InfoGuard
SWISS CYBER SECURITY

SECURITY & BIG DATA ANALYTICS VON SPLUNK

Überzeugende operative Intelligenz aus Expertenhand

Die Sicherheit und Zuverlässigkeit der IT-Infrastruktur ist für Unternehmen unerlässlich. Ihre IT-Infrastruktur generiert täglich riesige Mengen von Maschinendaten, die Ihnen wichtige Informationen über den Zustand und allenfalls notwendige Anpassungen liefern. Diese Daten zu sammeln, zu analysieren und daraus die richtigen Schlüsse zu ziehen, bleibt in der operativen Hektik oftmals auf der Strecke.

Auf der Basis von Splunk, der führenden Lösung für operative Intelligenz, verschaffen wir Ihnen ein neues Mass an Transparenz und liefern wichtige Ansatzpunkte, mit denen Sie die operative Performance Ihrer IT-Infrastruktur optimieren und die richtigen Massnahmen ableiten können.

- **Sammelt, identifiziert, analysiert und korrelliert Log- und Maschinendaten aus beliebigen Quellen.**
- **Schafft Transparenz in Ihre inhouse, cloud-basierte oder hybride IT-Umgebung.**
- **Liefert wichtige Informationen über die Sicherheit und den Zustand Ihrer Infrastruktur.**
- **Überwacht in Echtzeit alle Ereignisse und KPIs innerhalb Ihrer Infrastruktur.**
- **Reagiert auf Sicherheitsvorfälle mit Echtzeit-Alarmierung und rascher Wiederherstellung des Betriebs.**
- **Bedarfsgerecht erweiterbar über Apps für Sicherheit, IT Operation und Business Analytics.**

InfoGuard ist Premier-Partner von Splunk und verfügt über ein erfahrenes und zertifiziertes Team von Splunk-Engineers. Wir können Sie optimal bei der Integration von Splunk in Ihre bestehende Infrastruktur unterstützen.

