

Die Firma terreActive.
Kompetenz in IT-Sicherheit seit 1996.



14. Security Breakfast
terreActive

Herzlich Willkommen

Security Breakfast. Programm.

- 08:30 Begrüssung & Eröffnung Frühstücksbuffet
- 09:00 terreActive AG, Herr Marc-Yves Bächli CEO
Logdaten Management in Unternehmen
- 09:15 terreActive AG, Herr Meno Schnapauff
Splunk Live!
- 10:00 Pause
- 10:15 Swisscom AG, Herr Mika Borner
Splunk bei Swisscom (Bluewin)
- 10.45 Das terreActive Splunk Angebot
Fragerunde / persönliche Gespräche
- 11:00 Abschluss der Veranstaltung

Logdaten Management in Unternehmen

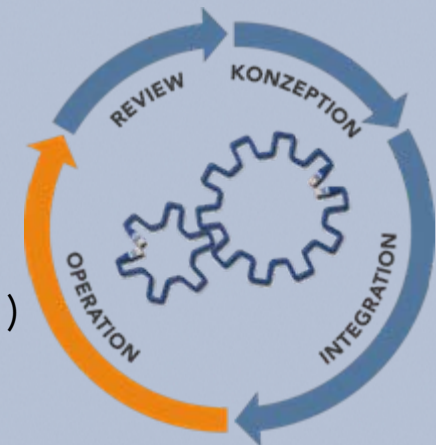
Marc-Yves Bächli, terreActive AG

Die Firma terreActive.

Über uns.



- **Positionierung**
 - IT-Security Engineering und Betrieb als Kernkompetenz
 - Kompetenter Vertrauenspartner für umfassende und nachhaltige IT-Security-Lösungen
- **Facts**
 - Gegründet im April 1996 - **über 10 Jahre Kompetenz in IT-Sicherheit**
 - Firma im Besitz der Mitarbeiter
 - 27 Mitarbeiter (20 Ingenieure) in Aarau
- **Profil**
 - **Unabhängig** und **Lösungsorientiert**
 - Dienstleistungen im IT-Security Lifecycle
- **Fokus**
 - Managed Security Services (2009: 65%)
 - IT Security Monitoring / Log Management (seit 2001)
- **Kunden**
 - Finanz-Institute (40%)
 - Verwaltung und Organisationen (30%)
 - Telecom und IT-Dienstleister (20%)
 - Industrie und Gesundheitswesen/Pharma (10%)



Die terreActive Kunden.

