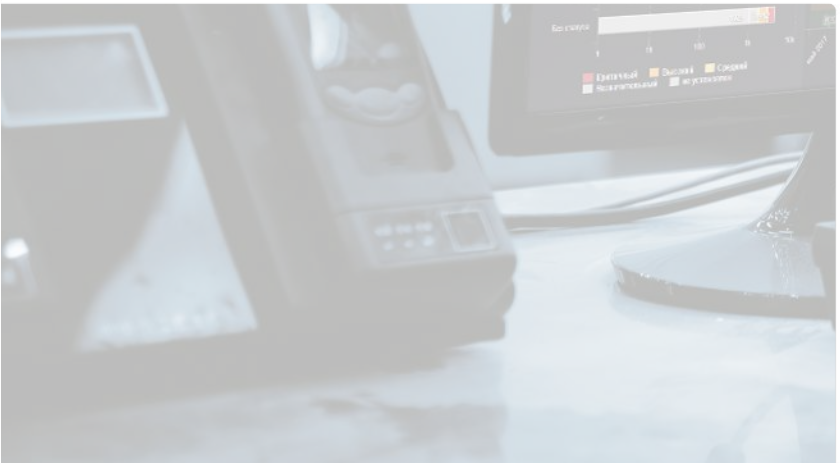
SOC·FORUM

R-Vision

ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И ИСПОЛЬЗОВАНИЕ ДАННЫХ КИБЕРРАЗВЕДКИ В ПРАКТИКЕ SOC



Сметанев Игорь
Коммерческий директор R-Vision
smetanev@rvision.pro

С ЧЕМ СТАЛКИВАЕТСЯ СРЕДНЕСТАТИСТИЧЕСКИЙ РУКОВОДИТЕЛЬ SOC?

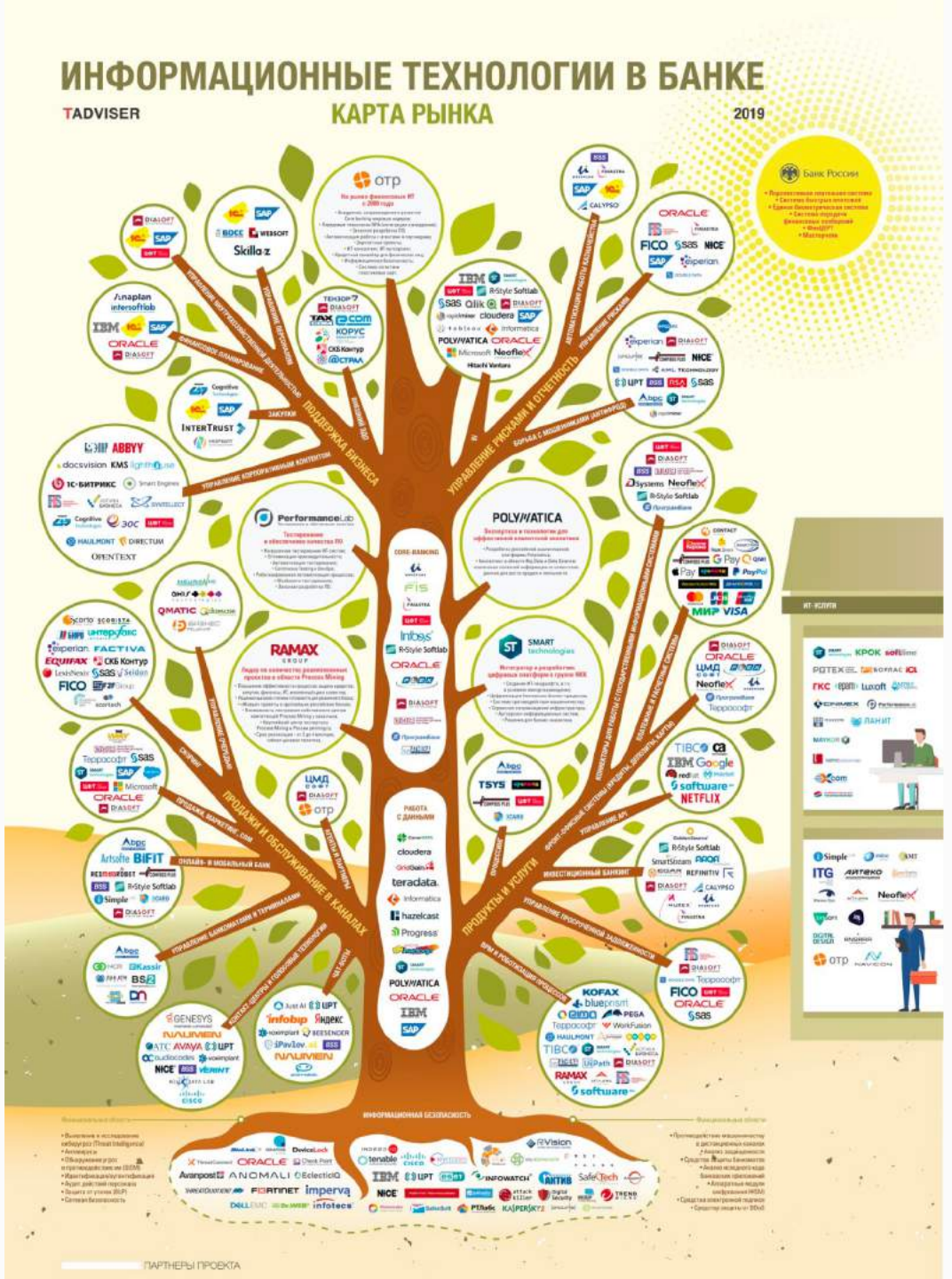
НЕ ХВАТАЕТ ЛЮДЕЙ


Руководитель SOC
Линия 1
- Колл-центр
- Мониторинг и приоритизация в реальном времени
- Сбор, анализ и распространение кибер-новостей
Линия 2+
- Анализ инцидентов
- Координация и реагирование на инциденты
- Обработка и анализ артефактов расследования
- Анализ закладок и вредоносного ПО
- Анализ данных разведки
- Поддержка в расследовании внутренних угроз
Тренды и данные разведки
- Сбор, анализ, распространение и создание кибер-новостей
- Анализ трендов
- Оценка угроз
- Анализ данных разведки
Системный администратор SOC
- Эксплуатация и сопровождение инфрструктуры SOC
- Настройка и поддержка сенсоров
- Создание пользовательских сигнатур
- Скрипты и автоматизация
- Сбор и хранение данных аудита
Разработка SOC
- Разработка и развертывание инструментов
- Скрипты и автоматизация

