Использование решения agileSI
для мониторинга информационной безопасности систем SAP

ДиалогНаука

Обо мне

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

ДиалогНаука

Работал в компаниях Philip Morris, Kerberus,

MIS Training Institute, (ISC)2, Ernst & Young

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)

Почему важен мониторинг ИБ систем SAP: особенности

Особенности систем SAP:

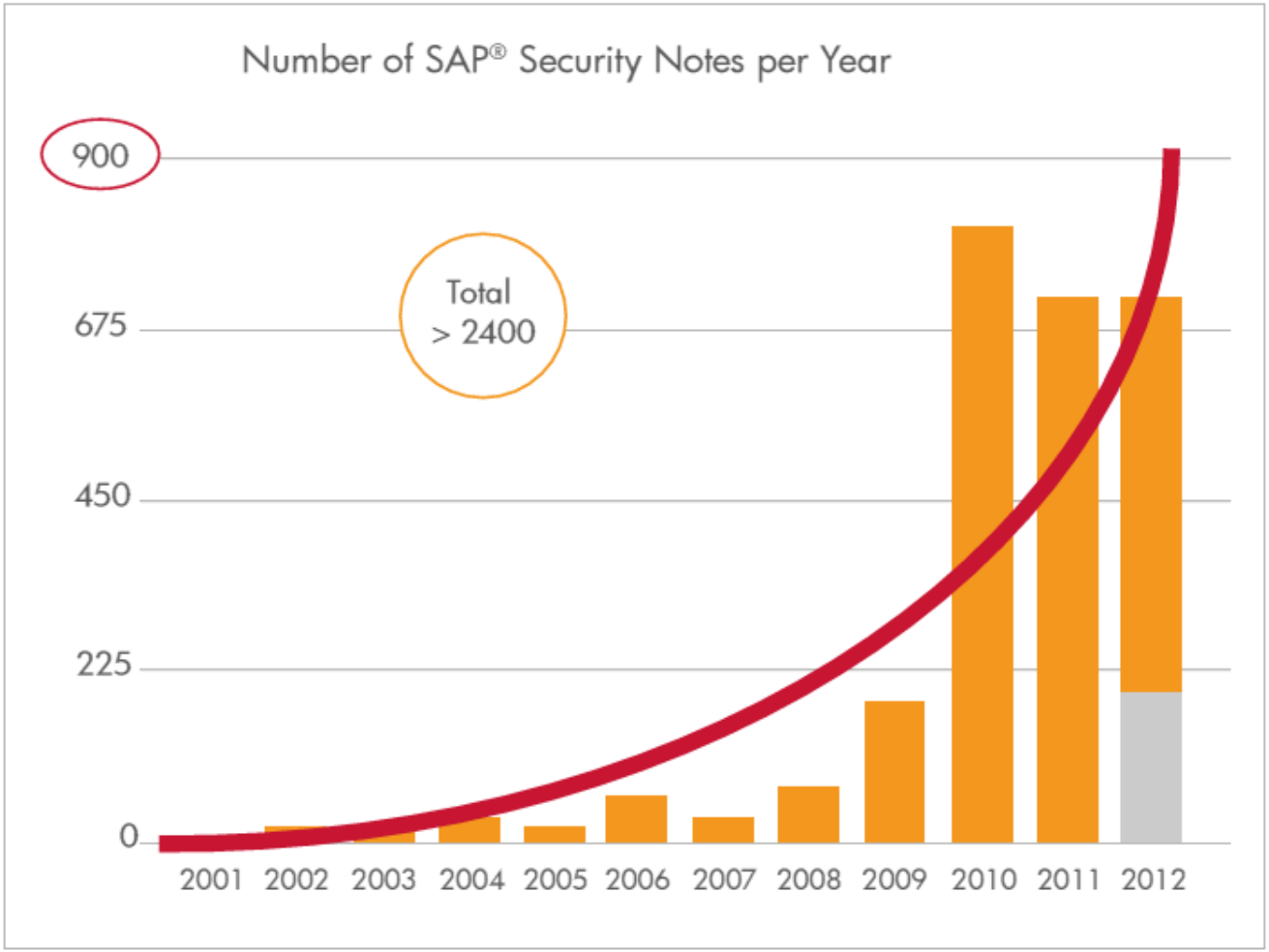
- **Кастомизация** – нет 2-х одинаковых SAP систем
- **Сложность системы** отрицательно сказывается на ее безопасности. SAP сложные распределенные системы, включающие в себя БД, сервера приложений, различные типы клиентов. В стандартных настройках более 1000 параметров
- **Высокий риск** – перерыв в 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
- Snifffing (перехват) учетных записей и паролей
- Уязвимости SAP Gateway - неограниченный доступ к системе

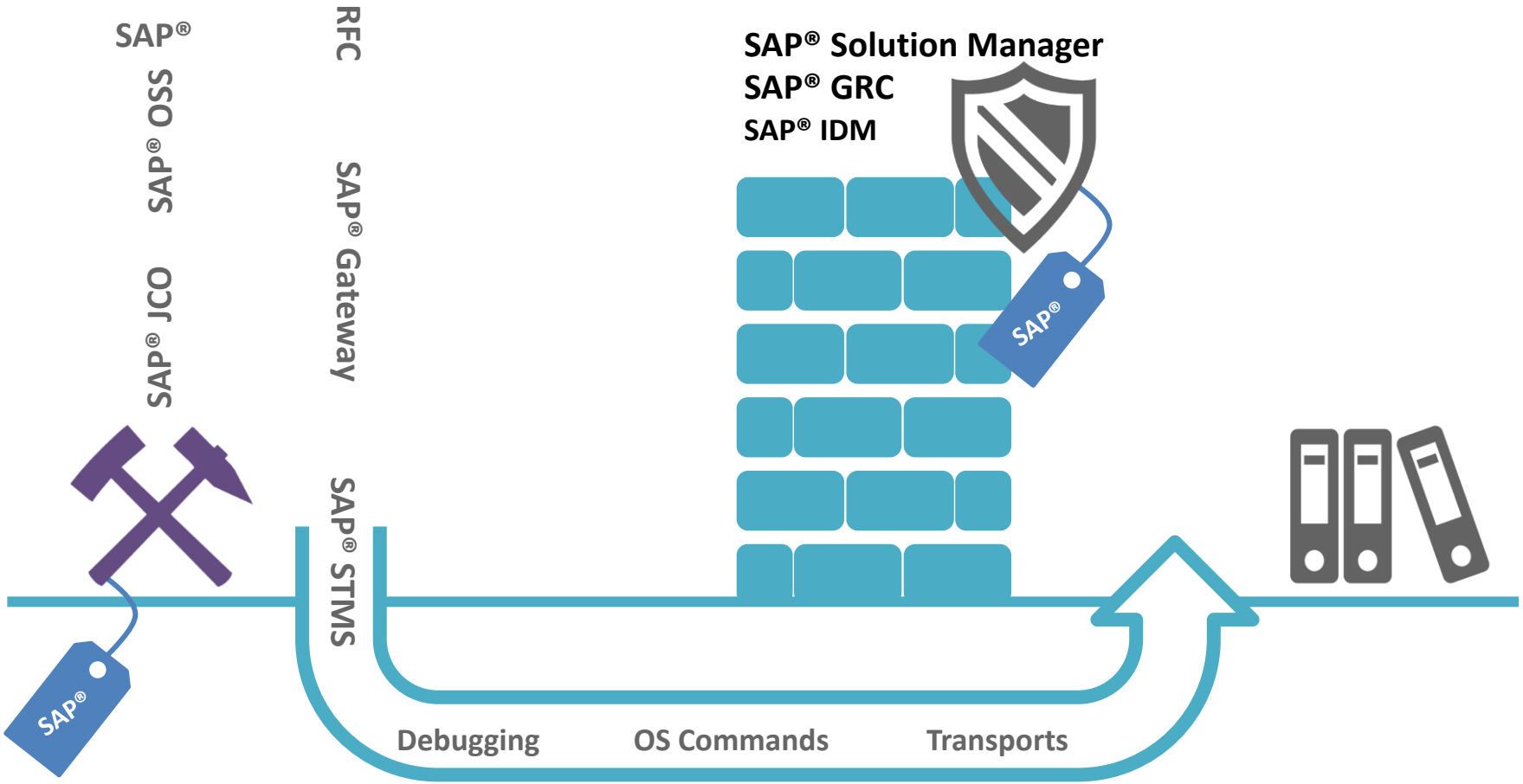
Почему важен мониторинг ИБ систем SAP: Security Notes