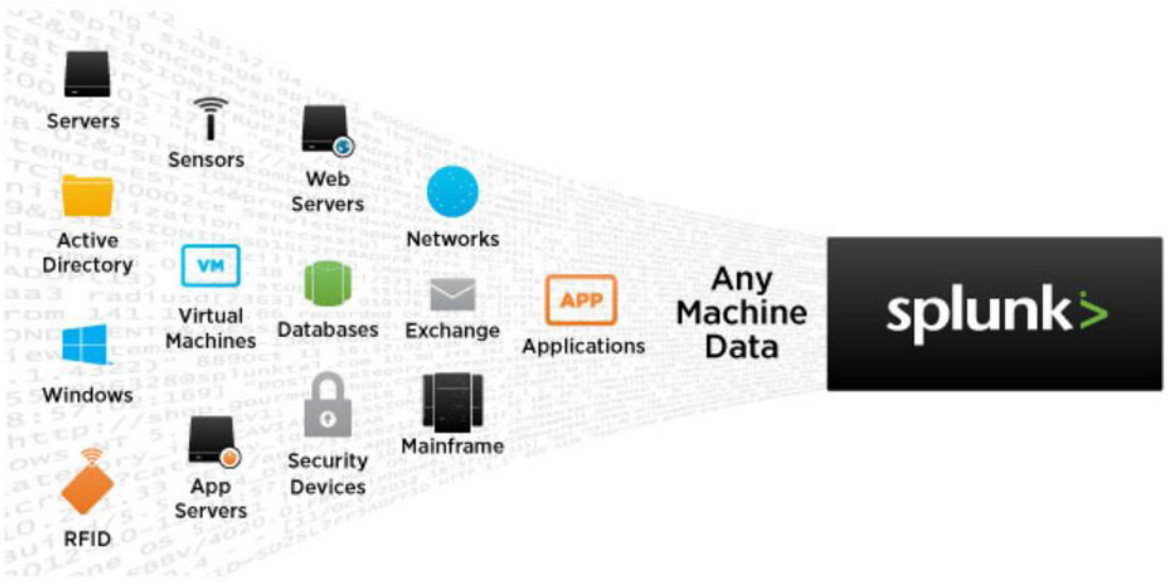
splunk>partner+

Splunk Enterprise – macht aus Maschinendaten Wissen

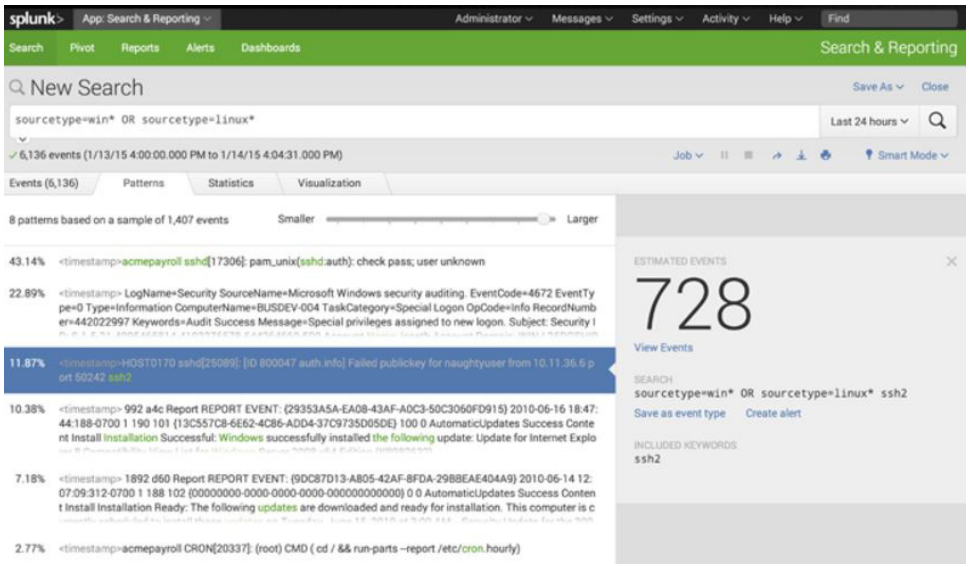
Splunk ist die marktführende Software Plattform für Operational Intelligence. Sie ermöglicht die zentrale Identifizierung von IT-Daten wie Logdateien, Konfigurationen und Geschäftsdaten sowie eine systemübergreifende Suche. Dabei können Daten miteinander verbunden und durch bereits vorhandene Informationen und Wissen ergänzt werden. Dies ermöglicht eine schnellere Erkennung und das Einkreisen von Bedrohungen sowie eine entsprechende Reaktion. Splunk wandelt den grösstenteils ungenutzten Wert der Big Data, die Ihre IT-Infrastruktur, Sicherheitssysteme und Geschäftsanwendungen erzeugt, in wertvolle Informationen und Transparenz.

Die Hauptfunktionen von Splunk im Überblick:

Sammeln und Indizieren von Daten
Splunk identifiziert Maschinendaten aus Logs, Clickstream-Daten, Sensordaten, Übertragungsdaten aus Netzwerken, Webservern, benutzerspezifischen Anwendungen, Hypervisoren, sozialen Medien und Cloud-Services, unabhängig von Format und Speicherort.

