

КОНТРОЛЬ

РЕАГИРОВАНИЕ

АВТОМАТИЗАЦИЯ

Incident Response Platform

R-Vision Incident Response Platform (IRP)



Единая точка консолидации информации
обо всех инцидентах информационной безопасности в компании (корпоративный SOC)

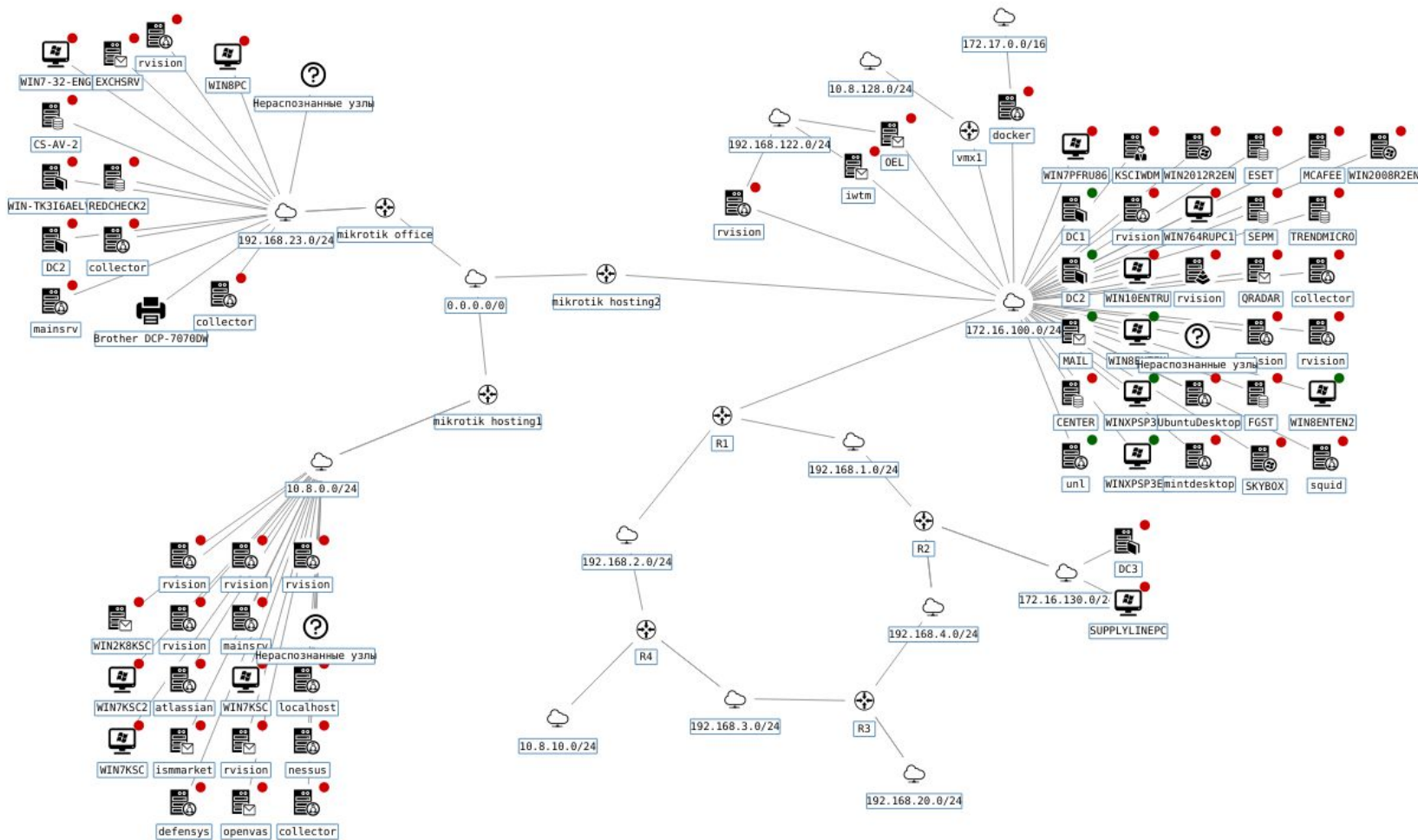
Платформа для совместной работы
группы реагирования на инциденты ИБ с возможностью сбора, анализа и хранения сведений, относящихся к инцидентам ИБ

Центр координации деятельности
сотрудников компании, распределения задач и учета выполненных мероприятий по реагированию на инциденты ИБ