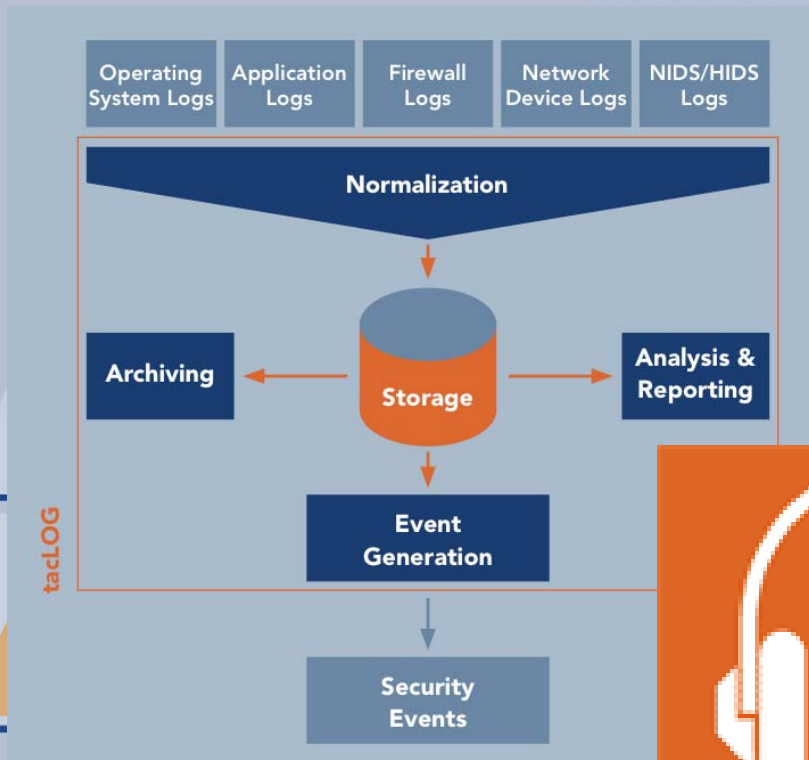
Resultat: Kundenprojekte

Finanz-Institute	Verwaltungen & Organisationen	Telecom / ISP & Dienstleistungen	Industrie	Gesundheitswesen & Pharma
AKB Bank von Roll Bank Sarasin Bank Vontobel BKB Lombard Odier Credit Suisse CSS DZ PB Dreyfus PB IHAG PB Julius Baer LUKB Postfinance Swiss Re ZKB	Abraxas CRB EDA EJPD IGE Kt. Aargau Kt. Basel-Stadt Kt. Bern (Connectis) ShareIT Stadt Aarau Stadt Baden Stadt Zürich (OIZ) Schweizer Post VRSG	Aspectra Bluewin Blue Infinity Cybernet GIA Phion RedIT SBB Sunrise Swisscom Ticketcorner TNT Swisspost Wüest&Partner	AMAG 4B Fenster Basler Lacke Franke KWC Geberit Philipp Morris Ringier Rivella TOTAL Oil Trüb Sadorex Suhner Holding Swiss Swisslog	Inselspital Bern Kinderspital ZH OEKK PDAG Roche Spitalzentrum Biel Spital Thurgau KS St. Gallen SwissEPI Zentrum Sympany UKBB Uni Spital Zürich Medidata

Die Firma terreActive. Logdaten Management.



Am Anfang (ab 2001) war viel Grundlagenarbeit nötig:

