UserGate

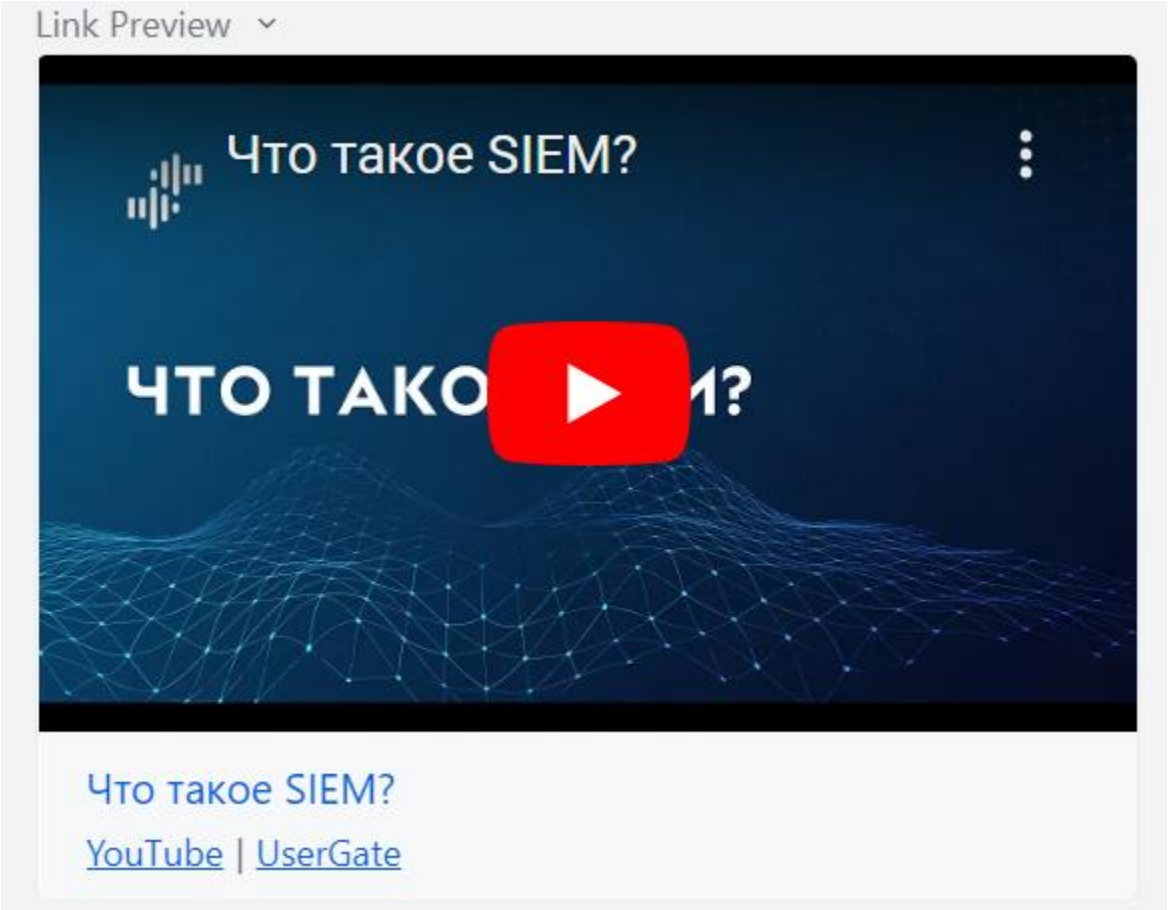
UserGate SIEM

Дмитрий Чеботарёв
Менеджер по развитию продукта

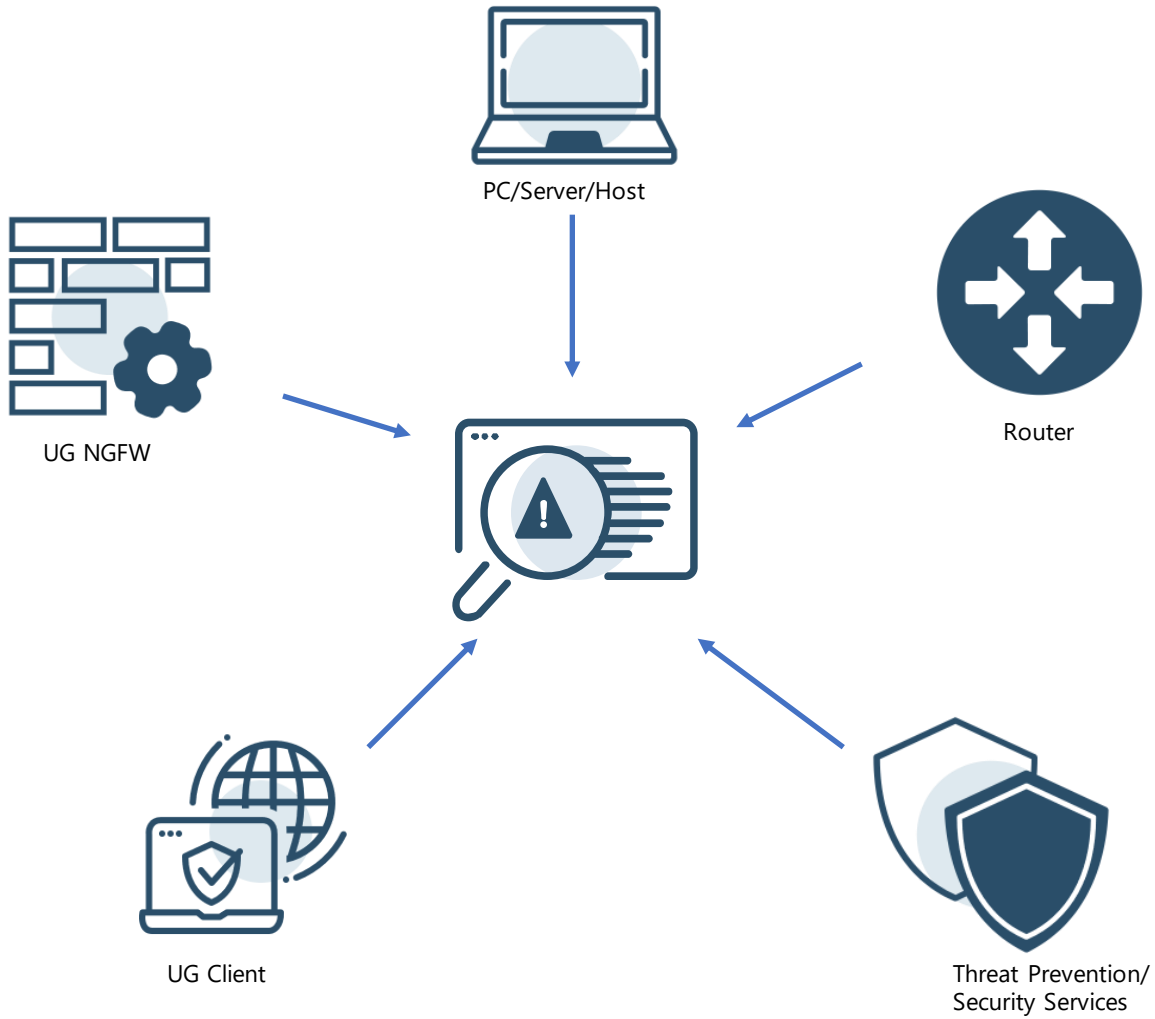
Что такое SIEM?

