UserGate

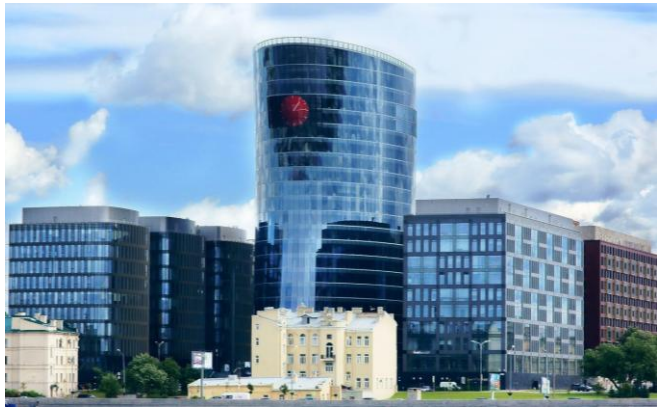
Современная SIEM-система на примере UserGate SIEM

Алексей Афанасьев
Менеджер по развитию
UserGate SIEM

Мы в Telegram

О КОМПАНИИ USERGATE

Основной офис разработки в Технопарке Новосибирского Академгородка



Офис разработки и сопровождения в Санкт-Петербурге

Фронт-офис в Москве, БЦ «ФилиГрад»

+ Минск

+ Томск

+ Хабаровск

25 лет
на ИБ-рынке России

600+ человек
в команде, и мы растем

70% штата
занимаются продуктами

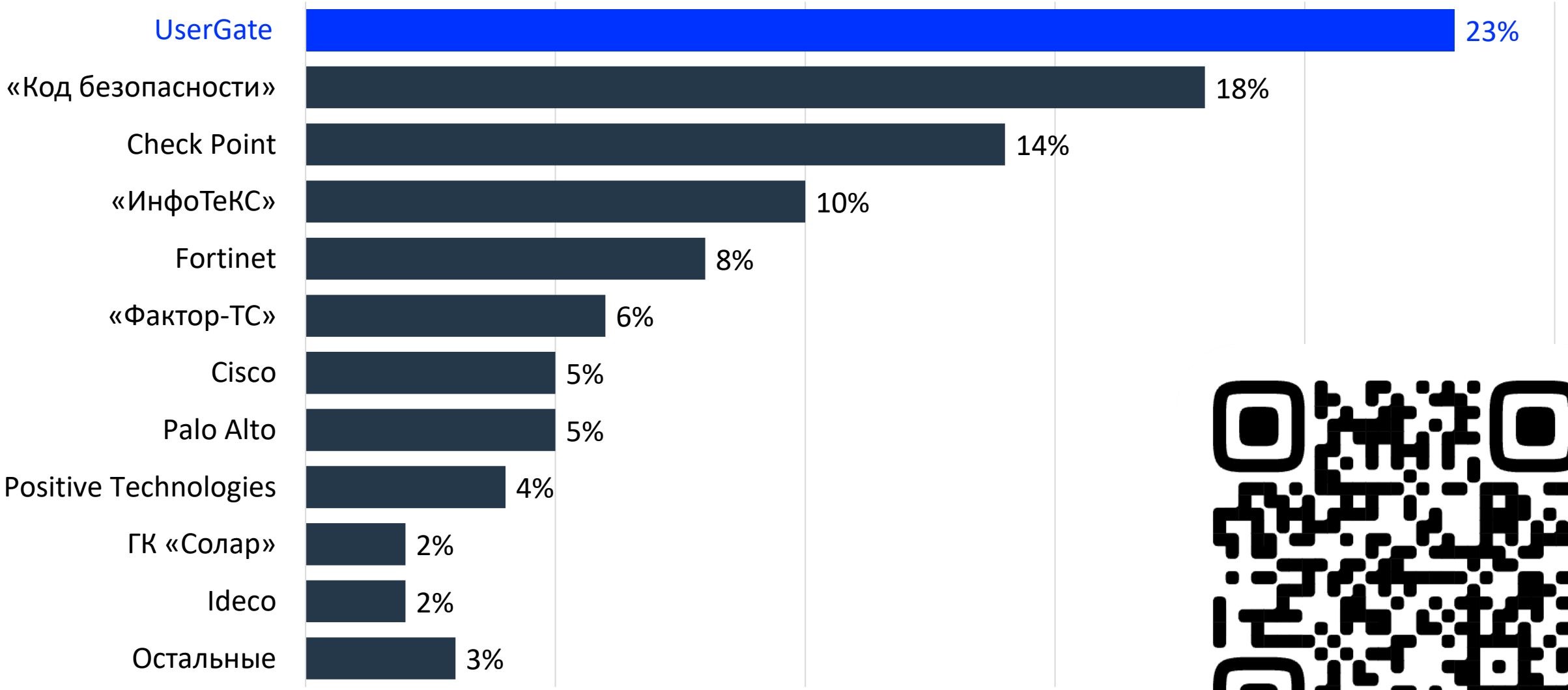
SOC
и ИБ-услуги

500+ партнеров
вендорская модель бизнеса

7 продуктов: NGFW +
DCFW, WAF, Client, SIEM, LogAn, MC

№1 по NGFW
в России, ЦСР, 2025

USERGATE – ЛИДЕР РЫНКА NGFW В 2024 ГОДУ (ЦСР, 2025)



Данные: «Рынок NGFW в Российской Федерации 2024-2030», Центр Стратегических Разработок, 3 апреля 2025

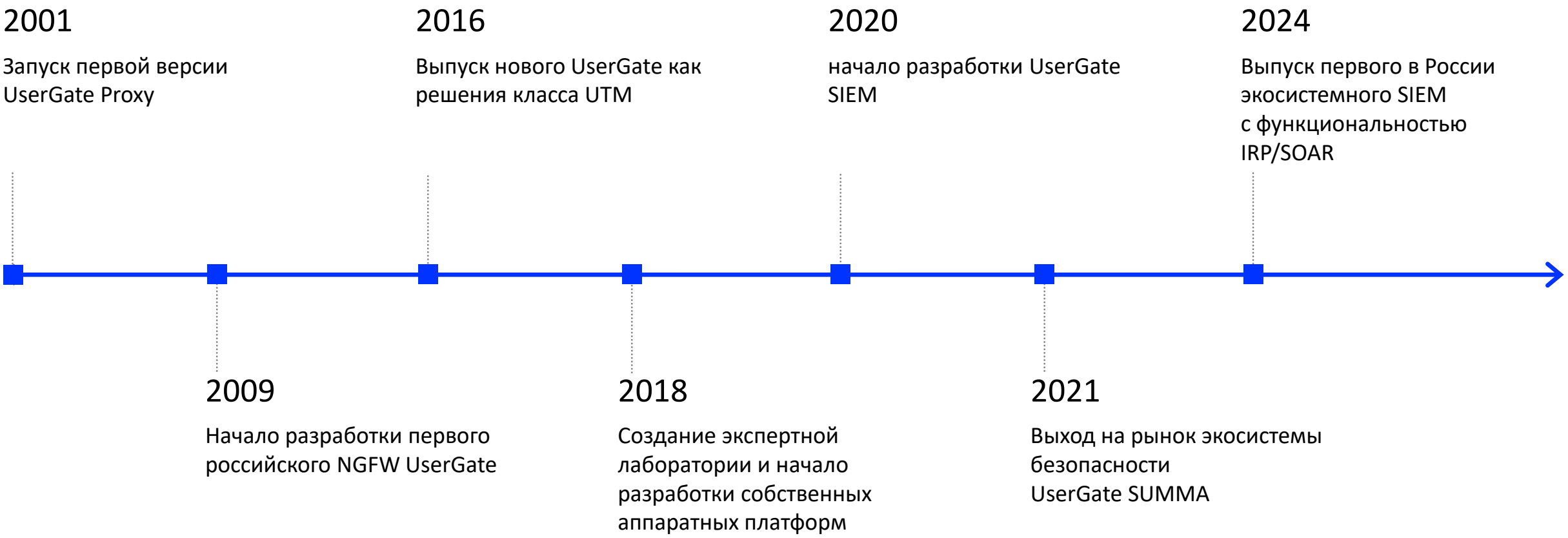
UserGate

SUMMA = Security Unified Management and Monitoring Architecture - Единая Архитектура Управления и Мониторинга Безопасностью

Список наших продуктов:

- NGFW
- MC
- SIEM
- LogAn
- Client
- DCFW
- WAF

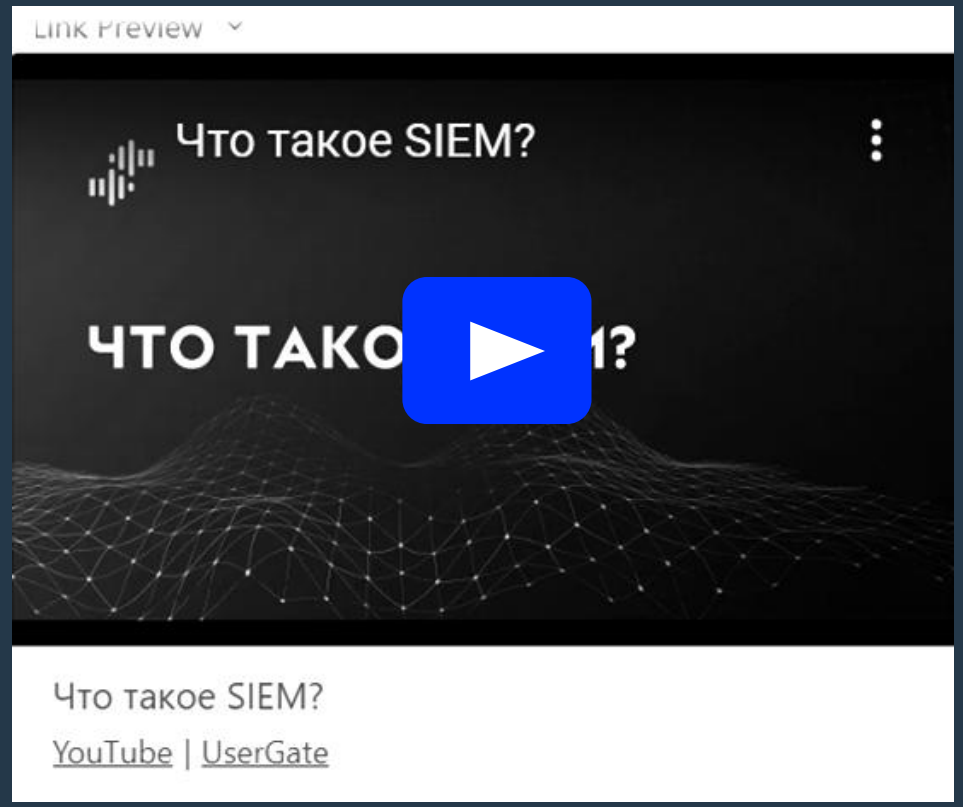
USERGATE.
ИСТОРИЯ УСПЕХА



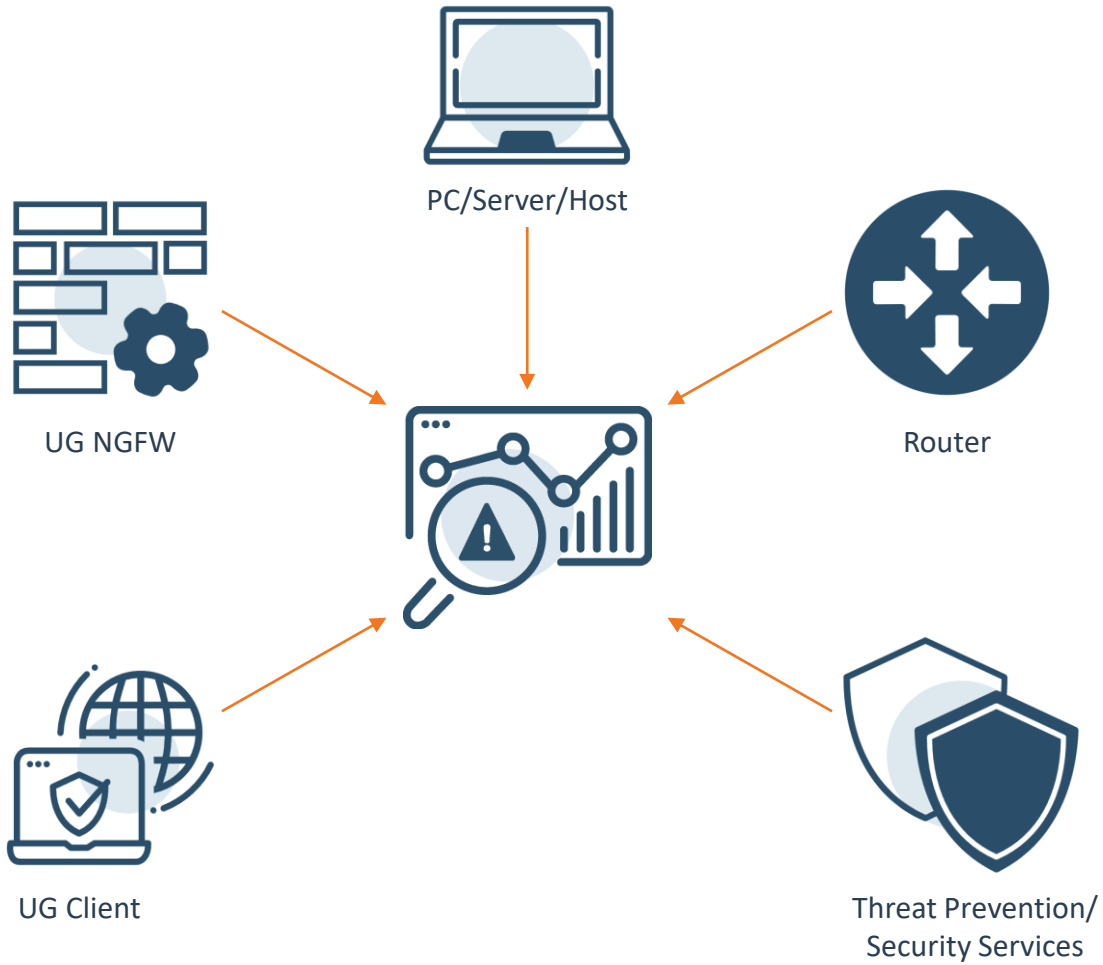
ЧТО ТАКОЕ SIEM?

SIEM
(Security Information and Event Management)
система управления событиями
информационной безопасности

https://www.youtube.com/watch?v=ddAzEN1iC5o
https://vkvideo.ru/video-211747929_456239139
https://rutube.ru/video/1d4c3321f002d531a6ef9cbd765fedf4/

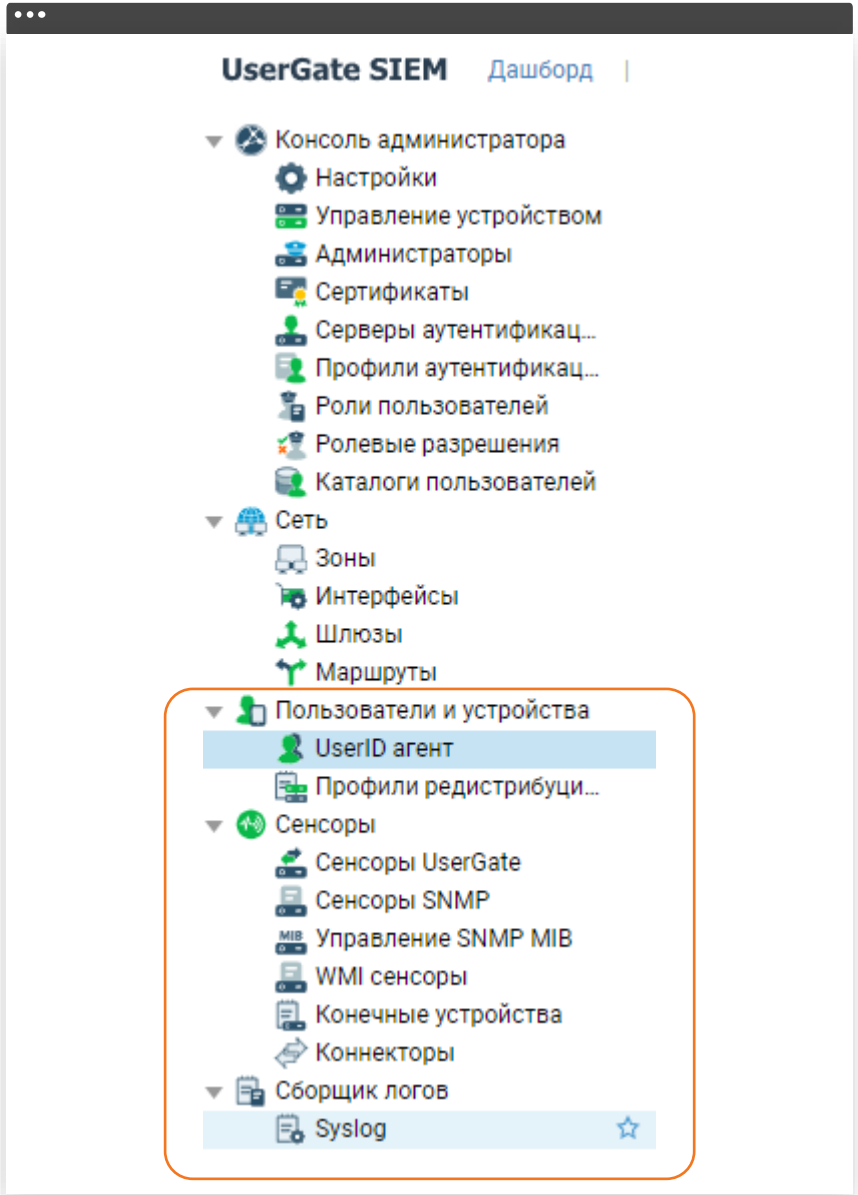


СБОР ДАННЫХ И НОРМАЛИЗАЦИЯ

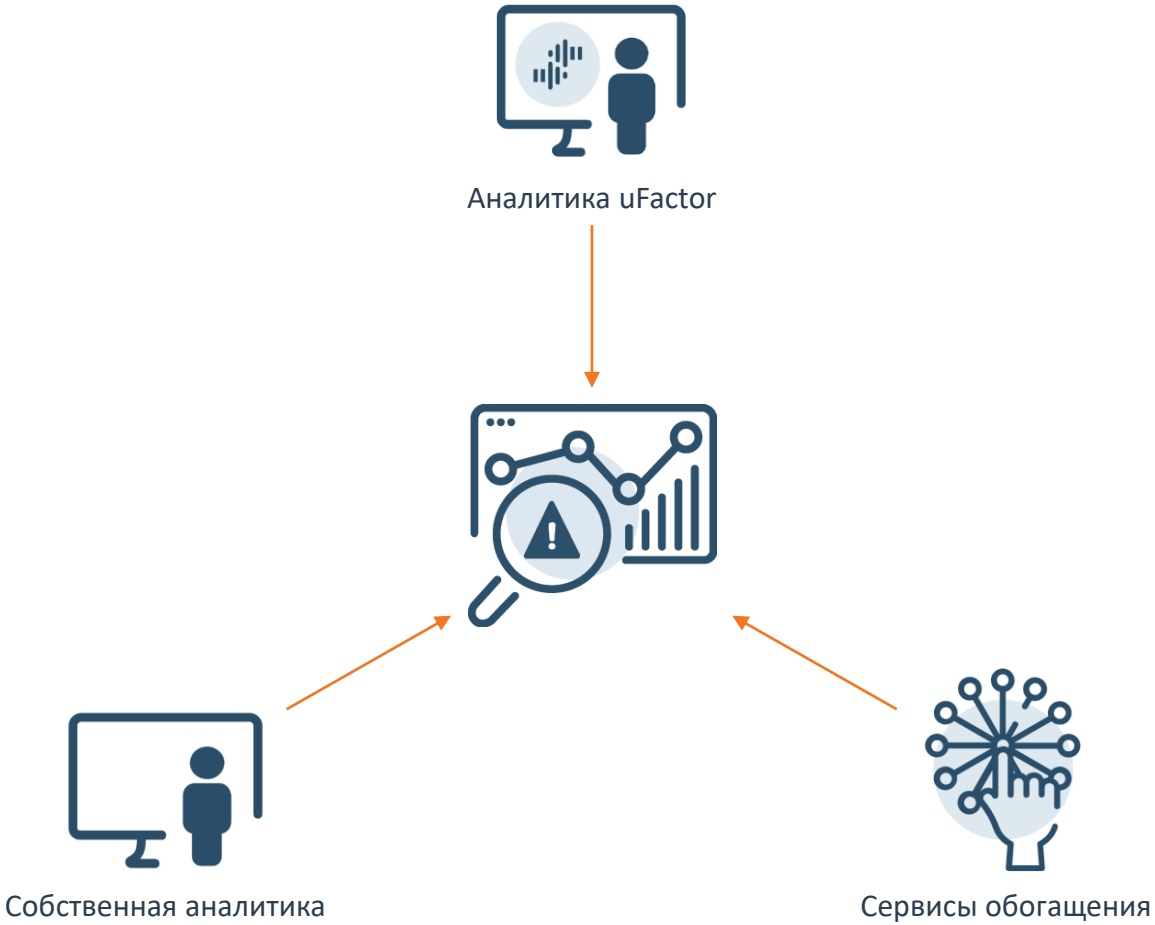


ИСТОЧНИКИ

- Межсетевые экраны UserGate
- Устройства SNMP
- Рабочие станции и сервера с WMI
- UserGate Client
- Хосты Syslog

