UserGate

СОВРЕМЕННЫЙ ПОДХОД К РАЗРАБОТКЕ SIEM-СИСТЕМЫ НА ПРИМЕРЕ USERGATE SIEM

Дмитрий Чеботарёв
Менеджер по развитию UserGate SIEM

UserGate

Делаем безопасное настоящим

USERGATE. ИСТОРИЯ УСПЕХА

UserGate

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

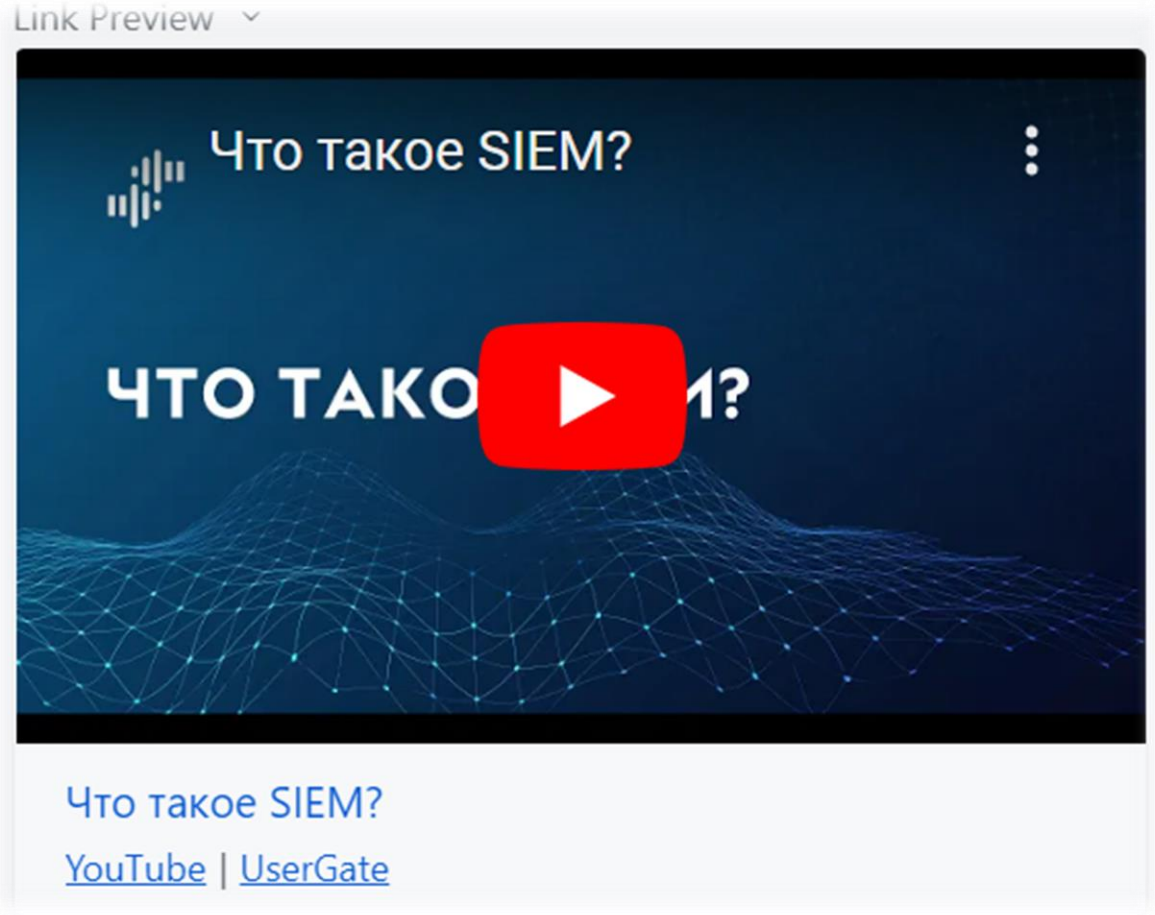
2024

Выпуск первого в России экосистемного SIEM с функциональностью IRP/SOAR

ЧТО ТАКОЕ SIEM?

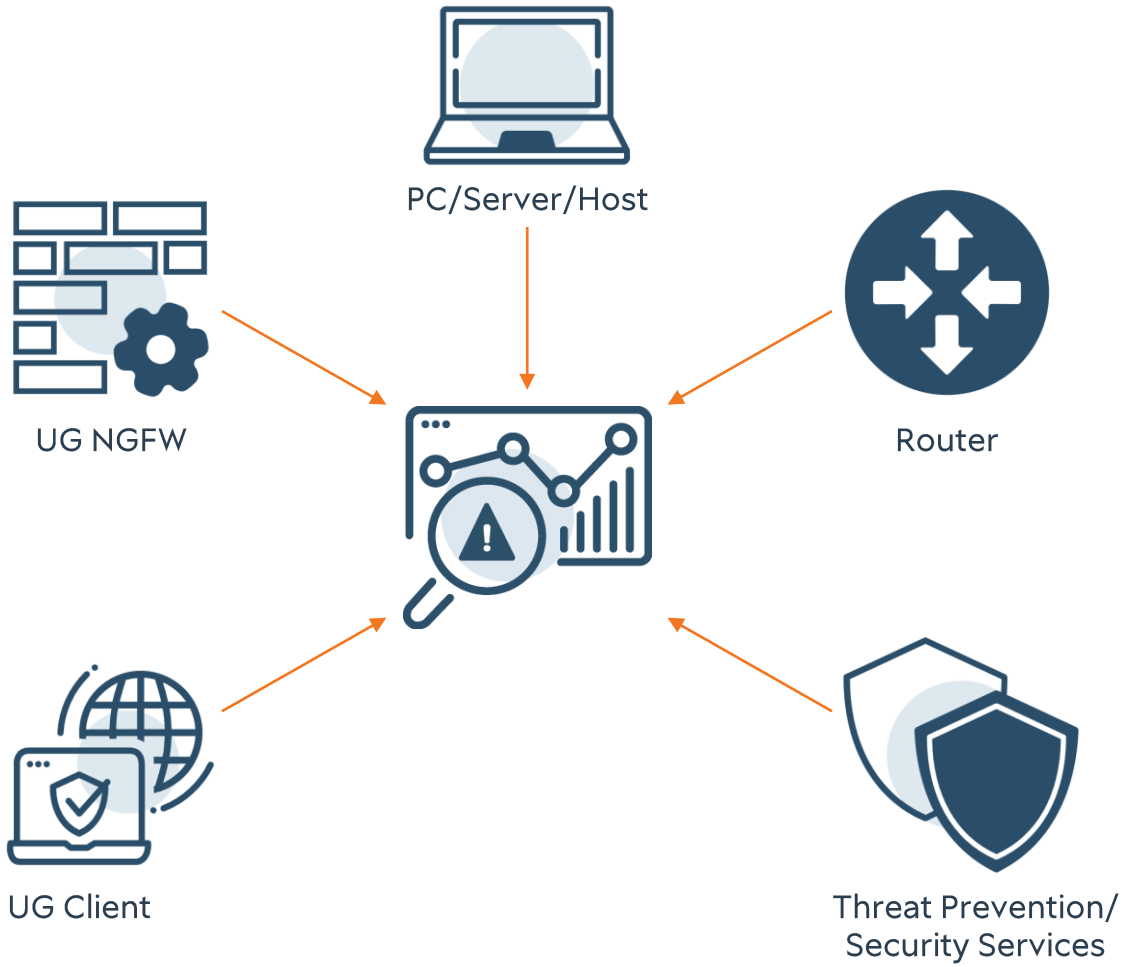
ЧТО ТАКОЕ SIEM?