«ЗООПАРК» СРЕДСТВ ЗАЩИТЫ

SIEM	1	SGRC	5	Anti-APT	9						
DLP	2	WAF	6	Anti-DDoS	10	SSO	4a				
PKI	3	Анализ кода	7	EDR	11	PUM	8a				
IDM	4	СКЗИ	8	UTM	12	AntiVirus	13				

ТЕХНОЛОГИИ ИСПОЛЬЗУЕМЫЕ В БАНКАХ



ИНЦИДЕНТОВ ВСЕ БОЛЬШЕ

Громкие инциденты ИБ

АПРЕЛЬ 2019

- Toyota объявила о возможной краже личных данных 3,1 млн клиентов хакерами. Дилерские компании сообщили о несанкционированном доступе к своим серверам. Факт утечки сведений клиентов пока не подтвержден, Toyota проводит расследование.
- Пользователи сервисов Gmail, Netflix и PayPal в Бразилии столкнулись с атаками со стороны хакеров, которые используют методику под названием «перехват DNS» (DNS hijacking). В период с декабря 2018 года и по март 2019 прошло три волны подобных атак. Четвертая волна началась 5 апреля 2019 года. В ходе акций злоумышленники крадут данные пользователей, которые те вводят на ложных сайтах.
- База данных, содержащая данные примерно о 360 000 вызовах, которые поступили подмосковным службам скорой помощи, выложены в открытом доступе на одном из интернет-сайтов. Доступ к этой базе бесплатный, данные хранятся в кодированном, но не зашифрованном виде.
- Хакеры украли криптовалюту пользователей кошелька Electrum на миллионы долларов, сейчас система находится под DoS-атакой, ее ведут 140 тыс. ботов, пишет The Next Web. Разработчики проекта рассказали, что клиентов сервиса перенаправляет на скомпрометированные версии ПО, которые моментально похищают их средства.
- Пользователи Facebook вновь пострадали от утечки данных. На этот раз информацию о 540 млн пользователей обнаружили на облачных серверах Amazon. По словам аналитиков компании UpGuard, нашедших утечку, данные были собраны в социальной сети сторонними компаниями.
- Фармацевтический концерн Bayer на протяжении года подвергался атакам со стороны хакеров. Вредоносное программное обеспечение находилось в системе Bayer как минимум до конца марта этого года. Специалисты считают, что за кибератакой стоит хакерская группа Winnti.

Источник: дайджест R-Vision

ИНЦИДЕНТЫ ИБ, ТРЕБУЮЩИЕ РЕАГИРОВАНИЯ

ПРИМЕРЫ ТИПОВ ИНЦИДЕНТОВ

ВНЕШНИЕ АТАКИ/ ВТОРЖЕНИЯ (DDOS, ДР.)

- Выявления атак типа «отказ в обслуживании»
- Выявления попыток осуществления вторжений и сетевых атак
- Ошибки в логике работы IPS

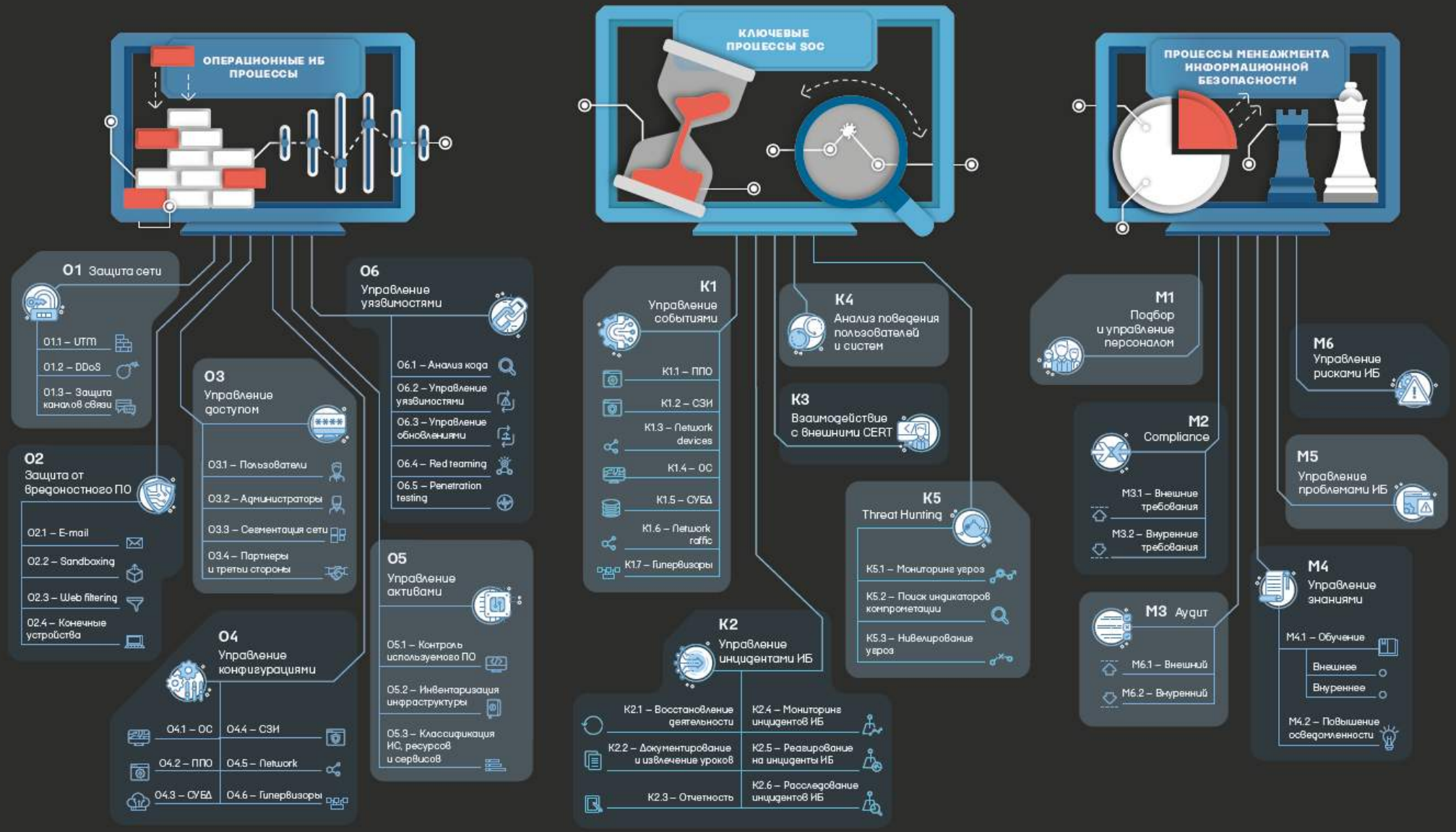
КОМПРОМЕТАЦИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ, ПЕРСОНАЛЬНЫХ ИДЕНТИФИКАТОРОВ, ПАРОЛЕЙ