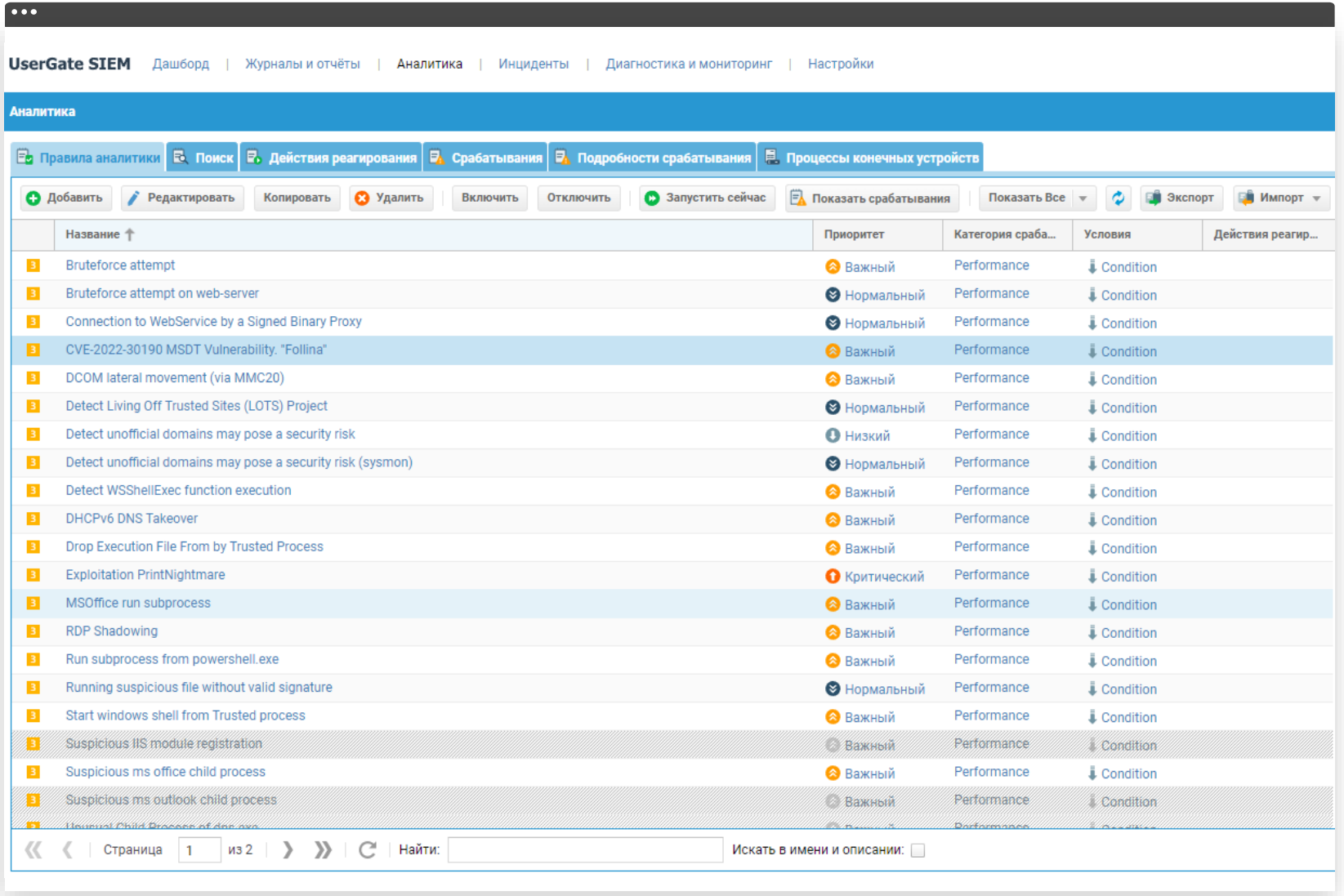


АНАЛИЗ И КОРРЕЛЯЦИЯ

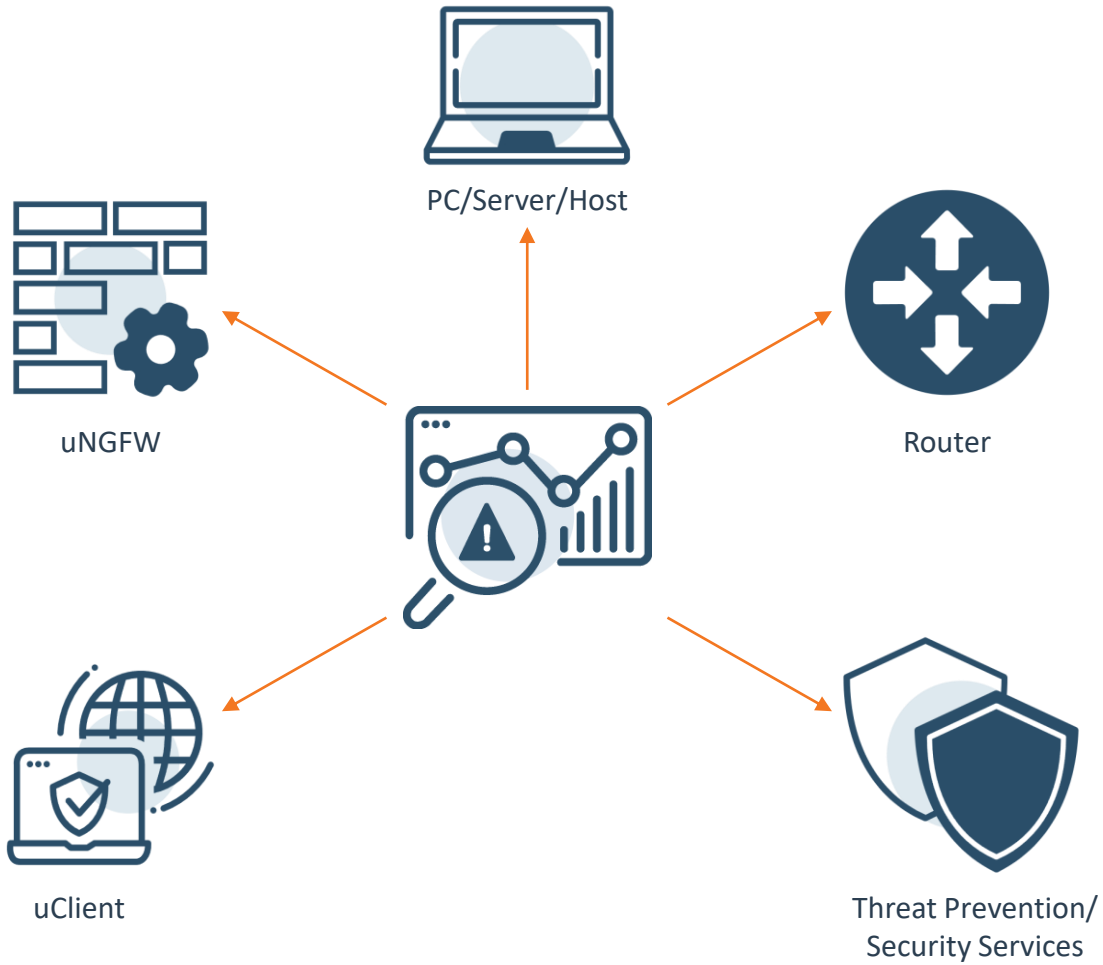


ПРАВИЛА АНАЛИТИКИ

- Правила из библиотеки (более 1000 правил, подготовленных uFactor).
- Правила добавленные пользователем.
- Возможность экспорта/ импорта правил.