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



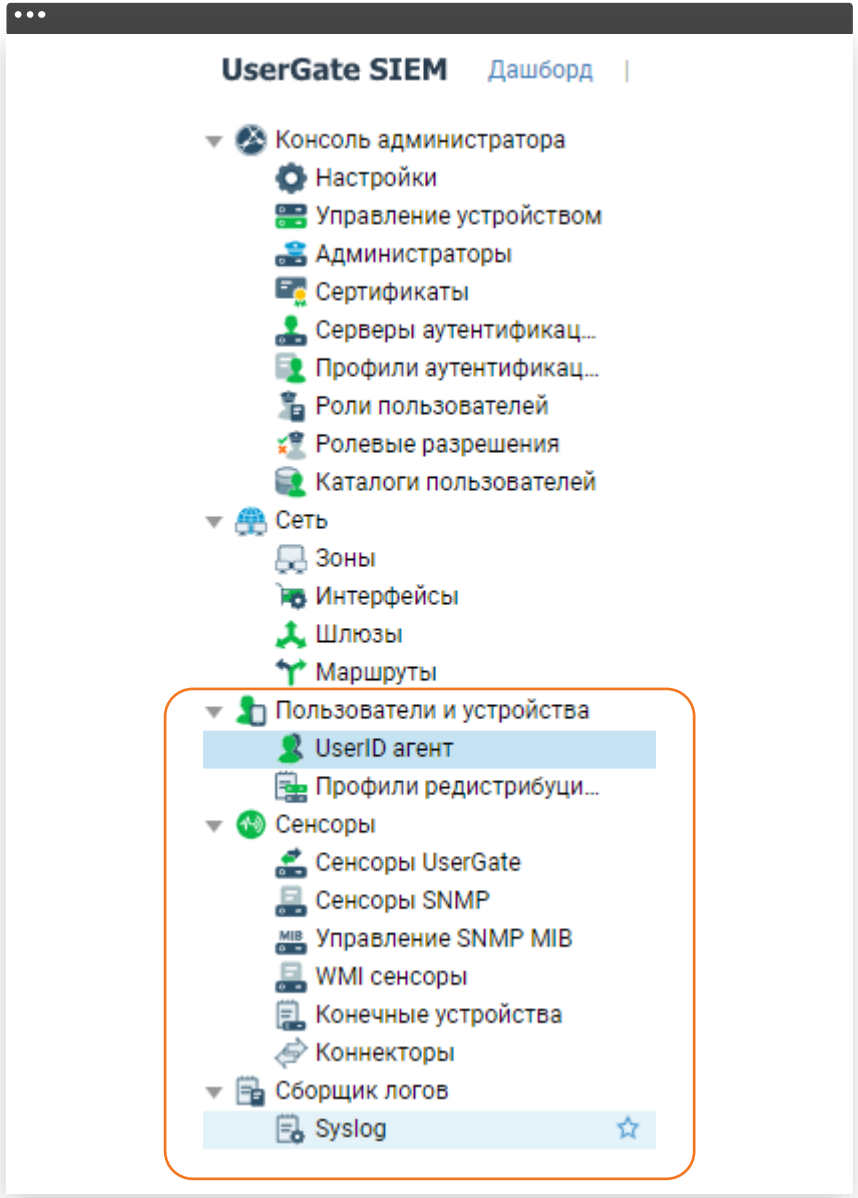
https://www.youtube.com/watch?v=ddAzEN1iC5o
https://vkvideo.ru/video-211747929_456239139
https://rutube.ru/video/1d4c3321f002d531a6ef9cbd765fedf4/