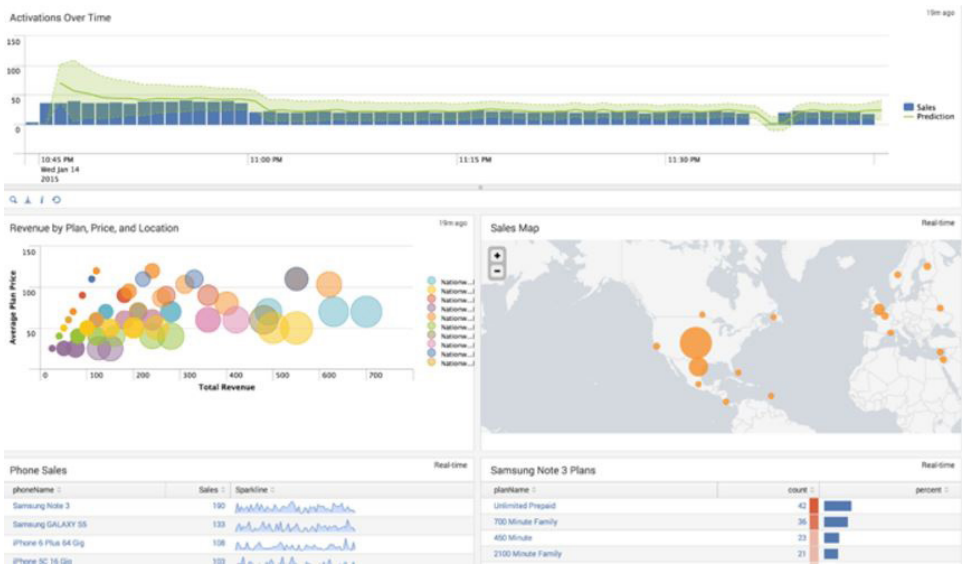


Suchen und Untersuchen
Sie können die identifizierten Daten mit der leistungsfähigen, intuitiven Search Processing Language (SPL) – eine Art Google für Maschinendaten – von Splunk durchsuchen lassen und so Trends, Spitzen und Muster erkennen.

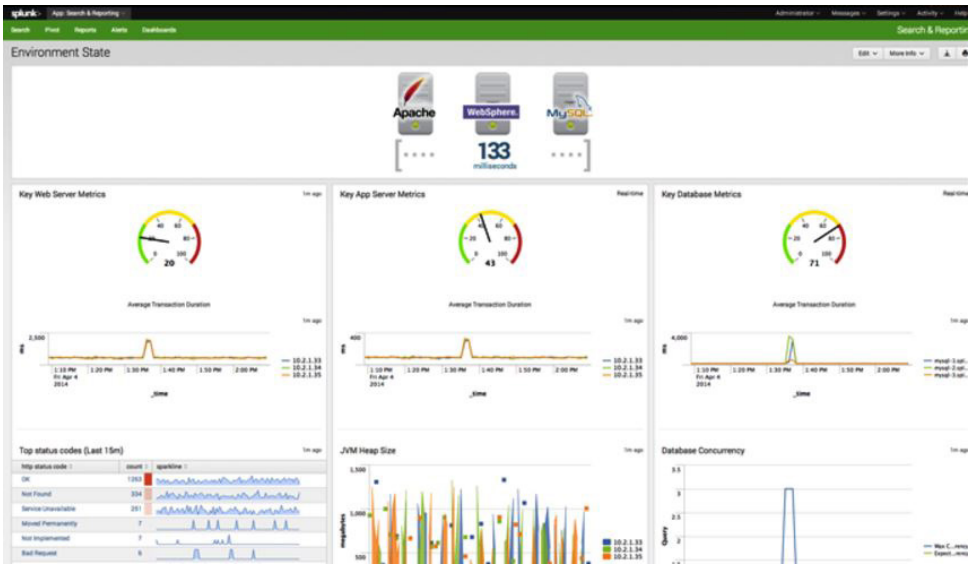


Korrelieren und Analysieren
Splunk macht es leicht, Beziehungen zwischen Ereignissen oder Aktivitäten festzustellen und so aus den Daten wichtige Erkenntnisse zu gewinnen. Dank dem Potential von Machine Learning lassen sich auch automatisch Anomalien und Sicherheitsvorfälle erkennen und entsprechende Gegenmassnahmen auslösen.

Visualisieren und in Berichten zusammenfassen
Alle Suchergebnisse und Analysen werden durch verständliche Grafiken visualisiert und stehen in Echtzeit oder langfristig für Auswertungen, Monitoring und Alarmierung bereit. Mit vorausschauenden Analysen können Sie zudem frühzeitig Trends erkennen, Systemressourcen planen und Workloads voraussehen.