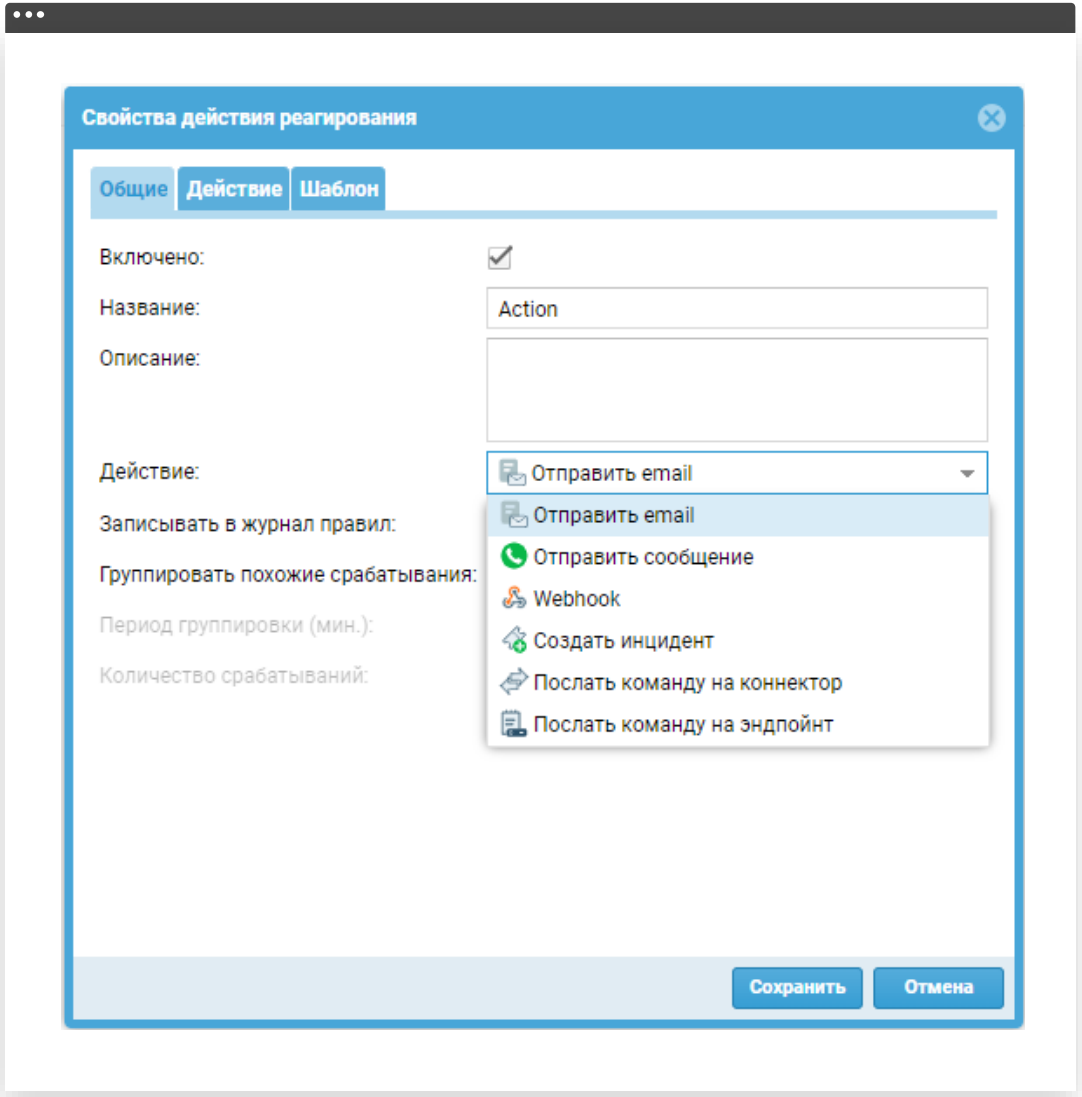


РЕАГИРОВАНИЕ



РЕАГИРОВАНИЕ ЧЕРЕЗ ИНФРАСТРУКТУРУ

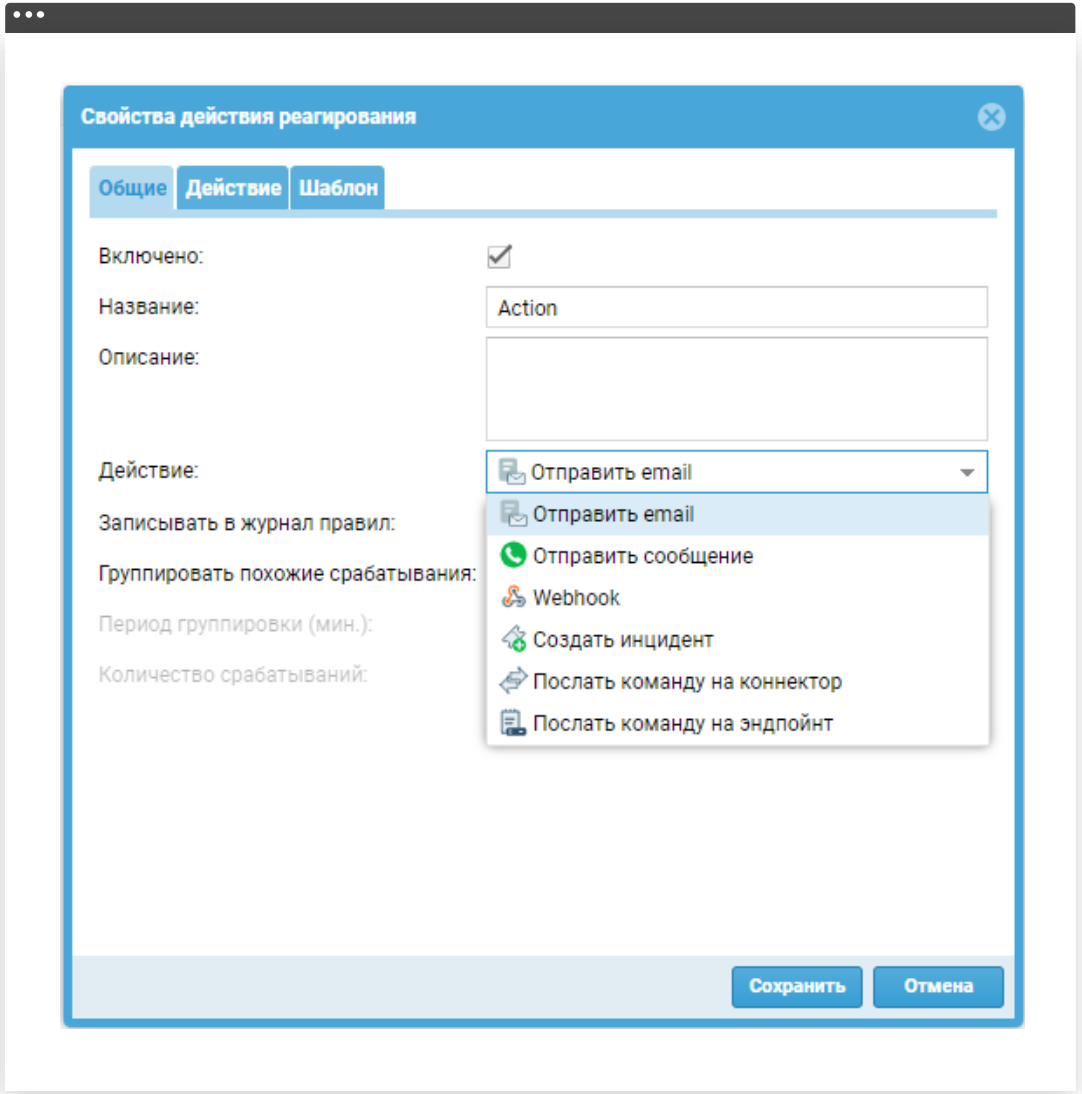
- Отправка команд через SSH/HTTP/HTTPS.
- Возможность передачи в команде артефактов, например IP-адресов.
- Возможность отправки команд на устройства других производителей (коммутаторы, маршрутизаторы и др.)



ВАРИАНТЫ РЕАГИРОВАНИЯ

- Оповещение e-mail/CMC/ Webhook.
- Создание инцидента.
- Отправка команд на устройство или UserGate Client.

Настройки группировки похожих событий



ПУТИ ЭВОЛЮЦИИ SIEM

ЭТАПЫ РАЗВИТИЯ SIEM

Log Manager

- сбор логов;
- дашборды и виджеты;
- отчеты.

01

Классический SIEM

- правила корреляции;
- анализ.

02

Экосистемный SIEM

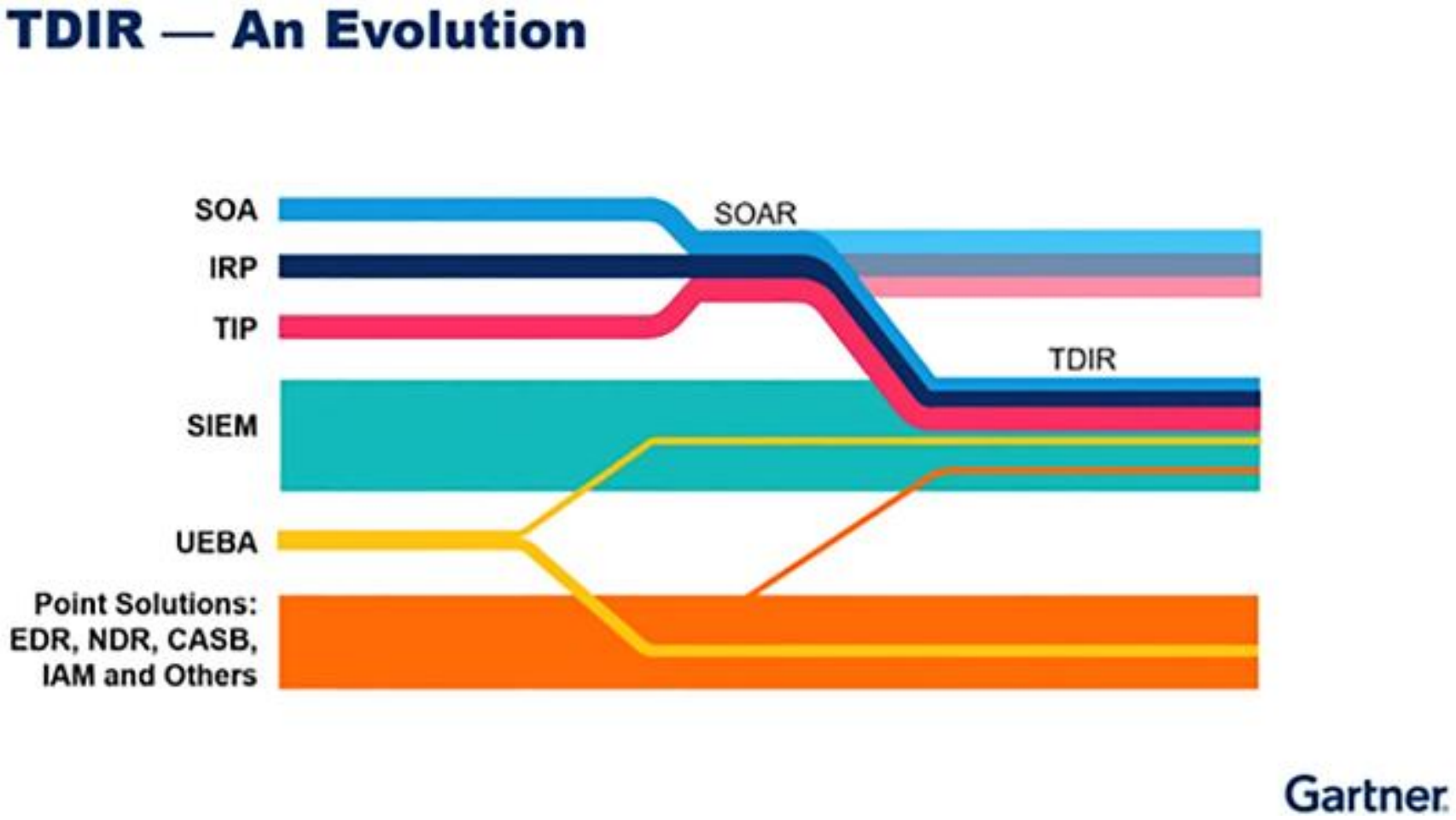
- улучшение логирования за счет экосистемных продуктов;
- увеличенный функционал системы.

03

Где взяли экспертизу?

Сами написали

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!



ЭКСПЕРТИЗА USERGATE

uFactor (ex. Monitoring and Response Center UserGate - Центр мониторинга и реагирования) – наш Центр Экспертизы!

- Внутри наших продуктов лежит пятнадцатилетний опыт компании по разработке средств защиты информации с их обильным применением на рынке. Мы насыщаем себя знаниями и быстро реагируем на новые вызовы и угрозы информационной безопасности, добавляя их в наши продукты.
- Мы оказываем услуги по аудиту и консалтингу, так же готовы предложить услуги SOC и обучение компаний цифровой гигиене (awareness).
- Мы делимся своими знаниями в крупных университетах, в т.ч. МАИ, Бауманка, МИФИ и др.

UserGate

ЗАЧЕМ ВАМ SIEM?

