5 ШАГОВ К ПРАВИЛЬНОЙ БЕЗОПАСНОСТИ

Роман Душков

Пресейл-менеджер

про процессы

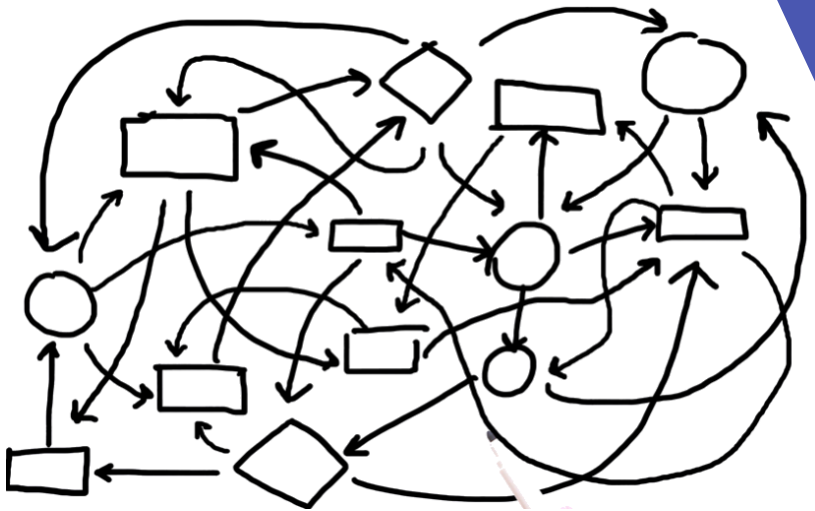
про рутину

про картину сверху

про технологии

про отчёты

про процессы



ИБ + SIEM + SOAR

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

1 **Разрозненные системы**

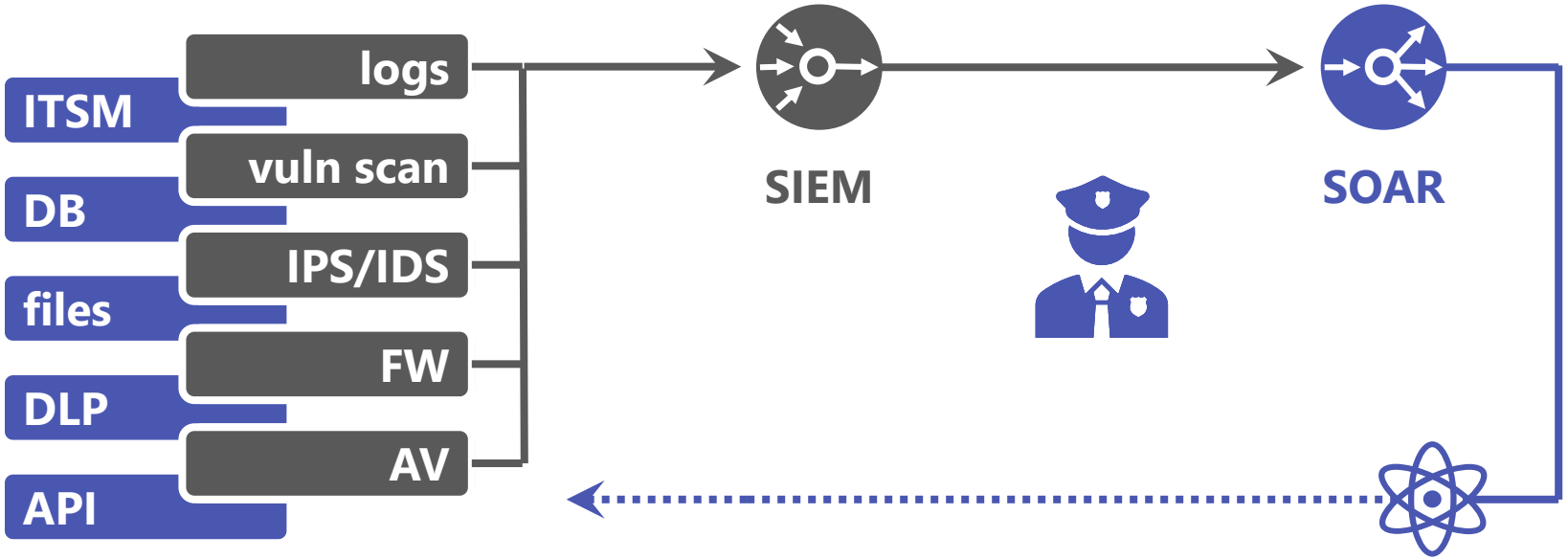
Разные формы отчётов, консоли управления, ответственные

