

# Projekt: 194805

## Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
1	Anzahl Splunk Dashboard Viele Splunk Dashboard sind aktuell im Einsatz, welche potentiell migriert werden müssen?	20 Dashboards, ca. 300 spezialisierte Suchen
2	BIT Server Hardware Das BIT bietet folgende Server an Large, Medium und Small. Ist es möglich einen XLarge Server mit 48 Cores und 512 GB RAM einzuführen und wie sieht da der Preis dafür aus. Server mit 48 Cores und 512 GB RAM sind heute State-Of-Art Server für solche Use Cases.	Nein, das ist nicht möglich, weil im aktuellen BIT-Portfolio z.Zt. kein solches Produkt vorhanden ist. Es können jedoch z.B. zwei Large Server eingesetzt werden. Dies ist jedoch kein Präjudiz für die spätere Lösung.
3	OP BA02 - Migration des bestehenden Systems Wir gehen richtig in der Annahme, dass keine Logdaten aus Splunk übernommen werden müssen? Die original Logdaten könnten bei Bedarf aus dem Archive nach indexiert werden.	Ja, das ist zutreffend. Wir gehen davon aus, dass es einen 90-tägigen Parallelbetrieb geben wird und dann die alte Lösung abgeschaltet wird.
4	Ungeklarheiten Kapitel 3.2.5 / 5.1 / 6.2.3 / 6.2.5 Im 00_19047_Pflichtenheft sind OP 7.4 und OP 8 nicht konsequent aufgeführt bzw. vermutlich korrigiert worden. Gilt ebenfalls für Kapitel 3.2.5 d). Leistungsumfang 4 ist dort identisch mit 3.2.5 e). Es sieht aus, dass OP7.4 in OP 8 überführt worden ist.	OP 7.4 und OP 8 sind insofern identisch als sie beide den Bezug von zusätzlichen Funktionen im Umfang von max. 40% der Investitionssumme regeln. OP 7.4 bezieht sich auf alle anderen Ämter innerhalb der Bundesverwaltung, OP 8 bezieht sich auf das BIT.
5	ZK14 Call in andere Applikationen auslösen Was soll anschliessend mit dem abgefragten Systemverantwortlichen geschehen? Welche Verwendung hat dieser dann?	In erster Line dient dies zur visuellen Information. Dies würde für weitere Abklärungen verwendet. Dient in den meisten Fällen als Lookup Table.
6	Referenzen Subunternehmer Ein Subunternehmer (z.B. Software und Lösungslieferant) bringt Architektur und Engineering Leistungen ein, also wichtiges Know How für die Umsetzung. Sind Referenzen eines solchen Subunternehmers ebenfalls zugelassen?	Ja, wenn der Subunternehmer dann auch tatsächlich bei der Erfüllung des Angebots zum Einsatz kommt.
7	Anzahl Logfile Typen Wieviele unterschiedliche Logfile Typen gibt es im heutigen System, welche verarbeitet werden?	Ca. 10 unterschiedliche Typen von Logfiles, mit Variationen ca. 15.

