UserGate

СОВРЕМЕННАЯ SIEM-СИСТЕМА НА ПРИМЕРЕ USERGATE SIEM

Алексей Афанасьев
Менеджер по развитию UserGate SIEM

USERGATE. ИСТОРИЯ УСПЕХА

2001

запуск первой версии UserGate Proxy

2009

начало разработки первого российского NGFW UserGate

2016

выпуск нового UserGate как решения класса UTM

2018

создание экспертной лаборатории и начало разработки собственных аппаратных платформ

2020

начало разработки UserGate SIEM

2021

выход на рынок экосистемы безопасности UserGate SUMMA

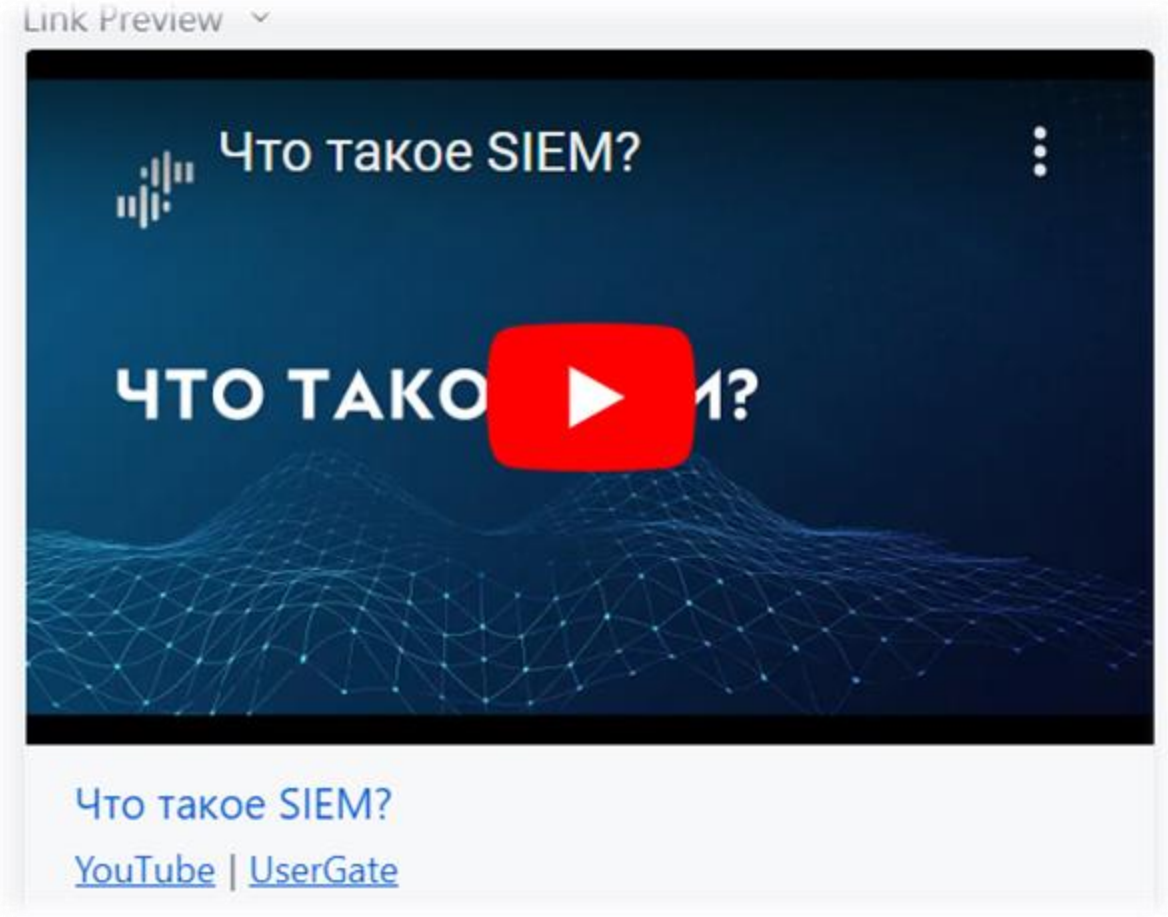
2024

Выпуск первого в России экосистемного SIEM с функциональностью IRP/SOAR

ЧТО ТАКОЕ SIEM?

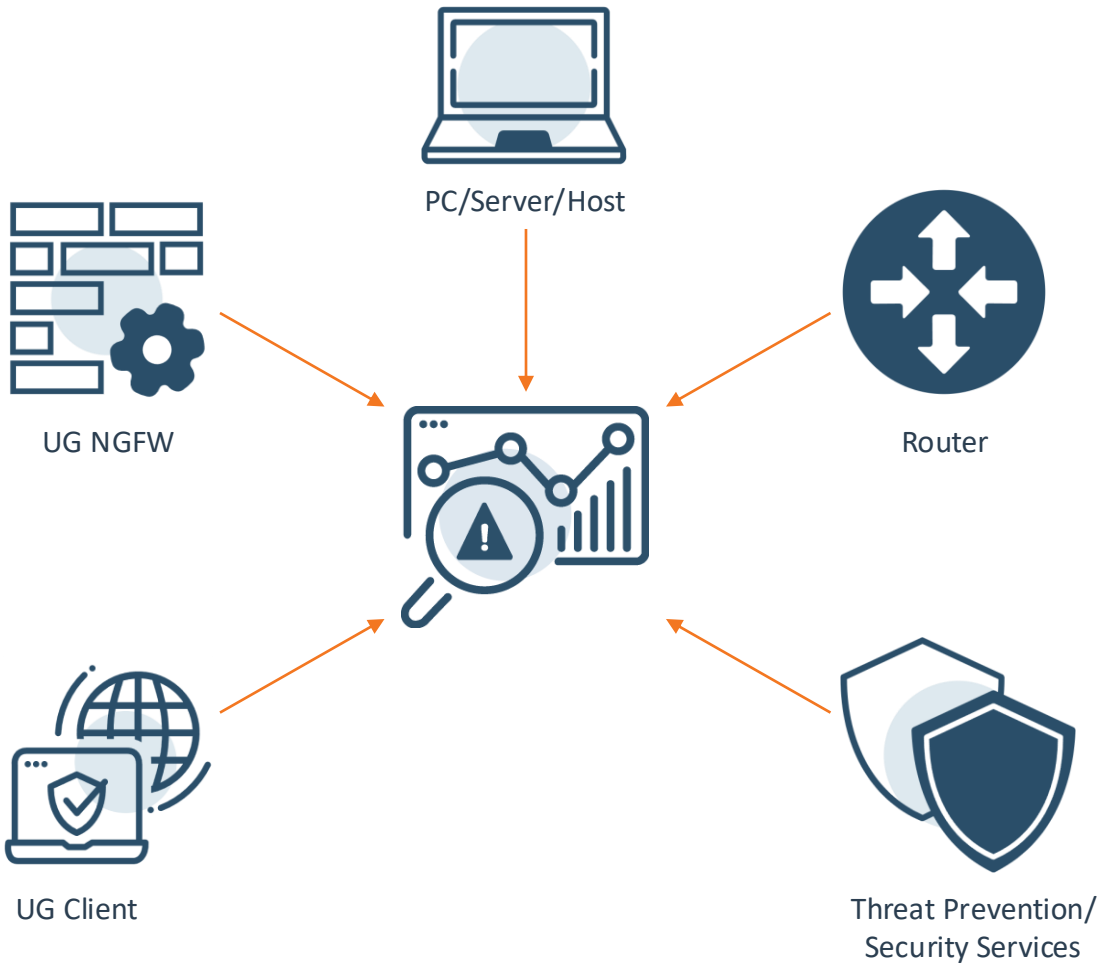
ЧТО ТАКОЕ SIEM?

