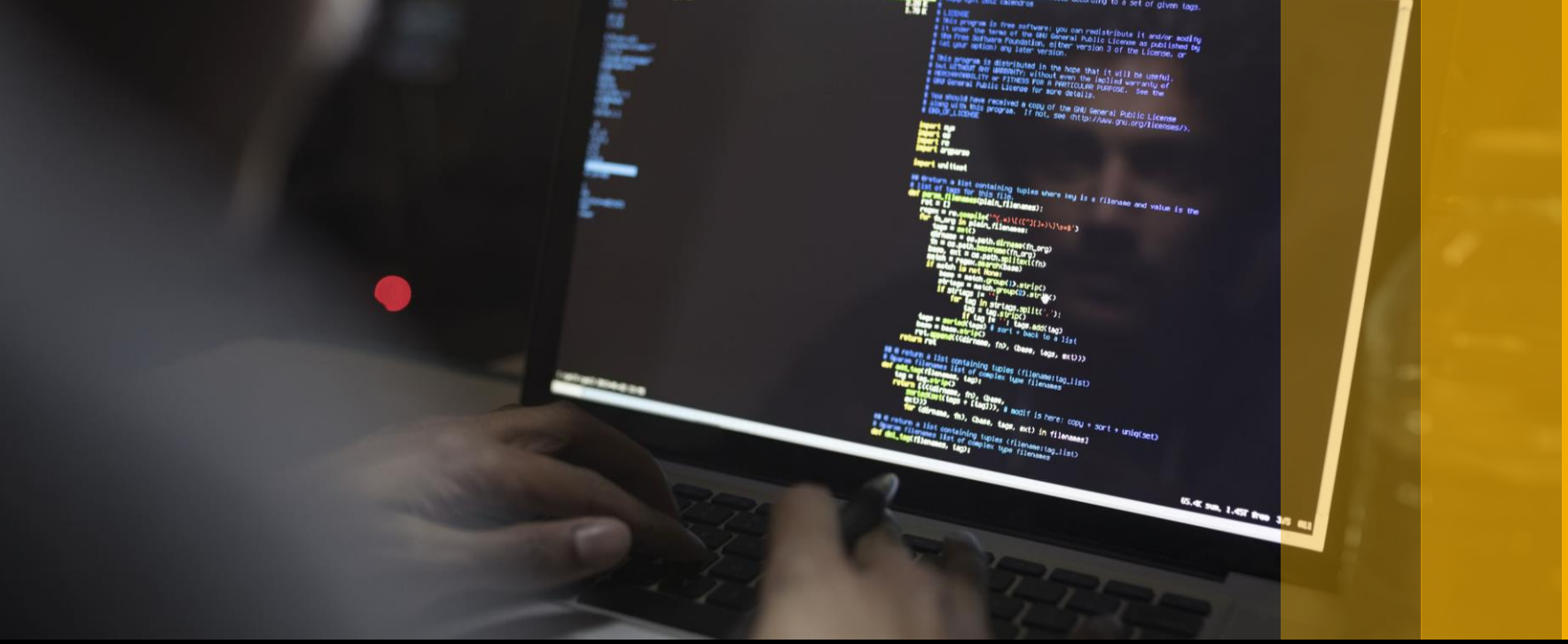


Кибербезопасность внутрикорпоративных данных

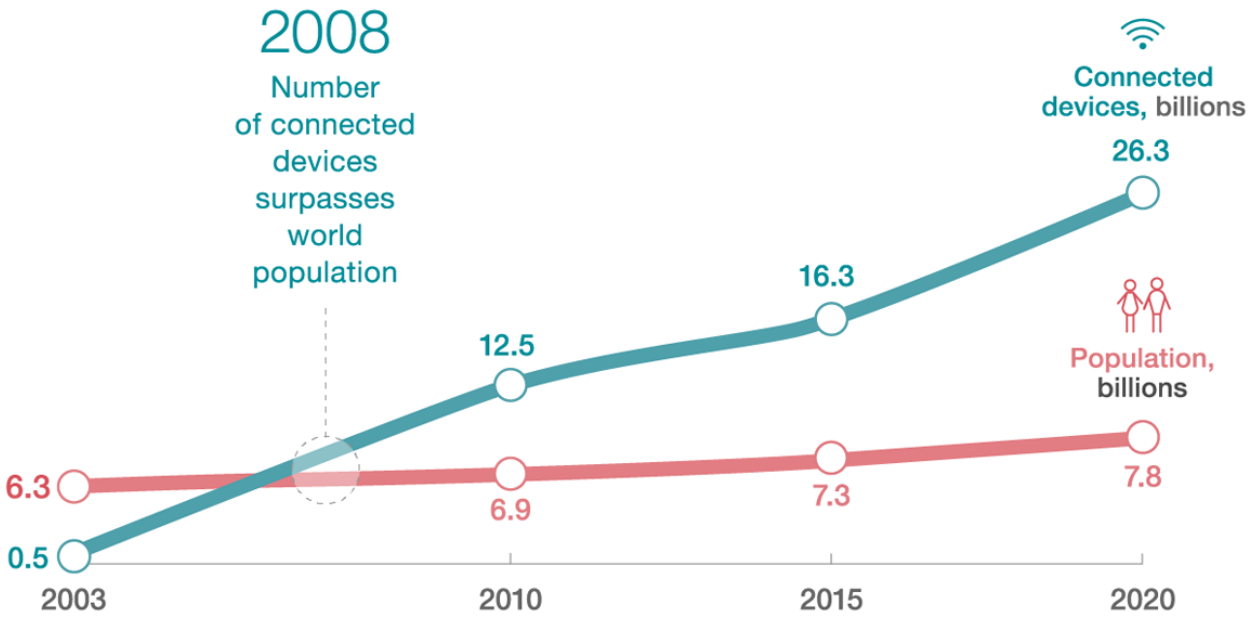
Прокудин Аркадий, Менеджер направления GRC и корпоративная безопасность, SAP CIS
Июнь 19, 2018

PUBLIC

THE BEST RUN SAP

Будущее наступило вчера

Online connectivity—including a plethora of connected devices—is growing exponentially.



McKinsey&Company | Source: Cisco; United Nations

The Global Risk Report 2018

What is the impact and likelihood of global risks?

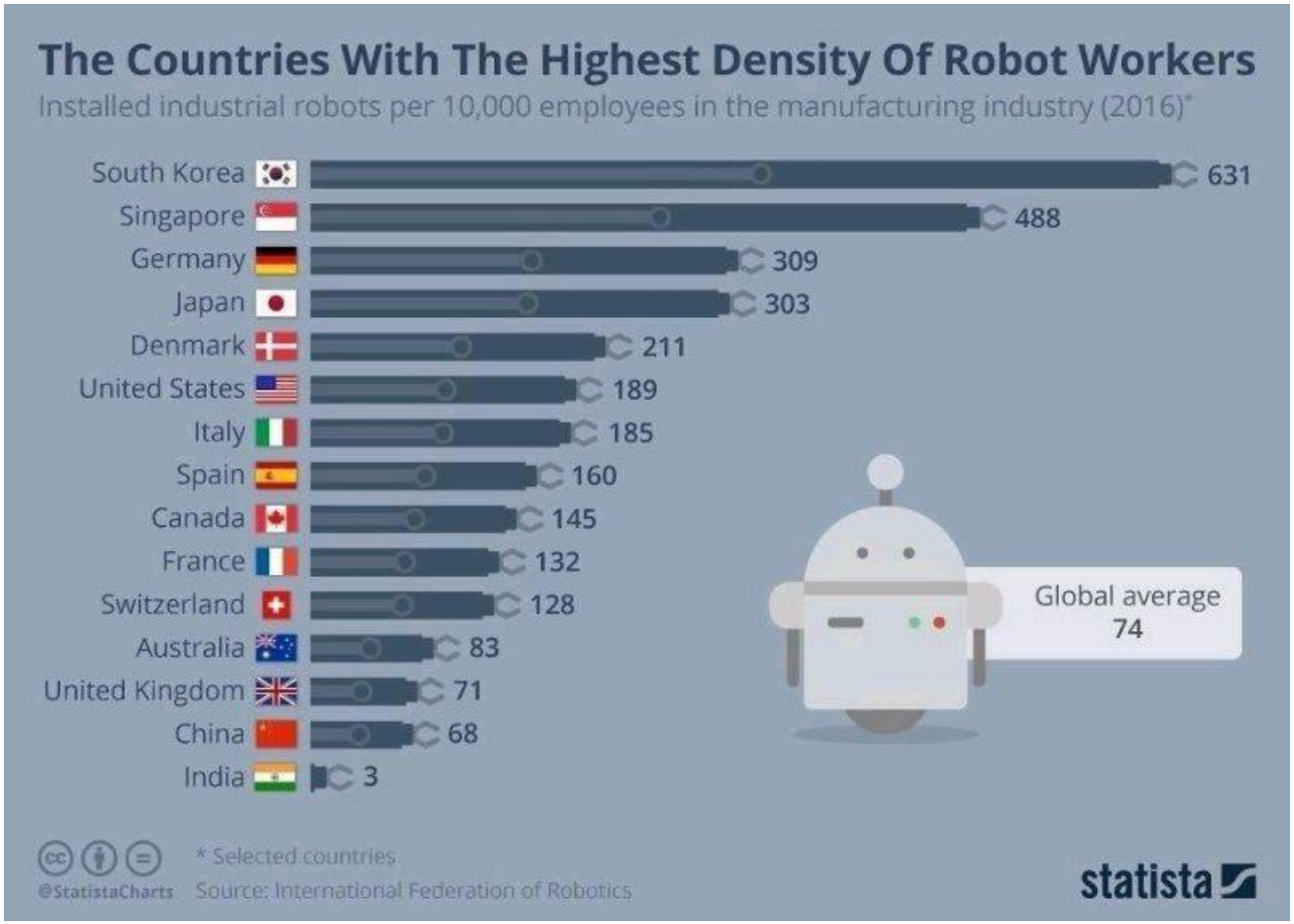
Top 5 Global Risks in Terms of Likelihood

	2014	2015	2016	2017	2018
1st	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events
2nd	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters
3rd	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
4th	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
5th	Cyber attacks	High structural unemployment or underemployment	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

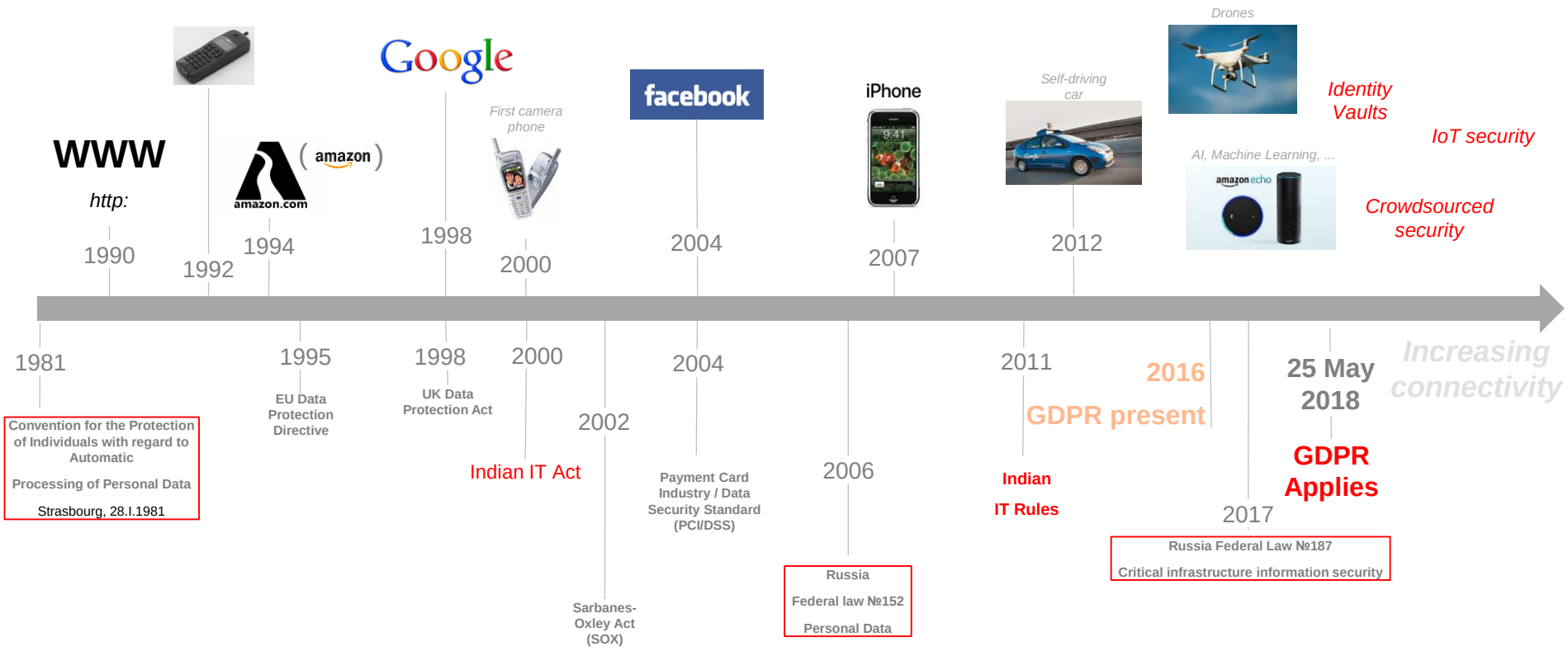
Economic Environmental Geopolitical Societal Technological

