InfoGuard
SWISS CYBER SECURITY

SECURITY & BIG DATA ANALYTICS BY SPLUNK

Compelling operative intelligence, from expert hands

No enterprise can do without a secure and reliable IT infrastructure. Every day, enormous masses of machine data are generated within the infrastructure; you rely on this information to keep control over its current state, and for any change that may be needed. In the everyday hustle and bustle, the activities of collecting and analysing these data, and of drawing the right conclusions from the results, often fall by the wayside.

With Splunk, the leading solution for operative intelligence, we make available for you a new degree of insight, and offer the relevant approach by which you can optimise the operative performance of your IT infrastructure, and derive the appropriate security measures. This is what Splunk can do for you:

- **Collect, identify, analyse and correlate log and machine data from the sources of your choice.**
- **Create insight in your IT environment, whether it be in-house, cloud-based, or hybrid.**
- **Provide important information on the security and current state of your infrastructure.**
- **Monitor all events and KPIs inside your infrastructure, in real time.**
- **React to security incidents with real-time alarms, and allows for a quick recovery of services.**
- **Can be extended according to requirements, connecting to apps for security, IT operation and business analytics.**

InfoGuard is a Premier-Partner of Splunk, and offers an experienced, certified team of Splunk engineers. We offer optimal support in integrating Splunk in existing infrastructures.