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

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

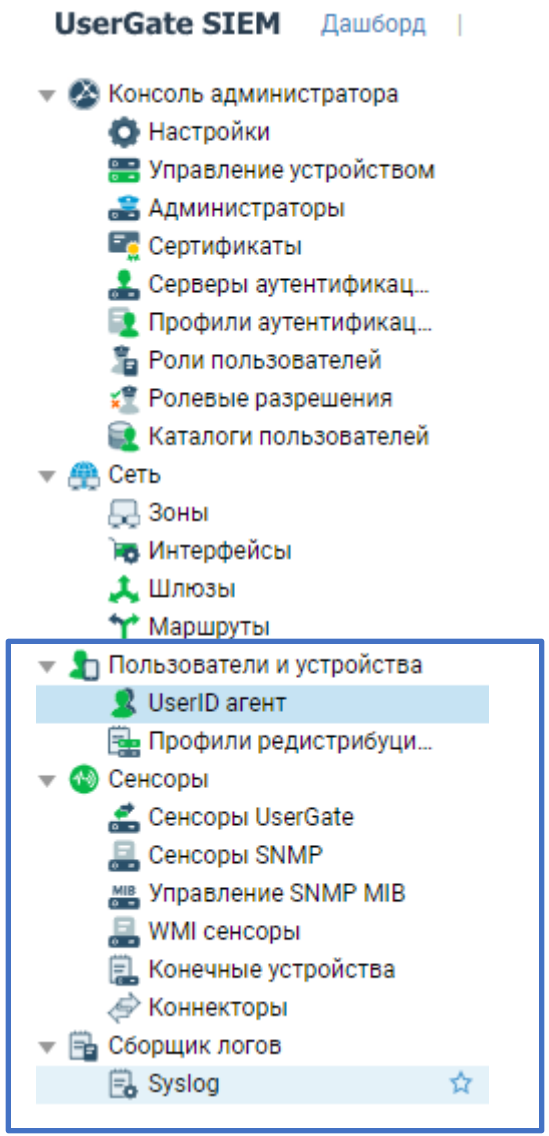


Сбор данных и нормализация

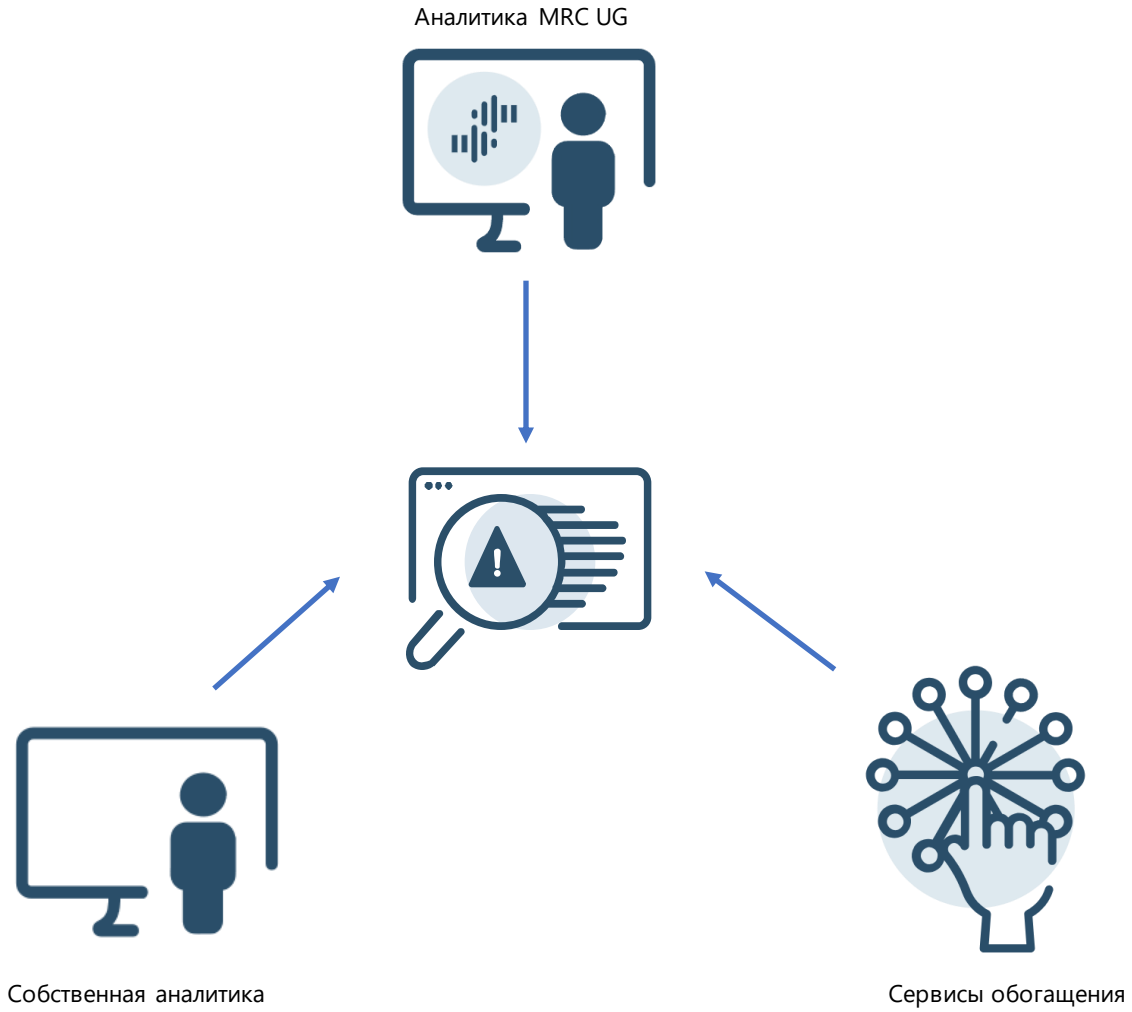


Источники

