

***Использование решения agileSI  
для мониторинга информационной безопасности систем SAP***

Николай Петров, CISSP

Директор по развитию бизнеса, ДиалогНаука

Первым в России был удостоен звания CISSP  
На протяжении многих лет являюсь единственным  
сертифицированным инструктором (ISC)2 в России

Работал в компаниях Philip Morris, Kerberus,  
MIS Training Institute, (ISC)2, Ernst & Young



ДиалОгНаука



# План презентации

---

1. Почему важен мониторинг ИБ систем SAP
2. Обзор решения agileSI
3. Выводы

Продолжительность 30 мин

# Почему важен мониторинг ИБ систем SAP: информация

---

Система SAP содержит интересующую злоумышленника информацию, например:

- Финансовые данные, финансовое планирование (FI)
- Информация о сотрудниках, их персональные данные (HR)
- Информация о продуктах (PLM)
- Информация о поставщиках и тендерах (SRM)
- Информация о клиентах (CRM)

## Особенности систем SAP:

- **Кастомизация** – нет 2-х одинаковых SAP систем
- **Сложность системы** отрицательно сказывается на ее безопасности. SAP сложные распределенные системы, включающие в себя БД, сервера приложений, различные типы клиентов. В стандартных настройках более 1000 параметров
- **Высокий риск** – перерыв в работе приводит к серьезным финансовым потерям. Обновления ПО связано с высоким риском. Поэтому уязвимые системы используются на протяжении многих лет

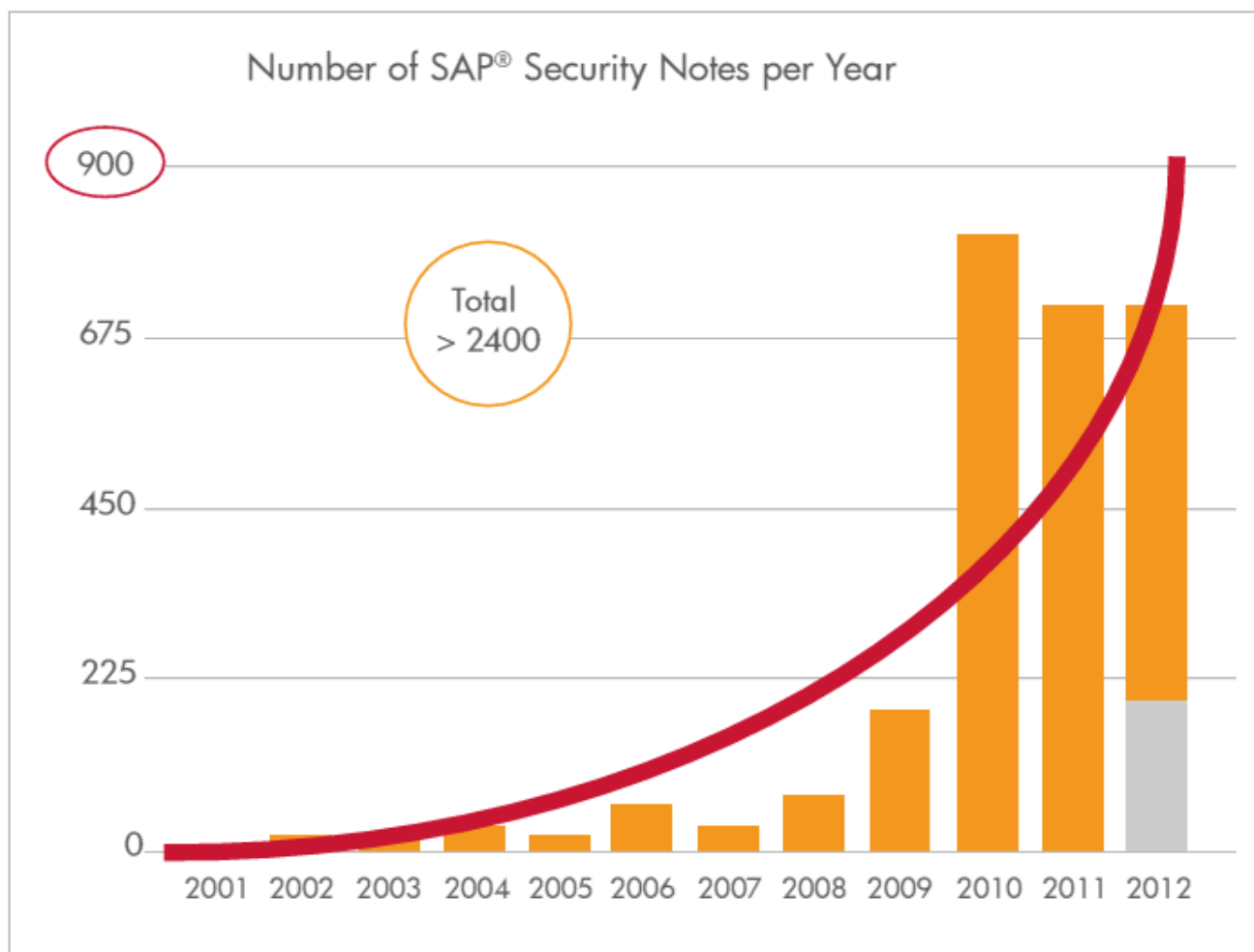
# Почему важен мониторинг ИБ систем SAP: уязвимости

---

## Примеры уязвимостей:

- Заголовки HTTP и сообщения об ошибках позволяют получить информацию о конфигурации SAP Web сервера
- Запуск службы SAP Web сервера не требует аутентификации
- Служба SOAP RFC позволяет вызывать функциональные модули ABAP
- Режим отладки позволяет манипулировать данными без аутентификации
- Атаки использующие Brute Force для подбора пароля
- Изменение ПО/Ролей посредством транспорта
- Выполнение команд ОС
- Sniffing (перехват) учетных записей и паролей
- Уязвимости SAP Gateway - неограниченный доступ к системе

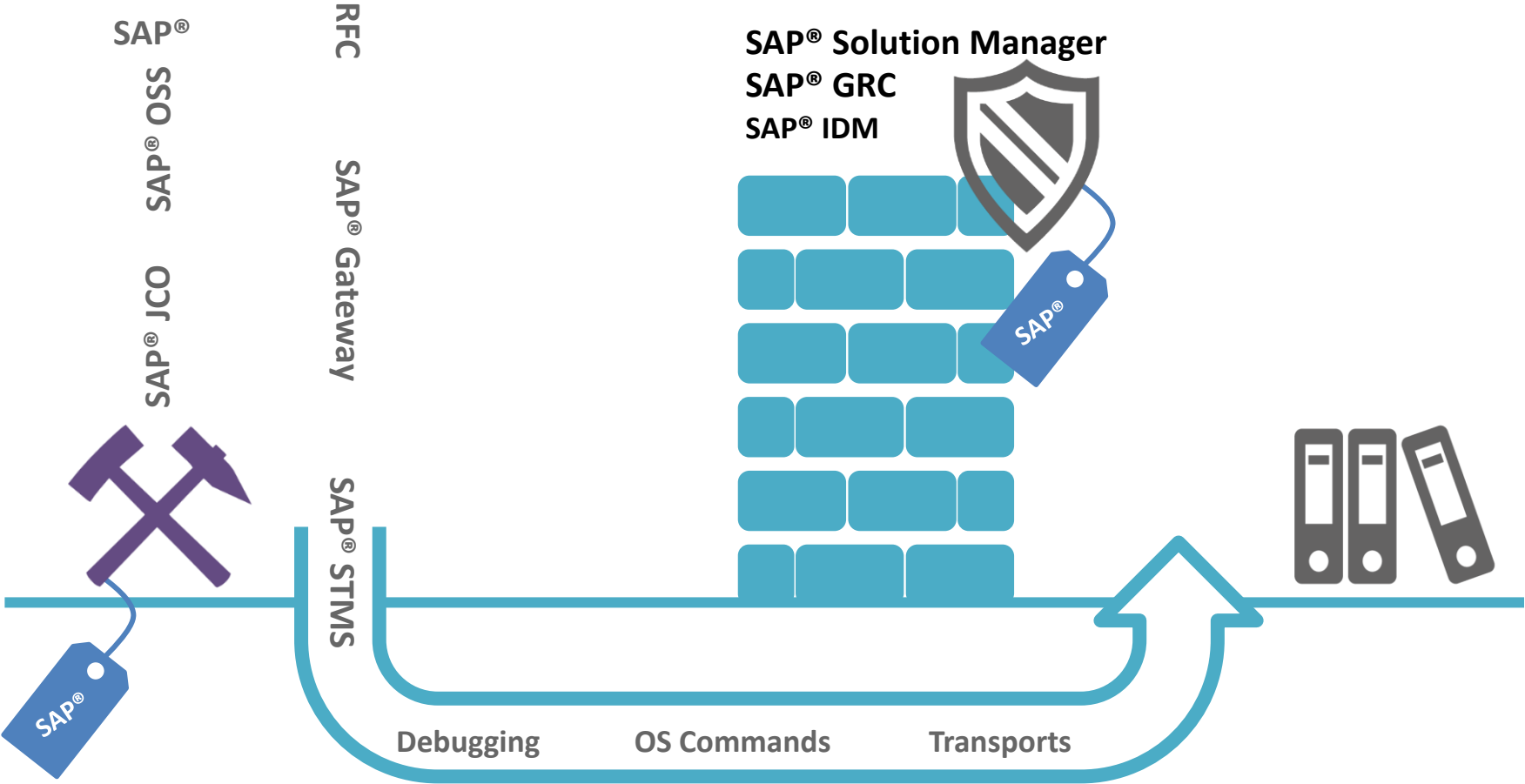
# Почему важен мониторинг ИБ систем SAP: Security Notes