SIEM ПОМОЖЕТ ЛПР ОТ БИЗНЕСА

UserGate

Минимизировать финансовые потери

из-за простоя бизнес-критических сервисов

Снизить риск

утечки данных

Выполнить

требования регулятора

Получить

качественную экспертизу

Облегчить

работу сотрудников в режиме постоянного дефицита кадров

SIEM ПОМОЖЕТ ТЕХНИЧЕСКИМ ЛПР

UserGate

Обезопасить

свою компанию
от сложных комплексных атак

Своевременно

обнаружить инцидент

Оперативно

реагировать на инцидент

Качественно

расследовать инцидент

Исключить

повторение инцидента

SIEM ПОМОЖЕТ ТЕХНИЧЕСКИМ СПЕЦИАЛИСТАМ

UserGate

Получить

стабильно работающий продукт

Получить

быструю и качественную техподдержку

Подготовить

отчет для руководства

Произвести

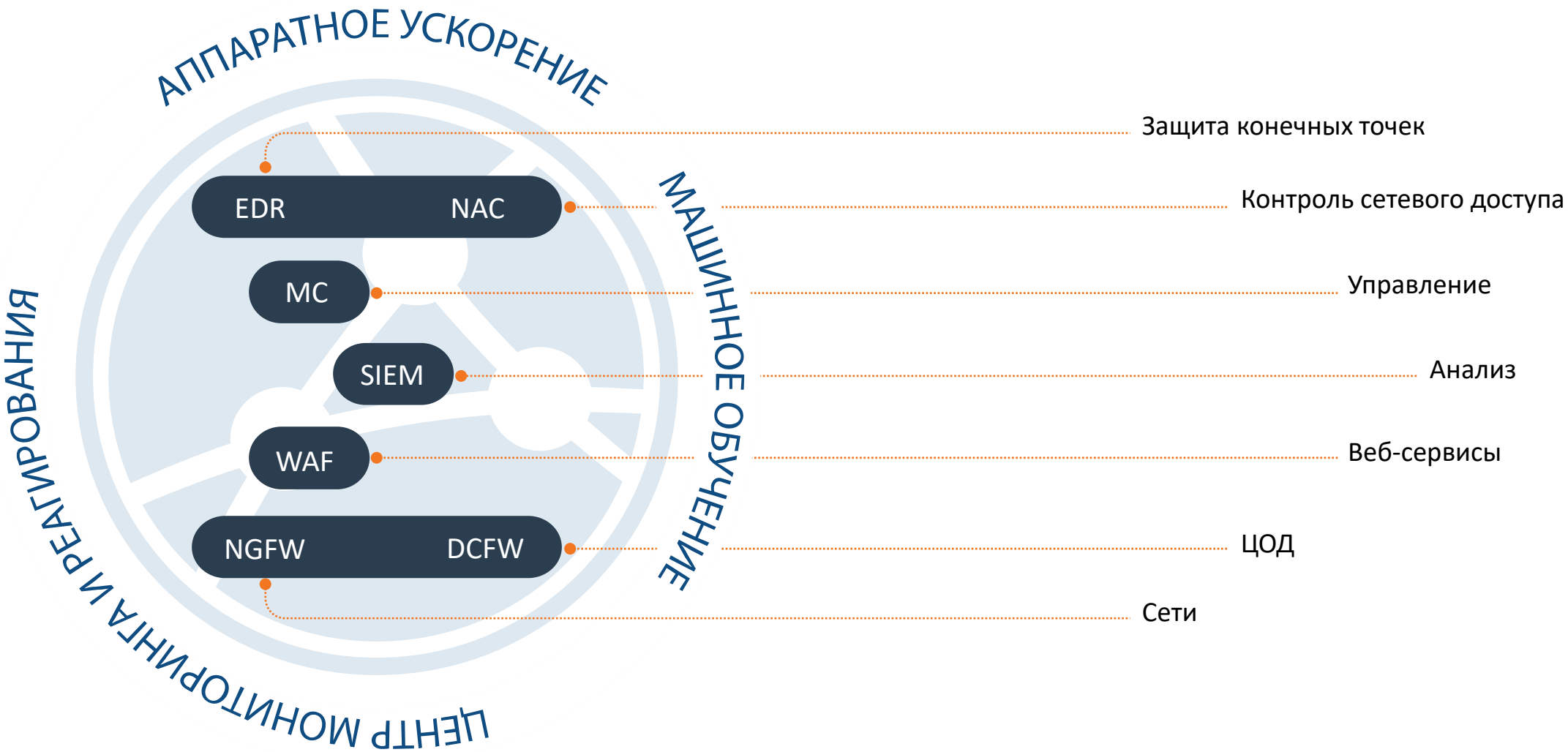
«безболезненные» обновления

SIEM ПОМОЖЕТ КОМПАНИИ

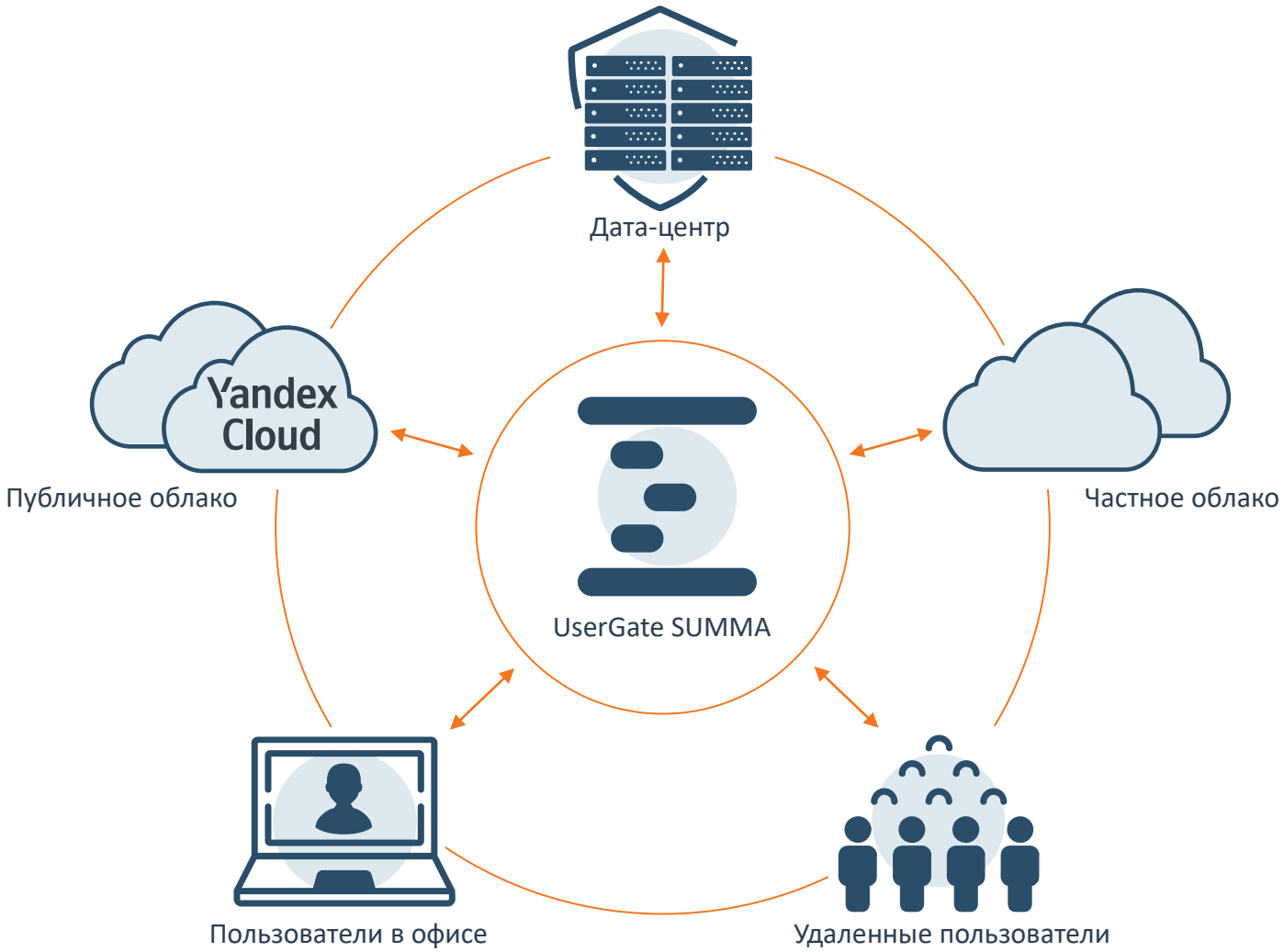
- выявление сложных комплексных атак на ранней стадии
- снижение общего количества инцидентов с тяжелыми последствиями
- обогащение инцидента дополнительной информацией
- приоритезация инцидентов
- своевременная реакция и быстрое реагирование на инцидент
- снижение трудозатрат на обнаружение и анализ инцидентов
- хранение исторических данных и ретроспективный анализ;
- формирование отчетности об инцидентах

В РАМКАХ USERGATE SUMMA

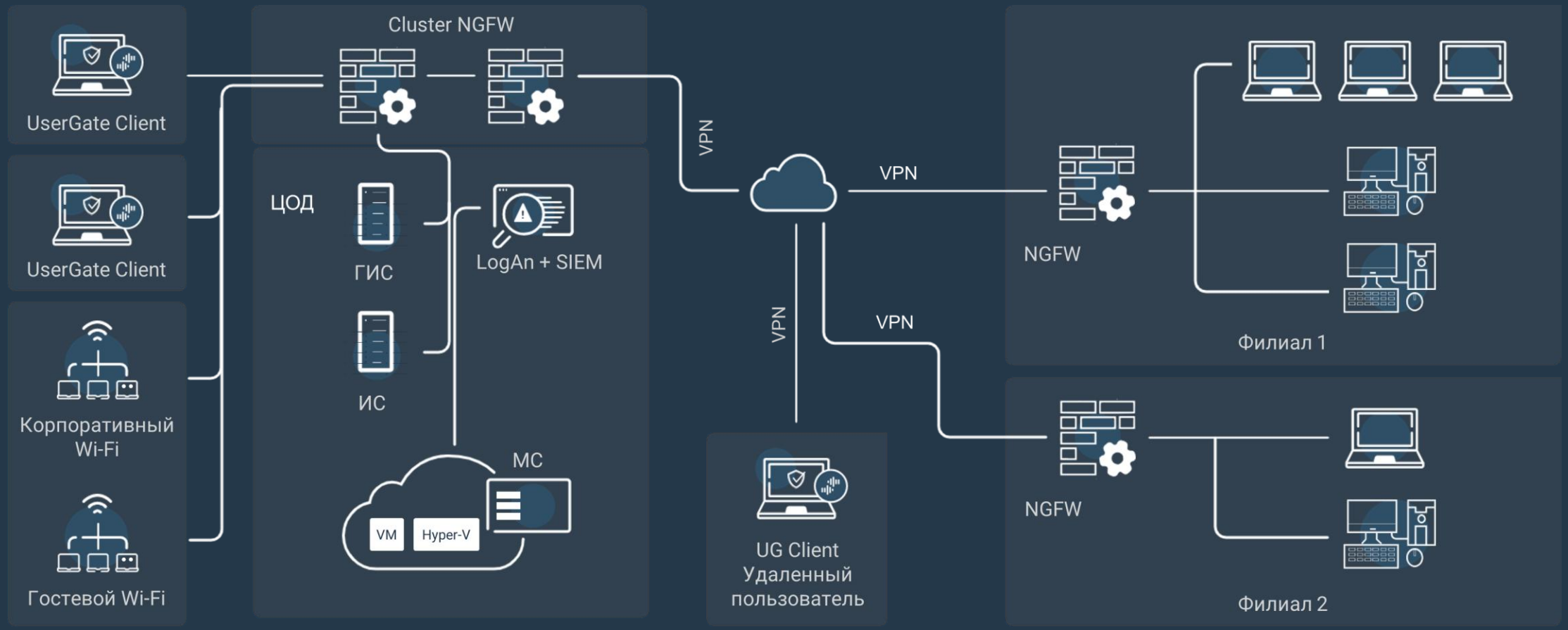
USERGATE SUMMA. 100% ВИДИМОСТЬ СОБЫТИЙ БЕЗОПАСНОСТИ



ZERO TRUST NETWORK ACCESS (ZTNA)