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

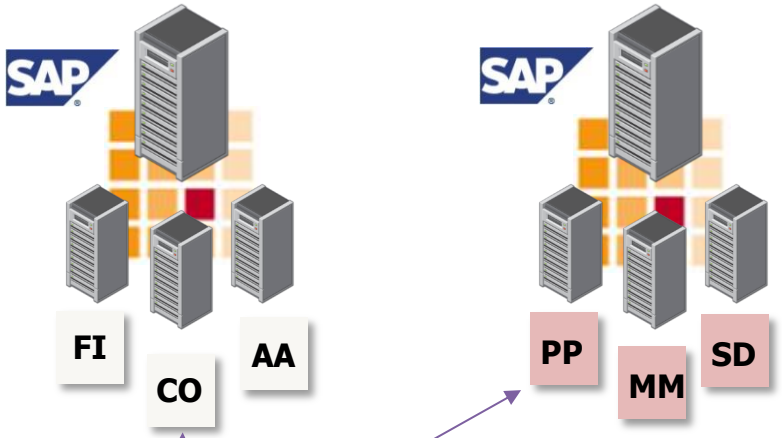
SAP® Certified
Integration with SAP Applications

Обзор решения agileSI

Агенты

Настройка

Планирование работы



Сбор

Центр управления агентами

Управление агентами

Преобразование форматов событий

Интерфейс WebDynPro

Администри-рование

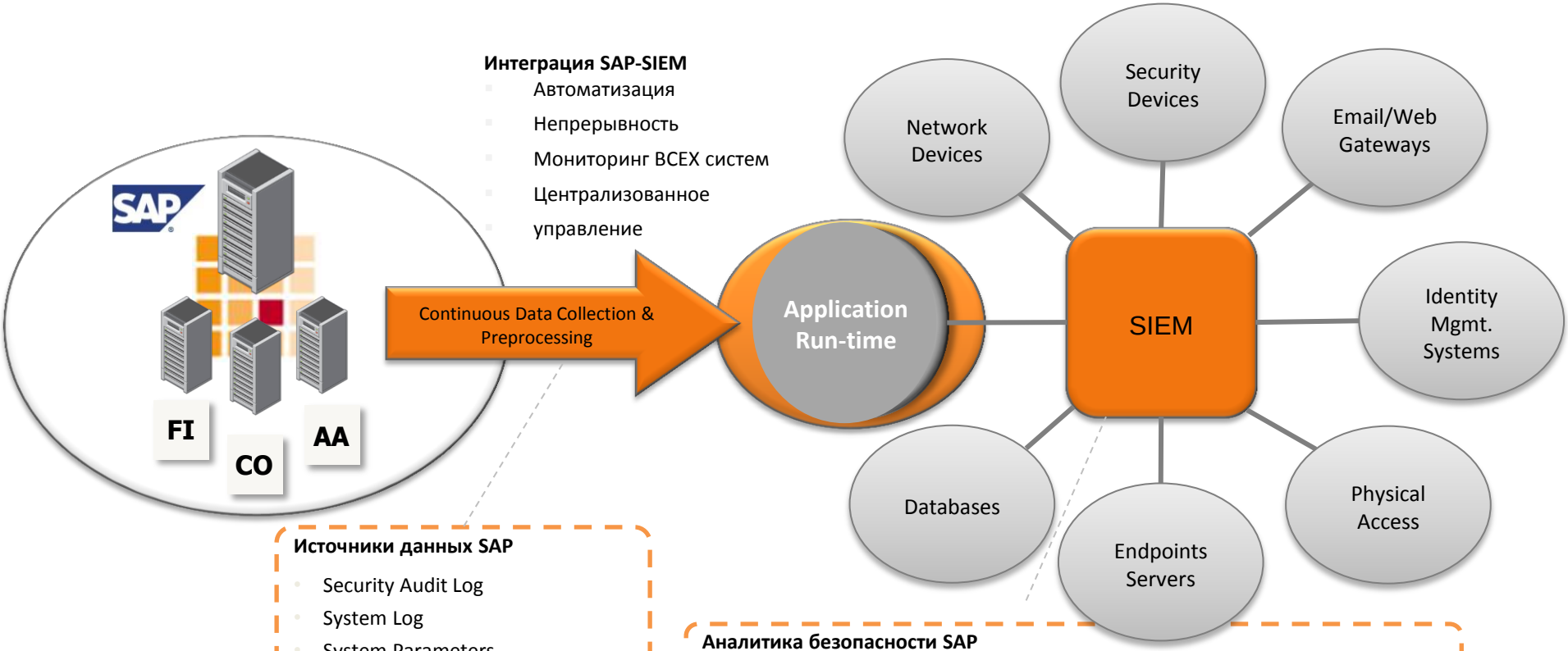
Внешняя аналитическая часть на базе SIEM

Информационные панели, отчеты, уведомления

Корреляция и анализ событий безопасности

Аналитика

Обзор решения agileSI



Источники данных SAP

- Security Audit Log
- System Log
- System Parameters
- Tables
- Transport Log
- Gateway Config & Log
- Change Documents
- Table Change Logging
- Access Control
- Security Notes

Аналитика безопасности SAP

- использует:
  - DSAG Audit Guidelines
  - SAP Security Recommendations
  - SAP Pentesting Practises
- Шаблоны обработки, представления и отчетности
- Категоризация SAP событий в SIEM
- Отслеживание критических параметров, правил и событий

Обзор решения agileSI: примеры использования

Источник	События/Данные	Примеры использования	
Security Audit Log	События безопасности SAP систем	• Попытки подбора пароля • Создание /удаление/блокировка пользователя	• Изменения пароля • Запуск отчетов
System Log	Системный журнал SAP , ошибки, security, события безопасности...	• Режим отладки • Исполнение команд ОС	• Пользователь выключает Table logging
System Parameters	Конфигурация SAP	• Password policy • SNC encryption status	• SAP Gateway
Tables	Данные в Tables	• Настройки Системы и Клиента • Конфигурация RFC	• Single Sign-On / Logon Tickets • Любые данные
Transport Log	Изменения посредством transports	• Изменения ролей • Transports критичных объектов, в необычное время	
Gateway Config & Log	Взаимодействие с внешними программами	• Мониторинг внешних вызовов	
Change Documents	Изменения Business Objects	• Роли, профили, User master data	
Table Change Logging	Изменения данных хранимых в таблицах	• Мониторинг (master data)	
Access Control	Проверка комбинации объектов авторизации	• Параметры учётных записей, конфликты SoD	
Security Notes	Статус SAP RSECNOTE	• Отсутствует реализация Security notes	