СБОР ДАННЫХ И НОРМАЛИЗАЦИЯ

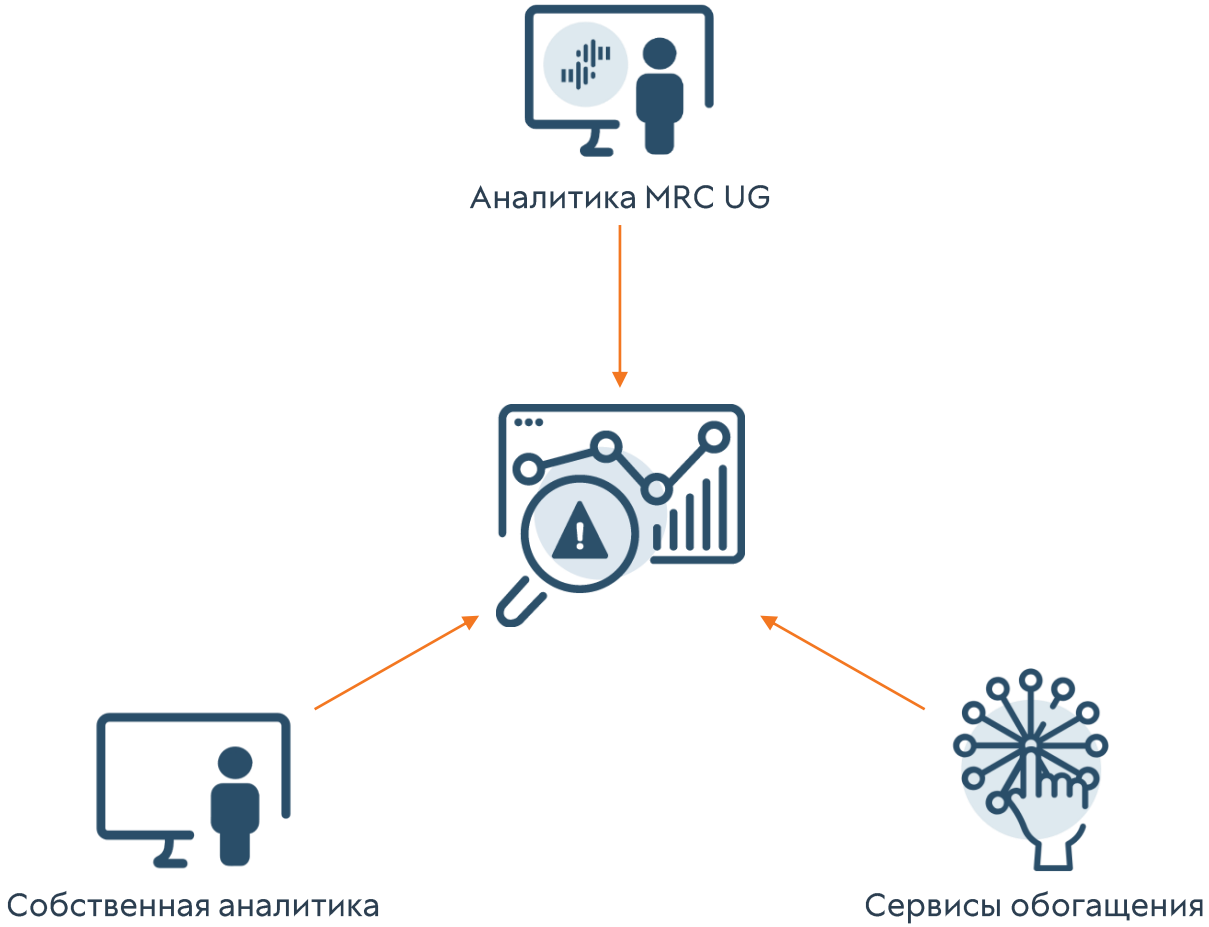


ИСТОЧНИКИ

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

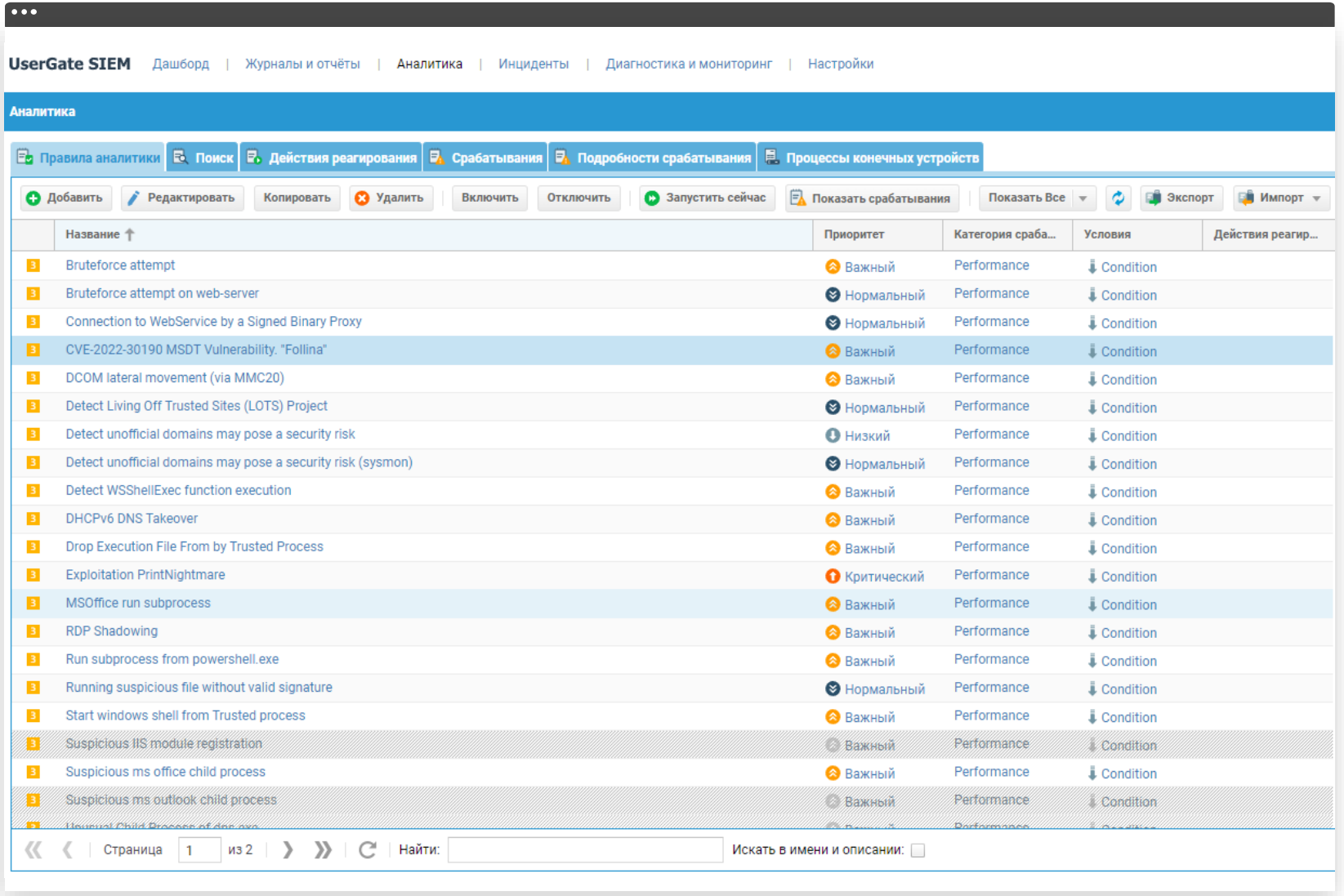


АНАЛИЗ И КОРРЕЛЯЦИЯ

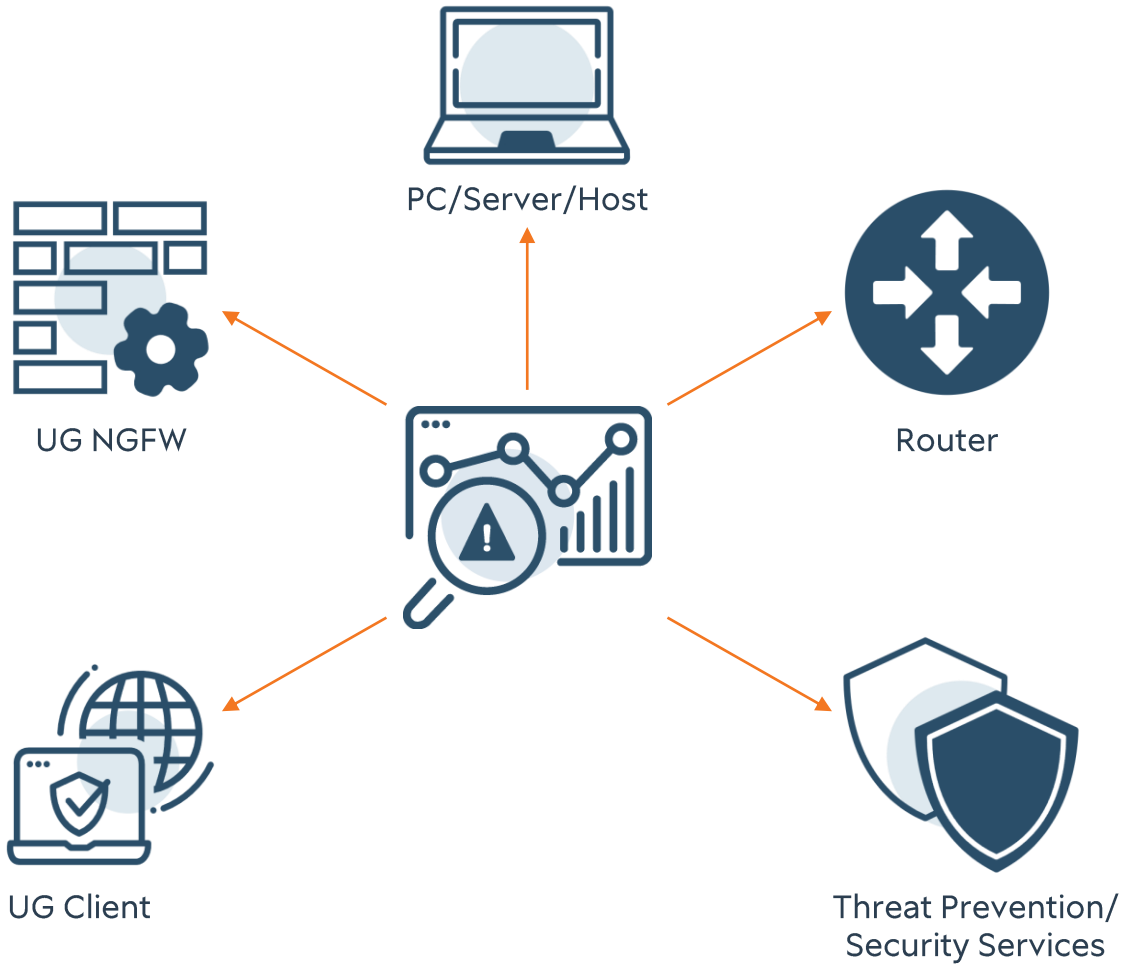


ПРАВИЛА АНАЛИТИКИ

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

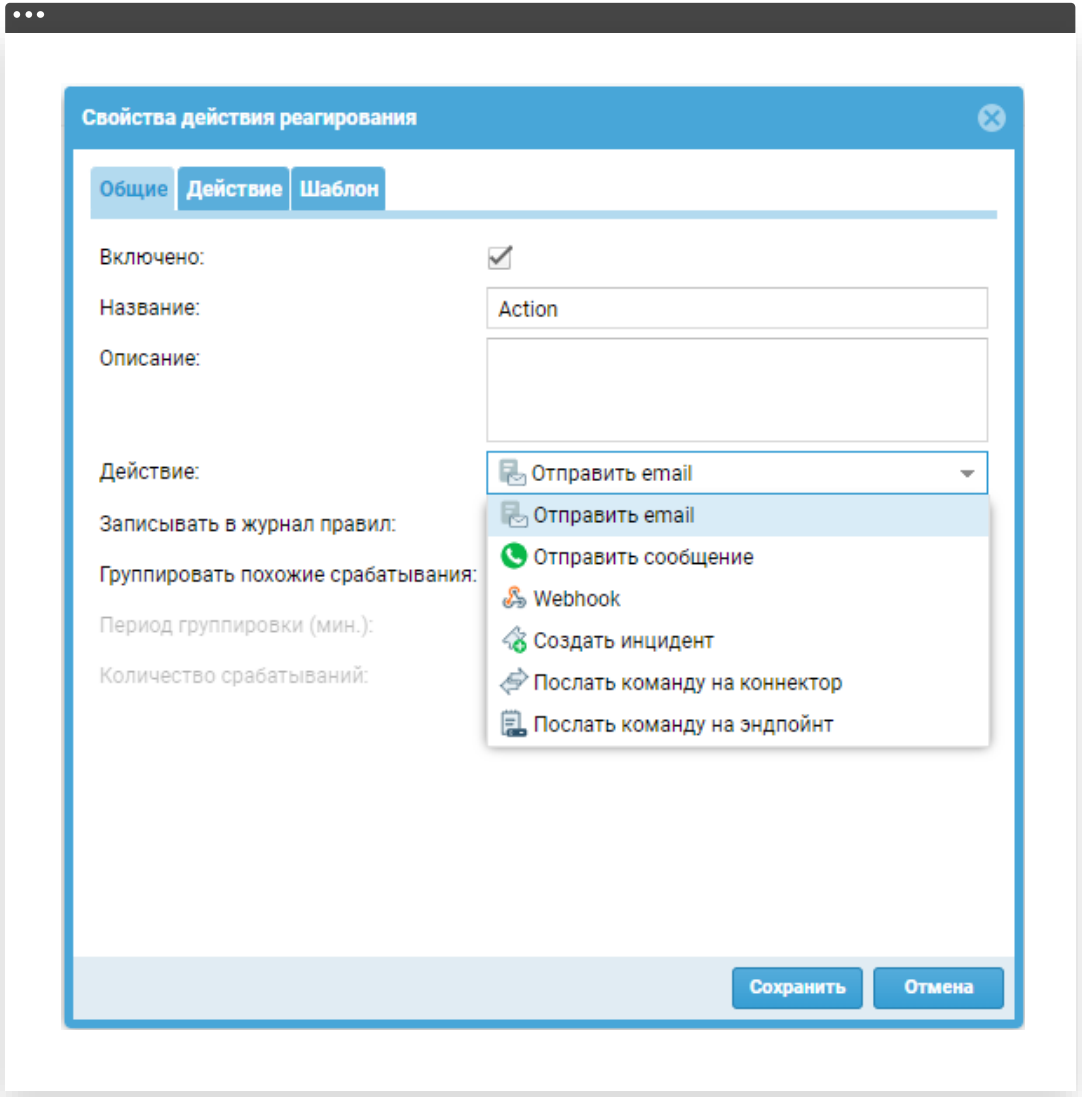


РЕАГИРОВАНИЕ



РЕАГИРОВАНИЕ ЧЕРЕЗ ИНФРАСТРУКТУРУ