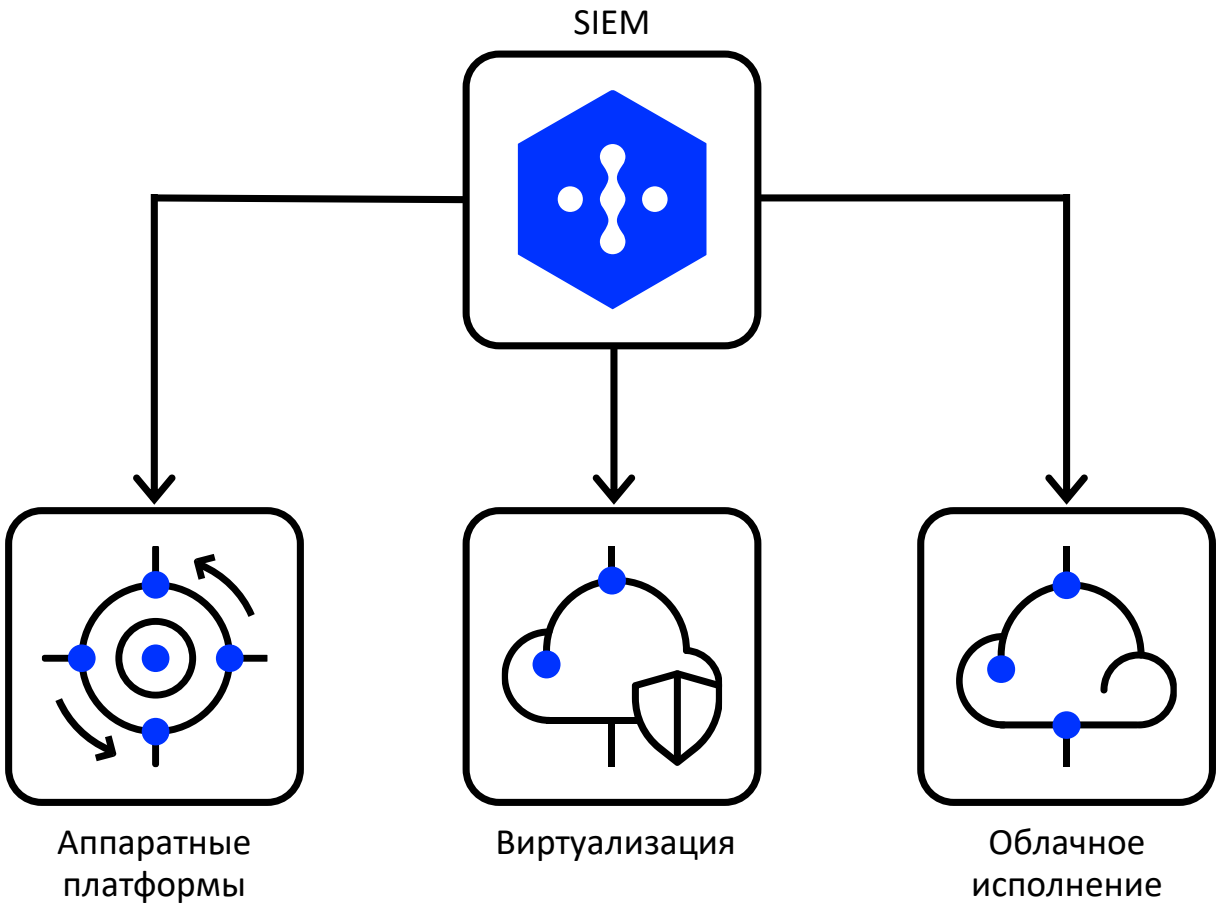
Экосистема продуктов безопасности UserGate SUMMA



UserGate

ВАРИАНТЫ ПОСТАВКИ

USERGATE SIEM –
SIEM ДЛЯ ГИБРИДНЫХ ИНФРАСТРУКТУР:



ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Аппаратные платформы

- модельный ряд, удовлетворяющий потребности каждого заказчика
- E6, E14, F25

01

Виртуализация

- поддержка всех популярных средств виртуализации
- VMware, Microsoft Hyper-V, KVM

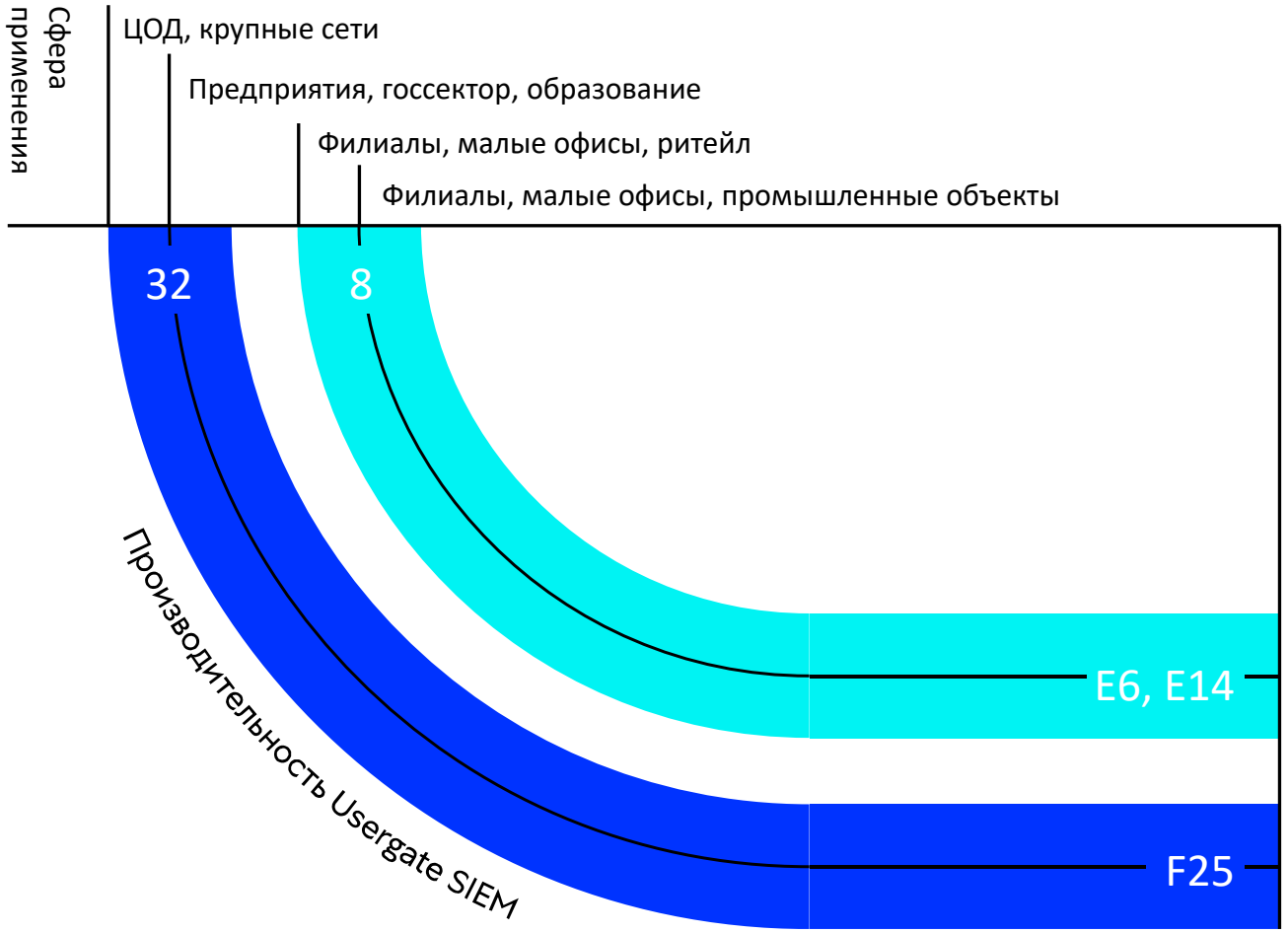
02

Облачное исполнение

- поддержка любых облаков, которые поддерживают стандартные реализации vmware и kvm (openstack)
- Yandex Cloud, Beeline cloud, МТС и VK

03

USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



6 ТБ
14 ТБ

25 ТБ

ВИРТУАЛЬНОЕ ИСПОЛНЕНИЕ

Гибкость и масштабируемость

- быстрое развертывание
- горизонтальное масштабирование
- широкий выбор виртуализации

Снижение затрат

- отсутствие затрат на железо
- экономия на обслуживании

Отказоустойчивость и доступность

- встроенная геораспределенность
- автоматическое восстановление VM

USERGATE SIEM –
SIEM ДЛЯ ГИБРИДНЫХ ИНФРАСТРУКТУР:

Аппаратные платформы

- модельный ряд удовлетворяющий потребности каждого заказчика: E6, E14, F25.

01

Виртуализация

- поддержка всех популярных средств виртуализации.

02

Облачное исполнение

- поддержка любых облаков, которые поддерживают стандартные реализации vmware и kvm (openstack);
- Yandex Cloud, Beeline cloud, МТС и VK.

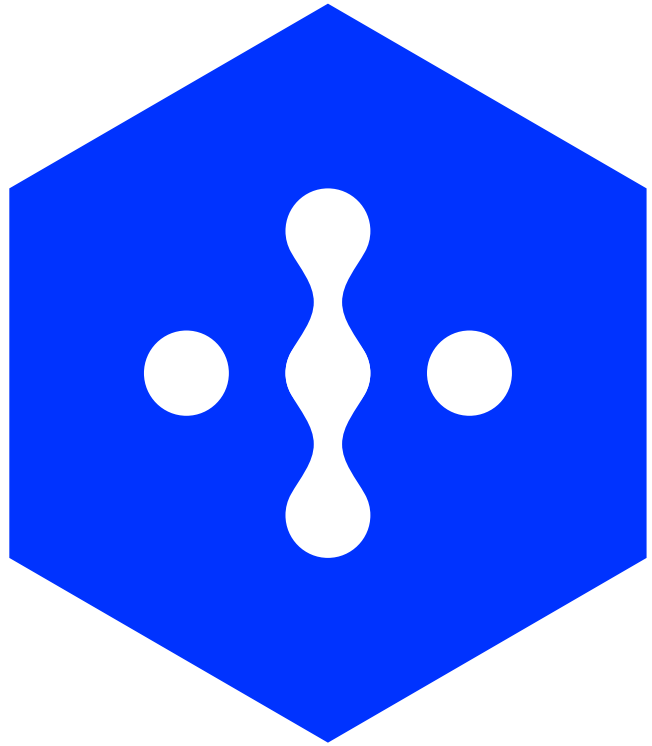
03

UserGate

ПРЕИМУЩЕСТВА

ПРЕИМУЩЕСТВА USERGATE SIEM

- пользовательские правила нормализации и корреляции
- обогащение инцидента дополнительной информацией
- кастомизация процесса обработки и приоритезация инцидентов
- возможность автоматического реагирования на инцидент
- хранение исторических данных и ретроспективный анализ
- формирование отчетности об инцидентах



ПРЕИМУЩЕСТВА ПРОДУКТА

IRP/SOAR

Возможности реагирования прямо из SIEM-системы. Как в автоматическом, так и в ручном режиме. При этом вам не нужно будет переключаться между различными продуктами ИБ, вся работа с инцидентом будет происходить в едином окне.

TI

Обогащения инцидента информацией из внешних сервисов, например, вы можете проверить адрес на предмет его чистоты на внешних базах данных, как платных, так и бесплатных.

Экспертиза

Собственная экспертиза от вендора на базе Центра мониторинга и реагирования UserGate (MRC UG);

Более 1’000 правил корреляции, отсортированных по матрице MITRE ATT&CK;

Различные способы реагирования.

НОРМАЛИЗАЦИЯ

Возможность создавать свои правила нормализации.
От того, как качественно вы выполните нормализацию, будет зависеть качество и скорость работы аналитиков.

ЭКОСИСТЕМА

Гибкость взаимодействия с продуктами из экосистемы;

Расширенное логирование за счет наличия экосистемных продуктов в инфраструктуре;

Удобство администрирования;

Единая точка тех. поддержки.

