SULZER

Actions Leave Traces

know what to look for

Andrea Klaes | Chief Information Security Officer | October, 2016

Agenda

- About Sulzer
- About Sulzer IT and Sulzer Information Security
- Monitoring Strategy
- Use cases

A Leading Equipment and Service Provider

Sulzer creates reliable and sustainable solutions for its markets oil and gas, power, water, and the general industry

Engineering and application expertise in:

Pumps Equipment
Pump technology and solutions

Rotating Equipment Services
Service solutions for rotating equipment

Chemtech
Separation technology and services, mixing and dispensing systems

Market-Oriented—Globally Operating—Integrated

- Founded in 1834
- Headquarters in Winterthur, Switzerland
- Global Network with over 170 production and service sites
- **Key markets:**
  - **Oil and gas**
  - **Power**
  - **Water**
  - **General industry**

2 971.0

Sales
(in millions of CHF)

14 253

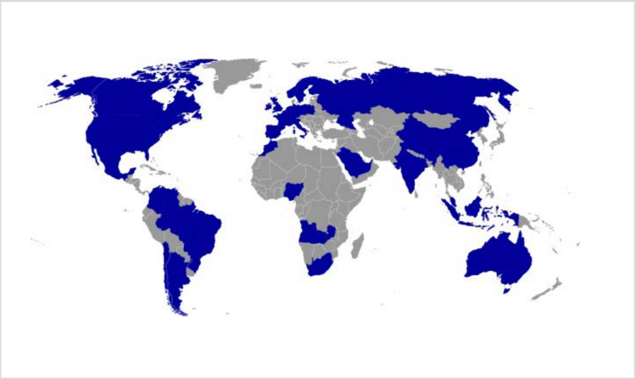
Employees (FTE)
as of Dec 31, 2015

Anticipating Trends for More Than 180 Years

Innovative industry solutions—a strong future commitment

Industrial pioneer in engineering, such as:

- One of the first Swiss steam central heatings in 1841
- First Diesel engine in 1898
- First shuttleless weaving machine in 1952



Leading equipment and service provider with global presence:

- Pumps business since 1857
- Chemtech since 1946
- Service business (pumps and turbines) since the beginning, service division for rotating equipment since 2000

Today, acting as an industry reference by:

- Anticipating future trends
- Offering state-of-the-art business solutions
- Known for reliable and responsible business partnerships

SULZER

About Sulzer IT / Information Security

3+ years ago

?? server rooms

?? clients

?? servers

divisional
organized IT organizations

missing
standards

fragmented
application portfolio

Information security
not officially existing, performed in an ad-hoc manner

now

180 server rooms

13200 clients

1930 servers

one
global IT organization

defined
standards

harmonized
application portfolio

Information security
handled within a 3.5 FTE team and well established organization

Why focus on Security Monitoring?

Cyber Security, Conclusions:

- As we all know: It’s just a question of time – preventing security incidents is not possible
- Effective, preventive security measures are often too expensive in a grown IT landscape

➡ Be able to identify how an attack / incident happened to learn / improve for the future

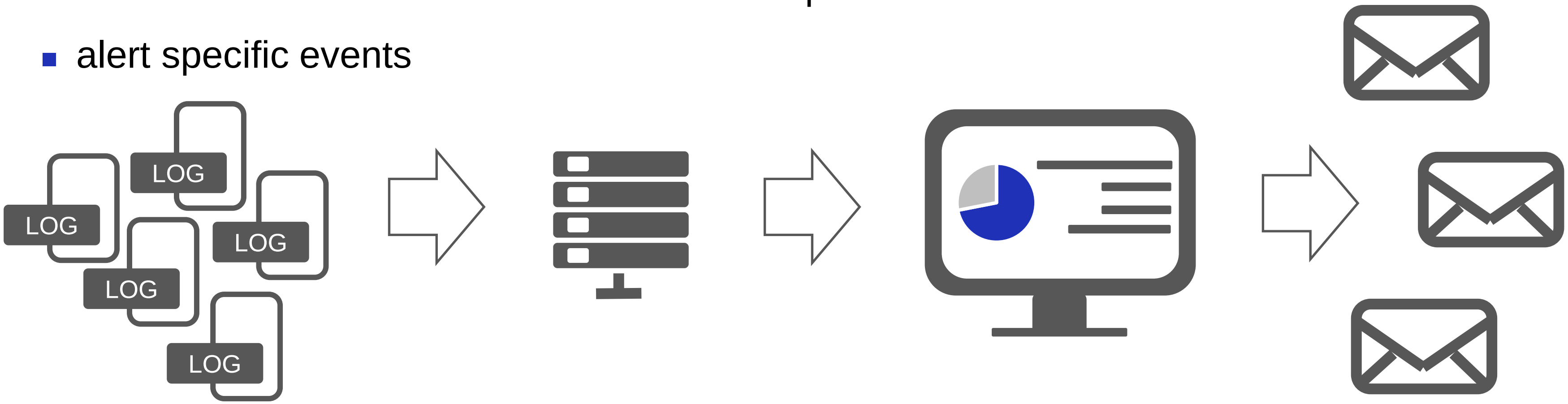
Security Controls

- Logs can be used to check the status and effectiveness of implemented security controls
- Monitoring systems can be used to inform about (in-)compliance with security regulations