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

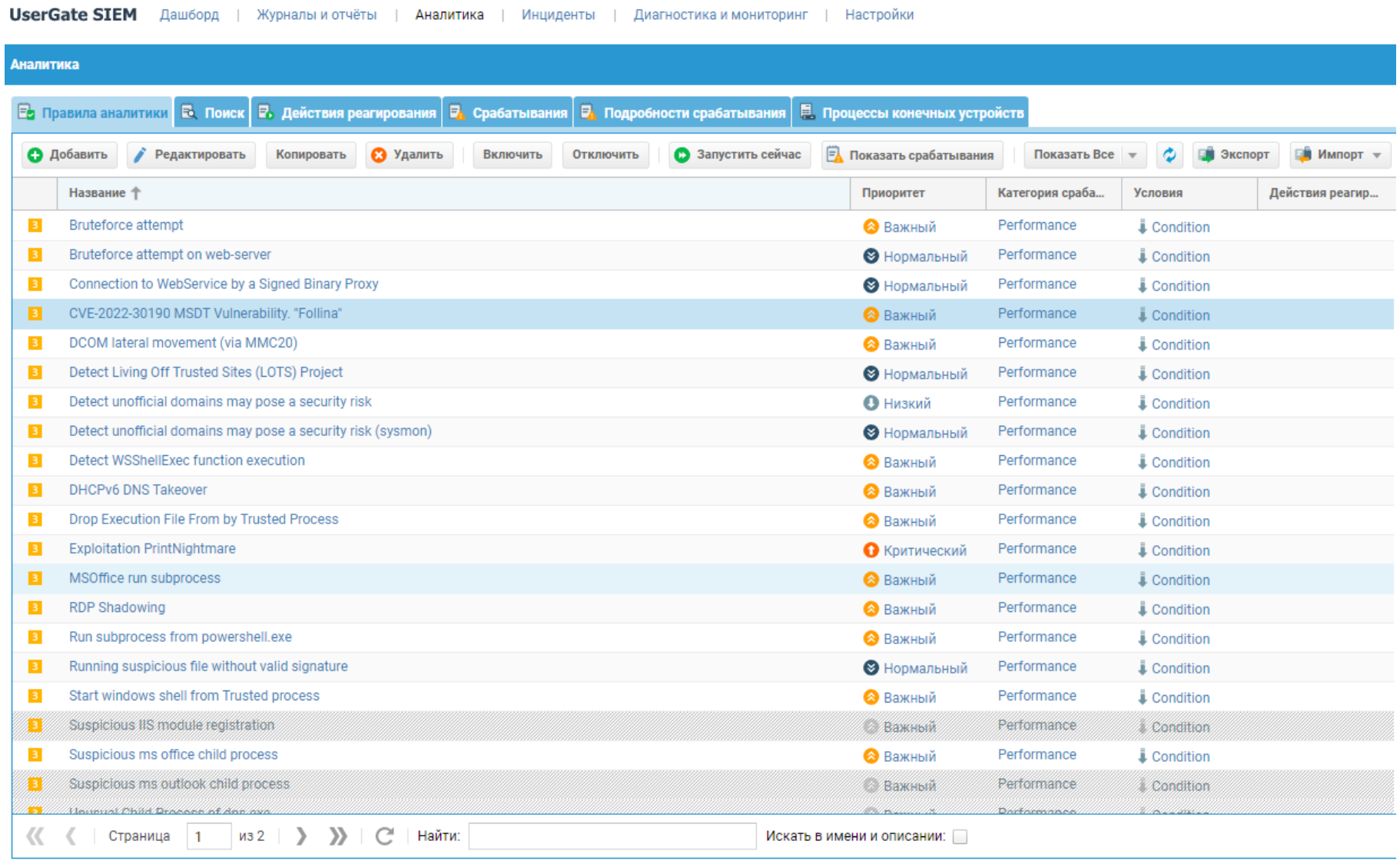


Анализ и корреляция

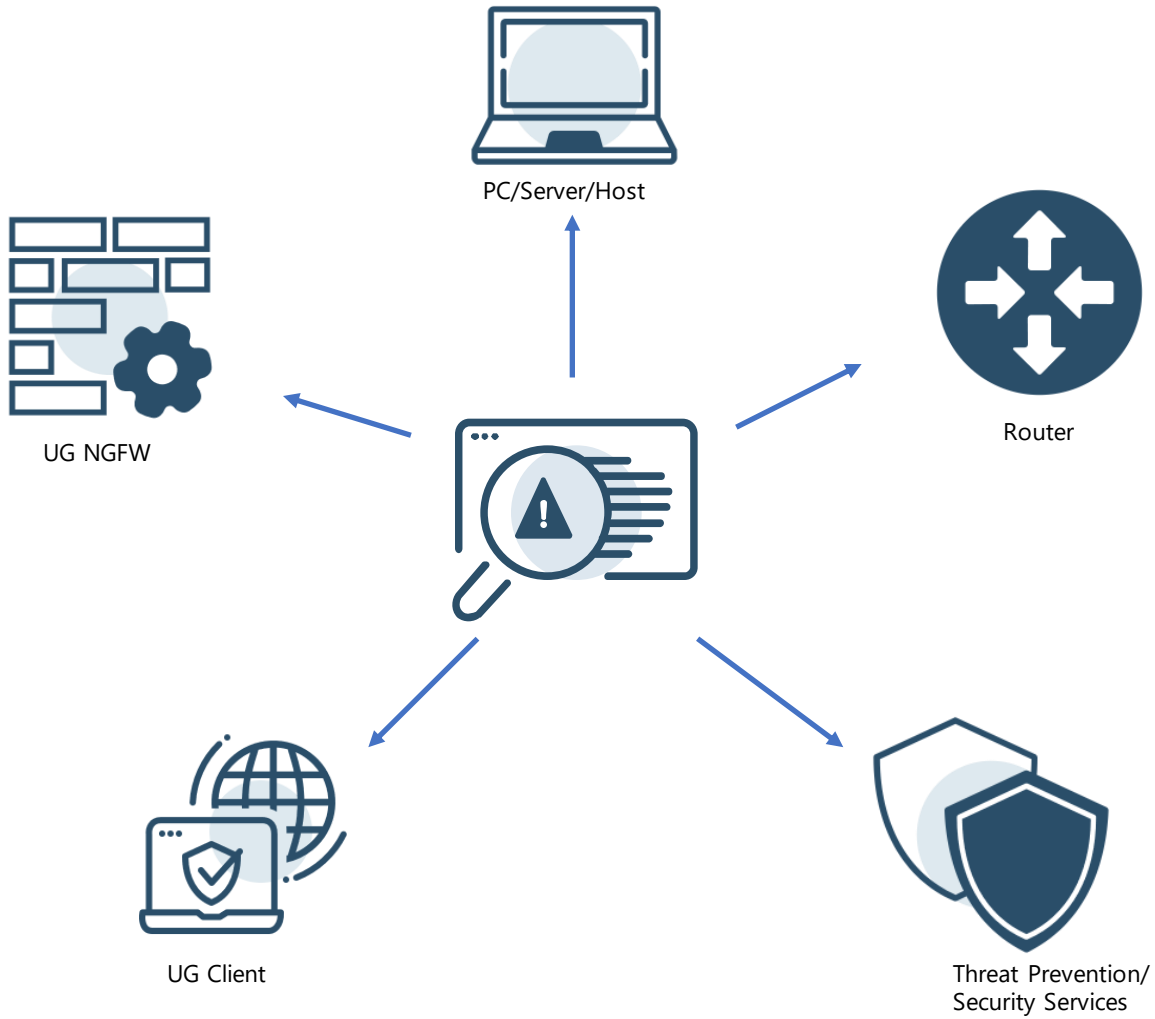


Правила аналитики

- Правила из библиотеки
- Правила добавленные пользователем
- Возможность экспорта/ импорта правил