Количество SAP Security Notes существенно увеличилось за последние 3 года

# Почему важен мониторинг ИБ систем SAP: SAP tools

## SAP® tools обходят средства безопасности SAP®





# Обзор решения agileSI: поддерживаемые платформы

---

Сертифицированное решение для мониторинга SAP

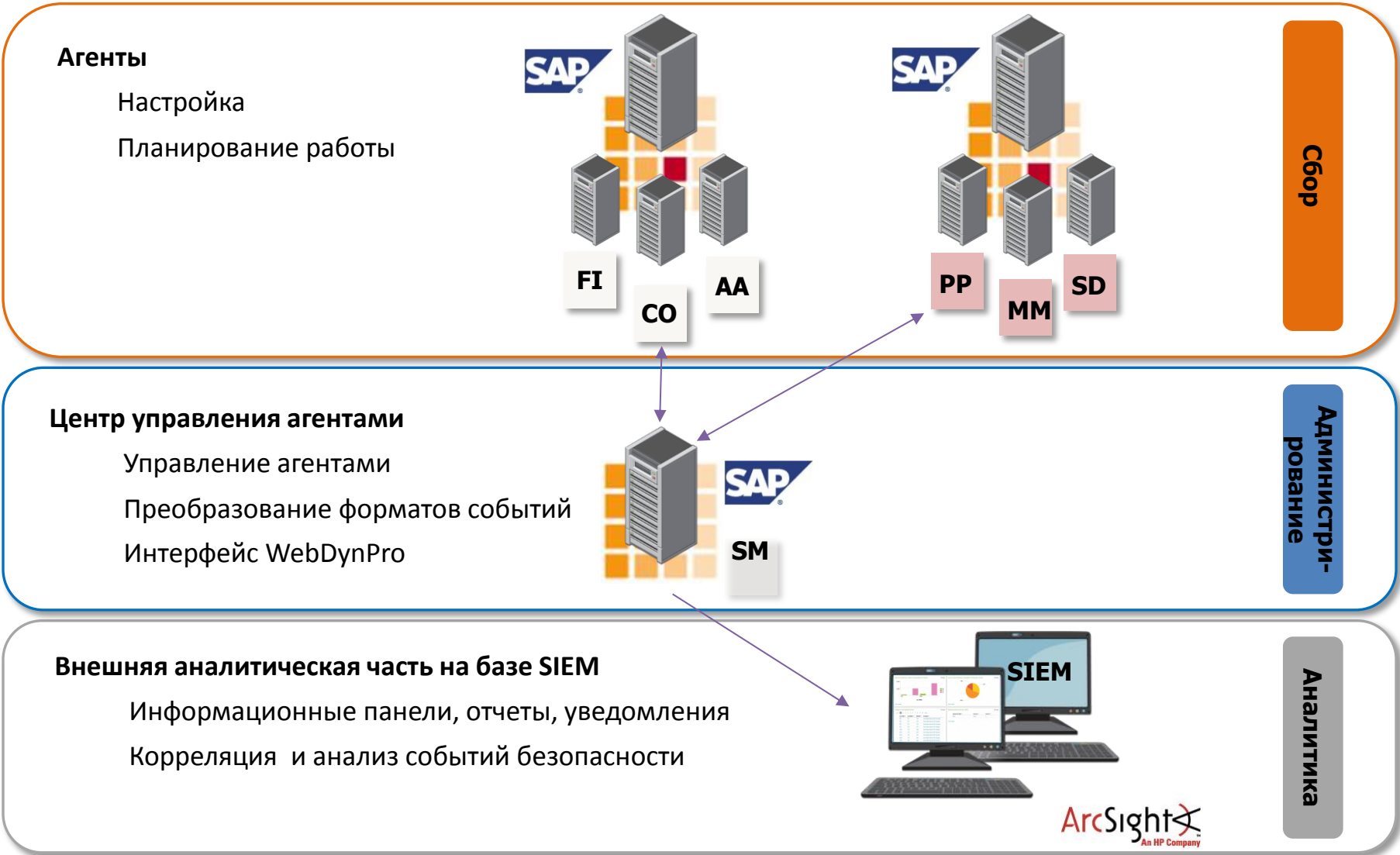
ABAP Systems in Mainstream Maint. (Basis 7.x)

- SAP Netweaver 7.0 EHP 1
- SAP Netweaver 7.3
- SAP ERP 6.0
- SAP CRM 6.0, 7.0
- SAP SCM 5.1, 7.0
- SAP CRM 6.0, 7.0