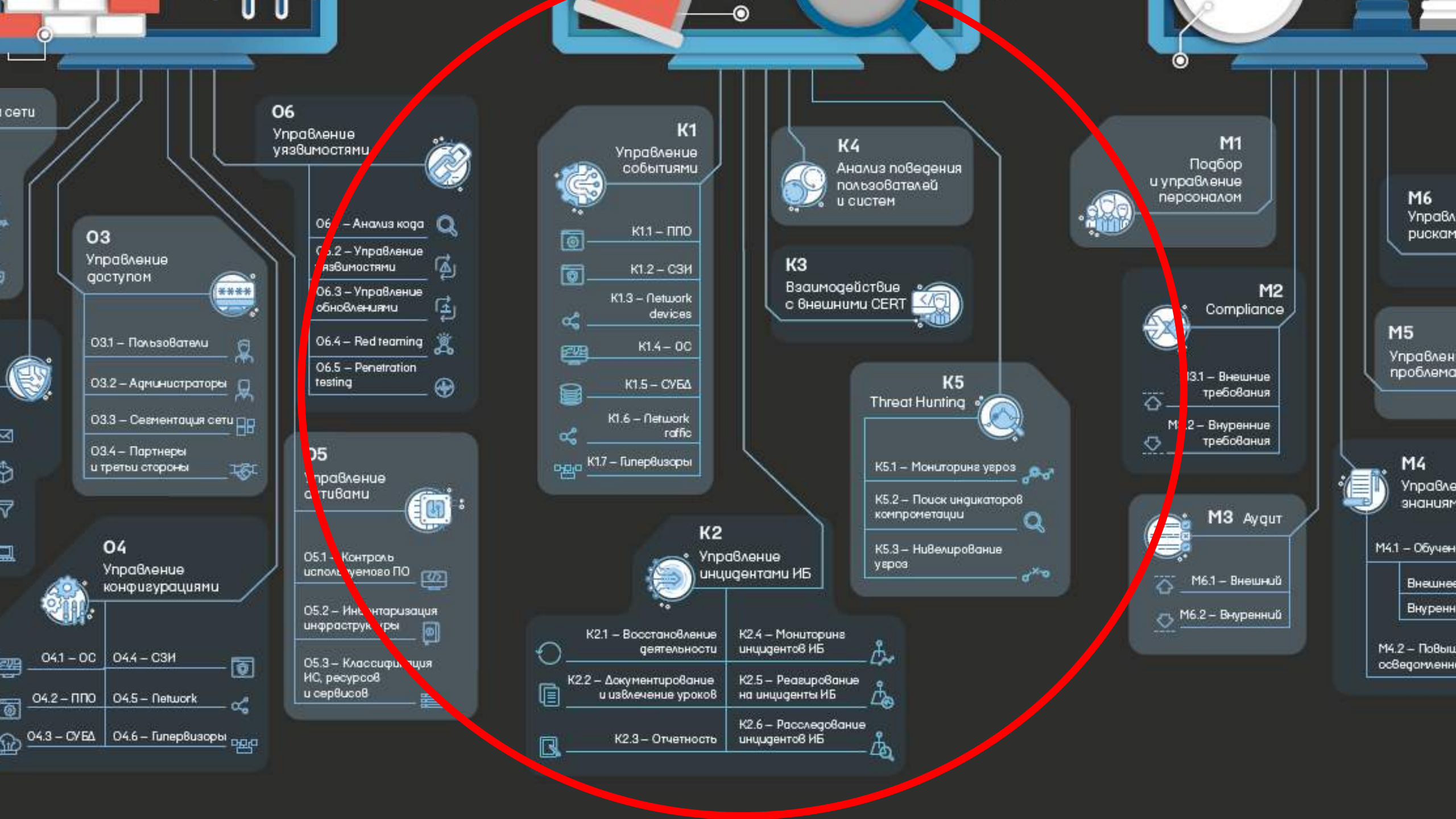
- Компрометация ключа ЭП работника Организации
- Несанкционированное создание, удаление, блокировка, разблокировка учетных записей
- Утрата работником персонального идентификатора (ТМ, Smart-карт)
- Передача другим лицам пользовательских идентификаторов и паролей