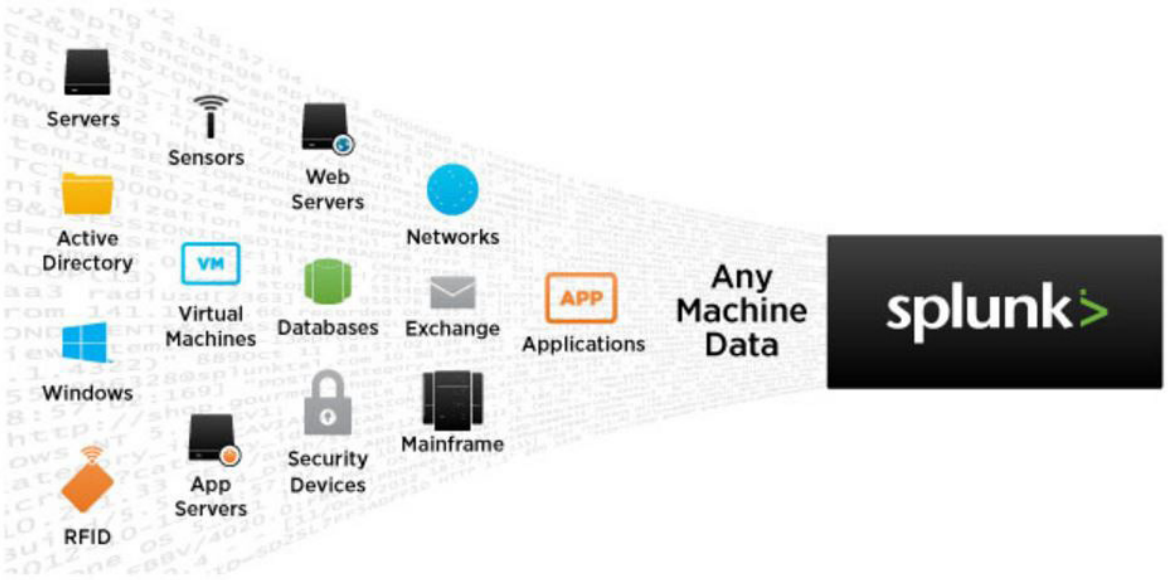
splunk>partner+

Splunk Enterprise – machine data providing the power of knowledge

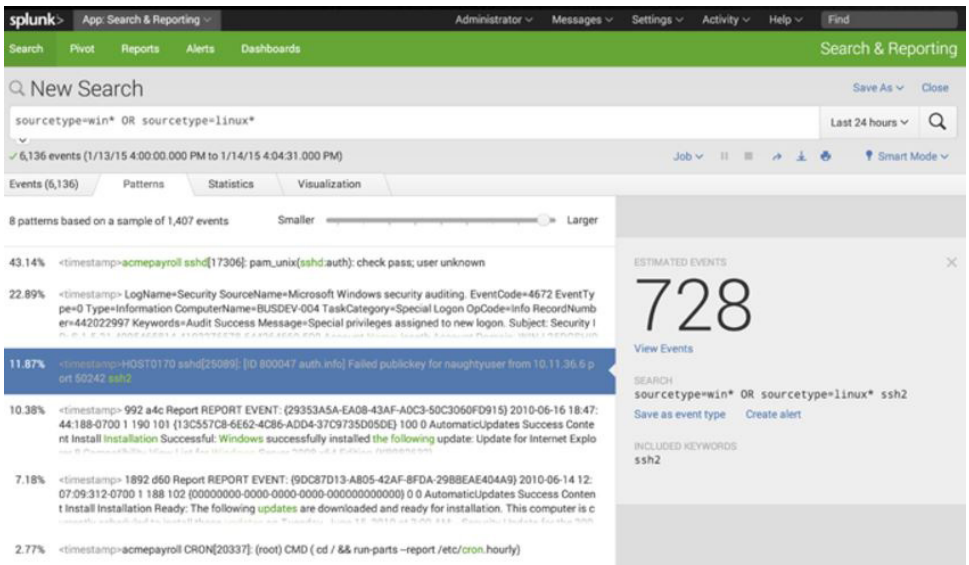
Splunk is the market leading software platform for operational intelligence. It can be used for the central identification of IT assets such as log files, configurations and business data, and also for searching beyond system boundaries. In this way, different data can be connected with one another, and supplemented with information and knowledge that is already available. Threats can be detected and contained with greater speed, and the appropriate reaction taken. Splunk converts most of the unused value of your Big Data, generated by your IT infrastructure, security systems and business applications, into valuable information and insight.

Overview of the main functions of Splunk:

Data collection and indexing
Splunk identifies computer data stemming from logs, clickstreams, sensors, stream network traffic, web servers, custom applications, hypervisors, social media and cloud services, regardless of their format and place of storage.

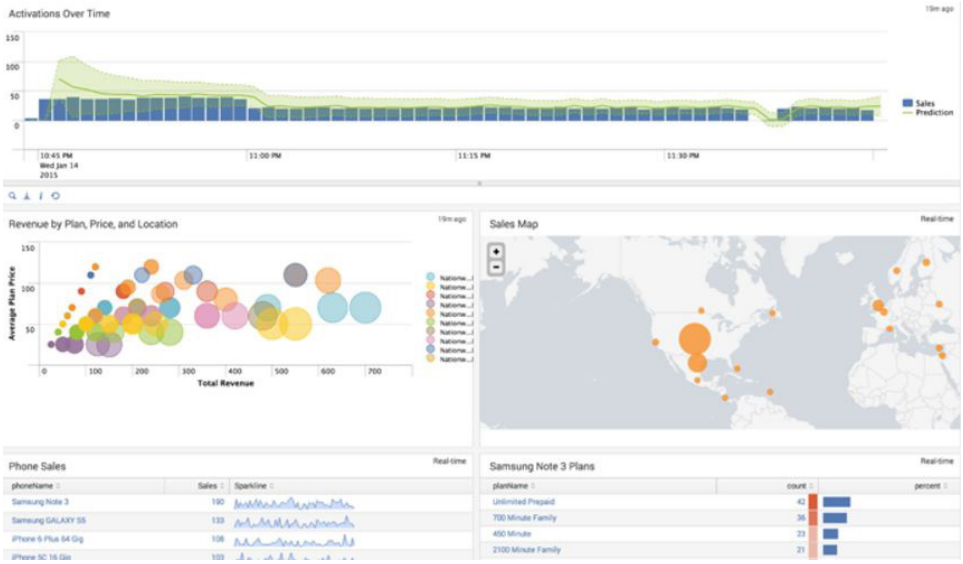


Search and investigation
You can request Splunk to search into the identified data by means of the powerful, intuitive Search Processing Language (SPL), a local Google of sorts, and thus detect trends, peaks and samples.



Correlate and Analyze
Splunk makes it easy to find relationships between events or activities and gain valuable insights from the data. Use the power of machine learning to automatically identify anomalies and incidents.