## Projekt: 194805

### Projekttitel der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
8	•Bei der Ausschreibung handelt es sich um ein «Logdatenanalyse-Werkzeug» und das Thema «IT-Security» wird nur nebensächlich genannt. Bei den Optionen für die nächste Jahren kann verstanden werden, dass es sich bei dieser Ausschreibung um eine SIEM Lösung handelt (IT-Security Management). Bitte erläutern Sie ob bei dieser Ausschreibung ein «IT-Security Lösung» im Mittelpunkt steht, oder ob es sich primär um ein «Logdatenanalyse-Werkzeug» handelt.	Gesucht wird ein allgemeines Logdatenanalyse-Werkzeug als Plattform. Darauf sollen dann Anwendungen für den Betrieb, präventive Massnahmen, KI, Machine Learning, Statistik, Monitoring und Security u.a. betrieben werden. Ein SIEM-Tool wäre zu spezifisch auf Security zugeschnitten, was aber nicht heisst, dass nicht die Security einer der grössten Nutzniesser des Werkzeugs sein wird (auch schon im bestehenden System).
9	Ist das Ziel, die vorhandene Logdatenanalyse-Lösung (SPLUNK) weiterhin zu verwendet oder wird diese Applikation vollständig abgelöst?	Ziel ist die vollständige Ablösung der heutigen Anwendung (jedoch allenfalls mit demselben Tool).
10	Können Standard HW-Appliances (x86 Intel) angeboten werden, die nicht HPE sind?	Ja, aber die Berechnung im Preisblatt für andere x86-Hardware basiert auf den aufgeführten Referenzpreisen. Siehe Kap. 1.7 Hardware im Preisblatt. Der Preisvergleich wird auf Grund der BIT-Hardware errechnet. Alternative Angebote werden nur als Lösungsvorschlag für die Umsetzung eines Projekts in Betracht gezogen. Ausgenommen von dieser Regel sind Appliances, die nur für diesen Zweck verwendet werden können. Für diese wird der Rack-Platz entsprechend der Höheneinheiten verrechnet.
11	Muss die Log Management Lösung Mandantenfähigkeit zur Verfügung stellen?	Ja, gemäss TS17 muss das Logdatenanalyse-Werkzeug mandatenfähig sein.
12	Brauchen parallel 150 aktive User die Lösung?	Ja, im Endausbau muss auf Stufe BIT mit 150 parallelen aktive Usern gerechnet werden (BA 01). Im bestehenden System sind es momentan ca. 30.
13	Cloud-Fähigkeit (Private Cloud), was ist da alles gemeint?	Die Strategie des Bundes ist es, möglichst viele Projekte (oder Teile davon) in der eigenen Cloud (HPE Helion) zu betreiben und von einem rein dedizierten System abzukommen.
14	Welche Cloud Lösungen müssen angebunden werden?	Grundsätzlich sind keine Cloud-Anbindungen vorgesehen (siehe Frage 13).

# Projekt: 194805

## Projekttitel der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
15	„Das Logdatenanalyse-Werkzeug erlaubt die Verrechnung der Ressourcen Rechenzeit, Speicherplatz und Netzwerk-Bandbreite an einzelne User oder Gruppen von Usern.“ # Was soll hier genau erreicht werden?	Ziel ist die präzise und möglichst verursachergerechte Verrechnung interner Leistungen.
16	Anhang_1-3_Kriterienkatalog, EK20 Eignungskriterium „Remote-Zugriff“: Wird für den Fall eines Incidents Remote Access gewährleistet oder muss jeglicher Support vor Ort geleistet werden?	Nein, siehe EK20: jeglicher Support muss vor Ort gewährleistet werden können.
17	Pflichtenheft, OP BA02, Schulung: Muss es sich bei der Zertifizierung um ein offizielles Zertifikat des Herstellers der Logmanagement Lösung handeln?	Wenn ein entsprechender Ausbildungstrack des Herstellers existiert, wäre ein Zertifikat des Herstellers wünschenswert. Spezifisch auf das BIT ausgerichtete Schulungen wären aber als Ergänzung ebenfalls gewünscht.
18	Pflichtenheft, Kapitel 3.2.5, Was ist der Unterschied der Option 3 im Vergleich zu Option 1 und 2? Möchten Sie mit Options 3 die Kosten zum Ausbau der weiteren 1000GB Schritte ab 3000 GB/Tag erhalten?	Option 3 gilt ab 1000 GB, nicht ab 3000 GB. Wir möchten folgende gestaffelte Bezugsvarianten bezüglich Leistungsfähigkeit abbilden: - BA01, OP1, OP2, OP3, ..., OP4 - BA01, OP1, 2 x OP3, OP3, ..., OP4 - BA01, 3 x OP3, ..., OP4 - BA01, OP4
19	Anhang_5_Preisblatt: Kann die BIT Standard Hardware angepasst werden, konkret Server Medium und/oder Large auf 48, bzw. 64 Cores erweitert werden?	Siehe Antwort auf Frage 2
20	Wo liegt der Fokus des Log-Analyse-Werkzeugs: Auf Log-Analyse oder sind auch SIEM-Funktionalitäten (Korrelation, Echtzeit-Analyse, usw.) gewünscht?	Siehe Antwort auf Frage 8. Wir wollen eine allgemeine Basis-Funktionalität. SIEM-Funktionalitäten würden durch Optionen 7.4 und 8 abgedeckt falls sie kostenpflichtig wären. Wir erachten Korrelation, KI und Echtzeitanalyse nicht als reine SIEM-Attribute.
21	Mit welchen Inhalten stellt der Log-Sammler die Daten (in der Linux File-Struktur) dem Log-Analyse-Werkzeug zur Verfügung? (RAW-Daten, inkl. Destination IPs usw. ...)	Es muss mit beliebigen Formaten (XML, JSON, Text) gerechnet werden, momentan ist die Grundstruktur fast immer Syslog, es gibt aber auch Multiline-Logs, UTF8 und auch andere Sonderzeichen. Anbindung via NFS-Share.
22	Gemäss Pflichtenheft müssen alle bestehenden Monitoring, Dashboards, etc. und Analysen übernommen/neu erstellt werden. Könnten Sie bitte die Bestehenden zur Verifikation zur Verfügung stellen.	Nein, das ist aus Security-Gründen nicht möglich.