2 **Нормализация и хранение**

Регистрация, сбор, корреляция, приведение к общему виду

3 **Процессы и автоматизация**

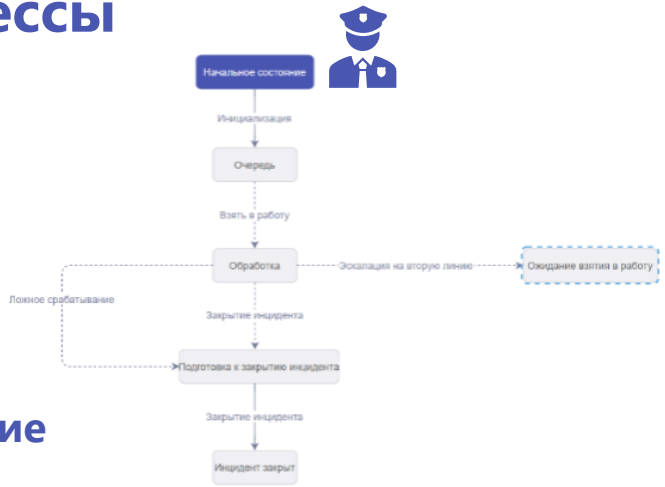
Общие процедуры реагирования и автоматизация реагирования

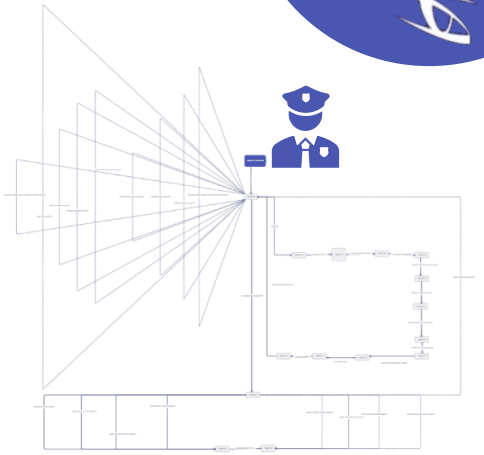


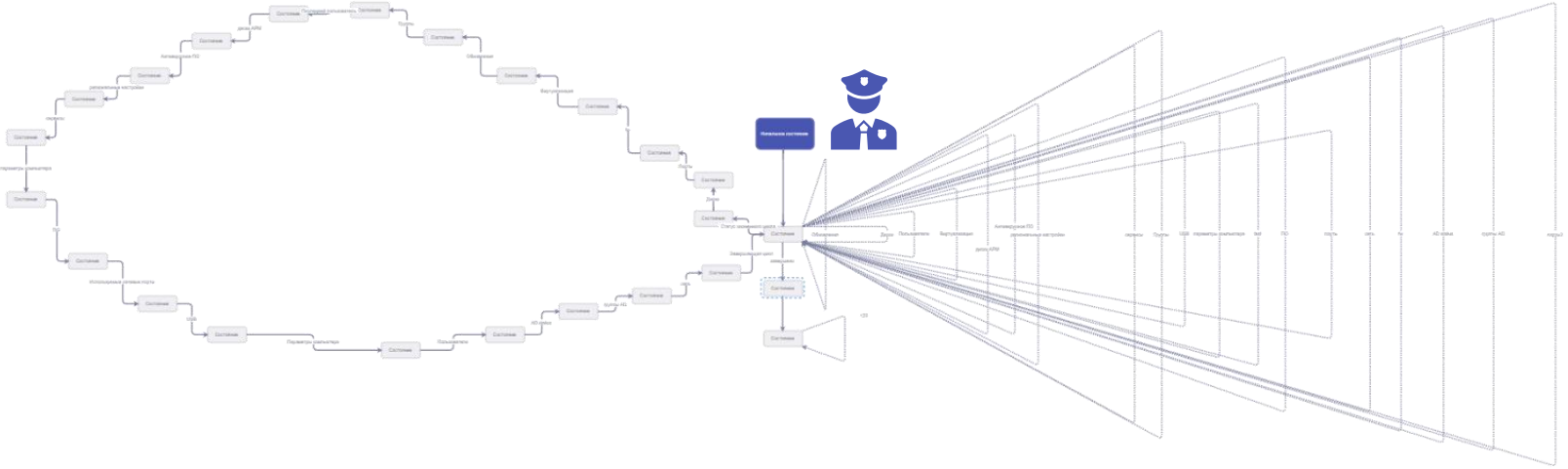
Рабочие процессы

Ручные

Автоматические







про процессы

Редактировать их нужно быстро и легко

Применять из коробки с осторожностью

Количество - не значит качество

про рутину

Управление инцидентами
без автоматизации

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

85 мин

1. **Анализ письма**

   выделение темы, содержимого, текста и ссылок

   HYBRID ANALYSIS

2. **Поиск деталей**

   проверка отправителя, домена, вложений и ссылок

   ThreatCrowd
   urlscan.io
   A sandbox for the web
   WhoisXML API
   Unified Results!

