



SOAR+TI как способ компенсировать

возможности ушедшего
с российского рынка ПО



Иван Чувилин

Руководитель Presale

ichuvilin@rvision.ru

О чем будем говорить?

- Что сейчас происходит в ИБ
- Как действовать
- Реализованные кейсы на проектах:
проблемы со сканерами уязвимостей, СЗИ и SIEM.

Что случилось

Ушли либо приостановили деятельность в РФ:

- ✓ **SIEM**
MicroFocus (ArcSight SIEM), Fortinet (FortiSIEM), RSA NetWitness, IBM (Qradar SIEM), Rapid7 InsightIDR
- ✓ **Сканеры уязвимостей**
Qualys, Tenable (Nessus) , IBM (Qradar VM), F-Secure, Rapid 7 (Nexpose Vulnerability Scanner)
- ✓ **UBA**
Exabeam, модули в ArchSight, Qradar
- ✓ **Threat Deception**
TrapX, Illusive
- ✓ **SOAR**
Fortinet, PaloAlto, IBM, Micro Focus, Cisco NGFW, системы обнаружения вторжений, Anti-DDoS, антивирусы, песочницы и пр.
- ✓ **ITSM, CMDB**
Micro Focus, Ivanti, Atlassian (Jira)

Ужесточение требований на законодательном уровне:

- ✓ Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (исполнение до 1 января 2025 г)
- ✓ Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
- ✓ ФЗ от 14.07.2022 №266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»
- ✓ № 187-ФЗ «О безопасности КИИ РФ»
- ✓ законопроект об оборотных штрафах за утечку личных данных

С чего начать?

- Какие бизнес процессы есть в организации
- Из чего они состоят
- Какие риски к ним относятся
- Какие меры защиты уже внедрены



КЕЙС № 0

Управление активами

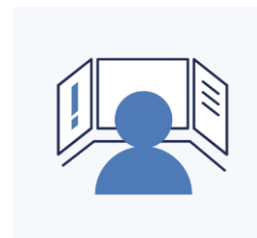
Кейс № 0 Проведите инвентаризацию активов



Внешние системы: AV, VM, SIEM, ITSM, CMDB



Инвентаризация R-Vision



Ручная настройка

Наименование	Владелец	Админист...	Критичность
ЦОД новосиби́рск			
Оборудование			
ИС оперативного учета нефти			
Автоматизированные системы управления			
АС вентиляции цеха УПЧ-4Н			
АС телемеханики цеха УПЧ-4Н			
Система автоматизации водоснабжения			
АСУ контроля работы нефтепровода			
ПАК "Приемо-передающая станция"	Мозгов Михаил (mmozgov@rvlab.net)	Семён Свиридов (admin)	
Корпоративная CRM система 019			
Системы Информационной Безопасности			
SAP системы	Александр Невский (anevsky@rvlab.net)	Семён Свиридов (admin)	
Юрьев Ю.Ю. (yuryevyu)			
Максим Комаров		Семён Свиридов	

Страница 1 из 1 | 50 | Отображаются записи с 1 по 39, всего 39

☒ АСУТП [Заполнить описание](#)

Владелец актива [\(контакты\)](#)
Мозгов Михаил (mmozgov@rvlab.net) x

Менеджер по контролю соответствия [\(контакты\)](#)
Александр Невский (anevsky@rvlab.net) x

Сведения о ежегодных затратах на сопровождение ИС
150 000 р

Администратор безопасности [\(контакты\)](#)
Семён Свиридов (admin) x

Категория конфиденциальности, обрабатываемая в системе
Коммерческая тайна x Инсайдерская информация x