СБОИ В РАБОТЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АИС

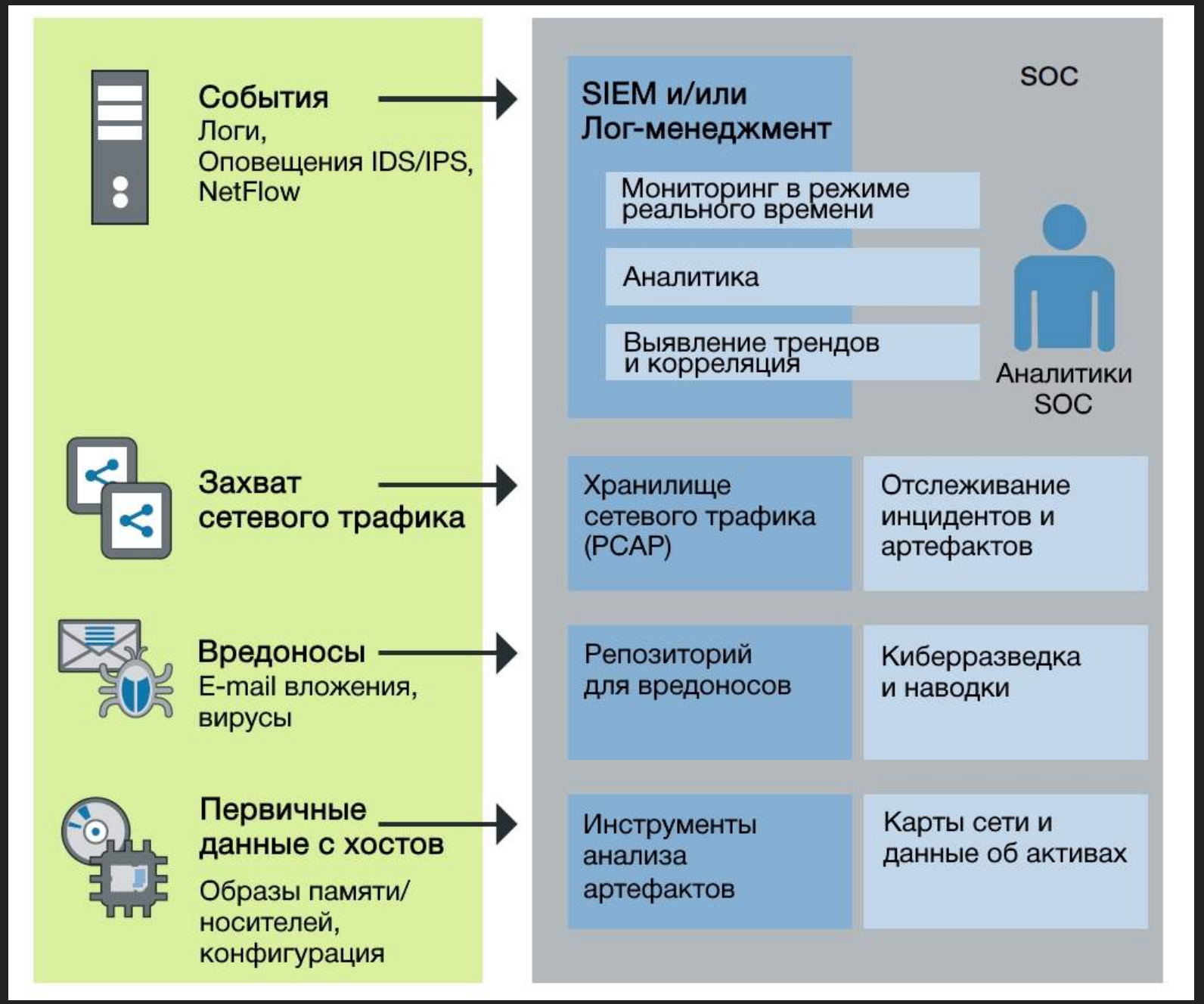
- Недоступность критичных систем
- Выявленные уязвимости в информационных системах
- Несанкционированное изменение ПО АРМ пользователей
- Несанкционированный запуск программных процессов