Display and incorporate into reports
The results of all searches and analyses are displayed in easily understood graphics, and are immediately ready for evaluation, monitoring and alarm-raising; they also stay available for long-term usage. Projections can be made to identify trends, plan for system resources, and predict workloads.

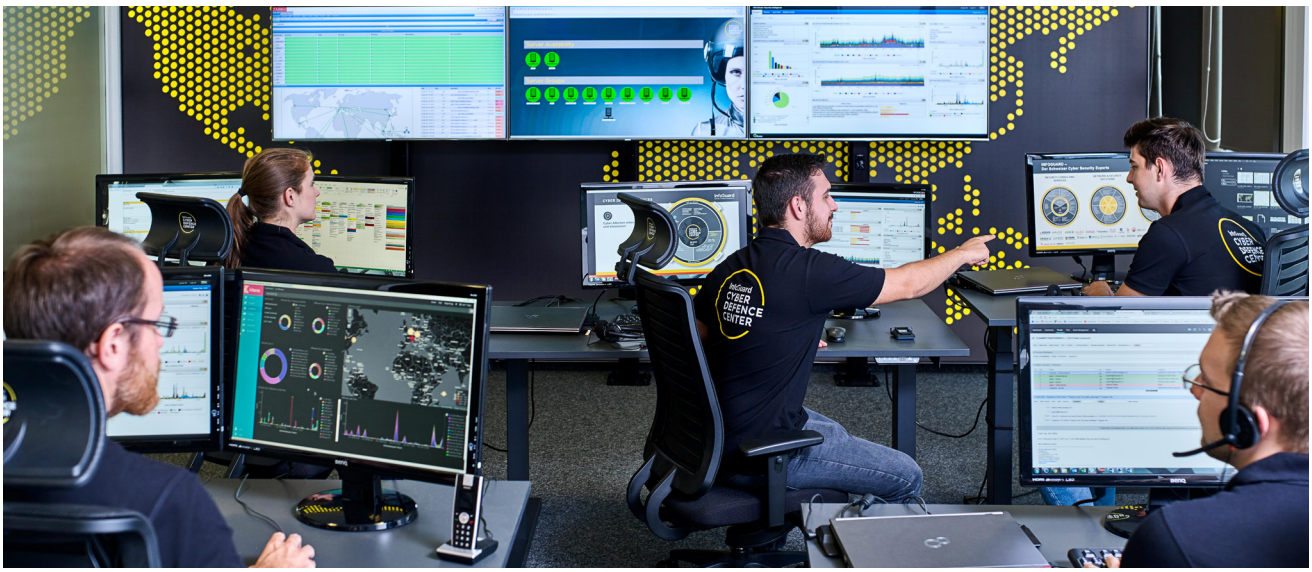


Monitoring and alert
Splunk can transform search procedures into real-time notifications, and issue automatic alerts per e-mail or RSS. As a follow-up, it is possible to directly apply corrective measures, send an SNMP trap to the system management console, or generate a ticket for the service desk.

Access from anywhere
The platform can be accessed at all times through any standard browser. With the Splunk Mobile Access app for IOS and Android, administrators can view existing operational intelligence on their mobile device, regardless of where they are, and monitor and check the status of operations.

InfoGuard – Premier Splunk-Partner in Switzerland

Surveillance and protection of the enterprise infrastructure becomes ever more complex, and requires highly specialised professionals. InfoGuard's certified specialists support you in setting up and running your operational intelligence.



Avail yourself of our Splunk specialists:

- Official Splunk Premier-Partner in Switzerland, with renowned customers
- Own team of certified, experienced Splunk specialists, available to draw the architecture, develop use cases, integrate and operate the system

- InfoGuard Cyber Defence Center (CDC), with 7x24 help desk, system configuration and update, and monitoring performed by qualified Splunk specialists
- Managed security and SIEM service from our own CDC in Switzerland
- Level 1 & 2 support by InfoGuard; level 3 & 4 support in close co-operation with Splunk
- InfoGuard is ISO 27001 certified

Major market research institutes have designed Splunk several times as the leader in the domain of security analytics

FORRESTER® Gartner IDC Analyze the Future

InfoGuard AG
Lindenstrasse 10
6340 Baar / Switzerland
Phone +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Switzerland
Phone +41 31 556 19 00

INFOGUARD.CH