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



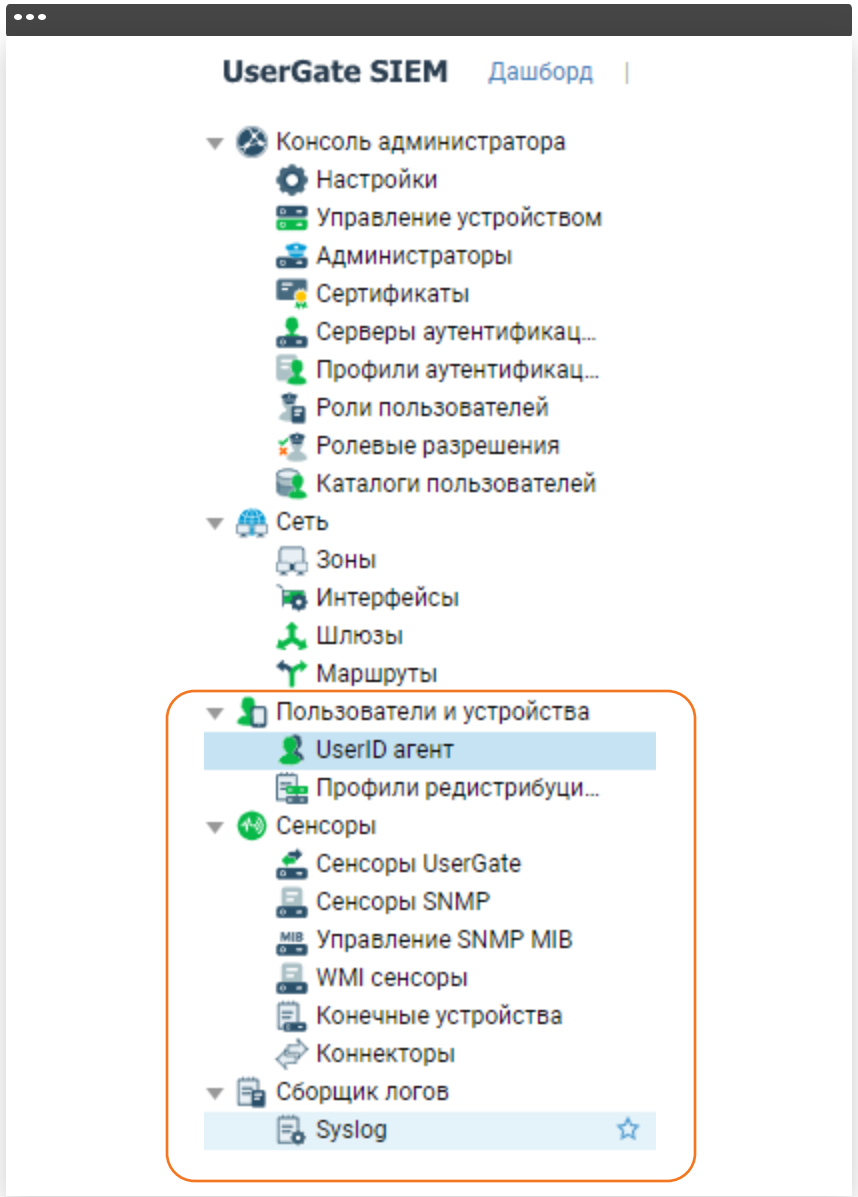
https://www.youtube.com/watch?v=ddAzEN1iC5o