#1 Интеграция



#2 Контроль ИТ-инфраструктуры



#3 Управление уязвимостями

Иденти...	Уровень	Название	Кол...	Статус
MP-7014		Подмена данных	11	Открыта
MP-7034		Некорректная цепочка сертификатов	11	Открыта
MP-8175		Не требуется подписывание SMB	10	Открыта
MP-1071		Планировщик заданий	10	Открыта
MP-183773		Выполнение произвольного кода	8	Открыта
MP-1065		Удаленное управление реестром	8	Открыта
MP-8122		Подобраны учетные записи	8	Открыта
MP-183198		Обход ограничений безопасности	7	Открыта
MP-412922		Уязвимость протокола удаленного рабо...	6	Открыта
MP-1304		Возможна атака Anti DNS Pinning	6	Открыта
MP-430006		Политика межсетевого экрана по умолч...	5	Открыта
MP-8225		Включена маршрутизация	5	Открыта
MP-412724		Уязвимость при обработке запросов к с...	4	Открыта
MP-183847		Разглашение информации	4	Открыта
MP-1013		Доступ к каталогам	4	Открыта
MP-182481		Разглашение информации	4	Открыта
MP-182482		Разглашение информации	4	Открыта
RC-18741		Уязвимость Win32k, связанная с неправ...	3	Открыта*
RC-74354		Уязвимость доступа к веб-браузерной п...	3	Открыта

Показать в списке оборудования

Название ↑
192.168.23.100 Ответственный: Срок устранения:
DC2 — 192.168.23.5 Ответственный: Срок устранения:
EXCHSRV — 192.168.23.22 Ответственный: Срок устранения:
HYPER-SRV — 192.168.23.200 Ответственный: Срок устранения:
NOTE — 192.168.23.227 Ответственный: Срок устранения:
REDCHECK2 — 192.168.23.67 Ответственный: Срок устранения:
WIN-SC — 192.168.23.23 Ответственный: Срок устранения:
WIN-TK316AELVQL — 192.168.23.3 Ответственный: Срок устранения:
WIN7-32-RUS-1 — 192.168.23.91 Ответственный:

Наименование
Политика по управлению уязвимостями 1 Политика уязвимостей 1
Политика управления критичными 123
Уязвимости ИС1 ИС1
Уязвимости по Системе ЭПД

Группы ИТ-активов:

Добавить Удалить

- IS-7 AC "Почтовый сервис"
- IS-12 Группа "сервера филиала 1"
- IS-10 Группа серверного оборудования 1
- IS-11 Информационная система "Важная"
- IS-8 Информационная система "Зарплата и кадры"

Ответственные:

Уровень	Ответственный
	Александров Иван (admin)
	Левин Михаил (m-user2)
	Петров Петр (cm-user1)
	Сидоров Андрей (m-user1)
	Кузнецов Антон (it-user1)

Срок устранения уязвимостей (дни):

Уровень	Срок устранения
	1
	3
	14
	21



#4 Управление инцидентами

ВЫЯВЛЕНИЕ

Централизованный сбор инцидентов из различных источников, анализ, классификация

РАССЛЕДОВАНИЕ

Сбор свидетельств, выявление источников, причин и обстоятельств инцидента

ОТЧЕТНОСТЬ

Формирование различной отчетности (сводка для руководства, отчеты для регуляторов и пр.)

РЕАГИРОВАНИЕ

Назначение ответственных лиц и группы реагирования, контроль выполняемых действий и сроков устранения

АНАЛИЗ И СТАТИСТИКА

Анализ статистики инцидентов по объектам, филиалам, типам и др. Выявление тенденций и системных проблем



Архитектура
+ Политики инвентаризации
Политики управления уязвимостями
Параметры уведомлений
Управление инцидентами
Типы инцидентов
Циклы обработки инцидентов
Поля инцидентов
Категории инцидентов
Шаблоны инцидентов
Уровни критичности
Действия по инциденту
+ Справочники
Правила уведомления
Правила назначения на инциденты
Правила реагирования
Правила автозаполнения
Интеграция с внешними системами
Обмен данными по инцидентам

№ ↑	Наименование
[-] Цикл обработки: Типовой цикл обработки инцидентов	
2	Правило уведомления рук-я Правило
3	Уведомление по критическим инцидентам Критические инциденты
4	Уведомление по ИС-123 Уведомление по конкретной системе
5	Уведомление по филиалу Уведомление об инциденте в филиале