# Projekt: 194805

## Projekttitel der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
23	Wie soll auf den Log-Sammler zugegriffen werden (tail -f oder gibt es RestAPI)? Oder werden alle Logs via syslog an das neue System weiter geleitet?	Die Daten stehen auf einem NFS-Share zur Verfügung (siehe TS03, ZK15). Alternativ kann auch SMB angeboten werden. Die Daten werden nicht via syslog an das neue System geliefert.
24	Wenn die Daten auf dem Logsammler 90 Tage zur Verfügung stehen und für 2 Jahre archiviert werden, können die Daten auf dem Log-Analyse-Werkzeug auch nach 90 Tagen gelöscht werden, korrekt?	Ja, das ist zutreffend.
25	Können die archivierten Daten (2 Jahre) auch für Analysen genutzt werden (z. B. einfache forensische Analysen)?	Ja, das wird heute schon so gemacht. Die Daten müssen jedoch zuvor wiederhergestellt werden.
26	Ist es zulässig, wenn die Produktschulungen ,inkl. Hersteller-Zertifizierungen von einem zertifizierten Trainings-Center, welches vom Hersteller empfohlen wird, erbracht werden?	Siehe Kap. 3.2.5, BA 02. Die Schulung durch Subunternehmer ist zulässig sofern sie die Vorgaben gem. Kap. 3.2.5, BA 02 erfüllen. Die Gesamtverantwortung liegt jedoch beim Anbieter.
27	Aktuell sind wir in Abklärung, ob unser Hersteller ein Pricing für "unlimitiertes Lizenzvolumen" anbieten kann. Wie wichtig ist dieses Kriterium?	Es handelt sich um ein Pflichtkriterium (es müssen alle Optionen angeboten werden, s. Kap. 8.2.6 im Pflichtenheft, Ausschluss von Teil-Angeboten).
28	EK03: Gelten Referenzprojekte, welche von einer Konzerngesellschaft (Muttergesellschaft oder Schwesterngesellschaften) erbracht wurden?	Ja, allerdings nur, wenn dann auch diese bei der Erfüllung des Angebots als Subunternehmer zum Einsatz kommen und im Angebot als solcher aufgeführt wird.
29	EK03: Gelten Referenzprojekte, welche vollständig durch den Subunternehmer erbracht wurden?	Ja, allerdings nur, wenn dann auch diese bei der Erfüllung des Angebots als Subunternehmer zum Einsatz kommen und im Angebot als solcher aufgeführt wird.
30	EK03: Gelten drei unterschiedliche Referenzprojekte beim gleichen Kunden?	Ja, allerdings nur, wenn sich die Projekte inhaltlich deutlich voneinander unterscheiden und sie in unterschiedlichen Abteilungen/ Divisionen realisiert wurden.
31	Anhang_5_Preisblatt: Sind in den Positionen SHO111-SHO115 die Datacenter-Netzwerkkosten enthalten?	Ja, darin sind alle Betriebskosten enthalten.
32	Optionen Generell: was sind die Auswirkungen, wenn man einzelne Optionen nicht anbieten würde. Bedeutet dies aufgrund der Punktevergabe automatisch den Ausschluss?	Siehe Antwort zu Frage 27.