3. **Поиск похожих**

   поиск других получателей

   IBM Radar
   MaxPatrol SIEM

4. **Блокировка**

   добавление отправителя и домена в чёрный список

   Exchange

5. **Очистка сервера**

   от опасных писем или вложений

6. **Проверка хостов**

   запуск проверки на рабочих станциях пользователей

   kaspersky

7. **Оповещение**

Управление инцидентами с автоматизацией

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

5 мин

1. Анализ письма
2. Поиск деталей
3. Поиск похожих
4. Блокировка
5. Очистка сервера
6. Проверка хостов
7. Оповещение

Автоматизация рутины

Снижение влияния человеческого фактора

Ускорение обработки

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Управление уязвимостями без автоматизации

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

10 | 40 | 20 | 20 | 10 | 10

110 мин

1. **Отчет со сканера**

   получение информации со сканера уязвимостей

   MaxPatrol 8
   Nessus
   RED Check
   Qualys.

2. **Анализ контекста**

   определение критичности уязвимостей, CVSS, CVE

3. **Определение срочности**

   Установка SLA в ИТ-отдел

4. **Задачи в ITSM**

   создание заявок на устранение

   JIRA
   HelpDesk

5. **Подготовка отчёта**

   контроль исполнения

6. **Повторная проверка**

   проверка обновлённых данных в отчётах сканера уязвимости

Управление уязвимостями с автоматизацией

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

10 мин

1. Отчет со сканера
2. Анализ контекста
3. Определение срочности
4. Задачи в ITSM
5. Подготовка отчёта
6. Повторная проверка

Совместная работа

База знаний

Обогащение модели активов и поиск патчей

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

про рутину

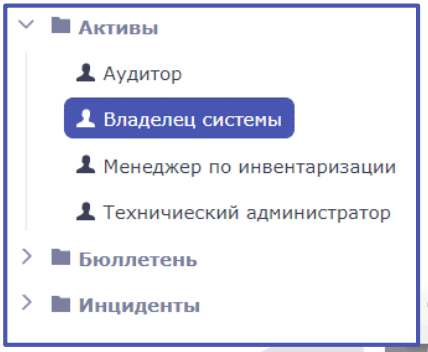
Рутину автоматизировать можно

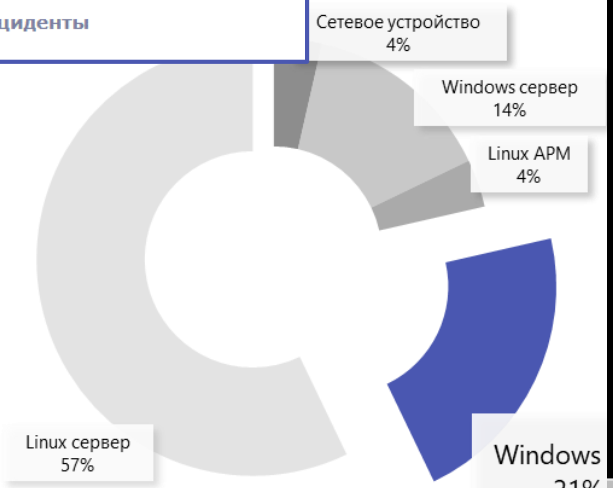
Есть задачи, которые нельзя автоматизировать