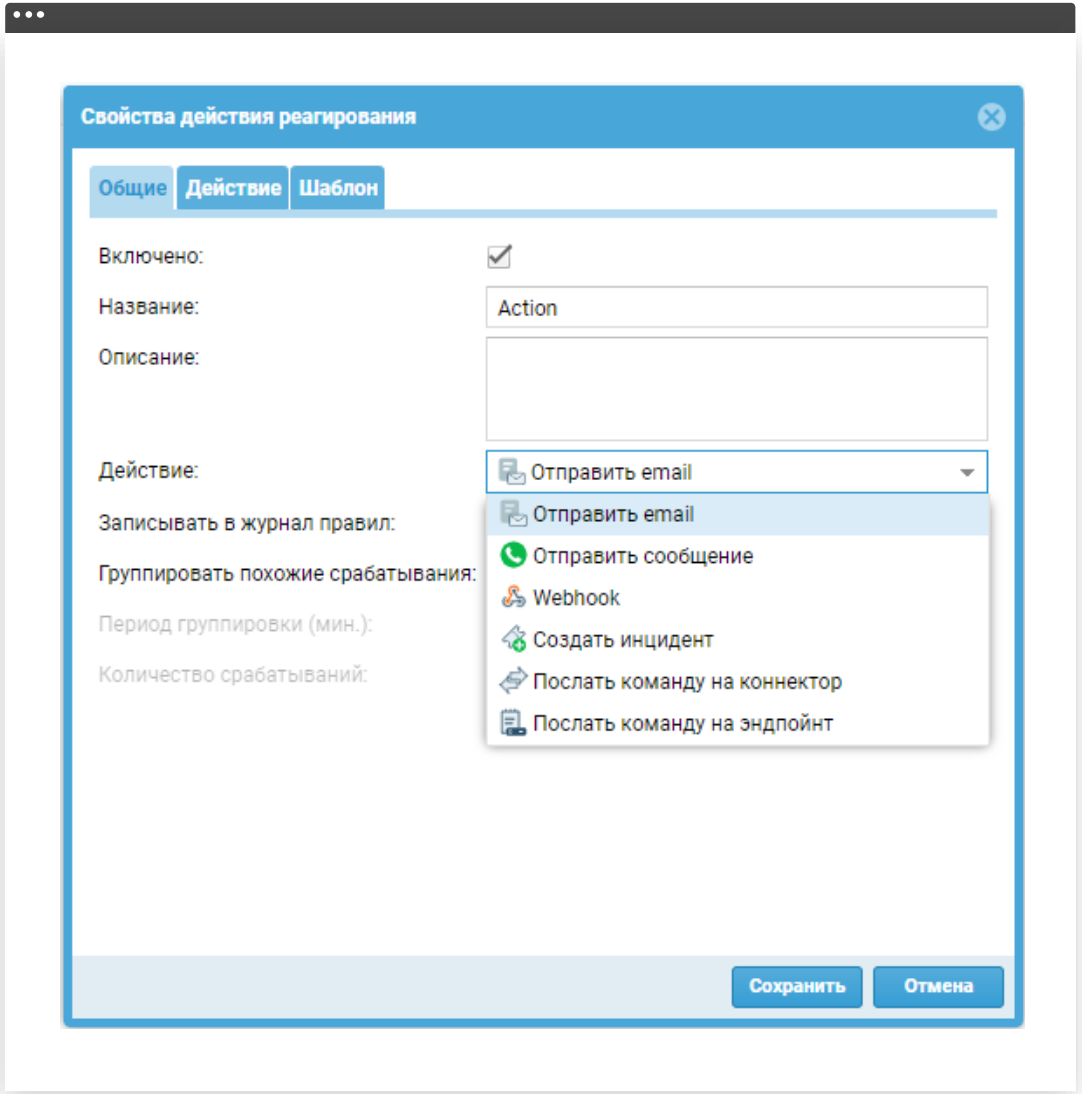
- Отправка команд через SSH/HTTP/HTTPS.
- Возможность передачи в команде артефактов, например IP-адресов.
- Возможность отправки команд на устройства других производителей (коммутаторы, маршрутизаторы и др.)

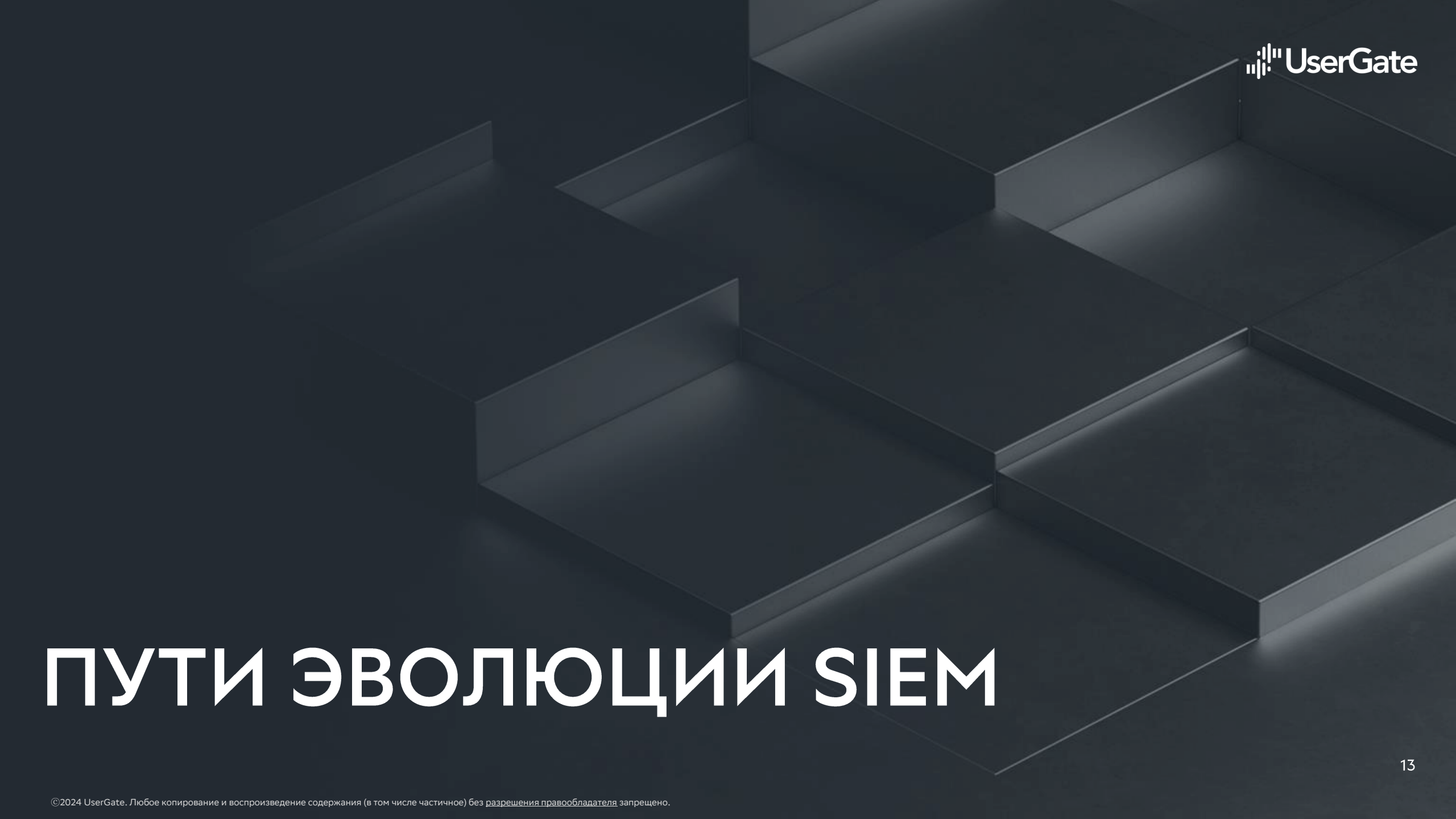


ВАРИАНТЫ РЕАГИРОВАНИЯ

- Оповещение e-mail/СМС/ 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?

Где взяли экспертизу?

