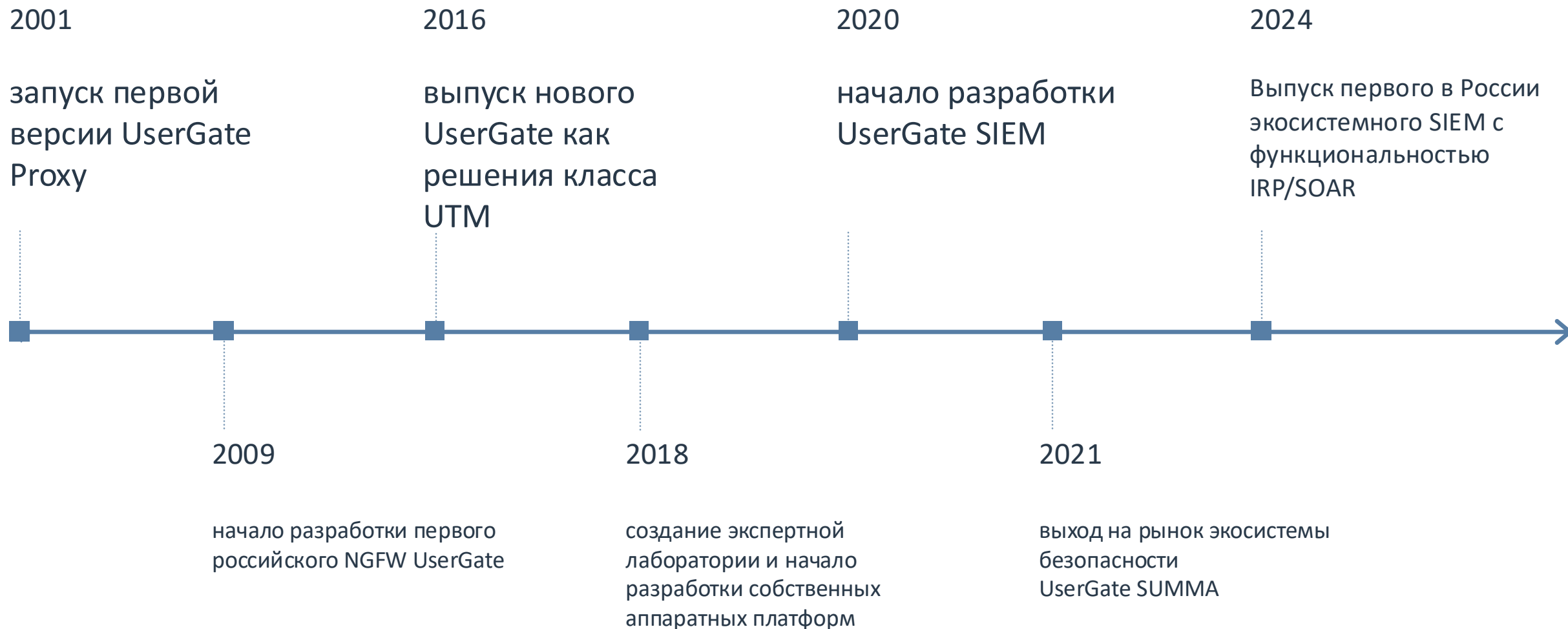




СОВРЕМЕННАЯ SIEM-СИСТЕМА НА ПРИМЕРЕ USERGATE SIEM

Алексей Афанасьев
Менеджер по развитию UserGate SIEM