Робот не заменит человека

про картину сверху

Объекты





Любые сущности

Каталоги

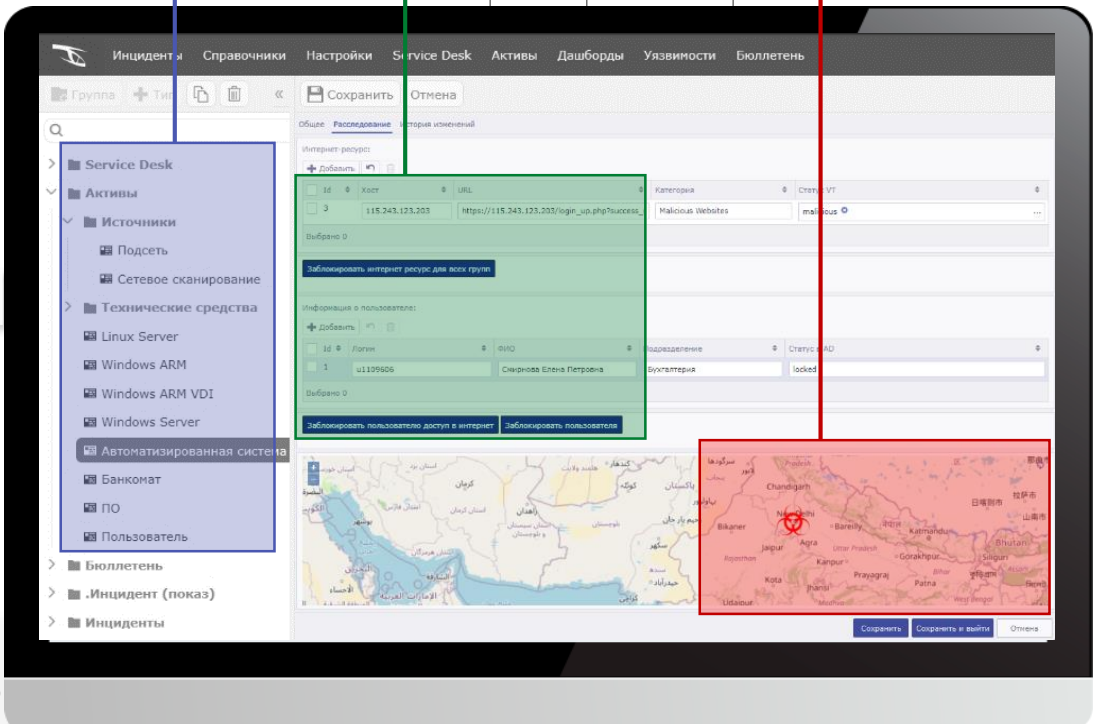
дата

время

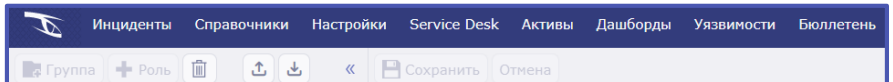
таблица

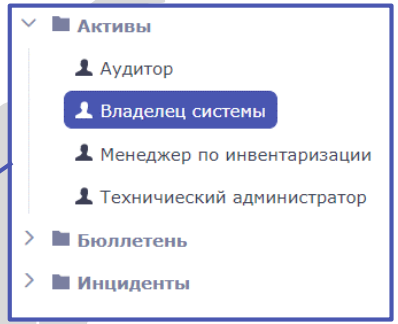
карта

и т.д.



Роли и меню

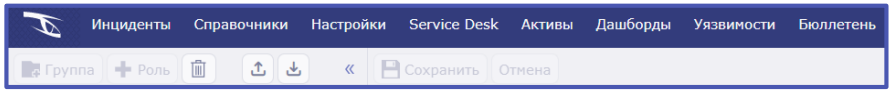

Инциденты
Справочники
Настройки
Service Desk
Активы
Дашборды
Уязвимости
Бюллетень
Группа
Роль
Сохранить
Отмена

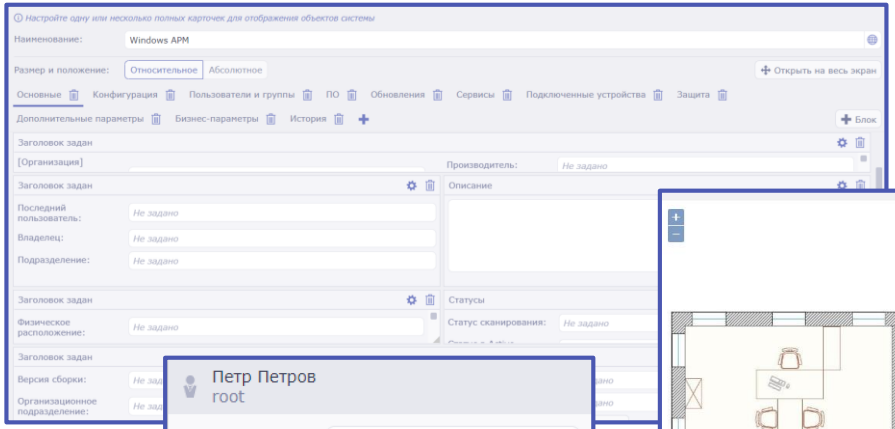

Активы
Аудитор
Владелец системы
Менеджер по инвентаризации
Технический администратор
Бюллетень
Инциденты

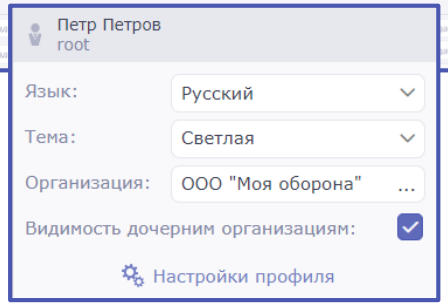
Петр Петров
root
Язык:
Русский
Тема:
Светлая
Организация:
ООО "Моя оборона"
Видимость дочерним организациям:
Настройки профиля