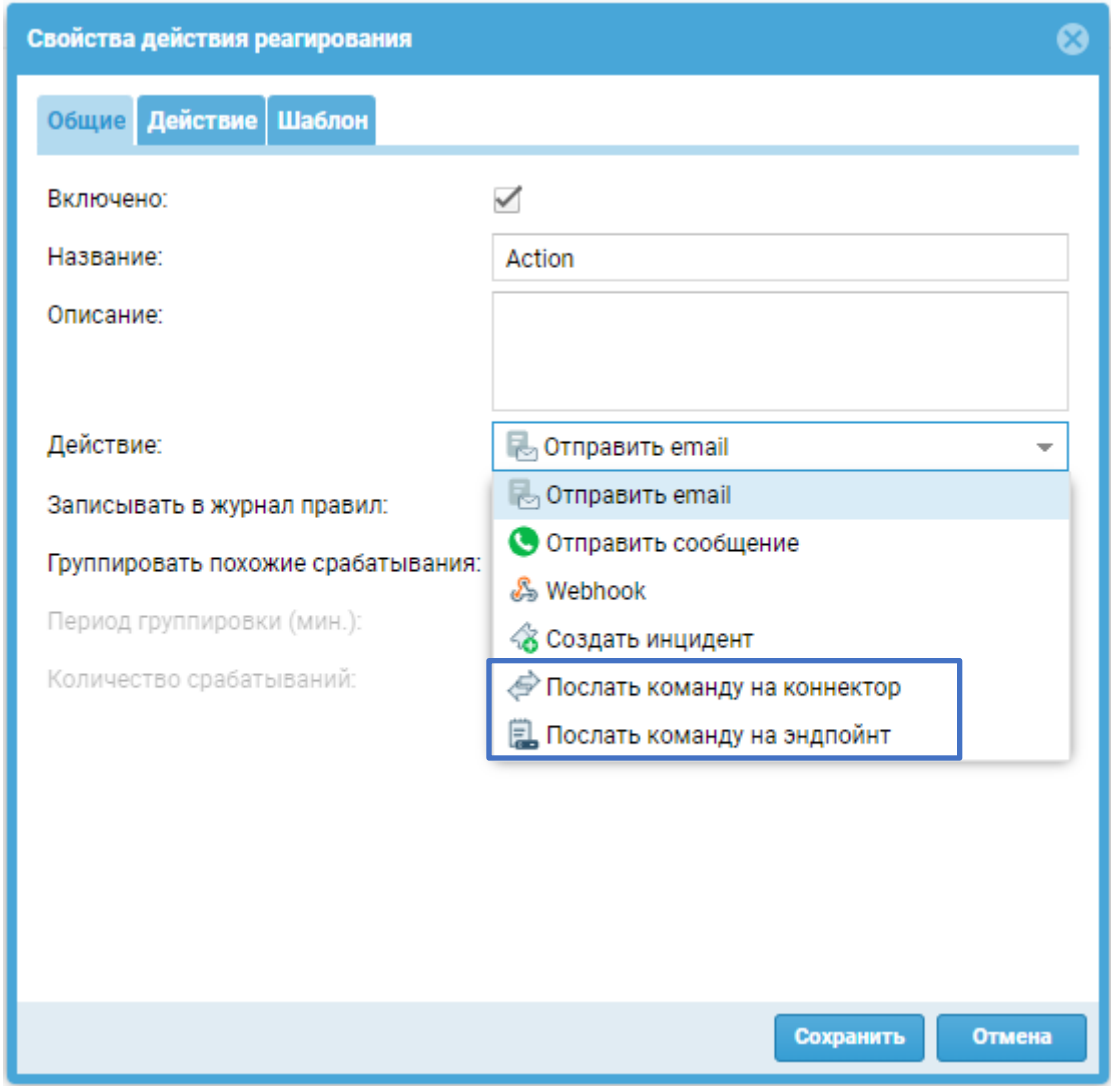


Реагирование



Реагирование через инфраструктуру

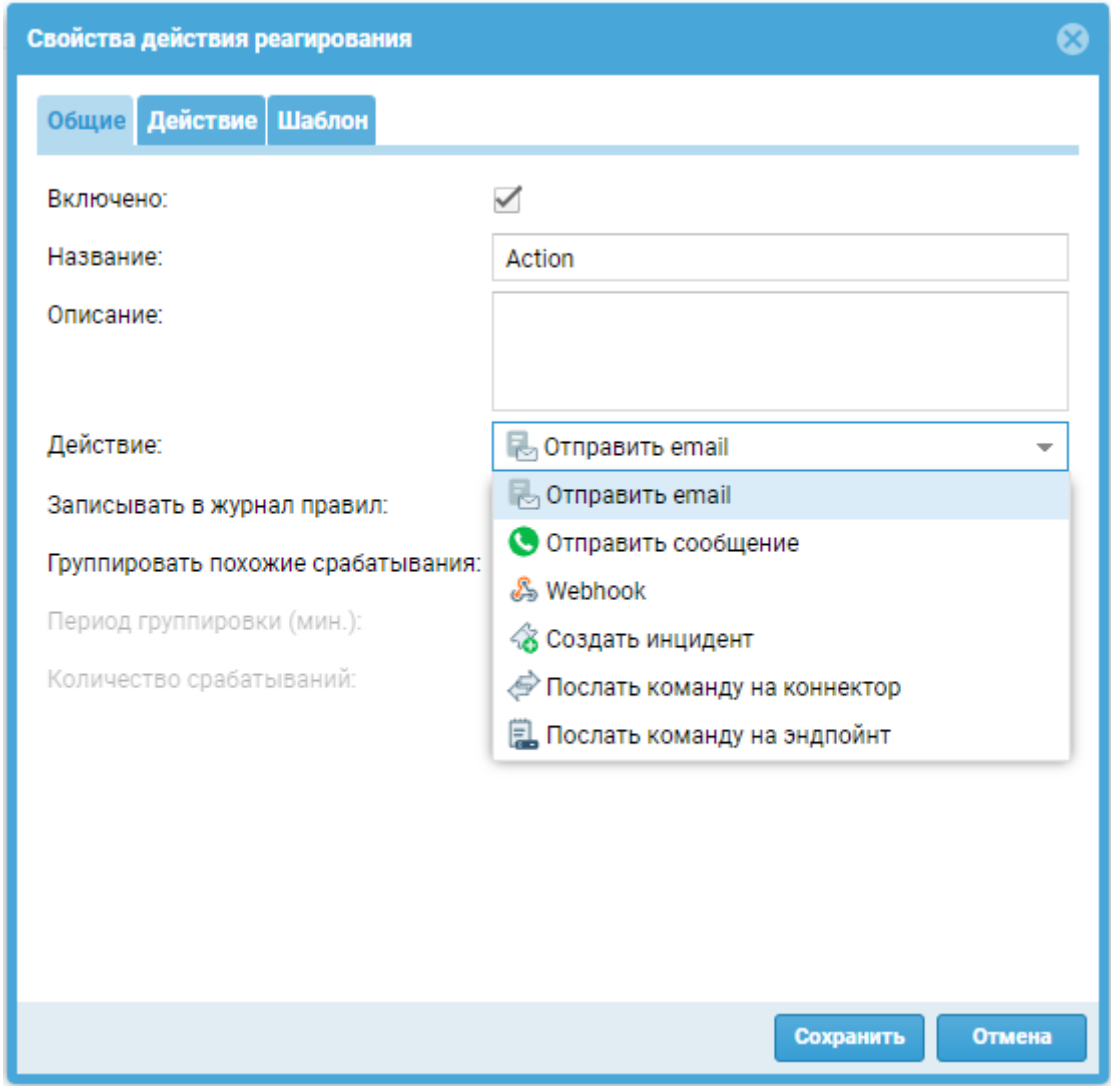
- Отправка команд через SSH/HTTP/HTTPS
- Возможность передачи в команде артефактов, например IP адресов
- Возможность отправки команд на устройства других производителей (коммутаторы, маршрутизаторы и др.)

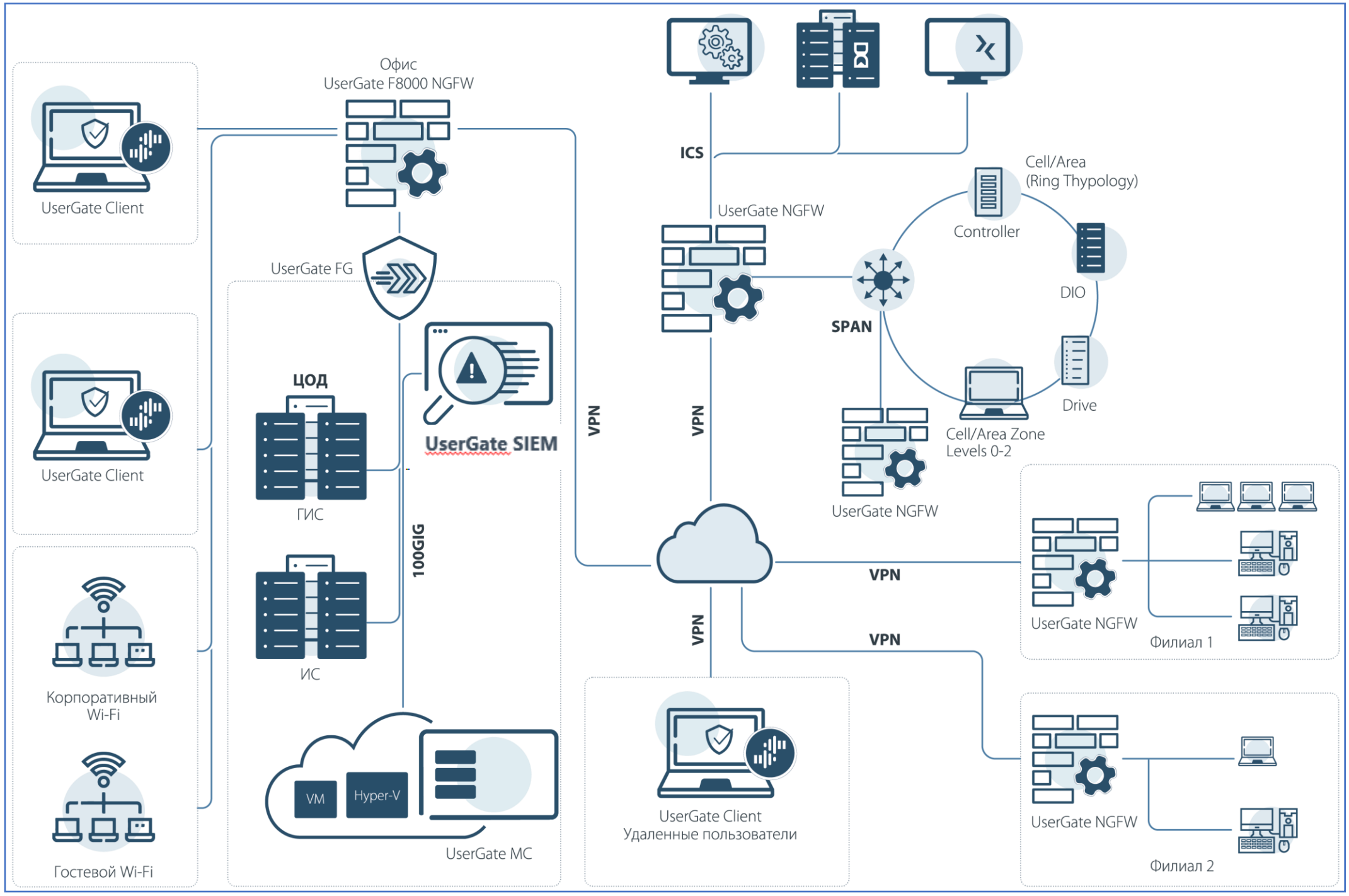


Варианты реагирования

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

Настройки группировки похожих событий




Офис
UserGate F8000 NGFW
UserGate Client
UserGate Client
Корпоративный Wi-Fi
Гостевой Wi-Fi
UserGate FG
ЦОД
ГИС
ИС
UserGate SIEM
100GIG
VM
Hyper-V
UserGate MC
VPN
ICS
UserGate NGFW
SPAN
Cell/Area
(Ring Thypology)
Controller
DIO
Drive
Cell/Area Zone
Levels 0-2
UserGate NGFW
VPN
VPN
VPN
VPN
UserGate Client
Удаленные пользователи
UserGate NGFW
Филиал 1
UserGate NGFW
Филиал 2

Этапы развития SIEM

Где взяли экспертизу?

Где взяли экспертизу?

Сами написали.

Что такое MRC?

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 поможет:

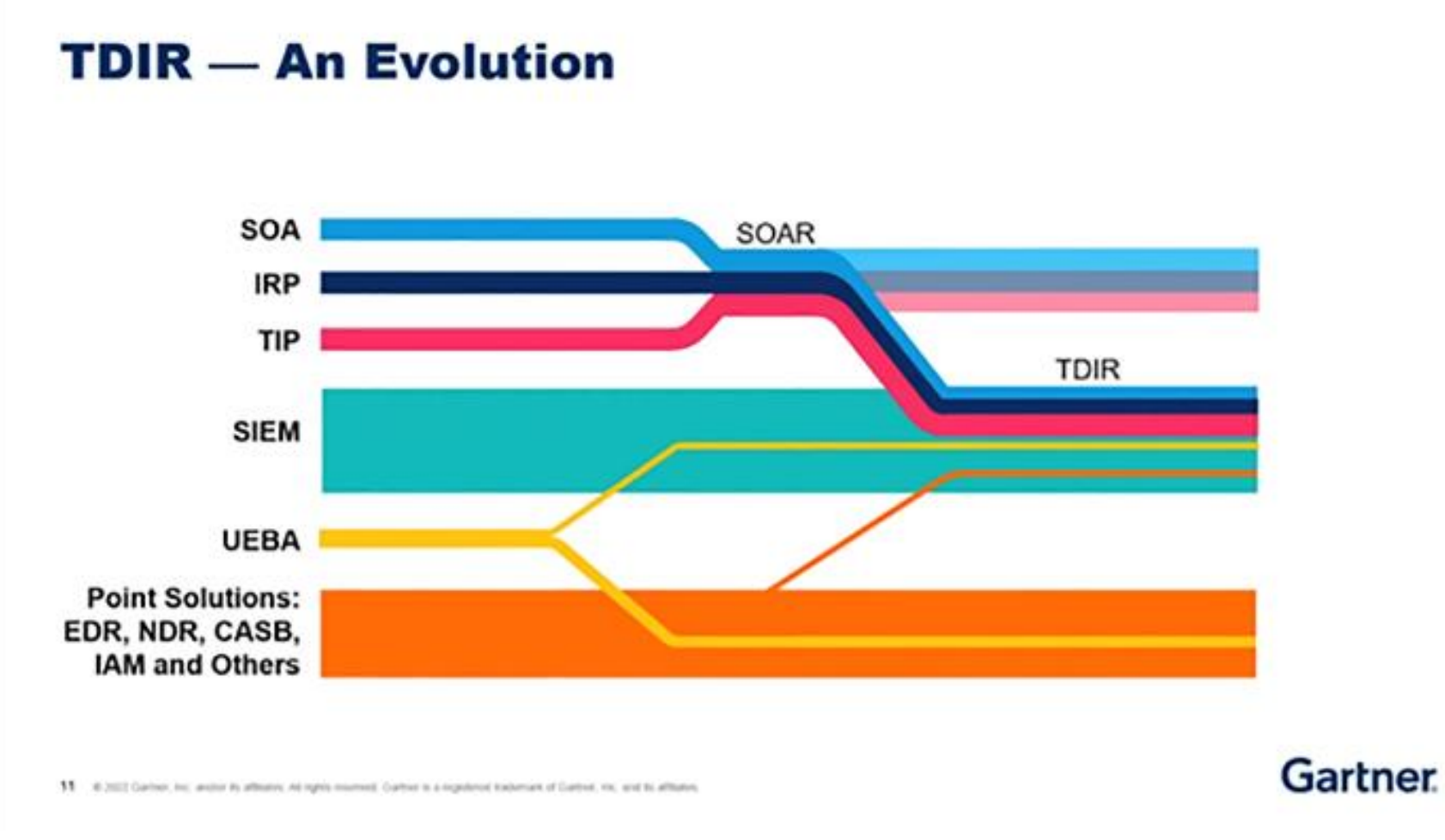
- Минимизировать финансовые потери из-за простоя бизнес-критических сервисов;
- Снизить риск утечки данных;
- Выполнить требования регулятора;
- Получить качественную экспертизу;
- Облегчить работу сотрудников в режиме постоянного дефицита кадров.

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

SIEM-системы должны эволюционировать!

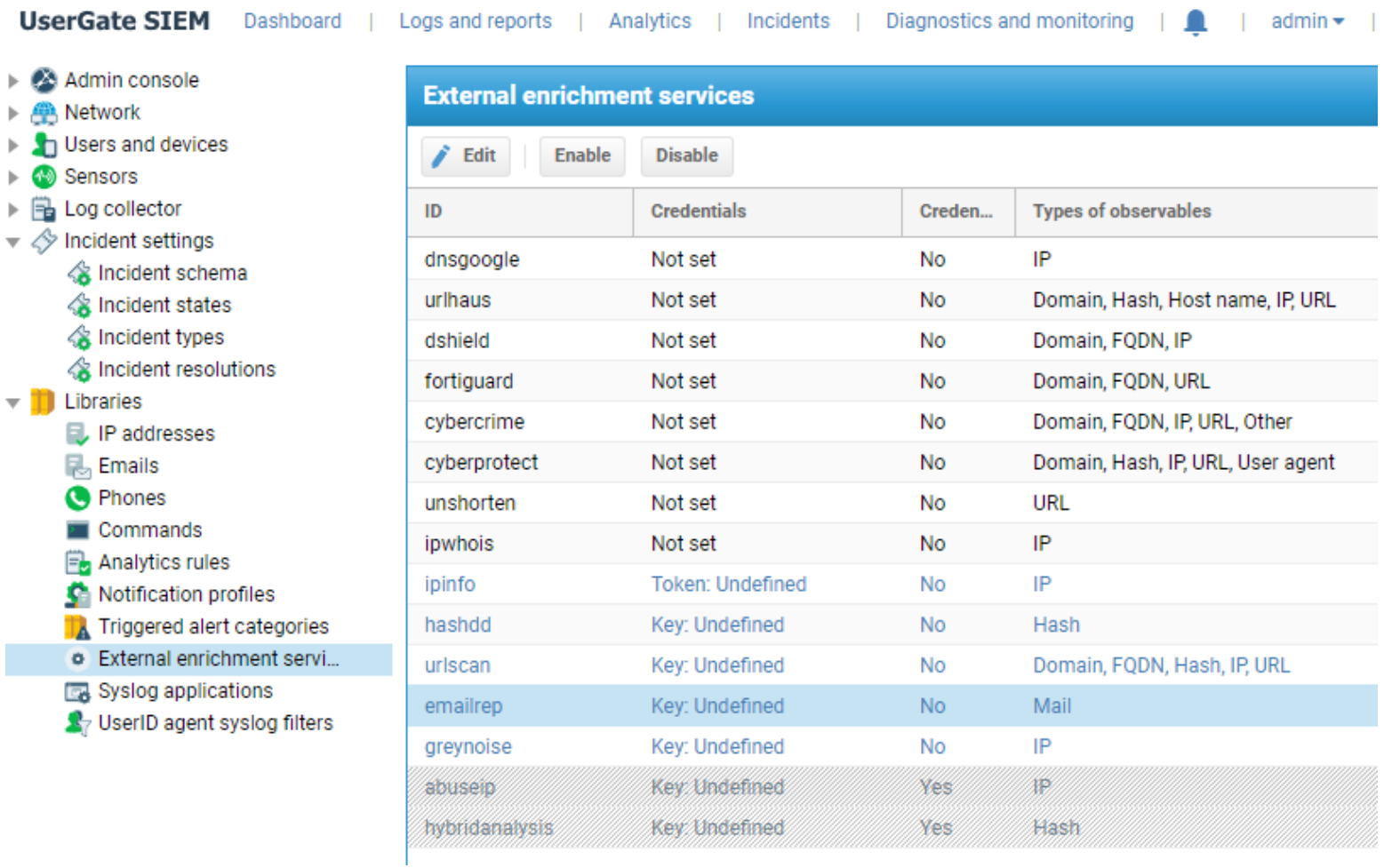


Экспертиза, IoC

Данные из логов, которые можно обогатить и найти следы компрометации:

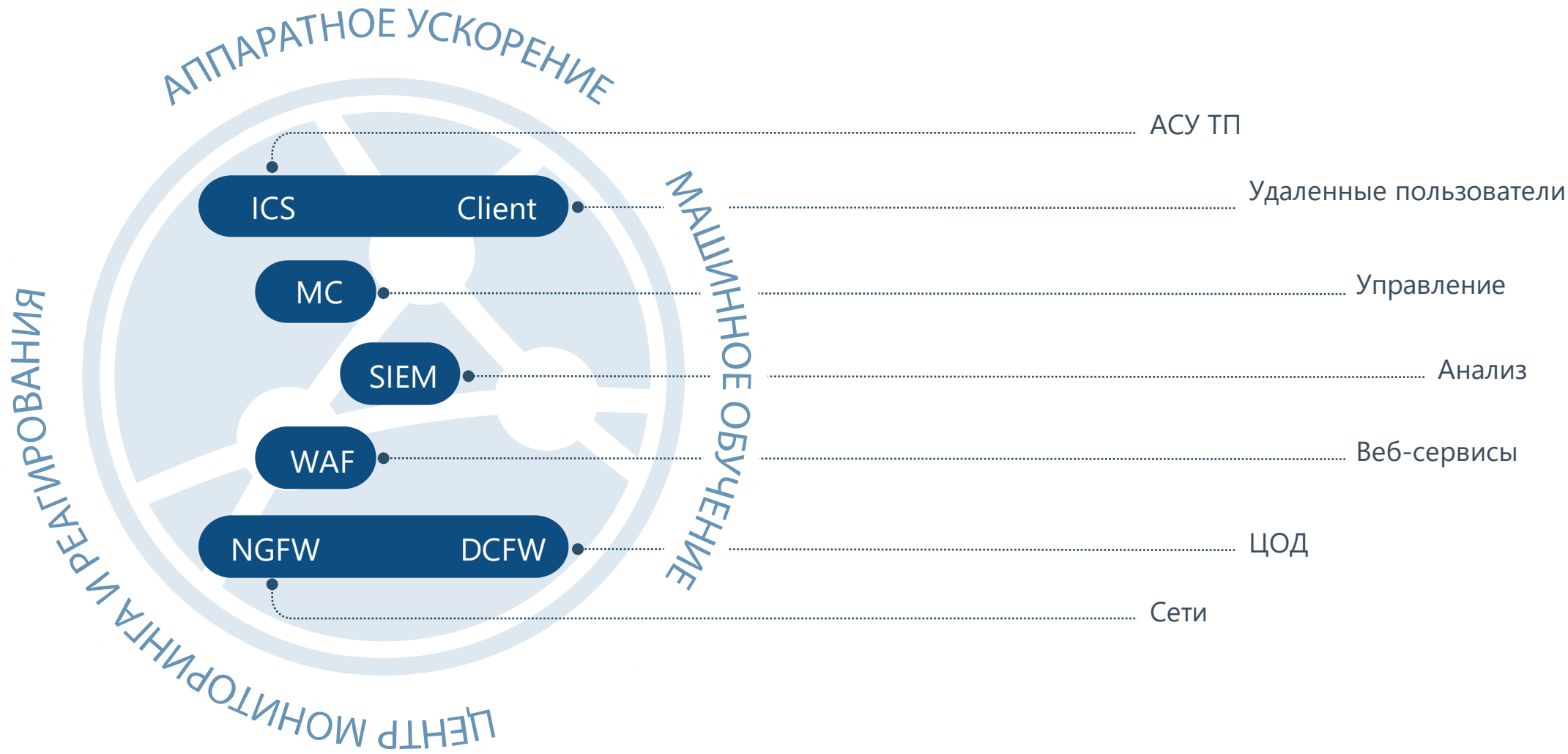
- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

