

# agile Security Intelligence for SAP® Customers with ArcSight ESM®

## Executive Summary

SAP business solutions are the first choice for many organizations to run their most critical business processes, from managing manufacturing to processing payments, and preparing financial statements. To actively manage risk companies rely on ArcSight ESM, a leading edge SIEM solution (SIEM: Security Information & Event Management) focusing on network-centric security aspects to protect against external and insider threats.

However, comprehensive security and business risk management requires the monitoring of event data from core business applications correlated with those from the supporting infrastructure such as databases, application servers, workstations, firewalls, proxies, remote access gateways, and other IT systems.

Unfortunately, SAP and other business applications do not integrate work with SIEM systems. There is a severe information gap integrating SAP systems in SIEM solutions, which we call the SAP-SIEM-Gap. Closing this gap requires three major steps to be performed:

1. Knowing, accessing and extracting all relevant data from a heterogeneous SAP landscape
2. Processing data and correlating disparate individual events
3. Turning terabytes of raw data into meaningful interpretable information

iT-CUBE has developed a solution to close the SAP-SIEM-Gap. It is called agile Security Intelligence (*agileSI*). *agileSI* extracts security data from SAP systems and forwards it to ArcSight ESM where the data is correlated, also with events outside SAP. Part of the solution is a special analytics content package for ArcSight that enriches raw data and enables security analysts to interpret events and check compliance with recommendations from SAP and best practices by dashboards and reports. Customers can adapt *agileSI* to their needs, defining which data to extract and which objectives have to be fulfilled.

*agileSI* helps customers to continuously monitor their SAP environment, hence reduce risk and audit costs and enable well-informed decisions.

## CONTACT

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

info@it-cube.net  
www.it-cube.net

Jens Kettler  
Vice President SAP Security  
j.kettler@it-cube.net

Dipl.-Ing. Andreas Mertz, CISSP  
Principal Consultant  
a.mertz@it-cube.net

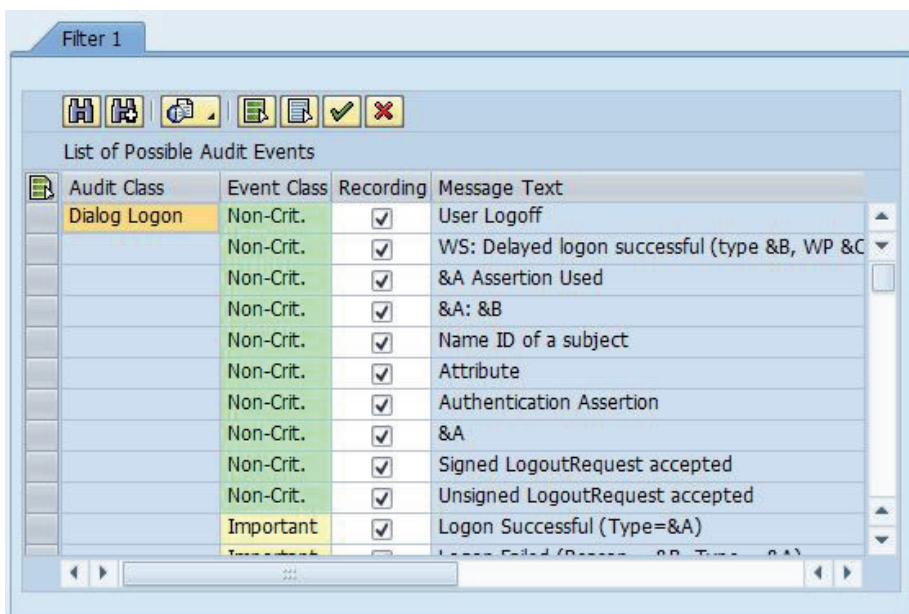


Figure 1: SAP Transaction SM19: Configuration of the Security Audit Log

### Drivers for SAP Security Monitoring

In fact organizations run their most critical business processes on SAP, employees, external consultants, providers, suppliers and others get access and accounts trusted with permissions, rights and privileges within SAP landscapes to perform specific tasks and ensure business operations. SAP access combined with other tools provided to users, can also be used to perpetrate fraud, harvest intellectual property, or sabotage operations. The scenario becomes even more frightening when we take into account the different potentially vulnerable endpoint devices to access SAP.