НАСТРОЙКА ПРОЦЕССОВ

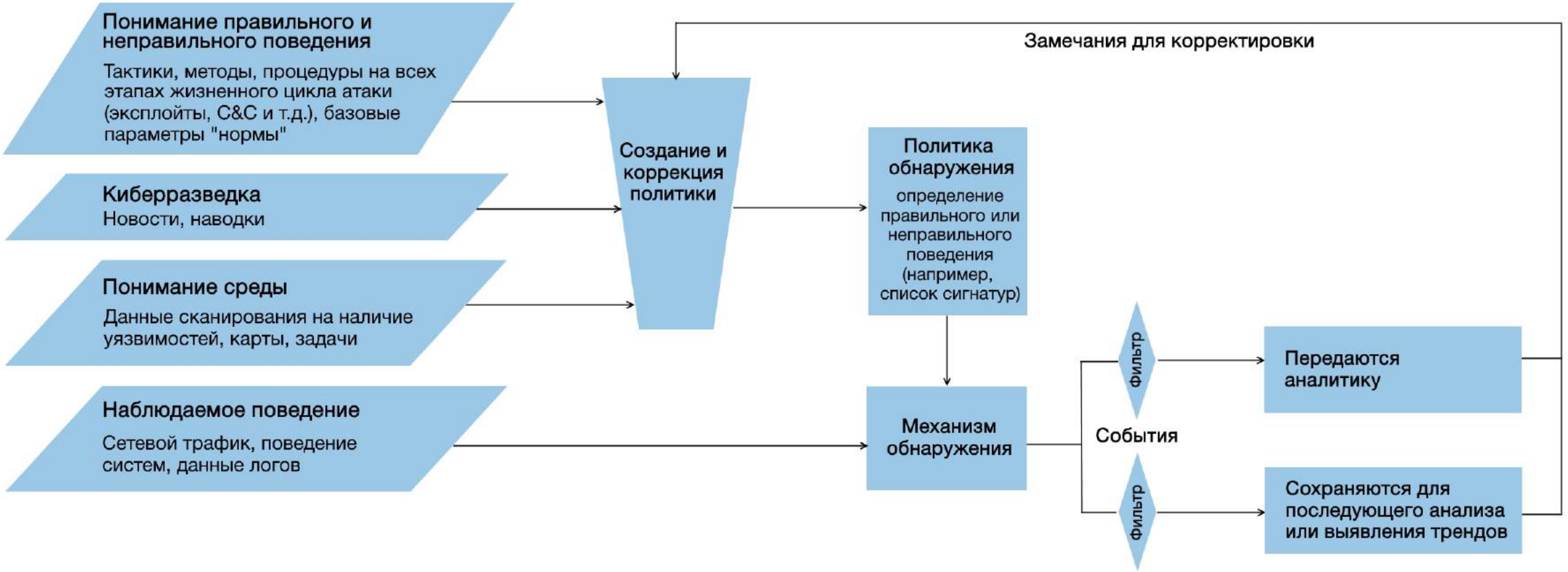



О6
Управление уязвимостями
О6.1 – Анализ кода
О6.2 – Управление уязвимостями
О6.3 – Управление обновлениями
О6.4 – Red teaming
О6.5 – Penetration testing
О3
Управление доступом
О3.1 – Пользователи
О3.2 – Администраторы
О3.3 – Сегментация сети
О3.4 – Партнеры и третьи стороны
О5
Управление активами
О5.1 – Контроль используемого ПО
О5.2 – Инвентаризация инфраструктуры
О5.3 – Классификация ИС, ресурсов и сервисов
О4
Управление конфигурациями
О4.1 – ОС
О4.4 – СЗИ
О4.2 – ППО
О4.5 – Network
О4.3 – СУБД
О4.6 – Гипервизоры
К1
Управление событиями
К1.1 – ППО
К1.2 – СЗИ
К1.3 – Network devices
К1.4 – ОС
К1.5 – СУБД
К1.6 – Network raffic
К1.7 – Гипервизоры
К4
Анализ поведения пользователей и систем
К3
Взаимодействие с внешними CERT
К5
Threat Hunting
К5.1 – Мониторинг угроз
К5.2 – Поиск индикаторов компрометации
К5.3 – Нивелирование угроз
К2
Управление инцидентами ИБ
К2.1 – Восстановление деятельности
К2.4 – Мониторинг инцидентов ИБ
К2.2 – Документирование и извлечение уроков
К2.5 – Реагирование на инциденты ИБ
К2.3 – Отчетность
К2.6 – Расследование инцидентов ИБ
М1
Подбор и управление персоналом
М2
Compliance
М3.1 – Внешние требования
М3.2 – Внуренние требования
М3 Аудит
М6.1 – Внешний
М6.2 – Внуренний
М6
Управл
рискам
М5
Управлен
проблема
М4
Управле
знаниям
М4.1 – Обучен
Внешнее
Внуренн
М4.2 – Повыш
осведомленн

1. ИНСТРУМЕНТЫ И КАЧЕСТВО ДАННЫХ


SOC
SIEM и/или
Лог-менеджмент
Мониторинг в режиме реального времени
Аналитика
Выявление трендов и корреляция
Аналитики SOC
События
Логи,
Оповещения IDS/IPS,
NetFlow
Захват
сетевого трафика
Хранилище сетевого трафика (PCAP)
Отслеживание инцидентов и артефактов
Вредоносы
E-mail вложения,
вирусы
Репозиторий для вредоносов
Кибеpразведка и наводки
Первичные
данные с хостов
Образы памяти/
носителей,
конфигурация
Инструменты анализа артефактов
Карты сети и данные об активах

НУЖНЫЕ ДАННЫЕ
В НУЖНОЕ ВРЕМЯ
В НУЖНОМ КОНТЕКСТЕ


Понимание правильного и неправильного поведения
Тактики, методы, процедуры на всех этапах жизненного цикла атаки (эксплойты, C&C и т.д.), базовые параметры "нормы"
Киберразведка
Новости, наводки
Понимание среды
Данные сканирования на наличие уязвимостей, карты, задачи
Наблюдаемое поведение
Сетевой трафик, поведение систем, данные логов
Создание и коррекция политики
Замечания для корректировки
Политика обнаружения
определение правильного или неправильного поведения (например, список сигнатур)
Механизм обнаружения
Фильтр
Фильтр
События
Передаются аналитику
Сохраняются для последующего анализа или выявления трендов

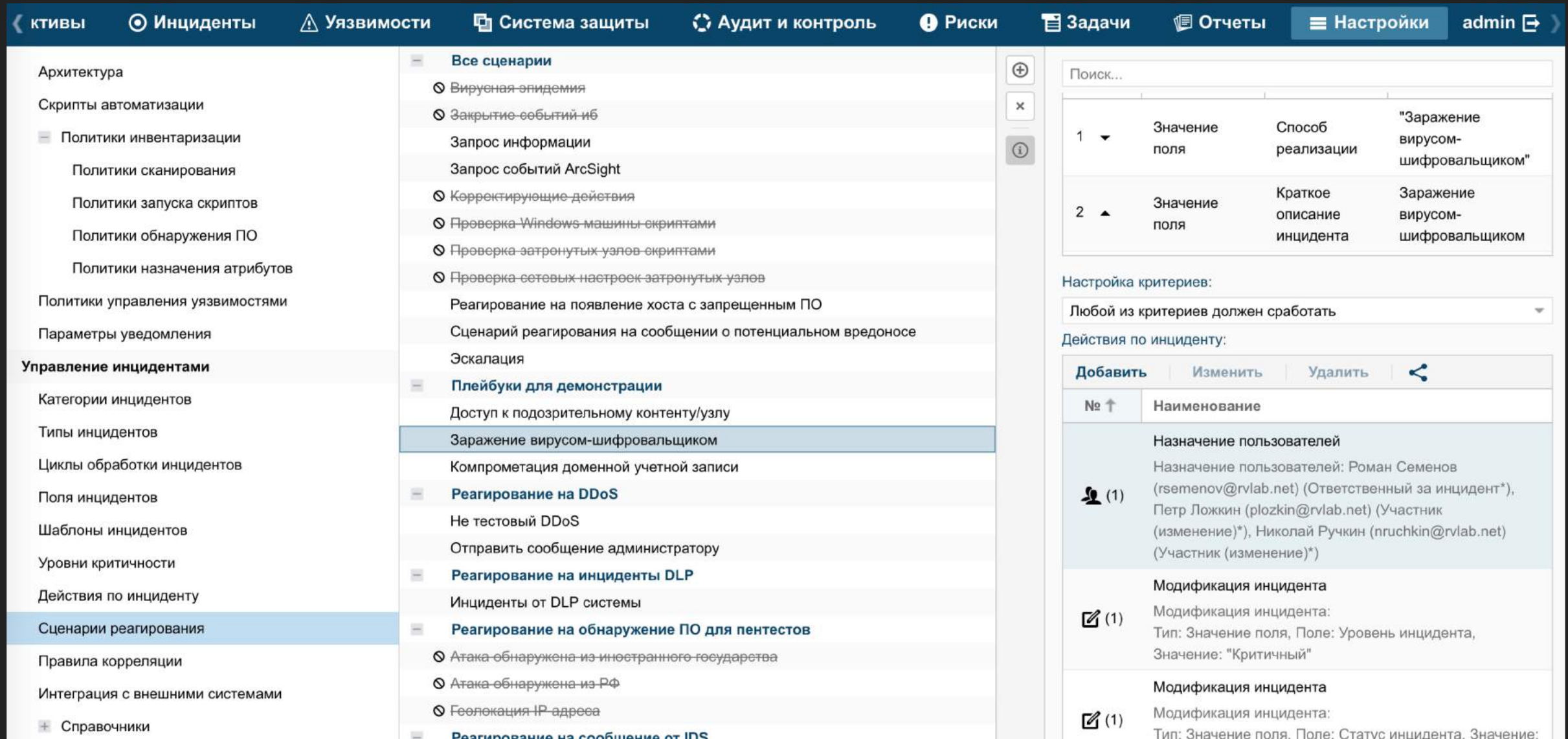
3 ключевых препятствия к повышению производительности и эффективности SOC