# Projekt: 194805

## Projekttitel der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
33	(OP BA02) Schulung mit Zertifizierung Ist eine offizielle Zertifizierung via des SW Herstellers gefragt oder eine in-house Zertifizierung nach den Richtlinien des Pflichtenheftes?	Siehe Antwort auf Frage 17.
34	Optionen/Unbegrenzt Datenvolumen lizenziert Für UVAs (unlimited volume agreements) liegt normalerweise eine max.Volumenschätzung zugrunde. Gibt es irgendwelche maximalen Volumina, mit denen wir rechnen könnten (z.B. bis zu 20TB innerhalb der nächsten 5 Jahre o.ä.)?	Aktuelle Schätzung: Für das BIT 5 TB pro Tag (siehe Kap. 3.2.3, Tab. 2 im Pflichtenheft, für den Gesamtbedarf des Bundes das Vierfache des BIT (siehe OP 7), d.h. insgesamt 25 TB pro Tag zum Ende des Vertragszeitraums.
35	Sind Referenzen von einem genannten Subcontractor gültig?	Ja, allerdings nur, wenn dann auch diese bei der Erfüllung des Angebots als Subunternehmer zum Einsatz kommen und im Angebot als solcher aufgeführt wird.
36	Was für Leistungen und Lizenzen ist bei der bereitgestellten Hardware des BITs alles dabei (Wartung, OS, Hypervisor, etc.) bzw. was muss zusätzlich noch offeriert werden?	Die angegebenen Preise enthalten alle Betriebsleistungen ausser das Logdatenanalyse-Werkzeug bis inkl. OS.
37	Nach Analyse der Anforderungen scheinen die meisten Kriterien zum bestehenden (namentlich genannten) Werkzeug SPLUNK zu passen. Liegt die Gewichtung der Ausschreibung darauf, einen neuen günstigeren Anbieter für Splunk zu finden? Oder werden mit der Ausschreibung auch neue und alternative Werkzeuge gesucht?	Ziel der WTO ist es, das Logdatenanalyse-Werkzeug zu finden welches die Anforderungen am besten abdeckt. Die Ausschreibung ist explizit Hersteller- und Tool-neutral.
38	Die angegebene PoC Hardware ist z.B. auch für SPLUNK minimal gewählt. Es macht bestimmt niemandem Spass, wenn ein Werkzeug auf Grund realitätsfremder Hardware Ressourcen kaum nutzbar ist. Ist es möglich im Sinne einer flüssigen und speditiven Präsentation der angebotenen Werkzeuge die Spezifikationen dieser PoC Hardware zu verbessern? (Vorschlag: Auswahl aus bestehenden BIT Cloud Servern, 2x Server Large)	Zielsetzung des PoC ist es, in erster Linie die Funktionalität und erst in zweiter Linie die Leistungsfähigkeit der verschiedenen Lösungen zu testen. Dazu erhalten alle Anbieter dieselbe Ausstattung. Es ist uns bewusst, dass dies nicht dem produktiven Endausbau entsprechen wird.
39	Mit dem Preisblatt wird ein Capex+jährliche Wartung Modell gefordert. Ist es auch möglich ein Subscription Modell (jährliche gleiche Zahlung) anzubieten? Wenn ja, wie soll das Preisblatt in diesem Fall angewendet werden?	In diesem Fall für Capex 0 eintragen und alle Kosten auf die jährliche Wartung aufteilen.