Наименование правила уведомления:

Уведомление по ИС-123

Описание:

Уведомление по конкретной системе

Цикл обработки:

Типовой цикл обработки инцидентов

Критерии:

Тип	Поле	Значение
Связанный актив	Группы ИТ-активов	"Группа 'laptop ABC'"

Список пользователей для уведомления:

Добавить	Удалить
Левин Михаил (m-user2)	

Наименование	
[-] Цикл обработки: Типовой цикл обработки инцидентов	
Зарегистрирован инцидент	
Назначение при регистрации инцидента с ИС	
Назначение на инцидент	Назначен ABC
Обработка ABC	Обработка инцидентов из системы ABC
Проверка и расследование	Проверка инциденты
Назначен на обработку	Инцидент с SIEM в обработке
Обработка SIEM	Обработка инцидентов, поступающих из системы SIEM 1
Обработка DLP	Обработка инцидентов с DLP

Наименование:

Обработка ABC

Описание:

Обработка инцидентов из системы ABC

Цикл обработки:

Типовой цикл обработки инцидентов

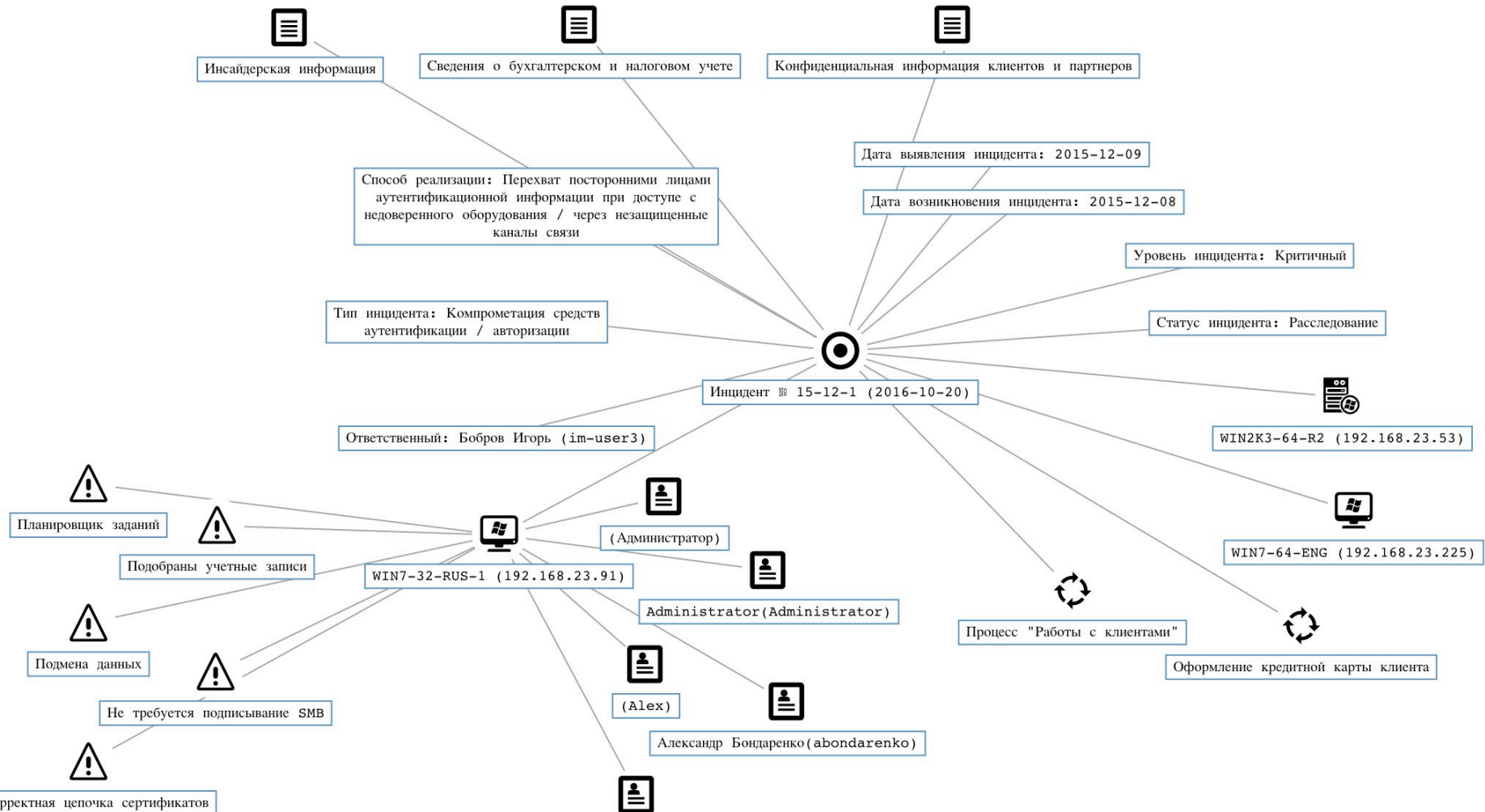
Критерии:

Тип	Поле	Значение
Связанный актив	Группы ИТ-активов	"ABC 'Bank'"
Значение поля	Способ реализации	"Внедрение вредоносного кода по сети"
Значение поля	Приоритет инцидента	"2 (Повышенный)"
Значение поля	Статус инцидента	"Обработка"

Пользователи:

Добавить	Удалить
Бобров Игорь (m-user3)	Участник (просмотр)
Петров Петр (cm-user1)	Участник (изменение)
Козлов Михаил (am-user2)	Ответственный за инцидент

#5 Визуализация и графы связей



#6 Автоматизация реагирования



№	Наименование
Цикл обработки: Типовой цикл обработки инцидентов	
1	Правила реагирования 123
	Правило 123

Наименование: Правила реагирования 123

Описание: Правило 123

Цикл обработки: Типовой цикл обработки инцидентов

Критерии:

Тип	Поле	Значение
Значение поля	Статус инцидента	"Зарегистрирован"
Связанный актив	Оборудование	"WIN7-64-ENG"

Действия по инциденту:

Наименование	Действие
Создание копии скопированных объектов (файлов, виртуальных систем и проч.)	
Ответственный: Александров Иван (admin)	
Срок выполнения: Часов 3	

- + Взаимодействие с третьими лицами
- + Восстановительные действия
- + Действия по сбору дополнительных сведений
- + Корректирующие действия
- + Общеорганизационные действия
- + Проверочные действия
- Экстренные действия
 - Аварийное выключение прикладных систем
 - Блокировка консоли конечного узла
 - Удаленная очистка содержимого мобильного устройства сотрудника
 - Уничтожение информации / носителей информации

#7 Платформа для взаимодействия с внешними SOC, CERT, ГосСОПКА

Обмен информацией

Обмен данными с внешними источниками (SOC, TI)



Оперативный контроль

Контроль сроков реагирования на инциденты



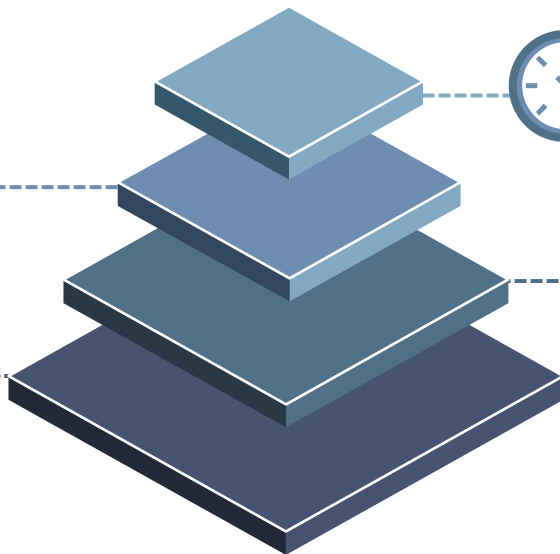
Совместная работа

Рабочие области по инцидентам, коммуникации и обмен данными, учет действий по инциденту



Автоматизация реагирования

Правила реагирования по типам инцидентов, распределение задач, уведомление, эскалация



