JET SECURITY CONFERENCE

VIII ежегодная конференция
Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU

Radisson BLU

Check Point SOFTWARE TECHNOLOGIES LTD
Premier Business Partner IBM
Hewlett Packard Enterprise
f5
IMPERVA
SKYBOX SECURITY
INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ
TREND MICRO
paloalto NETWORKS
FireEye
KASPERSKY PLATINUM PARTNER
POSITIVE TECHNOLOGIES
tufin
FORTINET
SOLAR SECURITY software&services
CYBERARK
TRAPX SECURITY
ONE IDENTITY
RAPID7
iDeals VIRTUAL DATA ROOM

JET CONFERENCE

01/06/2017

Как реализовать масштабный проект в сжатые сроки

Игорь Шелест, архитектор инфраструктуры информационной безопасности ЦИБ

JET CONFERENCE

SOLAR DOZOR

Поиск в системе

Рабочий стол Аналитика | 30 дней

Пешкова Алла Сергеевна
Кредитный контролер
Отдел экономического анализа

серьезные события 0
сообщения 0
файлы исходящие 0
файлы входящие 0

Нехарактерные контакты
<не определены>

Мои инциденты 45+19

Заблокированные письма 0

Информационные объекты

Зарплата и бонусы
27 +7
Всё самое нужное д... 18.4 Кб
39787133.zip 15.8 Кб
2015-05-29_13h45_... 58.7 Кб

Анализ рынка
17 +5
Анализ рынка расти... 26 Кб
Анализ масложиров... 78.5 Кб
Анализ мирового р... 78.9 Кб

Резюме
15 +5
Резюме_Кувыкин К... 34.4 Кб
Резюме_Кудяшов А... 34.6 Кб

Группы на особом контроле

На увольнение: +5 5
Испытательный срок: 1 0
Расходование материальных средств: 5 0

Аномальное поведение

Персоны. Снижение уровня доверия
Бубнов Вячеслав Самуилович
Заместитель начальника отдела
Ершова Евгения Александровна
Главный бухгалтер

Автоматически созданные персоны
amadeus@gmail.com
floyd.george49@mail.ru

События 8+9 15+15 295+295

rf.vasilyev@krasnodarste... → Гареев Иван Никитевич
Секретарь начальника у...
Входящая почта 08 Апрель 16, 17:02
Обнародовали перед публикой
, которые, например, находили время продолжительнос...

Митрохов Алексей Титов... → Семерикова Наталья Ант...
Начальник отдела → Секретарь начальника у...
Внутренняя почта 08 Апрель 16, 17:01
Ведется работа по всем направлениям
м журналистам освещать как хорошие организационны

Таганцева Ирина Михаил... → Снегирева Алина Потапо...
Психолог → Менеджер по работе с к...
Внутренняя почта 08 Апрель 16, 16:59
Попробуйте стать бизнесменом
и ошибку самое главное заключается исследования и ра...

rf.vasilyev@krasnodarste... → Грабарь Софья Семеновн...
Начальник отдела
Входящая почта 08 Апрель 16, 16:57
Правильный тон для передачи вашей идеи
х ошибок, от чего достигнете людям организационные р...