## Projekt: 194805

### Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
40	Wird für die Preisbewertung der TCO der vollen Laufzeit (14 Jahre) herangezogen?	Ja (siehe Preisblatt, Register "Übersicht").
41	Können technische Ausführungen, Experten-Antworten oder auch Dokumentationen in englischer Sprache eingereicht werden?	Ja
42	Wie sind die Spezifikationen der BIT Standard HW beim Storage? (NVMe, SDD, HDD, plus weitere Angaben bitte)	Gemischt: NVMe, SSD, HDD. Ausreichend für den Anwendungsfall.
43	Pflichtenheft Kap 3.2.3, OP BA02: Wo ist der Umfang und der Betrieb der aktuellen Splunk-Lösung beschrieben (angehängte Systeme, Logfile-Beschreibungen, aktuell gespeicherte Datenmenge, individuell konfigurierte Key-Values (Indices, siehe TS25), vorhandene Analysen, Reports und Dashboards (TS21-28), vorhandene Alerts, Netzwerk-Situation (Subnetze der diversen Komponenten, genutzte Ports, ...), aktueller Betriebsaufwand für BIT und Integrator)? Ohne diese Information ist ein Fixpreis-Angebot für OP BA02 nicht seriös möglich.	Diese detaillierten Angaben können aus Sicherheitsgründen nicht herausgegeben werden. Der Anbieter kann von einem 1-Server-System, welches täglich 1 TB Logdaten verarbeitet, ausgehen. Hinweis: Die Daten sind bereits gesammelt und zentral vorhanden. Siehe auch Antwort auf Frage 1.
44	Pflichtenheft Kap 3.2.2 und Kriterienkatalog ZK1: Gibt es genauere technische Angaben, wie die neue Lösung auf der Private Cloud aufsetzen soll? Neben dem Hardware-Typ vor allem Angaben zur Virtualisierungs-SW, Versionsvorgaben, erlaubte Berechtigungen, Vorgaben zu Skalierung und Monitoring etc.	Das BIT betreibt eine HPE Helion Cloud mit ESX als Hypervisor. Es bestehen noch keine genauen Architekturvorstellungen.
45	Kriterienkatalog, TS05: Gibt es Einschränkungen zur Verwendung von APIs? Gibt es Beispiele für solche Drittanwendungen?	Nein, es gibt keine Einschränkungen. Z.Zt. sind nur wenige Drittanwendungen integriert (z.B. mit Python).
46	Kriterienkatalog, ZK11: Ist für das IT Security Management die Anbindung eines SIEM-Tools (Security Information and Event Management) vorgesehen, das Einfluss auf das Referenzmodell hat?	Unsere Daten folgen momentan keinem Referenzmodell. ZK11 fordert daher, dass eine Referenzmodell festgelegt wird, welches die SIEM-Anforderungen auch abdecken kann.

## Projekt: 194805

### Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
47	Kriterienkatalog, ZK28: Verstehen wir das richtig, dass nur der Index archiviert werden muss, ohne dass wir wissen, ob auch die Rohdaten archiviert wurden und ob der Link auf diese noch stimmt? D.h. Index wäre für Analysen nach Recovery wieder verfügbar, Rohdaten aber evtl, nicht mehr.	Ja, das ist zutreffend. Es handelt sich um eine erweiterte Anforderung, mit welcher auf die Archivierung der Rohdaten verzichtet werden könnte. Es ist jedoch nicht ausgeschlossen, dass sowohl Index als auch Rohdaten archiviert werden (mit verschiedenen Zeiten).
48	POC Stellt der Anbieter eigene MitarbeiterIn für den POC oder kann das auch durch den Hersteller des Logdaten Tools wahrgenommen werden?	Die Gesamtverantwortung liegt beim Anbieter. Der Anbieter muss vor Ort sein und darf/kann vom Hersteller eine Person beziehen solange die im Drehbuch für den PoC festgelegten Limiten eingehalten werden.
49	POC Müssen die Personen für den POC beim BIT über eine PSP Zertifizierung verfügen?	Nein, ein unterschriebenes NDA genügt.
50	19047_Anhang_1-3_Kriterienkatalog.xls TS02 GUI: Im Browser lauffähig Alle GUIs des Logdaten-Werkzeugs müssen im Webbrowser (Internet Explorer V 11 oder neuer, Firefox ESR 45.7 oder neuer, Chrome und Edge) lauffähig sein, vorzugsweise HTML5. Frage: Sind alle genannten Browser zu unterstützen, oder ist auch einer der genannten ausreichend?	TS02 beschreibt die generelle Bedienbarkeit der Applikation via Web Browser. ZK22 bildet die verschiedenen Funktionen der Browserhersteller ab. Kein zwingendes Kriterium, gibt aber Zusatzpunkte.
51	21 Einsatz von Dritt- und Open Source Software Liegt im BIT eine Liste in der OSS Komponenten die nicht eingesetzt werden dürfen vor und kann diese bereitgestellt werden?	Nein, eine solche Liste ist beim BIT nicht vorhanden.
52	Dokument Pflichtenheft zum Projekt (19047) Kap 3.2.3, OP BA01: Logdatenanalyse-Werkzeug inkl. benötigte Hard- und Software oder Appliances Frage: Gibt es Randbedingungen für die Plattform (Virtualisierungssoftware, Storage, OS, Netzwerk etc.) können wir davon ausgehen, dass das OS vom BIT als managed Service zur Verfügung gestellt wird?	In den Referenzpreisen des BIT sind alle Kosten der Systeme/Speicher bis und mit OS einberechnet.
53	Dokument Pflichtenheft zum Projekt (19047) Kap 3.2.3, OP BA02: Migration des bestehenden Systems Frage: Umfasst das auch die Übernahme von bestehenden Dashboards, Reports und Suchen, wenn ja, wie viele?	Ja, Übernahme muss berücksichtigt werden. Mengengerüste siehe Antwort auf Frage 1.