WORLD ECONOMIC FORUM

Автоматизация и Роботизация



Развитие технологий и регулирование защиты данных



Безопасность персональных данных в странах БРИКс

Draft of Personal Data Protection Law - PDPL (2015)

Федеральный закон №152 (2006),

Приказ ФСТЭК №21 (2013)

IT Act (2000, 2008), Information technologies Act. for Data Protection,

IT rules (2011)

Personal information security specification (PISS) (2017)

National General Administration of Quality Supervision, Inspection and Quarantine of People's Republic of China
Standardization Administration of the People's Republic of China

Государственная программа «Цифровой Казахстан»

Утверждена Постановлением Правительства РК № 827 от 12.12.2017

Сроки реализации 2018–2022 годы

Задачи программы:

10. Обеспечение информационной безопасности в сфере ИКТ.

……. Президент страны обозначил актуальность борьбы с киберпреступностью, религиозным экстремизмом и терроризмом. В Послании Главы государства сделано поручение Правительству и Комитету национальной безопасности разработать концепцию «Киберщит Казахстана», целью которой является обеспечение информационной безопасности общества и государства в сфере информатизации и связи, а также защиты неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационной инфраструктуры…..

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РЕСПУБЛИКИ КАЗАХСТАН
#407 от 30 июня 2017

Концепции кибербезопасности («Киберщит Казахстана»)

GDPR (General Data Protection Regulation)

GDPR распространяется на организации, находящиеся на территории ЕС и его за пределами, чья деятельность по обработке персональных данных связана с предложением товаров и услуг (даже на безвозмездной основе) субъектам данных в ЕС или с мониторингом их поведения на территории ЕС

Закон вступает в силу **25 мая 2018 года**

В случае утечки ПД, Контролер обязан уведомить об этом соответствующий компетентный орган:

- в течение 72 часов
- незамедлительно, если утечка данных ведет к высокой степени риска для прав и свобод физических лиц

Max

Min

Максимальный штраф: **до 4% годового мирового оборота организации или € 20 миллионов***
(в частности, за нарушение требований к международной передаче данных или основных принципов обработки, таких, как условия для получения согласия)

Другие нарушения: **штраф до 2% годового мирового оборота или € 10 миллионов*** .
Документ включает список обстоятельств, принимаемых во внимание при определении размера штрафа (таких как характер, тяжесть, продолжительность нарушения, наличие умысла и т.п.)

* Из расчета большей величины

Полная версия Закона доступна по ссылке https://gdpr-info.eu/

SAP – это …

Глобальная ИТ компания

ONE Global Network

> **70** countries,

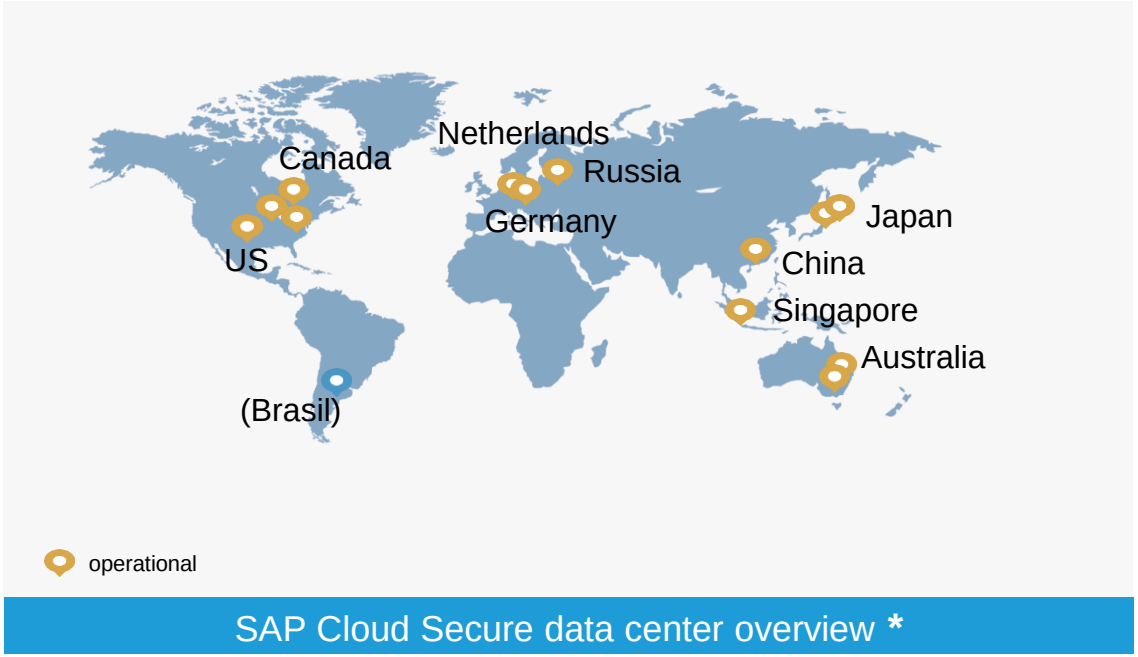
> **220** subsidiaries

…connecting

- **> 75.000** end-users
- **> 100.000** PCs/laptops
- **> 8.500** SAP systems
- > **30.000** servers
- a highly centralized segment of core business systems (incl. ERP, HR, CRM, BW)

…. Cloud Company.

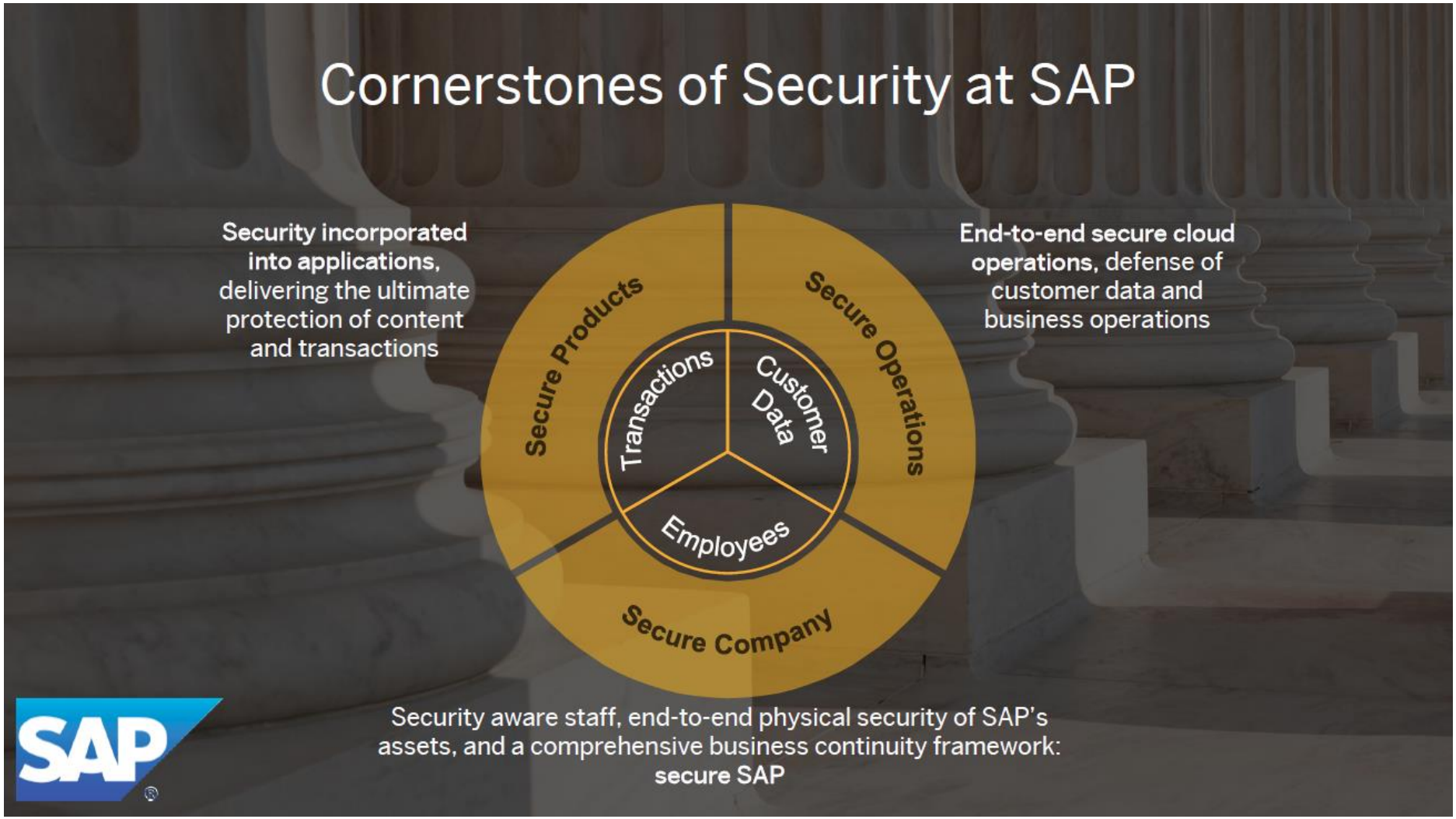
- Data Center on level III or IV
- SAP Data Centers around the world
  14 countries, 30 locations, 40 DCs
- Benefit from local regulations
  (e.g. strong German & EU regulations)
- Low latency speeds-up access
- Customer can choose
  - Region of data storage
  - EU-only operations available
  - preferred datacenter partner



SAP Cloud Secure data center overview *

*) Not all Cloud Solutions are available in all Data Center; for the availability of Cloud Solutions please compare the official availability matrix

Подход к вопросам безопасности SAP



SAP Global Security – Secure operations

Global IT Security, Compliance Process & Privacy Approach

2005/2006	2007/2008	2009/2010	2011	2012	2013	2014	2015	2016
• Set-up global unified Security & Quality Mgmt. • Develop and Implement an Integrated Information Security Mgmt. System • Certificates – ISO9001 (Corp.& Americas) – ISO27001 (Corp.)	• Integrated Risk-Control-Mapping • New SoA on risk level • ISO27001 Certificate (Americas) • ImInternal Control System improved • Process Mgmt. added • Improved Process Map (AS)	• Initiate Process Efficiency Prg. • Establish IT Risk & Security Gov. across SAP • Restructure/Build Performance Measurement • Expand IISMS • State of the art BCM • Restructure Team • Re-focus IT Sec. Strategy	• Establish IT Sec. Monitoring Center • Establish Digital Rights Mgmt. Service • Establish federated Risk Mgmt. • Application Security Management	• Increase Awareness • ISO22301 Certificate (Corporate) • Launch IT Sec. Strategy 2015 • Establish Cross LoB IT Risk Mgmt. • IT Security Award 2012 at it-sa	• Sec. relevant processes across SAP • Network Admission Control • Strengthen Vulnerability & Threat Mgmt. • Ovum BYOX Strategy Award • HEC Security	• Leverage Security cube approach in all relev. areas • Establish Cloud Security Governance • CSO40 Award for excellent custom code management • BMC Innovation Award 2014 'Compliance'	• Major clouds BS10012 Data Protection Mgmt. Systems certified • HEC Customer Compliance Dashboard Live • Harmonization of Security Monitoring & Sec. Incident Mgmt. • IT Security Award 2015 at it-sa • CSO50 2016 award Cloud Compliance	• Strong Co-innovation • Extend and deepen Vulnerability Mgmt. • Strengthen preventive measures • Expand coverage of central security measures • New security strategy 2020