Обзор решения agileSI: использование DSAG

DSAG : 100+ проверок

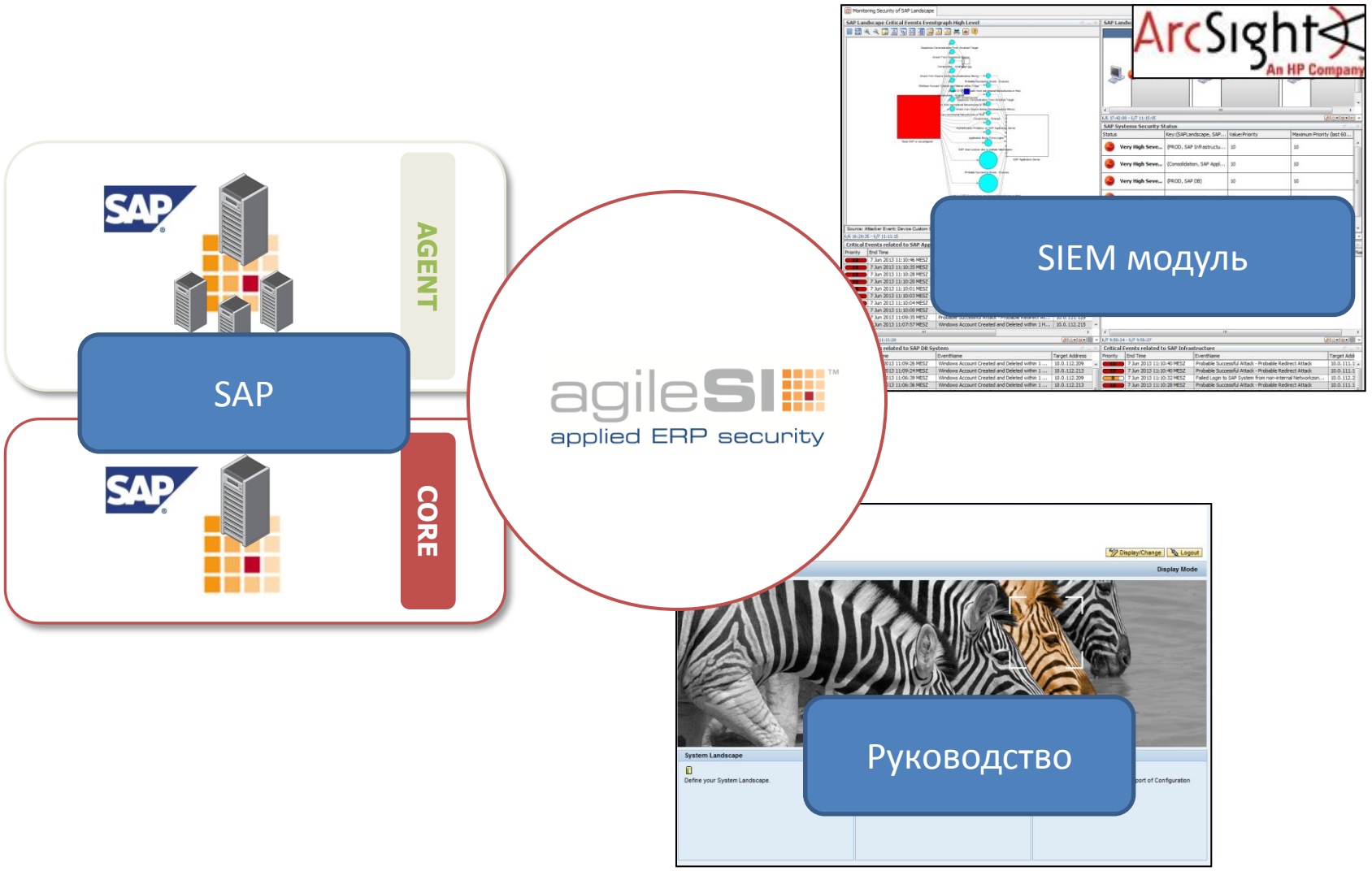
Рекомендация DSAG	Применение agileSI
1. Управление Доступом, SoD конфликты	agileSI проверяет SAP_ALL авторизацию и другие конфликты
2. Мониторинг стандартных учетных записей SAP	agileSI проверяет статус блокировки и активность стандартных учетных записей
3. Выключение / изменение авторизаций	agileSI 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

Обзор решения agileSI: мониторинг транзакций

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)

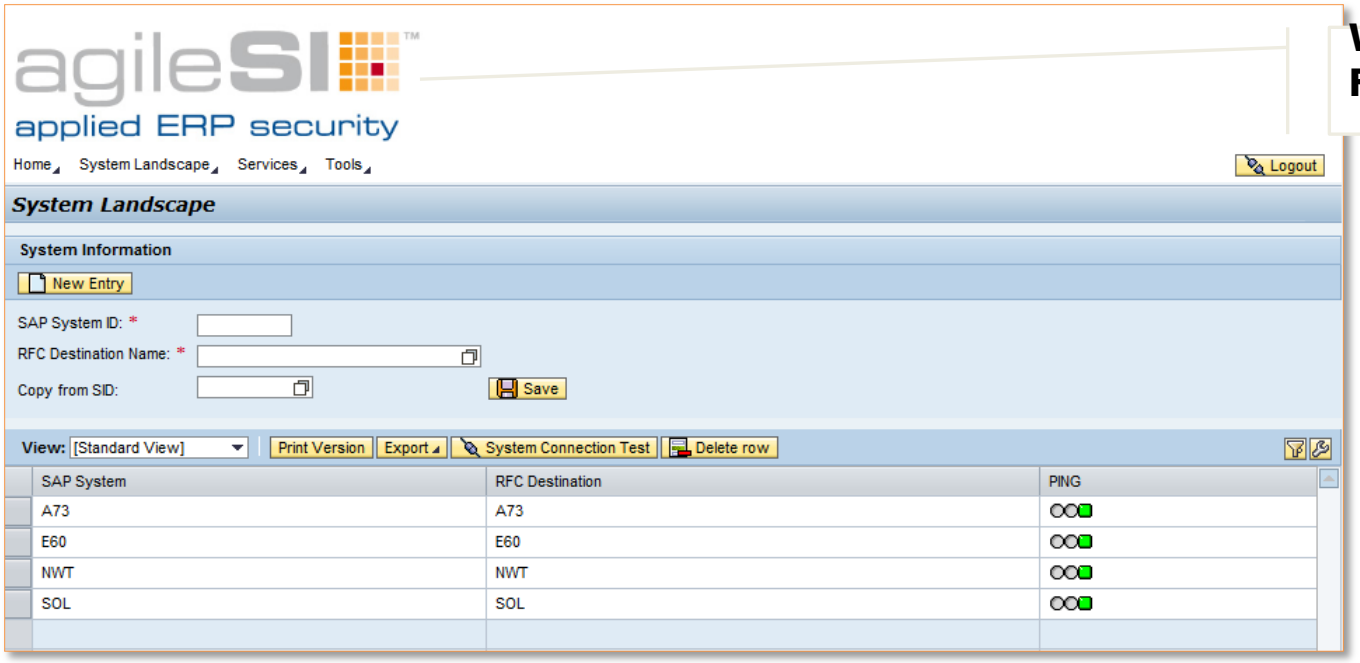
Обзор решения agileSI: установка



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)