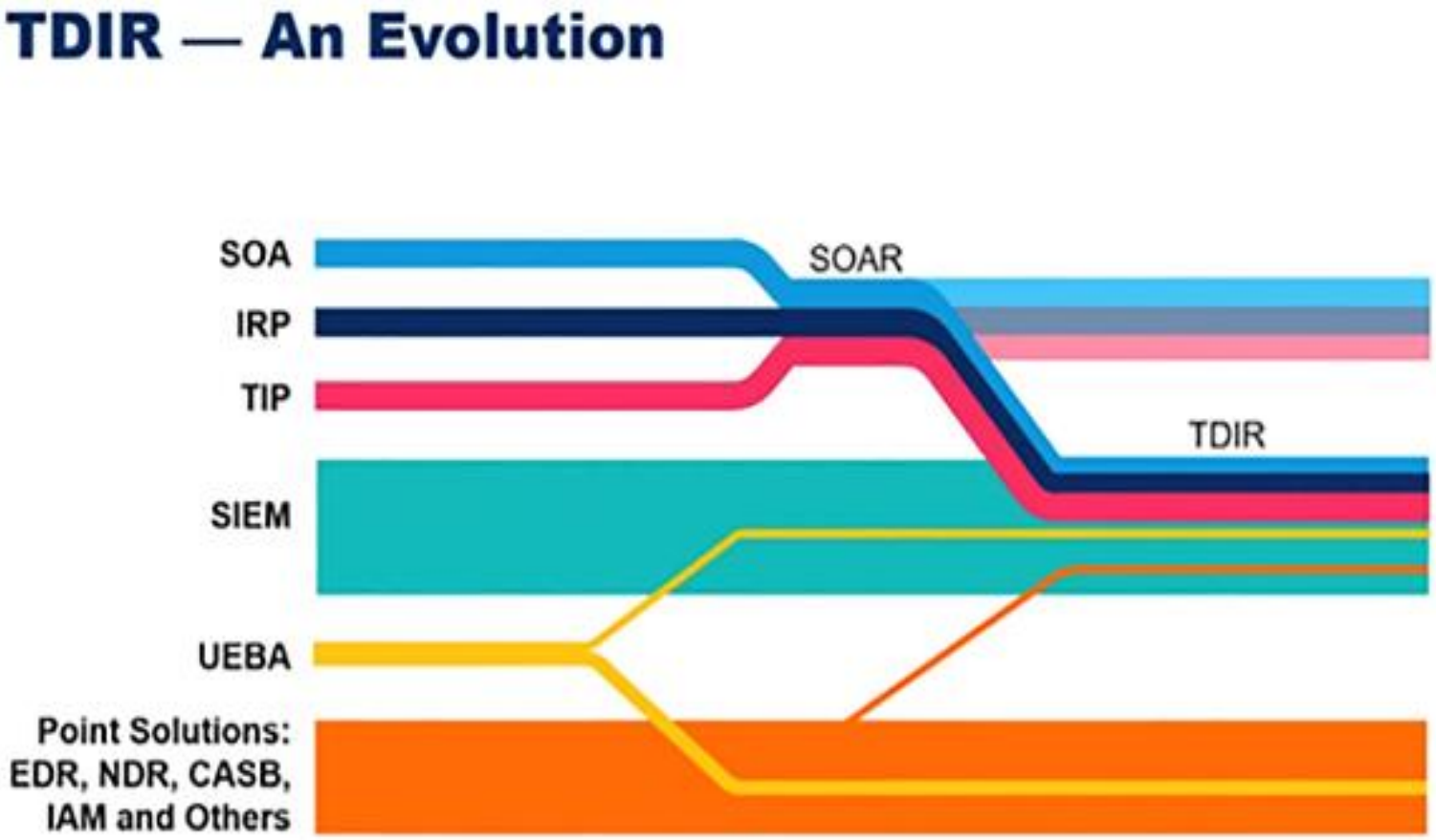
Сами написали

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.

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!



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.

SIEM ПОМОЖЕТ

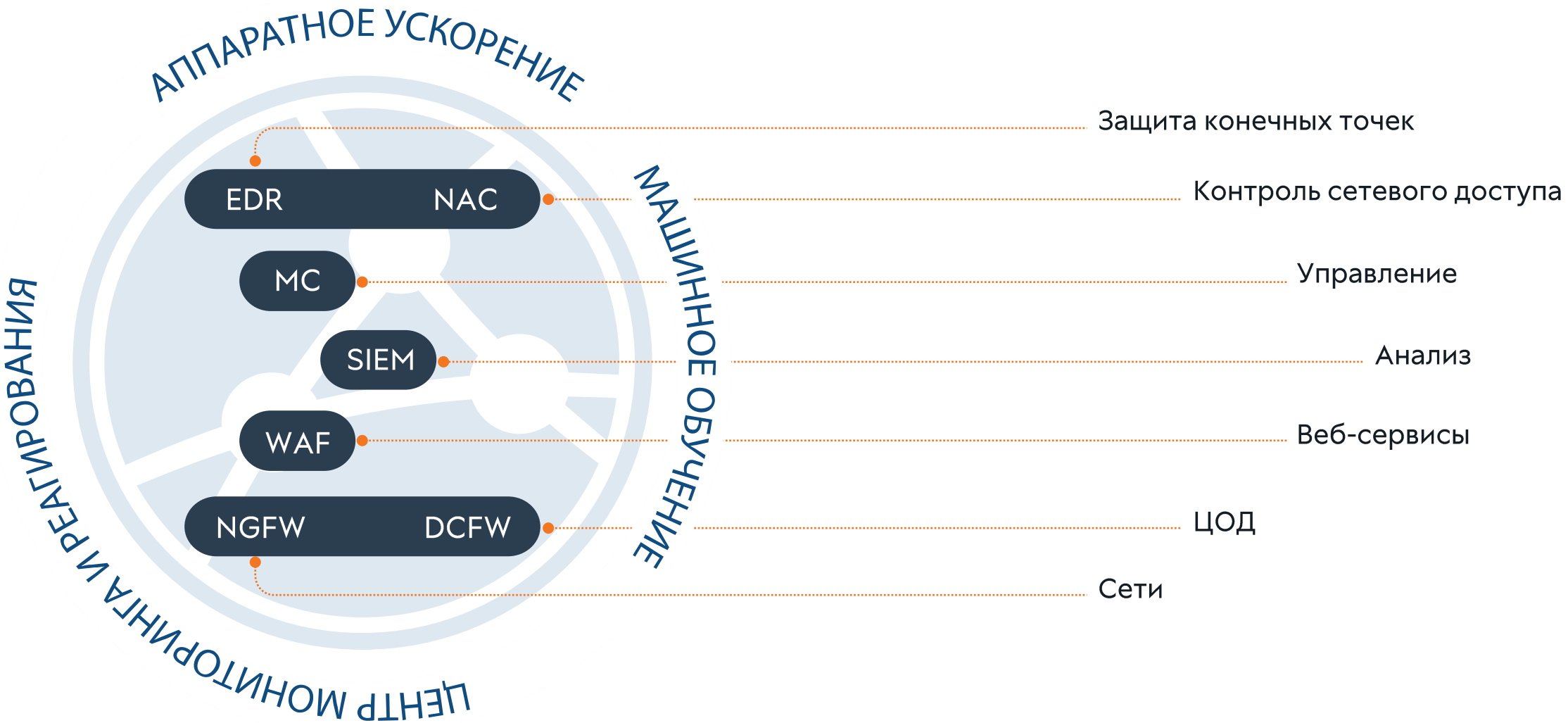
- Получить стабильно работающий продукт;
- Быстрая и качественная тех. поддержка;
- Возможность подготовки отчетов для руководства;
- «Безболезненные» обновления.

UserGate

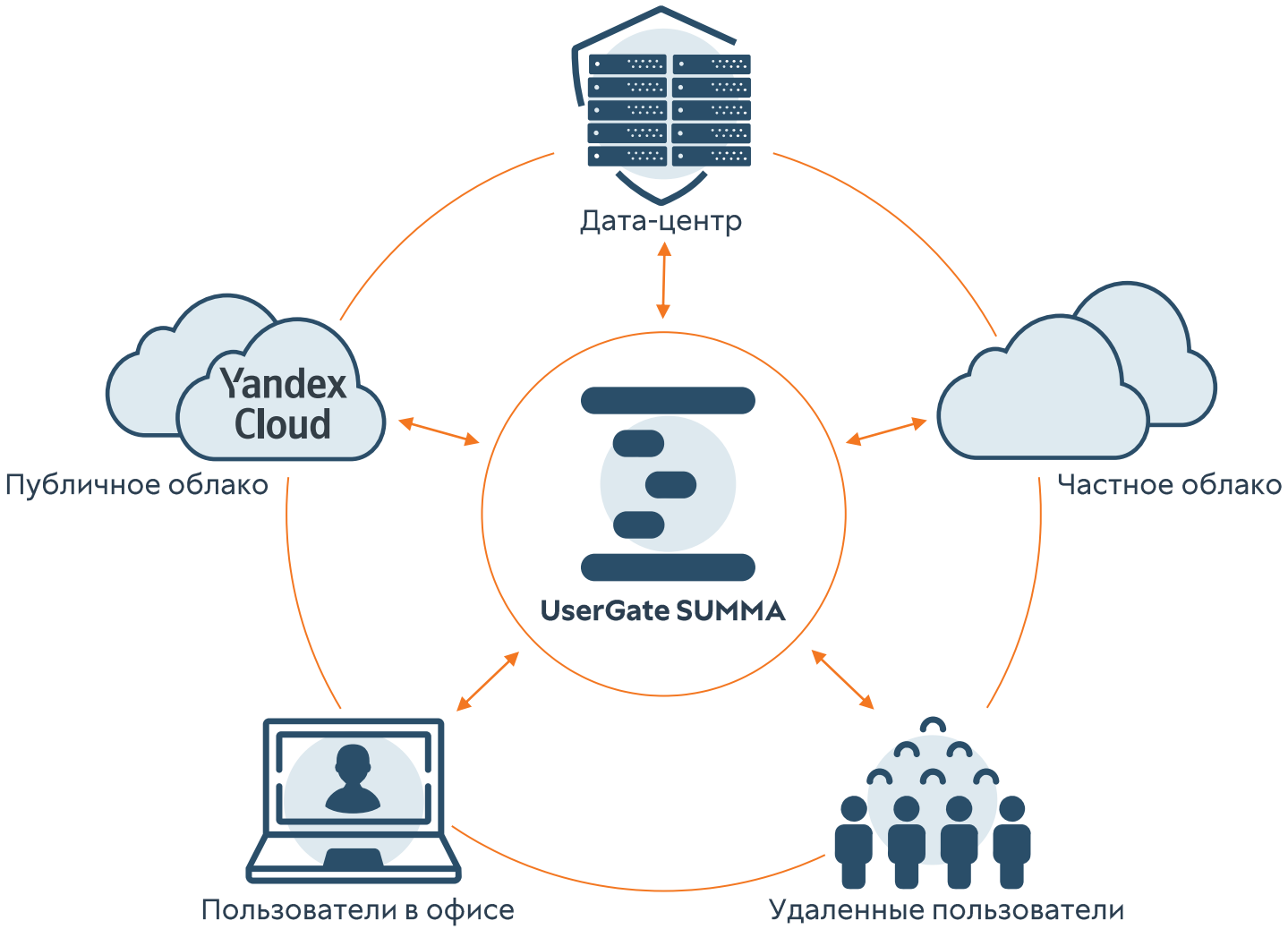
Защита цифрового мира технологиями, которым доверяют без границ