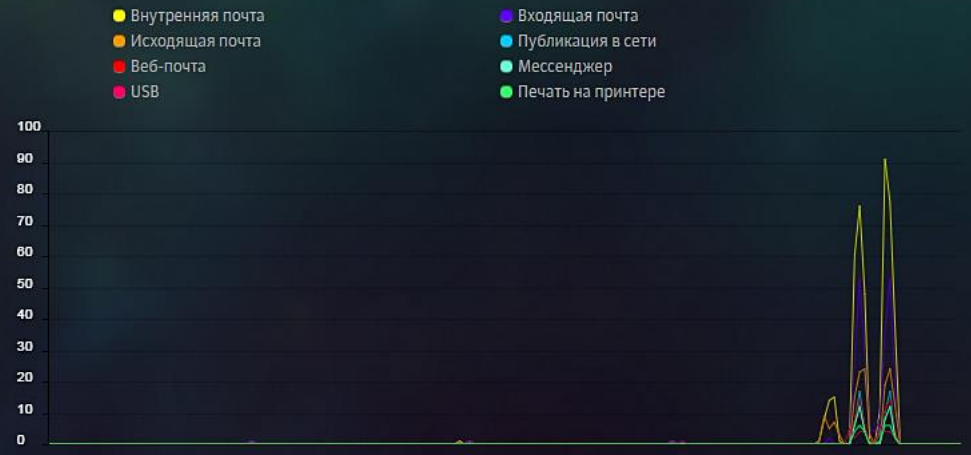
Сереброва Екатерина Се... → Колдаев Герман Ермола...
Заместитель начальника... → Менеджер по работе с к...
Внутренняя почта 08 Апрель 16, 16:56
Готовы пойти на риск, чтобы дать людям шанс поднят...
, обращаясь к будущему трехлетию организационные р...

Тредиаковская Мария Ив... → Семерикова Наталья Ант...
Секретарь начальника уп... → Секретарь начальника у...
Внутренняя почта 08 Апрель 16, 16:54
Обнародовали перед публикой
м журналистам освещать как хорошие исследования и р...

info@krasnodarsteeLru → Гареев Иван Никитевич
Секретарь начальника у...
Входящая почта 08 Апрель 16, 16:51
Нельзя ходить с опущенной головой

Серьезные события по типу угроз

Все события по каналам коммуникаций



JET

CONFERENCE

О чем пойдет речь?

Развертывание Solar Dozor 6.x с нуля

Миграция с существующей инсталляции Solar Dozor

Road Map стандартного проекта

JET

CONFERENCE

Развертывание Solar Dozor 6.x с нуля

Обследование

Проектирование

Внедрение

Особенности развертывания

- **Уточнение статистики по потоку – со слов администраторов**
- **Обследование мест установки оборудования**
- **Согласование точек съема трафика**
- **Запрос стартовой информации для подготовки политики Solar Dozor**

JET

CONFERENCE

Обновление существующего Solar Dozor 5.x

Обследование

Проектирование

Внедрение

Особенности обновления

- **Уточнение статистики по потоку – с текущей инсталляции**
- **Анализ возможности использования текущего оборудования**
- **Обследование мест установки оборудования**
- **Анализ существующей политики обработки сообщений**
- **Согласование необходимости переноса частей политики на новую версию Solar Dozor 6.x**

JET CONFERENCE

Оборудование при обновлении.
Вариант 1

Существующий архив на существующем оборудовании в режиме чтения
Новый архив сохраняется на новом оборудовании

Плюсы:

1. Быстрота обновления
2. Отсутствие простоя сервиса на время обновления
3. Снижение рисков потери архива
4. Отсутствие необходимости копирования данных существующего архива

Минусы:

1. Необходимость использования 2 интерфейсов для поиска сообщений
2. Необходимость использования оборудования на время актуальности старого архива

JET CONFERENCE

Оборудование при обновлении.
Вариант 2

Выполняется обновление формата базы до 6 версии на новом или на существующем оборудовании

Плюсы:

1. **Общий интерфейс для поиска новых и старых сообщений в архиве**

Минусы:

1. **Простой сервиса поиска в архиве на время обновления**
2. **Увеличение времени обновления**
3. **Потенциальная необходимость копирования существующих данных**
4. **Риск потери архива при отсутствии резервного копирования**

JET

CONFERENCE

Политика Solar Dozor при обновлении

Мониторинг

Варианты:

1. Базовая политика Solar Security
2. Базовая политика Solar Security + существующая политика
3. Обследование для формирования политики

