360° SAP Security
Protecting your SAP Systems against Hackers and industrial Espionage
Andreas Mertz, CISSP, iT-CUBE SYSTEMS GmbH
Motivation
The forgotten world: Corporate Business Application Systems

Security Silos:
Applications have versatile security models, interfaces, formats...

Manual Handling:
Audits are snapshots and expensive as they are done manually.

Multiple ID’s:
Administrators, technical users, account sharing, ...

Network Exposure:
Applications and threats pass network barriers.

After-The-Fact:
Only real-time monitoring and alerting allows counter-actions.

Incomplete, undetected:
SAP / Transactional data – It’s the blind spot of IT-Security.
How to bridge the SAP–SIEM –GAP?

Security Professionals are not Application Experts

Application Experts don’t know about IT-Security
Why are Business Applications in Focus of Attacks? Why SAP?

1. All business processes are generally contained in ERP systems.
2. Any information an attacker wants is stored in a company’s ERP.
3. The most critical data to be targeted in SAP are:
   - Financial Data, Financial Planning (FI)
   - HR data, personal, contact details (HR)
   - Corporate Secrets (PLM)
   - Supplier tenders (SRM)
   - Customer Lists (CRM)
4. SCADA and ERP systems are often connected. And prone to sabotage.
5. Software has vulnerabilities. ERP has more issues; being different:
   - Customization – No two SAP systems are the same.
   - Complexity kills security. - ERP systems are huge complex landscapes that contain different DBs, APP servers, middleware, frontend SW, OS, use many technologies.
   - Risky – ERP systems store and process business-critical data. Any downtime incurs significant costs. Patching is risky. Vulnerable SW lives for years.
   - Unknown – ERP systems are less researched, much less scrutinized, less targeted but often contain simple and easy to discover vulnerabilities and now get connected to the Internet.
SAP stores the most critical business info.
... and you are loosing control.

- Program Vulnerabilities
  - The number of SAP Security Notes has increased drastically over the last 3 years.
  - Most of these issues affect the Business Runtime.
- Architecture Flaws
- Configuration Errors
MYTH: SAP systems are inaccessible from the Internet, so SAP vulnerabilities can be only exploited by insiders.

- **TRUTH:** Business processes are changing and anticipate the need to for remote and mobile access via web portals.
- **PROVE:** Increasing numbers of SAP systems are exposed to the Internet, including Dispatcher, Message Server, HostControl, Web Services, Solution Manager, etc.
- **STATS:** Searches performed using well-known Google search requests or ShodanHQ result in hundreds of SAP Servers accessible from the Internet.

<table>
<thead>
<tr>
<th>Application Server Type</th>
<th>Search String</th>
<th>Number based on Shodan Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver J2EE (Enterprise Portal)</td>
<td>inurl:/irj/portal</td>
<td>834</td>
</tr>
<tr>
<td>SAP BusinessObjects (SAP ITS)</td>
<td>inurl:infoviewap</td>
<td>20</td>
</tr>
<tr>
<td>SAP NetWeaver ABAP</td>
<td>inurl:/sap/bc/bsp</td>
<td>113</td>
</tr>
</tbody>
</table>
SAP ABAP Attack Vectors

- **SAP Web Server leaks information in HTTP headers and error messages**
  - Config. approved?
  - (Table Data)
- **SAP Web Server runs services without authentication**
  - Services deactivated?
  - (Table Data)
  - Standard users secured?
  - (Table Data, Profile Parameters)
- **SOAP RFC Service allows to call ABAP Function Modules**
  - Execution deactivated?
  - (Table Data)
- **Debugging Mode allows data manipulation without authentication**
  - Debugging enabled?
  - (System Log)
- **Brute Force Attacks**
  - Config. Checked?
  - (SAL + Table Data)
- **Privileged escalations from low risk to high risk SAP Systems (RFC, SSO)**
  - Intrinsic relationships hardened?
  - (Table Data + Cross Device Correlation)
- **Backdoor implementation (Program/ Role changes through transports)**
  - Suspicious transports detected?
  - deactivated?
  - (Transport Log)
- **OS Command execution**
  - Execution discovered?
  - (System Log + Cross Device Correlation)
- **Password Sniffing in unencrypted Srv-Srv / Client – Srv Communication**
  - Config. Checked?
  - (Profile Parameters)
- **Program Code Vulnerabilities in AddOns**
  - Code scanned for vulns?
  - (Code Profiler + Table Data)
- **SAP Gateway Weaknesses (unlimited acces for external programs)**
  - Weak configs detected?
  - (Gateway Cfg. + Log)
- **Changes of critical data**
  - Changes discovered?
  - (Table Log)

Over 95% of SAP® systems are exposed to espionage, sabotage and fraud attacks.