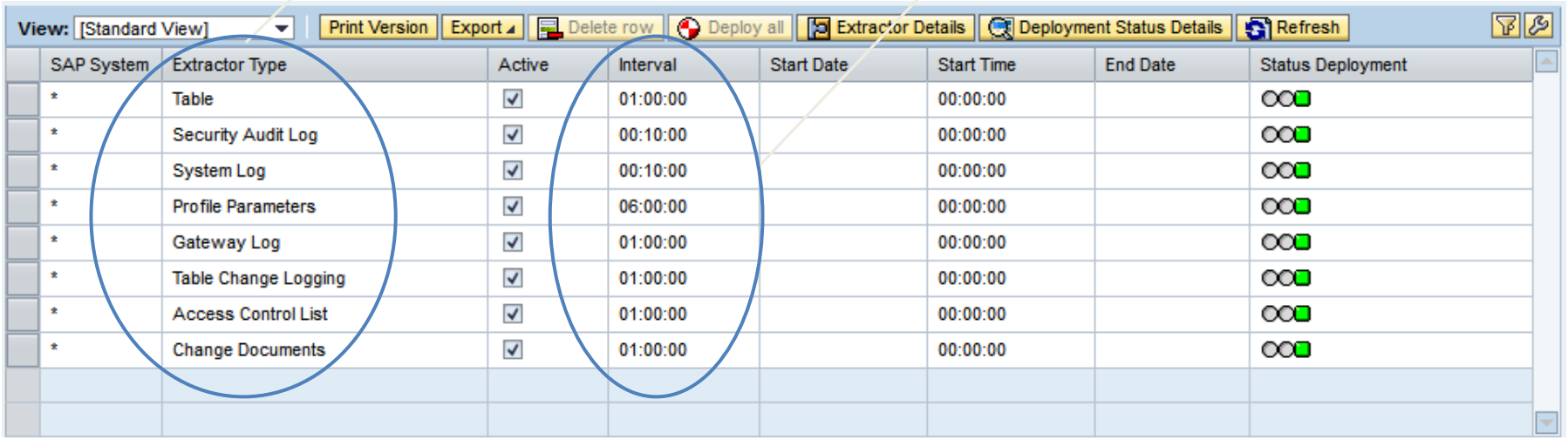
WebDynPro ABAP Frontend

Обзор решения agileSI: установка

Управление экстракторами

Определяем экстракторы

Определяем интервалы

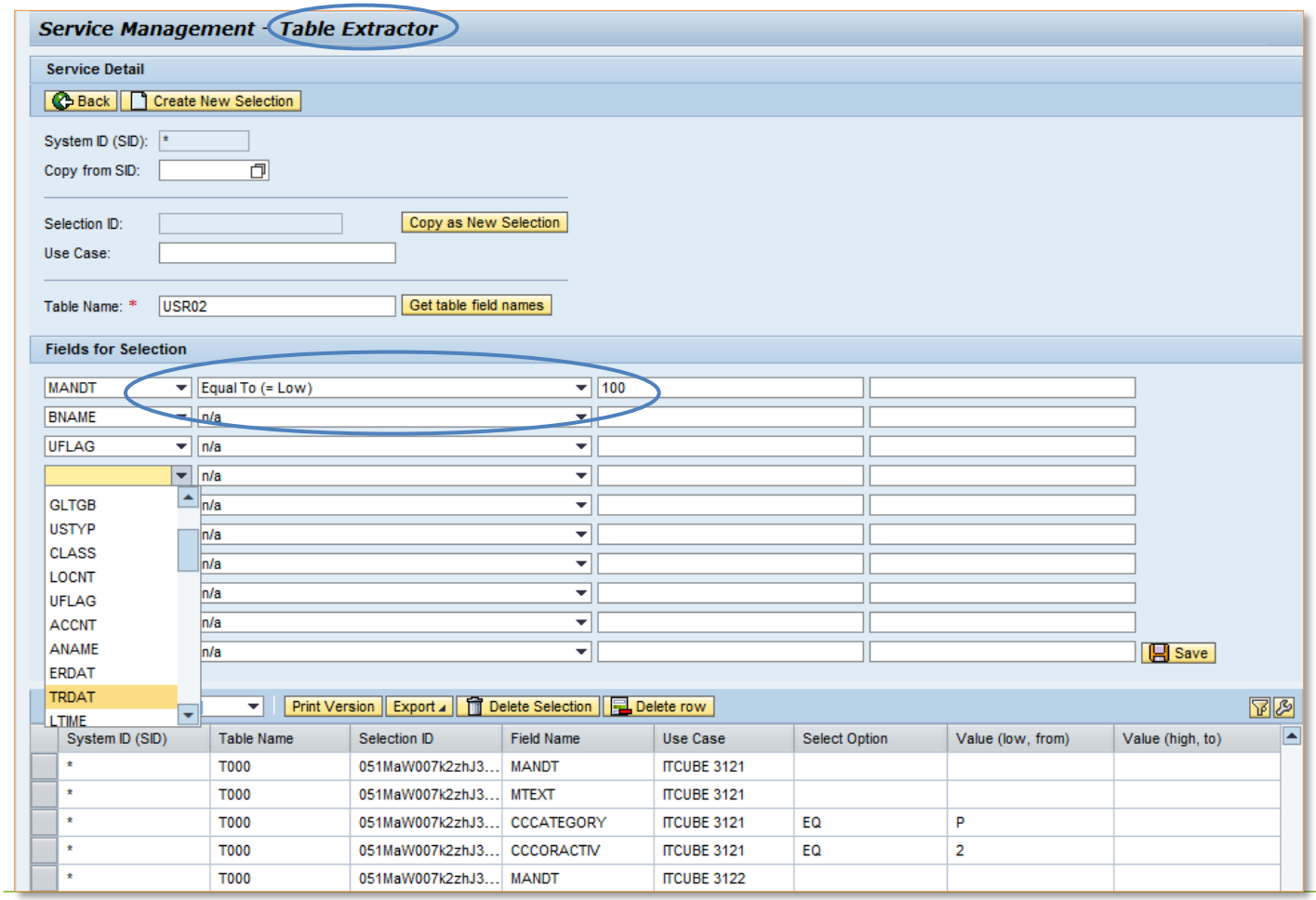


SAP System	Extractor Type	Active	Interval	Start Date	Start Time	End Date	Status Deployment
*	Table	☑	01:00:00		00:00:00		
*	Security Audit Log	☑	00:10:00		00:00:00		
*	System Log	☑	00:10:00		00:00:00		
*	Profile Parameters	☑	06:00:00		00:00:00		
*	Gateway Log	☑	01:00:00		00:00:00		
*	Table Change Logging	☑	01:00:00		00:00:00		
*	Access Control List	☑	01:00:00		00:00:00		
*	Change Documents	☑	01:00:00		00:00:00		