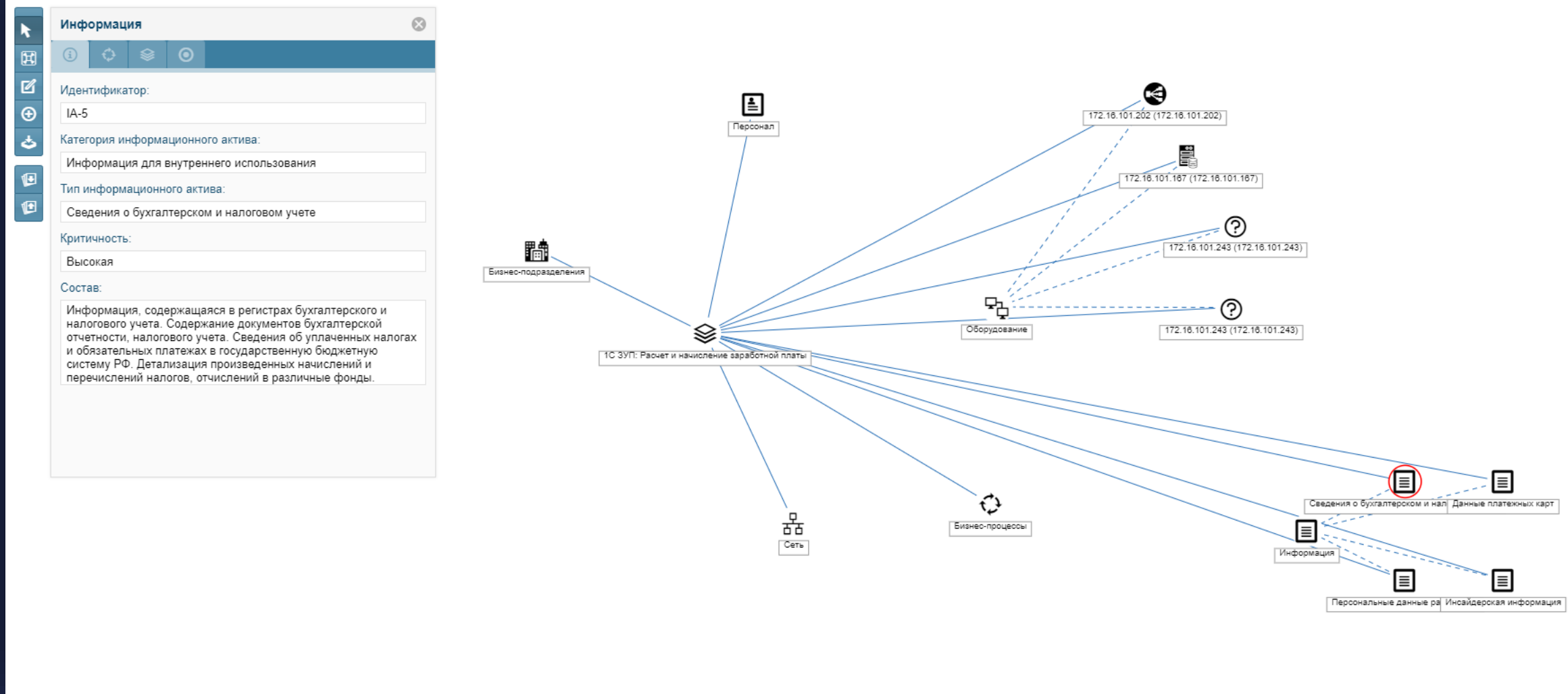
Связанные активы

Тип	Количество
Персонал	1 ⇌
Сети	3 ⇌
Хосты	6 ⇌
ПО	26 ⇌
Уязвимости	451 ⇌

Связанные инциденты

Уровень	Количество
---------	------------

Результат: CMBD для ИБ/ИТ, ресурсно-сервисная модель



Результат: CMBD для ИБ/ИТ, ресурсно-сервисная модель

КЕЙС № 1

Vulnerability Management

Сканер уязвимостей – альтернативы по качеству нет

- ✓ **Open Source**
необходимо настраивать и поддерживать самостоятельно, не хватает контекста
- ✓ **Отечественный сканер**
ложные срабатывания, слепые зоны, отсутствие приоритезации, качество продукта
- ✓ **Импортные решения из дружественных стран**
нет сертификата ФСТЭК, нет проектов и опыта использования

Решение

Процесс работы с уязвимостями на базе R-Vision SOAR + сканер:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ Приоритезация
- ✓ Автоматизированное управление

Управление уязвимостями: инвентаризация

R-Vision SOAR:

- ✓ список всех активов и полная, подробная информация по ним
- ✓ ресурсно-сервисная модель
- ✓ нет слепых зон

Управление уязвимостями: сканирование

Любой подходящий сканер:

- ✓ список уязвимостей
- ✓ оценка CVSS

Работа с уязвимостями на базе R-Vision SOAR + сканер:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ **Обогащение**
- ✓ Приоритезация
- ✓ Автоматизированное управление

R-TIP

Дашборд

Уведомления

Индикаторы

Аналитика

Обнаружения

Угрозы

Бюллетени

Автоматизация

Настройки

Свернуть

Уязвимости

admin

Поиск...