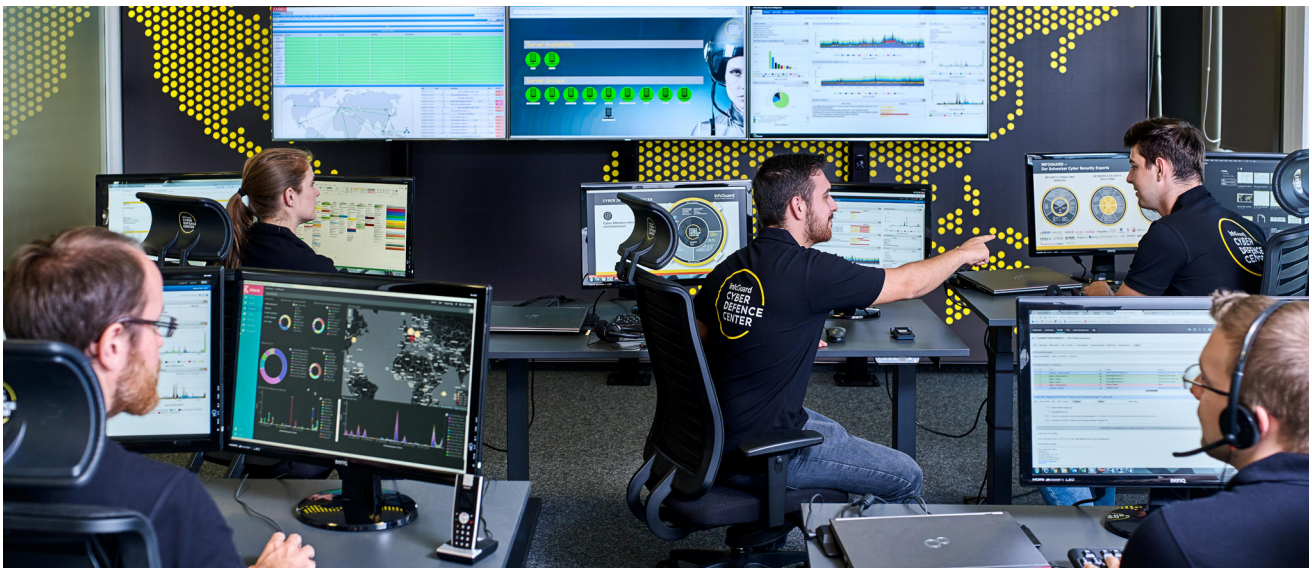
Überwachen und Benachrichtigen
Splunk kann Suchvorgänge in Echtzeitbenachrichtigungen umwandeln und automatisch per E-Mail oder RSS alarmieren. Im Anschluss werden direkt Korrekturmassnahmen ausgeführt, ein SNMP-Trap an die Systemmanagement-Konsole gesendet oder ein Service Desk-Ticket erstellt.



Zugriff von überall
Über jeden beliebigen Standard-Browser haben Sie jederzeit Zugriff auf die Plattform. Mit Splunk Mobile Access (für iOS und Android) können sich Administratoren die bereitgestellte Operational Intelligence unabhängig vom Standort auf mobilen Geräten anzeigen oder den operativen Status überwachen und prüfen lassen.

InfoGuard – Premier Splunk-Partner in der Schweiz

Die Überwachung und der Schutz der eigenen Infrastruktur werden immer komplexer und benötigen hochspezialisierte Fachkräfte. InfoGuard kann Sie dabei mit ausgewiesenen Spezialisten beim Aufbau und Betrieb Ihrer Operational Intelligence unterstützen.



Profitieren Sie von unseren Splunk-Spezialisten:

- Offizieller Splunk Premier-Partner in der Schweiz mit namhaften Kunden
- Ein eigenes Team von zertifizierten und erfahrenen Splunk-Spezialisten für die Architektur, Use-Case Entwicklung, Integration und den Betrieb

- InfoGuard Cyber Defence Center (CDC) mit 7×24 Helpdesk, System-Konfiguration und -Update sowie Monitoring durch qualifizierte Splunk-Spezialisten
- Managed Security und SIEM-Service aus unserem eigenen CDC in der Schweiz
- Level 1 & 2 Support durch InfoGuard; Level 3 & 4 Support in enger Zusammenarbeit mit Splunk
- InfoGuard ist ISO 27001 zertifiziert

Splunk wurde von führenden Marktforschungsinstituten mehrfach im Bereich Security Analytics als Leader ausgezeichnet:

FORRESTER® Gartner IDC Analyze the Future

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Telefon +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Telefon +41 31 556 19 00

INFOGUARD.CH