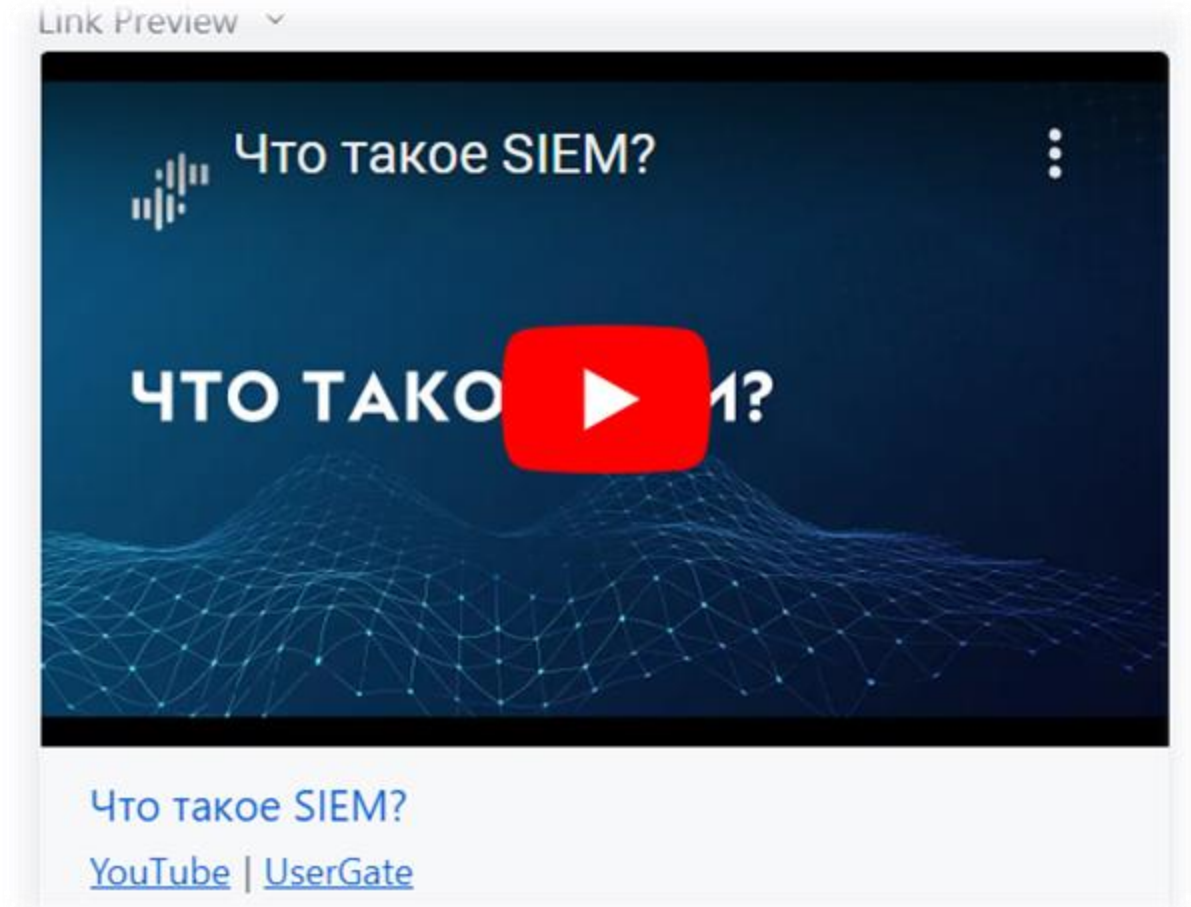


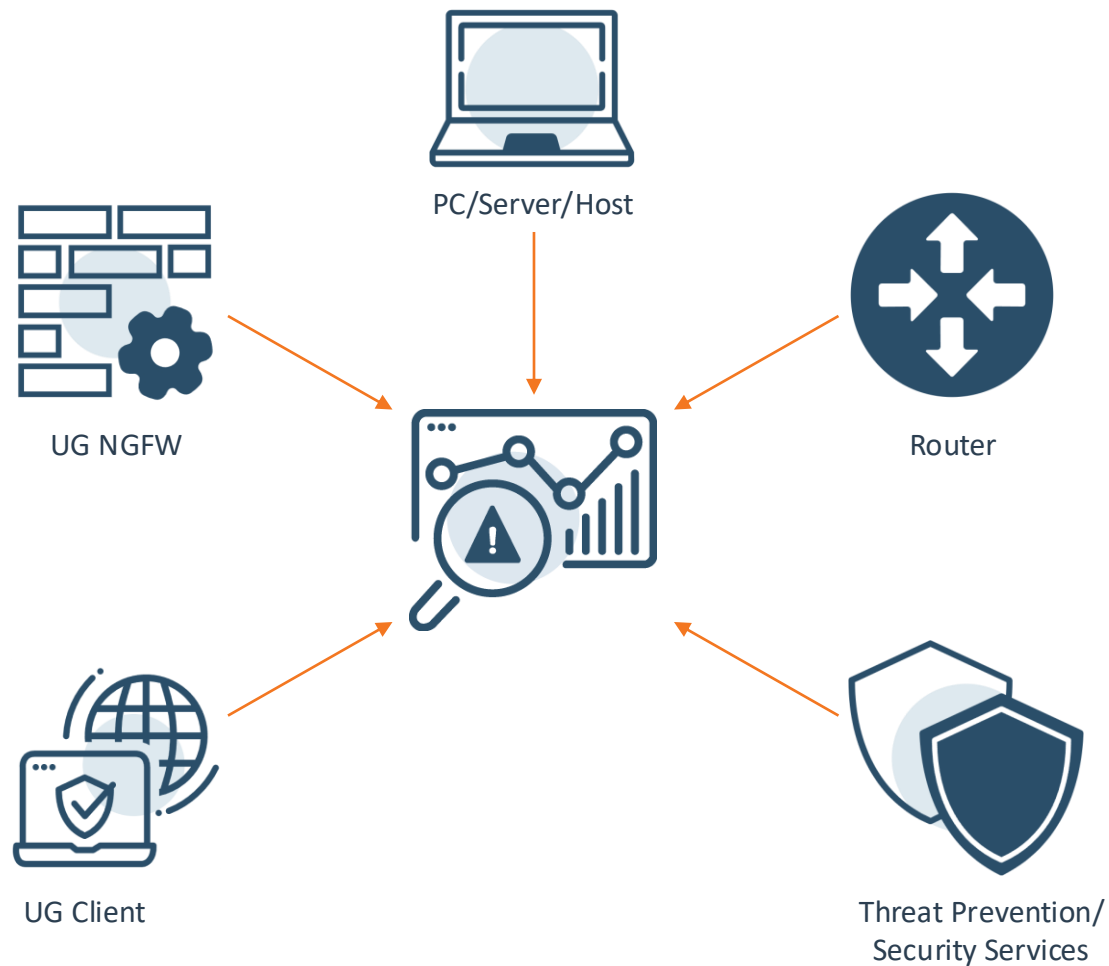
ЧТО ТАКОЕ SIEM?

ЧТО ТАКОЕ SIEM?