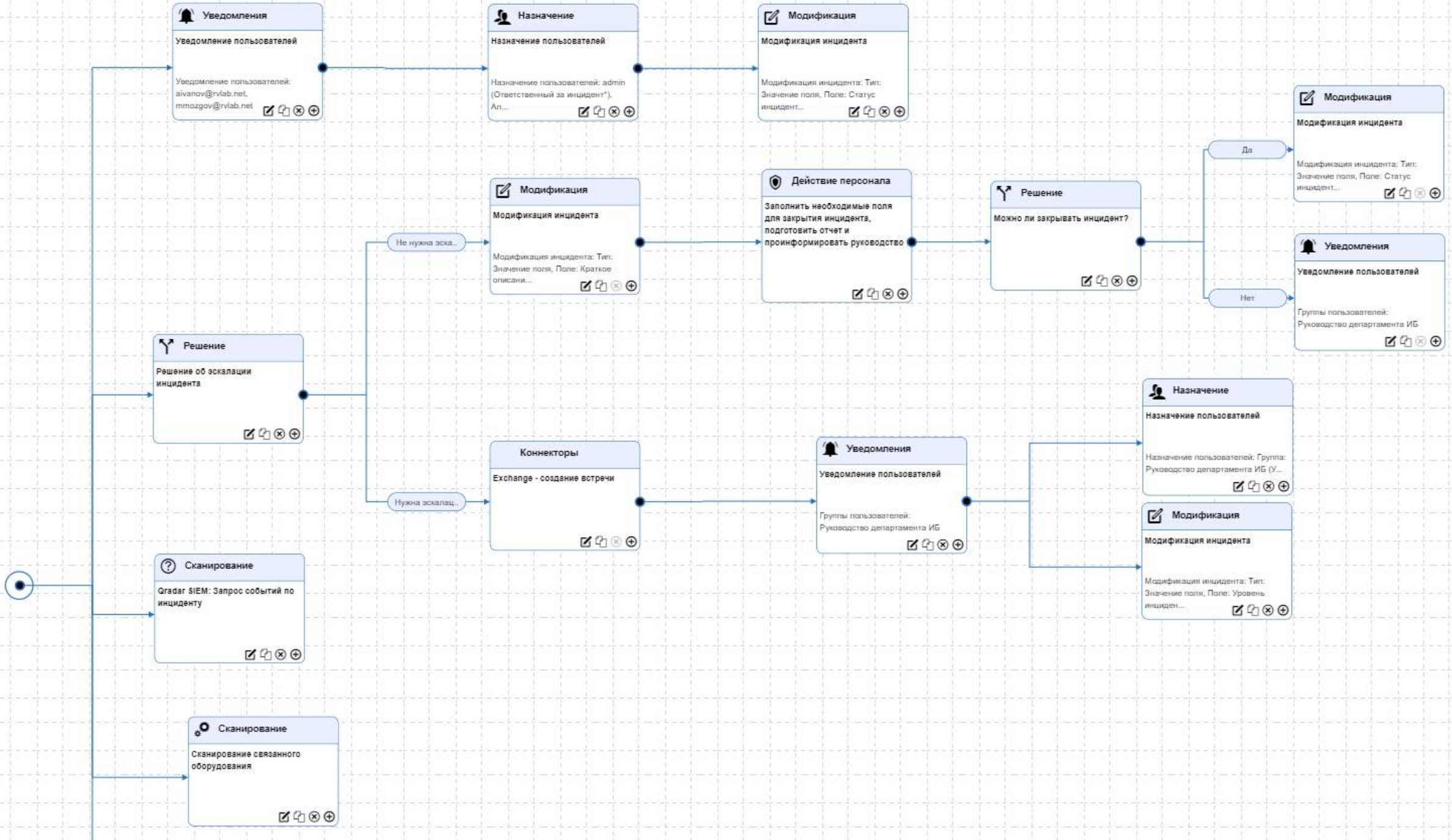
- Отсутствие высококлассных специалистов — отметили 62% респондентов
- Отсутствие метрик. Лишь 54% респондентов собирают метрики, при этом большинство метрик количественные, не имеющие прямого отношения к эффективности бизнеса. С непонятными (или отсутствующими) метриками сложнее убедить руководство, почему необходимо продолжать финансировать SOC и тратить бюджет на персонал и повышение его квалификации
- Отсутствие инструментов автоматизации/оркестрации, интеграции средств и процессов/сценариев отмечают 53% опрошенных

