.

Splunk Workshop

Anmeldung an SPP Handels GmbH

Wienerbergstraße 11, 1100 Wien, Tel.: 01/59733 40-11, Fax: 01/59733 40 – 40

Name, Vorname:

Name, Vorname:

Firma:

Anschrift:

Telefon:

Fax:

Email:

Hiermit melden wir uns für den Splunk Workshop für den 13. bis 14. Mai 2019 wie folgt an:

Anzahl der Personen:

Gesamtpreis für die zweitägige Veranstaltung inkl. Mittagessen und Schulungsunterlagen: 1.260,- € pro Teilnehmer.

Preis in Euro, exkl. USt.

Bei Rücktritt bis eine Woche vor Beginn des Workshops stellen wir 50 % der Teilnahmegebühr in Rechnung.
Bei einem späteren Rücktritt müssen wir die gesamte Seminargebühr verrechnen.

Firmenstempel, Datum, Unterschrift

This Document is classified as Internal.

SPP Handelsges.m.b.H.
Vienna Twin Tower
Wienerbergstrasse 11
1100 Wien, Österreich

T +43 1 597 33 40 – 0
F +43 1 597 33 40 – 40
office@spp.at
www.spp.at

FN 89331w
Handelsgericht Wien
UID ATU 37465907
Steuer Nr 059/0549

Raiffeisenbank NÖ-Wien
Konto Nr 2.378.891, BLZ 32000
IBAN AT55 3200 0000 0237 8891
BIC RLNWATWW