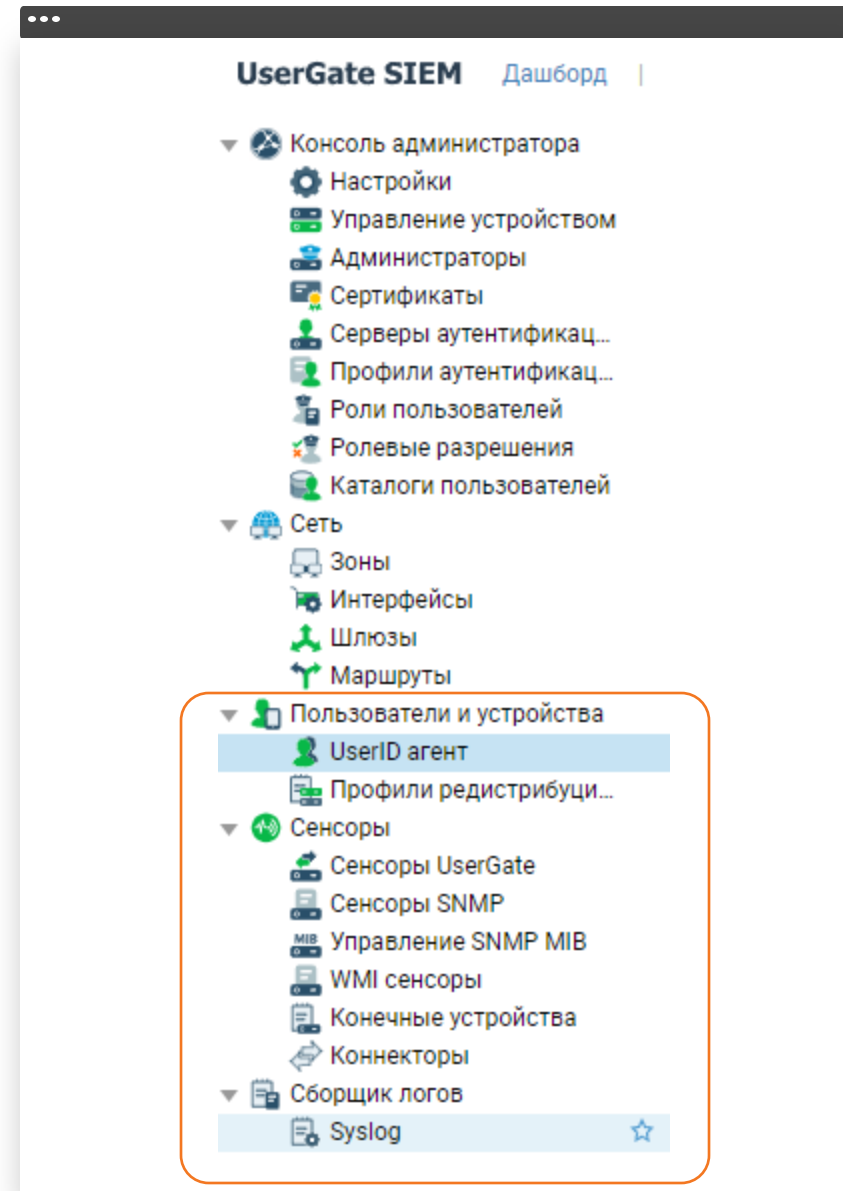
SIEM (Security Information and Event Management) – система управления событиями информационной безопасности.

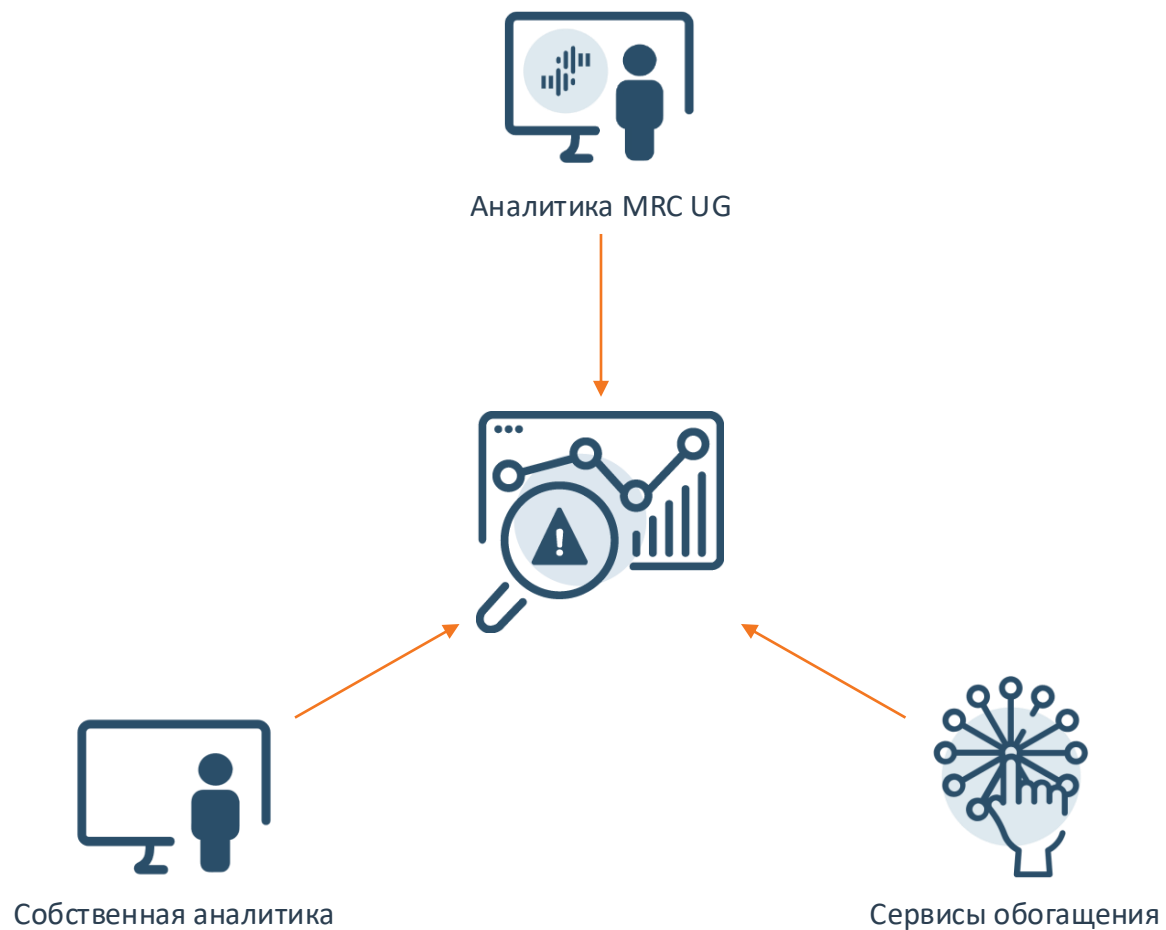
<https://www.youtube.com/watch?v=ddAzEN1iC5o>