СБОР ДАННЫХ И НОРМАЛИЗАЦИЯ

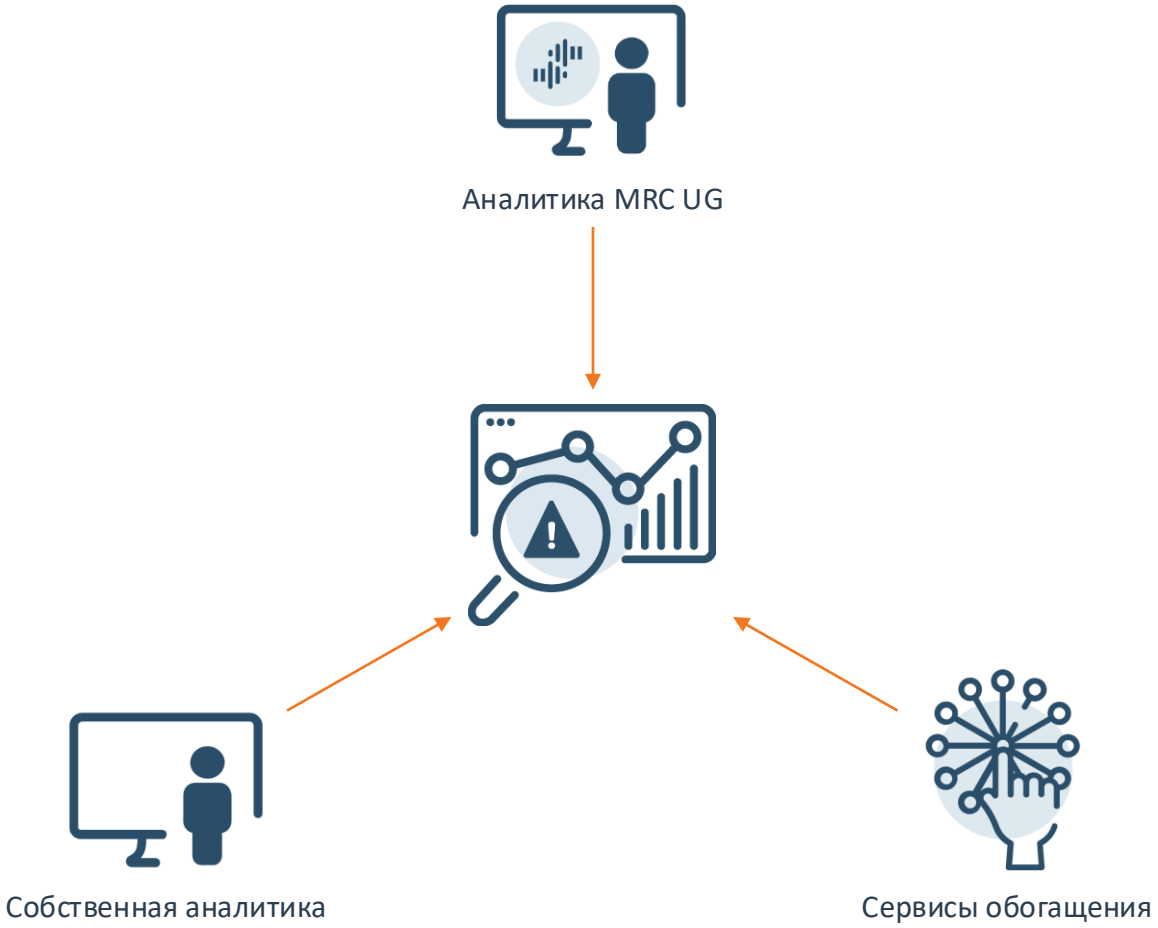


ИСТОЧНИКИ

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

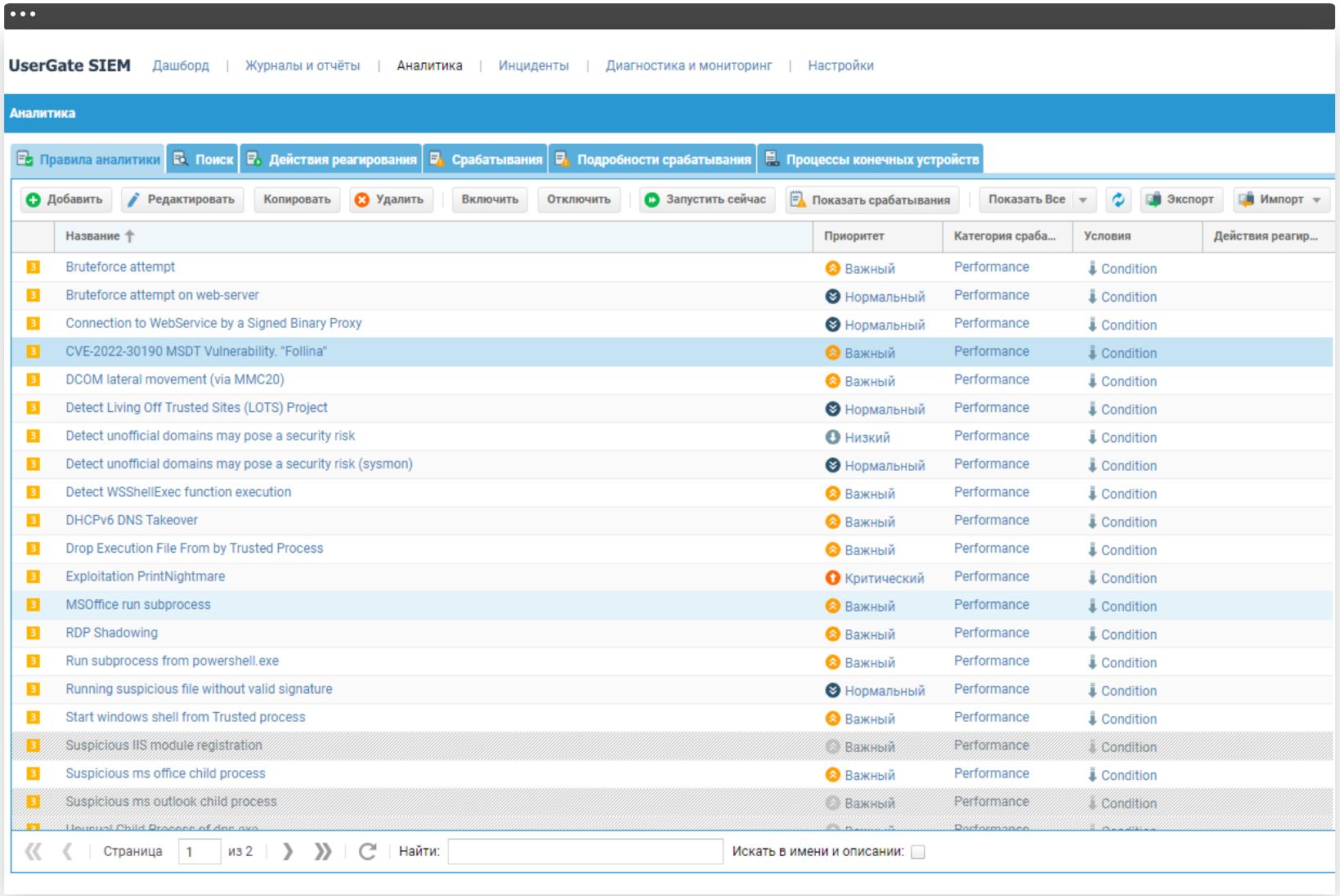


АНАЛИЗ И КОРРЕЛЯЦИЯ

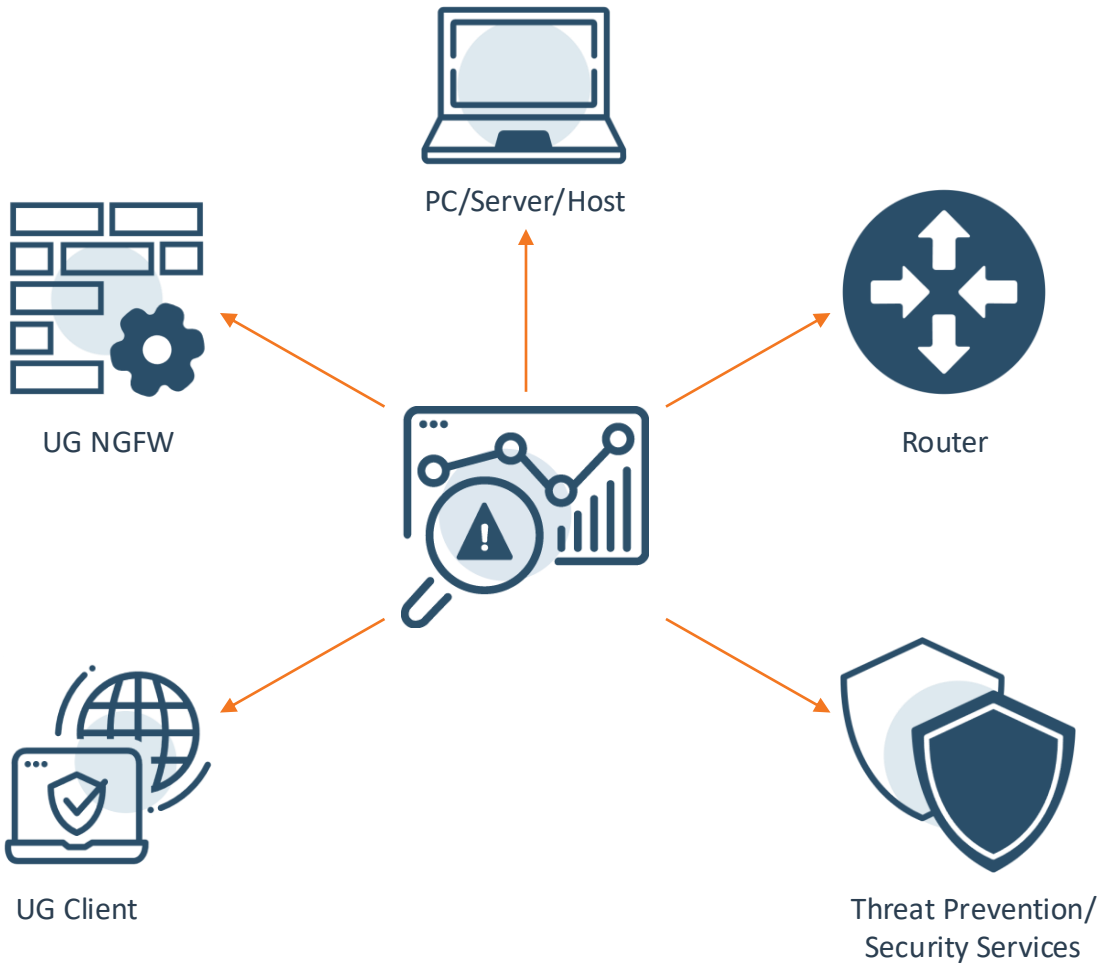


ПРАВИЛА АНАЛИТИКИ

- Правила из библиотеки (более 750 правил, подготовленных MRC UG).
- Правила добавленные пользователем.
- Возможность экспорта/ импорта правил.