В РАМКАХ USERGATE SUMMA

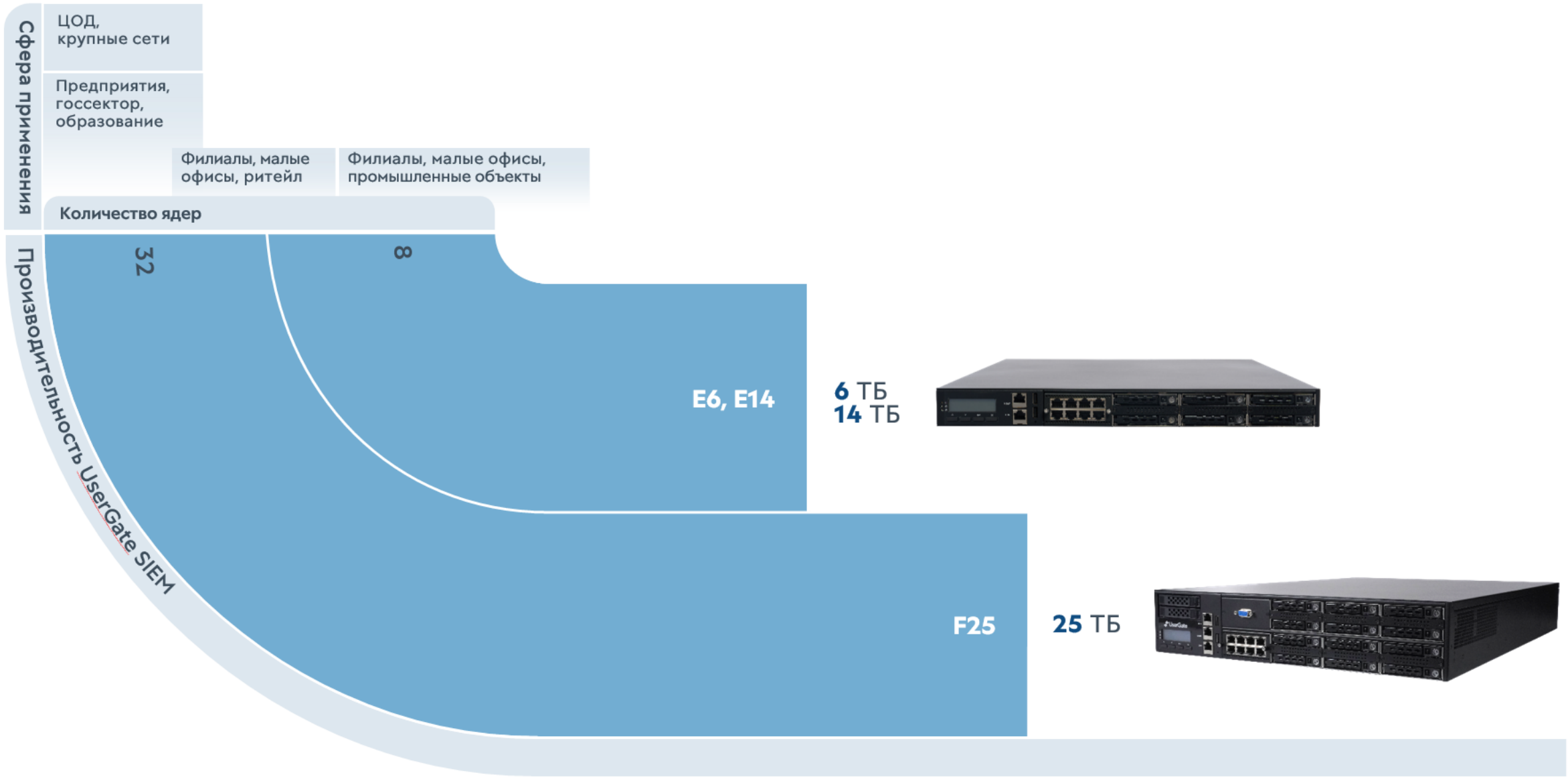
USERGATE SUMMA. 100% ВИДИМОСТЬ СОБЫТИЙ БЕЗОПАСНОСТИ



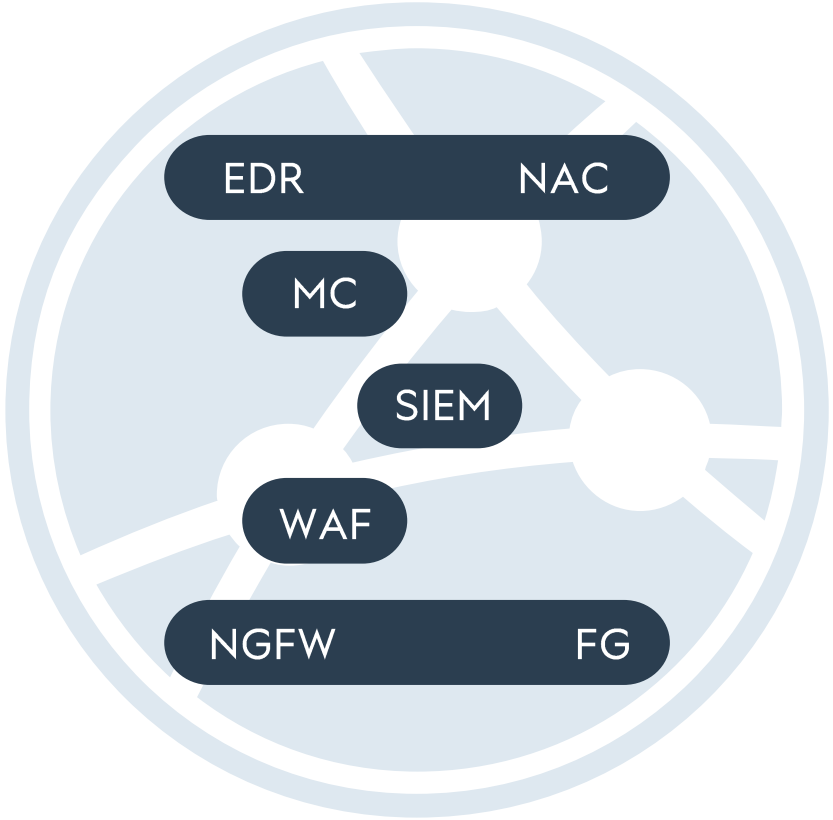
ZERO TRUST NETWORK ACCESS (ZTNA)



USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



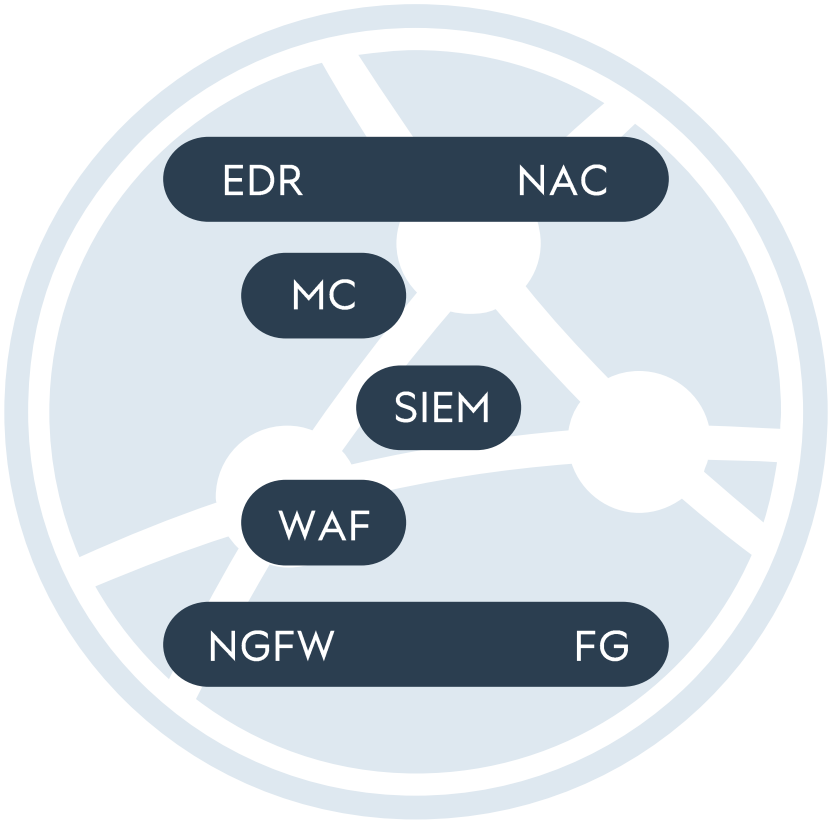
ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ВИРТУАЛЬНОМ ИСПОЛНЕНИИ



Гипервизоры

Xen
vmware
Hyper-V
БРЕСТ
ROS ПЛАТФОРМА
base alt
VirtualBox
openstack.
РЕД ВИРТУАЛИЗАЦИЯ
KVM
ГОРИЗОНТ-ВС ЦИФРОВОЕ БУДУЩЕЕ НАЧИНАЕТСЯ СЕГОДНЯ
zVirt

ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ВИРТУАЛЬНОМ 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