Because SAP applications are running in networked environments connected to web, email, cloud services and even the Internet it is inevitable to monitor SAP in the context of its surrounding IT infrastructure. Thus it is imperative to collect event data from numerous systems, including:

- Networking equipment (e.g., routers, switches, load balancers),
- Security devices (e.g., firewalls, IPS, content filters, proxies),
- Operating systems,
- Databases and application servers,
- Client systems (e.g., workstations, notebooks, smartphones),
- Communication activity (e.g., MS Exchange / Lotus Notes, Chat, Peer-to-Peer, cloud services),
- Other corporate applications.

SAP landscapes in large organizations can be highly complex, comprising thousands

of users and roles, countless processes spanning the entire enterprise and massive infrastructure requirements. Organizations are obliged to create and deploy various controls to ensure that their SAP environment functions as intended, e.g.

- Preventing a user from creating a supplier and paying that supplier (Segregation of Duties)
- Ensure that basis administrators do not create users or modify permissions (SoD)
- Assign user privileges ensuring that only needed rights are granted (least privilege)

Quite often organizations struggle with demonstrating the effectiveness of those controls during audits since it can be hard to automate controls. In those cases compensating controls allow organizations to remain protected in cases where the con-

trol cannot be enforced, or when enforcement requires an additional process to achieve the goal. The “firefighter scenario” is a good example to illustrate the need to temporarily assign roles to users, while violating the SoD control. To compensate for this risk, it becomes necessary to monitor the firefighter’s activities for potential abuse of the exceptional but intended temporary role assignment.

### A Challenging Scenario

Let’s assume you are an auditor or security analyst and your task is to ensure compliant operation of the SAP system landscape in your company, and detect incidents and quickly react to them. SAP systems (and throughout the text we mean systems that are based on the SAP NetWeaver Application Server ABAP; that comprises all Business Suite solutions)

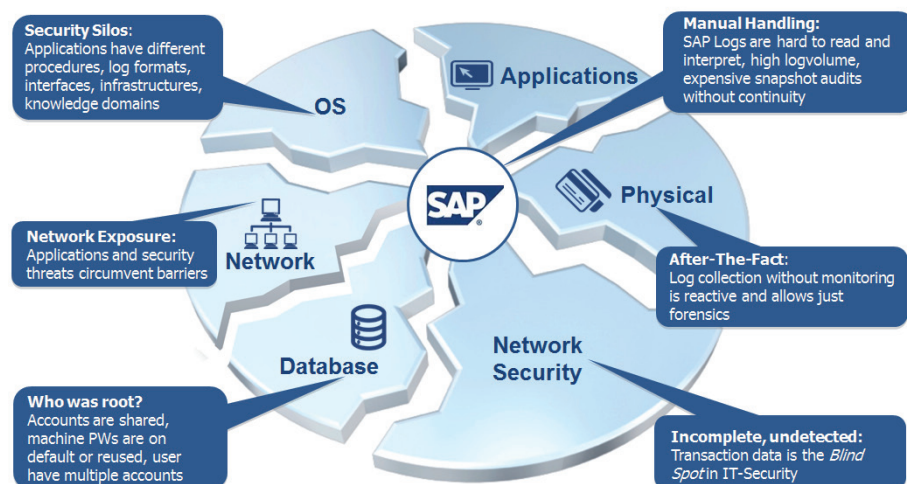


Figure 2: SAP and “the rest of the IT” - Security silos causing blind spots

store security information in several places, and there are various ways to get to that information. An auditor or someone who wants to find out about the state of the system or investigate an incident can look at or use some of these tools:

Security Audit Log, System Log, CCMS and Solution Manager Diagnostics, Other logs (Transport, Gateway, ...), System Parameters, Tables, Table Logging, Change Documents, User Information System, Audit Information System (AIS), Early-Watch and Security Optimization Service, RSECNOTE, Trust Manager, and SSO and SNC settings, ...