Achievements

- Global IT AS Process Landscape
- IT Security Framework cross SAP
- IT Security Strategy 2012 and 2013-2015, 2016-2020
- ISO 9001 certification (Global IT Corporate & Americas)
- ISO 27001 certification (Global IT Corporate & Americas)
- ISO 22301 (Global IT Corporate) – first company in Germany
- Effective IT Security Governance Structure & Process
- Global Security Monitoring Center
- IT Security Award 2012 for Integrated Management System
- Ovum BYOX Strategy Award 2013
- CSO40 2014 award for effective internal code management
- CSO50 2016 award for efficient automated secure configuration monitoring

Requirements

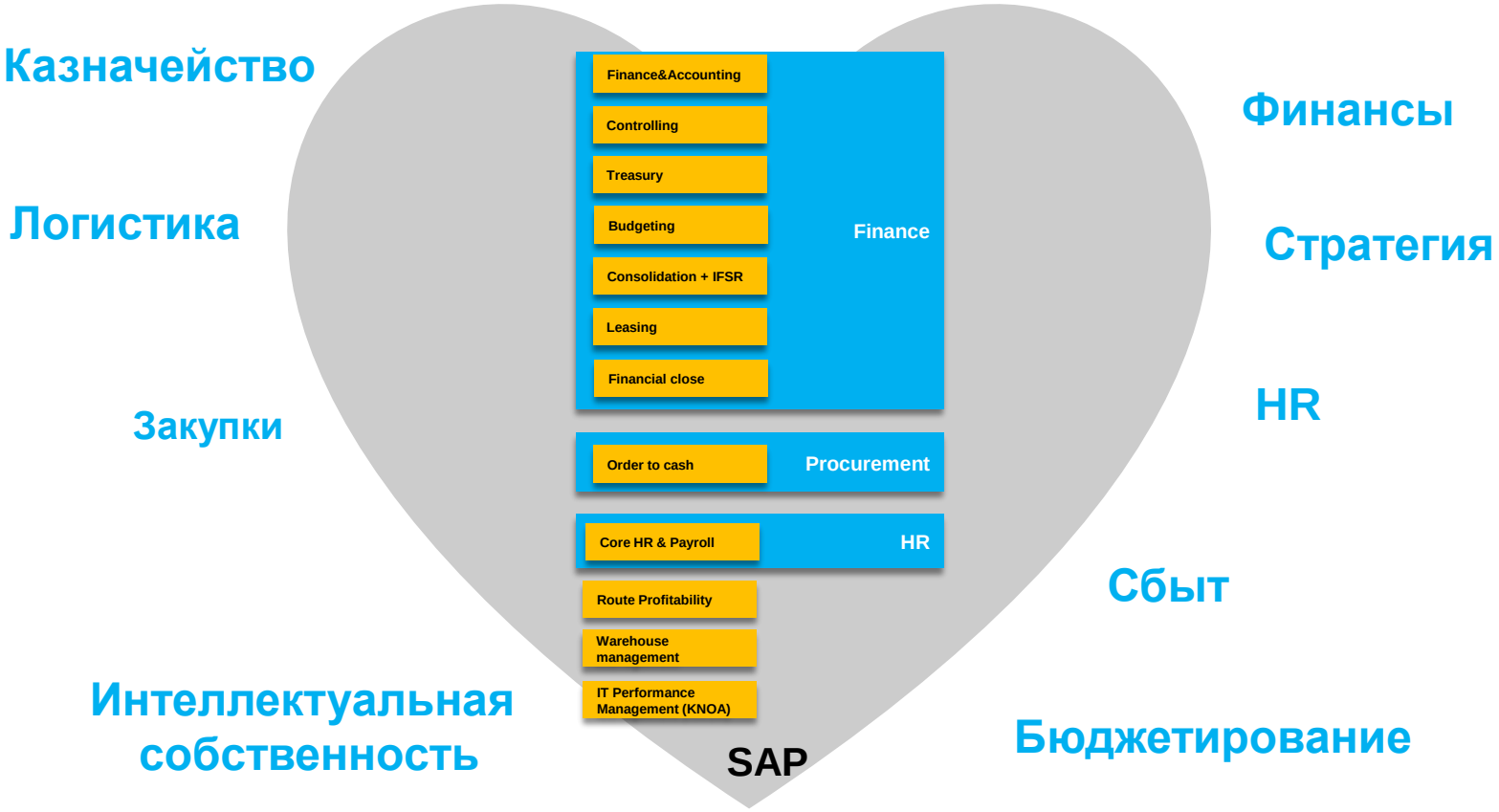
- Achieve KonTraG / SOX compliance of Global IT
- Achieve adequate Security level for main infrastructure, systems & applications
- Establish unique IT Security level across SAP
- Establish and maintain Secure Cloud operation

IT Governance Tools

- Security: BS7799 / ISO27001, SOC 1-3 Quality: ISO9001
- IT SCM: BS 25999 / ISO22301
- Privacy/Data Protection: EU Directive, ISO27018, BS10012
- Service Management: ITIL / ISO20000
- Overall Framework: COBIT, ISACA, ISF Good Practice

SAP – это …

Сервисы и данные наших клиентов



Что хранится в SAP-системах?