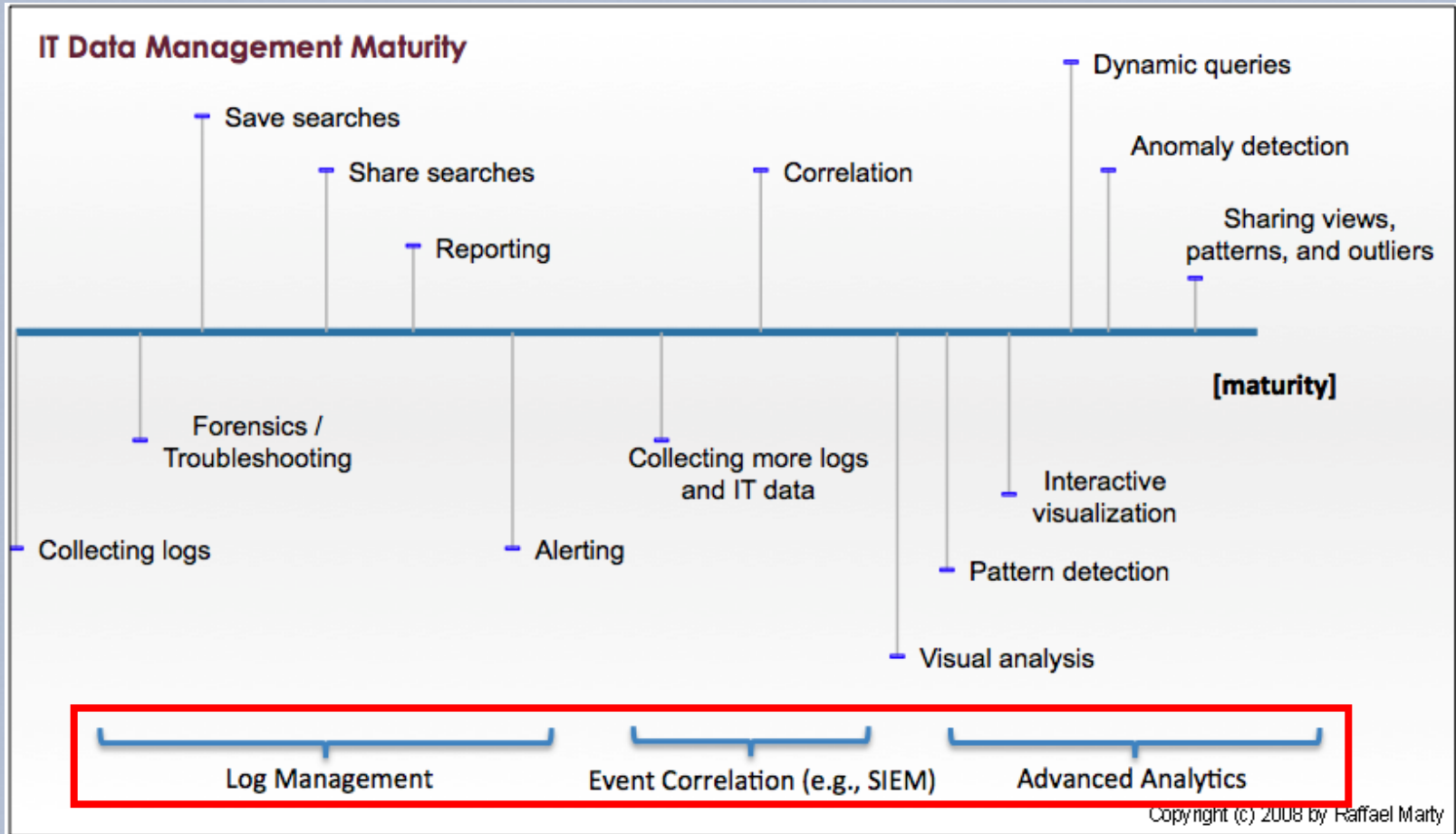


your logs



Die terreActive Kunden.

Logdaten Management: Entwicklungsschritte



Die terreActive Kunden.

Logdaten Management.



- **bis heute**
 - weit über 50 Logdaten Management Projekte realisiert
- **Schwerpunkte**
 - System/Network/Application (real-time) Monitoring
 - Beweissicherung / Log Analyse
 - Entkopplung Systembetrieb <-> Systemüberwachung
 - Security Event Management (SEM)
 - **Ausweitung der Logdaten Management Plattform**
- **terreActive & Splunk**
 - Splunk Architektur unterstützt Konzept der „Entwicklungsschritte“
 - Splunk ist „cool“

[Splunk.com](#) | [Documentation](#) | [Splunkbase](#) | [Answers](#) | [Wiki](#) | [Blogs](#)

splunk> Finding your faults, just like mom.

Die terreActive Kunden.

Fallbeispiel Lombard Odier Privatbank



- **Auswahl von splunk**
 - Testinstallation durch Lombard Odier Engineering
- **splunk Einsatzbereich**
 - Logauswertung zuerst im Network Team (Router Firewalls)
 - Phase 2: Security Team Sicherheitskomponenten
 - Phase 3: Windows Team
- **Erfahrungen mit Splunk**
 - Neues Engineering Team macht Log Management
 - Nutzen: Nachvollziehbarkeit, Transparenz, proaktives Monitoring
- **tA**
 - Splunk Architektur und Integration der Logquellen
 - Performance Tuning
 - Training vor Ort

Die terreActive Kunden.

Fallbeispiel TOTSA



– Auswahl von splunk

- PoC über 3 Monate gegen ArcSight Logger und LogLogic (gleiche HW für alle)
- Inbetriebnahme:
 - ArcSight 10 Tage
 - LogLogic Resultat nicht erreicht
 - Splunk 2 Tage
- PoC gewonnen weil: Inbetriebnahme (Visuelle Ergebnisse), steile Lernkurve, Anpassung an Logformate

TOTSA
TOTSA TOTAL OIL TRADING SA



– splunk Einsatzbereich

- Sicherheitskomponenten

– tA

- PoC durchgeführt vor Ort
- Splunk Architektur (hochverfügbar)

Die terreActive Kunden.

Logdaten Management.