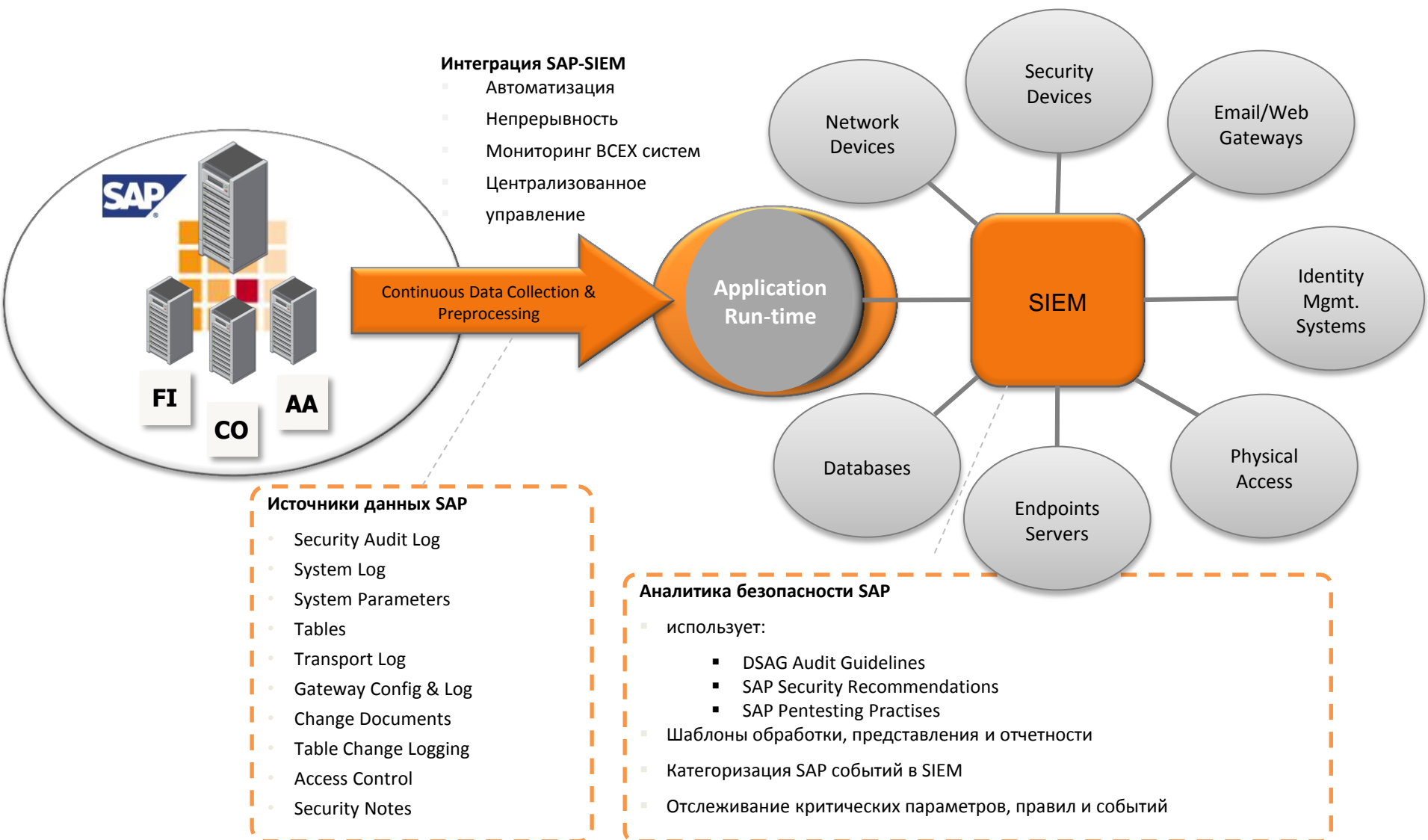


**SAP**<sup>®</sup> Certified  
Integration with SAP Applications

# Обзор решения agileSI



# Обзор решения agileSI



# Обзор решения agileSI: примеры использования

| Источник             | События/Данные   | Примеры использования  |  |
|----------------------|--|--|--|
| Security Audit Log   | События безопасности SAP систем                                  | <ul style="list-style-type: none"> <li>• Попытки подбора пароля</li> <li>• Создание /удаление/блокировка пользователя</li> </ul> | <ul style="list-style-type: none"> <li>• Изменения пароля</li> <li>• Запуск отчетов</li> </ul>             |
| System Log           | Системный журнал SAP , ошибки, security, события безопасности... | <ul style="list-style-type: none"> <li>• Режим отладки</li> <li>• Исполнение команд ОС</li> </ul>                                | <ul style="list-style-type: none"> <li>• Пользователь выключает Table logging</li> </ul>                   |
| System Parameters    | Конфигурация SAP   | <ul style="list-style-type: none"> <li>• Password policy</li> <li>• SNC encryption status</li> </ul>                             | <ul style="list-style-type: none"> <li>• SAP Gateway</li> </ul>  |
| Tables               | Данные в Tables  | <ul style="list-style-type: none"> <li>• Настройки Системы и Клиента</li> <li>• Конфигурация RFC</li> </ul>                      | <ul style="list-style-type: none"> <li>• Single Sign-On / Logon Tickets</li> <li>• Любые данные</li> </ul> |
| Transport Log        | Изменения посредством transports                                 | <ul style="list-style-type: none"> <li>• Изменения ролей</li> <li>• Transports критичных объектов, в необычное время</li> </ul>  |  |
| Gateway Config & Log | Взаимодействие с внешними программами                            | <ul style="list-style-type: none"> <li>• Мониторинг внешних вызовов</li> </ul>   |  |
| Change Documents     | Изменения Business Objects                                       | <ul style="list-style-type: none"> <li>• Роли, профили, User master data</li> </ul>  |  |
| Table Change Logging | Изменения данных хранимых в таблицах                             | <ul style="list-style-type: none"> <li>• Мониторинг (master data)</li> </ul>   |  |
| Access Control       | Проверка комбинации объектов авторизации                         | <ul style="list-style-type: none"> <li>• Параметры учётных записей, конфликты SoD</li> </ul>                                     |  |
| Security Notes       | Статус SAP RSECNOTE  | <ul style="list-style-type: none"> <li>• Отсутствует реализация Security notes</li> </ul>  |  |

# Обзор решения agileSI: использование DSAG

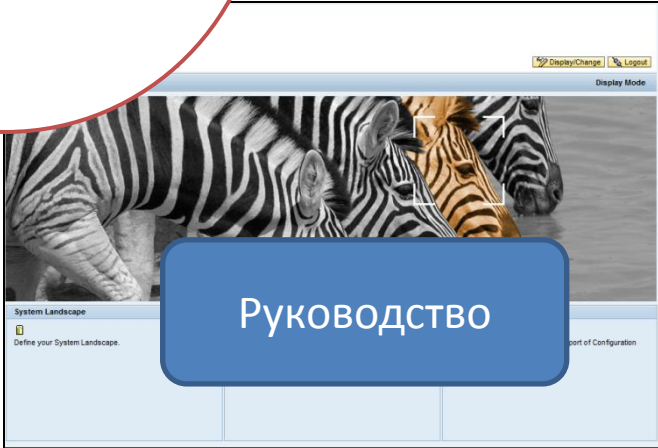
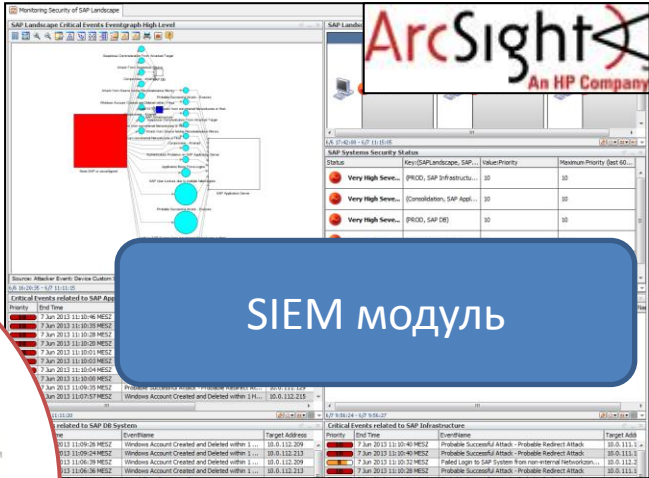
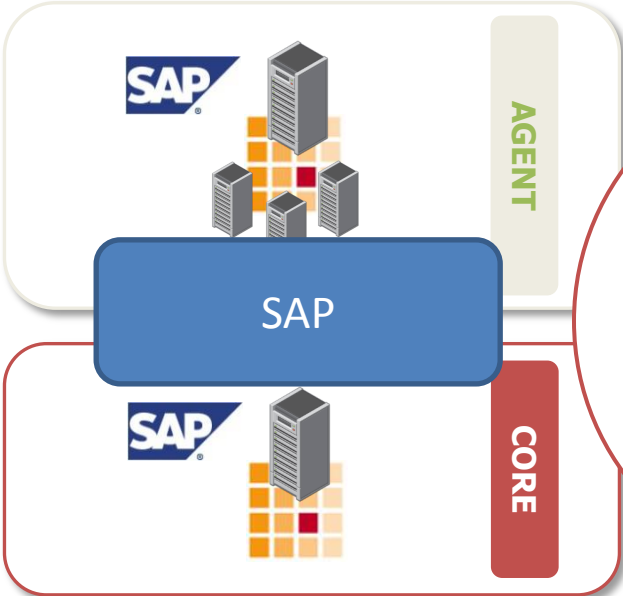
## DSAG : 100+ проверок

| Рекомендация DSAG                             | Применение agileSI   |
|---|--|
| 1. Управление Доступом, SoD конфликты         | agileSI проверяет SAP_ALL авторизацию и другие конфликты   |
| 2. Мониторинг стандартных учетных записей SAP | agileSI проверяет статус блокировки и активность стандартных учетных записей   |
| 3. Выключение / изменение авторизаций         | agileSI контролирует транзакции, например, SU24, SU25, SU26, SM01 и AUTH_SWITCH_OBJECTS и параметр auth/object_disabling_active отвечающий за изменения и выключении проверок авторизации на глобальном уровне |
| 4. Security Audit Log активирован?            | agileSI проверяет настройки Security Audit Log, такие как статус активации, конфигурацию посредством контроля Table data и Table Change Logging  |
| 5. Изменения системы и клиента                | agileSI отслеживает изменения  |
| 6. Мониторинг Transport Management System     | agileSI контролирует transport imports для критичных объектов, импорт в необычное время, и STMS параметры, такие как RECCLIENT и VERS_AT_IMPORT в TMSPCONF   |
| 7. Table Change Logging                       | Установки системных параметров rec/client для Table Change Logging контролируются  |
| 8. PC Download                                | Контролирует выгрузку данных из SAP  |

Мониторинг транзакций и выявление мошенничества, примеры:

- Оплата счета без регистрации заявки на закупку
- Разница в суммах в заказе и счете при одинаковом перечне товаров/услуг
- Получение и оплата счета до поступления товаров
- Контроль критичных операций (пример, золотые изделия)