Точное совпадение

Фильтры

Источники	Имя	CVE	Вендоры	Базовая оцен...	Базовая оцен...	CWE
NVD Vulnerabilities	CVE-2015-6435	CVE-2015-6435	Cisco	10	9.8	CWE-78: Improper Neutralization of...
NVD Vulnerabilities	CVE-2014-3306	CVE-2014-3306	Cisco	10	N/A	CWE-20: Improper Input Validation
NVD Vulnerabilities	CVE-2016-10150	CVE-2016-10150	Linux	10	9.8	CWE-264
NVD Vulnerabilities	CVE-2004-0216	CVE-2004-0216	Microsoft	10	N/A	
NVD Vulnerabilities	CVE-2003-0819	CVE-2003-0819	Microsoft	10	N/A	CWE-119: Improper Restriction of...
NVD Vulnerabilities	CVE-2007-0213	CVE-2007-0213	Microsoft	10	N/A	CWE-20: Improper Input Validation
NVD Vulnerabilities	CVE-2007-0938	CVE-2007-0938	Microsoft	10	N/A	
NVD Vulnerabilities	CVE-2001-0538	CVE-2001-0538	Microsoft	10	N/A	
NVD Vulnerabilities	CVE-2010-0231	CVE-2010-0231	Microsoft	10	N/A	CWE-264
NVD Vulnerabilities	CVE-2019-15504	CVE-2019-15504	Linux	10	9.8	CWE-415: Double Free
NVD Vulnerabilities	CVE-2001-0500	CVE-2001-0500	Microsoft	10	N/A	
NVD Vulnerabilities	CVE-2004-1137	CVE-2004-1137	2 вендора	10	N/A	
NVD Vulnerabilities	CVE-2003-1357	CVE-2003-1357	2 вендора	10	N/A	CWE-16
2 источника	CVE-2021-34473	CVE-2021-34473	Microsoft	10	9.8	CWE-918: Server-Side Request...
NVD Vulnerabilities	CVE-2007-4747	CVE-2007-4747	Cisco	10	N/A	CWE-287: Improper

<<<1>>>

20

Таблица

CVE-2003-0819

Buffer overflow in the H.323 filter of Microsoft Internet Security and Acceleration Server 2000 allows remote attackers to execute arbitrary code in the Microsoft Firewall Service via certain H.323 traffic, as demonstrated by the NISCC/OUSPG PROTOS test suite for the H.225 protocol.

CVE

CVE-2003-0819

Опубликовал

cve@mitre.org

Источник

NVD Vulnerabilities

Создана

12:52:55 08 октября 2021

Изменена

11:36:10 10 февраля 2022

Опубликована

08:00:00 17 февраля 2004

Обновлена

00:33:00 13 октября 2018

Затронутые конфигурации ПО

Посмотреть содержимое

CWE

Improper Restriction of Operations within the Bounds of a Memory

CVSSv2.0

Базовая оценка

10

Оценка эксплуатируемости

10

Оценка влияния

10

+ Дополнительная информация

Работа с уязвимостями на базе R-Vision SOAR + сканер:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ **Приоритезация**
- ✓ Автоматизированное управление

R-Vision

АктивыИнцидентыУязвимостиМеры защитыАудит и контрольРискиЗадачиДокументыОтчеты...?1ichuvilin

⚙️★↺

Поиск...