All these data sources and tools provide some parts of the answers to your questions, like: Are my systems configured according to my security policy? Are there any security incidents or critical changes? All you need to do is to look up information from these sources continuously throughout your SAP system landscape, interpret it, and correlate the data in real-time to provide notification and reporting. Don't forget to also include information from the surrounding IT infrastructure - otherwise you will miss important pieces of the puzzle.

Depending on what system, application or device is being monitored, log data and status information has different fields and formats. SAP itself has thousands of different event types, each containing a distinct set of relevant information. Apart from this fact the methods to access the data vary from syslog, JDBC, XML to file access, and others.

Impossible task? - Maybe, but let's see how close we can get.

### The Status Quo in Security Event Management

ArcSight ESM is a leading edge SIEM solution which collects, aggregates, parses, normalizes and categorizes security data from a wide range of sources and provides sophisticated methods to analyze event data. The list of supported data sources contains more than 350 products from all categories mentioned above. ArcSight also has a powerful, highly scalable correlation engine that supports in-memory, statistical and historical correlation based on 100+ threshold- and scenario-based rules. Active Lists enable the intelligent escalation of events as they grow in the level of threat, using events are prioritized based on the level of risk to the organization. The results are presented via a graphical engine in the most common formats. The presentation can be adapted to technical, business, audit or executive users.

ArcSight ESM also integrates with SAP systems using a file adapter that reads the SAP Security Audit Log. The SAP Security Audit Log (SAL) log events such as successful and failed logons, transaction starts, RFC calls, changes to user master data, and other (figure 1). These messages help to determine critical events and start an investigation into the incident. The information in the log is not sufficient to come to a conclusion on the severity of an event, detect fraud or bad system confi-

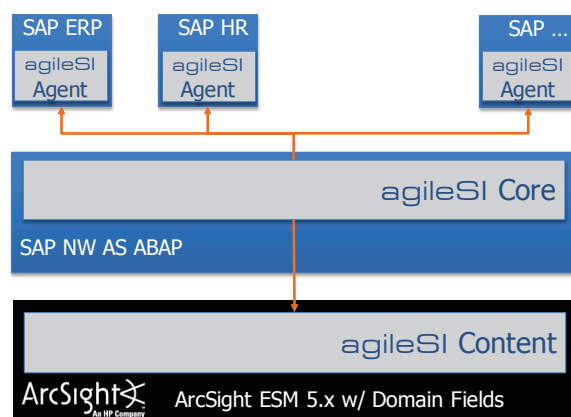


Figure 3: agileSI Architectural Overview

guration, or say whether some action has to be taken because of the log message. It always triggers a manual investigation, which is costly, and in the end only a few messages actually can be investigated. So there is only an incomplete picture.

For instance, when an administrator changes role assignments, like adding critical authorizations to a user or removing a role, the corresponding Security Audit Log message will be "User Master Record Changed/Authorizations Changed" and the user ID. There is no information on the details of the change, which requires a lookup in the Change Document for the user. The administrator can display this by running a report in the SAP system.

Often, critical events don't trigger an entry in the Security Audit Log at all. Examples are changes to system change options, starting the debug mode, changes through transports. Also, the Security Audit Log does not provide information on the state of the system, like whether a password policy is active and in compliance to the company security policy.

To interpret data from the Security Audit Log, additional information is required. This comes from the various sources in SAP listed in the first table above (and possibly others). ArcSight ESM – as all other SIEM solutions – cannot access this additional data.