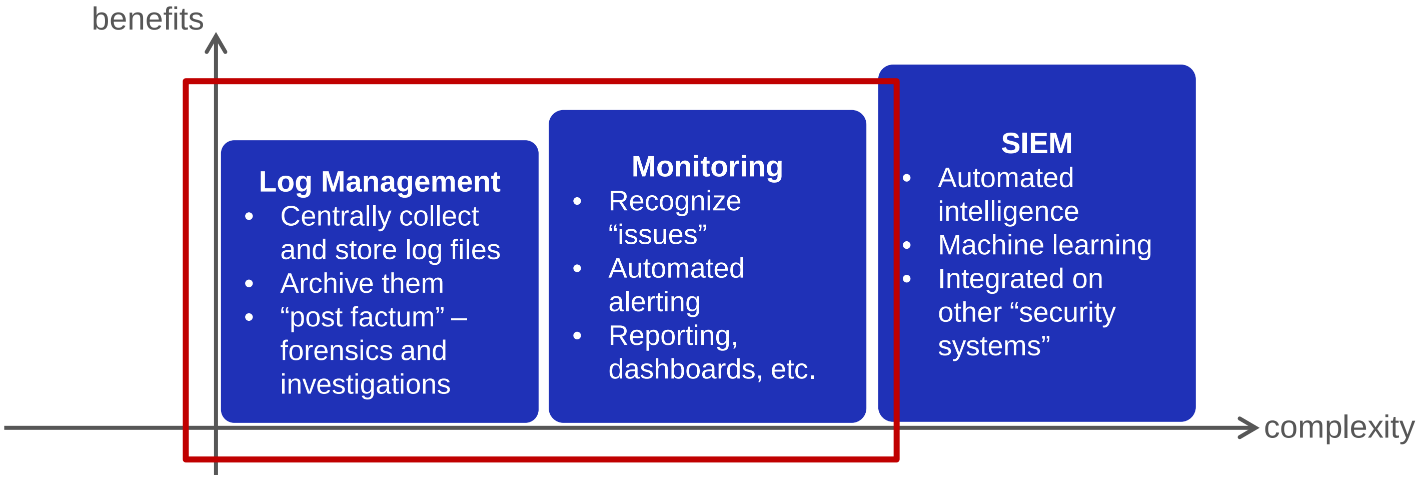
Monitoring Strategy

- Aims
  - Traceability in case of issues, security incidents, compliance cases
  - Store logs tamper proof for a defined time period
  - Recognizing trends and anomalities deviating from baselines

- Approach
  - collect log files centrally
  - store them
  - define «useful» data for dashboards and reports
  - alert specific events



Monitoring Strategy



Log Management
- Centrally collect and store log files
- Archive them
- "post factum" – forensics and investigations

Monitoring
- Recognize "issues"
- Automated alerting
- Reporting, dashboards, etc.

SIEM
- Automated intelligence
- Machine learning
- Integrated on other "security systems"

- Why not start directly with a SIEM?
  - A lot of effort to manage, clean false positives, adjust default rules to reflect own environment, etc.
  - "many red alerts": overwhelming, important alerts might be overlooked
  - You need to know your environment – a SIEM does not solve operational issues

Monitoring Strategy

- We decided to use the “Bottom Up” approach instead of going for a full SIEM
  - Define use cases
    - What do we want to know / identify
  - Identify necessary systems to collect logs from
  - Create alerts, reports, dashboards, etc.

- Pro’s
  - Manageable also for small security teams
  - Growing your maturity over time (learning curve)
  - Don’t create hundreds of alerts which nobody can handle
    - Focus on relevant areas

- Con’s
  - You don’t know what you don’t know
    - Expectation management : monitoring will never be complete

Use Cases

what to collect	potential use cases
Active Directory (Windows Event logs from domain controllers)	Changes on users, groups, group policies, etc. • user added to the enterprise admins • failed logins • locked user accounts
Web Traffic	• Detect downloads of “unwanted” software • Monitor uploads of data to cloud storage • Usage of “non standard” gateways
Client Computers	• Users with Admin Privileges • Clients where software distribution is not working • Outdated or unauthorized software installed

Statistics, graphs

Slide with statistics shown during presentation
Not included in download version

Actions leave Traces, know what to look for

Thank you for your attention!!

Andrea Klaes
Chief Information Security Officer

Project Partner
Swiss IT Security
since 1996

terreActive
terreActive
terreActive
terreActive