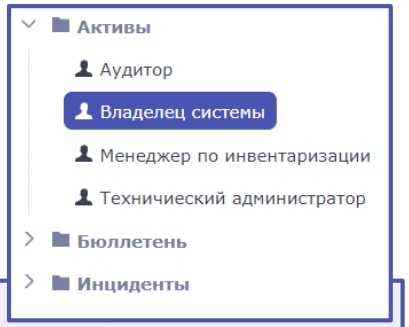

ЧТЕНИЕ
ВКЛАДКИ МЕНЮ
РЕДАКТИРОВАНИЕ
АДМИНИСТРИРОВАНИЕ

Не нужно программировать









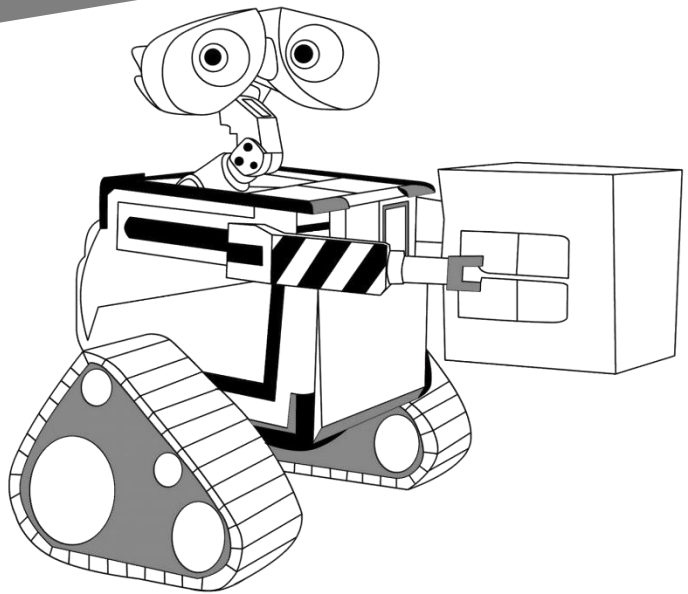
про картину сверху

Управлять ролевой моделью и доступами

Видеть детали и разные типы данных

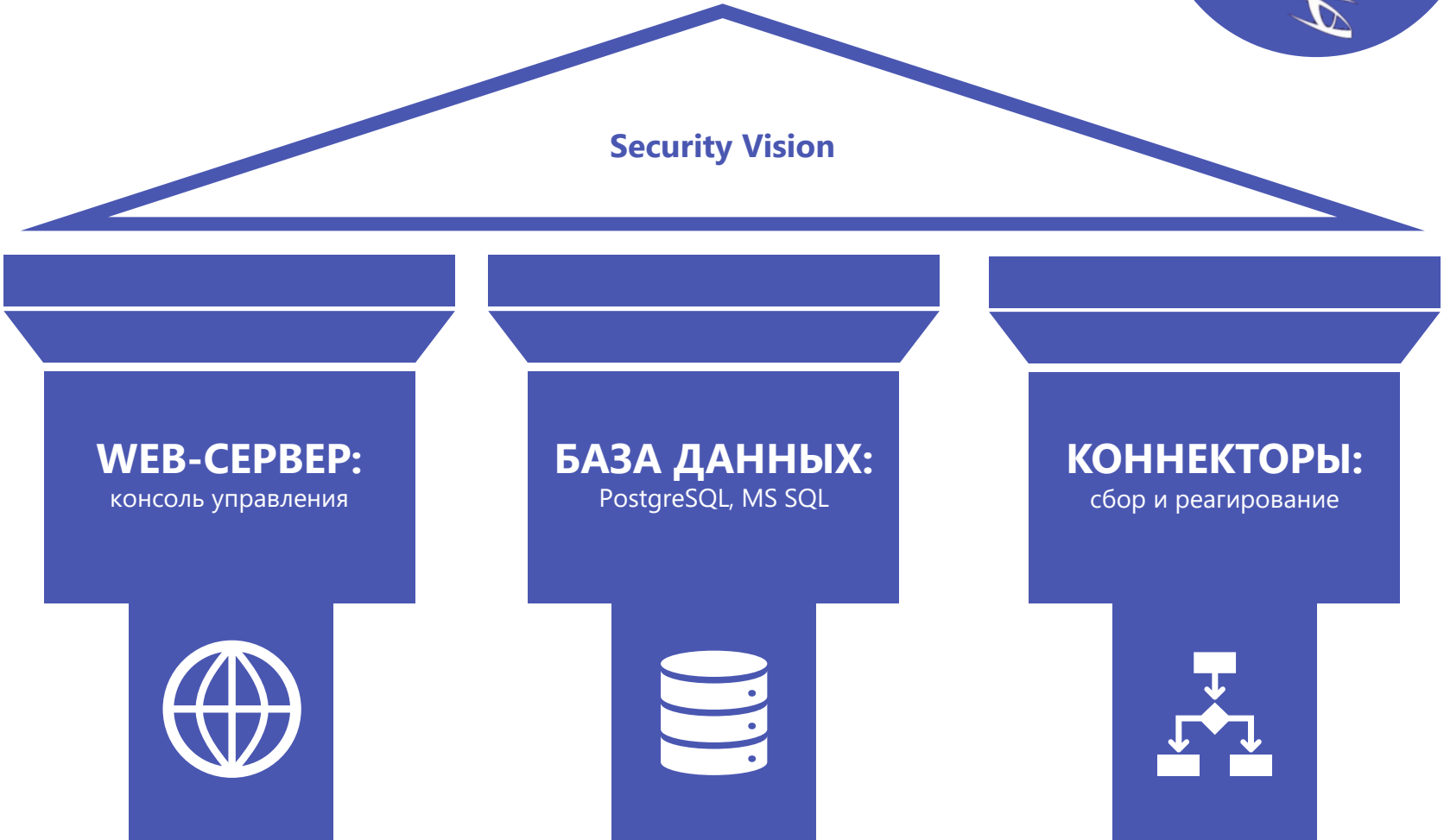
Настраивать всё под себя

про технологии



Архитектура

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ



Коннекторы

Сбор и обогащение

Реагирование на события

Коннекторы

email | Syslog | файлы | БД | API | DNS | SNMP | LDAP | SOAP | скрипты

Сбор и обогащение

Реагирование на события

про технологии

Разные ОС и СУБД для платформы

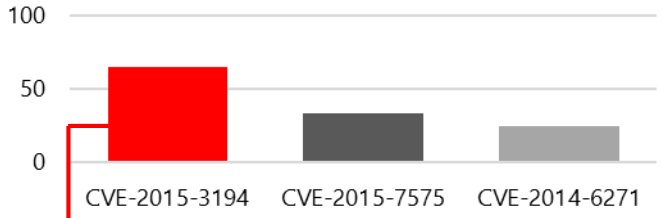
Интеграции через графический интерфейс

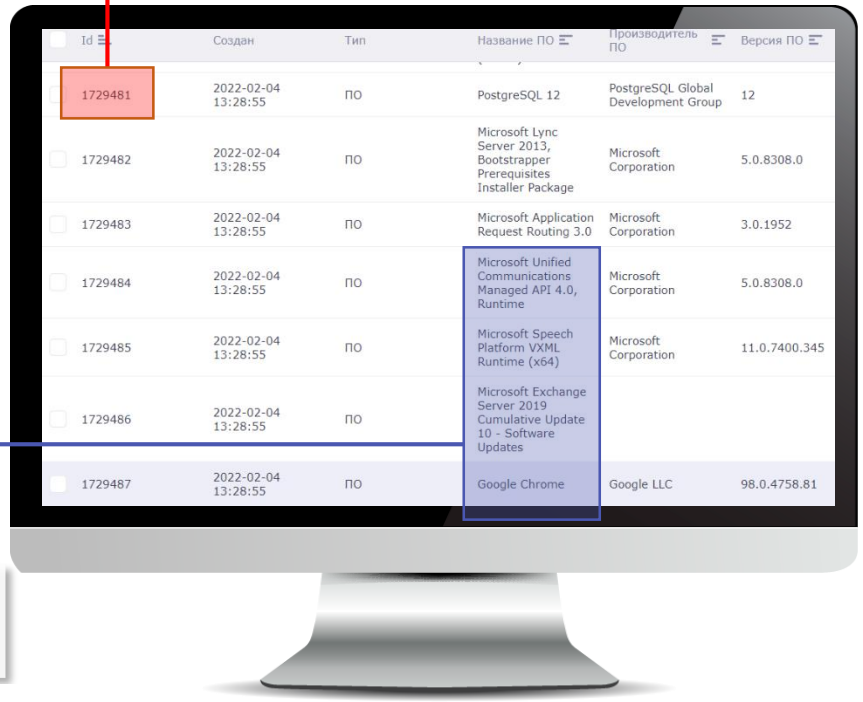
Разные технологии для необычных внедрений