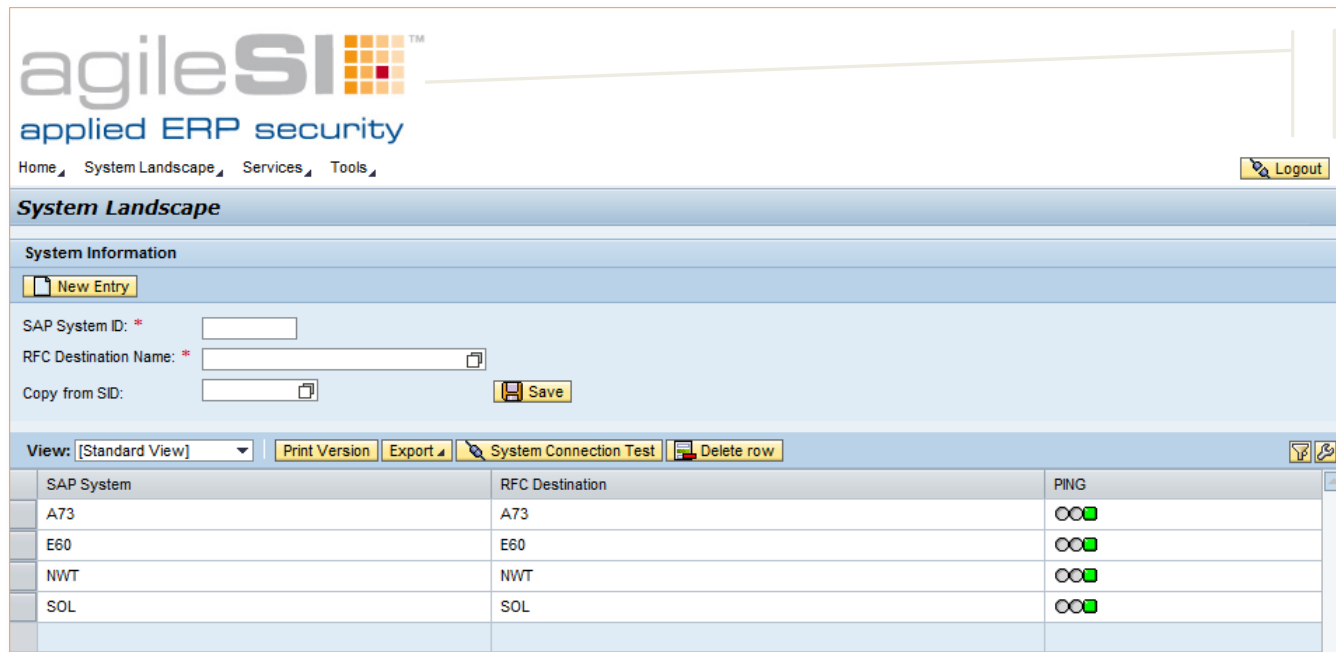
# Обзор решения agileSI: установка



# Обзор решения agileSI: установка

Последовательность действий:

1. Импорт Agents and Core в SAP (минуты)
2. Импорт модуля SIEM (минуты)
3. Создание учетных записей для agileSI™ (минуты)
4. Конфигурация SAP мониторинга (часы)
5. Кастомизация экстракторов и содержимого мониторинга (дни)



The screenshot displays the agileSI WebDynPro ABAP Frontend interface. The header includes the agileSI logo and the text "applied ERP security". Below the header, there are navigation links for "Home", "System Landscape", "Services", and "Tools", along with a "Logout" button. The main content area is titled "System Landscape" and contains a "System Information" section with a "New Entry" button. The form includes fields for "SAP System ID: \*", "RFC Destination Name: \*", and "Copy from SID:", with a "Save" button. Below the form, there is a toolbar with options for "View: [Standard View]", "Print Version", "Export", "System Connection Test", and "Delete row". The main data area is a table with three columns: "SAP System", "RFC Destination", and "PING".

| SAP System | RFC Destination | PING |
|------------|-----------------|------|
| A73        | A73             | ○○●  |
| E60        | E60             | ○○●  |
| NWT        | NWT             | ○○●  |
| SOL        | SOL             | ○○●  |

**WebDynPro ABAP  
Frontend**



# Обзор решения agileSI: установка

## Управление экстракторами

Определяем экстракторы

Определяем интервалы

| SAP System | Extractor Type       | Active                              | Interval | Start Date | Start Time | End Date | Status Deployment |
|------------|----------------------|-------------------------------------|----------|------------|------------|----------|-------------------|
| *          | Table                | <input checked="" type="checkbox"/> | 01:00:00 |            | 00:00:00   |          | ○○●               |
| *          | Security Audit Log   | <input checked="" type="checkbox"/> | 00:10:00 |            | 00:00:00   |          | ○○●               |
| *          | System Log           | <input checked="" type="checkbox"/> | 00:10:00 |            | 00:00:00   |          | ○○●               |
| *          | Profile Parameters   | <input checked="" type="checkbox"/> | 06:00:00 |            | 00:00:00   |          | ○○●               |
| *          | Gateway Log          | <input checked="" type="checkbox"/> | 01:00:00 |            | 00:00:00   |          | ○○●               |
| *          | Table Change Logging | <input checked="" type="checkbox"/> | 01:00:00 |            | 00:00:00   |          | ○○●               |
| *          | Access Control List  | <input checked="" type="checkbox"/> | 01:00:00 |            | 00:00:00   |          | ○○●               |
| *          | Change Documents     | <input checked="" type="checkbox"/> | 01:00:00 |            | 00:00:00   |          | ○○●               |

# Обзор решения agileSI: установка

## Кастомизация экстракторов Поддержка регулярных выражений

**Service Management - Table Extractor**

**Service Detail**

Back Create New Selection

System ID (SID): \*

Copy from SID:

Selection ID:  Copy as New Selection

Use Case:

Table Name: \*  Get table field names

**Fields for Selection**

|       |                  |     |  |  |
|-------|------------------|-----|--|--|
| MANDT | Equal To (= Low) | 100 |  |  |
| BNAME | n/a              |     |  |  |
| UFLAG | n/a              |     |  |  |
|       | n/a              |     |  |  |
| GLTGB | n/a              |     |  |  |
| USTYP | n/a              |     |  |  |
| CLASS | n/a              |     |  |  |
| LOCNT | n/a              |     |  |  |
| UFLAG | n/a              |     |  |  |
| ACCNT | n/a              |     |  |  |
| ANAME | n/a              |     |  |  |
| ERDAT |                  |     |  |  |
| TRDAT |                  |     |  |  |
| LTIME |                  |     |  |  |

Save

Print Version Export Delete Selection Delete row

| System ID (SID) | Table Name | Selection ID       | Field Name | Use Case    | Select Option | Value (low, from) | Value (high, to) |
|-----------------|------------|--------------------|------------|-------------|---------------|-------------------|------------------|
| *               | T000       | 051MaW007k2zhJ3... | MANDT      | ПТСUBE 3121 |               |                   |                  |
| *               | T000       | 051MaW007k2zhJ3... | MTEXT      | ПТСUBE 3121 |               |                   |                  |
| *               | T000       | 051MaW007k2zhJ3... | CCCATEGORY | ПТСUBE 3121 | EQ            | P                 |                  |
| *               | T000       | 051MaW007k2zhJ3... | CCCORACTV  | ПТСUBE 3121 | EQ            | 2                 |                  |
| *               | T000       | 051MaW007k2zhJ3... | MANDT      | ПТСUBE 3122 |               |                   |                  |

# Обзор решения agileSI: установка

## Кастомизация экстракторов Выбор из 1800 параметров

The screenshot shows the 'Service Management - System Log Extractor' interface. A 'Search Message Area' dialog box is open, displaying search criteria and an 'Available Area' table. The dialog has fields for 'AREA' (set to 'LC') and 'SUBID'. Below the dialog, a table lists message areas with columns for 'Message Area', 'Message Name', and 'TXT'. The first row of the table is circled in blue.