Обзор решения agileSI: установка

Кастомизация экстракторов

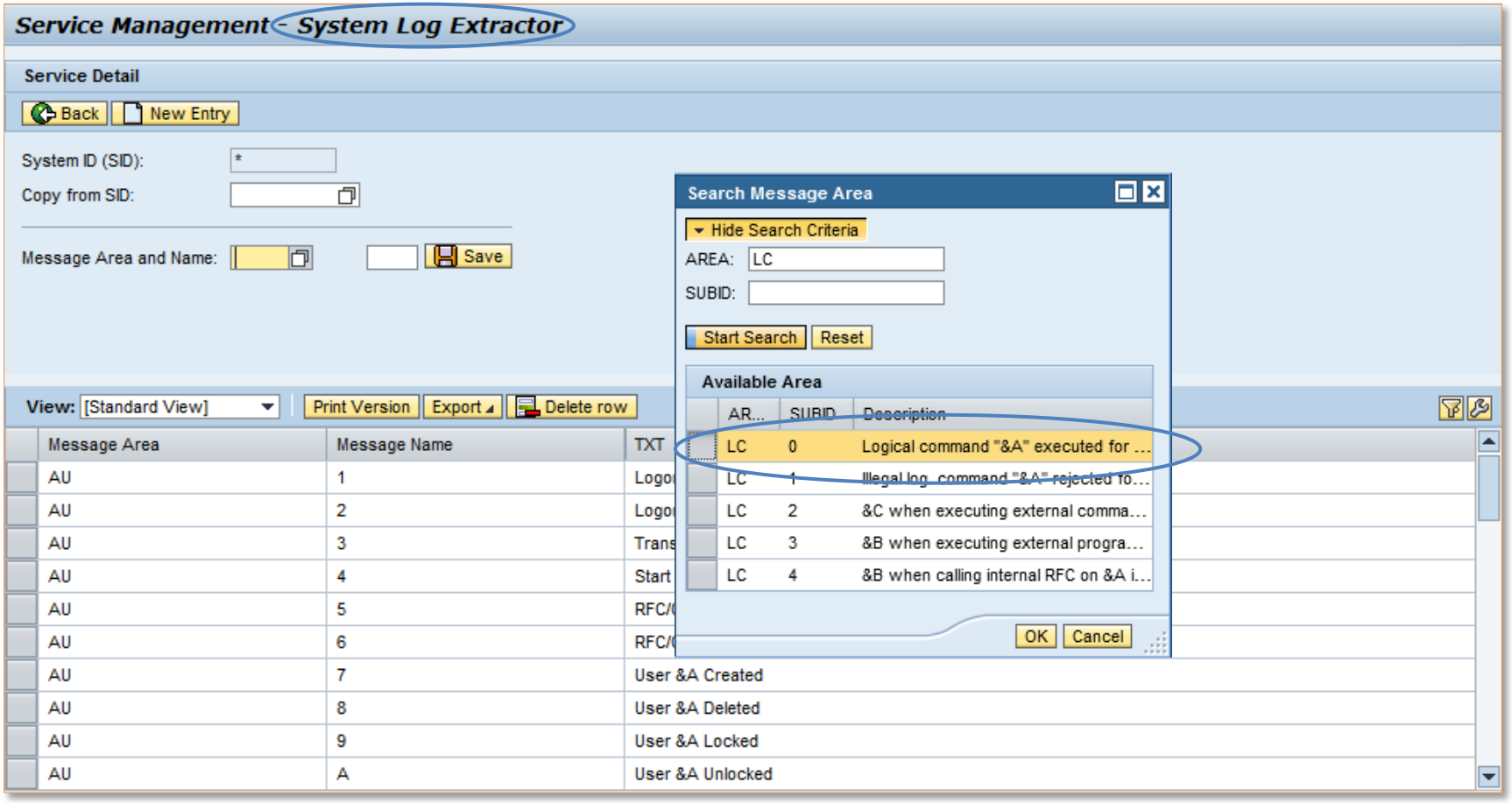
Поддержка регулярных выражений



Обзор решения agileSI: установка

Кастомизация экстракторов

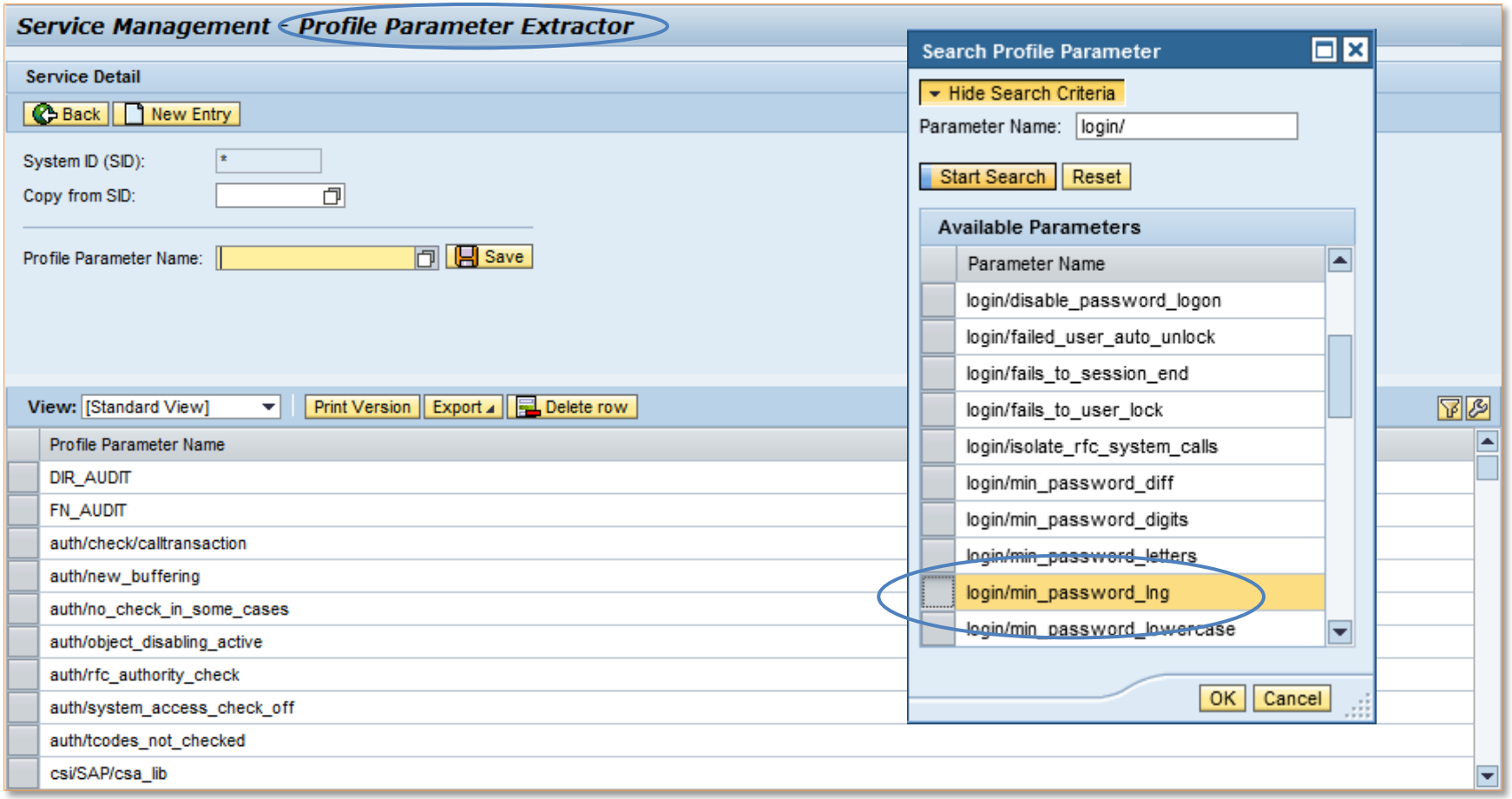
Выбор из 1800 параметров



Обзор решения agileSI: установка

Кастомизация экстракторов

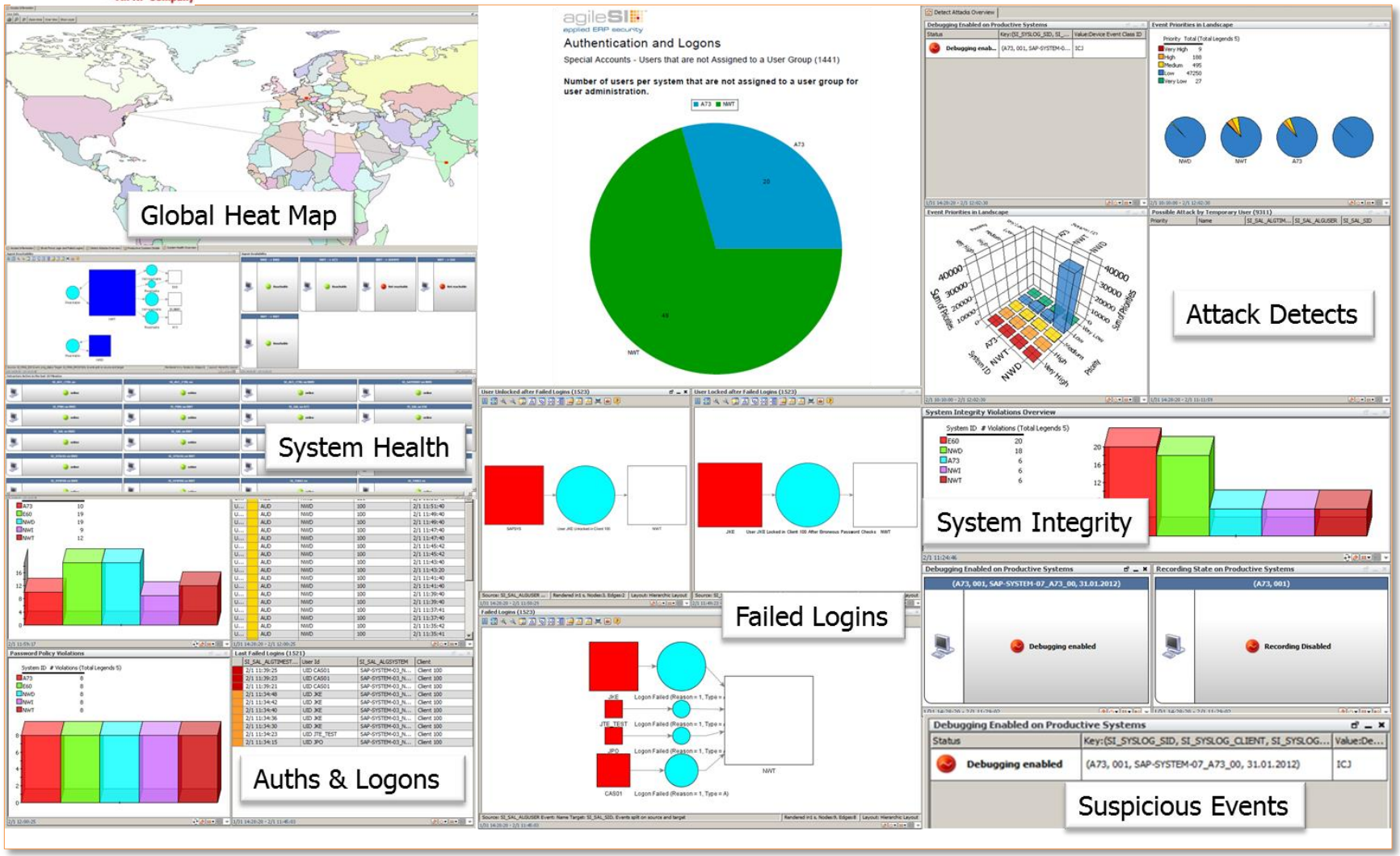
Выбор из 1000+ параметров



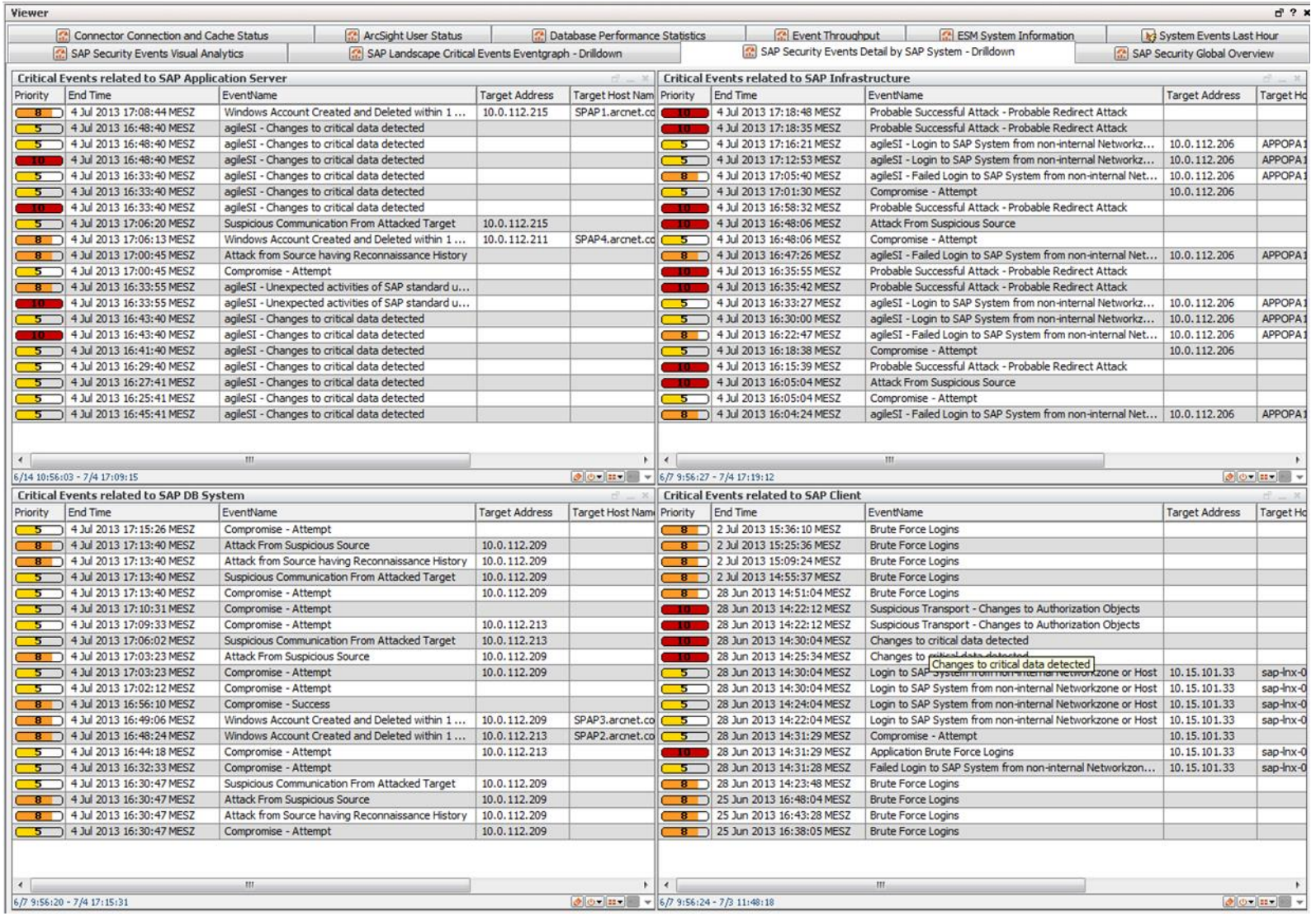