про отчёты

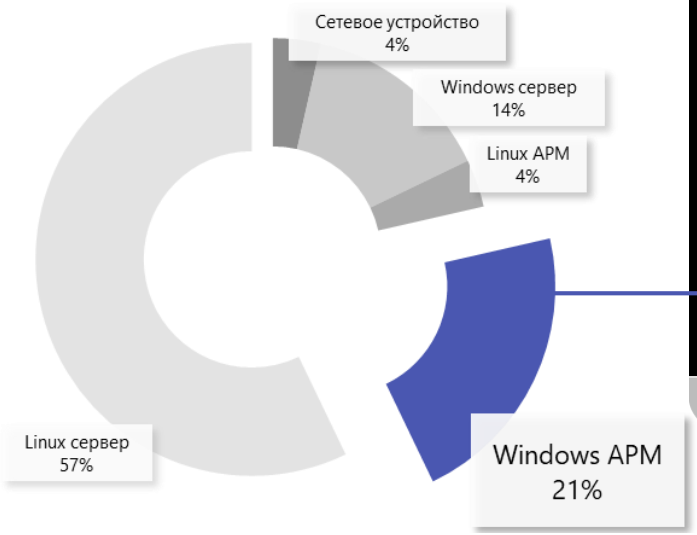

ВАЛЕНТИН ВЕНИАМИНОВИЧ, ВЫ ПРОСИЛИ ОТЧЕТ. ВОТ, Я РАСПЕЧАТАЛА
А МОЖНО В ЭЛЕКТРОННОМ ВИДЕ?

Отчеты и база знаний





Id	Создан	Тип	Название ПО	Производитель ПО	Версия ПО
1729481	2022-02-04 13:28:55	ПО	PostgreSQL 12	PostgreSQL Global Development Group	12
1729482	2022-02-04 13:28:55	ПО	Microsoft Lync Server 2013, Bootstrapper Prerequisites Installer Package	Microsoft Corporation	5.0.8308.0
1729483	2022-02-04 13:28:55	ПО	Microsoft Application Request Routing 3.0	Microsoft Corporation	3.0.1952
1729484	2022-02-04 13:28:55	ПО	Microsoft Unified Communications Managed API 4.0, Runtime	Microsoft Corporation	5.0.8308.0
1729485	2022-02-04 13:28:55	ПО	Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	11.0.7400.345
1729486	2022-02-04 13:28:55	ПО	Microsoft Exchange Server 2019 Cumulative Update 10 - Software Updates		
1729487	2022-02-04 13:28:55	ПО	Google Chrome	Google LLC	98.0.4758.81



Отчеты и база знаний

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

» Выгрузить отчет

Настройки выгрузки

Название файла: Все активы

Форматы отчета: Docx Pdf Xlsx Ods Odt

Импортировать настройки из дашборда

Наименование: Из карточки

Описание:

Группа: Активы

Формат документа: A5 A4 A3

Ориентация документа: Портретная Альбомная

Отступы документа: Настроить

Word

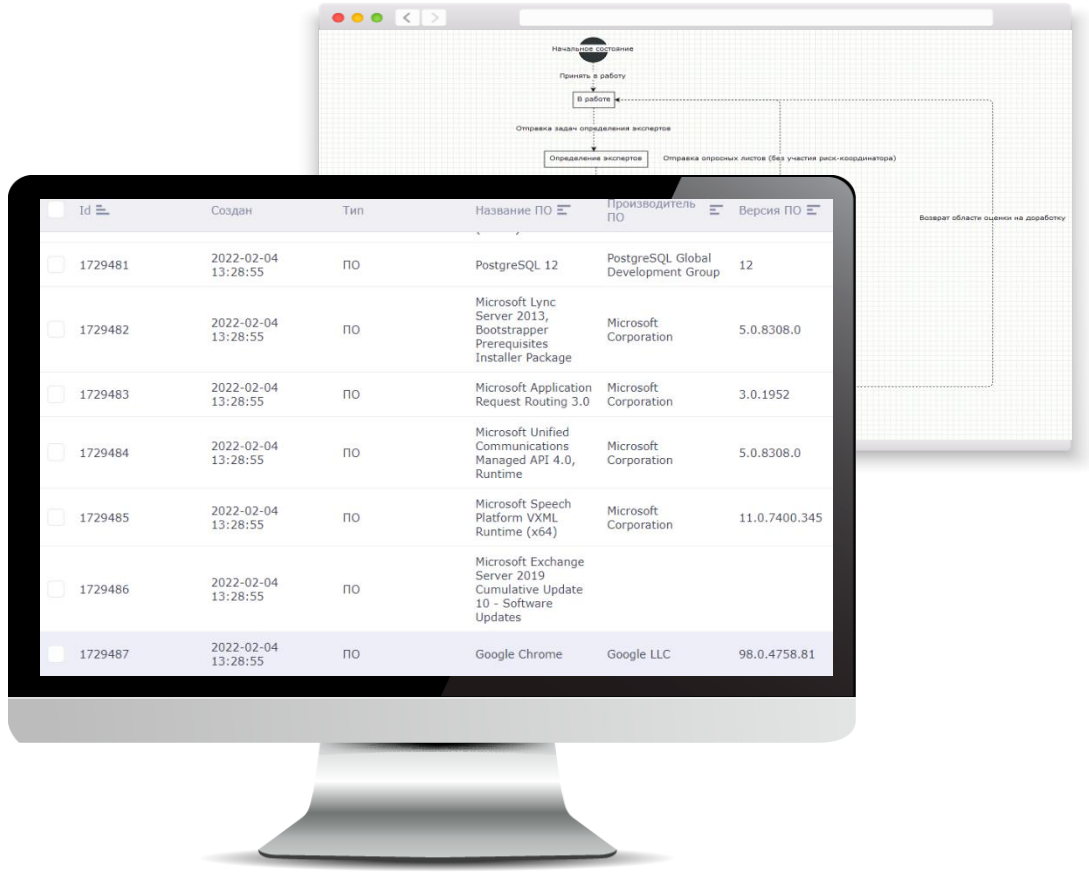
Нумерация страниц:

Колонтитулы:

Excel

Кол-во страниц в ширину: Не задано

Кол-во страниц в длину: Не задано



про отчёты

Отчёты – это важно в стратегическом плане

В них можно сохранять детали

Их нужно кастомизировать

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

про процессы

про рутину

про картину сверху

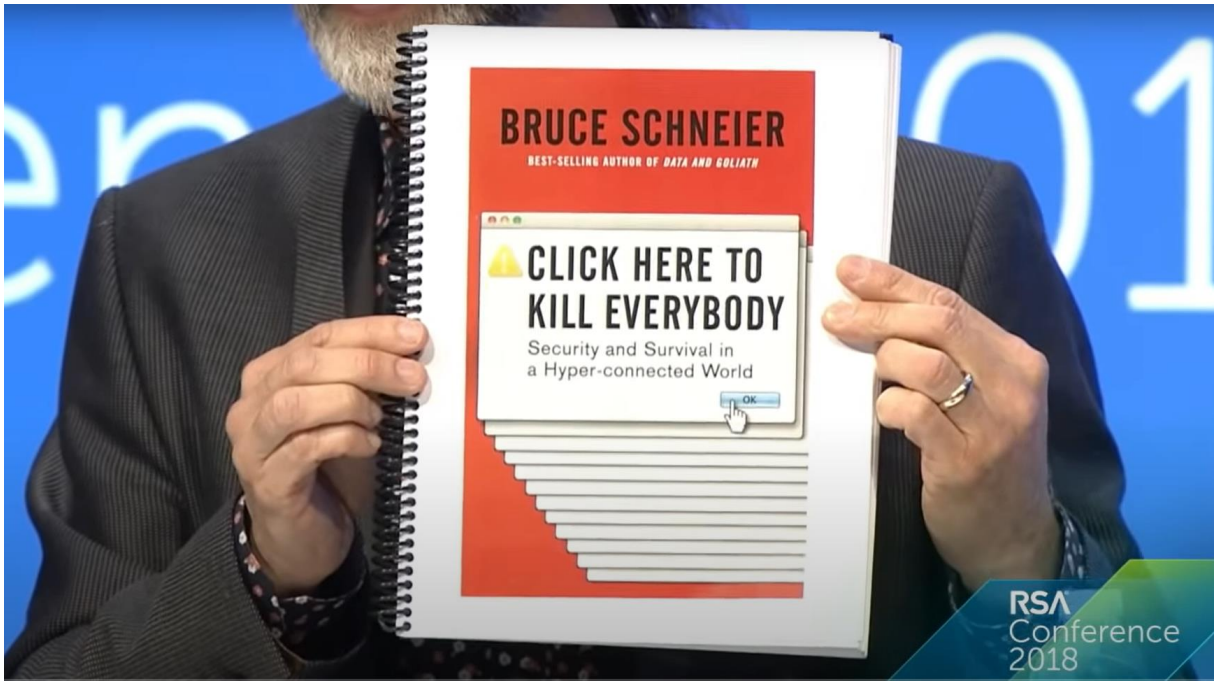
про технологии

про отчёты

https://www.menti.com/

7947 0527

Если бы хакеры были ураганом



https://www.youtube.com/watch?v=Zog1WipbE9c

5 ШАГОВ К ПРАВИЛЬНОЙ БЕЗОПАСНОСТИ

Роман Душков

Пресейл-менеджер