Управление уязвимостями

Политики управления уязвимостями

Расчет рейтинга уязвимости

Управление инцидентами

Категории инцидентов

Типы инцидентов

Поля инцидентов

🔍 Справочники

Уровни критичности

Циклы обработки инцидентов

Сценарии реагирования

Коннекторы

Связи и корреляция

Представления

Шаблоны инцидентов

ГосСОПКА

Интеграция с внешними системами

Система защиты

Типы документов

Поля документов

🔍 Каталоги защитных мер

ОтменаСохранить

Формула расчета рейтинга уязвимости

(CVSS*0.55+ASSETCR*0.3+EXP*0.15)*VULSTATUS

ℹ️

Рейтинг уязвимости рассчитывается для каждой уязвимости на хосте. Рейтинг уязвимости рассчитывается на основе оценки CVSS, поэтому эту переменную нельзя удалить. Система работает с двумя версиями оценки CVSS: V2 и V3. По умолчанию используется CVSS V3, если для уязвимости доступны обе оценки. В остальных случаях используется CVSS V2. Для расчета рейтинга могут использоваться поля Уязвимости и поля с типом Справочник или Чек-бокс активов Оборудование, Группы ИТ-активов. После добавления в формулу каждому значению поля нужно задать коэффициент, который будет заменять текстовое значение поля при расчете.

Переменные

ДобавитьУдалить

ID	Наименование
ASSETCR	Группа ИТ-активов: Критичность
CVSS	Уязвимости: Оценка CVSS
VULSTATUS	Уязвимости: Статус
EXP	Наличие эксплойта

Поле актива

Группы ИТ-активов: Критичность

ID

ASSETCR

Наименование

Группа ИТ-активов: Критичность

Список значений :

Значение	Коэффициент
Низкая	7✎
Критическая	10✎
Высокая	9✎
Средняя	8✎

Сохранить

Рейтинг уязвимостей в R-Vision SOAR

Работа с уязвимостями на базе R-Vision SOAR + сканер:

- ✓ Инвентаризация
- ✓ Сканирование
- ✓ Обогащение
- ✓ Приоритезация
- ✓ Автоматизированное управление

R-Vision

АктивыИнцидентыУязвимостиМеры защитыАудит и контрольРискиЗадачиДокументыОтчеты...

УязвимостиОбновления

ЭксплойтЭффективный эксплойт, Широко распространен/Не требуетсяИРейтингБольше 8

Название	Имя устройства	Уровень	Рейтинг	CVSS V2 ↑	Эксплойт	Статус	Вектор V2		Основное	Детали	Оборудование
Microsoft CVE-2020-17...	REDCHECK01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	ID NP-msft-cve-2019-0543		
Microsoft CVE-2020-06...	SEP01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Организация		
Centos Linux: CVE-201...	nessus02		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Министерство информационных технологий		
Microsoft CVE-2019-05...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Рейтинг		
Microsoft CVE-2019-07...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	8.3		
Microsoft CVE-2018-07...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Ложное срабатывание		
Microsoft CVE-2018-85...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Принять риск		
Microsoft CVE-2018-07...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Создать задачу		
Microsoft CVE-2020-06...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	Создать инцидент	19-0543: Microsoft Windows Elevation of Privilege Vulnerability	
Microsoft CVE-2019-07...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	CVSS V2	Вектор	
Microsoft CVE-2019-08...	WIN7X64RU01		8.3	4.6	Эффективный эксплойт	Открыта	AV:L/AC:L/Au:N/...	7	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	
									CVSS V3	Вектор	
									7.8	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F	
									Наличие эксплойта		
									Эффективный эксплойт		
									Статус		
									Открыта		
									Дата обнаружения [UTC+03:00]		
									09.09.2021 13:23:02		
									Источник		

Страница 1 из 450

Автоматизация управления в R-Vision SOAR



Алгоритм принятия решения по обновлению критичного ПО от НКЦКИ

КЕЙС № 2
Blacklist на СЗИ

TIP как база для обогащения

Что произошло:

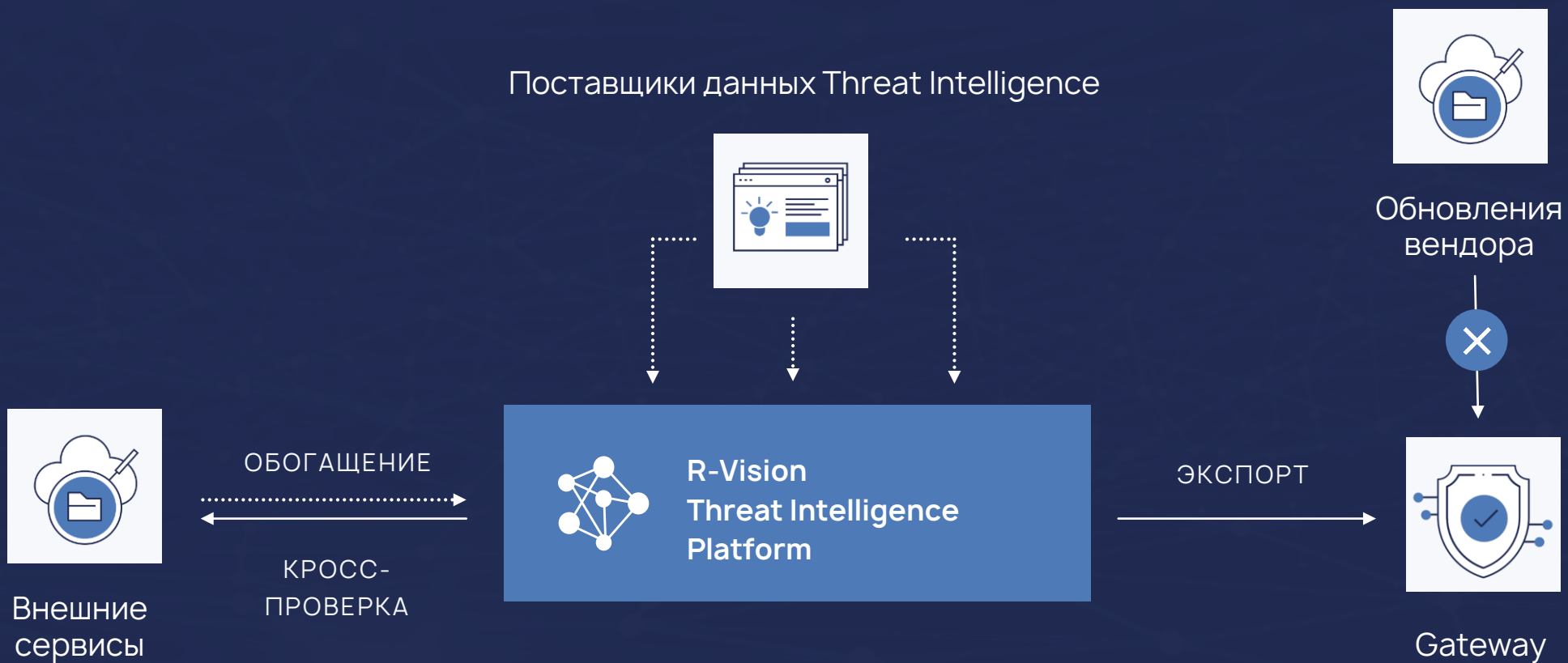
- ✗ Вендор отключил доступ к фидам и индикаторам в одностороннем порядке
- ✗ Gateway работает, но не защищает от новых угроз. Нет обновлений

TIP как база для обогащения

Решение:

-  Сделали экспорт в СЗИ в список правил запрета те индикаторы, которые имеют высокий рейтинг

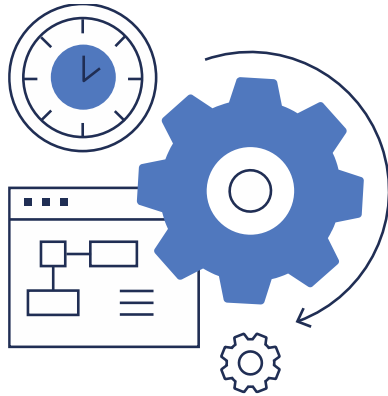
Решение



КЕЙС № 3

SIEM: заменить нельзя оставить

Спешить с заменой SIEM не обязательно



- ✓ Срочное обновление продукта не требуется, система работает – есть время все взвешенно обдумать
- ✓ Но хочется перестраховаться на случай, если с решением пойдет что-то не так