A SIEM is as smart as the provided information it can process. Missing data, in particular transactional data and manual data handling are problems that customers face in SAP security monitoring:

1. It is neither sufficient nor feasible to manually sift through terabytes of system and user activity data when needed. Thus automation is the key to monitoring SAP as part of daily

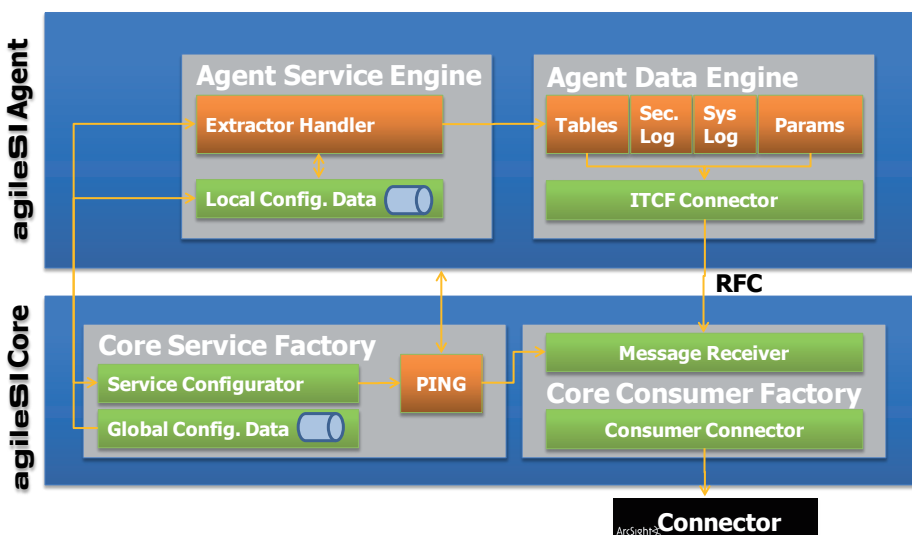


Figure 4: agileSI functional modules and interworking

Extractor	Events/Data	Example Use Cases	SI Release
Security Audit Log	Subset of security events in SAP systems, such as (failed) logins, transaction starts, etc.	<ul style="list-style-type: none"> <li>• Brute Force Login</li> <li>• User Created / Deleted / Locked / Unlocked</li> <li>• Password Changes</li> </ul>	1.0
System Log	SAP basis log, error tracking, security, ...	<ul style="list-style-type: none"> <li>• User SAP* deleted</li> <li>• Debugging</li> <li>• Table logging in program disabled by user</li> </ul>	1.0
System Parameters	SAP system configuration	<ul style="list-style-type: none"> <li>• ESM Active List, preconfigured, recommended values from DSAG</li> <li>• Customizable through Active List import</li> <li>• Password policy checks</li> </ul>	1.0
Tables	Data stored in Tables	<ul style="list-style-type: none"> <li>• Trusted RFC</li> <li>• SAP Logon Tickets</li> <li>• Any data stored in any table (with "where" conditions)</li> </ul>	1.0
Transport Log	Change Management through transports with code, customizing	<ul style="list-style-type: none"> <li>• Updates to roles</li> </ul>	1.1
Change Documents	Changes to Business Objects	<ul style="list-style-type: none"> <li>• Roles</li> <li>• User Master Data</li> </ul>	1.1
Tables/ Table Logging	Changes to data stored in tables	<ul style="list-style-type: none"> <li>• Critical tables (master data, conditions of purchase)</li> </ul>	1.1
Gateway	Gateway configuration and log	<ul style="list-style-type: none"> <li>• White list of external programs</li> </ul>	1.1
RSECNOTE	SAP Security Notes status	<ul style="list-style-type: none"> <li>• Status of SAP Security Notes applied/patch level</li> </ul>	1.2

### agileSI - The ultimate solution

agileSI uses agents on the SAP source systems to extract data. agileSI also has a Core that controls the Agents and is a proxy for the ArcSight ESM, collecting the data from the SAP systems and providing CEF formatted output. (CEF=Common Event Format, an ArcSight specific data format that allows to add meta-data to the events and provides easy import of the data into the SIEM tool (figure 3)).

Part of the agileSI solution is a special analytics content package for ArcSight, which helps to interpret the data and covers use cases for security monitoring driven by recommendations from SAP, the German SAP Users Group (DSAG) and best practices.

The agileSI Core and the Agents are ABAP programs that closely integrate with the SAP systems. They are developed adhering to SAP's best practices and shipped as Add-Ons, ensuring easy deployment and security. The SAP authorization concept works to protect the data in the source systems, the system owner can define which data can be extracted. agileSI has its own authorization objects to protect the administration and other components (such as the Extractors) from unauthorized use. On the transport layer, SAP security functions like Secure Network Communication ensure confidentiality and integrity of the data. The solution is designed to be scalable for large installations (figure 4).