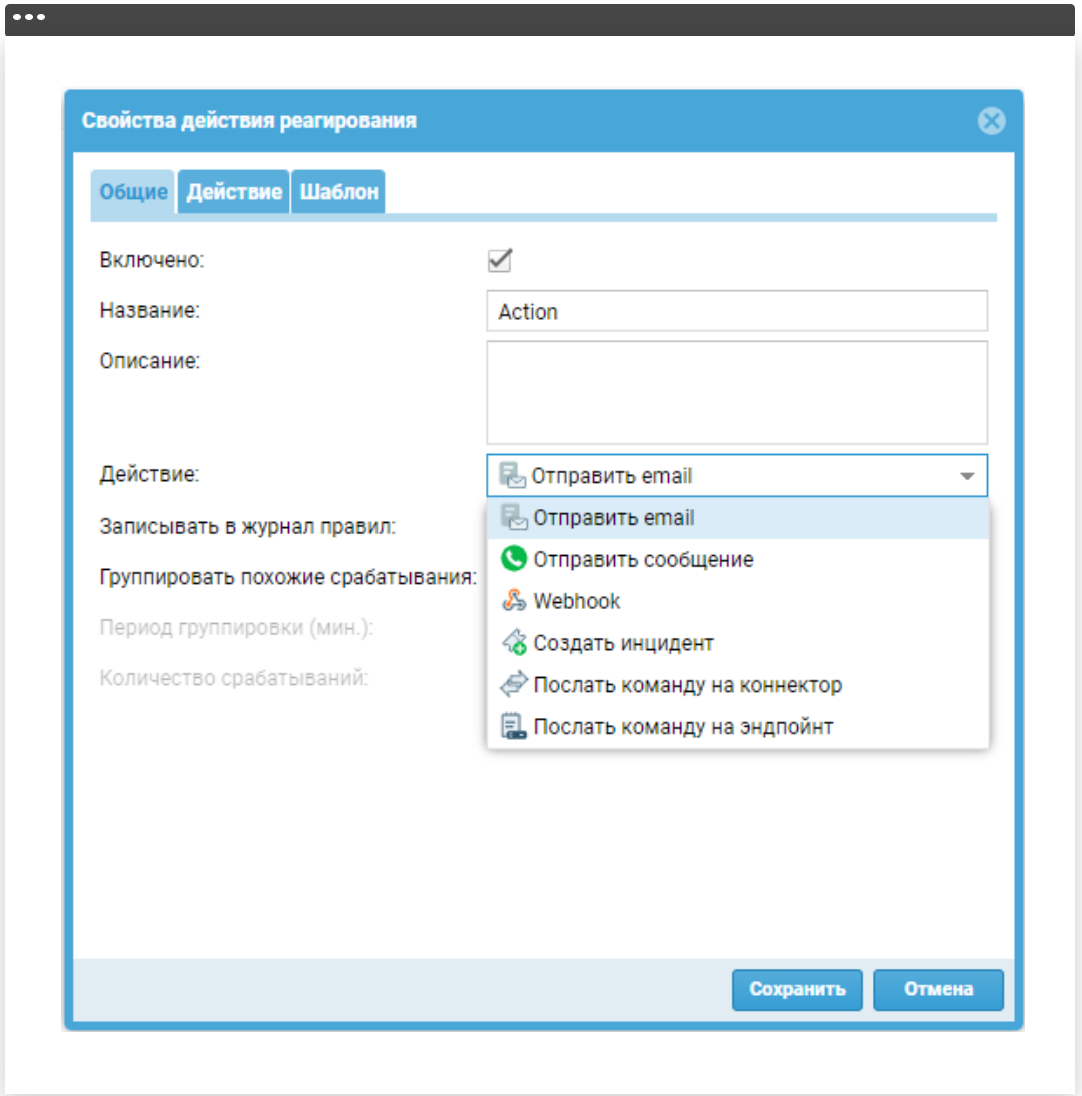


РЕАГИРОВАНИЕ



РЕАГИРОВАНИЕ ЧЕРЕЗ ИНФРАСТРУКТУРУ

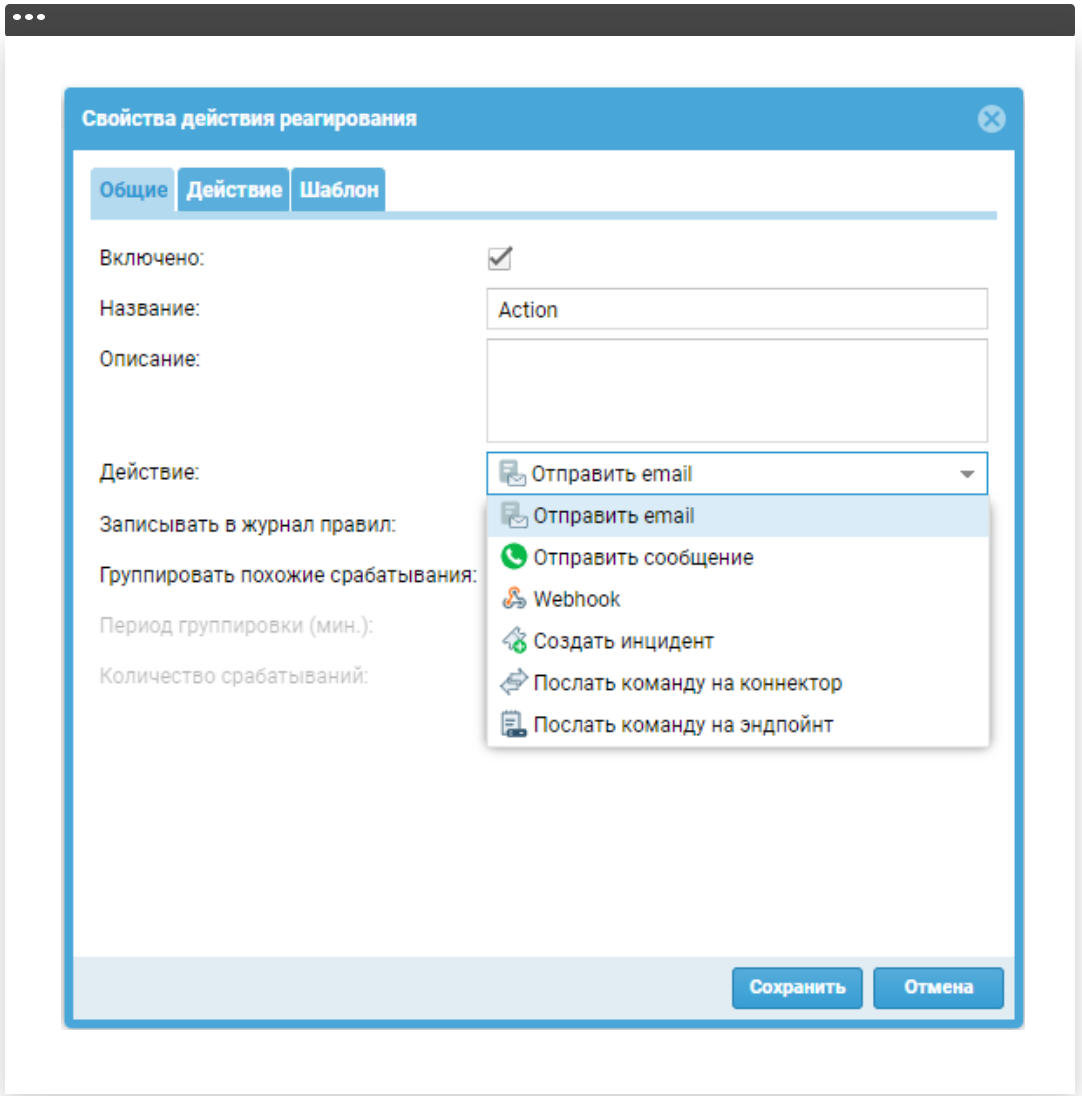
- Отправка команд через SSH/HTTP/HTTPS.
- Возможность передачи в команде артефактов, например IP-адресов.
- Возможность отправки команд на устройства других производителей (коммутаторы, маршрутизаторы и др.)



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.

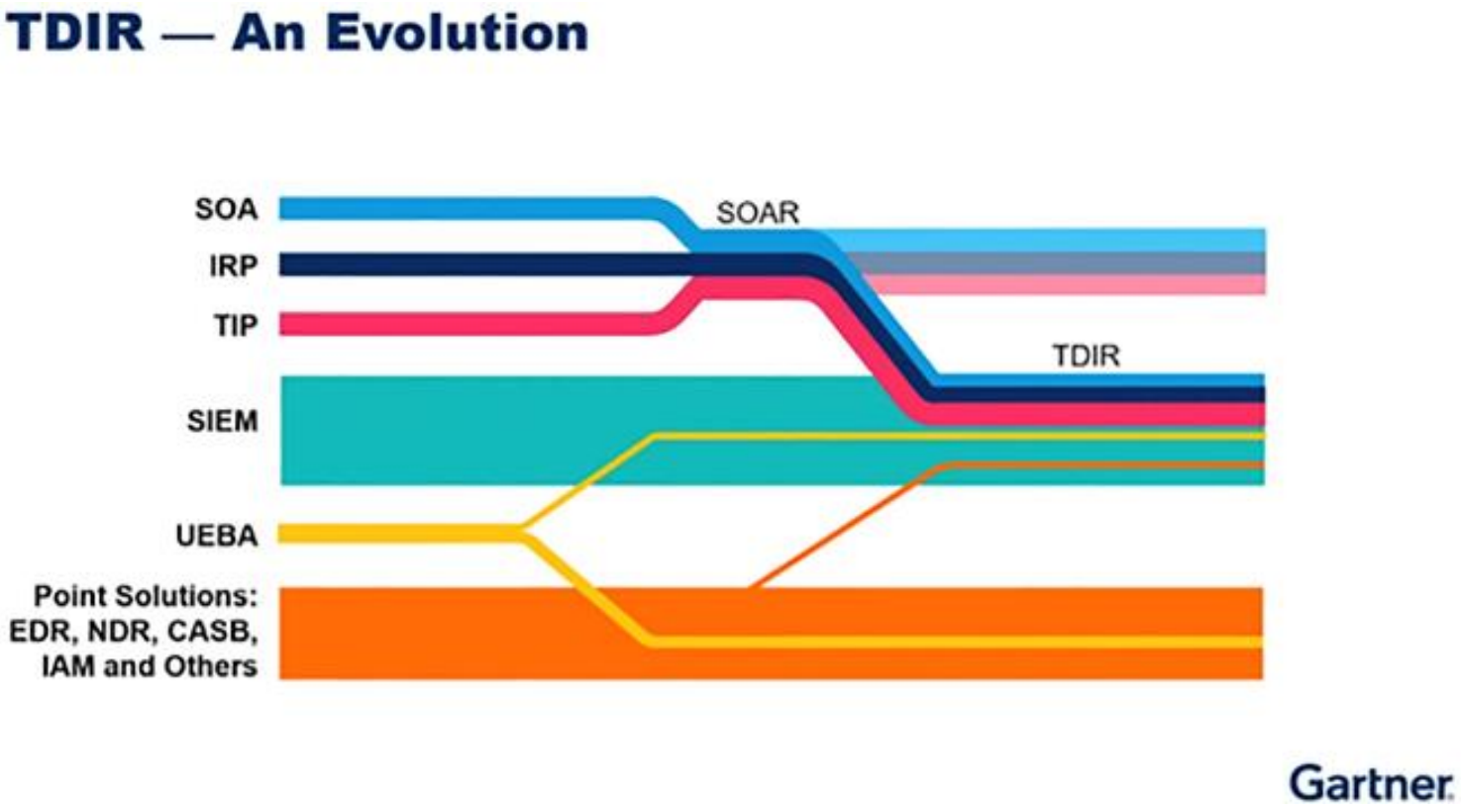
02

Экосистемный SIEM

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

03

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!



Где взяли экспертизу?

Где взяли экспертизу?

Сами написали

ЭКСПЕРТИЗА USERGATE

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.

ВЫБОР ЗАКАЗЧИКА

SIEM-системы неминуемо должны эволюционировать!

Предложений на рынке много и заказчику уже не нужна классическая SIEM-система.

Ключевыми при выборе продукта будут такие факторы как:

- качество тех. поддержки;
- собственная уникальная экспертиза от вендора;
- взаимодействие со всеми другими продуктами в инфраструктуре заказчика;
- масштабная экосистема;
- наличие дополнительного функционала, который будет выделять решение на фоне конкурентов и облегчать работу заказчика.

В конечном счете, заказчик будет выбирать между качеством, экспертизой, ценой и удобством.