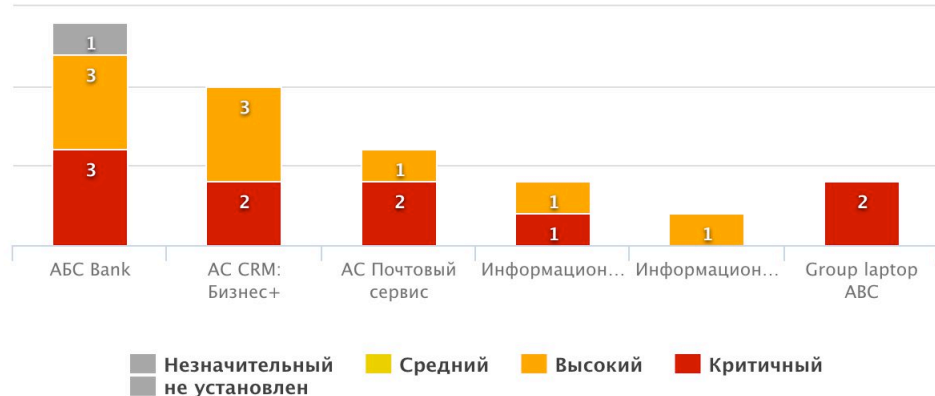
#8 Диаграммы. Графики. Схемы

Сводка Карты и схемы Активы × Инциденты × Важная1 × Важная2 × Схема1 × Схема2 × Помещение Спб × Помещение Мск × Риски × 123

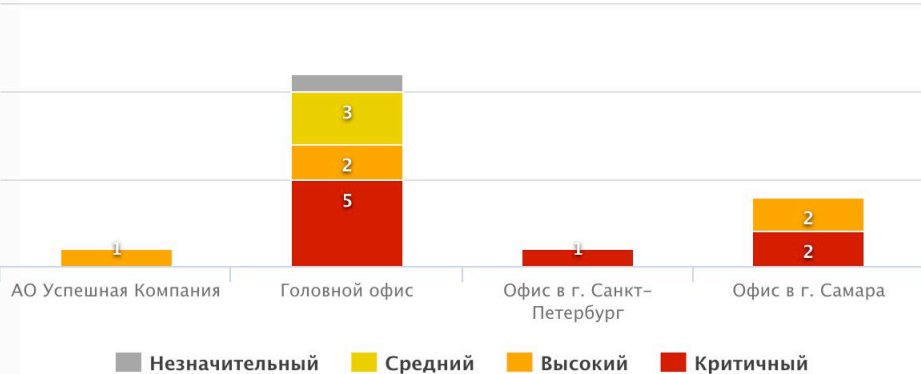
Инциденты в работе



Инциденты по объектам инфраструктуры



Инциденты по подразделениям

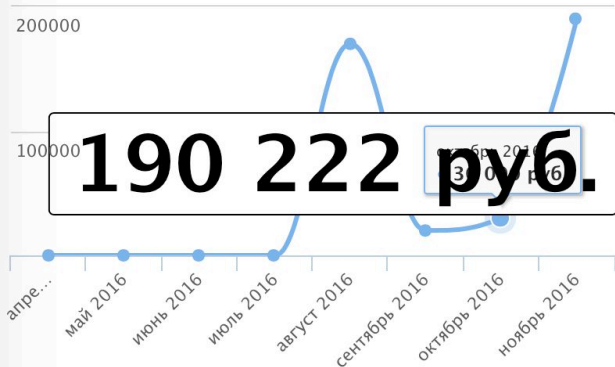


История инцидентов



#9 Метрики

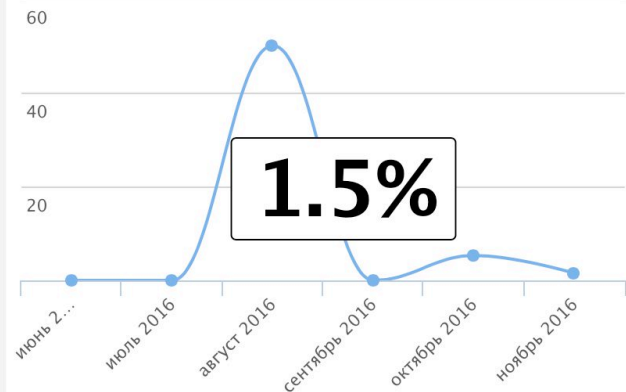
Метрика: Ущерб от реализации инцидентов



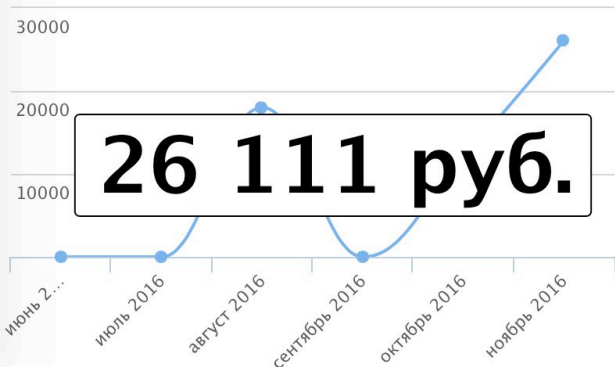
Метрика: Доля инцидентов с соблюдением сроков реагирования