The agileSI Core contains the Service Factory. This is a web interface (figure 5) for the administrator that allows de-

business operations so that threats can be detected and remediated proactively.

2. Events in SAP may involve many disparate individual actions which, taken together, will make a correlation rule fire and trigger other actions. As the data is not available in the SIEM system, there is no correlation for coherent events from a single or multiple SAP systems and also not for data from the surrounding IT infrastructure.
3. Auditors and security analysts often need to investigate past activity to understand the scope of an incident, retrace the steps of fraud events, and uncover other advanced persistent threats (APT). Security events and

status information from SAP must no longer reside isolated from SIEM (figure 2).

To help SAP and ArcSight customers accomplish the "impossible" task and answer the critical questions on their system security, iT-CUBE has developed a solution that closes the gap between SAP systems and ArcSight ESM. Organizations need a flexible, intelligent approach to collect and interpret the data from SAP sources providing meaningful intelligence used to make informed decisions. agileSI is exactly that powerful solution to extract data from SAP systems, forward it to ArcSight ESM, and analyze it by means of special content and ArcSight's correlation engine.

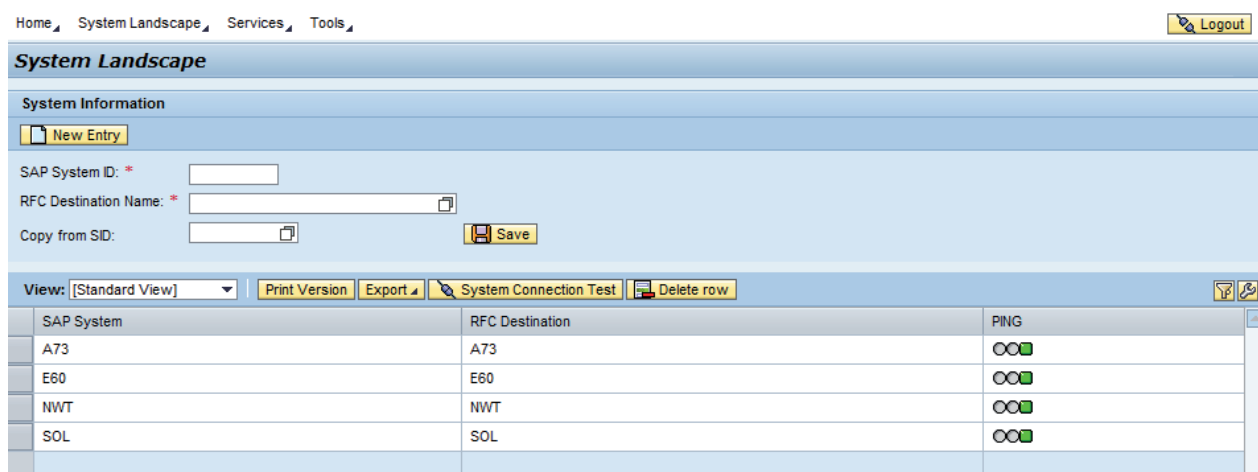


Figure 5: agileSI Web interface allows maintaining the system landscape.

fining the system landscape and also which data will be extracted from the SAP systems. The data extraction can be defined for each system or for groups of systems. The Service Factory holds the configuration of all Agents in the landscape and distributes the local configuration data to the Agents in the source systems.

The *agileSI* Core can run on any SAP system with an AS ABAP 7.0 or 7.3. So this can be deployed e.g. on the Solution Manager, an SAP application, or on a dedicated server.

Each Agent (one per source system) contains several Extractors and one Extractor Handler. The Extractors are ABAP programs that can extract data from one type of data source, and run as batch jobs. The Extractor Handler manages the local configuration data and schedules the Extractors (table).