SIEM ПОМОЖЕТ

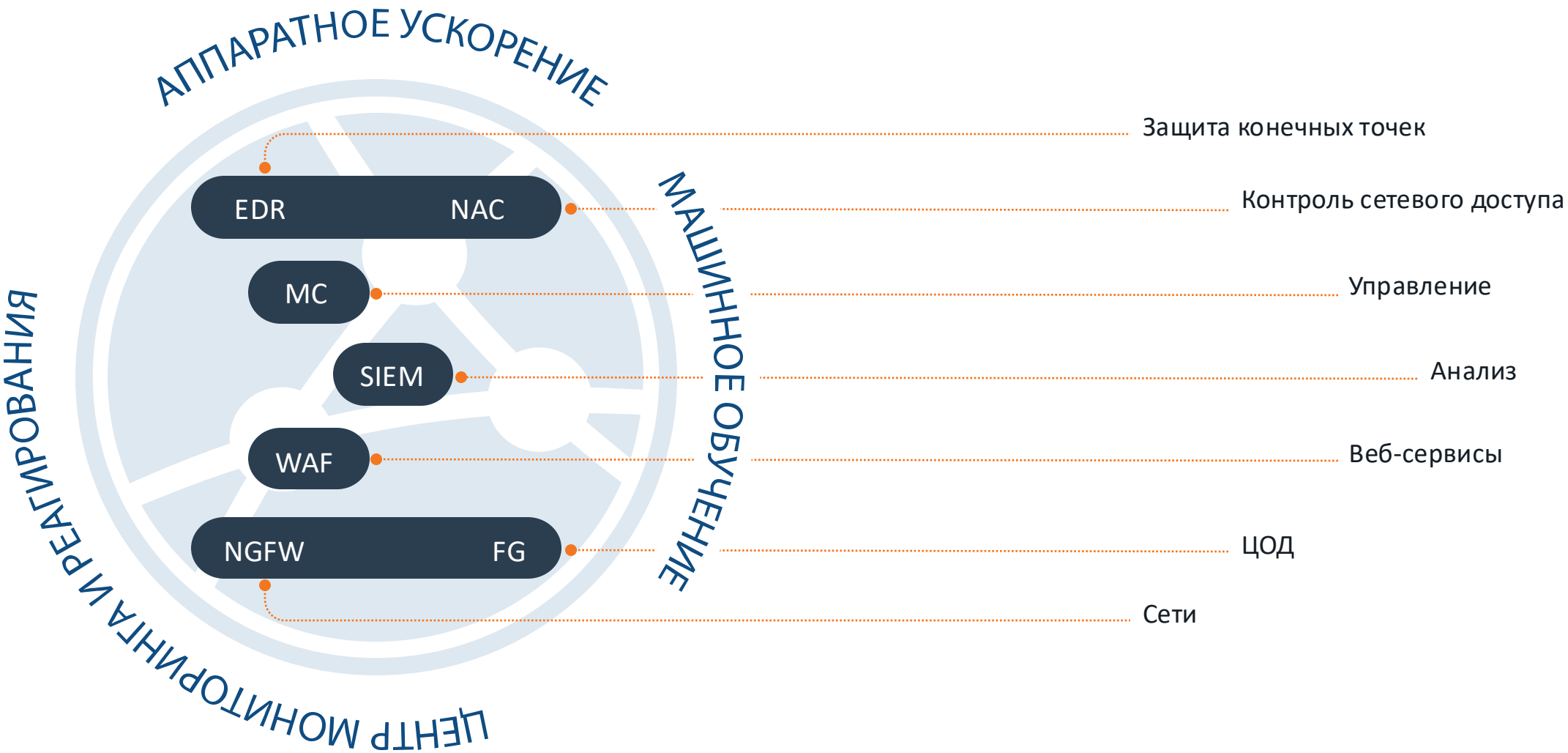
- Минимизировать финансовые потери из-за простоя бизнес-критических сервисов;
- Снизить риск утечки данных;
- Выполнить требования регулятора;
- Получить качественную экспертизу;
- Облегчить работу сотрудников в режиме постоянного дефицита кадров.

SIEM ПОМОЖЕТ

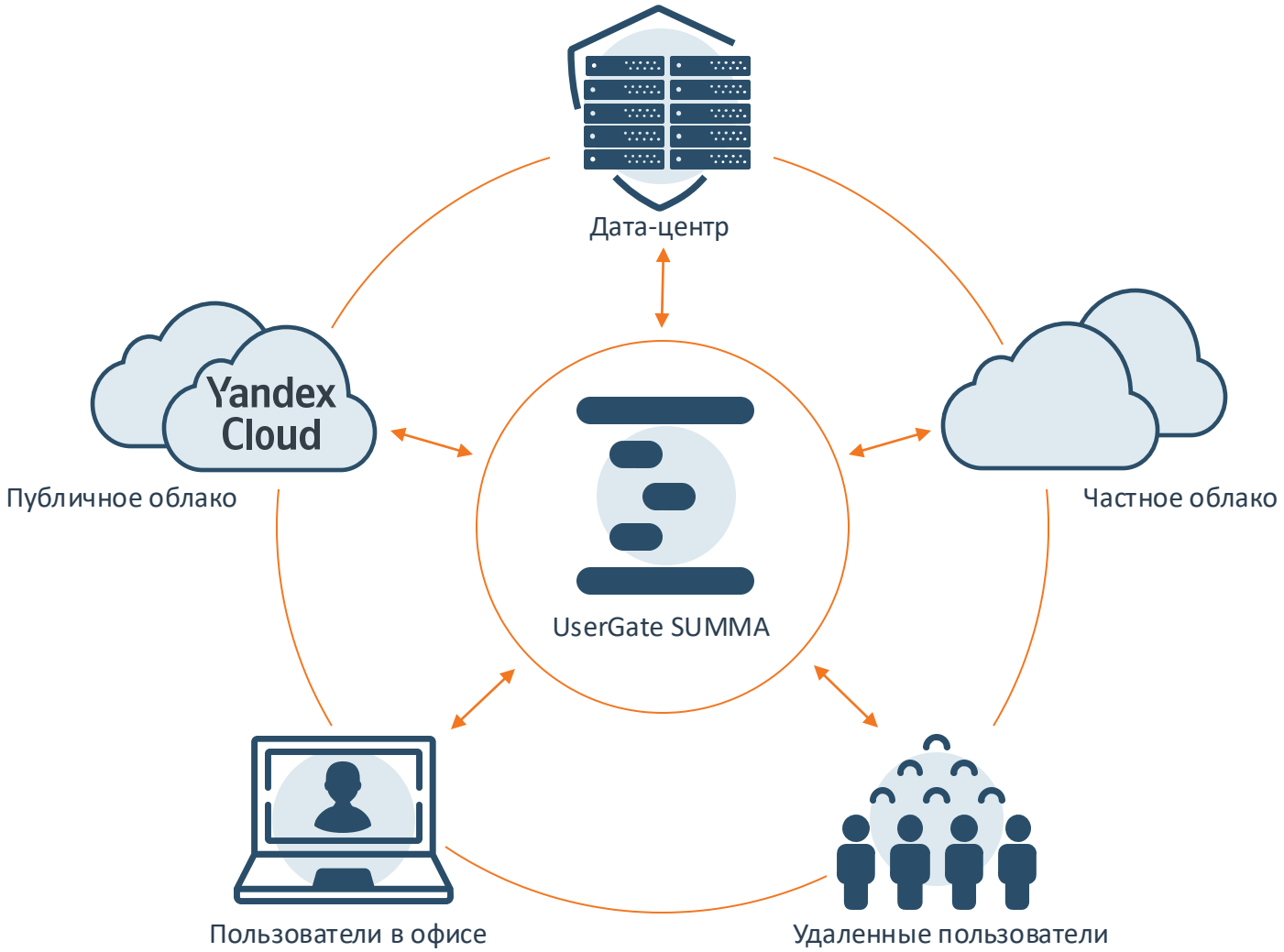
- Обезопасить свою компанию от сложных комплексных атак.
- Своевременно обнаружить инцидент.
- Оперативно реагировать на инцидент.
- Качественно расследовать инцидент.
- Не допустить повторения инцидента.

В РАМКАХ USERGATE SUMMA

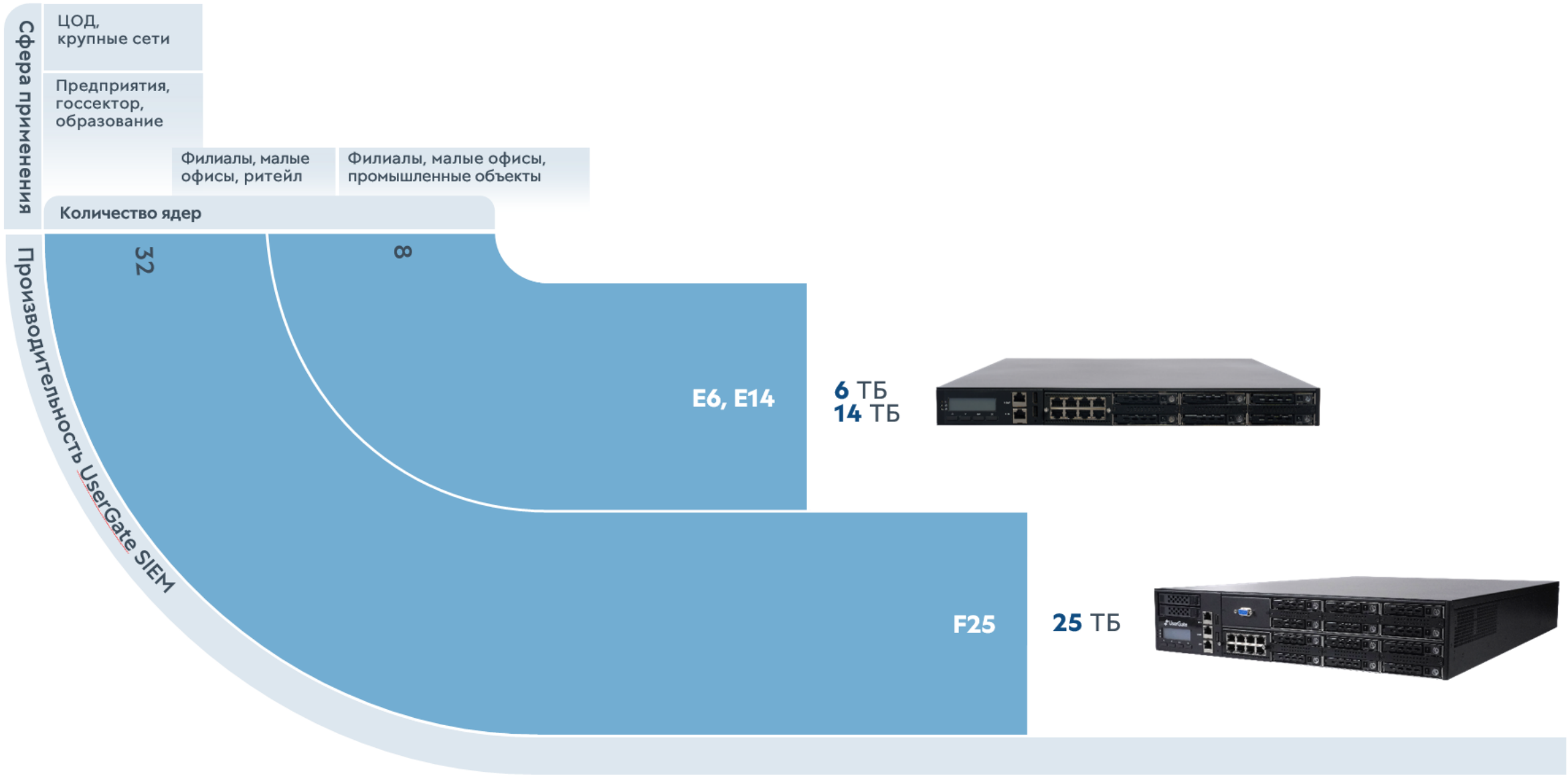
USERGATE SUMMA. 100% ВИДИМОСТЬ СОБЫТИЙ БЕЗОПАСНОСТИ