Обзор решения agileSI: поддержка SIEM

Обзор решения agileSI

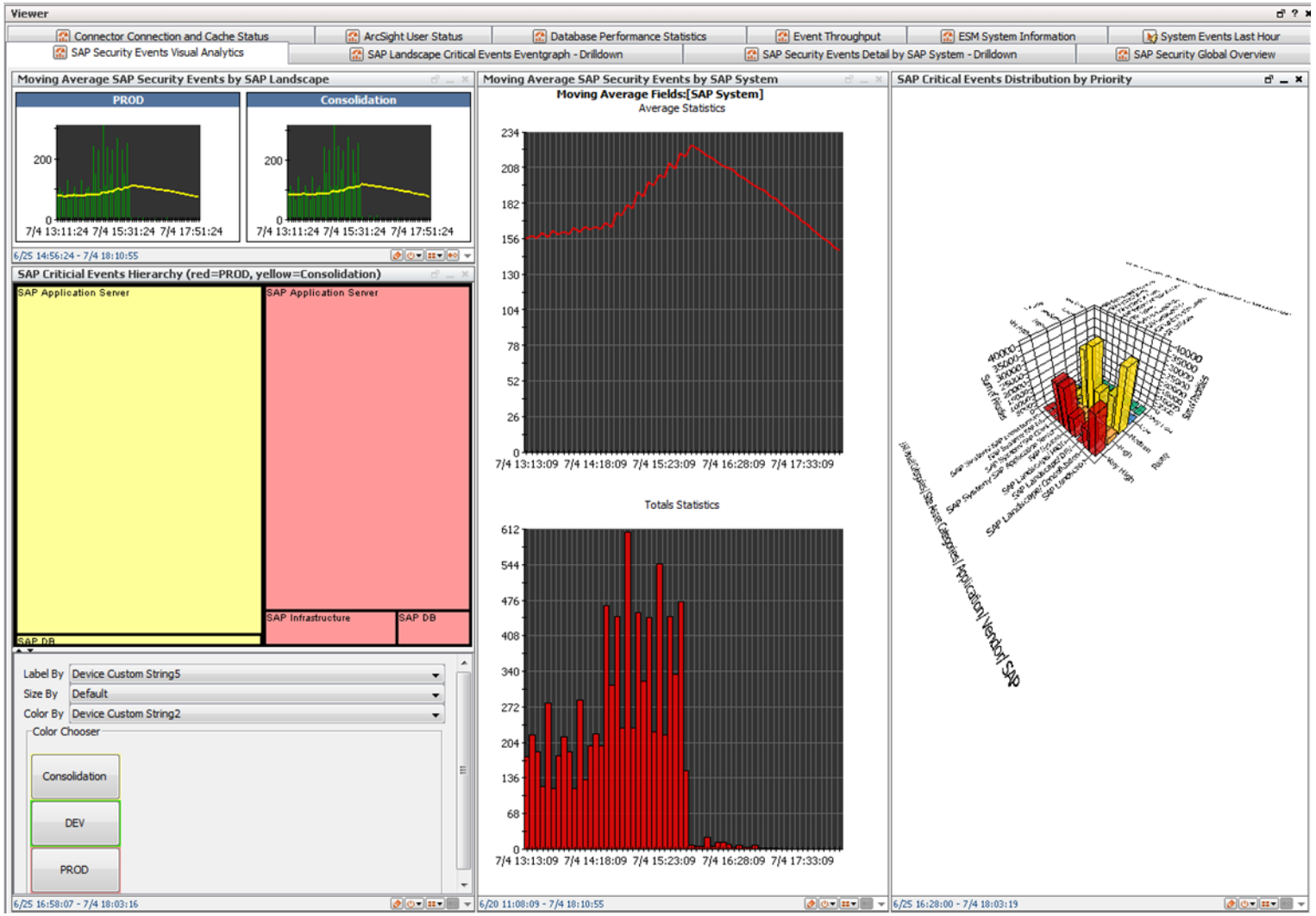
ArcSight
An HP Company



Обзор решения agileSI

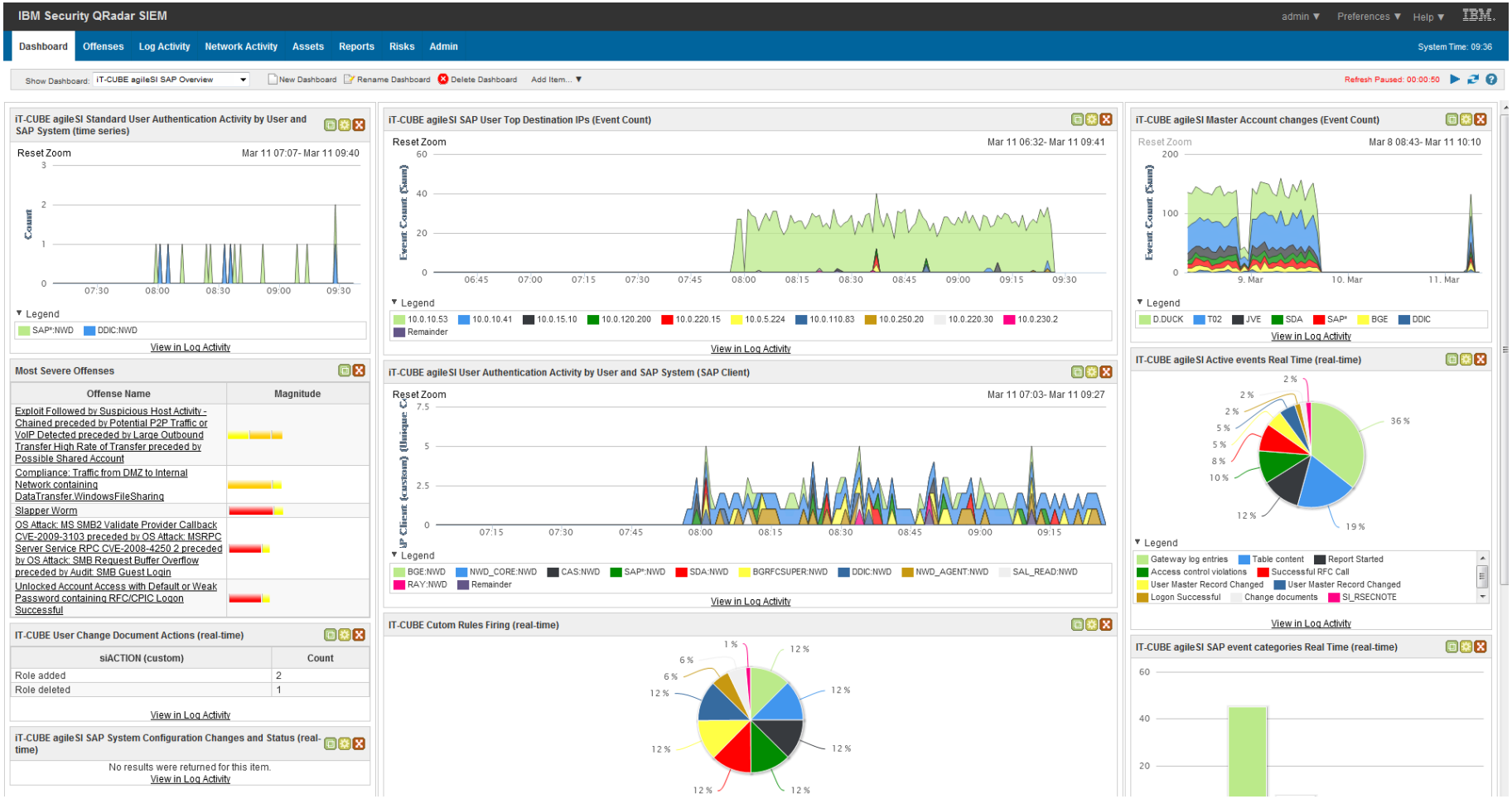


Обзор решения agileSI



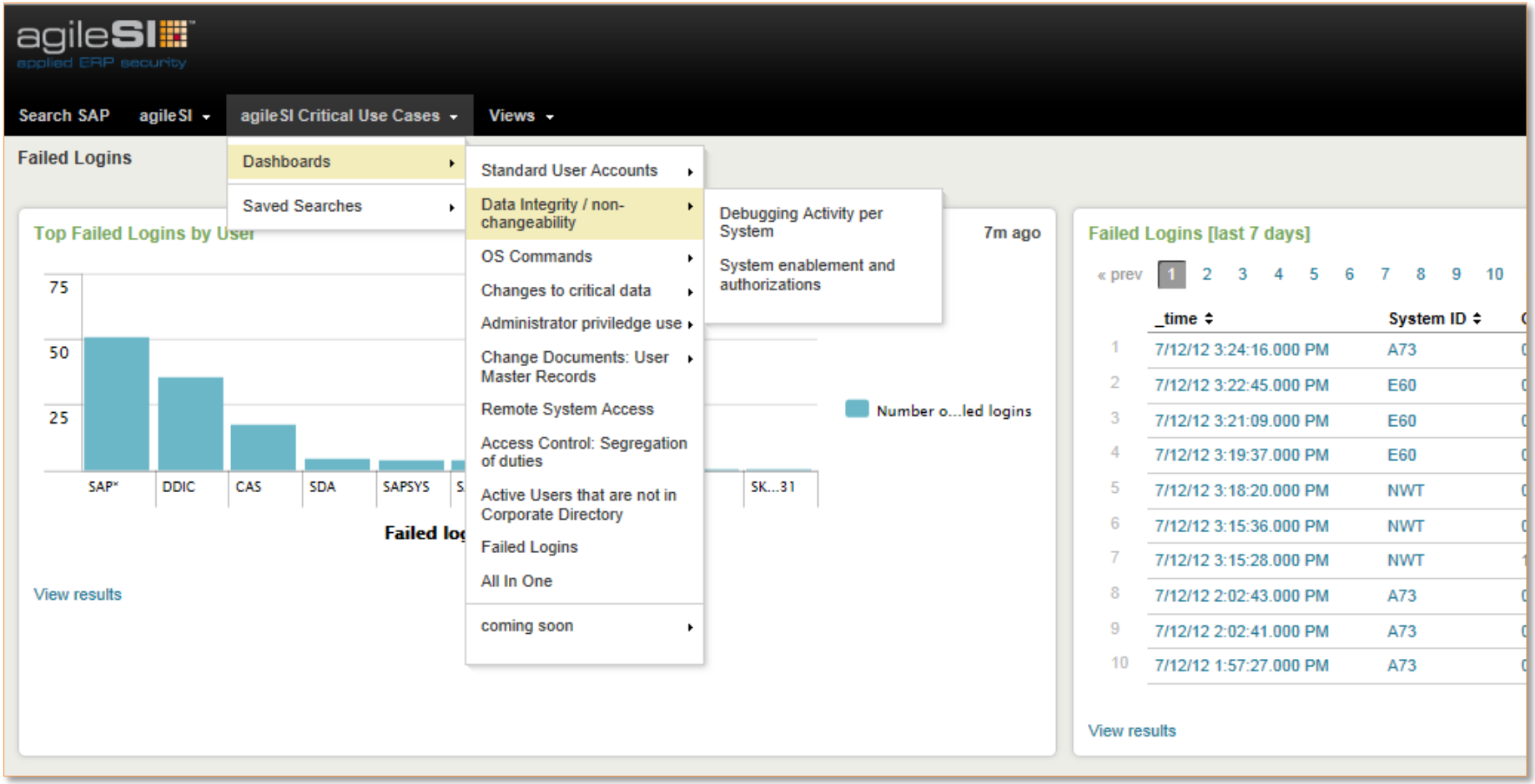
Обзор решения agileSI

agileSI™ IBM Qradar:



Обзор решения agileSI

agileSI™ Splunk:



Обзор решения agileSI: сравнение с ArcSight SAL коннектор

ArcSight Security Audit Log коннектор vs. agileSI™