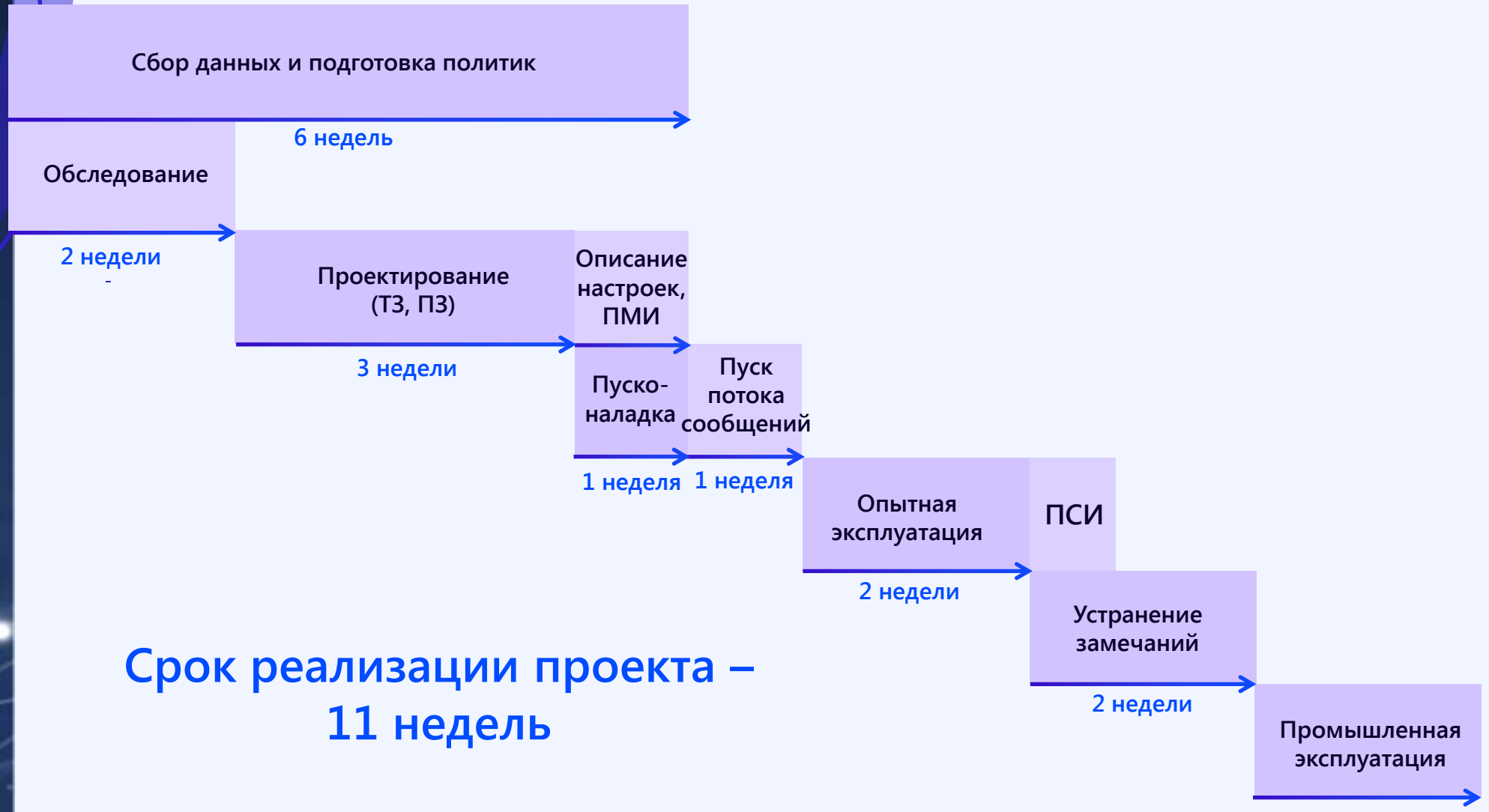
Фильтрация

Варианты:

1. Миграция существующей политики
2. Миграция существующей политики + обследование для формирования политики
3. Запрос данных по активной фильтрации + базовая политика Solar Security (без фильтрации)
4. Создание политики с нуля

JET CONFERENCE

RoadMap стандартного проекта



Срок реализации проекта – 11 недель

JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!