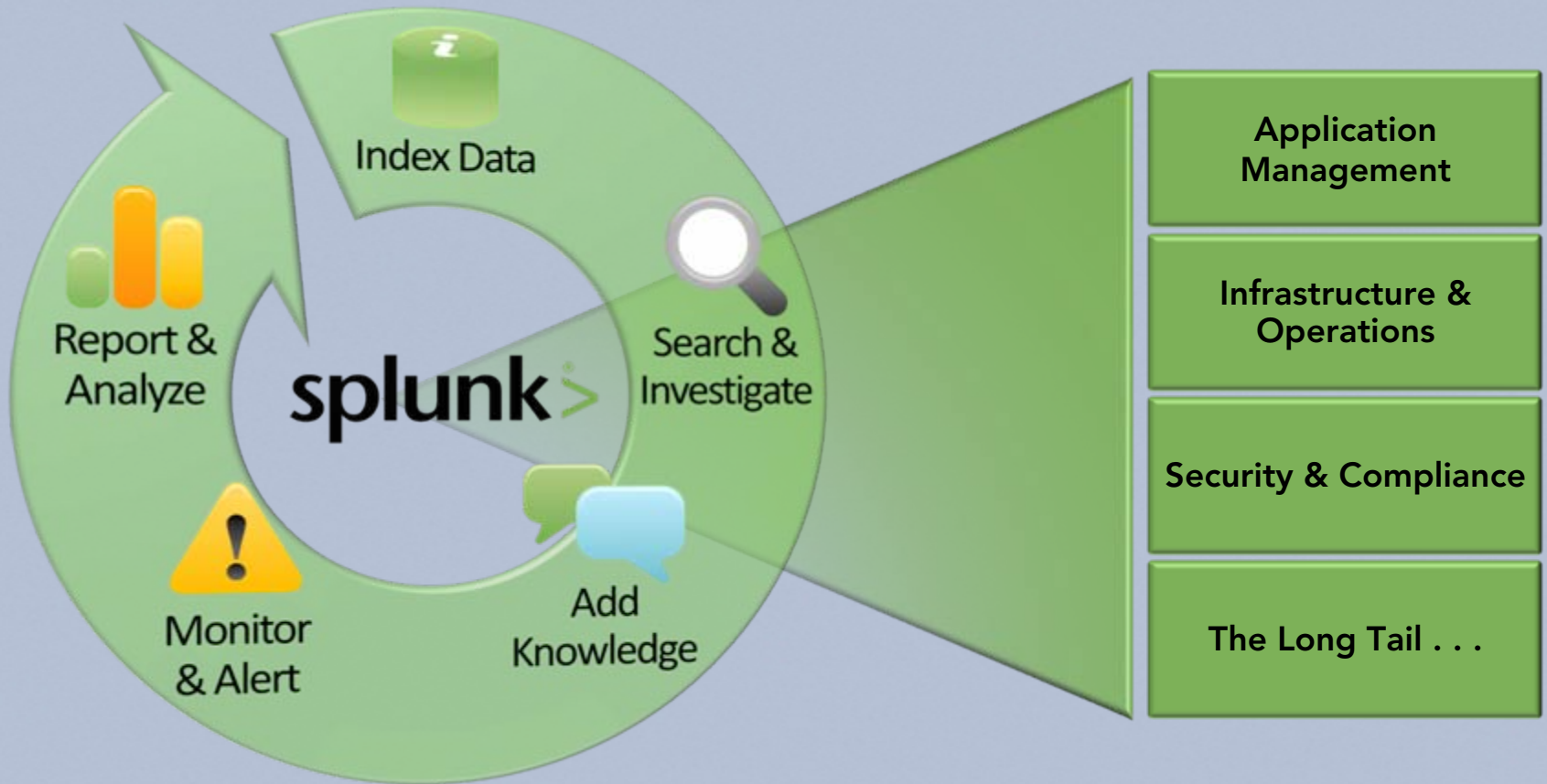
Top-5 Anzeichen, dass Logdaten Management fest verankert ist in Ihrer Firma...

- 5. Kein Systemabsturz mehr wegen „disk full“ provoziert durch Logfiles**
- 4. Zugangsberechtigungen zur Loganalyse
(≠Zugangsberechtigungen zu den Systemen)**
- 3. Sicherheitsrelevante Systeme mit schlechter Log Qualität werden ausser Betrieb genommen**
- 2. Die SW Entwicklungsabteilung erkundigt sich nach dem gewünschten Logformat**
- 1. Die Mitarbeiter entwickeln splunk Apps und Dashboards übers Wochenende**

Splunk Live!