*agileSI* can extract almost any information from the systems, as defined by the customer. This allows a range of use cases that goes far beyond the native SAP-SIEM integration, from monitoring the configuration state of the SAP systems to detecting incidents and transaction monitoring.

The data provided by the Extractors is in various formats; table data looks different than entries in log files. So for routing these messages, *agileSI* uses an internal data format that we call ITCF (IT-CUBE Format). Extractors can pass data in their specific format to the ITCF Connector, which can handle all these data types and transforms the data into ITCF. This data is sent to the *agileSI* Core via RFC. *agileSI* ensures quality of delivery, each message gets sent/delivered exactly once to the Message Receiver in the Core.

The next step is to transform data into the ArcSight CEF and write it to a file. This file can be read and preprocessed by ArcSight's standard file adapter. *agileSI* utilizes Domain Field Sets – a new feature of ArcSight ESM V5.x which offers significantly more label+value pairs than standard device custom fields. It allows customizing the name of the label making it easier to identify fields according to their function. Domain fields are “dynamic,” because they can mean different things for different events depending on the domain an event belongs to. The flexibility of dynamic domain field sets within a SIEM is a fundamental technical precondition to integrate business environments that must support monitoring, investigation, and analysis for use cases in

Parameter_name	Param_val_low	Param_val_high	Param_val_string	Description
auth/rfc_authority_check	1			
login/disable_multi_gui_login	0			
login/failed_user_auto_un...	1			unlock user at midnight that had been locked due to m
login/fails_to_session_end	3			to prevent dictionary attacks, close session after num
login/fails_to_user_lock	5			to prevent dictionary attacks, lock user after number
login/max_time_not_logg...	10			What is the longest time a user may not have been lo
login/min_password_diff	4			new passwords have to contain at least n different c
login/min_password_digits	4			minimum digits in passwords
login/min_password_letters	4			min letters in password
login/min_password_lng	8			check, if minimum length is configured
login/min_password_lowe...	4			This is optional
login/min_password_specia...	4			password should at least have 1 special character
login/min_password_upper...	4			This is optional
login/no_automatic_user...	1			by default, SAP* is inactive; check settings
login/password_change...	1			user have to wait eg 1 day after password change to
login/password_charset	4			all unicode characters are allowed
login/password_complianc...	1			when password policy changes users with non-compli
login/password_expiratio...	365			force users to change passwords in certain intervals
login/password_history_size	15			check whether password history is sufficient
login/password_max_idle...	7			initial passwords should be changed within 7 days
login/password_max_idle...	180			productive (not initial) passwords that are not used to

Figure 6: ArcSight ESM Console view of SAP system parameters for the password policy.

multiple business verticals, such as integrating data from SAP and other applications.

ArcSight ESM standard content and *agileSI*'s special analytics content package supports a number of common use cases out of the box. This content consists of data monitors, rules, dashboards, notifications and reports, and it can be modified and enhanced by customers whenever necessary (figure 6).

Systems that can be monitored with *agileSI* are ABAP-based systems (this includes all Business Suite applications) in SAP Mainstream Maintenance mode.

Deployment of the solution is easy, using standard SAP software logistics. When ArcSight already is in use, adding *agileSI* and SAP monitoring is a matter of days. *agileSI* will become generally available in October 2011 (release 1.0). Release 1.1 will follow in Q1/2012 and provide additional Extractors and content. By end of year 2011 *agileSI* will be certified by SAP.

### Key benefits and value propositions

The combined *agileSI* / ArcSight ESM solution provides capabilities to extract almost all information from SAP systems and over 350 other devices in the IT land-

scape. Combined with the powerful correlation engine in ESM and pre-defined content this gives customers the perfect solution for maximum visibility regarding their most important IT assets and critical processes.

Key benefits are:

- Transparency, through continuous monitoring and cross-device/application correlation
- Fulfillment of compliance requirements
- Reduction of audit efforts and costs

The Return On Investment for *agileSI* comes directly from savings in the daily security operations and lower efforts in audits, as all information is available in a central spot and customers can prove compliance directly.

### Seeking for more information ...

To read more about using agile Security Intelligence for SAP monitoring visit <http://www.it-cube.net/sap>