https://www.sans.org/reading-room/whitepapers/analyst/membership/38570

2. ОРКЕСТРАЦИЯ И АВТОМАТИЗАЦИЯ

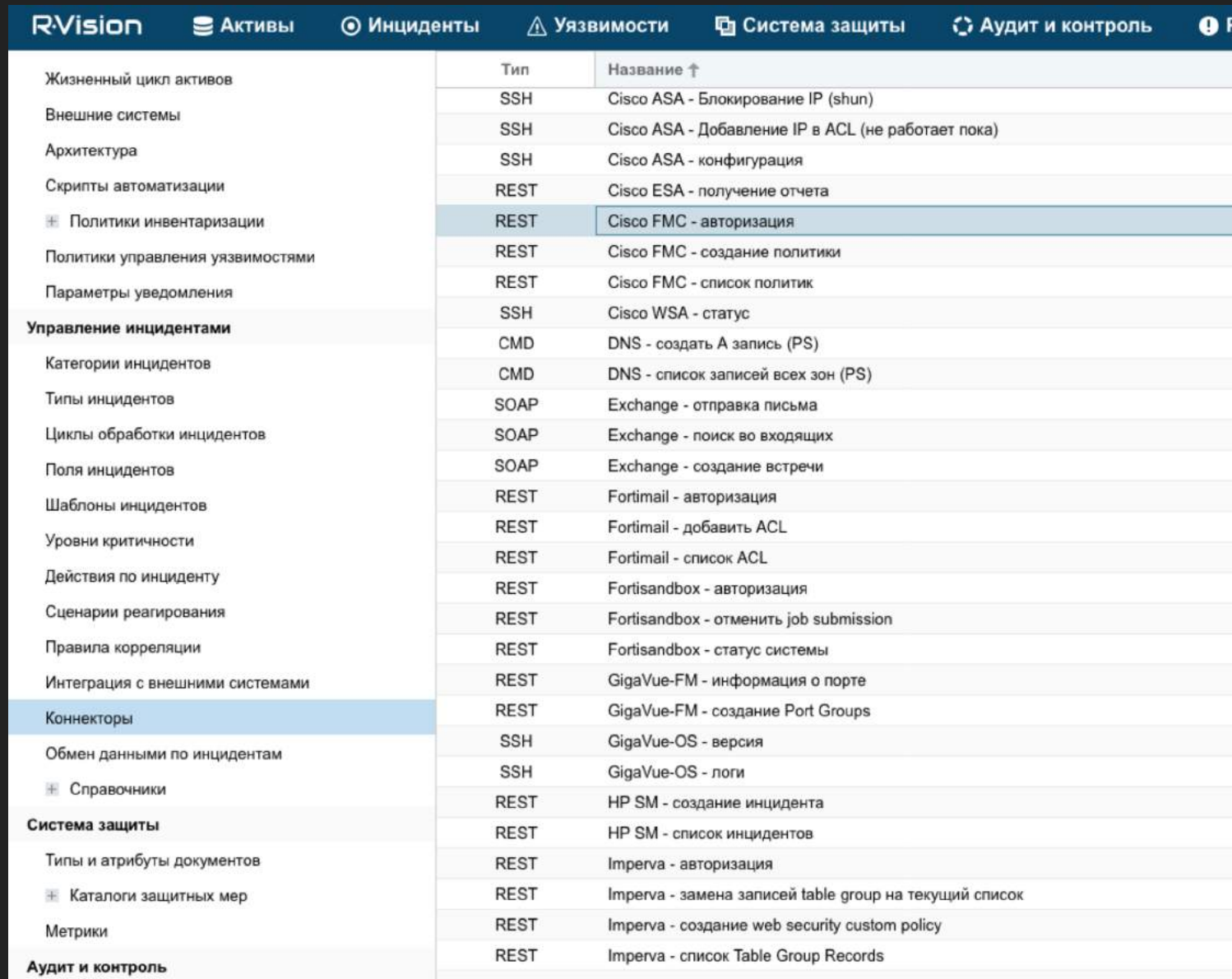
СЦЕНАРИИ ОБРАБОТКИ ИНЦИДЕНТОВ



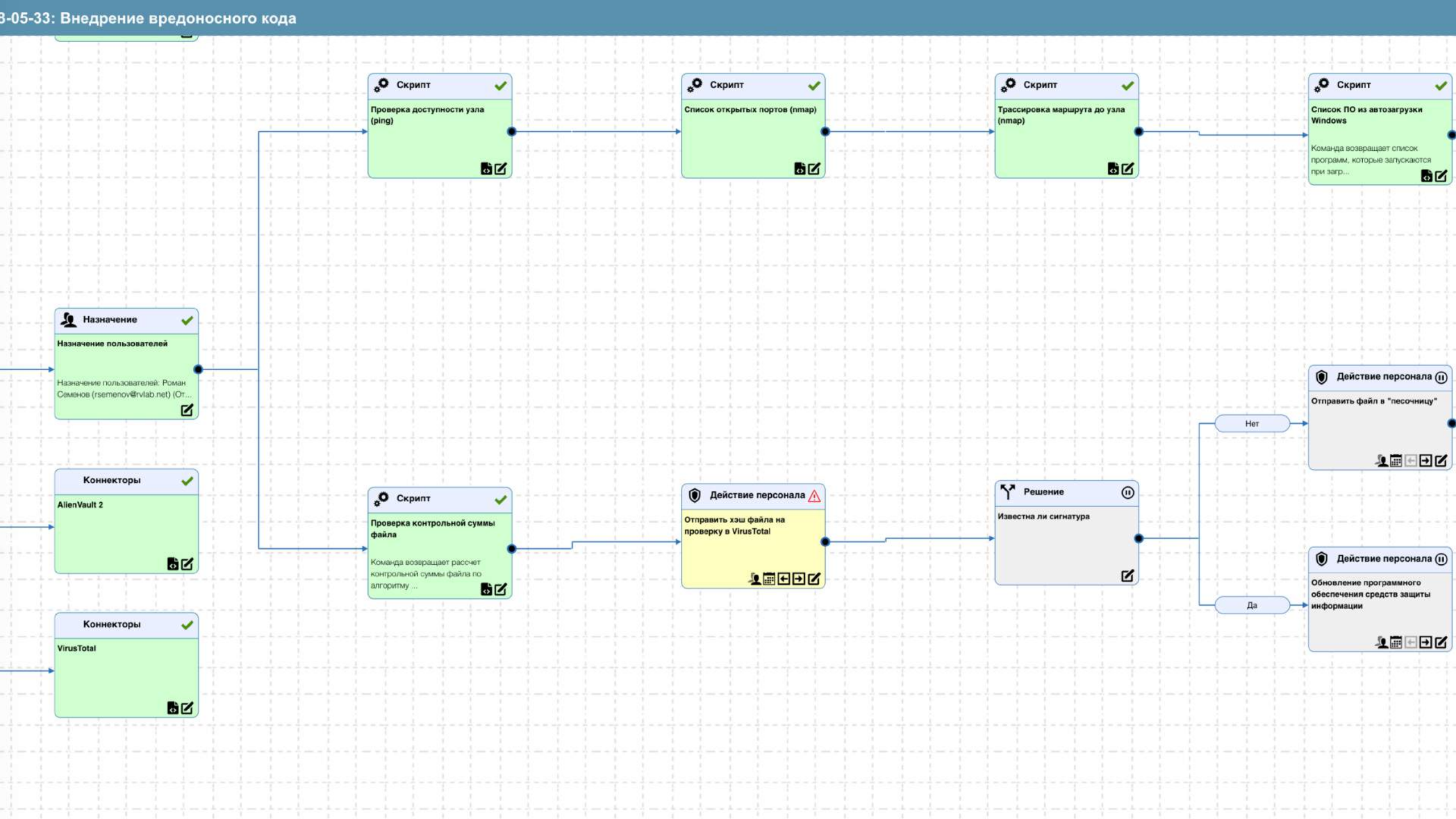

Уведомления
Уведомление пользователей
Уведомление пользователей: aivanov@rvlab.net, mmozgov@rvlab.net
Назначение
Назначение пользователей
Назначение пользователей: admin (Ответственный за инцидент*), An...
Модификация
Модификация инцидента
Модификация инцидента: Тип: Значение поля, Поле: Статус инцидент...
Модификация
Модификация инцидента
Модификация инцидента: Тип: Значение поля, Поле: Статус инцидент...
Да
Нет
Действие персонала
Заполнить необходимые поля для закрытия инцидента, подготовить отчет и проинформировать руководство
Решение
Можно ли закрывать инцидент?
Уведомления
Уведомление пользователей
Группы пользователей: Руководство департамента ИБ
Не нужна эска...
Модификация
Модификация инцидента
Модификация инцидента: Тип: Значение поля, Поле: Краткое описани...
Решение
Решение об эскалации инцидента
Нужна эскалац...
Коннекторы
Exchange - создание встречи
Уведомления
Уведомление пользователей
Группы пользователей: Руководство департамента ИБ
Назначение
Назначение пользователей
Назначение пользователей: Группа: Руководство департамента ИБ (У...
Модификация
Модификация инцидента
Модификация инцидента: Тип: Значение поля, Поле: Уровень инциден...
Сканирование
Qradar SIEM: Запрос событий по инциденту
Сканирование
Сканирование связанного оборудования

Запуск коннектора

- LDAP
- SSH
- SOAP
- REST
- CMD
- Power Shell
- SNMP
- MS SQL / PostgreSQL
- MySQL / Oracle
- Bash, Java / JavaScript
- Python, SMB