*Do you really think auditing SoD controls is sufficient?*
Continuous Auditing / Continuous Monitoring
Simplify it! Automate it! Secure it!

Status Quo SAP Security
- Many point solutions
- Different report formats
- For single systems only
- Not fully customizable
- Several people involved
- Manual tasks

SAP-SIEM Integration
- Automated
- Continuous
- Complete
- In one spot
360° SAP Security
A HOLISTIC APPROACH TO AUTOMATE SAP SECURITY ASSESSMENTS.

- Secure Code
  - Virtual Forge
  - Fortify
  - Scan source code for vulnerabilities

- Secure Apps
  - Change Mgmt
  - Check patch status, changes (transports)

- Secure Systems
  - SOS
  - Check configs, settings, SoD & critical authoriz.

- Detect Attacks
  - GRC
  - CSI AA
  - Detect critical command exec., suspicious activity

- Transaction Monitoring
  - manual/custom tools
  - ACL/Oversight
  - Detect fraud, anomalies in workflows, trace priv. users

CodeScanner

agileSI
applied ERP security

Enterprise IT Environment
Collect & Process what’s relevant.

**SAP Security Sources**
- Security Audit Log
- System Log
- CCMS and Solution Manager Diagn.
- Other logs (Transport, Gateway, …)
- Report for System Parameters
- Tables
- Table logging
- Reports for Change Documents
- User Information System (suim)
- Audit Information System (AIS)
- EarlyWatch & Sec. Optimiz. Servc.
- RSECNOTE
- Trust Manager and SSO, SNC

**SAP Security Analytics Pack**
- Content & Use Cases derived from:
  - DSAG Audit Guidelines
  - SAP Security Recommendations
  - SAP Pentesting Practises
- Dashboards, Reports, Notifications
- SAP specific categorization for SIEM
- Data Monitors, Active Lists, Rules

SIEM Integration without agileSI™:
- Security Audit Log only
- no SAP-specific Content
## agileSI Extractors: Visibility & Coverage

<table>
<thead>
<tr>
<th>Event Source</th>
<th>Event Type</th>
<th>Use Case</th>
</tr>
</thead>
</table>
| Security Audit Log | Subset of security events in SAP systems, such as (failed) logins, transaction starts, etc | • Brute force login  
• User created / deleted / locked / unlocked  
• Password changes  
• Execution of reports |
| System Log      | SAP basis log, for availability, error tracking, security, ...             | • Debugging  
• Execution of OS commands  
• Table logging in program disabled by user |
| System Parameters | SAP system configuration                                                  | • Password policy checks  
• SNC encryption status  
• SAP Gateway check |
| Tables          | Data stored in Tables                                                     | • System and client change settings  
• RFC configuration  
• Single Sign-On / Logon Tickets  
• Any data stored in any table |
| Ping            | Monitor availability                                                      | • Check availability of SAP systems |
| Transport Log   | Change management through transports with code, customizing               | • Updates to roles  
• Transports of critical objects, at unusual times |
| Gateway Config & Log | Communication with external programs                                     | • Monitor “denied” external calls |
| Change Documents | Changes to Business Objects                                               | • Roles, profiles and User master data |
| Table Change Logging | Changes to data stored in tables                                         | • Monitor critical tables (master data, conditions of purchase) |
| Access Control  | Checks against critical combinations of authorization objects             | • SoD Conflicts  
• Backdoor implementation via transports |
| Security Notes  | SAP RSECNOTE implementation status                                       | • Security notes missing in system landscape |
Use Cases
Technical Use Case & Detection Scenarios