Meno Schnapauff, terreActive AG

Splunk. Funktionsübersicht.



Splunk.

Search and Investigate.



- Powerful ad-hoc search
- Connect related data across different hosts
- Search all your data by time or for anything in the original events
- Even events in multi-line and custom application logs
- Distribute searches across multiple Splunk servers in different datacenters and geographies
- Save, share and schedule your searches



Splunk.

Add Knowledge.



– Enrich collected data with external knowledge

- Classification
Ok/NotOk, Deny/Allow, Normal/Critical
- EventTypes, Tags
- Administrator Know-How, Developer Translation
- External Information Lookup
IP>Hostname resolution, GeoLocation,
UserId>UserGroup, URL>BusinessUnit,
CustomerID>Emailaddress



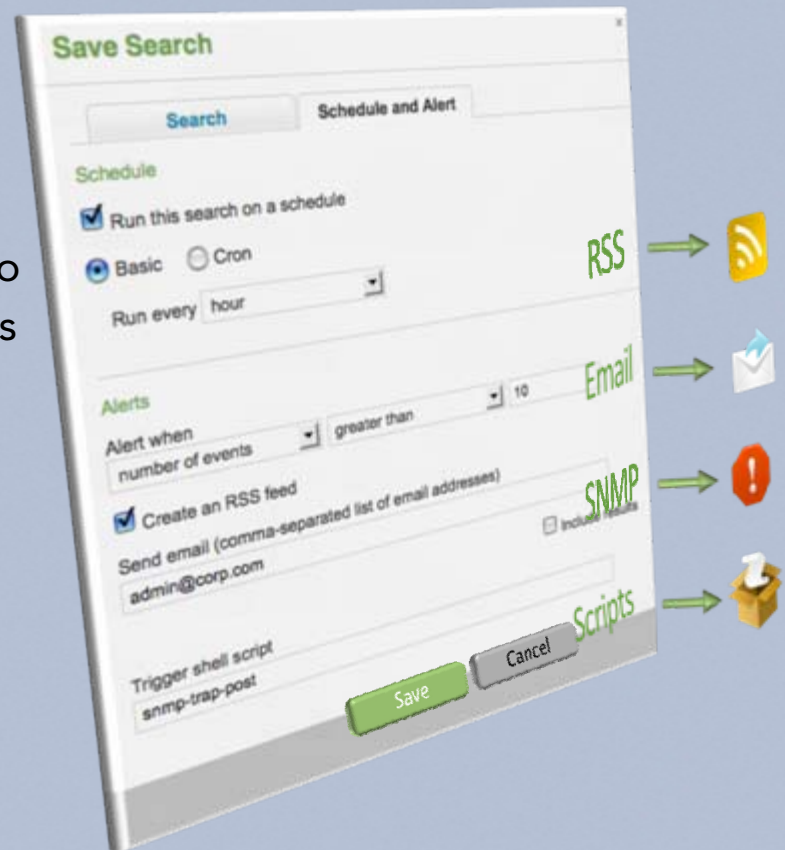
Splunk.

Monitor and Alert.



– Proactively monitor with notifications and action

- Alerts based on scheduled searches
- Notifications and actions triggered by content of search results
- Notifications via RSS, Email or SNMP to other management or security consoles
- Automate routine IT activities such as restarting a server or posting a ticket