- WMI



8-05-33: Внедрение вредоносного кода



3. ВАЖНО ИСПОЛЬЗОВАТЬ ДАННЫЕ THREAT INTELLIGENCE В SOC

Если не использовать данные кибербразведки?

- Мониторинг SOC ни на чем не фокусируется и не улучшается
- SOC не успевает реагировать на изменения в ландшафте угроз
- SOC не воспринимается клиентами как ресурс для ситуационной осведомленности
- В инструментах мониторинга неэффективно используются TTP и индикаторы из доступных источников данных кибербразведки и, следовательно, они не соответствуют текущему уровню угроз и уязвимостей

ОБРАБОТКА THREAT INTELLIGENCE

Сбор
из разных источников

Обнаружение
индикаторов компрометации внутри инфраструктуры

Обработка
нормализация данных, связывание

Распространение
на средства защиты для мониторинга и блокировки

Обогащение
информацией из внешних систем

Автоматизация
сценариев использования индикаторов

СХЕМА РАБОТЫ
THREAT INTELLIGENCE PLATFORM

РЕЗУЛЬТАТ

Упрощается работа с данными TI
осуществляя непрерывный сбор, нормализацию и хранение данных из различных источников в единой базе

Облегчается выявление скрытых угроз
обеспечивая автоматический мониторинг релевантных индикаторов в SIEM, syslog и DNS-запросах

Ускоряет процессы ИБ
за счет быстрого поиска информации в доступных источниках и автоматизации ключевых сценариев

Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб

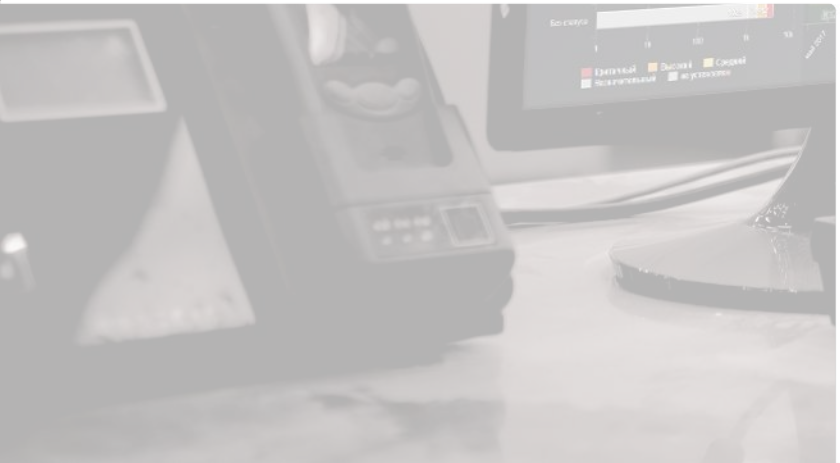
АТОМАТИЗАЦИЯ И ОРКЕСТРАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SOC·FORUM

R·Vision

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

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



8 (800) 350 77 57 ■ sales@rvision.pro ■ www.rvision.pro