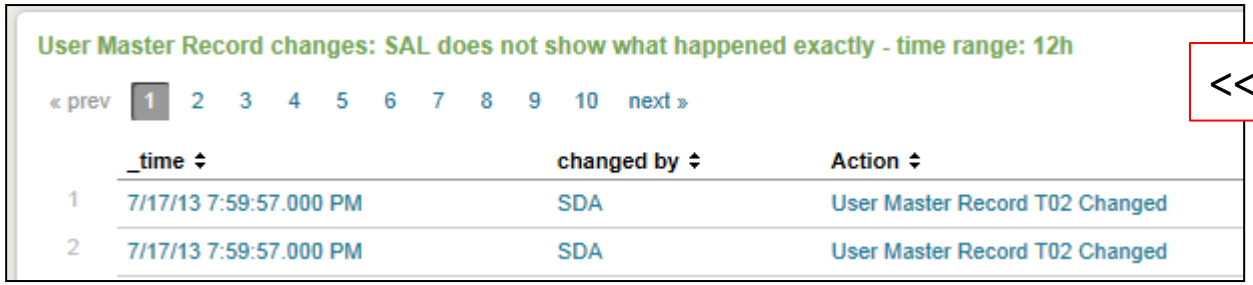
- ArcSight SAL коннектор не рекомендован SAP (Транзакция SM20 предоставляет полную информацию)
- SAL содержит только часть значимой информации
- Требует наличия знаний SAP
- Возможности ArcSight по анализу SAL событий ограничены

Обзор решения agileSI: сравнение с ArcSight SAL коннектор

Security Audit Log – сообщения необходимо интерпретировать

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

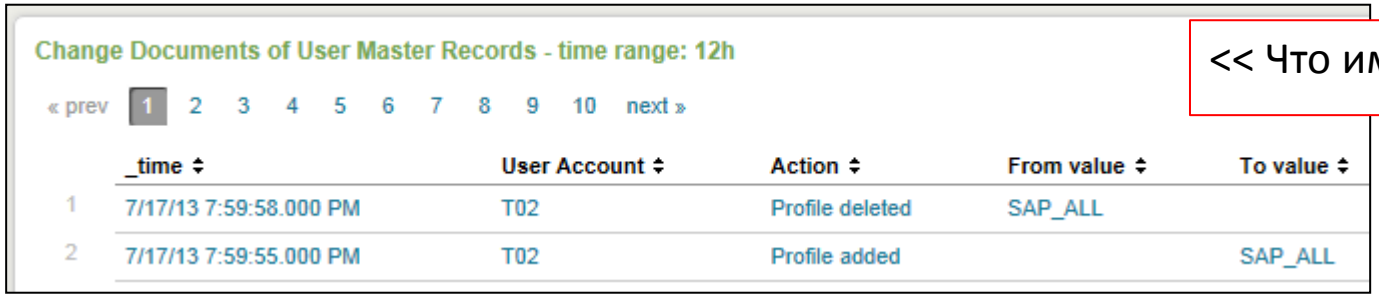