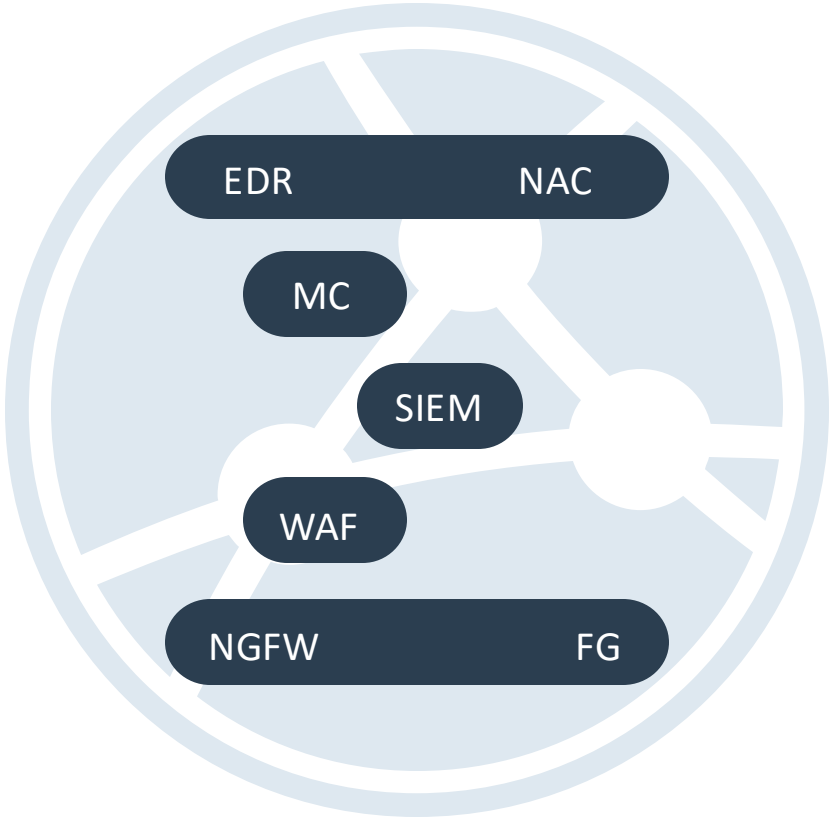
ZERO TRUST NETWORK ACCESS (ZTNA)



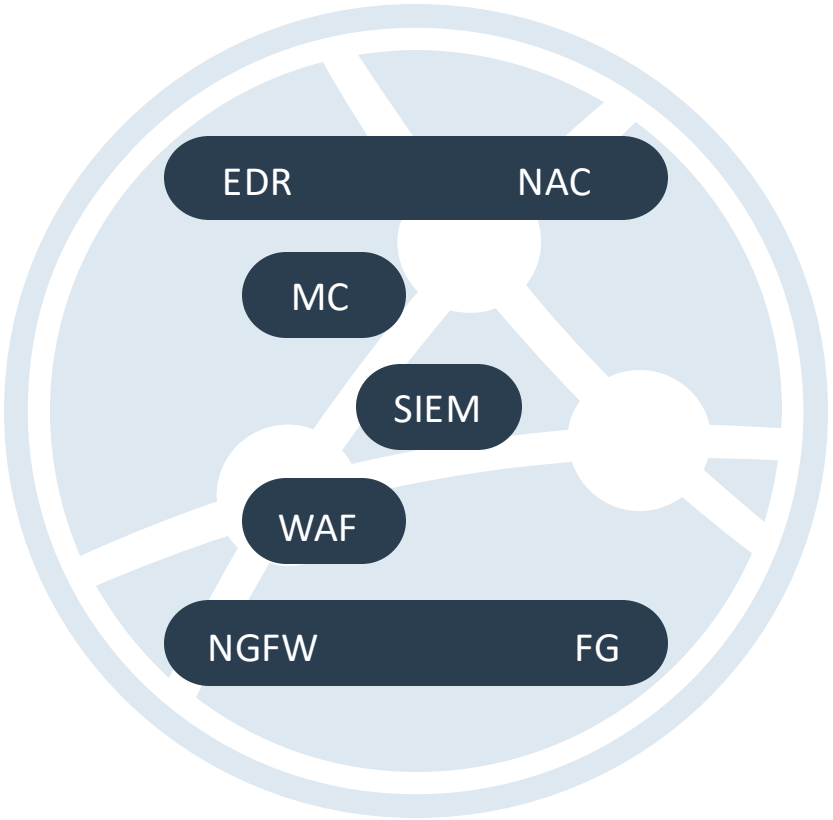
USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ВИРТУАЛЬНОМ ИСПОЛНЕНИИ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ОБЛАЧНОМ ИСПОЛНЕНИИ



В любых облаках, которые поддерживают стандартные реализации vmware и kvm (openstack). Такие как **Yandex Cloud, Beeline cloud, MTC и VK.**

https://www.usergate.com/ru/for-partners/mssp-partners

ПРЕИМУЩЕСТВА

USERGATE SIEM

- 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.