Финансы

Финансовая отчётность компании \ группы компаний

Бюджетные документы

Финансовые операции с клиентами

Финансовые операции с поставщиками

HR

Информация о позиции

Информация о заработной плате

Информация об опыте

Рекрутинг

и прочие персональные данные

Интеллектуальная собственность

Планы развития продуктов

Маркетинговые планы

Проекты прототипов и концептов

Стратегия

Утвержденная стратегия компании

Стратегические KPI

Стратегия продаж

Стратегия выхода на новые рынки

Стратегия по развитию

CRM/SRM

Данные клиентов

Данные поставщиков

Состояние сделок

Потенциал будущих сделок с клиентами и поставщиками

Логистика

Данные по транспорту и товарам

Расположение товара на складах

Маршруты передвижения товара

Документы

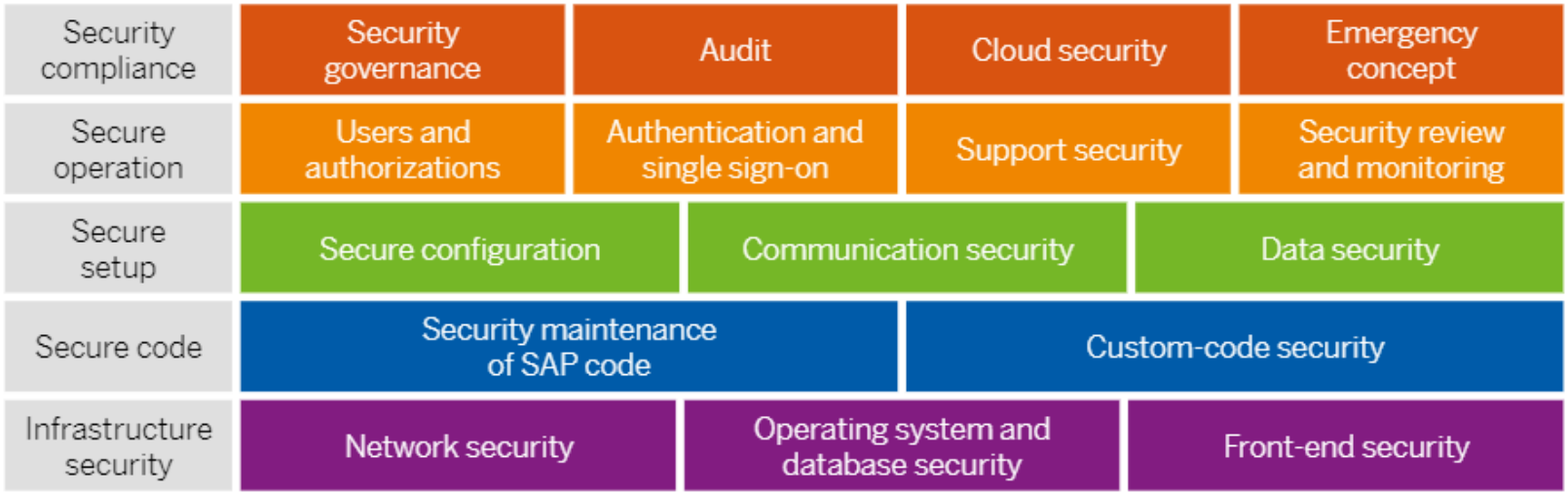
Договора

Описание товара

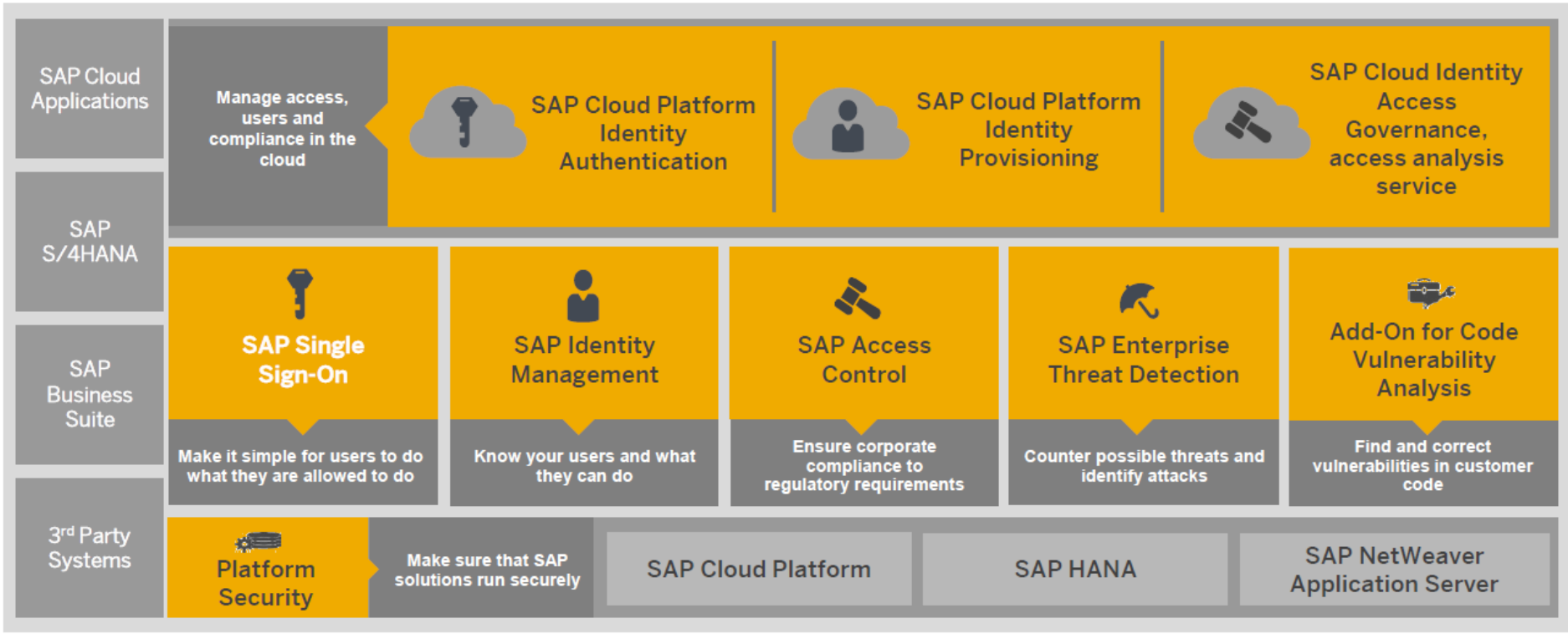
Вложенные документы

Многоуровневая безопасность бизнес-систем

Карта операционной безопасности

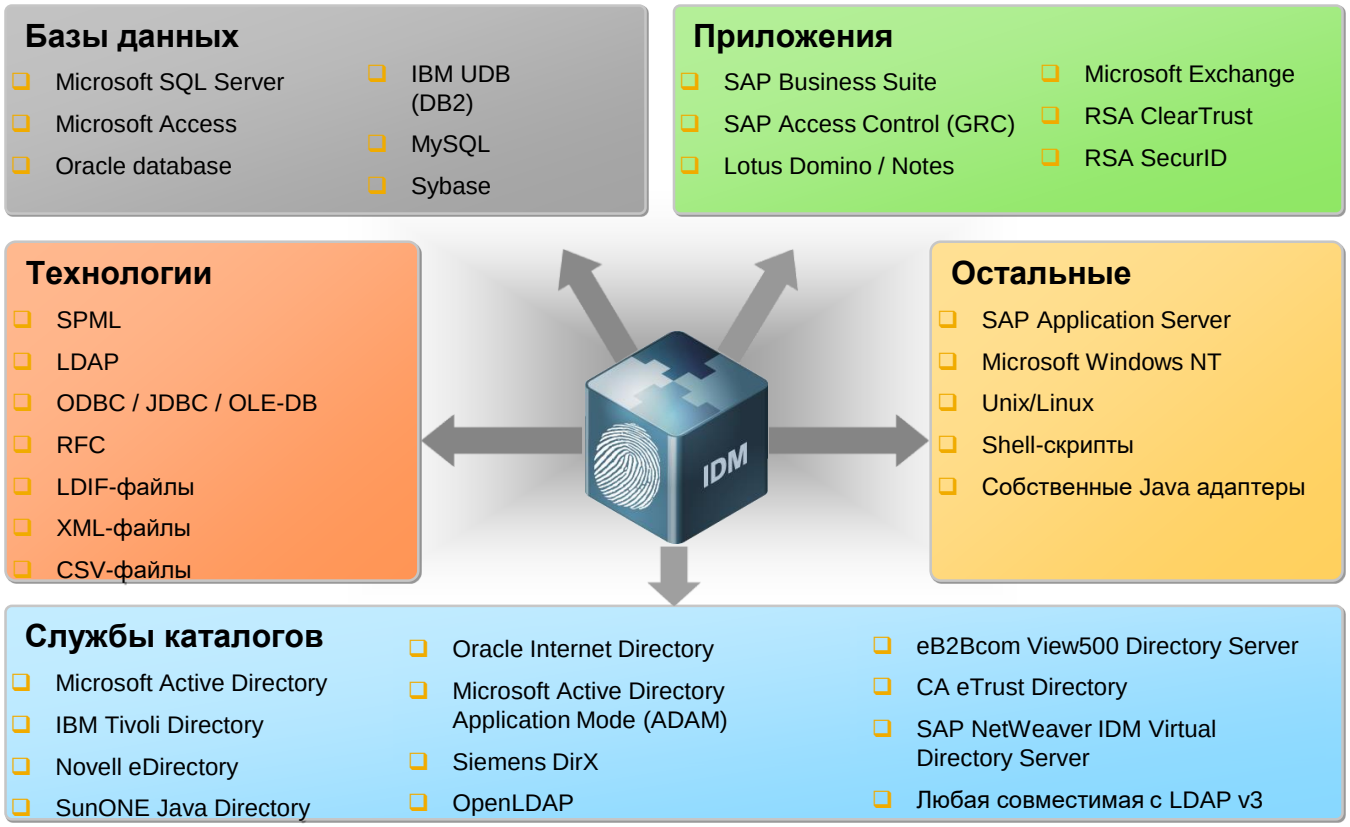


Портфолио продуктов SAP security



Управление доступом в бизнес-системы

Управление доступом в системах SAP и non-SAP



Coca-Cola Hellenic Bottling Company: Exceeding Expectations in Identity Management with Help from SAP

Company
Coca-Cola Hellenic Bottling Company

Headquarters
Zug, Switzerland

Industry
Consumer products – beverages

Products and Services
Soft drinks, fruit juice, and mineral water

Employees
33,000 (2015)

Revenue
US$7.0 billion (2015)

Web Site
www.coca-colahellenic.com

Partner
IBsolution Bulgaria EOOD
www.ibsolution.bg

Objectives

- Align user access with Coca-Cola Hellenic Bottling Company's organizational structures
- Facilitate compliance tracking and reporting
- Track user access to SAP® and non-SAP applications

Why SAP

- Recommendation of partner IBsolution Bulgaria EOOD
- Ability to easily integrate key SAP software

Resolution

- Implemented the SAP Identity Management component plus various rapid-deployment solutions
- Integrated SAP Identity Management with SAP Business Process Management software, the SAP ERP Human Capital Management solution, and Microsoft Active Directory

Benefits

- Handling of access requests largely automated
- Security enhanced across the entire company
- Better prepared for audits
- More cost-effective use of business software licenses

52%
Of access-related requests handled automatically

33,000
Users in 28 countries supported by SAP Identity Management

1
System to manage and monitor user access to SAP and non-SAP applications

44%
Automation target for identity management

"Without robust and largely automated identity management, we would have needed another 12 IT people to handle the growth in headcount."

Stoian Valchev, Global Service Desk Manager, Coca-Cola Hellenic Bottling Company

LEVI STRAUSS & CO

Индустрия:
Производитель одежды

Решения:
Access Control

Сценарий:

- Медленный процесс предоставления полномочий пользователям в SAP системы

Решение

- Внедрение процесса идентификации и устранения рисков разделения полномочий SoD
- Сокращение времени предоставления полномочий с 14 до 1.42 дня
- Основным владельцем системы SAP Access Control 10.0 является бизнес

Полученные преимущества

- Сокращение времени согласования и предоставления полномочий на 89.9% (65% запросов исполняются в день создания)
- Сокращение количества пользователей с рисками доступа на 99.4%

Fiat India: Strengthening Control and Governance and Minimizing Access Risk with SAP® Access Control

Company
Fiat India Automobiles Private Limited (FIAPL)

Headquarters
Pune, Maharashtra, India

Industry
Automotive

Products and Services
Fiat and Tata passenger cars and passenger car engines

Employees
4,000

Revenue
4,000 crore (US$628 million)

Web Site
www.fiat-india.com

Partner
Robert Bosch Engineering and Business Solutions Private Ltd. (RBEI)
www.bosch-india-software.co

Objectives
- Become better informed about best practices for remediation and mitigation of access risk
- Adapt segregation-of-duties (SoD) rules to meet company's needs
- Proactively identify risks prior to user provisioning

Why SAP
- Central repository for mitigation controls
- Flexible and scalable role management framework
- Comprehensive documentation of role management activities for audit purposes

Resolution
- Expedited adoption of the SAP® Access Control application thanks to RBEI's rapid implementation methodology and value-adding best practices for security
- Tailored the SoD rule set to the company's business scenarios and rationalized naming conventions
- Streamlined the role management process with risk-free roles and harmonized user access administration

Future plans
- Grow with and adapt to changes, thanks to future-proof, scalable technology
- Encourage and empower employees with enhanced self-services
- Improve monitoring and analysis of risks and controls with one-click access to dashboards and reports

90%
Fewer SoD violations

50%
Less cycle time for access management

30%
Reduction in composite and single roles

Lower
Cost of compliance

Противодействие финансовому мошенничеству через управление рисками доступа

Типовой жизненный цикл сотрудника организации

Дата выхода на работу

Иван Горемыкин устроился на работу

Доступно:

- Временные учетные данные

Три недели спустя

Иван Горемыкин может работать бухгалтером

Доступно:

- E-Mail
- Портал
- Интернет
- Бухгалтерия

Один год спустя

Иван Горемыкин перешел в продажи

Доступно:

- E-Mail
- Портал
- Интернет
- Бухгалтерия
- CRM (Сибирь)
- Маркетинг (Сибирь)

Семь лет спустя

Иван Горемыкин стал виде-президентом по продажам

Доступно:

- E-Mail
- Портал
- Интернет
- Бухгалтерия
- CRM (Глобально)
- Маркетинг (Глобально)

Восемь лет спустя

Иван Горемыкин уволился

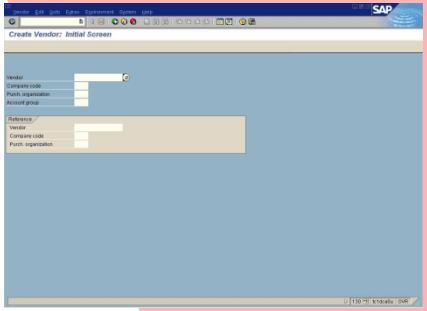
Все известные учетные записи удалены

Иван Горемыкин продолжает иметь доступ

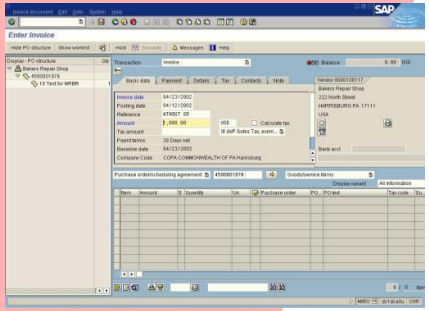
Доступно:

- Бухгалтерия
- Маркетинг (Глобально)

Пример риска доступа (SoD конфликт)

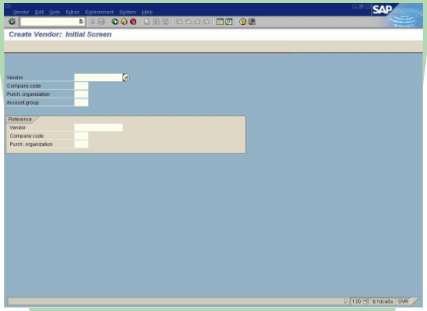


Создание нового поставщика

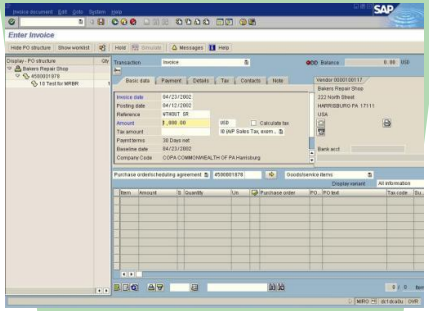


Осуществление Платежа

VS.



Создание нового поставщика



Осуществление Платежа

Пример автоматизированного процесса

Требование:
Обеспечить автоматизированное управление ролями, ориентированное на должности и обеспечивающее проверку рисков.

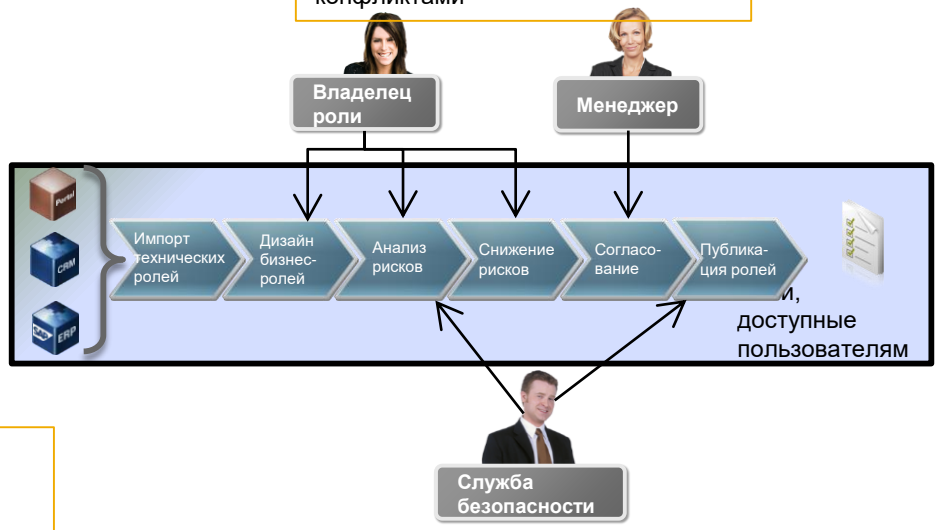
- Снижение TCO за счет упрощения порядка присвоения полномочий пользователям по событиям из кадровой системы
- Снижение рисков доступа посредством предварительной проверки и корректировки
- Автоматизация ручных процессов за счет интеграции с целевыми системами

Управление рисками злоупотреблений в результате конфликта полномочий

Владельцы бизнес-процессов
Снижение рисков финансового мошенничества за счет разделения конфликтов полномочий (SoD)

Служба внутреннего контроля
Создание и управление контрольными процедурами при согласовании ролей с SoD-конфликтами

Информационная безопасность
Разделение и управление доступом к информационным ресурсам организации