- **Standard User Accounts**
  - Account status (locked, initial passwords)
  - Standard user activity
- **Data integrity/non-changeability**
  - Debugging activity per system
  - System enablement and authorizations
- **OS Commands**
  - List of authorizations
  - Alert of execution
- **Changes to critical data**
  - SAL is not enough (SAL does not provide sufficient information)
  - SAL transaction monitoring
- **Administrator privilege use**
  - High privileged accounts, special accounts (e.g. Firefighter usage)
  - Changes to user master records by SAP*, DDIC*
- **Change Documents User Master Records**
  - Authorization Assignment (Roles, Profiles)
  - Changes to user master records (validity, password reset, ...)
- **System Access**
  - Active User Accounts vs. Corporate Directory
  - SOAP service in use, configuration settings
- **Access Control Violations**
  - Large number of DSAG security checks preinstalled
- **Failed Logins**
  - Technical users with PW typo
- **Check Transport Imports**
  - Critical transports of authorizations and access rights
  - Transports changing authorization assignments
  - Check transports at unusual time window
  - Scan objects by given list and check target client
Business Transaction Monitoring Use Cases

- Major Invoices being made without purchase orders
- Deviation of: value of purchase order and invoice value at equal quantity of goods
- Invoice receipt and payment before date of good receipt
- Control of critical data of application within customer namespace (e.g. applications in production process)
Solution Architecture
Product Overview

Industry’s first automated & SAP-certified solution

ABAP Application
Runs on SAP NW AS

3 Tier Architecture
- Collection layer
- Admin layer
- Analysis layer

QRadar® Integration
- SAP Parser
- SAP specific Categorization
- Correlation Rules, Dashboards, Reports

SOLUTION ARCHITECTURE

Monitored systems

SAP NW AS ABAP

Collection

AgileSI™ Agent

Administration

SAP ERP
SAP SCM
SAP PLM
SAP CRM
SAP ...

Central configuration and control

AgileSI™ Core

Analysis

Dashboards, Reports, Alerting

Q1Labs QRadar

AgileSI™ Frontend
**Extractor Infrastructure**
- Extractor Agents
- Configuration Handling
- Extractor Scheduling

**Service Factory**
- Extractor Management
- Event Format Transformation
- WebDynPro Interface

**SIEM-based Analytics Frontend**
- Dashboards, Reports, Notifications
- SAP specific Categorization for SIEM
- Event Correlation, Security Analytics
Supported SAP Products

- ABAP Systems in Mainstream Maint. (Basis 7.x)

Certification & Built-in Security

- Own SAP name space & approved quality of code
- Use security functions built into NetWeaver (RFC/SNC, authoriz., ...)
- agileSI™ authorization objects
- Data integrity: Store log data in SIEM system
- Application logging to enable agileSI™ audit
agileSI: custom dashboard

Offenses Integration

Custom Rules firing

agileSI/custom use cases
Example use cases

- Changes to user master records on productive systems...
  - ... are unusual,
  - ... severe auditors findings
  - ... need to be monitored
  - ... must only be done by a small set of administrators

- Security Audit log is not enough. Change documents give transparency and need to be correlated
Example use cases: SAP Standard Account logon activity

- SAP standard user accounts are high privileged accounts
  - Login and action via free accessible terminals or terminal servers are anonymous
    - SAP* = root
    - SAP* must be locked in system landscape
- SAP* activity is highly critical and needs to be checked
- Top severe auditor finding

SAP* = "root"

>> Event drilldown
Log activity: dashboard drilldown

>> Event drilldown
Log activity: dashboard drilldown

- Logon and user account changes
### agileSI log integration: log activity

- **Event Name:** Gateway log entries, Table content, Change documents, User Master Record Changed, Access control violations
- **Category:** Information, N/A, N/A, Warning, Warning
- **Username:** N/A, N/A, N/A, N/A, N/A
- **Event Log:** View real time events, Display: Custom