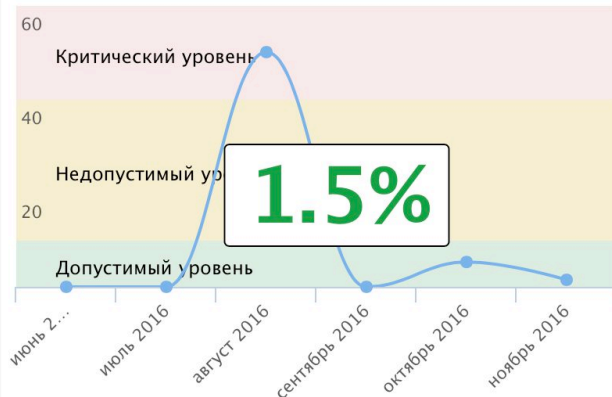
Метрика: Доля инцидентов по типам



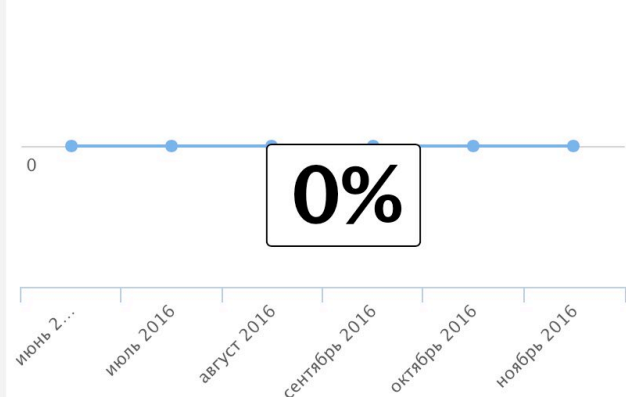
Метрика: Предотвращенный ущерб от инцидентов



Метрика: Доля инцидентов по типам



Метрика: Доля инцидентов по типам



#10 Обмен информацией по инцидентам

Все внутренние инциденты | Внешние инциденты | Критичные инциденты | Инциденты ИС

Идентификатор	Тип инцидента	От ↑	Дата последнего обно...	Комментарии
EXT-16-11-33	Нарушение доступнос...	User2 (user2@rvision...	16 ноября 2016 г., 01:05	0
EXT-16-11-32	Внедрение вредоносн...	User2 (user2@rvision...	16 ноября 2016 г., 01:05	0
EXT-16-11-31	Компрометация средс...	User2 (user2@rvision...	16 ноября 2016 г., 01:05	0
EXT-16-11-30	Компрометация средс...	User2 (user2@rvision...	16 ноября 2016 г., 01:05	0
EXT-16-11-29	Внедрение вредоносн...	User2 (user2@rvision...	16 ноября 2016 г., 01:05	0
EXT-16-11-28	Нарушение в работ...	User2		
EXT-16-11-27	Внедрение вредоносн...	User2		
EXT-16-11-26	Внедрение вредоносн...	User2		
EXT-16-11-25	Несанкционированны...	User2		
EXT-16-11-24	Компрометация средс...	User2		
EXT-16-11-23	Нецелевое использо...	User2		
EXT-16-11-22	Проникновение посто...	User2		
EXT-16-11-21	Внедрение вредоносн...	User2		
EXT-16-11-20	Нарушение доступнос...	User2		

Взять в работу | В архив

Тип инцидента:
Нарушение доступности онлайн-сервисов организации

Дата выявления инцидента:
11.01.2016

Бизнес-подразделения:
Офис в г. Самара

Все внутренние инциденты | Внешние инциденты | Критичные инциденты | Инциденты ИС

ID	Тип инцидента	Уровень инци...	Статус инциде...	Ответственный	Категория
15-12-1	Несвоевременное ...		Расследование	Бобров Игорь (im-u...	Общий инцидент
15-12-2	Внедрение вредо...		Расследование	Кузнецов Антон (im...	Общий инцидент
15-12-3	Несвоевременное ...		Расследование	Суворов Николай (...)	Общий инцидент (подробно)
15-12-4	Несвоевременное ...		Расследование	Суворов Николай (...)	Инцидент, связанный с переводом денежных средств
15-12-5	Несвоевременное ...		Зарегистрирован		Инцидент, связанный с переводом денежных средств