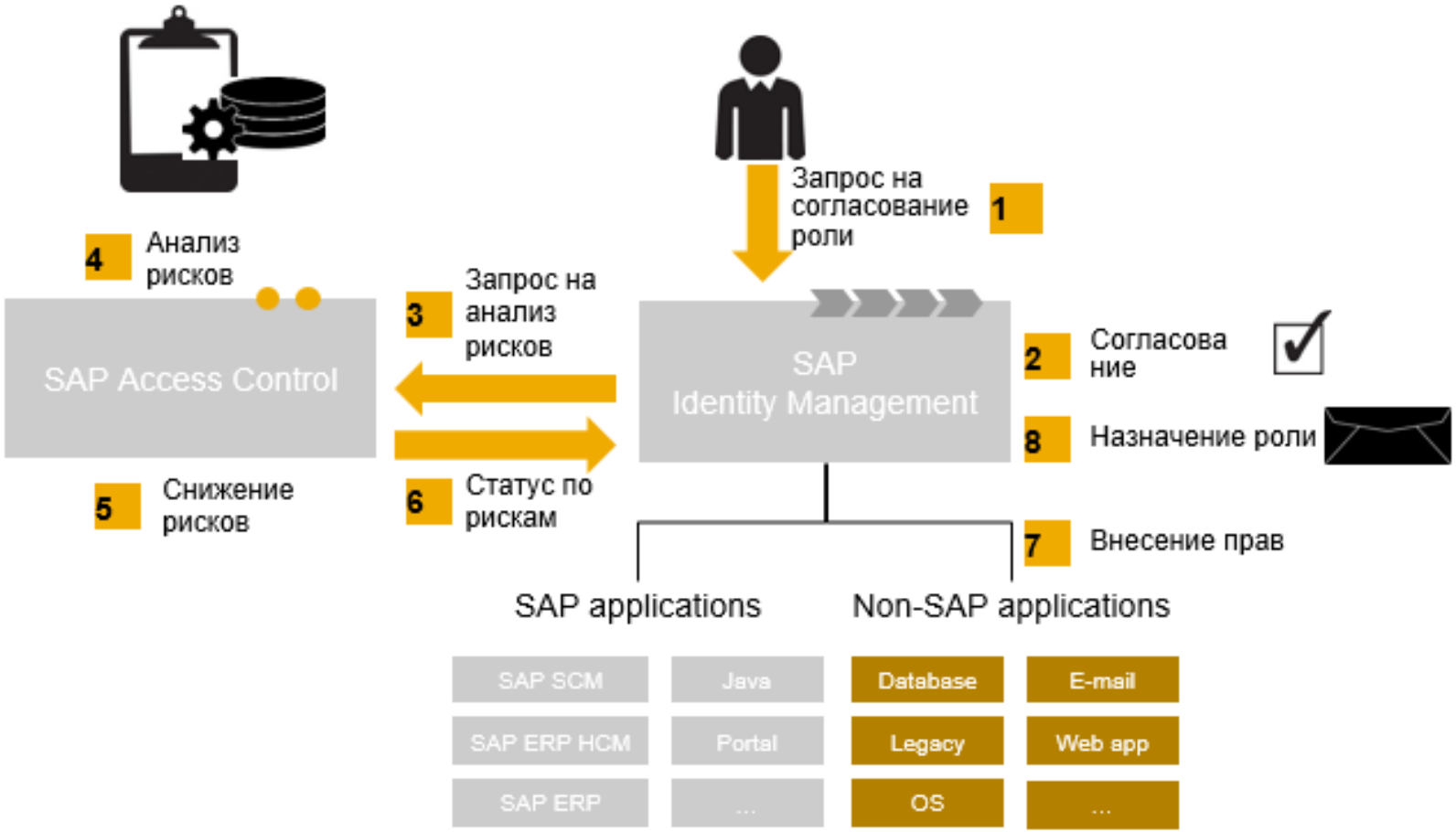
Департамент безопасности
Снижение возможности проведения мошеннических операций сотрудниками

Служба внутреннего аудита
Быстрый аудит конфликтов полномочий и запрошенных расширенных прав в бизнес-системах

Департамент рисков
Снижение рисков финансового мошенничества за счет разделения управления и конфликтов полномочий (SoD)

Информационные технологии
Быстрый анализ новых ролей, снижение времени ожидания выдачи полномочий по запросу

SAP Access control + SAP Identity management



Северсталь

Индустрия: Металлургия

Страна: Россия

Решения: Access Control

Предпосылки внедрения

- Сжатые сроки внедрения ИС. Отсутствие внимания к ролям и полномочиям пользователей на стадии внедрения ИС;
- Массовое присвоение полномочий пользователям на этапе старта ИС;
- Неконтролируемое изменение ролей;
- Неконтролируемое расширение полномочий пользователя в ИС. Предоставление пользователю полномочий в обход установленных процедур и контролей;
- Неограниченный доступ разработчиков и консультантов в ИС;
- Неэффективные коммуникации в процессе внесения изменении в ИС.

Полученные преимущества:

- Комплексное решение для соблюдения требований разграничения полномочий и подтверждения достоверности финансовой отчетности
- Повышение эффективности управления жизненным циклом полномочий пользователей и ролей:
  - Обеспечение корректной обработки запроса пользователя на расширение полномочий в ИС
  - Обзор нарушений SOD и доступа к критическим транзакциям
  - Организация контроля над полномочиями пользователя (снижение рисков)
  - Моделирование ролей и присвоений пользователям
  - Стандартная отчетность по анализу рисков, пользователей
- Минимизация времени и затрат на аудит

Возможен референс-визит

Chevron

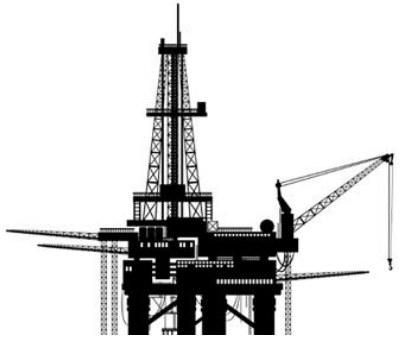
Индустрия: Нефть и Газ

Страна: США

Решения: Access Control, Process Control

Полученные преимущества:

- Минимизация различных рисков, в том числе SOX.
- Более 3000 пользователей выполняют свои ежедневные задания, используя SAP Interactive Forms by Adobe через электронную почту, без необходимости проходить повторную авторизацию в системе.

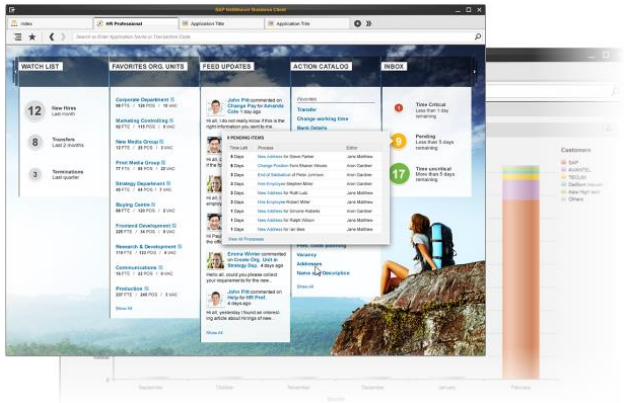


Прозрачный доступ между бизнес-приложениями

Single Sign-On для новых SAP Clients

SAP User Interface Integration

- Комбинация красивого интерфейса и грамотной безопасности
- Поддержка SAP clients out of the box
  - SAP Fiori
  - SAP NetWeaver Business Client
  - SAP Screen Personas



SAP Single Sign-On

Security

- Пароль вводим один раз
- Не нужно запоминать пароли для каждой системы
- Все пароли защищены и управляются централизованно

Reduce Costs

- Эффективное управление временем пользователя, самообслуживание
- Повышение продуктивности за счет использования прозрачного входа,автоматизация сброса пароля, высвобождение рук в helpdesk,…

Simplicity

- Быстрое внедрение новых решений для пользователей
- Нет проблем с частой сменой паролей в разных системах
- Нет проблем выполнением парольной политики и политики безопасности компании

SAP Single Sign-On

SAP Single Sign-On обеспечивает быстрый и защищенный доступ к IT приложениям для бизнес-пользователей, и обеспечивая дополнительную безопасность в бизнес-приложениях.

Simple and secure access

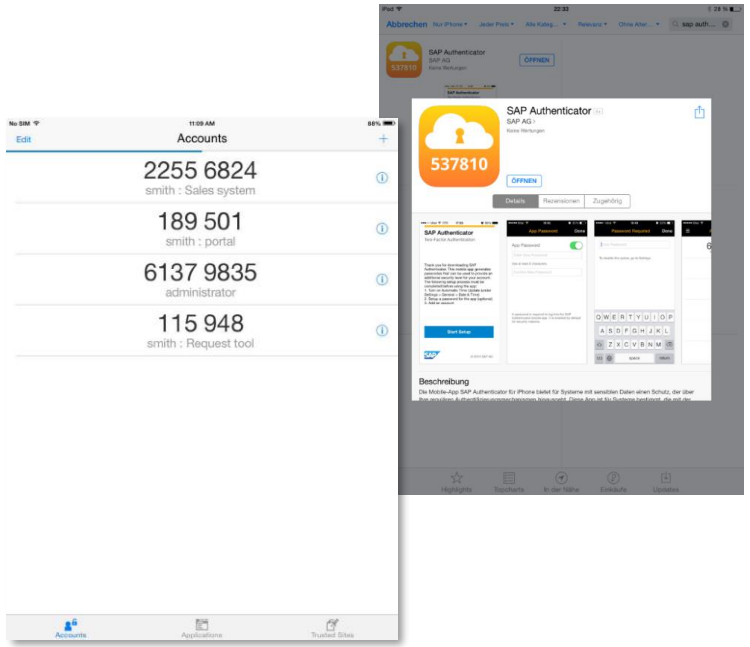
- Single sign-on для SAP клиентов и web приложений
- Single sign-on для мобильных устройств
- Поддержка cloud и on-premise ландаштов приложений

Защищенное подключение

- Криптографическая защита подключения SAP GUI
- Цифровая подпись данных
- Возможность встраивания ГОСТ 28147-89 с сертификация ФСБ

Дополнительные возможности

- Двухфакторная аутентификация
- RFID-аутентификация
- Использование СМС, меток, дополнительной проверки



Газпром нефть

Развитие системы аутентификации SAP с помощью SAP SSO

Компания

ПАО «Газпром нефть»

Штаб-квартира

Санкт-Петербург, Россия

Индустрия

Нефтегазовый сектор

Продукция

Нефть и нефтепродукты

Количество сотрудников

55,900

Веб-сайт

www.gazprom-neft.com

Цели проекта

- Снижение рисков кражи или подбора пароля пользователей
- Уменьшение задержек выполнения бизнес-процессов из-за ожидания разблокировки или восстановления пароля
- Повышение удобства использования систем SAP для пользователей
- Оптимизация нагрузки на службу технической поддержки

Почему SAP

- Простота использования и настройки
- Легкость интеграции в корпоративный ландшафт
- Прозрачность применения для рядового пользователя

Результат проекта

- Для всех SAP системах Компании был настроен процесс аутентификации с помощью SAP SSO
- Пользователи используют сертификат для входа в SAP
- Пользователи строго соблюдают парольную политику компании, контролируемую через SAP SSO

Выгоды

- Оптимизация затрат на службу технической поддержки
- Снижение издержек за счет уменьшения непроизводительных потерь рабочего времени на ожидание восстановления пароля
- Снижение рисков информационной безопасности за счет применения стойких паролей, в соответствии с парольной политикой компании
- Рост эффективности сотрудников, за счет применения сквозного входа в бизнес-приложения.

Безопаснее

снижение риска кражи или подбора пароля

на **95%**

уменьшились задержки на выполнение бизнес процессов

40 систем

включено в контур SAP SSO

Возможен референс-визит

38444 (15/07) This content is approved by the customer and may not be altered under any circumstances.

Протоколирование данных и их анализ

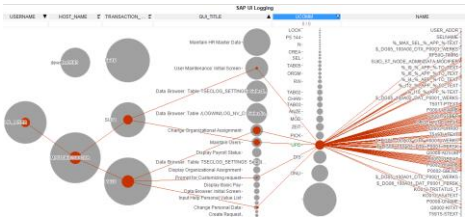
SAP UI Logging

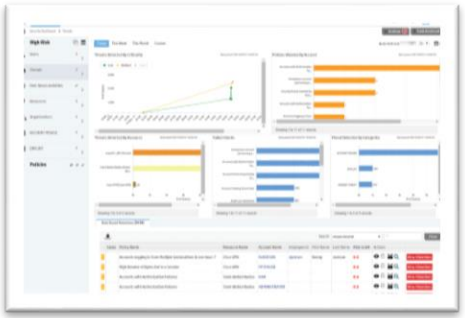
Расследование инцидентов ИБ

- Кто, откуда, куда имел доступ
- Кто работает больше всех с информацией определенного типа
- Кто работает меньше всех с информацией опредлеенного типа
- Кто изменил значение параметра
- Кто изменил логику бизнес-процесса
- Кто забыл вернуть обратно выданные ранее временные права доступа в систему
- Кто внес несогласованные изменения в «продуктивную» систему

Сценарии использования

- Отслеживание просмотра персональных данных, сведений о заработной плате
- Контроль выплаты премий
- Контроль расчета отпускных
- Контроль доступа к списку на увольнение
- Контроль просмотра данных VIP клиентов
- Отслеживание просмотра данных о поставщиках, об условиях контрактов, предварительных отчетах акционерам
- Контроль портала закупок





Протоколировать или маскировать?