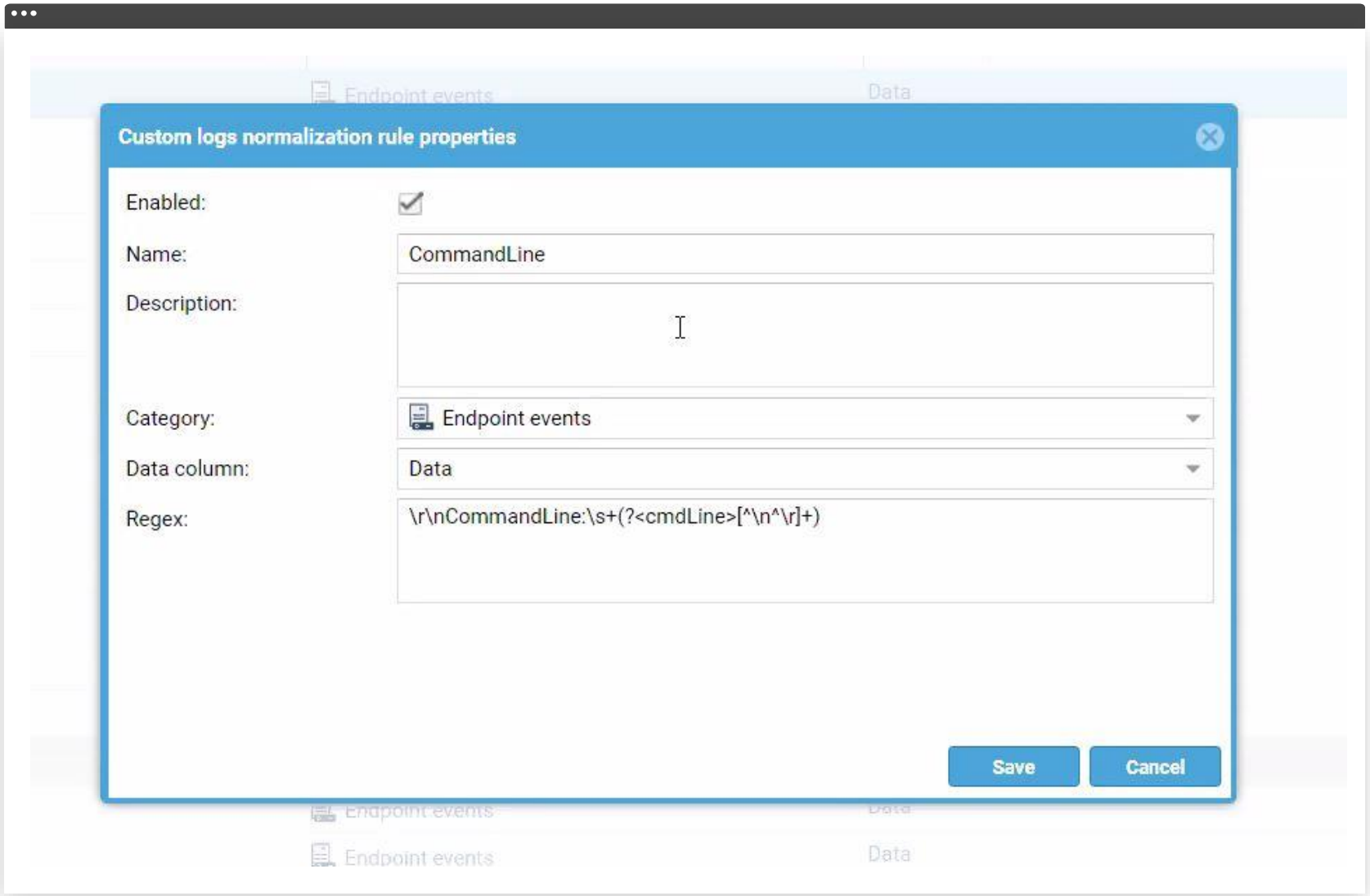
ПРЕИМУЩЕСТВА

USERGATE SIEM

- 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.

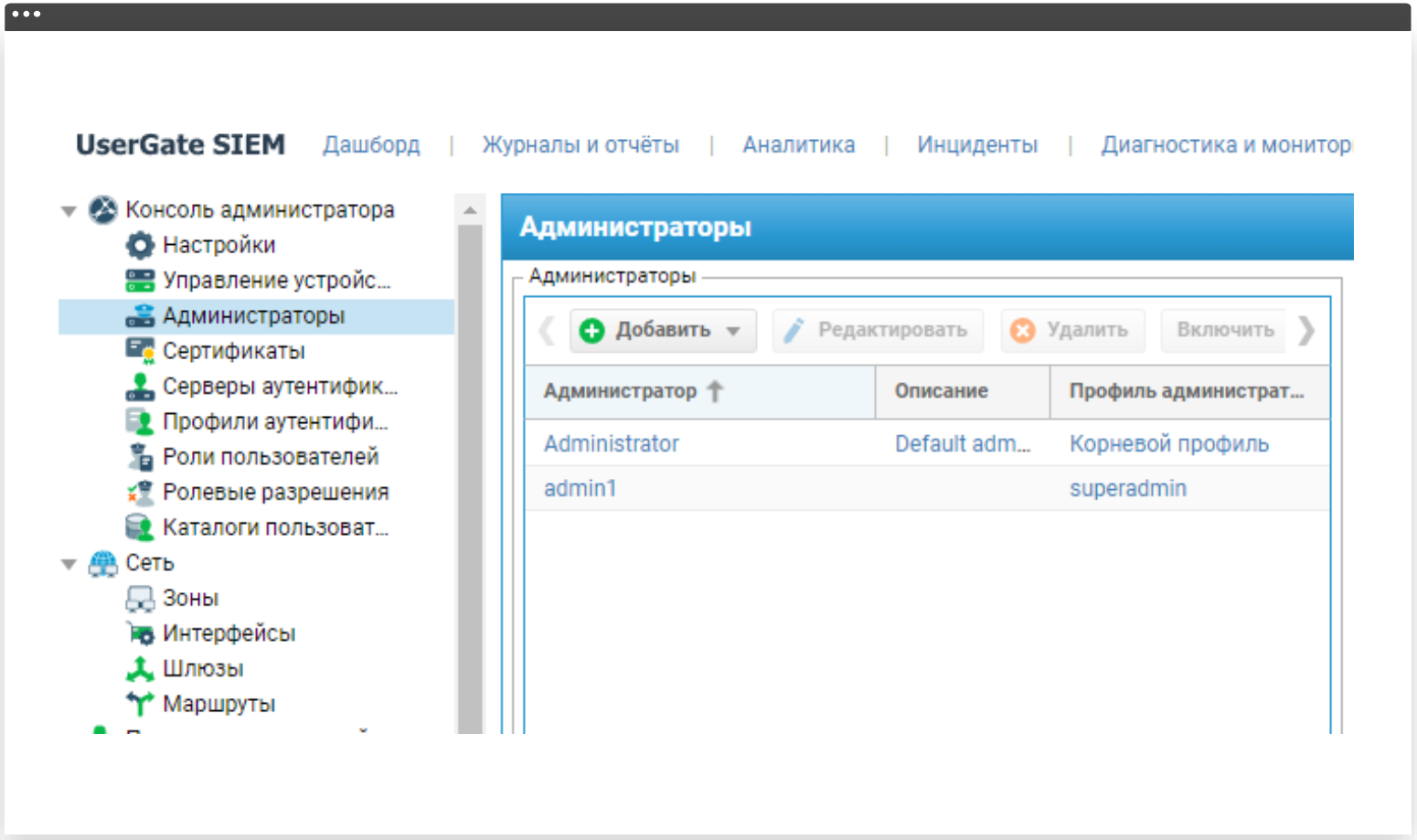
- Интеграция с ГосСОПКА.