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Category</th>
<th>Username</th>
<th>Event ID</th>
<th>Source</th>
<th>Event Type</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>05562700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Table content</td>
<td>N/A</td>
<td>N/A</td>
<td>12588700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Change documents</td>
<td>Information</td>
<td>GBD</td>
<td>12588700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_CHANGEDOC</td>
</tr>
<tr>
<td>User Master Record Changed</td>
<td>Information</td>
<td>TGS</td>
<td>23462400</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_CHANGEDUR</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>EBO</td>
<td>09571500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_ACC_CTRL, User 'Tob' is authorized to change authenticator attributes</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>EBO</td>
<td>21562300</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_ACC_CTRL, User 'Tob' is auth. to disallow other users</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>N/A</td>
<td>10013200</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>05562700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>17234500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Change documents</td>
<td>Information</td>
<td>GBD</td>
<td>02372100</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_CHANGEDOC</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>09571500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>10516200</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>09571500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Report Started</td>
<td>Service Started</td>
<td>SAPSYS</td>
<td>23451000</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Successfull RFC Call</td>
<td>Information</td>
<td>N/A</td>
<td>09452700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>EWA</td>
<td>09571500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_ACC_CTRL, User 'EWA' is authorized to generate custom attribute</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>N/A</td>
<td>15448500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_CHANGEDU</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>N/A</td>
<td>08504700</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>N/A</td>
<td>01024000</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_TABLE</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>09571500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Gateway log entries</td>
<td>Information</td>
<td>N/A</td>
<td>25533000</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_GATEWAY</td>
</tr>
<tr>
<td>Access control violations</td>
<td>Warning</td>
<td>TMB3</td>
<td>03548500</td>
<td>N/A</td>
<td>N/A</td>
<td>SI_CHANGEDU, User 'TMB3' is authorized to copy a client</td>
</tr>
</tbody>
</table>
Eliminate the blind spot in SAP® Security Monitoring

- Continuously monitor your critical system conditions and events
- Automate collection, correlation, visualization & reporting
- Reduce your audit costs & efforts and safe costly SAP consultants
- Utilize standard checks and SAP®-specific threat vector detection
- Enable your SOC team to interpret SAP® security events and act
Key use & benefits

Regain control with Security Intelligence for SAP®

- Improve your SAP® Security & Risk Management
- Lower the number and criticality of auditor’s findings
- Transform your risks into remediation
- Fulfill compliance requirements for your SAP® landscapes
- Consolidate the SAP® tool zoo into one holistic approach
Let's discuss it!
IT’S ABOUT THE I IN IT, NOT JUST THE T!

Thank you for attending this session!

iT-CUBE SYSTEMS GmbH
Paul-Gerhardt-Allee 24
81245 München
Germany

P:  +49 (89) 2000 148 00
F:  +49 (89) 2000 148 29
M:  info@it-cube.net
W:  www.it-cube.net
Company Overview
Our Expertise

- Full-service provider for IT-/SAP-Security with 10+ years experience
- Vendor-neutral consulting, system integration, product development
- Founded in 2001, privately held
- Partnerships with 20+ A-brand vendors
- 28 consultants, 8 developers
- Approved for classified information (Ü2) by BMWi
**SOLUTION PORTFOLIO**

**iT-CUBE SYSTEMS – We keep IT trusted.**

### iT-CUBE Solutions

#### Security Intelligence
- Security Information & Event Management (SIEM)
- Log-Management & IT-Search
- Threat Intelligence
- Digital Forensics
- Industrial/SCADA Security
- Governance Risk Compliance (GRC)

#### Managed Services
- Managed Security Services (MSS)
- Security Outsourcing
- Operational Outtasking
- Service & Support Helpdesk

#### Professional Services
- Security Consulting
- Security Training
- Security Assessments
- System Integration
- Product Development
- Customizing & Engineering

### People & Processes
- IT-/Business Application Monitoring
- Transaction Monitoring
- SOC / NOC Process Design
- Identity and Access Management (IAM)
- Security Awareness Building
- Security Training

### Data Analytics
- Operational Intelligence
- Big Data Analysis
- Business Analytics
- IT-Search
- Business Application Monitoring

### Applications
- SAP-Security
- Data Loss Prevention (DLP)
- Malware Protection
- Software Code Analysis
- Secure Data Exchange
- Database Virtualization

### Network & Infrastructure
- IT-Monitoring
- Firewalling
- Intrusion Prevention
- Web/E-Mail Security
- Remote Access
- Network Access Control
- Vulnerability Management
- Virtualization Security