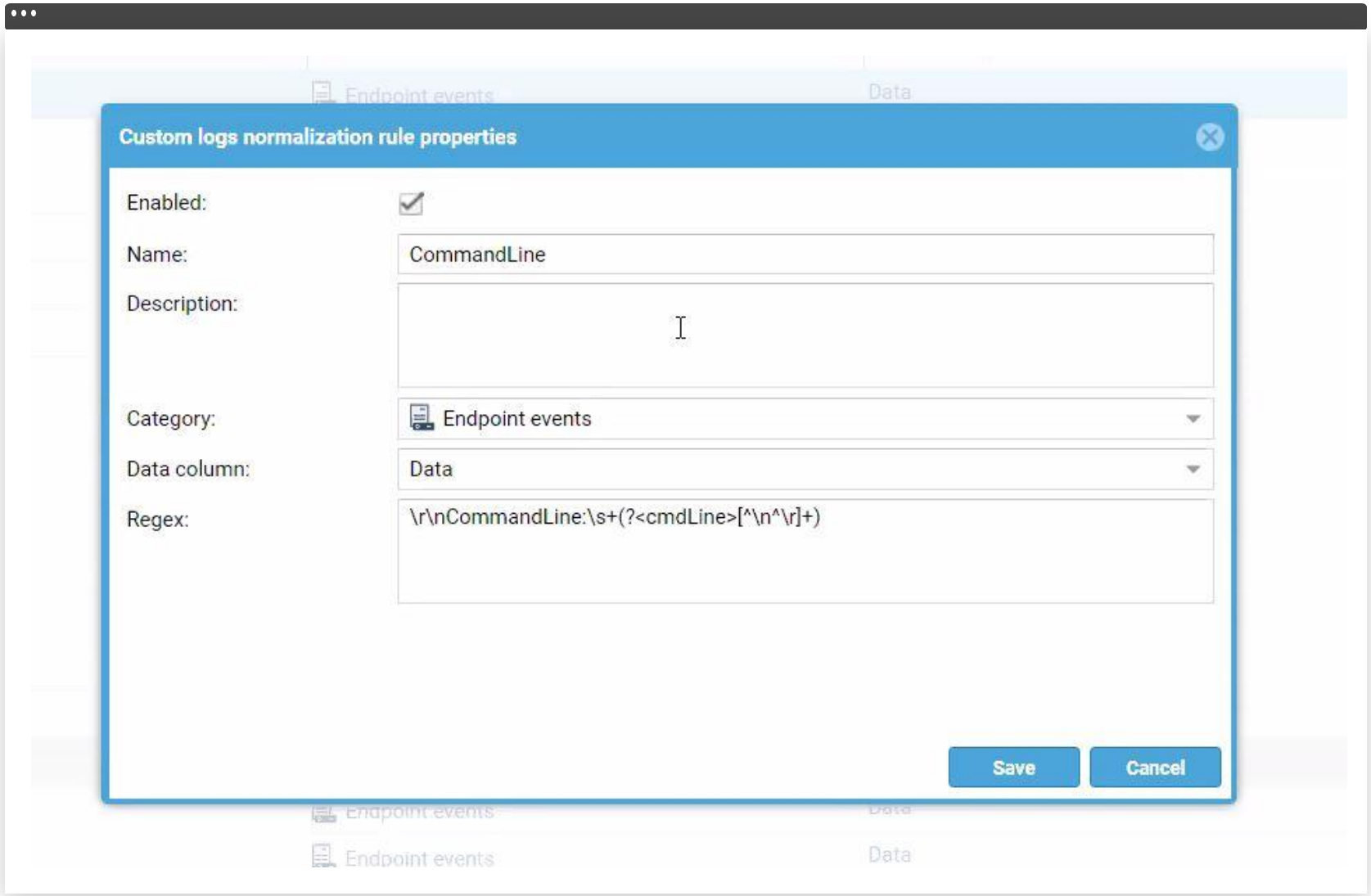
USERGATE SIEM

- Снижение издержек на логирование (журналирование);
- Снижение трудозатрат на обнаружение и анализ инцидентов;
- Повышение эффективности выявления угроз;
- Безопасность и мониторинг облачной инфраструктуры;
- Расширение контроля ИБ в облаке;
- Выгодная стоимость владения;
- Высокая производительность;
- Автоматическое реагирование;
- Повышение продуктивности аналитиков;
- Минимизировать зависимость от нескольких инструментов (продуктов, решений).

СЛЕДСТВИЕ ОТ ВЛАДЕНИЯ USERGATE SIEM

- Сотрудники лучше узнают инфраструктуру компании;
- Выстроенные регламенты и требования;
- Своевременная реакция на инцидент;
- Выстроенные процессы автоматизации реагирования на инциденты.

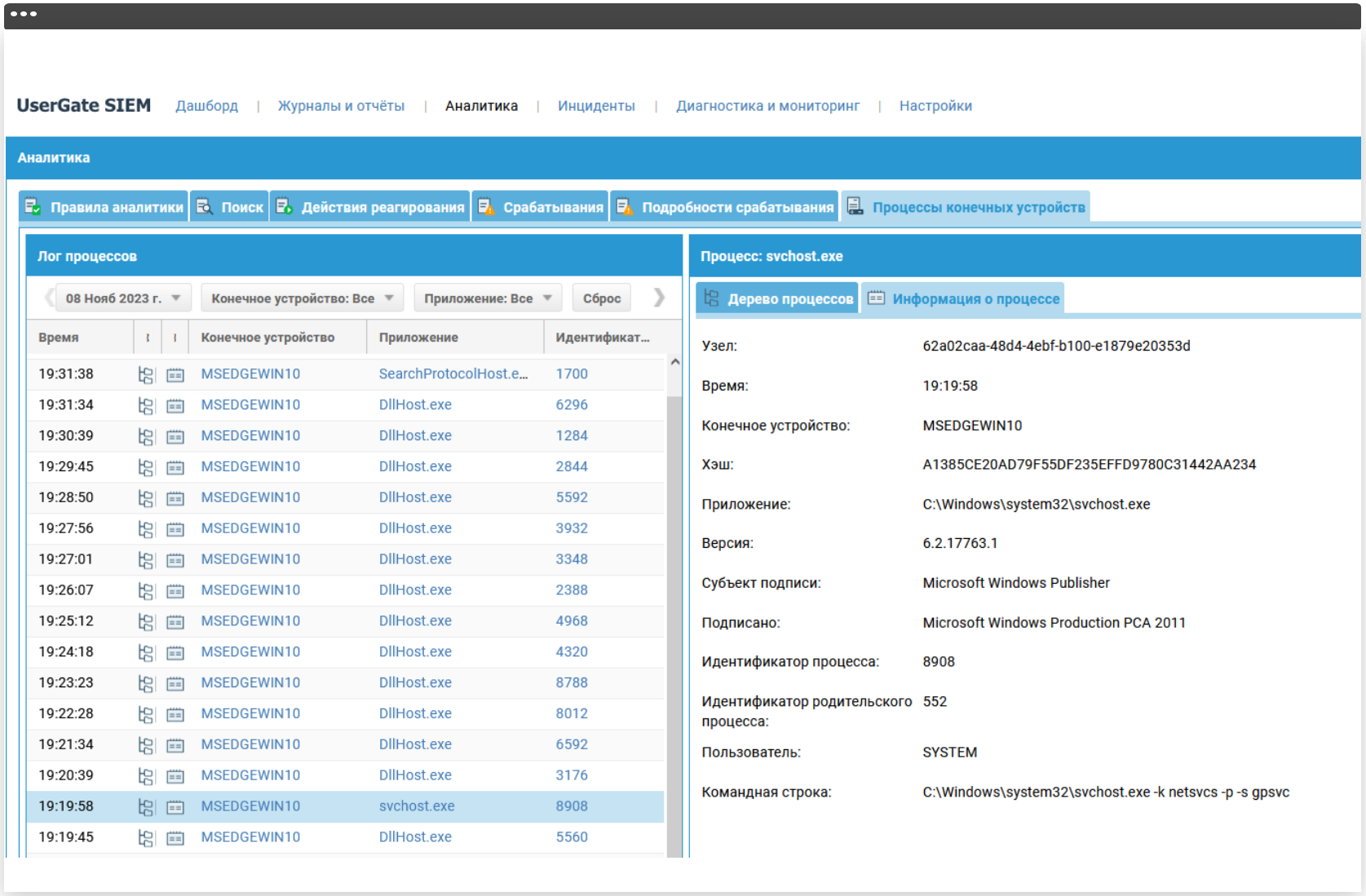
ПОЛЬЗОВАТЕЛЬСКАЯ НОРМАЛИЗАЦИЯ



ПРОЦЕССЫ КОНЕЧНЫХ УСТРОЙСТВ

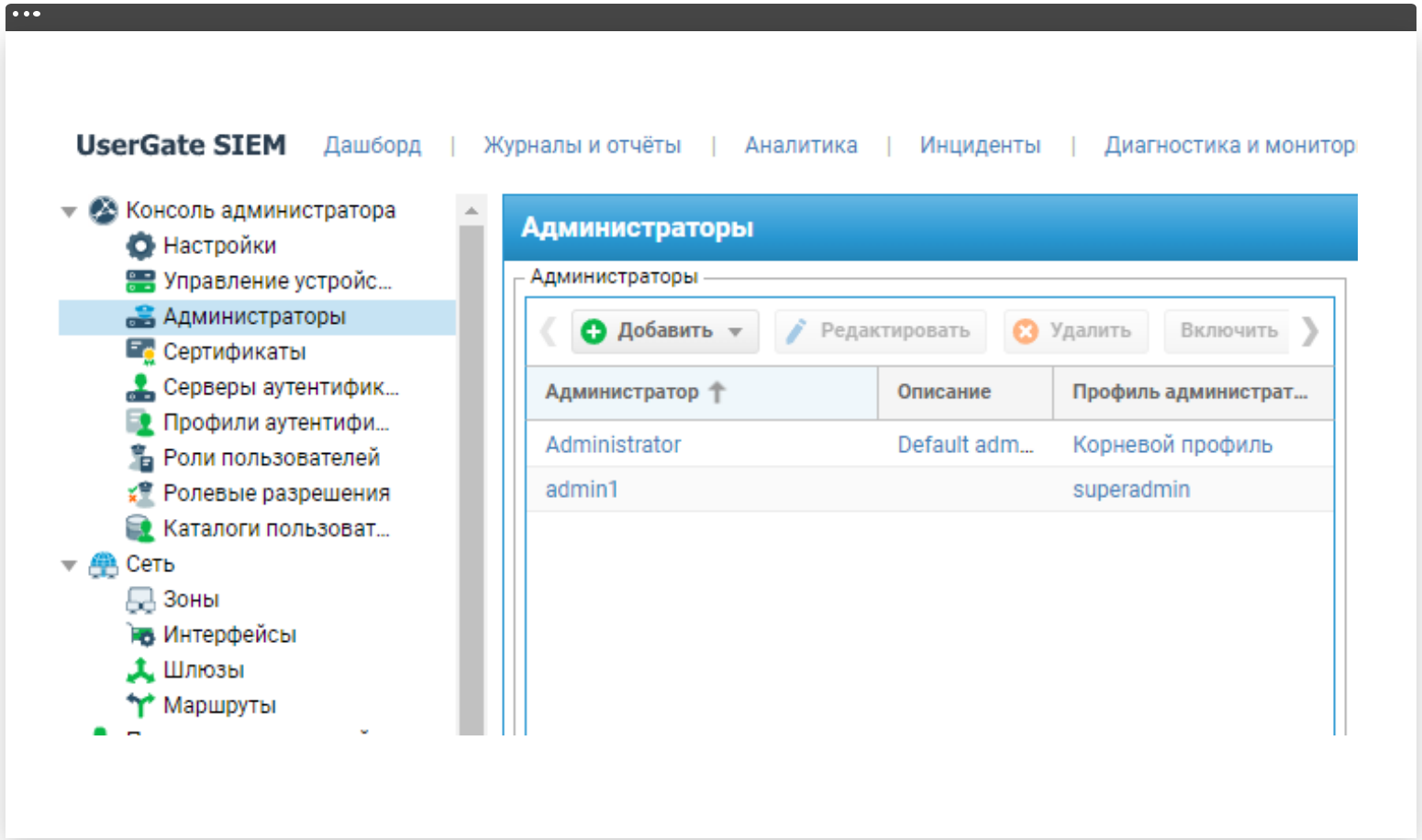
В разделе аналитики добавлены журналы о процессах на конечных устройствах.