Библиотеки (сервисы обогащения)

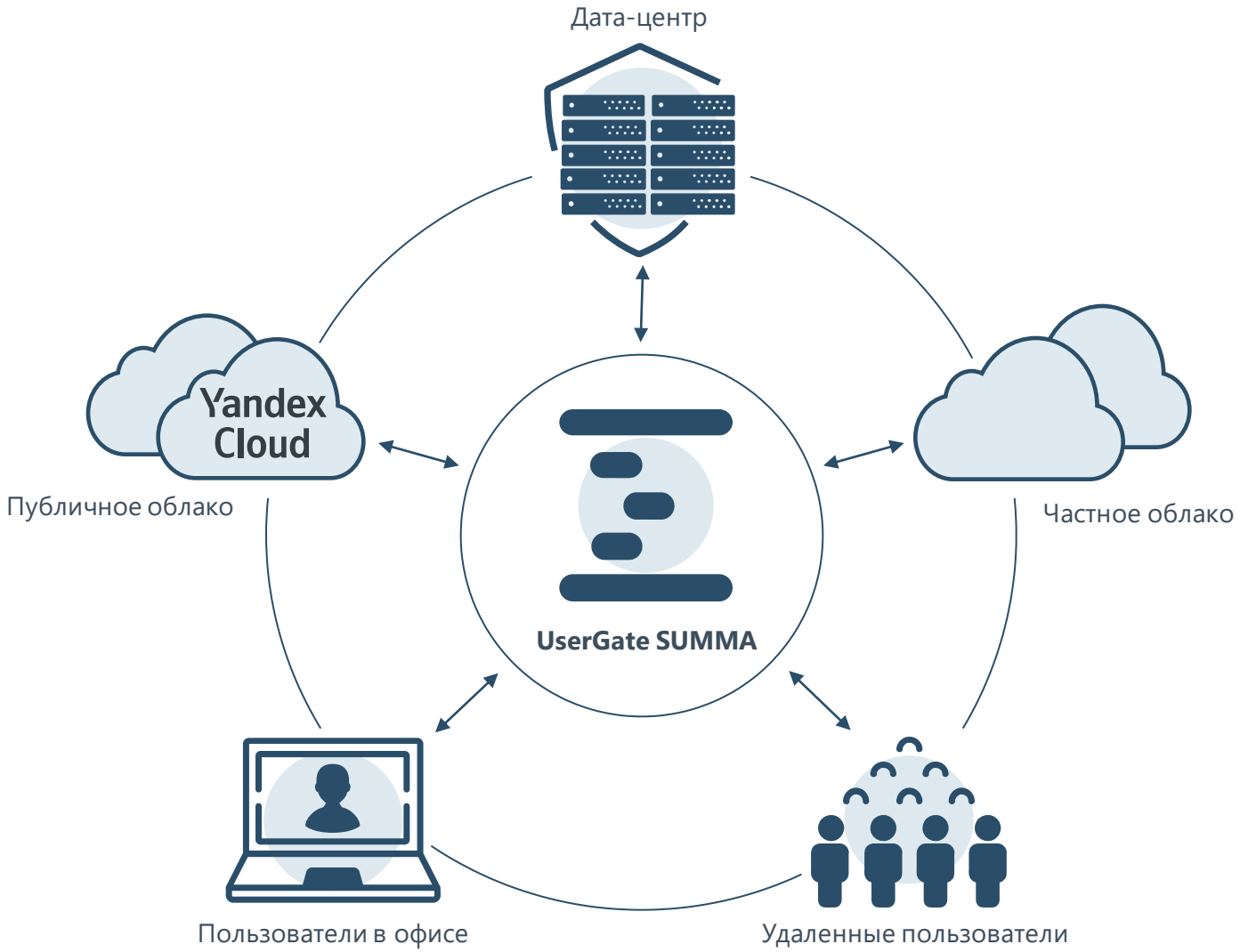


UserGate SUMMA

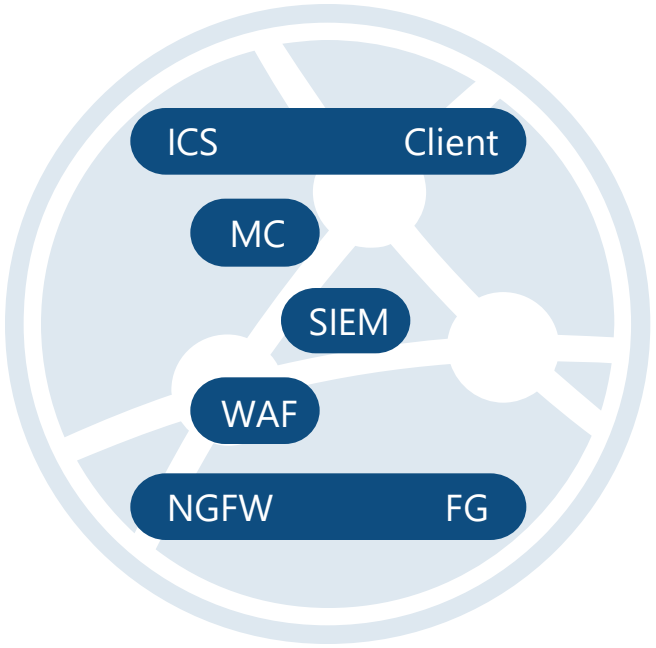
100% видимость событий безопасности



Zero Trust Network Access (ZTNA)



Все продукты UserGate SUMMA доступны в виртуальном исполнении

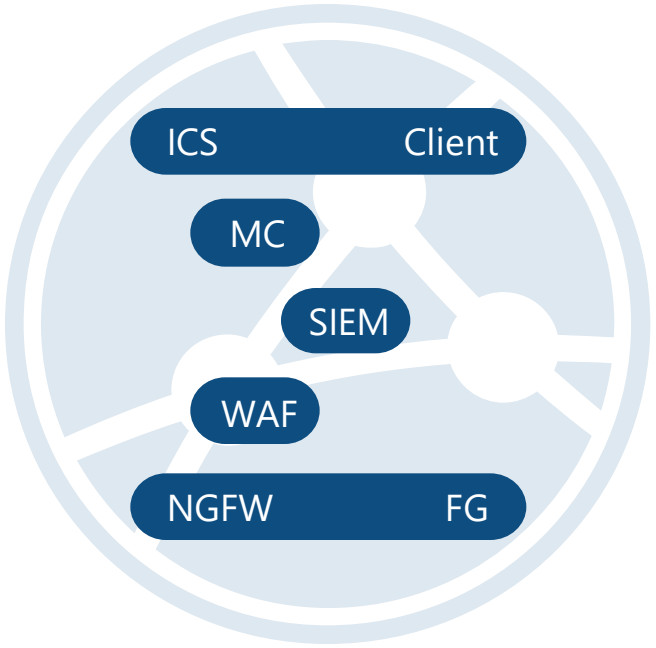


Гипервизоры

:

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

Все продукты UserGate SUMMA доступны в облачном исполнении



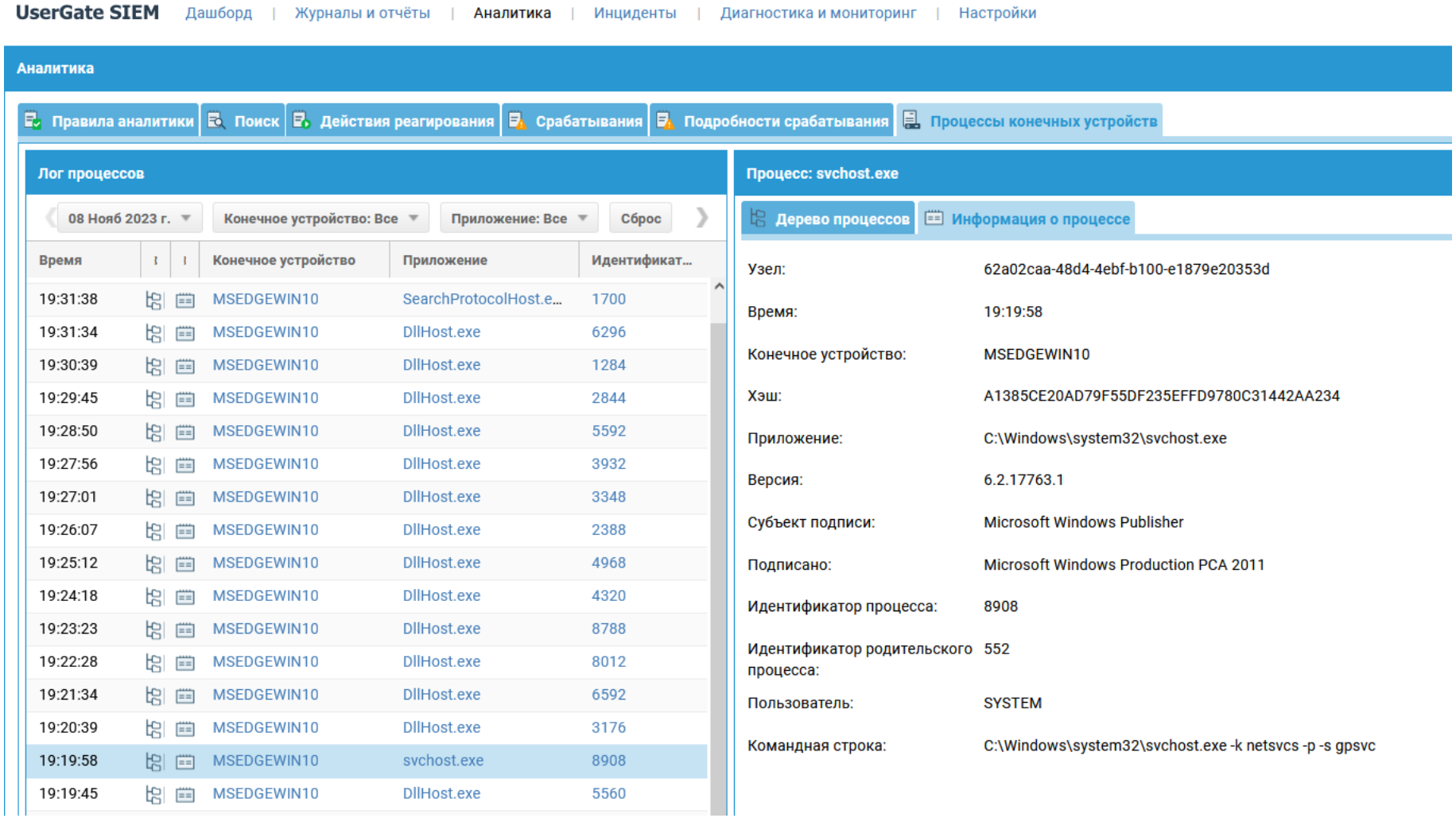
Yandex Cloud

Преимущества

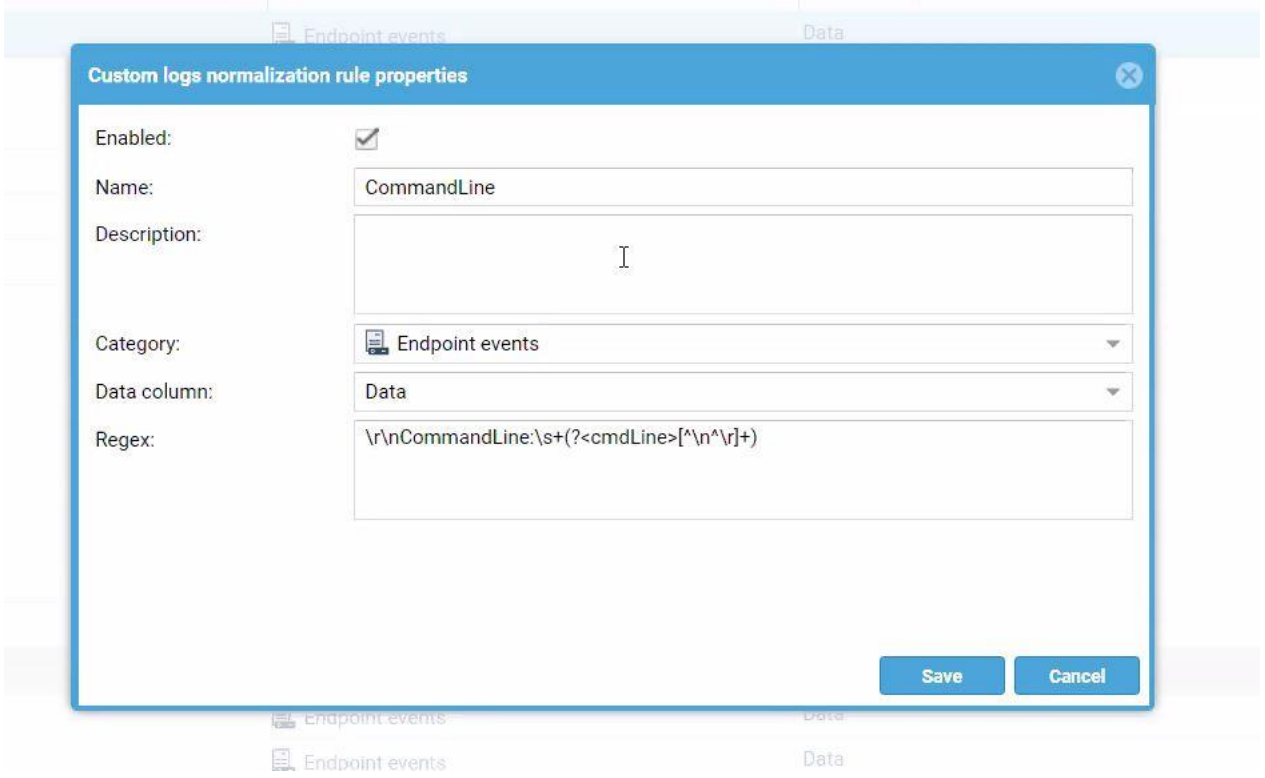
Преимущества

- Готовое решение «из коробки»
- Простая настройка и внедрение
- Готовая экспертиза от специалистов Центра Мониторинга и Реагирования компании UserGate
- Подключаемые источники данных для обогащения событий и расследования инцидентов
- Интеграция с ГосСОПКА
- Широкий спектр поддерживаемых платформ и протоколов для интеграции
- Автоматизация реагирования
- Возможность расширения функциональности Log Analyzer лицензией