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

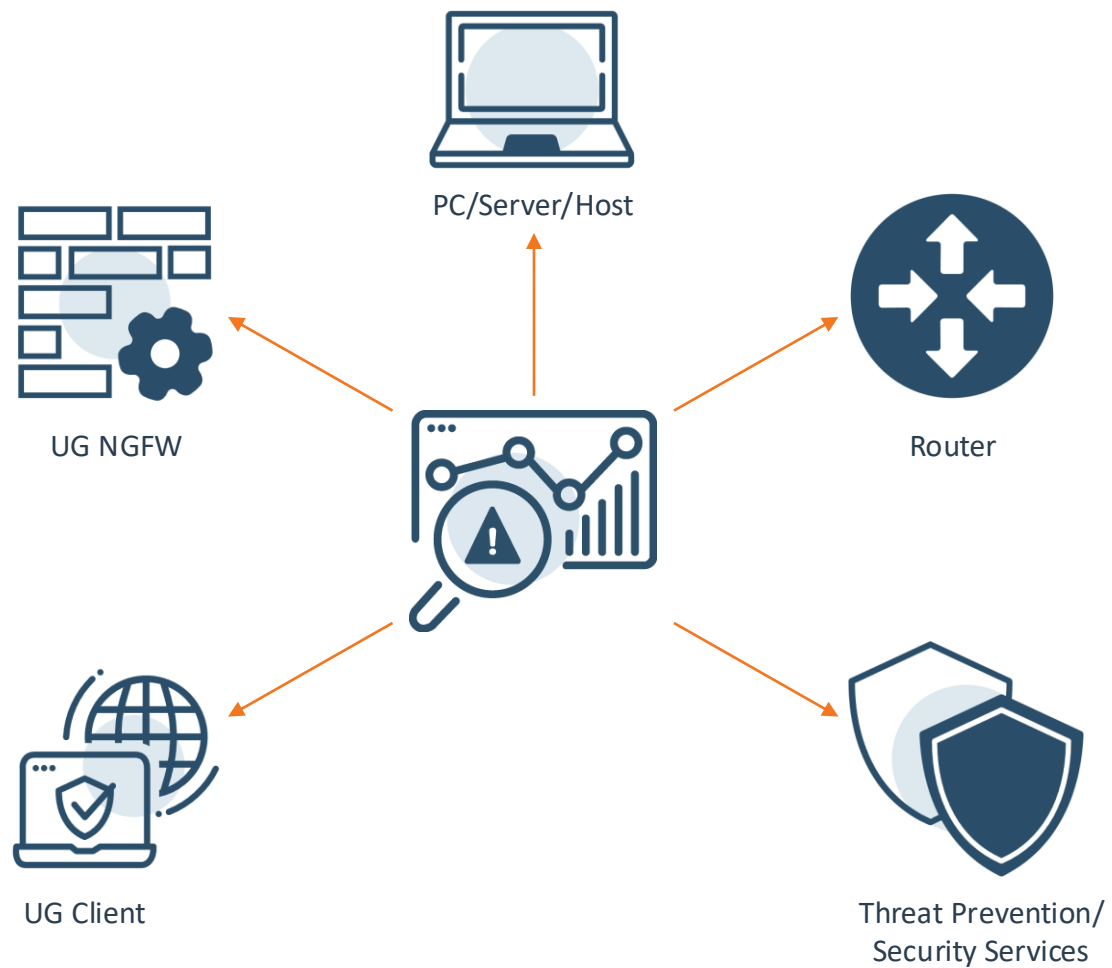




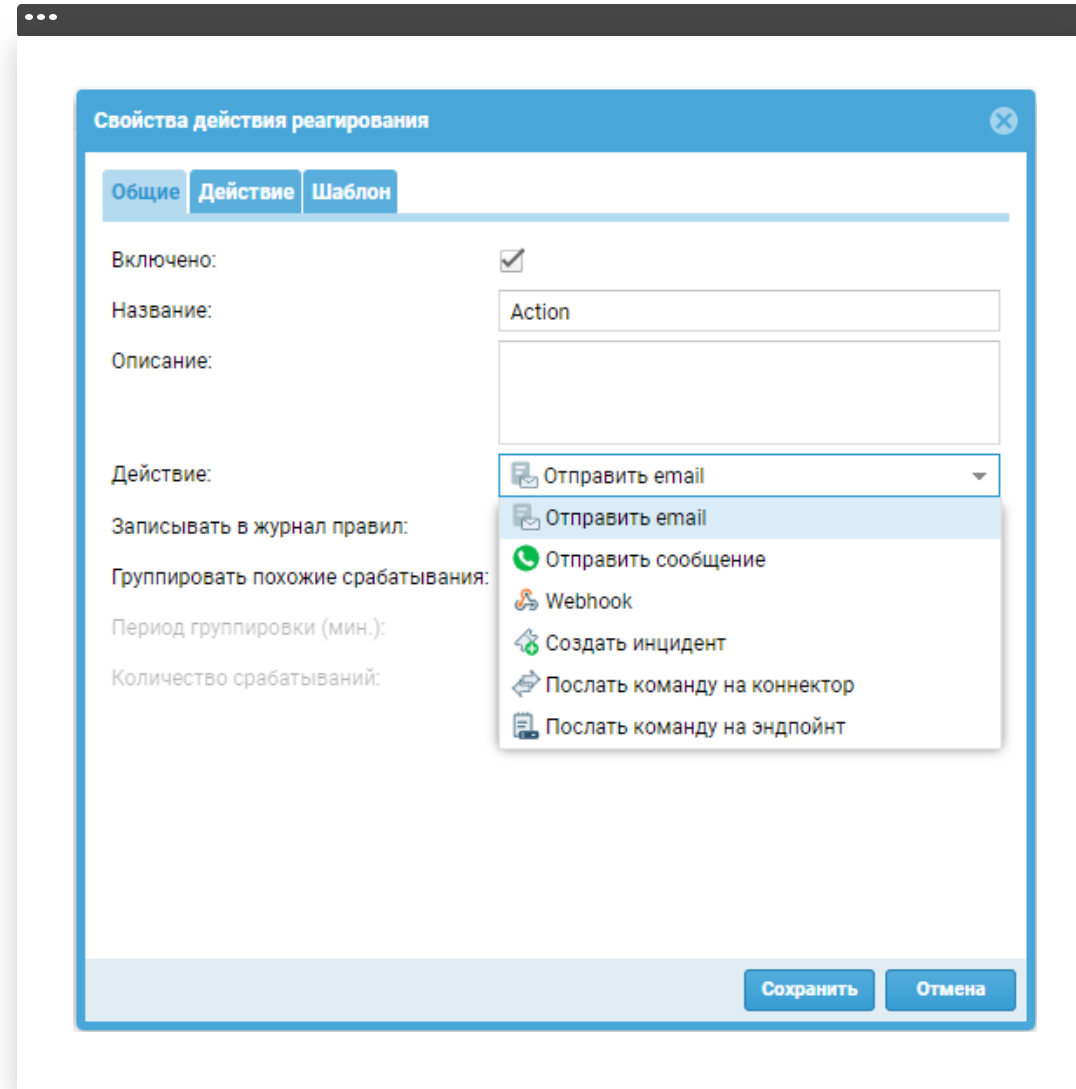
- Правила из библиотеки (более 750 правил, подготовленных MRC UG).
- Правила добавленные пользователем.
- Возможность экспорта/ импорта правил.

The screenshot displays the 'UserGate SIEM' interface, specifically the 'Аналитика' (Analytics) section. The top navigation bar includes 'Дашборд', 'Журналы и отчёты', 'Аналитика', 'Инциденты', 'Диагностика и мониторинг', and 'Настройки'. Below this, a sub-header 'Аналитика' is followed by a toolbar with buttons for 'Правила аналитики', 'Поиск', 'Действия реагирования', 'Срабатывания', 'Подробности срабатывания', and 'Процессы конечных устройств'. A secondary toolbar contains actions like 'Добавить', 'Редактировать', 'Копировать', 'Удалить', 'Включить', 'Отключить', 'Запустить сейчас', 'Показать срабатывания', 'Показать Все', 'Экспорт', and 'Импорт'. The main area is a table of rules with columns for 'Название', 'Приоритет', 'Категория сраба...', 'Условия', and 'Действия реагир...'. The table lists various security rules such as 'Bruteforce attempt', 'CVE-2022-30190 MSMT Vulnerability. "Follina"', and 'MSOffice run subprocess'. At the bottom, there is a pagination control showing 'Страница 1 из 2' and a search input field.