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 SIEM

01

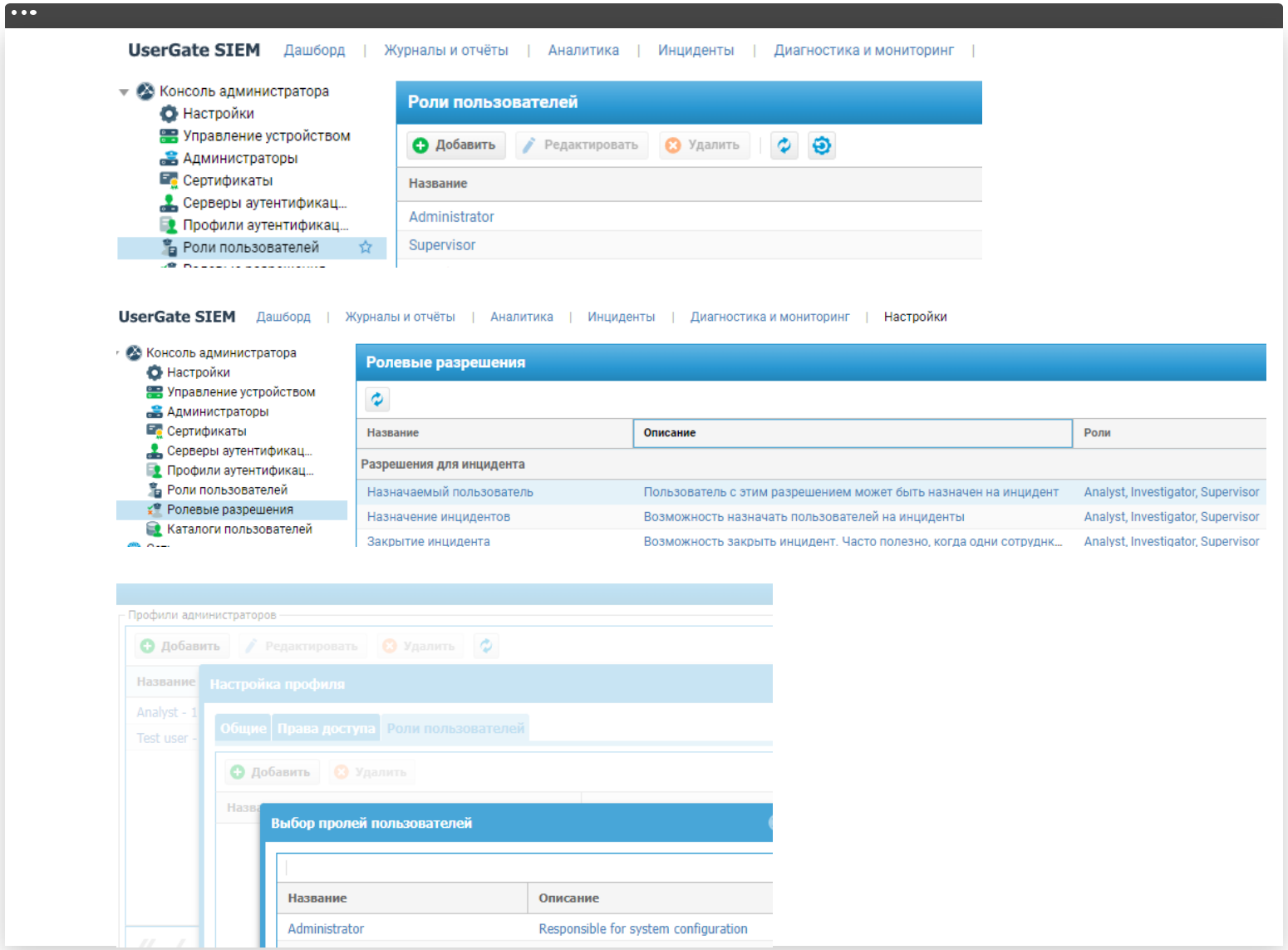
Роли пользователей

02

Ролевые разрешения

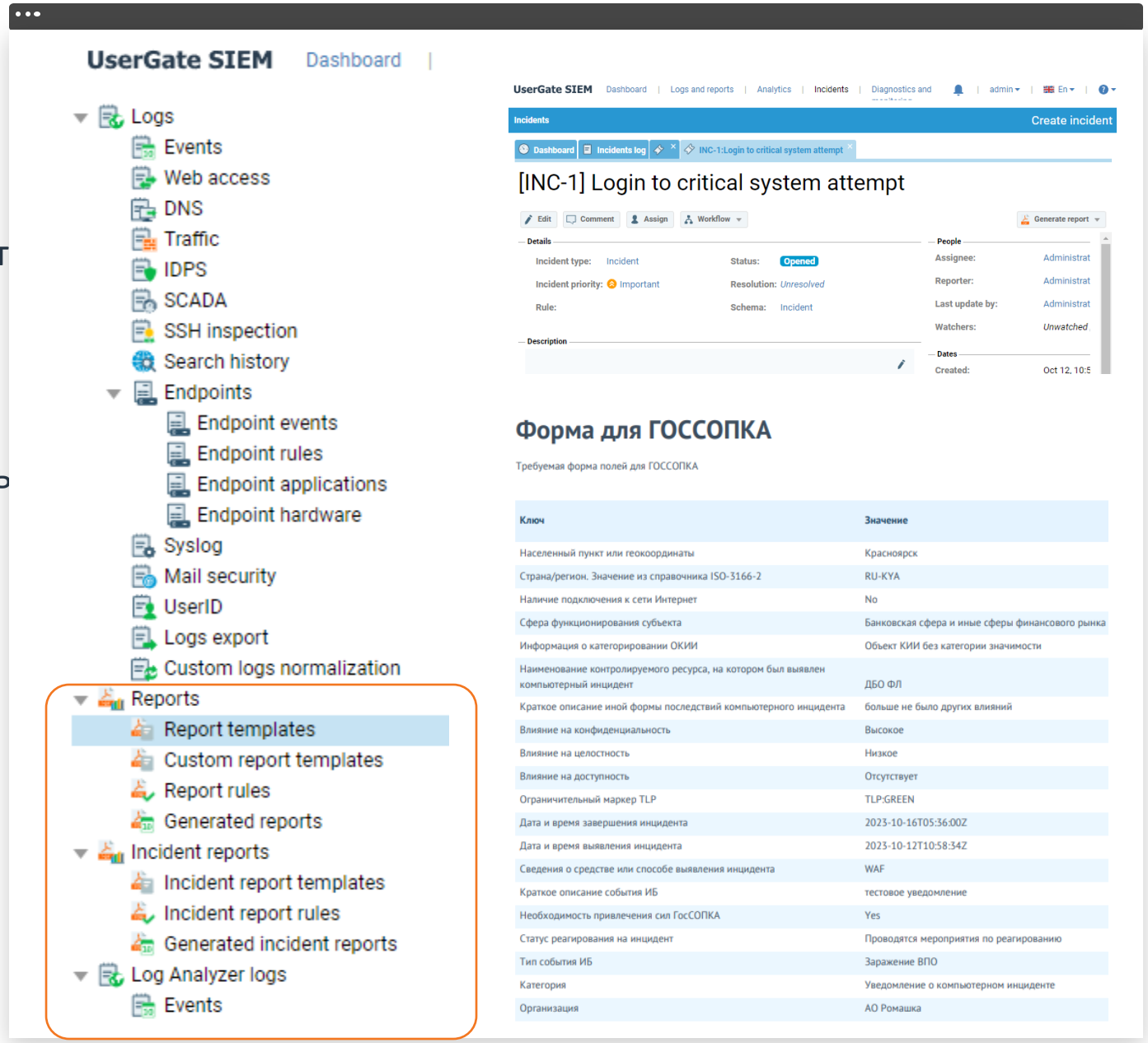
03

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.
- Как следствие - возможность реагирования прямо «из коробки».
- Готовое решение «из коробки» с простотой установки, настройки и эксплуатации.
- Возможность создавать пользовательские правила нормализации событий.
- Простой язык создания правил корреляции. Меньше требований к знаниям.
- Возможность обогащения инцидента информацией из сторонних баз и из нашей библиотеки.
- Что приводит к экономии бюджета на стороннем IRP/SOAR решении и дорогостоящем персонале.

- Интеграция с ГосСОПКА.

СПАСИБО ЗА ВНИМАНИЕ

Алексей Афанасьев
Менеджер по развитию UserGate SIEM