ОТКРЫТОСТЬ

Полноценная SIEM-система, которая может работать и в инфраструктуре, где нет других продуктов из экосистемы UserGate SUMMA.

ОСОБЕННОСТИ ПРОДУКТА

Гибкость развертывания

Железное исполнение;
Виртуальное исполнение;
Облачное исполнение.

Корреляция событий

Широкие возможности по выявлению и расследованию инцидентов.

Реагирование на инциденты

Автоматизация реагирования на инциденты прямо из SIEM-системы.

Простота и удобство

Система интуитивно понятна, не требует от сотрудников специфических знаний и навыком.

Отказоустойчивость

Возможность построения кластера для обеспечения поддержания работоспособности системы в случае сбоев, сохранности данных и безболезненных обновлений.

Требования законодательства

№ 152-ФЗ; № 187-ФЗ; приказ ФСТЭК № 21, 31; указ президента №250; ГОСТ Р 57580.1-2017; ГОСТ Р 57580.2-2018

ГосСОПКА

Подготовка отчетов в формете ГосСОПКА. Отправка инцидентов в ГосСОПКу. Как в ручном режиме, так и в автоматическом.

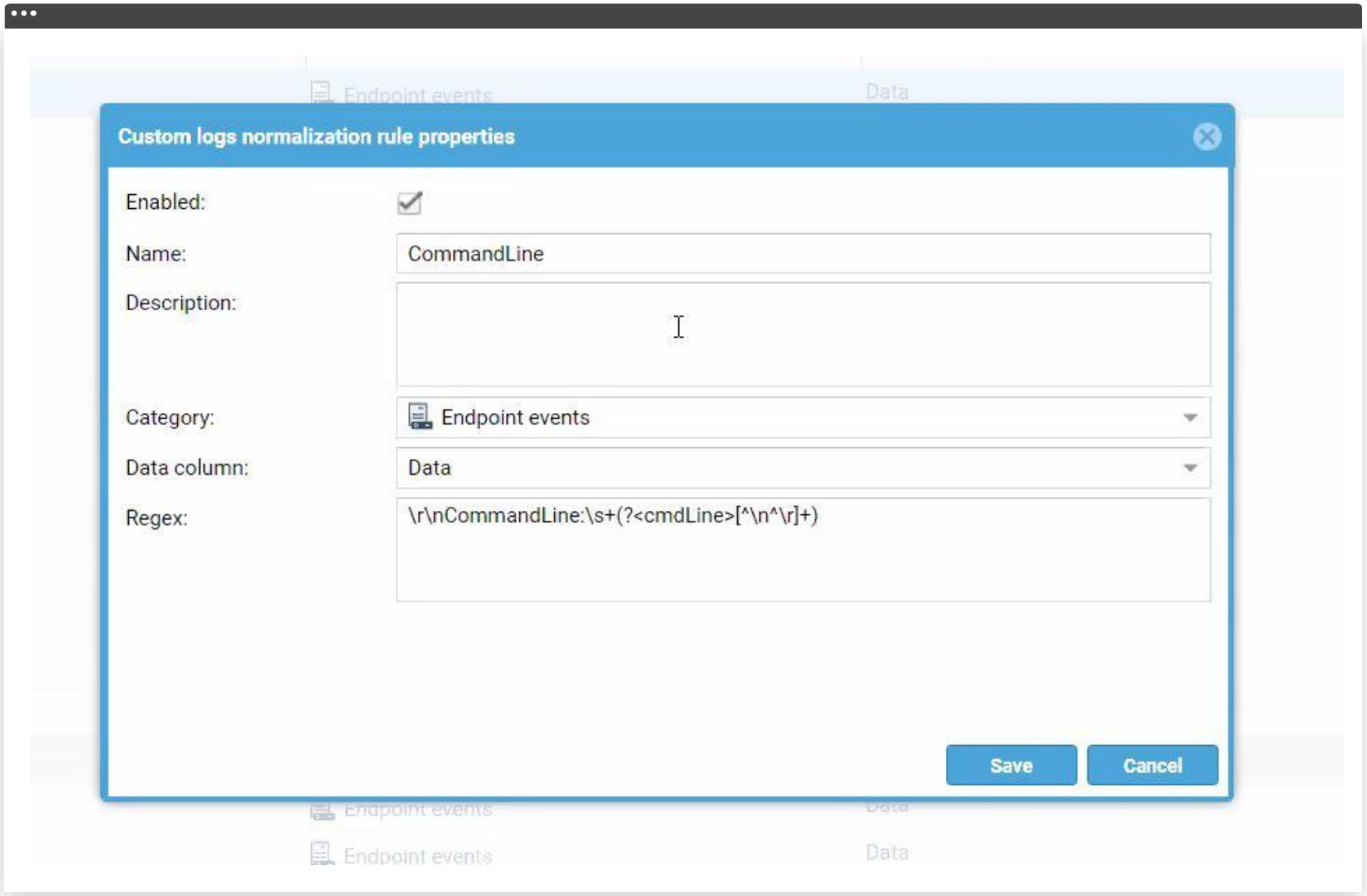
Интеграция с экосистемой

Глубокая совместимость с другими продуктами из экосистемы UserGate SUMMA, что обеспечивает единую платформу для управления безопасностью.

ПРАВИЛА АНАЛИТИКИ

- правила из библиотеки (более 1000 правил, подготовленных uFactor)
- правила добавленные пользователем
- возможность экспорта/импорта правил
- использование фильтров в качестве условий
- возможность загрузки правил в YAML-формате
- использование правил из библиотеки SIGMA