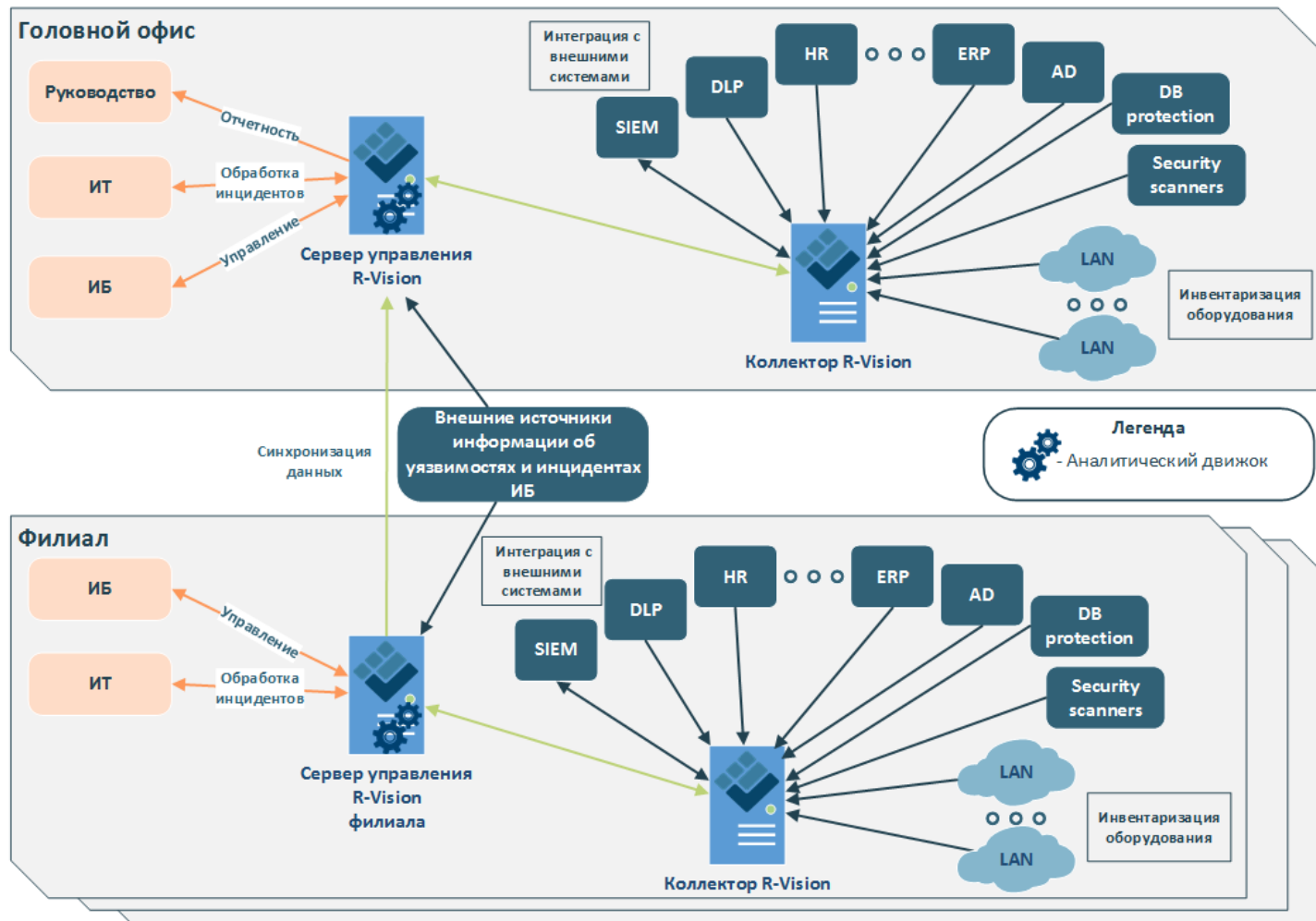
Изменить идентификаторы

Копировать

Закрыть

Поделиться

#11 Организация SOC на базе R-Vision IRP





R.Vision

At the root of your security