**Search Message Area Dialog:**

- Hide Search Criteria
- AREA: LC
- SUBID:
- Start Search
- Reset

**Available Area Table:**

| AR... | SUBID | Description                             |
|-------|-------|---|
| LC    | 0     | Logical command "&A" executed for ...   |
| LC    | 1     | Illegal log_command "&A" rejected to... |
| LC    | 2     | &C when executing external comma...     |
| LC    | 3     | &B when executing external progra...    |
| LC    | 4     | &B when calling internal RFC on &A i... |

**Main Table:**

| Message Area | Message Name | TXT              |
|--------------|--------------|------------------|
| AU           | 1            | Logo...          |
| AU           | 2            | Logo...          |
| AU           | 3            | Trans...         |
| AU           | 4            | Start...         |
| AU           | 5            | RFC/...          |
| AU           | 6            | RFC/...          |
| AU           | 7            | User &A Created  |
| AU           | 8            | User &A Deleted  |
| AU           | 9            | User &A Locked   |
| AU           | A            | User &A Unlocked |

# Обзор решения agileSI: установка

## Кастомизация экстракторов Выбор из 1000+ параметров

The screenshot displays the 'Service Management Profile Parameter Extractor' interface. A search dialog box titled 'Search Profile Parameter' is open, showing a search for 'login/'. The dialog includes a 'Hide Search Criteria' dropdown, a 'Parameter Name' input field containing 'login/', and 'Start Search' and 'Reset' buttons. Below the search field is a list of 'Available Parameters'. The parameter 'login/min\_password\_lng' is selected and highlighted with a blue background and a red circle. The main interface shows a table of profile parameters with columns for 'Profile Parameter Name' and a list of parameters including DIR\_AUDIT, FN\_AUDIT, and various authentication-related parameters.

**Service Management Profile Parameter Extractor**

Service Detail

Back New Entry

System ID (SID): \*

Copy from SID:

Profile Parameter Name: Save

View: [Standard View] Print Version Export Delete row

| Profile Parameter Name       |
|------------------------------|
| DIR_AUDIT                    |
| FN_AUDIT                     |
| auth/check/calltransaction   |
| auth/new_buffering           |
| auth/no_check_in_some_cases  |
| auth/object_disabling_active |
| auth/rfc_authority_check     |
| auth/system_access_check_off |
| auth/tcodes_not_checked      |
| csi/SAP/csa_lib              |

**Search Profile Parameter**

Hide Search Criteria

Parameter Name: login/

Start Search Reset

**Available Parameters**

| Parameter Name                 |
|--------------------------------|
| login/disable_password_logon   |
| login/failed_user_auto_unlock  |
| login/fails_to_session_end     |
| login/fails_to_user_lock       |
| login/isolate_rfc_system_calls |
| login/min_password_diff        |
| login/min_password_digits      |
| login/min_password_letters     |
| <b>login/min_password_lng</b>  |
| login/min_password_lowercase   |

OK Cancel

# Обзор решения agileSI: поддержка SIEM

---



# Обзор решения agileSI



**Global Heat Map**

**System Health**

**Auths & Logons**

**agileSI**  
applied ERP security

**Authentication and Logons**  
Special Accounts - Users that are not Assigned to a User Group (1441)

Number of users per system that are not assigned to a user group for user administration.