## Projekt: 194805

### Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
54	Dokument Pflichtenheft zum Projekt (19047) Kap 3.2.3, OP6 und OP7. Frage: Was umfasst der Betrieb, bzw. was für Basisleistungen können bezogen werden.	Prinzip: Infrastruktur wird durch das BIT betrieben. Der Anbieter stellt nur den Betrieb der Applikation sicher.
55	Dokument: Drehbuch Proof of Concept zum Projekt (19047) Kap 1.5 "Den Anbietern ist jegliche Art des Kontaktes zu anderen Personen als den vom BIT zugewiesenen verboten." Frage: Betrifft das nur Kommunikation bezüglich dieser Ausschreibung?	Ja, betrifft nur die vorliegende Ausschreibung
56	Dokument: Drehbuch Proof of Concept zum Projekt (19047) Kap PP 1.13 / Datenstruktur Frage: Wie sind die strukturierten Datensätze aufgebaut?	Die wird zu Beginn des PoC mitgeteilt (Testdatenbeschreibung). Grundsätzlich: Logs in Textfile Format: Syslog. Logs, abgelegt in Directory-Struktur. Ein File pro Tag und Quelle/System.
57	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 146, TS12 Datenintegrität "Die Rohdaten (Logdaten) können durch das Logdatenanalyse-Werkzeug nicht verändert werden. Die Datenintegrität des generierten Index ist trotzdem durch geeignete Methoden (z.B. digitale Signatur) basierend auf aktueller Technologie (Mindeststandard gemäss Leitfaden für Lieferanten, V 3.0) sicherzustellen." Frage: Wo ist der Leitfaden für Lieferanten zu finden	Die fehlenden Dokumente "IT-Leitfaden für Lieferanten" und "Empfehlungen für den Einsatz von Betriebsumgebungen im BIT" liegen nunmehr bei.
58	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 164, TS17 Mandantenfähigkeit Frage: Wird unter Mandantenfähigkeit nur die Einschränkung des Zugriffs auf Daten und Dashboards basierend auf Rollen verstanden?	Der Anbieter soll erklären, wie er die Mandantenfähigkeit umsetzt. Es sind verschiedene Lösungen erlaubt: Systemtrennung, Rollen, ...
59	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 164, TS17 Mandantenfähigkeit Frage: Dürfen alle Daten in der gleichen Plattform gehalten werden, oder müssen sie aufgrund der Klassifizierung in getrennten Systemen gespeichert werden. Gibt es weitere Anforderungen bezüglich Schutz der Daten?	Es gibt keine unterschiedlichen Schutzklassen weil der Schutzbedarf aller Daten sehr hoch ist. Grundsätzlich ist der höchstmögliche Schutz anzustreben.