User Master Record changes: SAL does not show what happened exactly - time range: 12h

« 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>>



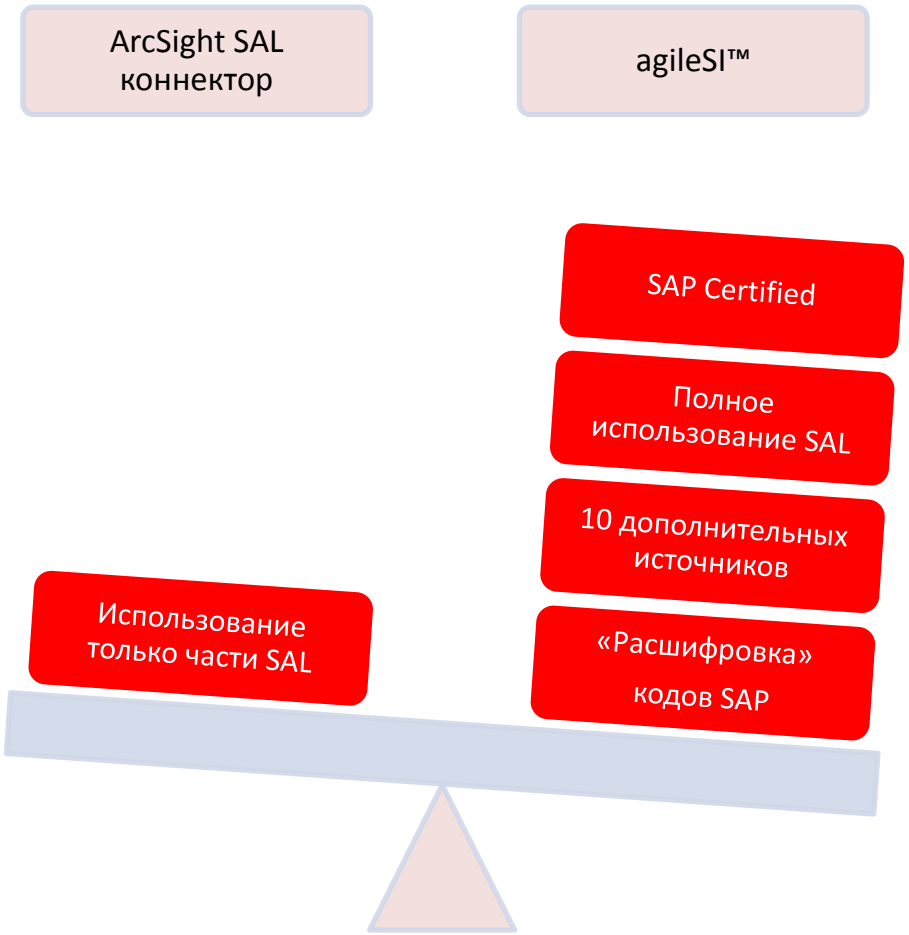
Change Documents of User Master Records - time range: 12h

« 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

Выводы

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?

Наши контакты

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