**Failed Logins**

**Attack Detects**

**System Integrity**

**Suspicious Events**

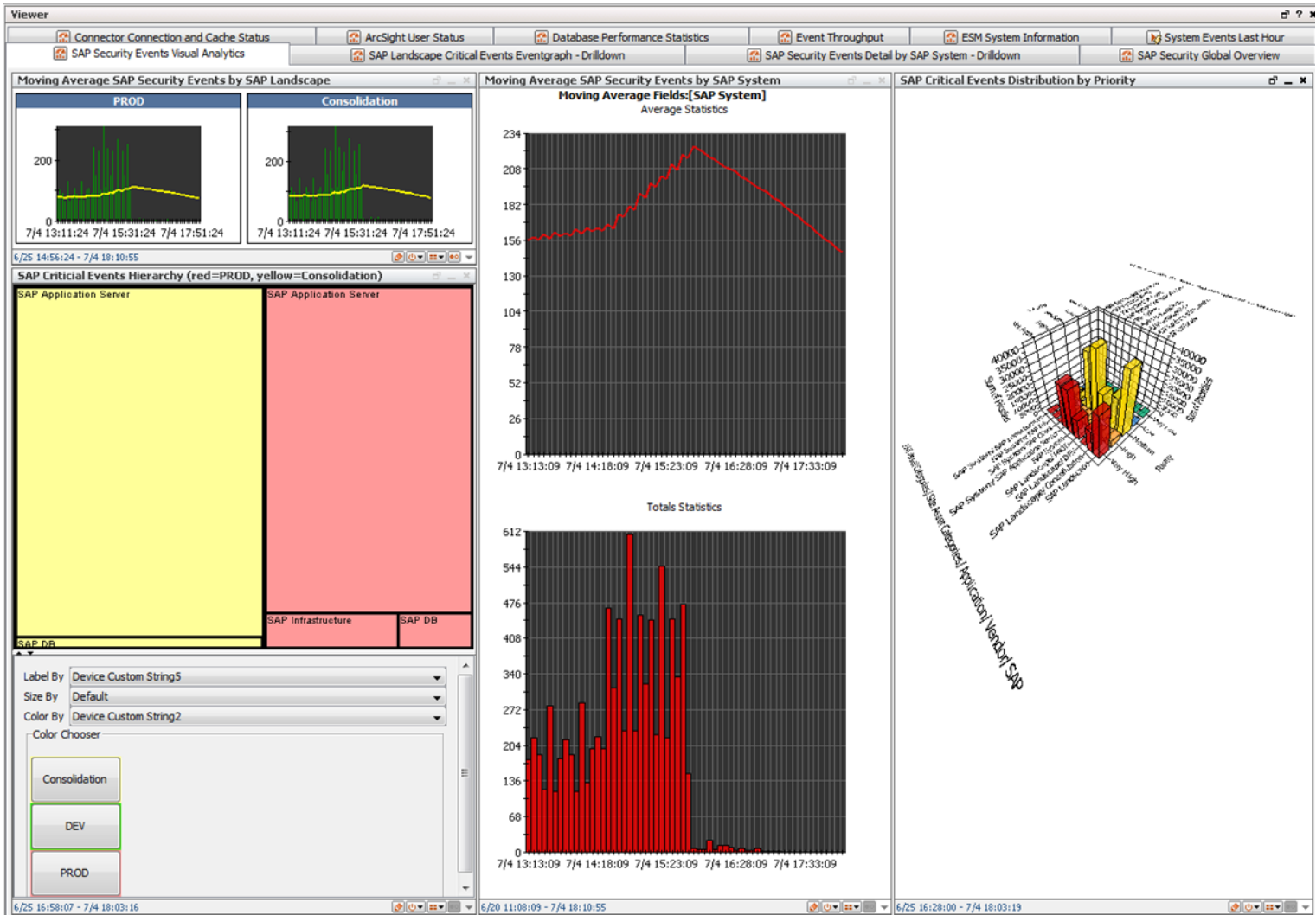
# Обзор решения agileSI

| Critical Events related to SAP Application Server |                          |  |                |                  | Critical Events related to SAP Infrastructure |                          |   |                |                  |
|---|--------------------------|--|----------------|------------------|---|--------------------------|---|----------------|------------------|
| Priority  | End Time                 | EventName  | Target Address | Target Host Name | Priority                                      | End Time                 | EventName   | Target Address | Target Host Name |
| 8   | 4 Jul 2013 17:08:44 MESZ | Windows Account Created and Deleted within 1 ...     | 10.0.112.215   | SPAP1.arcnet.co  | 10  | 4 Jul 2013 17:18:48 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 5   | 4 Jul 2013 16:48:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 10  | 4 Jul 2013 17:18:35 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 5   | 4 Jul 2013 16:48:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 17:16:21 MESZ | agileSI - Login to SAP System from non-internal Networkz...   | 10.0.112.206   | APPOPA1          |
| 10  | 4 Jul 2013 16:48:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 17:12:53 MESZ | agileSI - Login to SAP System from non-internal Networkz...   | 10.0.112.206   | APPOPA1          |
| 5   | 4 Jul 2013 16:33:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 17:05:40 MESZ | agileSI - Failed Login to SAP System from non-internal Net... | 10.0.112.206   | APPOPA1          |
| 5   | 4 Jul 2013 16:33:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 17:01:30 MESZ | Compromise - Attempt  | 10.0.112.206   |                  |
| 10  | 4 Jul 2013 16:33:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 10  | 4 Jul 2013 16:58:32 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 5   | 4 Jul 2013 17:06:20 MESZ | Suspicious Communication From Attacked Target        | 10.0.112.215   |                  | 10  | 4 Jul 2013 16:48:06 MESZ | Attack From Suspicious Source                                 |                |                  |
| 8   | 4 Jul 2013 17:06:13 MESZ | Windows Account Created and Deleted within 1 ...     | 10.0.112.211   | SPAP4.arcnet.co  | 5   | 4 Jul 2013 16:48:06 MESZ | Compromise - Attempt  |                |                  |
| 8   | 4 Jul 2013 17:00:45 MESZ | Attack from Source having Reconnaissance History     |                |                  | 8   | 4 Jul 2013 16:47:26 MESZ | agileSI - Failed Login to SAP System from non-internal Net... | 10.0.112.206   | APPOPA1          |
| 5   | 4 Jul 2013 17:00:45 MESZ | Compromise - Attempt                                 |                |                  | 10  | 4 Jul 2013 16:35:55 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 8   | 4 Jul 2013 16:33:55 MESZ | agileSI - Unexpected activities of SAP standard u... |                |                  | 10  | 4 Jul 2013 16:35:42 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 10  | 4 Jul 2013 16:33:55 MESZ | agileSI - Unexpected activities of SAP standard u... |                |                  | 5   | 4 Jul 2013 16:33:27 MESZ | agileSI - Login to SAP System from non-internal Networkz...   | 10.0.112.206   | APPOPA1          |
| 5   | 4 Jul 2013 16:43:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 16:30:00 MESZ | agileSI - Login to SAP System from non-internal Networkz...   | 10.0.112.206   | APPOPA1          |
| 10  | 4 Jul 2013 16:43:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 8   | 4 Jul 2013 16:22:47 MESZ | agileSI - Failed Login to SAP System from non-internal Net... | 10.0.112.206   | APPOPA1          |
| 5   | 4 Jul 2013 16:41:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 16:18:38 MESZ | Compromise - Attempt  | 10.0.112.206   |                  |
| 5   | 4 Jul 2013 16:29:40 MESZ | agileSI - Changes to critical data detected          |                |                  | 10  | 4 Jul 2013 16:15:39 MESZ | Probable Successful Attack - Probable Redirect Attack         |                |                  |
| 5   | 4 Jul 2013 16:27:41 MESZ | agileSI - Changes to critical data detected          |                |                  | 10  | 4 Jul 2013 16:05:04 MESZ | Attack From Suspicious Source                                 |                |                  |
| 5   | 4 Jul 2013 16:25:41 MESZ | agileSI - Changes to critical data detected          |                |                  | 5   | 4 Jul 2013 16:05:04 MESZ | Compromise - Attempt  |                |                  |
| 5   | 4 Jul 2013 16:45:41 MESZ | agileSI - Changes to critical data detected          |                |                  | 8   | 4 Jul 2013 16:04:24 MESZ | agileSI - Failed Login to SAP System from non-internal Net... | 10.0.112.206   | APPOPA1          |

| Critical Events related to SAP DB System |                          |  |                |                  | Critical Events related to SAP Client |                           |   |                |                  |
|--|--------------------------|--|----------------|------------------|---------------------------------------|---------------------------|---|----------------|------------------|
| Priority                                 | End Time                 | EventName  | Target Address | Target Host Name | Priority                              | End Time                  | EventName   | Target Address | Target Host Name |
| 5  | 4 Jul 2013 17:15:26 MESZ | Compromise - Attempt                             |                |                  | 8                                     | 2 Jul 2013 15:36:10 MESZ  | Brute Force Logins  |                |                  |
| 8  | 4 Jul 2013 17:13:40 MESZ | Attack From Suspicious Source                    | 10.0.112.209   |                  | 8                                     | 2 Jul 2013 15:25:36 MESZ  | Brute Force Logins  |                |                  |
| 8  | 4 Jul 2013 17:13:40 MESZ | Attack from Source having Reconnaissance History | 10.0.112.209   |                  | 8                                     | 2 Jul 2013 15:09:24 MESZ  | Brute Force Logins  |                |                  |
| 5  | 4 Jul 2013 17:13:40 MESZ | Suspicious Communication From Attacked Target    | 10.0.112.209   |                  | 8                                     | 2 Jul 2013 14:55:37 MESZ  | Brute Force Logins  |                |                  |
| 5  | 4 Jul 2013 17:13:40 MESZ | Compromise - Attempt                             | 10.0.112.209   |                  | 8                                     | 28 Jun 2013 14:51:04 MESZ | Brute Force Logins  |                |                  |
| 5  | 4 Jul 2013 17:10:31 MESZ | Compromise - Attempt                             |                |                  | 10                                    | 28 Jun 2013 14:22:12 MESZ | Suspicious Transport - Changes to Authorization Objects     |                |                  |
| 5  | 4 Jul 2013 17:09:33 MESZ | Compromise - Attempt                             | 10.0.112.213   |                  | 10                                    | 28 Jun 2013 14:22:12 MESZ | Suspicious Transport - Changes to Authorization Objects     |                |                  |
| 5  | 4 Jul 2013 17:06:02 MESZ | Suspicious Communication From Attacked Target    | 10.0.112.213   |                  | 10                                    | 28 Jun 2013 14:30:04 MESZ | Changes to critical data detected                           |                |                  |
| 8  | 4 Jul 2013 17:03:23 MESZ | Attack From Suspicious Source                    | 10.0.112.209   |                  | 10                                    | 28 Jun 2013 14:25:34 MESZ | Changes to critical data detected                           |                |                  |
| 5  | 4 Jul 2013 17:03:23 MESZ | Compromise - Attempt                             | 10.0.112.209   |                  | 5                                     | 28 Jun 2013 14:30:04 MESZ | Login to SAP System from non-internal Netzwerkzone or Host  | 10.15.101.33   | sap-ix-0         |
| 5  | 4 Jul 2013 17:02:12 MESZ | Compromise - Attempt                             |                |                  | 5                                     | 28 Jun 2013 14:30:04 MESZ | Login to SAP System from non-internal Netzwerkzone or Host  | 10.15.101.33   | sap-ix-0         |
| 8  | 4 Jul 2013 16:56:10 MESZ | Compromise - Success                             |                |                  | 5                                     | 28 Jun 2013 14:24:04 MESZ | Login to SAP System from non-internal Netzwerkzone or Host  | 10.15.101.33   | sap-ix-0         |
| 8  | 4 Jul 2013 16:49:06 MESZ | Windows Account Created and Deleted within 1 ... | 10.0.112.209   | SPAP3.arcnet.co  | 5                                     | 28 Jun 2013 14:22:04 MESZ | Login to SAP System from non-internal Netzwerkzone or Host  | 10.15.101.33   | sap-ix-0         |
| 8  | 4 Jul 2013 16:48:24 MESZ | Windows Account Created and Deleted within 1 ... | 10.0.112.213   | SPAP2.arcnet.co  | 5                                     | 28 Jun 2013 14:31:29 MESZ | Compromise - Attempt  | 10.15.101.33   |                  |
| 5  | 4 Jul 2013 16:44:18 MESZ | Compromise - Attempt                             | 10.0.112.213   |                  | 10                                    | 28 Jun 2013 14:31:29 MESZ | Application Brute Force Logins                              | 10.15.101.33   | sap-ix-0         |
| 5  | 4 Jul 2013 16:32:33 MESZ | Compromise - Attempt                             |                |                  | 5                                     | 28 Jun 2013 14:31:28 MESZ | Failed Login to SAP System from non-internal Netzwerkzon... | 10.15.101.33   | sap-ix-0         |
| 5  | 4 Jul 2013 16:30:47 MESZ | Suspicious Communication From Attacked Target    | 10.0.112.209   |                  | 8                                     | 28 Jun 2013 14:23:48 MESZ | Brute Force Logins  |                |                  |
| 8  | 4 Jul 2013 16:30:47 MESZ | Attack From Suspicious Source                    | 10.0.112.209   |                  | 8                                     | 25 Jun 2013 16:48:04 MESZ | Brute Force Logins  |                |                  |
| 8  | 4 Jul 2013 16:30:47 MESZ | Attack from Source having Reconnaissance History | 10.0.112.209   |                  | 8                                     | 25 Jun 2013 16:43:28 MESZ | Brute Force Logins  |                |                  |
| 5  | 4 Jul 2013 16:30:47 MESZ | Compromise - Attempt                             | 10.0.112.209   |                  | 8                                     | 25 Jun 2013 16:38:05 MESZ | Brute Force Logins  |                |                  |