# Projekt: 194805

## Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
60	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 176, TS20 Kontinuierliche Datenlieferung/Anzeige Frage: Müssen Daten, die während dem die Suche läuft neu eintreffen, im Suchergebnis angezeigt werden?	Nein (TS 20 behandelt den Fall aller lange laufender Abfragen, bei welchen schon Daten angezeigt werden müssen während die Abfrage noch läuft, damit man zeitnah auf die ersten Resultate reagieren kann).
61	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 216, TS30 Benutzer Frage: von wievielen Suchanfragen pro Stunde für User und Poweruser müssen wir ausgehen und wieviele regelmässige zeitgesteuerte Suchen sind zu erwarten?	Diese Werte sind nicht definiert und dynamisch.
62	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 245, ZK04 Verrechnungsmöglichkeit für Ressourcen Frage: Wie feingranular muss die Verrechnung erfolgen, wie sollen Ressourcen die nicht einem User zugeordnet werden können, z.B. das Einlesen der Logdaten verrechnet werden?	Nicht feingranularer als in ZK04 beschrieben (User, Usergruppe, Rechenkapazität, Indexspeicher und Netzwerkbandbreite). Ressourcen, die nicht einem User zugeordnet werden können, werden auf Basis des Logdatensammlers (Logdatenmenge) verrechnet.
63	Dokument 19047_Anhang_1-3_Kriterienkatalog Zeile 341, ZK27 Storageverbrauch der Indexierten Daten Frage: Welche Anforderungen bezüglich Redundanz und Verfügbarkeit müssen bei der Speicherung der Daten eingehalten werden?	Keine. Das System wird prinzipiell nicht redundant ausgelegt.
64	Frage: Geht es bei Option 6 wirklich nur um 3024 Stunden? Wenn man gemäss Preisblatt in den ersten Jahren 3 bzw. 2 Mitarbeiter zu 18 h pro Monat einsetzt, ergibt sich ein Total von 4320 h.	Ja, es ist davon auszugehen, dass es ab einem gewissen Zeitpunkt zu einem fließenden Übergang in den BIT-Betrieb kommen wird.
65	Subunternehmen Ist der Hersteller des Logdaten Analyse Tools bei einem Anbieter als Subunternehmen aufzuführen?	Das ist abhängig von der geplanten Rolle des Herstellers im Angebot. Falls der Hersteller nicht in die Leistungserbringung involviert ist, müsste er nicht als Subunternehmer aufgeführt werden. Falls er in irgend einer Weise aber involviert sein sollte (Wartung, Support oder dgl.), dann ist er aufzuführen.
66	Pflichtenheft; 5.1 Übersicht Zuschlagskriterien Wir gehen davon aus, dass OP8 und dessen Preis nicht in die Preis Bewertung mit einfließt?	Ja

# Projekt: 194805

## Projekttitel der Beschaffung: (19047) 609 Logdatenanalyse-Werkzeug WTO

	Frage	Antwort
67	OP BA02, Migration des bestehenden Systems Ist es richtig, dass beim einem künftigen Einsatz einer Lösung basierend auf Splunk mit dieser Migration lediglich eine 1:1 Übernahme auf eine neue Plattform zu berücksichtigen ist	Ja (OP 7.4 und OP 8 fließen nicht in die Berechnung ein).
68	Pflichtenheft OP4, Logdatenverarbeitung von unlimitieren GB/Tag und Tabelle 2, Geschätzte Entwicklung der Logdatenmenge Ist es richtig, dass eine unlimitierte Menge an Logdaten (OP4) auf max. 5'000GB und bis ins Jahr 2032 abzudecken ist (Spalte Logvolumen in GB/Tag)	Siehe Antwort auf Frage 34
69	OP 4 - maximale Logdatenmenge in GB pro Tag in Verbindung zu OP8, weitere/max 40% des Anteils der Zuschlagssumme BA01, OP1-OP4; Wenn mit OP4 eine unlimitierte Logdatenverarbeitung ermöglicht wird, von welcher Basis aus sollen max. 40% mehr Volumen für Logdatenverarbeitung kalkuliert werden in OP8?	Die Bezugsmenge ist limitiert auf 40% der zu diesem Zeitpunkt bereits getätigten Investitionssumme in das Logdaten-Analysewerkzeug ((BA01, OP01 bis OP04) x 0.4). Hinweis: Es handelt sich hier nicht um eine Volumenerweiterung sondern um Funktionserweiterungen!
70	Dokument „19047_Beilage_1_Rahmenvertrag.pdf“ Es hat 5 x "Fehler! Verweisquelle konnte nicht gefunden werden"	Verweise im Dokument aktualisiert. Siehe Dokument „19047_Beilage_1_Rahmenvertrag.pdf“
71	Pflichtenheft ap. 3.1.2 Wie viele Logdateien sind heute vorhanden ?	Heute sind mehrere Tausend Logdateien vorhanden
72	Pflichtenheft Kap. 3.1.2 Wie viele Verzeichnisse existieren heute und wie viele Ebenen hat die Verzeichnisstruktur ?	Verzeichnisse: ca. 150 Verzeichnisstruktur: 5-6 Ebenen
73	Pflichtenheft Kap. 3.2.3 Warum ist der geplante Leistungszeitraum für OP-BA02-Migration und OP-BA02-Schulung auf knapp 7 Jahren festgelegt ? In Tabelle 10 (Kap. 3.2.6) wird die Einführung im 2020 festgelegt.	Es ist nur eine Migration geplant. BA02: Hier ist die Schulung relevant, welche kontinuierlich erbracht werden muss. Die Leistungen bitte sinnvoll auf die Jahre verteilen.
74	Pflichtenheft Kap. 3.2.4 Mit wie vielen unterschiedlichen Logdatentypen ist zu rechnen (was bedeutet „mit einer hohen Anzahl“) ?	Z.Zt. sind ca. 15 Typen vorhanden. Bei ca. 500 Applikationen ist damit zu rechnen, dass noch zahlreiche weitere dazukommen werden.
75	Pflichtenheft Kap. 3.2.4 Welche bestehenden Funktionalitäten und Parametrisierungen von Splunk sollen übernommen werden ?	Es sollen alle Funktionalitäten übernommen werden. Siehe auch Antwort auf Frage 1.