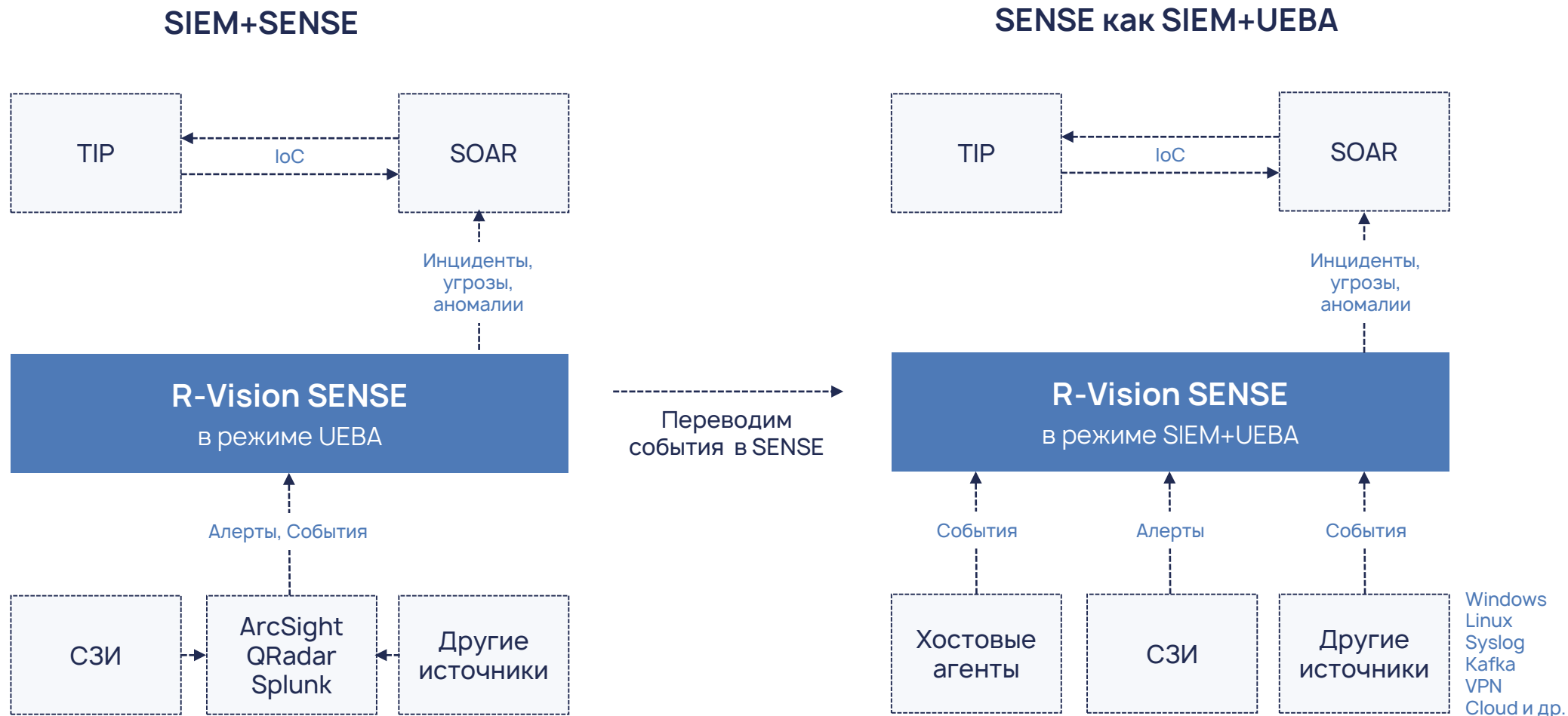
Решение



- ✓ Мы поставили R-Vision SENSE как UEBA:
снижаем false-positive, даем дополнительные инструменты анализа для более качественного детекта и выявления аномалий
- ✓ В нужный момент поток событий заворачивается напрямую в SENSE
- ✓ При этом правила переносятся, и система переходит в режим работы «SIEM + UEBA»