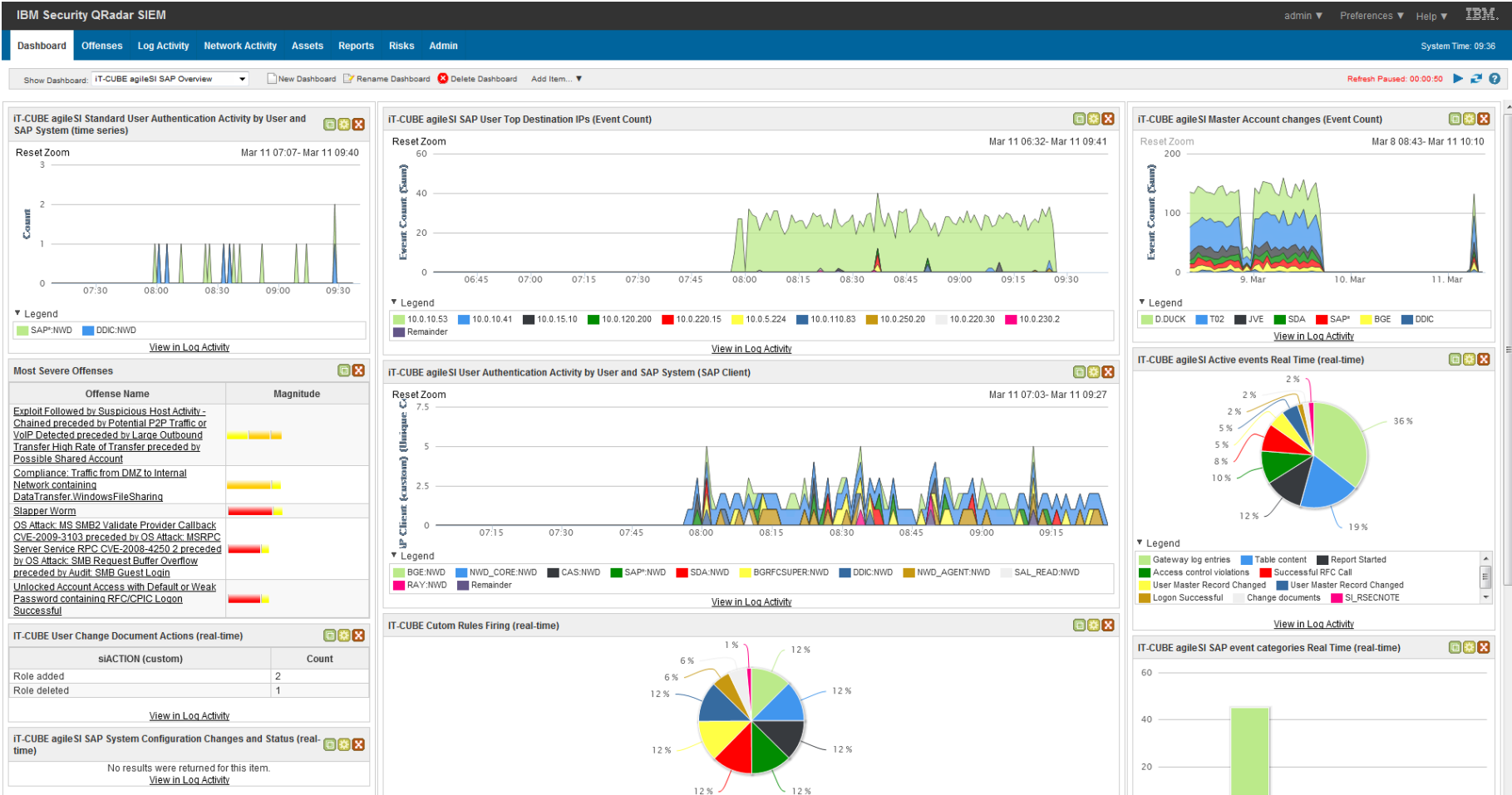
# Обзор решения agileSI





# Обзор решения agileSI

## agileSI™ IBM Qradar:



# Обзор решения agileSI

## agileSI™ Splunk:

The screenshot displays the agileSI interface with a navigation menu and two main data visualization panels. The navigation menu includes 'Search SAP', 'agileSI', 'agileSI Critical Use Cases', and 'Views'. The 'Views' dropdown is open, showing a list of use cases such as 'Standard User Accounts', 'Data Integrity / non-changeability', 'OS Commands', 'Changes to critical data', 'Administrator privilege use', 'Change Documents: User Master Records', 'Remote System Access', 'Access Control: Segregation of duties', 'Active Users that are not in Corporate Directory', 'Failed Logins', and 'All In One'. The 'Failed Logins' view is selected, and a secondary dropdown shows 'Debugging Activity per System' and 'System enablement and authorizations'. The 'Failed Logins' panel features a bar chart titled 'Top Failed Logins by User' and a table titled 'Failed Logins [last 7 days]'. The bar chart shows the number of failed logins for various users, with SAP\* having the highest count at approximately 55. The table lists the time and system ID for the most recent failed logins.

| User   | Number of Failed Logins |
|--------|-------------------------|
| SAP*   | 55                      |
| DDIC   | 45                      |
| CAS    | 25                      |
| SDA    | 10                      |
| SAPSYS | 10                      |
| S...   | 5                       |

| Time                   | System ID |
|------------------------|-----------|
| 7/12/12 3:24:16.000 PM | A73       |
| 7/12/12 3:22:45.000 PM | E60       |
| 7/12/12 3:21:09.000 PM | E60       |
| 7/12/12 3:19:37.000 PM | E60       |
| 7/12/12 3:18:20.000 PM | NWT       |
| 7/12/12 3:15:36.000 PM | NWT       |
| 7/12/12 3:15:28.000 PM | NWT       |
| 7/12/12 2:02:43.000 PM | A73       |
| 7/12/12 2:02:41.000 PM | A73       |
| 7/12/12 1:57:27.000 PM | A73       |

## ArcSight Security Audit Log коннектор vs. agileSI™

- ArcSight SAL коннектор не рекомендован SAP (Транзакция SM20 предоставляет полную информацию)
- SAL содержит только часть значимой информации
- Требуется наличие знаний SAP
- Возможности ArcSight по анализу SAL событий ограничены