RCS UI Logging / UI Field Security

UI Logging

Пример использования: Конфиденциальная информация остается доступной для некоторых сотрудников

Мягкий подход к защите данных

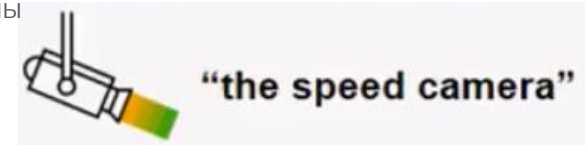
- Сдерживание нелояльных нарушителей

Ретроспективный подход (гигиенический фактор)

- Позволят выявить и наказать нарушителей
- Позволяет назвать имена подозреваемых

Построение “human firewall”

- Информирование, что события логируются и есть возможность контроля
- Повышение осведомленности о защите данных
- Помогает создать атмосферу доверия между сотрудниками и клиентами, что данные надежно защищены



UI Masking

Пример использования: конфиденциальные данные должны быть скрыты от некоторых пользователей/ролей

Строгий подход к защите данных

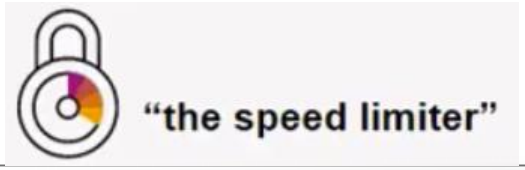
- Техническое блокирование доступа к конфиденциальной информации

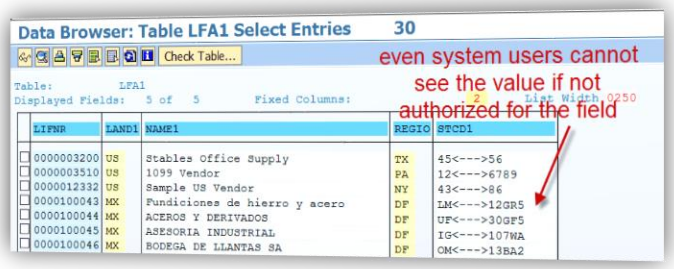
Преактивный подход

- Невозможность воспользоваться информацией из интерфейсов
- Предотвращение утечек данных

Построение “human firewall”

- Повышение значимости вопросов безопасности
- Защита сотрудников от случайных нарушений
- Улучшение возможностей выполнять конфиденциальную работу





MHH: Защита информации о пациентах при помощи SAP UI Logging

Клиент
Medizinische Hochschule Hannover (MHH) (Медицинская школа Ганновера)

Штаб квартира
Ганновер, Германия

Индустрия
Здравоохранение

Продукты и сервисы
Образование, Исследования, Стационарное лечение

Штат
7,731 штатных сотрудников

Web Site
www.mh-hannover.de

Цели

- Логгирование всех попыток доступа к медицинским данным и расследования в случае необходимости
- Обеспечение конфиденциальности данных о пациентах при обработке данных
- Контроль неавторизованного доступа не связанного с выполнение задач
- Повышение качества исполнения внутренних требований защиты данных

Почему (UI) logging

- MHH использует большое количество решенийSAP®
- Программа, которая работает в фоновом режиме
- Предоставляет данные для анализа
- Rollout проект, который был реализован за пару недели без единого простоя системы
- Отсутствие негативного влияния на производительность системы

Положительные эффекты

- Возможность мониторинга доступа на лету
- Возможность проверить конкретные подозрительные ситуации
- Отслеживание несанкционированного доступа и предотвращение его в будущем
- Повышенное внимание к защите данных
- Высокое доверие со стороны пациентов и сотрудников

Планы на будущее

Распространение опыта использования решения на другие медицинские учреждения.

Hannover Medical School

Эффективная
защита данных

Быстрая
Реакция на злоупотребления с информацией

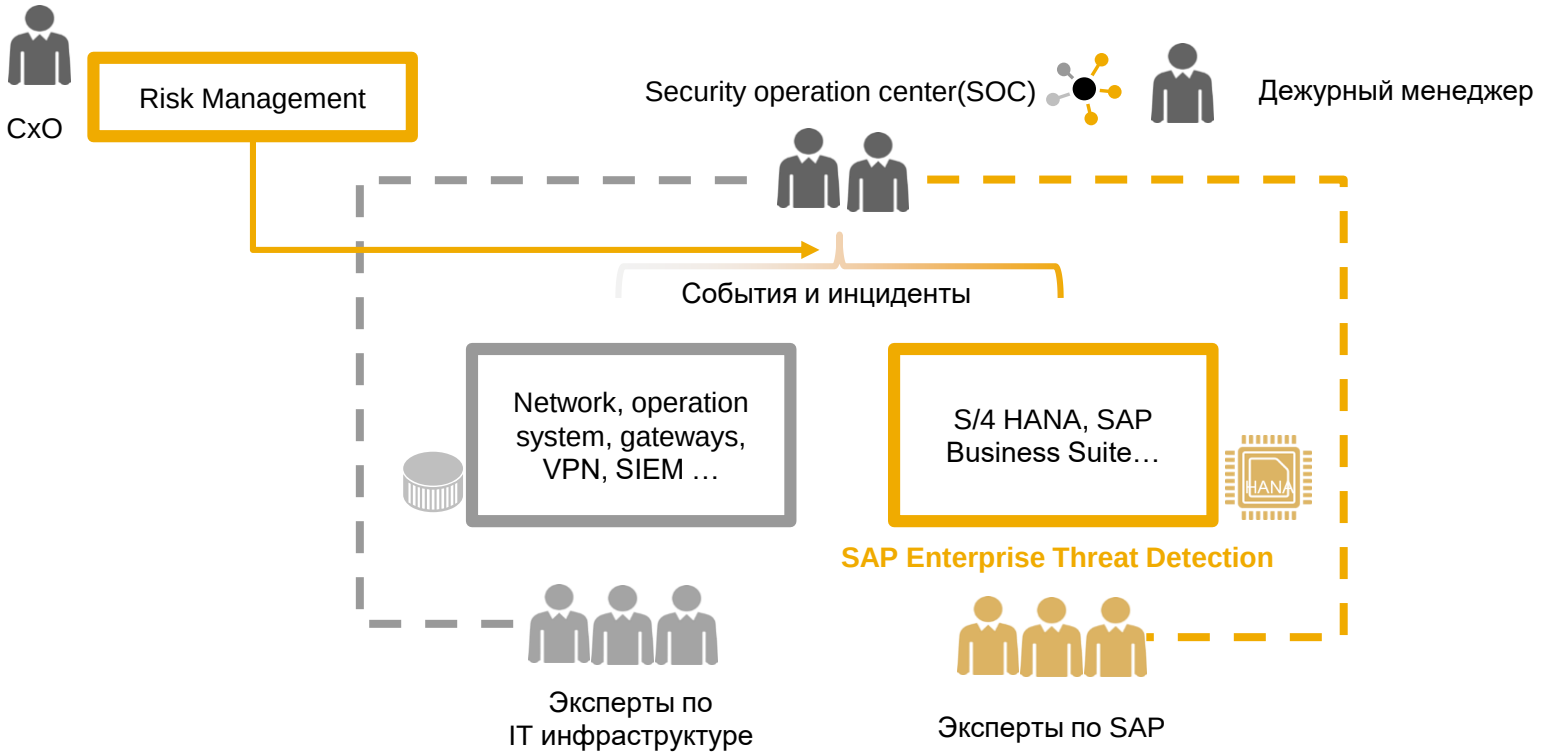
Повышающая
доверие со стороны пациентов и сотрудников

“Если кардиолог, к примеру, получает доступ к данным по онкологии, мы можем понять правомерно это или нет. Сегодня мы можем четко определить это. А также проверять подобные случаи и принимать соответствующие меры в случае необходимости.”

Татьяна Нейтц-Клюге, Руководитель Проекта, Медицинской Школы Ганновера

Построение Security Operation Center (SOC)

Центр управления информационной безопасностью

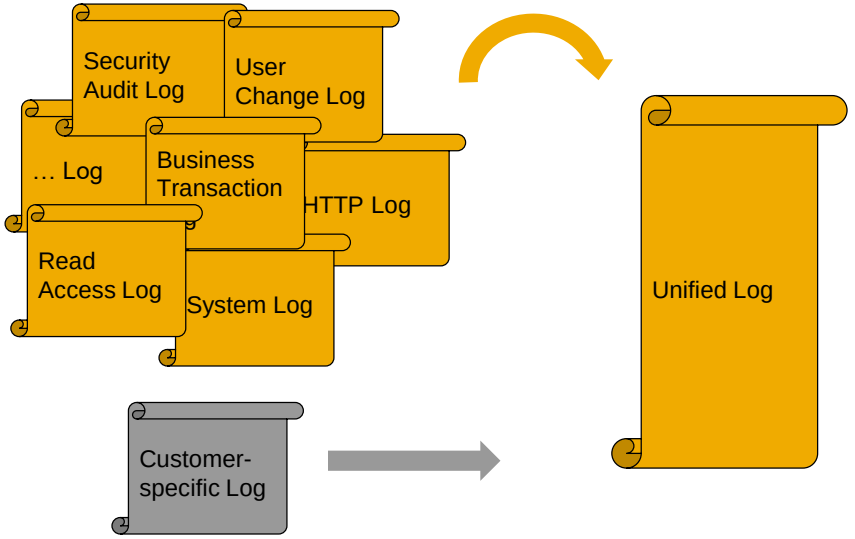


SAP Enterprise Threat Detection

Сбор и нормализация данных

Единый формат данных

- Единое представление временных штампов
- Идентификации пользователей
- Поддержание дополнительной информации о событиях
- Корреляция данных по правилам
- Идентификация инцидента
- Трансляция инцидентов во внешний SOC или SIEM



Управление журналами

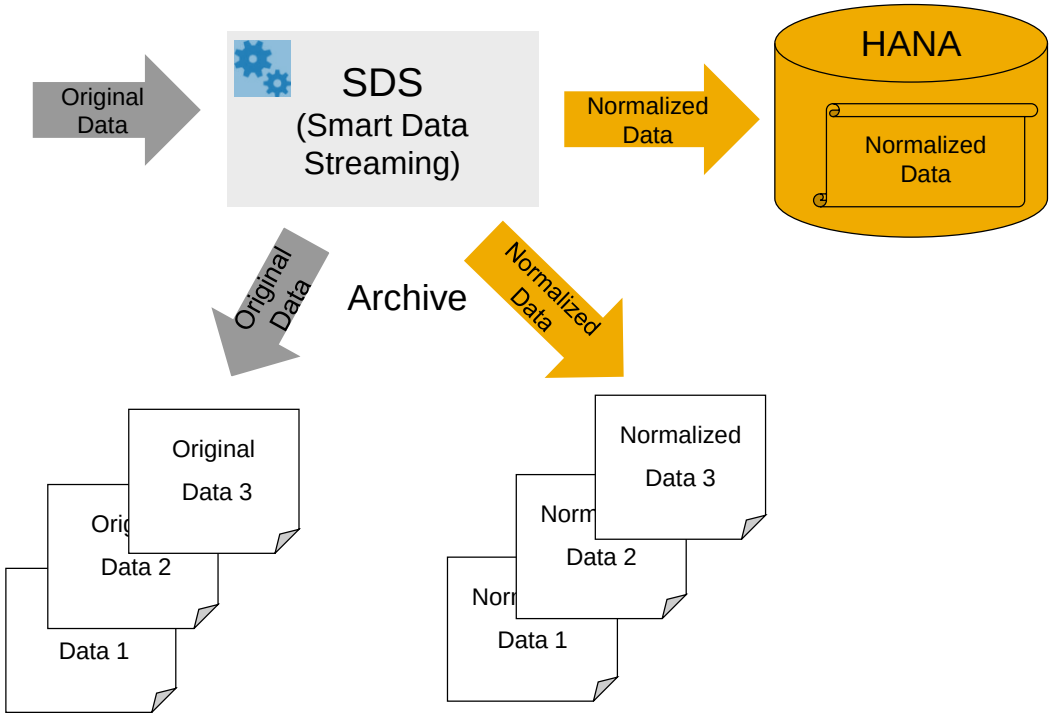
Долгосрочное хранение и архивирование журнала событий