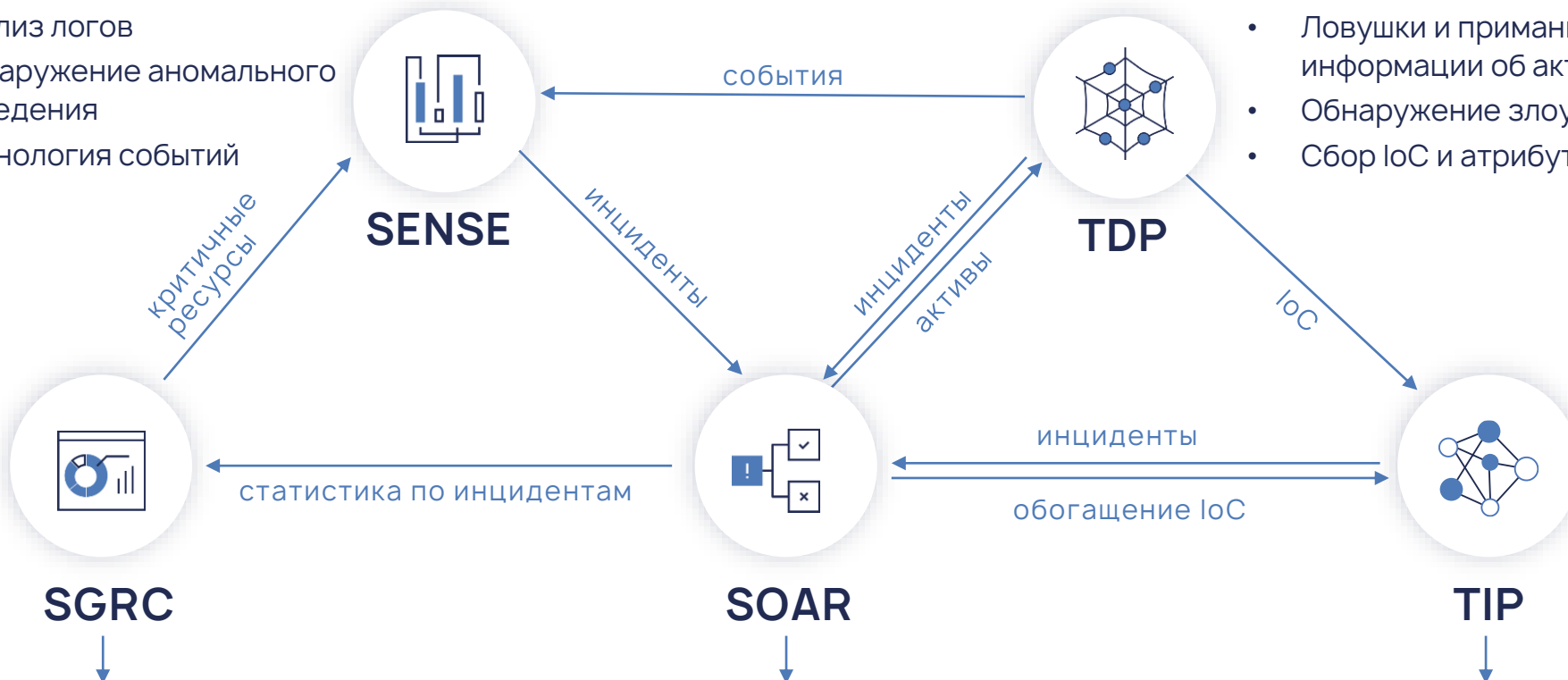
До 2025 года есть время на закупку расширенной лицензии и миграцию в R-Vision SENSE полностью

Схема работы SIEM+SENSE+SOAR



Экосистема R-Vision

- Анализ логов
- Обнаружение аномального поведения
- Хронология событий



- Ловушки и приманки на основе информации об активах
- Обнаружение злоумышленника
- Сбор IoC и атрибутов атакующего

- Полная картина ИБ
- Управление ИТ-активами
- Аудиты с ретроспективой
- Риски с учётом инцидентов

- Оркестрация, автоматизация ИБ
- Управление ИТ-активами
- Единое рабочее пространство для команды SOC
- Взаимодействие с регуляторами

- Агрегация всех данных TI
- Поиск IoC в инфраструктуре
- Экспорт IoC на СЗИ

R-Vision

 + 7 (499) 322 80 40

 sales@rvision.ru

 rvision.ru

Подписывайтесь на наш бесплатный
дайджест ИБ: rvision.ru/blog