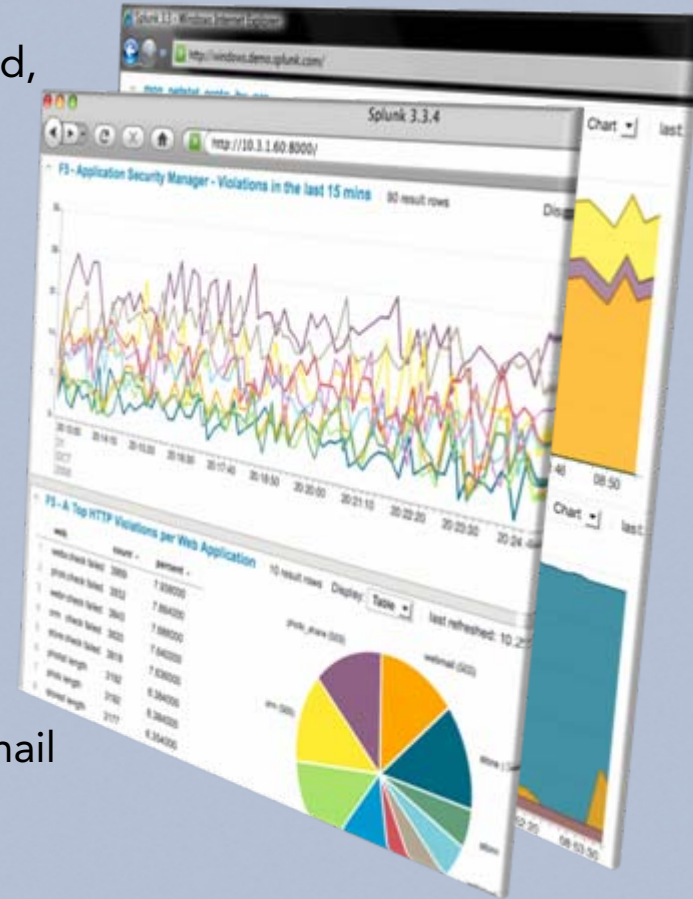


Splunk.

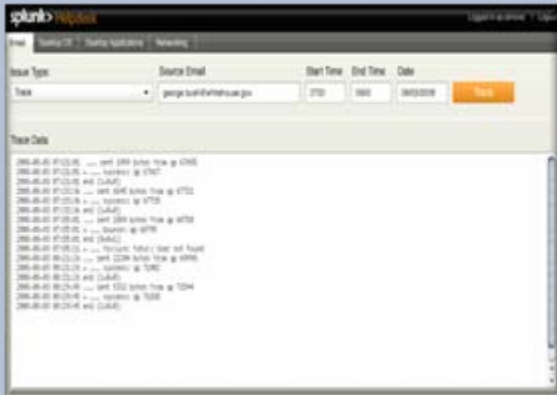
Report and Analyze.



- **Summarize, visualize and analyze search results**
 - Interactive reporting combined with the speed, flexibility and scale of Splunk Search
 - Summaries, statistics, trends
 - Incorporate business data from RDBMSs and other sources
 - Pivot on any fields without complicated schemas or re-indexing of data
 - Schedule and distribute reports via RSS or Email



Splunk. Dashboards and Views for Every Role.