Название ↑	Приоритет	Категория сраба...	Условия	Действия реагир...
Bruteforce attempt	Важный	Performance	Condition	
Bruteforce attempt on web-server	Нормальный	Performance	Condition	
Connection to Webservice by a Signed Binary Proxy	Нормальный	Performance	Condition	
CVE-2022-30190 MSMT Vulnerability. "Follina"	Важный	Performance	Condition	
DCOM lateral movement (via MMC20)	Важный	Performance	Condition	
Detect Living Off Trusted Sites (LOTS) Project	Нормальный	Performance	Condition	
Detect unofficial domains may pose a security risk	Низкий	Performance	Condition	
Detect unofficial domains may pose a security risk (sysmon)	Нормальный	Performance	Condition	
Detect WShellExec function execution	Важный	Performance	Condition	
DHCPv6 DNS Takeover	Важный	Performance	Condition	
Drop Execution File From by Trusted Process	Важный	Performance	Condition	
Exploitation PrintNightmare	Критический	Performance	Condition	
MSOffice run subprocess	Важный	Performance	Condition	
RDP Shadowing	Важный	Performance	Condition	
Run subprocess from powershell.exe	Важный	Performance	Condition	
Running suspicious file without valid signature	Нормальный	Performance	Condition	
Start windows shell from Trusted process	Важный	Performance	Condition	
Suspicious IIS module registration	Важный	Performance	Condition	
Suspicious ms office child process	Важный	Performance	Condition	
Suspicious ms outlook child process	Важный	Performance	Condition	
Unusual Child Process of dnc.exe	Важный	Performance	Condition	



- 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.)



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

Настройки группировки
похожих событий

Свойства действия реагирования

Общие Действие Шаблон

Включено:

Название: Action

Описание:

Действие: Отправить email

Записывать в журнал правил:

Группировать похожие срабатывания:

Период группировки (мин.):

Количество срабатываний:

Отправить email

Отправить сообщение

Webhook

Создать инцидент

Послать команду на коннектор

Послать команду на эндпойнт

Сохранить Отмена

ПУТИ ЭВОЛЮЦИИ 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.

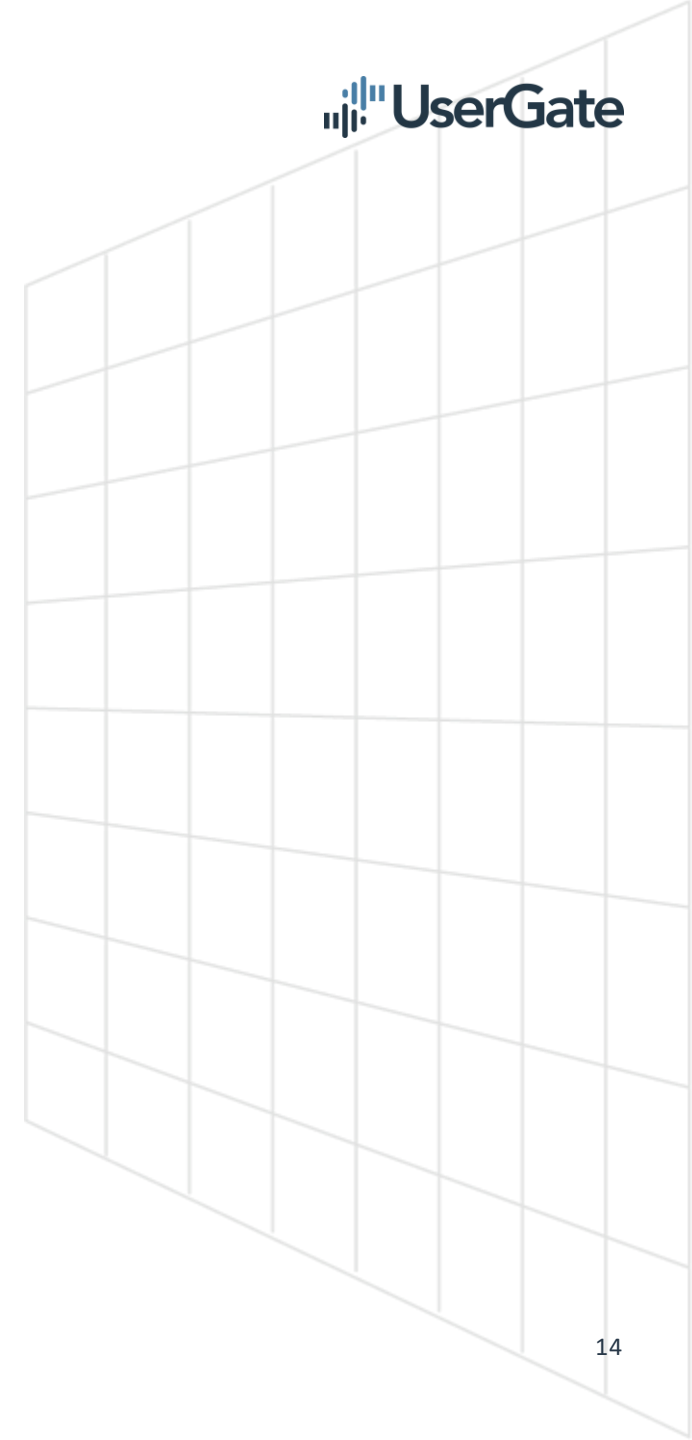
03

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!

TDIR — An Evolution



Gartner.



Где взяли экспертизу?