Сохранение оригиналов

- Оригиналы (для последующего аудита и расследования)
- Нормализованный

Чтение нормализованных событий из фалов

- Проведение расследований



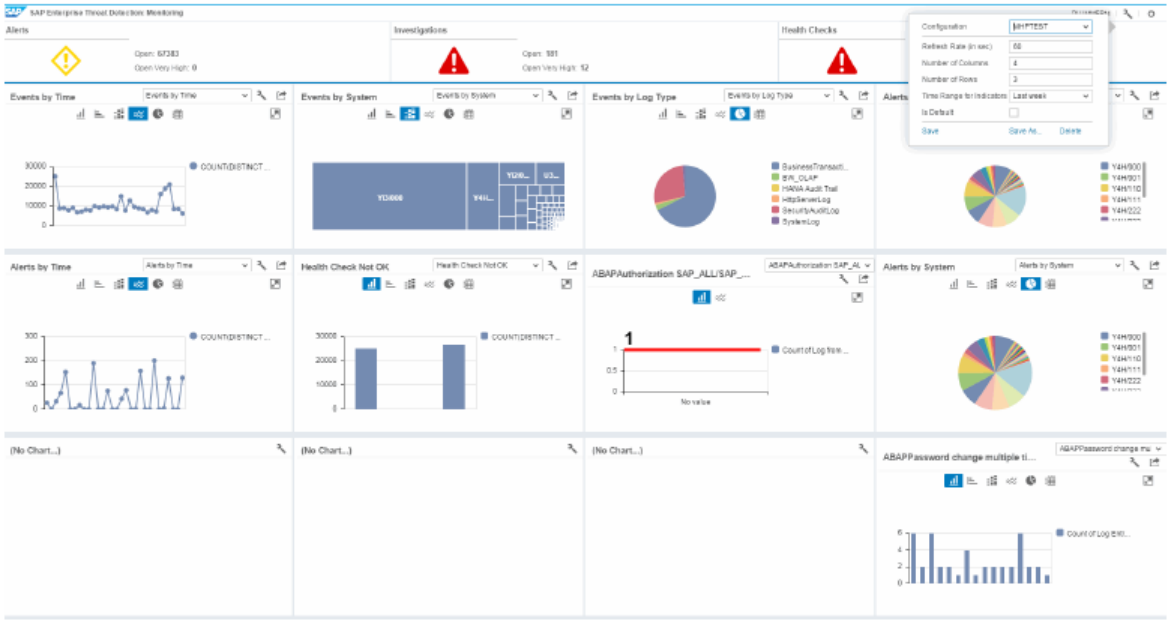
SAP Enterprise Threat Detection

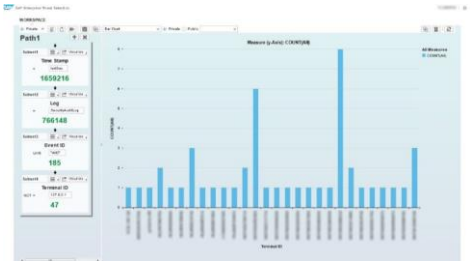
– Сбор данных с SAP-систем

– Анализ и проведение расследований

– Может использоваться как дополнительный инструмент к SOC

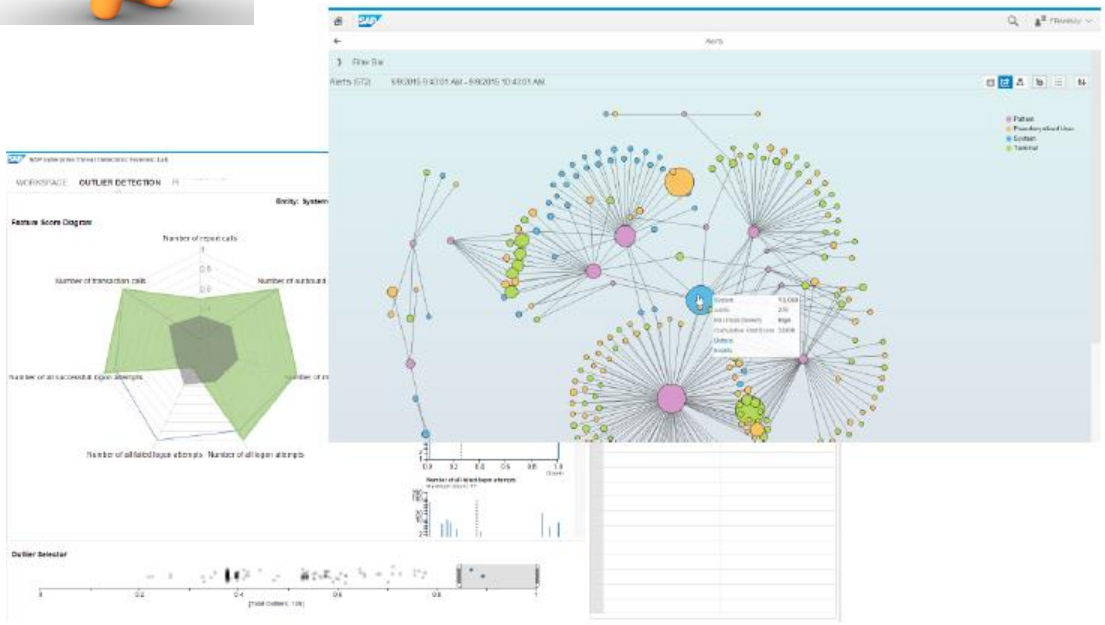
– Хранит дополнительную информацию об операциях в ERP, необходимую для проведения расследований финансовых преступлений





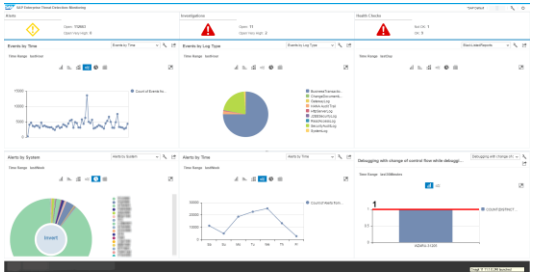
Примеры выявляемых ситуаций

- Массовая выгрузка данных
- Неправомерный запуск транзакций
- Неавторизованный запуск процедур
- Доступ к данным
- Доступ к компонентам
- Передача данных между разными уровнями пользователей.
- Изменение данных
- Протоколирование подключений
- Использование debug-функций
- Пересылка данных
- Неудавшиеся авторизации
- Успешные авторизации
- Ошибки конфигурации систем
- Не установленные ноты безопасности

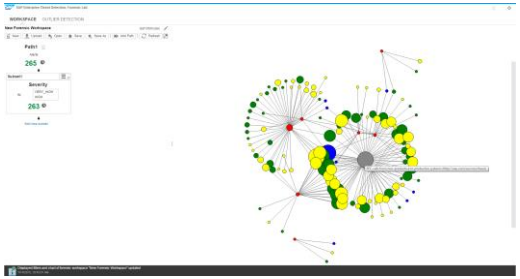


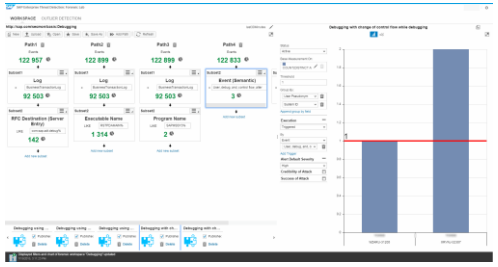
Мониторинг и Forensic Lab

(Лаборатория исследований атак)

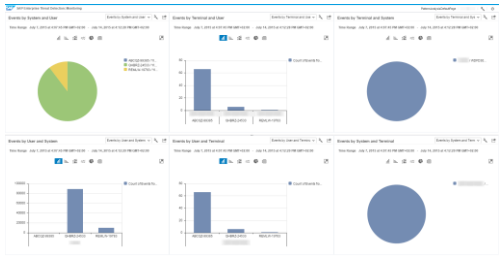


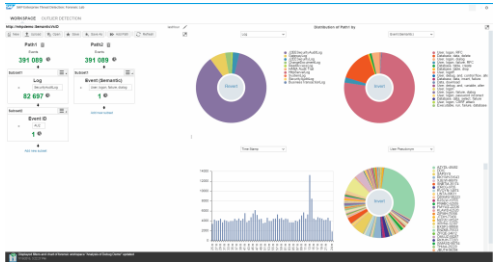
Инциденты





Расследование

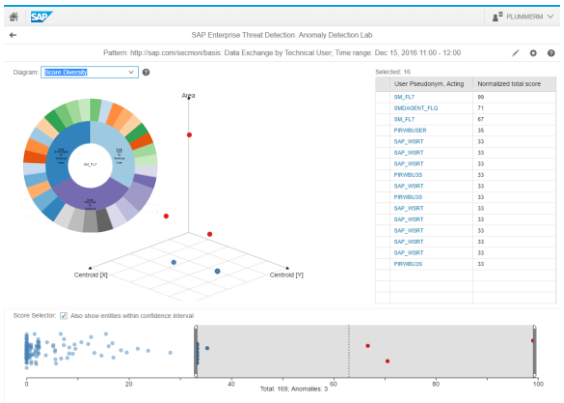




Создание новых и изменение старых плавил автоматического выявления

Интеграция с другими системами SIEM

- **Публикация инцидентов во внешний SIEM**
  - Автоматическая отправка через Email
  - Отправка по протоколу JSON
  - Получение по протоколу JSON



SAP ETD

JSON

SIEM
(прочие системы)

Email

Выявляемые нарушения

SAP Enterprise Threat Detection

- Массовая выгрузка данных
- Неправомерный запуск транзакций
- Неавторизованный запуск процедур
- Доступ к данным
- Доступ к компонентам
- Передача данных между разными уровнями пользователей.
- Изменение данных
- Протоколирование подключений
- Использование debug-функций
- Пересылка данных
- Неудавшиеся авторизации
- Успешные авторизации
- Ошибки конфигурации систем
- Не установленные ноты безопасности

- Access to Generic Path (Distinct) by Dialog User
- Access to Generic Path (Distinct) by Technical User
- Access to Generic Path by Dialog User
- Access to Generic Path by Technical User
- Access to New Application Component by Dialog User
- Access to New Application Component by Technical User
- Access to New Restricted Generic Path by Dialog User
- Access to New Restricted Service Function by Dialog User
- Access to New Restricted Service Transaction by Dialog User
- Access to New Target Generic Path by Technical User
- Access to New Target Service Function by Technical User
- Access to New Target Service Transaction by Technical User
- Access to New Target System by System Id
- Access with New Logon Method by Technical User
- Data Exchanged by Dialog User
- Data Exchanged by Technical User
- Data Received by Dialog User
- Data Received by Technical User
- Data Received from Third Party System by System Id

- Data Sent by Dialog User
- Data Sent by Technical User
- Data Sent to Third Party System by System Id
- Downloaded Resource Volume by System Id
- Downloaded Resources (Distinct) by System Id
- Failed LogOn Events by System Id
- Log Volume by System Group
- Service Function Calls (Distinct) by Dialog User
- Service Function Calls (Distinct) by Technical User
- Service Function Calls by Dialog User
- Service Function Calls by System Id
- Service Function Calls by Technical User
- Service Transaction Calls (Distinct) by Dialog User
- Service Transaction Calls (Distinct) by Technical User
- Service Transaction Calls by Dialog User
- Service Transaction Calls by System Id
- Service Transaction Calls by Technical User
- Successful LogOn Events by System Id
- Transactions by User and System

Безопасность бизнес-приложений SAP

SAP Enterprise Threat Detection

- Сбор событий со всего ландшафта SAP
- Оценка эффективности обнаружения атак
- Получение сигнала о возникновении угрозы
- Формирование автоматической реакции
- Запрос информации на расширенный анализ инцидента
- Расследование инцидентов
- Соответствие требованиям регуляторов

City of Wolfsburg: Monitoring the IT Security Situation with SAP® Enterprise Threat Detection

Organization
City of Wolfsburg

Location
Wolfsburg, Germany

Industry
Public Sector

Products and Services
- SAP Enterprise Threat Detection
- Data Privacy Mgmt. (Partner)
- Windows-Agent (Partner)
- Network Appliance (Partner)
- Honeynet (Partner)

Employees
4,000

Revenue
Budget - € 448 Mio.