## Projekt: 194805

### Projekttitle der Beschaffung: (19047) 609 Logdatenanalyse- Werkzeug WTO

	Frage	Antwort
76	Pflichtenheft Kap. 3.2.4 Müssen Daten aus Splunk übernommen werden ?	Nein, siehe Antwort auf Frage 3.
77	Pflichtenheft Kap. 3.2.4 Wie viele Suchmasken, Dashboards und Alerts müssen übernommen werden ? Was ist mit „weiteren Komponenten“ gemäss Kap. 3.1 gemeint ?	Siehe Antwort auf Frage 1. Weitere Komponenten: Fehlerhafter Verweis (keine weiteren Komponenten vorhanden).
78	Pflichtenheft Kap. 5.1 In der Tabelle 11, Teil ZK Preis, ist die Option 8 nicht aufgeführt. Im Preisblatt im Register „Übersicht“ ist die Option 8 aufgeführt mit Gewichtung 1. Wir nehmen an, dass das Preisblatt stimmt ?	Die Option 8 wurde im Register "Übersicht" aus der Bewertungssumme gelöscht. Zusätzlich wurde im Preisblatt im Register "Option 6" in der Spalte 'Jahr' die Laufzeit von 2019-2032 auf 2020-2033 geändert. Siehe Dokument „19047_Anhang_5_Preisblatt“
79	Pflichtenheft Kap. 6.2.3 In der Tabelle „Beispiel Preisgewichtungsfaktor“ fehlt die Option 8. Warum ?	Die Option wird aus ausschreibungstechnischen Gründen benötigt, nicht um die Preise zu vergleichen (konstanter Faktor von 40% des Gesamtinvestitionssumme, siehe Antwort zu Frage 78).
80	Pflichtenheft Kap. 6.2.5 Im Abschnitt „Zusätzliche Funktionen“ wird „Position 8.1 von OP8“. Hier ist wohl einfach OP8 gemeint, korrekt ?	Es ist ein Unterpunkt von Option 8 gemeint (gleiches Wording mit anderen Optionen).
81	ZK13 Anforderungs Katalog Ist es zulässig für die graphische oder eine Service orientierte Darstellung /Dashboards ein Dritthersteller Tool zu verwenden (Logstash, Kibana, Graphana). Spezieller Gebrauch im Open Source Umfeld?	Wenn die Integration sauber erfolgt ist und die Lösung als einheitliches Paket (Dritthersteller-Tool als Teil des Stacks) funktioniert dann wird ZK13 erfüllt, ansonsten werden dafür keine Punkte vergeben.