Процессы конечных устройств

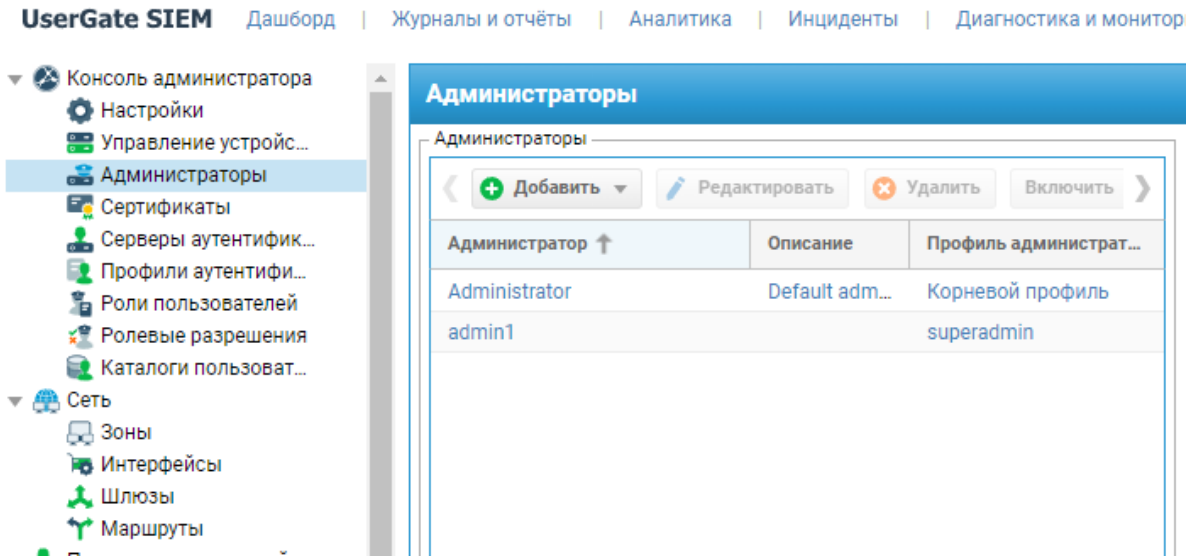


Пользовательская нормализация



Администраторы

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

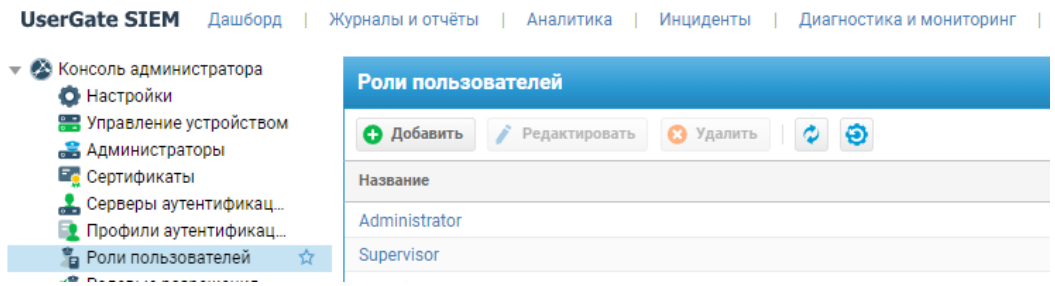


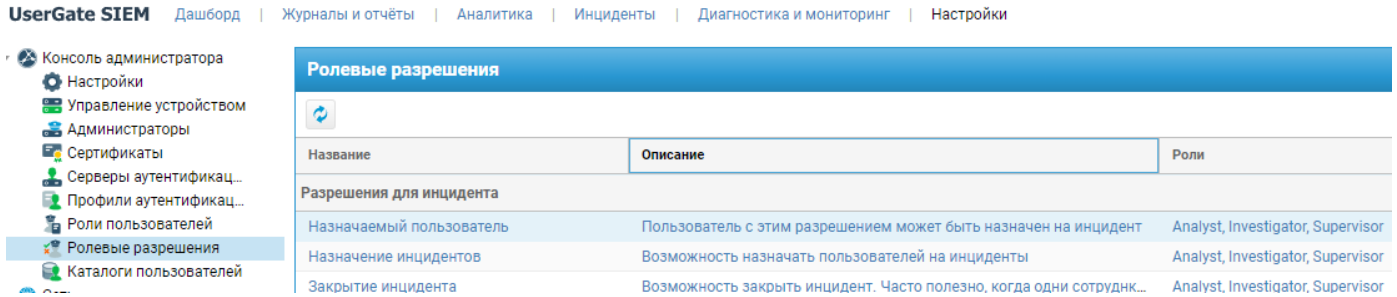
Ролевой доступ SIEM

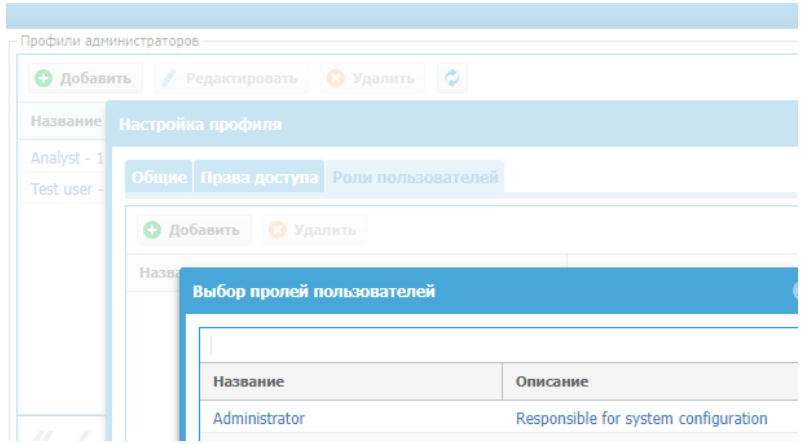
Роли пользователей

Ролевые разрешения

Профиль пользователя

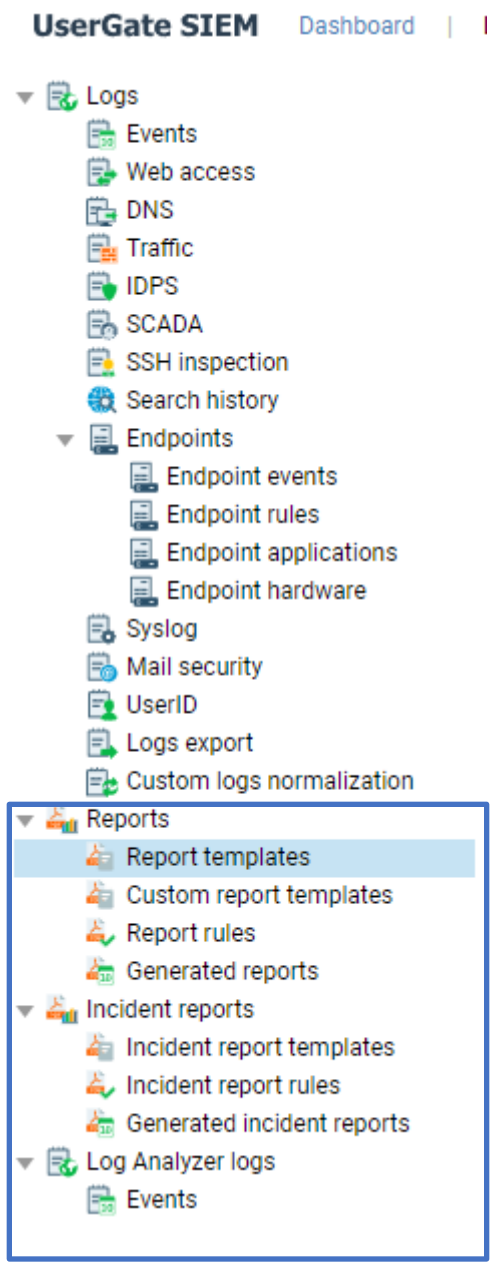


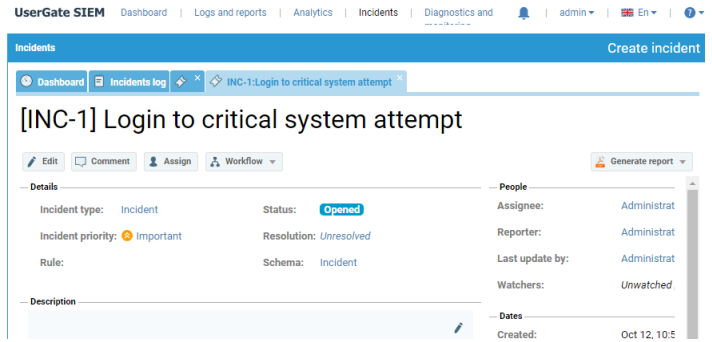




Отчеты

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





Форма для ГОССОПКА

Требуемая форма полей для ГОССОПКА

Ключ	Значение
Населенный пункт или геокоординаты	Красноярск
Страна/регион. Значение из справочника ISO-3166-2	RU-KYA
Наличие подключения к сети Интернет	No
Сфера функционирования субъекта	Банковская сфера и иные сферы финансового рынка
Информация о категорировании ОКИИ	Объект КИИ без категории значимости
Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент	ДБО ФЛ
Краткое описание иной формы последствий компьютерного инцидента	больше не было других влияний
Влияние на конфиденциальность	Высокое
Влияние на целостность	Низкое
Влияние на доступность	Отсутствует
Ограничительный маркер TLP	TLP:GREEN
Дата и время завершения инцидента	2023-10-16T05:36:00Z
Дата и время выявления инцидента	2023-10-12T10:58:34Z
Сведения о средстве или способе выявления инцидента	WAF
Краткое описание события ИБ	тестовое уведомление
Необходимость привлечения сил ГосСОПКА	Yes
Статус реагирования на инцидент	Проводятся мероприятия по реагированию
Тип события ИБ	Заражение ВПО
Категория	Уведомление о компьютерном инциденте
Организация	АО Ромашка

UserGate

Спасибо за внимание!

Дмитрий Чеботарев
Менеджер по развитию продукта