# Обзор решения agileSI: сравнение с ArcSight SAL коннектор

## Security Audit Log – сообщения необходимо интерпретировать

```
SAPMSSY1 1001/ITCUBE/CCF_FACTORY&&/ITCUBE/CCF_MSGRECEIVER sap-lnx-03.w2010.itc2
AUK20130717033950002718700003D3sap-lnx-SDA SAPMSSY1 1001BGRFC_EXTERN&&BGRFC_DEST_CONFIRM
sap-lnx-03.w2010.itc2AUK20130717033950000612300011Bb CAS /ITCUBE/CREATE_TRANSPORT
1001STPA&&TRINT_PROGRESS_INDICATOR 2AUK20130717033950000612300011Bb CAS
/ITCUBE/CREATE_TRANSPORT 1001STPA&&TRINT_PROGRESS_INDICATOR 2AUK2
0130717033950000612300011Bb CAS 2AUK20130717033950000612300011Bb CAS
1001F&0&R 2AU520130717033950002718700003D3sap-lnx-SDA SAPMSSY1 1001STPA&&TRINT_PROGRESS_INDICATOR
SAPMSSY1 1001BGRFC_EXTERN&&BGRFC_DEST_SHIP sap-lnx-03.w2010.itc2AUK20130717033950002718700003D3sap-lnx-SDA
717033950002718700003D3sap-lnx-SDA SAPMSSY1 1001/ITCUBE/CCF_FACTORY&&/ITCUBE/CCF_MSGRECEIVER sap-lnx-03.w2010.itc2AUK20130
sap-lnx-03.w2010.itc2AUK20130717033950000612300011Bb CAS /ITCUBE/CREATE_TRANSPORT
1001STPA&&TRINT_PROGRESS_INDICATOR 2AUK20130717033950000612300011Bb CAS
/ITCUBE/CREATE_TRANSPORT 1001STPA&&TRINT_PROGRESS_INDICATOR 2AUK201307170
33950002718700003D3sap-lnx-SDA SAPMSSY1 1001BGRFC_EXTERN&&BGRFC_DEST_CONFIRM
sap-lnx-03.w2010.itc2AUK20130717033950002719300009D9sap-lnx-SDA SAPMSSY1 100
1ARFC&&ARFC_DEST_CONFIRM sap-lnx-03.w2010.itc2AU520130717033950002719300009D9sap-lnx-SDA
SAPMSSY1 1001R&0&P sap-lnx-03.w2010.itc2AUK2013071703395
0002719300009D9sap-lnx-SDA SAPMSSY1 1001SRFC_SERVER_RESOURCES&&RFC_SERVER_GROUP_RESOURCES
sap-lnx-03.w2010.itc2AU520130717033950002719000006D6sap-lnx-SDA SAPMSSY1 1001R&0
&P sap-lnx-03.w2010.itc2AUK20130717033950002719000006D6sap-lnx-SDA
SAPMSSY1 1001ERFC&&ARFC_DEST_SHIP sap-lnx-03.w2010.itc2AUK20130717033950002
719000006D6sap-lnx-SDA SAPMSSY1 1001ARFC&&ARFC_DEST_CONFIRM sap-lnx-03.w2010.itc2AUK20130717033950002
sap-lnx-03.w2010.itc2AU520130717033950002719000006D6sap-lnx-SDA SAPMSSY1 1001R&0&P
EMSSY1 1001ERFC&&ARFC_DEST_SHIP sap-lnx-03.w2010.itc2AUK201307170339500027190
00006D6sap-lnx-SDA SAPMSSY1 1001ARFC&&ARFC_DEST_CONFIRM SA
sap-lnx-03.w2010.itc2AU520130717033950002719000006D6sap-lnx-SDA SAPMSSY1 1001R&0&P
00006D6sap-lnx-SDA SAPMSSY1 1001ERFC&&ARFC_DEST_SHIP sap-lnx-03.w2010.itc2AUK2013071703395000271900000
6D6sap-lnx-SDA SAPMSSY1 1001ARFC&&ARFC_DEST_CONFIRM SAPMSS
sap-lnx-03.w2010.itc2AU520130717033950002718500001D1sap-lnx-SDA SAPMSSY1 1001F&0&R
sap-lnx-03.w2010.itc2AUK20130717033950002718500001D1sap-lnx-SDA SAPMSSY1
1001BGRFC_EXTERN&&BGRFC_DEST_SHIP sap-lnx-03.w2010.itc2AU520130717033950002719000006D6s
ap-lnx-SDA SAPMSSY1 1001R&0&P sap-
lnx-03.w2010.itc2AUK20130717033950002719000006D6sap-lnx-SDA SAPMSSY1 1001ERFC&&ARFC_DEST_SHI
P sap-lnx-03.w2010.itc2AUK20130717033950002719000006D6sap-lnx-SDA SAPMSSY1
1001ARFC&&ARFC_DEST_CONFIRM sap-lnx-03.w2010.itc2AU520130717033950002719000006D6sap-l
nx-SDA SAPMSSY1 1001R&0&P sap-lnx-
03.w2010.itc2AUK20130717033950002719000006D6sap-lnx-SDA SAPMSSY1 1001ERFC&&ARFC_DEST_SHIP
DA sap-lnx-03.w2010.itc2AUK20130717033950002719000006D6sap-lnx-SDA SAPMSSY1
1001ARFC&&ARFC_DEST_CONFIRM sap-lnx-03.w2010.itc2AU520130717033950002719000006D6sap-lnx-S
SAPMSSY1 1001R&0&P sap-lnx-03.w
```

# Обзор решения agileSI: сравнение с ArcSight SAL коннектор

- Security Audit Log показывает что что-то произошло
- Что именно произошло можно узнать только сопоставив информацию с другими источниками, такими как Change Documents или Table Change Logging

User Master Record changes: SAL does not show what happened exactly - time range: 12h

« prev 1 2 3 4 5 6 7 8 9 10 next »

|   | _time ↕                | changed by ↕ | Action ↕                       |
|---|------------------------|--------------|--------------------------------|
| 1 | 7/17/13 7:59:57.000 PM | SDA          | User Master Record T02 Changed |
| 2 | 7/17/13 7:59:57.000 PM | SDA          | User Master Record T02 Changed |

<< Что-то произошло >>

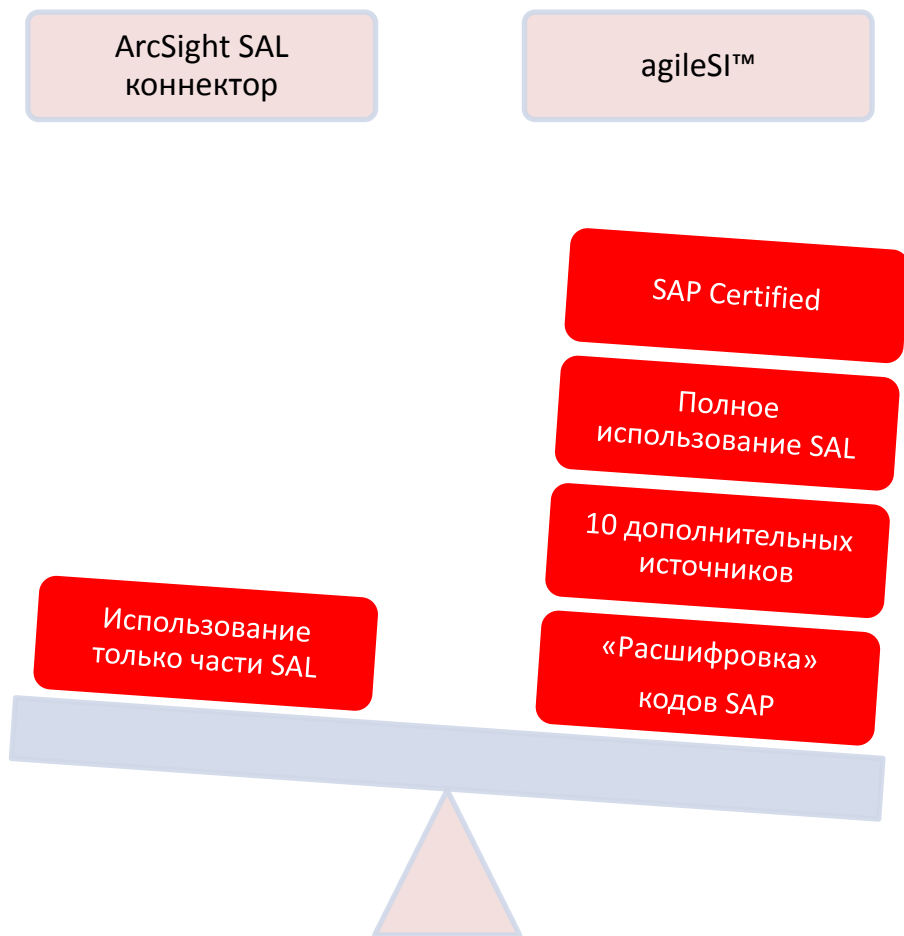
Change Documents of User Master Records - time range: 12h

« prev 1 2 3 4 5 6 7 8 9 10 next »

|   | _time ↕                | User Account ↕ | Action ↕        | From value ↕ | To value ↕ |
|---|------------------------|----------------|-----------------|--------------|------------|
| 1 | 7/17/13 7:59:58.000 PM | T02            | Profile deleted | SAP_ALL      |            |
| 2 | 7/17/13 7:59:55.000 PM | T02            | Profile added   |              | SAP_ALL    |

<< Что именно произошло >>

# Обзор решения agileSI: сравнение с ArcSight SAL коннектор



## Дополнительные источники agileSI™

- Table Data
- System Log of SAP systems
- Profile or System parameter settings
- Gateway Log and Settings
- Table Change logs
- Access Control, SoD Conflicts
- SCDO Change Documents (generally)
- Change Documents in regards to Changes to User Master Records
- Transport: import of objects; import at unusual time frame; STMS settings
- SAP security patch recommendations

## **Благодаря автоматизации процесса мониторинга критических событий и параметров безопасности, agileSI обеспечивает:**

- Постоянный анализ систем SAP на предмет наличия эксплуатационных уязвимостей, ошибок в конфигурации, превышения полномочий, мониторинг критических транзакций и действий пользователей
- Автоматизацию процесса сбора, корреляции, визуализации информации и формирования отчетов
- Снижение затрат на аудит и привлечение дорогостоящих экспертов SAP
- Обнаружение атак на системы SAP
- Возможность обрабатывать события безопасности систем SAP специалистами SOC

Вопросы?



# Спасибо за внимание

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>

e-mail: [npetrov@DialogNauka.ru](mailto:npetrov@DialogNauka.ru)