Где взяли экспертизу?
Сами написали

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

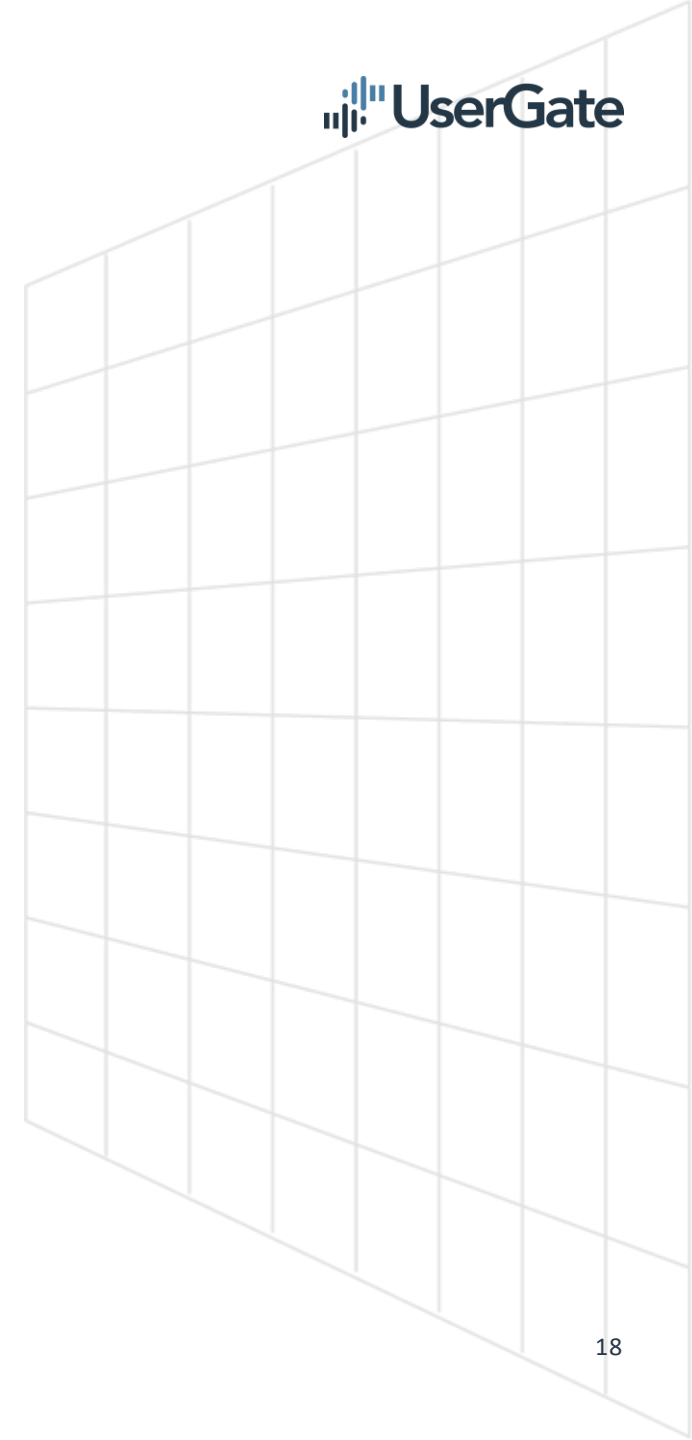
SIEM-системы неминуемо должны эволюционировать!

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.