Web Site
www.wolfsburg.de

Partner
Schönhofer – Sales & Engineering
www.schoenhofer.de

Objectives
- Real time visualization of the IT security situation
- Creating a visual which compares the threat situation and helps the management in decision making
- Monitoring of external and especially also internal threats
- Identification and reporting of system anomalies
  - Identification of potential attack vectors due to unpatched systems
- Integration of non-SAP systems
  - Windows event log of domain controllers, e-mail gateway, proxy, firewall
- Correlation of comparable and functional dependent events from different source systems (e.g. internal and external firewall)
- Monitoring of system configuration defined in concepts and guidelines
  - Security relevant Windows logging, monitoring guidelines, authorizations
- Monitoring system specific patterns
  - Monitoring of user and system logins, communication between systems, extension of authorizations, creation of new users

Why SAP?
- Monitoring page of SAP Enterprise Threat Detection allows visualization of the IT security situation
- Performant analysis and correlation of log information
- Possibility to enrich the log data (IP/MAC addresses)
- Optional integration of meta information to aid analysis
- Complementary monitoring of SAP and non-SAP world
- Reporting of identified anomalies

Next Steps
- Proceed in conformance with IT regulations (iterative integration of systems that are relevant for protection)
- Integrate SAP Enterprise Threat Detection in existing concepts (emergency procedures, authorization and role concept,…)
- Combine all relevant systems with SAP Enterprise Threat Detection

„Knowing what is going on in our network and systems outside working hours is extremely reassuring.“

Wolfgang Beuermann, Director „Zentrale Systeme, Netze und TK“

> 10
Connected non-SAP systems

52 Mio.
Monitored E-mails per month

200 Mio.
Processed logs per month

The most dangerous attackers according to surveys:

SAP Enterprise Threat Detection

A Big-data Solution to a Serious Security Challenge

Company
SAP SE

Headquarters
Walldorf, Germany

Industry
High Tech

Products and Services
Enterprise software and services

Employees
74,000

Revenue
€16.82 billion

Web Site
www.sap.com

Implementation Partners
-

BUSINESS TRANSFORMATION

The company's top objectives

- Add the layer of application level security monitoring to the existing security measures at SAP
- Bring knowledge about attack patterns into an executable form, so attacks can be detected automatically and accurately
- Enable Security Operations to timely identify and act on attacks and malicious behavior in SAP Systems

The resolution

- Implementation of dedicated SAP Enterprise Threat Detection (ETD) landscape with sufficient sizing to cope with the vast amount of log data available
- Tailoring of attack patterns to the specifics of the business systems being monitored
- Continuous expansion of pattern repository
- Close collaboration with product development teams to implement required features and integrate them into the standard product

The key benefits

- Readily and efficiently identify security lapses in SAP's business systems
- Detection of threats and attacks as they happen
- On the fly security analytics capabilities

"SAP Enterprise Threat Detection enables us to identify real attacks to our business systems as they are happening and analyze the threats quickly enough to neutralize them before serious damage occurs."

Maximilian Adrian, Vice President Business Application Security, SAP SE

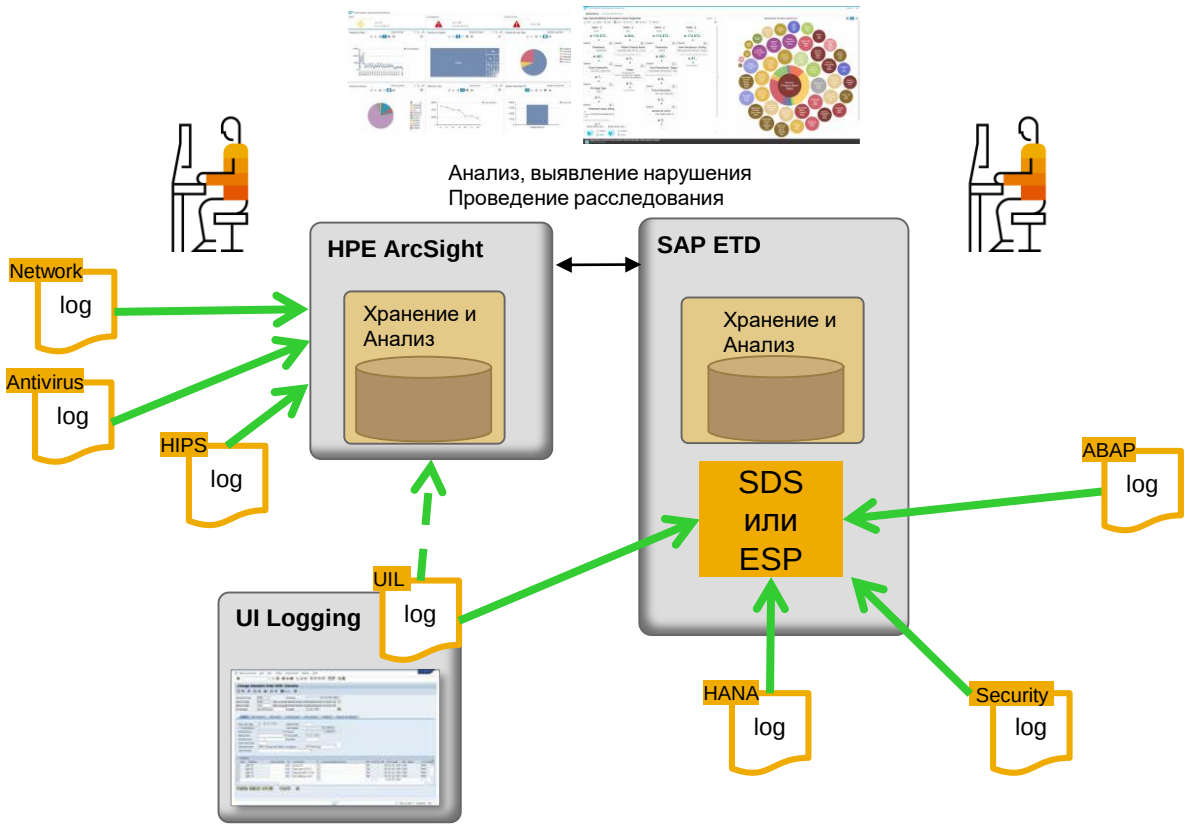
TOP BENEFITS ACHIEVED

>80
Available attack patterns

~250 Mio
Events per Day

0,7% to 1,5%
CPU load on monitored systems

Архитектура взаимодействия протоколирования и обнаружения



Сценарий

1. Зафиксирована подозрительная активность: *доступу к хранилищу и выгрузка большого объема данных*
2. Создан инцидент, назначен ответственный, доступ к данным заблокирован/разрешен
3. Выяснилось, что этот сотрудник не должен выполнять задачу по выгрузке данных в большом объеме
4. Доказательная база по действиям сотрудника подготовлена с помощью UI Logging, запущено расследование
5. Расследование завершено, инцидент закрыт и помещён в историю
6. Создано правило, запрещающее выгрузку данных более чем на 10 клиентов

Компании горнодобывающей промышленности и металлургии

используюющие SAP GRC решения

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

- Противодействие финансовому мошенничеству и управление доступом
- Прозрачный безопасный доступ в бизнес-приложения

Северсталь

- Противодействие финансовому мошенничеству и управление доступом
- Построение системы внутреннего контроля за формированием финансовой отчетности
- Управление рисками

НЛМК

- Противодействие финансовому мошенничеству и управление доступом
- Контроль за корректностью бизнес-процессов

Металлоинвест

- Противодействие финансовому мошенничеству и управление доступом

exxaro POWERING POSSIBILITY

- *Sibanye Gold Limited-Corporate Divi*
- *AEL MINING SERVICES LIMITED*
- *Stora Enso Oyj*
- *CRH Nederland B.V.*
- *OTTO FUCHS*
- *Kardemir Karabuk*
- *PanAust Limited*
- *Pacific Aluminium Services Pty Ltd*
- *Polyus gold*
- *Corporacion Nacional del Cobre*

ArcelorMittal

- *Aptar Group, Inc.*
- *Antofagasta Minerals S.A.*
- *Gebr. Kemper GmbH & Co. KG*
- *Novelis AG*
- *Almatis GmbH*
- *Tata Steel Ltd*
- *The Iron Ore Company of Canada*
- *RioTinto*
- *Impala Platinum Holdings Ltd*
- *Lonmin Platinum*
- *Votorantim S.A.*

ЧТПЗ

Votorantim

LONMIN

CODELCO

POLYUS GOLD INTERNATIONAL

RioTinto

sesa sterlite a vedanta company

IMPALA PLATINUM

Нефте-газовые компании

использующие SAP GRC решения

- Противодействие финансовому мошенничеству и управление доступом

- Противодействие финансовому мошенничеству и управление доступом
- Построение системы внутреннего контроля за формированием финансовой отчетности
- Защищённый прозрачный доступ к бизнес-системам

- Противодействие финансовому мошенничеству и управление доступом

- *Empresa Nacional del Petroleo*
- *Promigas S.A. E.S.P.*
- *Nigeria LNG Limited*
- *Peru LNG S.R.L.*
- *Pacific Drilling Services, Inc.*
- *Bharat Petroleum Corporation*
- *REPSOL, S.A.*
- *Nigerian National Petroleum Corp. NNPC*
- *Essar Oil Limited*
- *Petroleum Development Oman LLC*
- *Chevron U.S.A. Inc.*
- *Nexen Energy ULC*
- *Surgutneftegas OAO*
- *Valero Services, Inc*
- *Oil & Natural Gas Corporation*

Компании в индустрии химия и нефте-химия

использующие SAP GRC решения

- Противодействие финансовому мошенничеству и управление доступом
- Прозрачный безопасный доступ в бизнес-приложения
- Контроль корректности финансовой отчетности

- Противодействие финансовому мошенничеству и управление доступом

- Управление рисками

- Противодействие финансовому мошенничеству и управление доступом

- *Nizhnekamskneftekhim PAO*
- *Química Amparo Ltda*
- *Gujarat State Fertilizers &*
- *Braskem S/A*
- *TASNEE*
- *Rashtriya Chemicals & Fertilizers Ltd*
- *Kansai Nerolac Paints Ltd*
- *DuluxGroup (Australia) Pty Ltd*
- *RAG Aktiengesellschaft*
- *Ashland LLC*
- *W.R. Grace & Co.*
- *Agrium Inc.*
- *Entegris, Inc.*
- *Mitsubishi Chemical Systems, Inc.*

Компании в индустрии ритейла

использующие SAP GRC решения

- Противодействие финансовому мошенничеству и управление доступом
- Противодействие финансовому мошенничеству
- Противодействие финансовому мошенничеству и управление доступом
- Противодействие финансовому мошенничеству

- *Grupo Ramos, S.A.*
- *Netretail, s.r.o.*
- *Indústria e Comércio de Confecções*
- *El Palacio de Hierro, S.A. de C.V.*
- *Zedach eG*
- *Loblaws Inc.*
- *Woolworths Limited*
- *Caleres, Inc.*
- *METRO AG*
- *Ulta Salon, Cosmetics & Fragrance,*

Проекты в телеком-компаниях

используюющие SAP GRC решения

МегаФон

- Контроль корректности финансовой отчетности
- Противодействие финансовому мошенничеству и управление доступом

vodafone

- Управление доступом
- Противодействие мошенничеству

Bouygues Telecom

- Противодействие финансовому мошенничеству и управление доступом

ҚАЗАҚТЕЛЕКОМ

- Управление рисками
- Управление внутренним контролем

ÇALIK HOLDİNG

- *Bouygues Telecom*
- *Telecom Argentina S.A.*
- *Calik Holding A.S*
- *Deutsche Telekom AG*
- *Tata Teleservices Ltd. Selected*
- *Telecom Italia*
- *KT Corporation*

TELECOM

kt

Deutsche Telekom

TATA indicom

TELECOM ITALIA

Рекомендации по шагам к Безопасности данных в SAP

Спасибо

Прокудин Аркадий
Arkady.Prokudin@sap.com

Mob. +7(903) 224-59-50

Tel. +7(495) 755-98-00 (ext.4190)

THE BEST RUN SAP