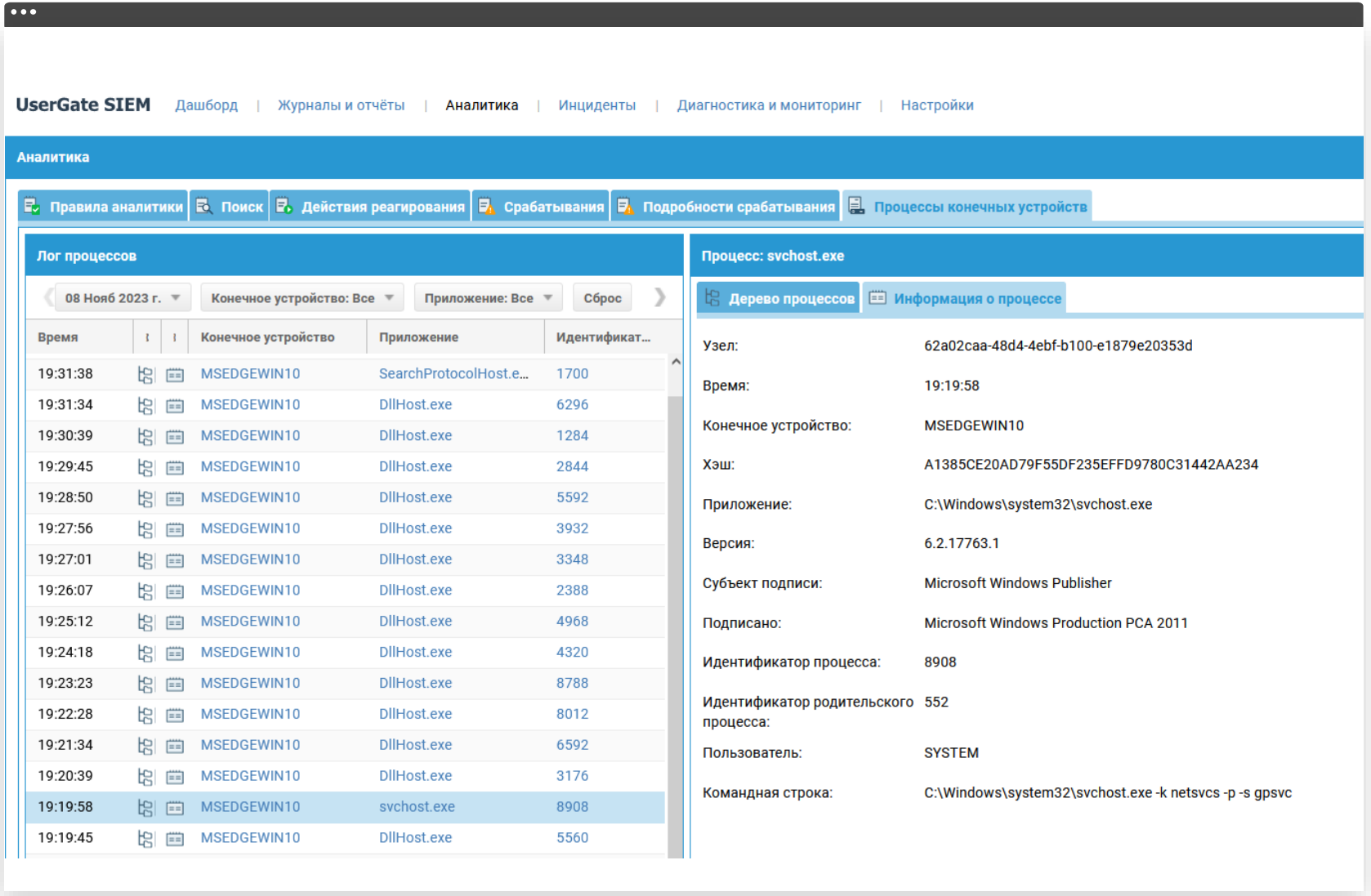
ПОЛЬЗОВАТЕЛЬСКАЯ НОРМАЛИЗАЦИЯ



ПРОЦЕССЫ КОНЕЧНЫХ УСТРОЙСТВ

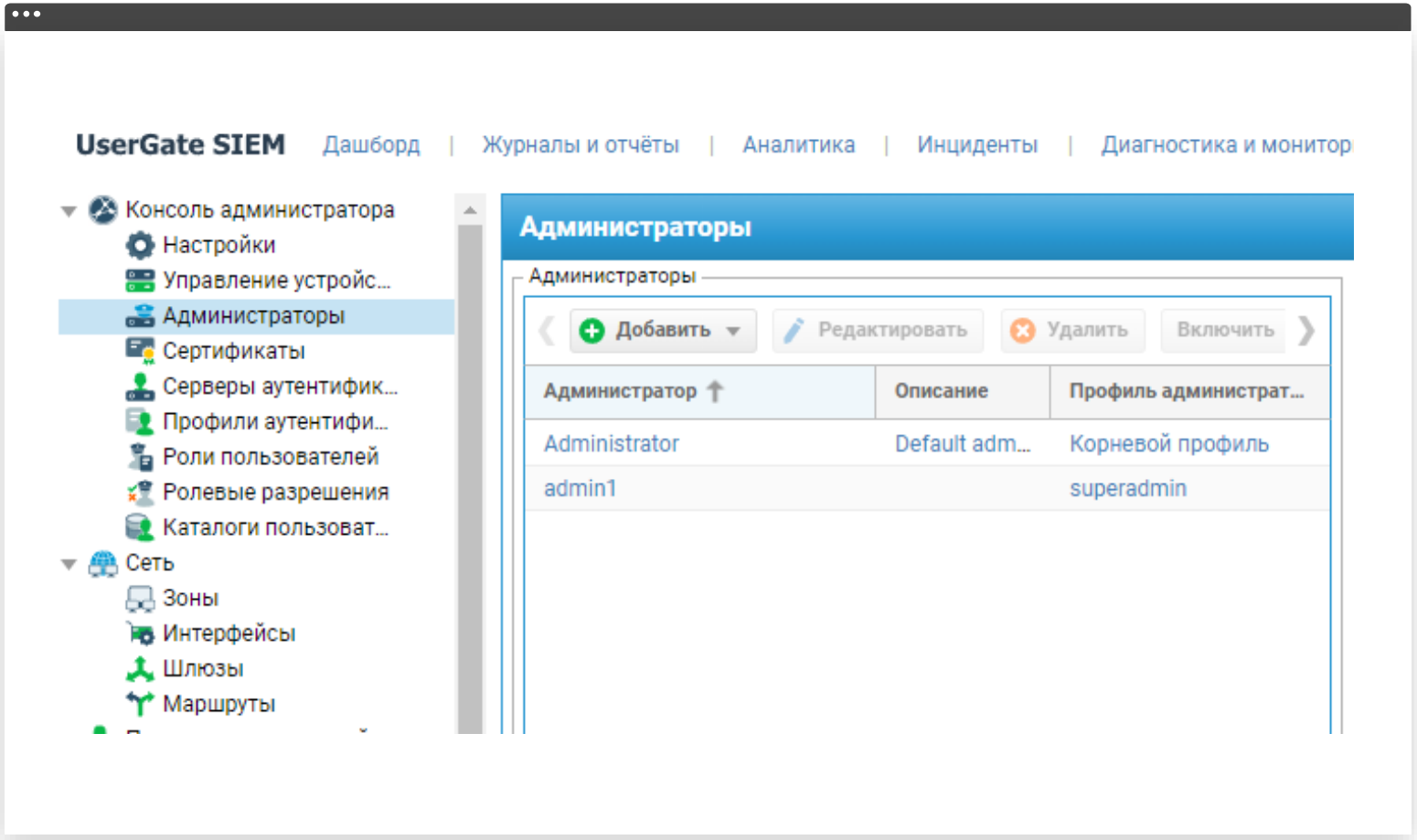
В разделе аналитики добавлены журналы о процессах на конечных устройствах.

Вся информация о когда-то запущенных процессах хранится тут.



АДМИНИСТРАТОРЫ

- Управление пользователями в системе.
- Добавление пользователей/ групп из LDAP.
- Отображение активных сессий пользователей.



РОЛЕВОЙ ДОСТУП

01

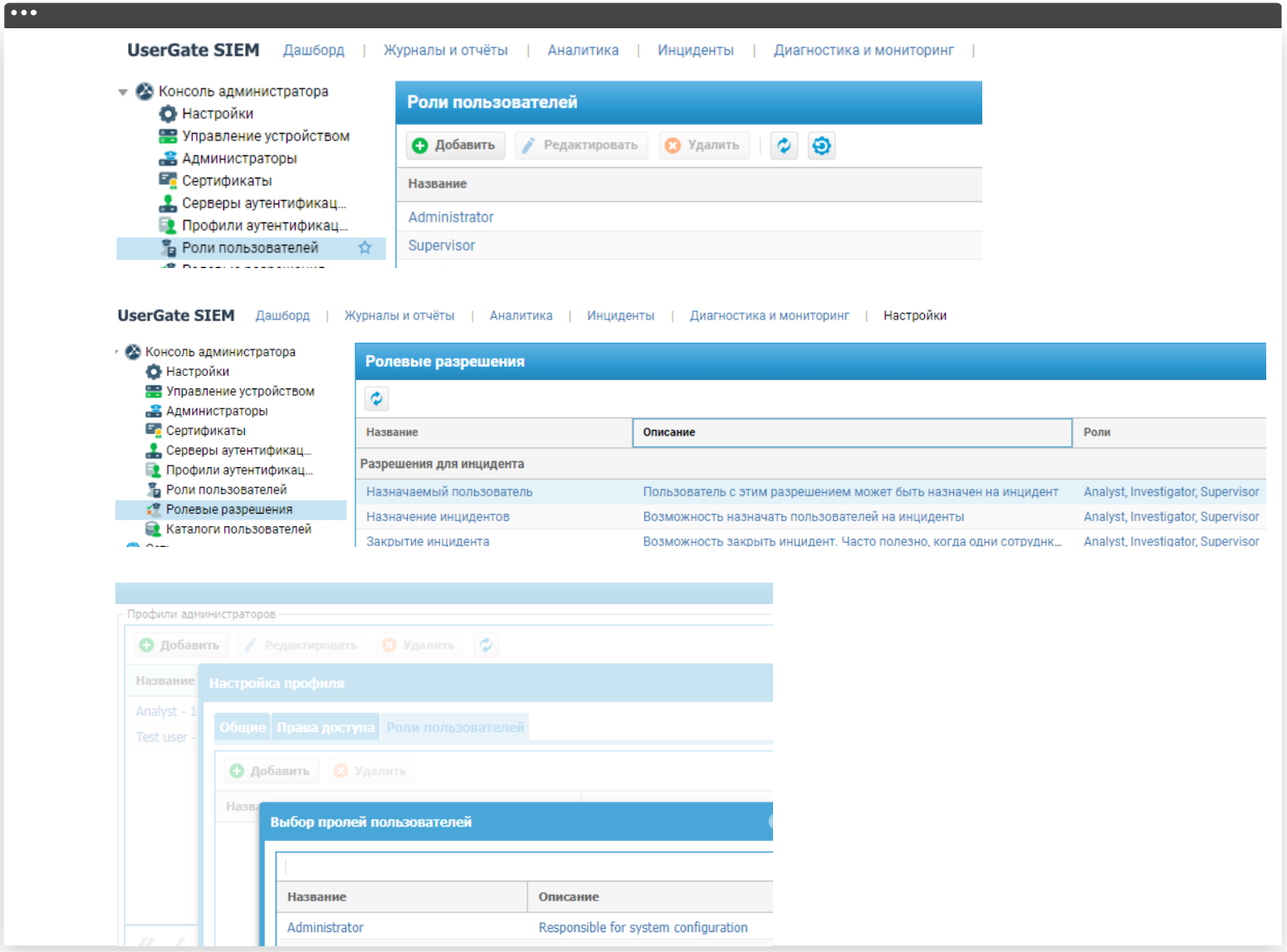
Роли пользователей

02

Ролевые разрешения

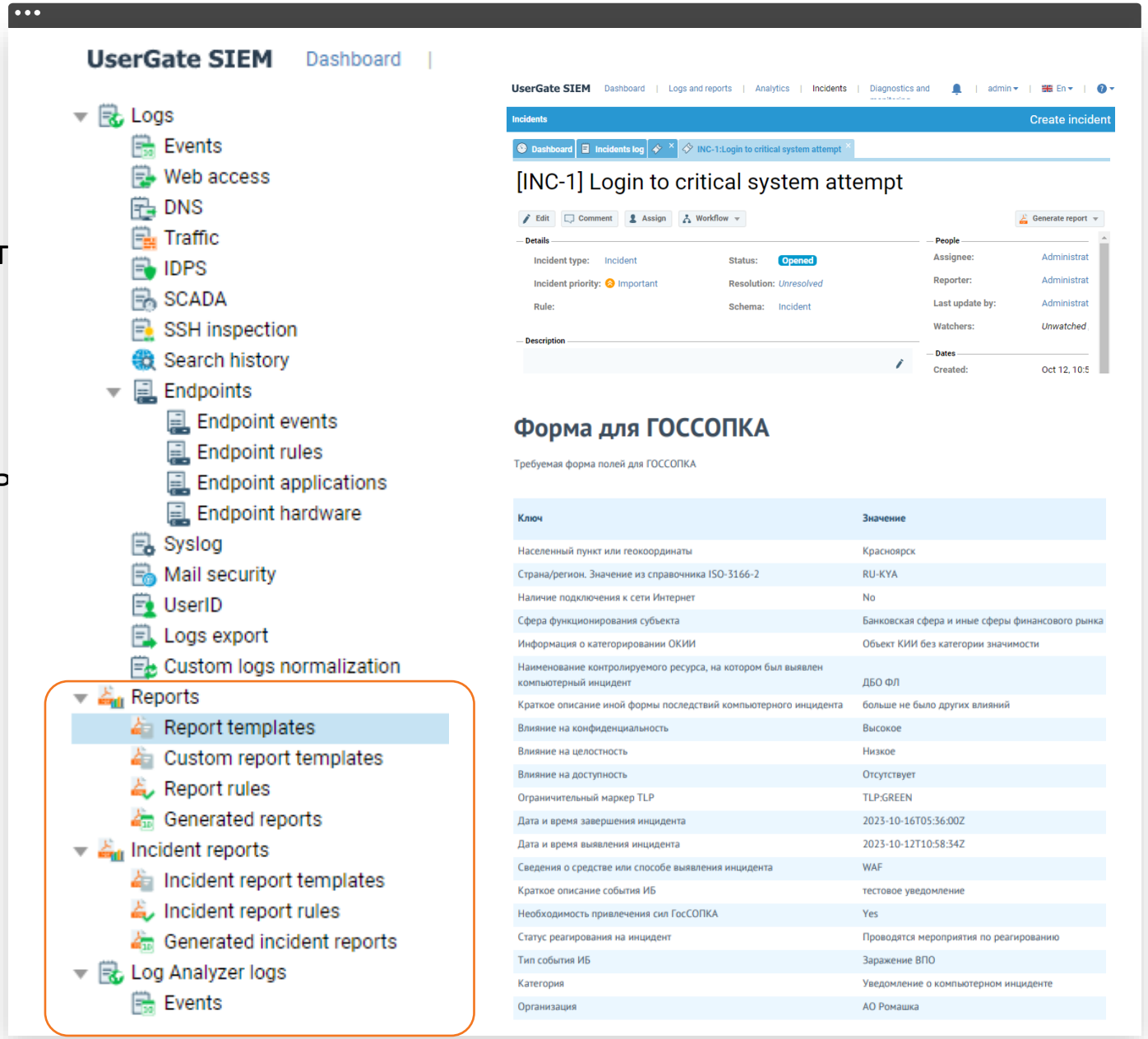
03

Профиль пользователя



ОТЧЕТЫ

- Генерация отчета по инцидент
- Отчеты в формате ГосСОПКА.
- Встроенные отчеты.
- Возможность создавать отчеты по своим требованиям.



USERGATE SIEM

- Первый экосистемный SIEM в России с функциональностью IRP/SOAR.
- Реагирование прямо «из коробки».
- Экономия бюджета на стороннем IRP/SOAR-решении и дорогостоящем персонале.
- Обогащения инцидента информацией из сторонних баз и из нашей библиотеки.
- Готовое решение с простотой установки, настройки и эксплуатации.
- Простой язык создания правил корреляции. Меньше требований к знаниям.
- Возможность создавать пользовательские правила нормализации событий.
- Интеграция с ГосСОПКА.

СПАСИБО

По вопросам приобретение: sales@usergate.com

Алексей Афанасьев
Менеджер по развитию
UserGate SIEM

Записаться на пилот!