Splunk. LIVE



– Szenario „Harley Shop“

- WebSphere Application Server
- Apache WebServer
- MySQL Database
- LDAP



- Splunk Server
- Splunk WebServer & Browser
- Logdatei Generator



Business

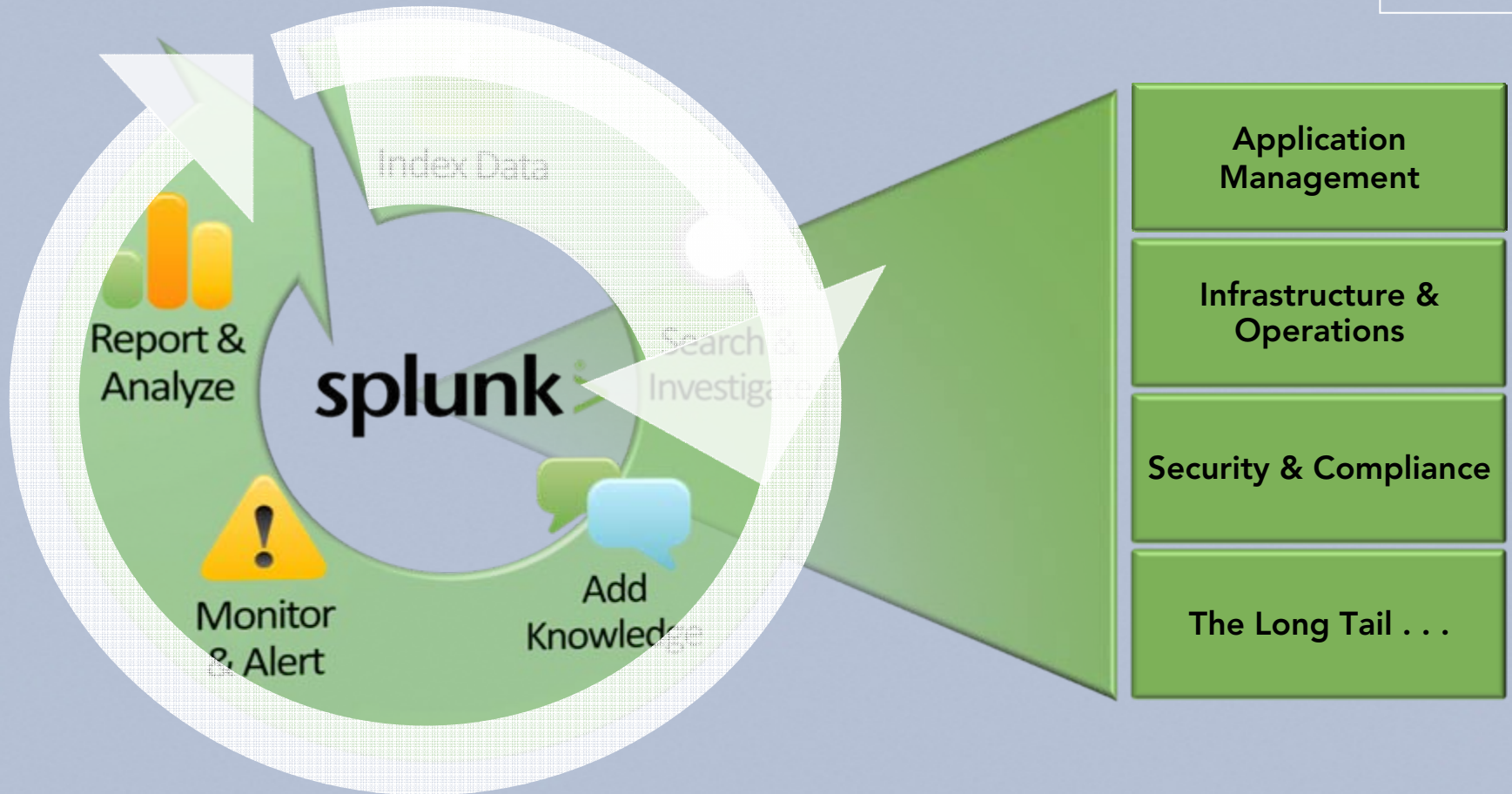


Operations



Helpdesk

Splunk. Funktionsübersicht.



Splunk.

Was bietet terreActive.



- **Log Management Konzept / Workshop**
- **Splunk Architektur**
 - Installations- & Konfigurations- Support
- **Kundenspezifische Reports, Dashboards**
- **Schulung (Deutsch):**
 - Using Splunk
 - Administrating Splunk
- **Betriebssupport für Splunk (MSS)**
- **Proof of Concept (PoC) mit Ihren Daten in Ihrer Infrastruktur**

Splunk.

Proof of Concept (PoC).

- **Splunk in Ihrer Umgebung**
 - Was soll mit Nutzung von Splunk> erreicht werden ?
 - Beteiligte Systeme, Datenquellen, Abteilungen ?
- **Ablauf PoC**
 - Standardisiertes Vorgehen
 - Identifizierung der Erfolgskriterien für PoC
 - Splunk Installation und Einbindung von Datenquellen
 - Der gesamte Funktionsumfang von Splunk> wird gezeigt
 - Einweisung, grafische Reports, Alerts, Dashboard
- **Unser Angebot**
 - 1-5 Tage mit Vorbereitung und Installation vor Ort
 - Support von Splunk Europa / USA wenn nötig



Die Firma terreActive.
Kompetenz in IT-Sicherheit seit 1996.



15. Security Breakfast
terreActive
am 2. November 2010

Besten Dank für Ihre Zeit.
und Ihrem Feedback Formular.