ПОЛЬЗОВАТЕЛЬСКАЯ НОРМАЛИЗАЦИЯ



АДМИНИСТРАТОРЫ

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

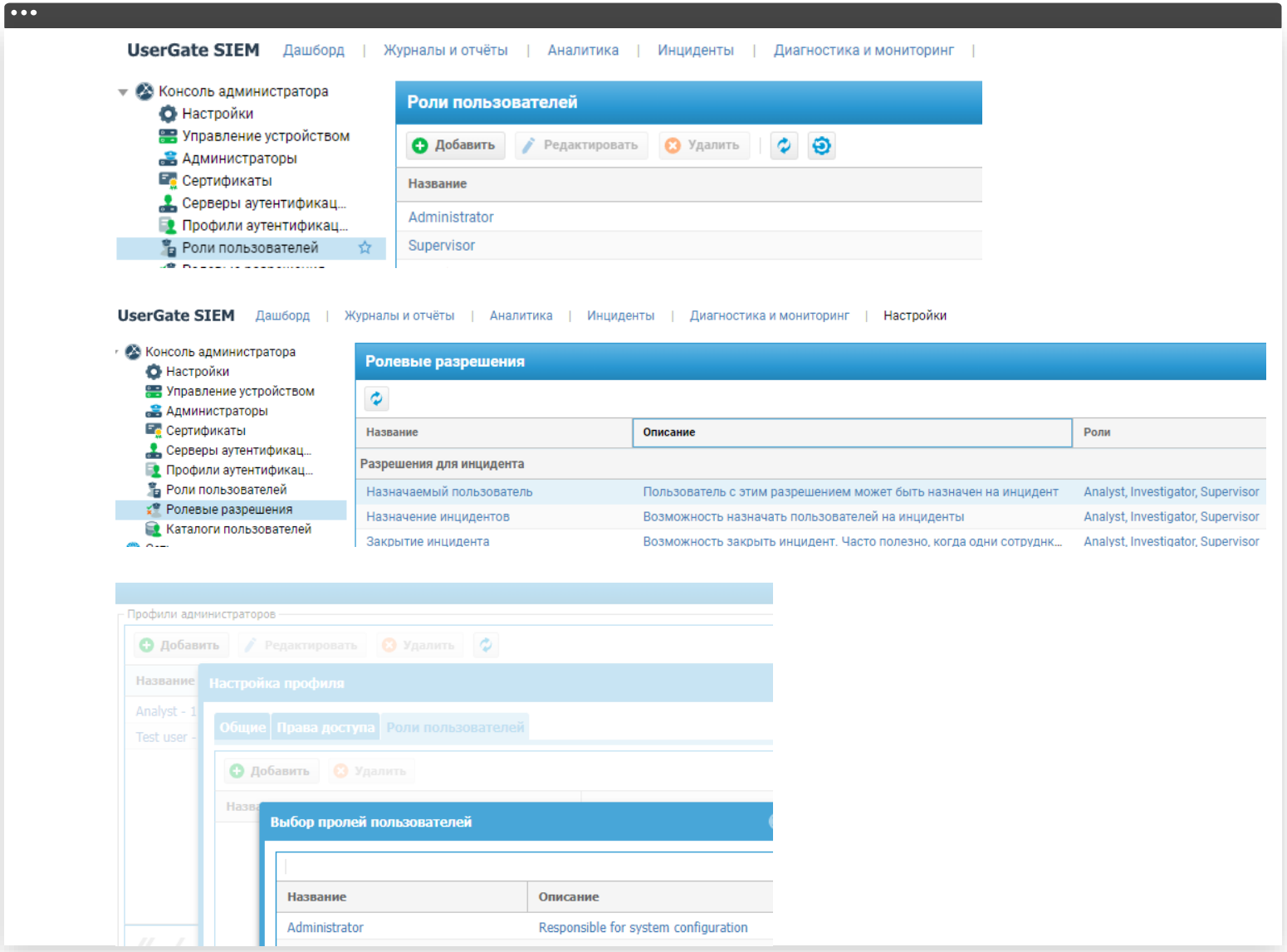


РОЛЕВОЙ ДОСТУП SIEM

01
Роли пользователей

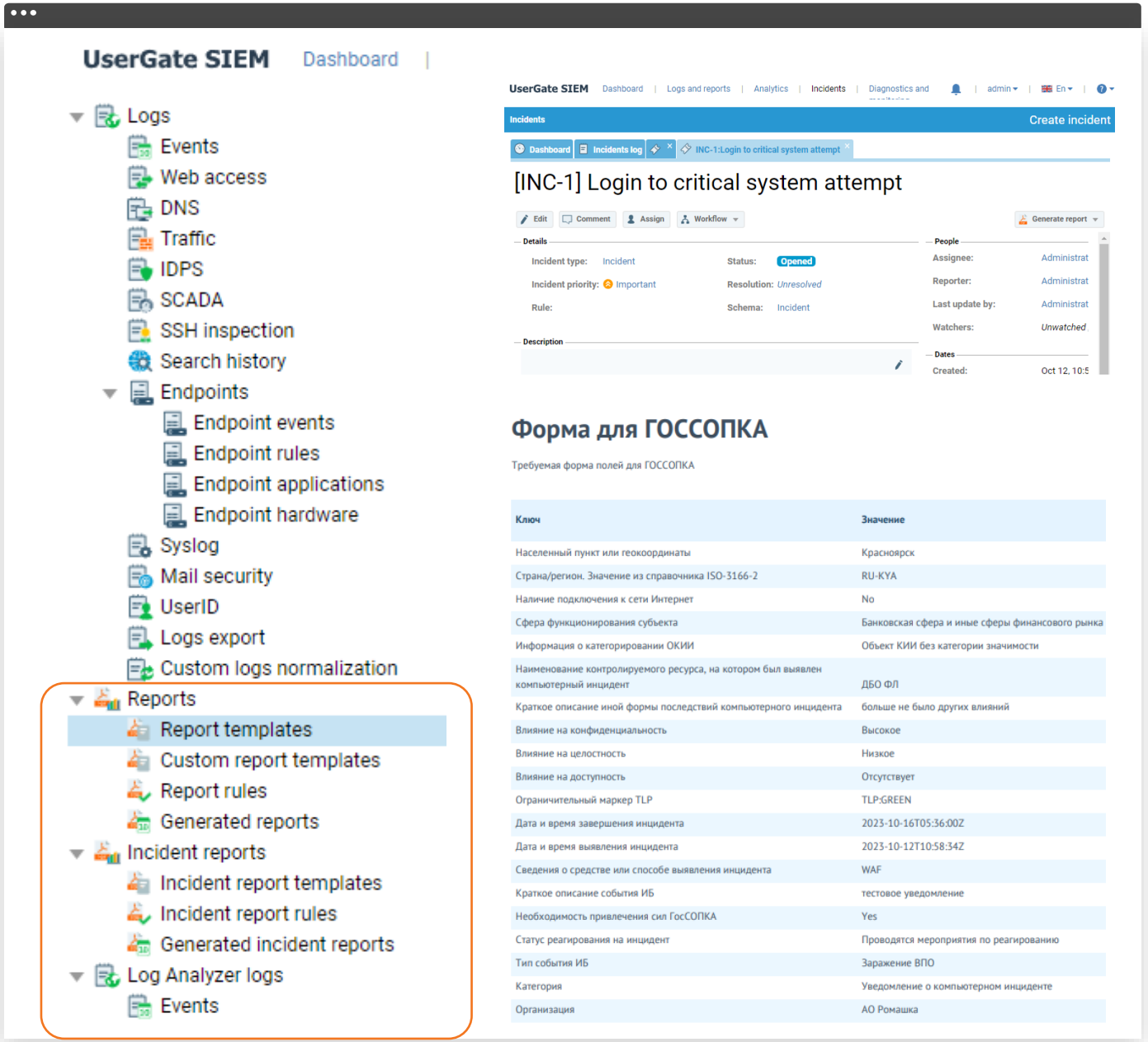
02
Ролевые разрешения

03
Профиль пользователя



ОТЧЕТЫ

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



СЛЕДСТВИЕ ОТ ВЛАДЕНИЯ USERGATE SIEM

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

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ: ВНУТРЕННИЙ ЗЛОУМЫШЛЕННИК

UserGate

Внутренние угрозы остаются одними из самых сложных в обнаружении.

UserGate SIEM позволит обеспечить:

- Сбор всех необходимых данных безопасности без дополнительных расходов;
- Обнаружение внутренних угроз и рисков в режиме реального времени;
- Комплексный анализ событий со всех подключенных систем безопасности;
- Выявление дальнейшего распространения через любой узел, IP-адрес, учетные данные;
- Быстрое и своевременное расследование угроз и рисков;
- Автоматизация реагирования с помощью встроенной функциональности IRP/SOAR.

UserGate

ЧТО НУЖНО ПРЕДПРИНЯТЬ БИЗНЕСУ ДЛЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА

USERGATE SIEM — ПЕРВЫЙ В РОССИИ ЭКОСИСТЕМНЫЙ SIEM С ФУНКЦИОНАЛЬНОСТЬЮ IRP/SOAR ПОМОГАЕТ

**Соответствовать требованиям законодательства,
в рамках реализации следующих нормативных документов:**

- ФЗ РФ от 27 июля 2006 г. № 152 ФЗ «О персональных данных»
- ФЗ РФ от 26 июля 2017 г. № 187 ФЗ «О безопасности критической информационной инфраструктуры РФ»
- приказ ФСТЭК № 21
- приказ ФСТЭК № 31
- указ президента №250
- стандарт ГОСТ Р 57580.1 2017
- стандарт ГОСТ Р 57580.2 2018

USERGATE SIEM — ПЕРВЫЙ В РОССИИ ЭКОСИСТЕМНЫЙ SIEM С ФУНКЦИОНАЛОМ IRP/SOAR ПОМОГАЕТ СООТВЕТСТВОВАТЬ ТРЕБОВАНИЯМ 21 ПРИКАЗА

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них

USERGATE SIEM — ПЕРВЫЙ В РОССИИ ЭКОСИСТЕМНЫЙ SIEM С ФУНКЦИОНАЛОМ IRP/SOAR ПОМОГАЕТ СООТВЕТСТВОВАТЬ ТРЕБОВАНИЯМ 21 ПРИКАЗА

V. Регистрация событий безопасности	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности

XIV. Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и регирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов

UserGate

Мы защищаем вас,
пока вы делаете мир лучше

СПАСИБО ЗА ВНИМАНИЕ

Дмитрий Чеботарёв
Менеджер по развитию UserGate SIEM