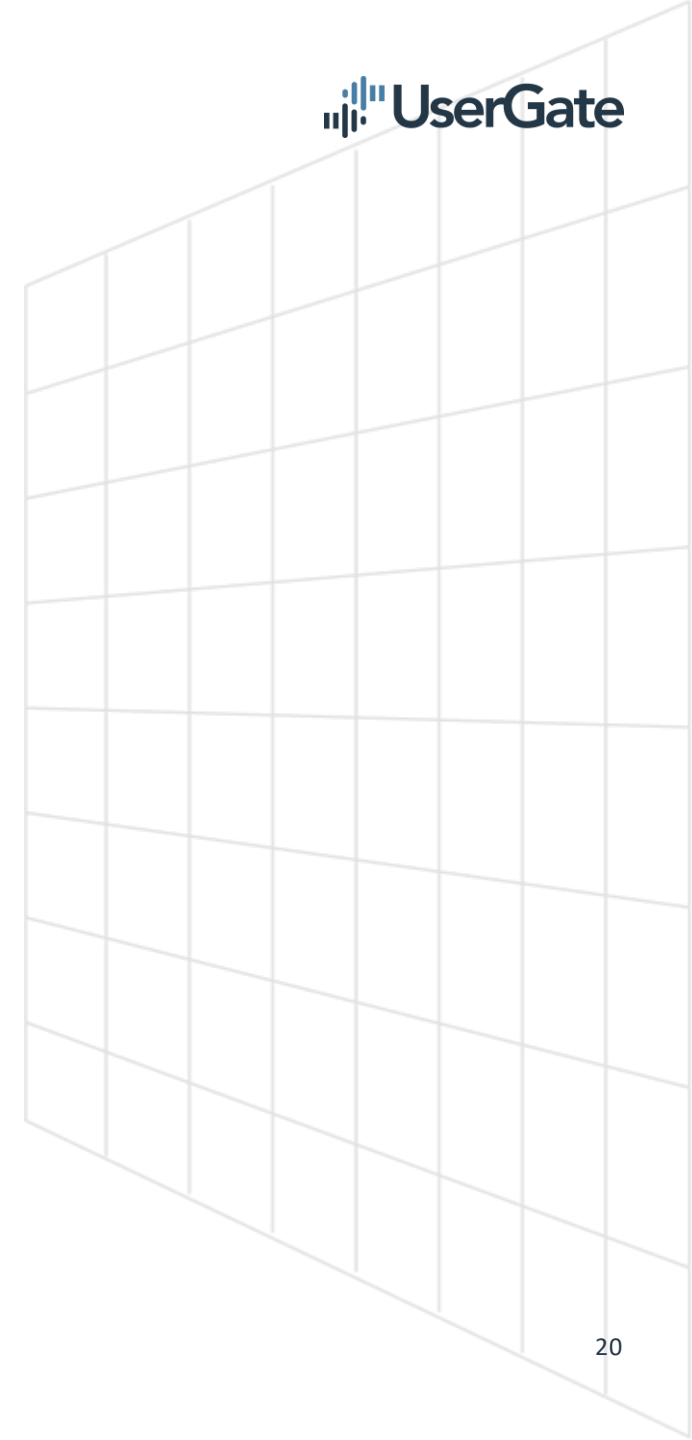


SIEM ПОМОЖЕТ

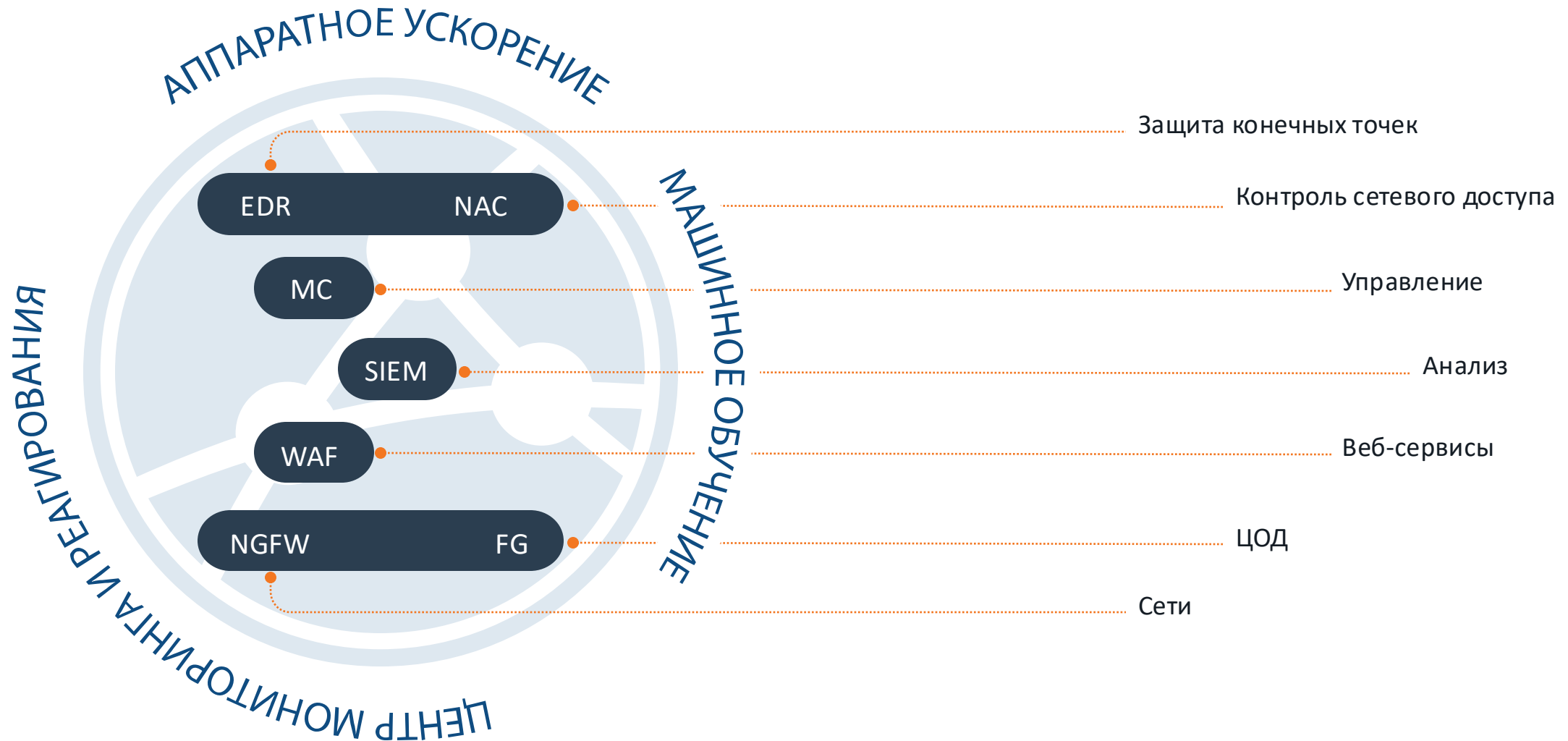
- Минимизировать финансовые потери из-за простоя бизнес-критических сервисов;
- Снизить риск утечки данных;
- Выполнить требования регулятора;
- Получить качественную экспертизу;
- Облегчить работу сотрудников в режиме постоянного дефицита кадров.

SIEM ПОМОЖЕТ

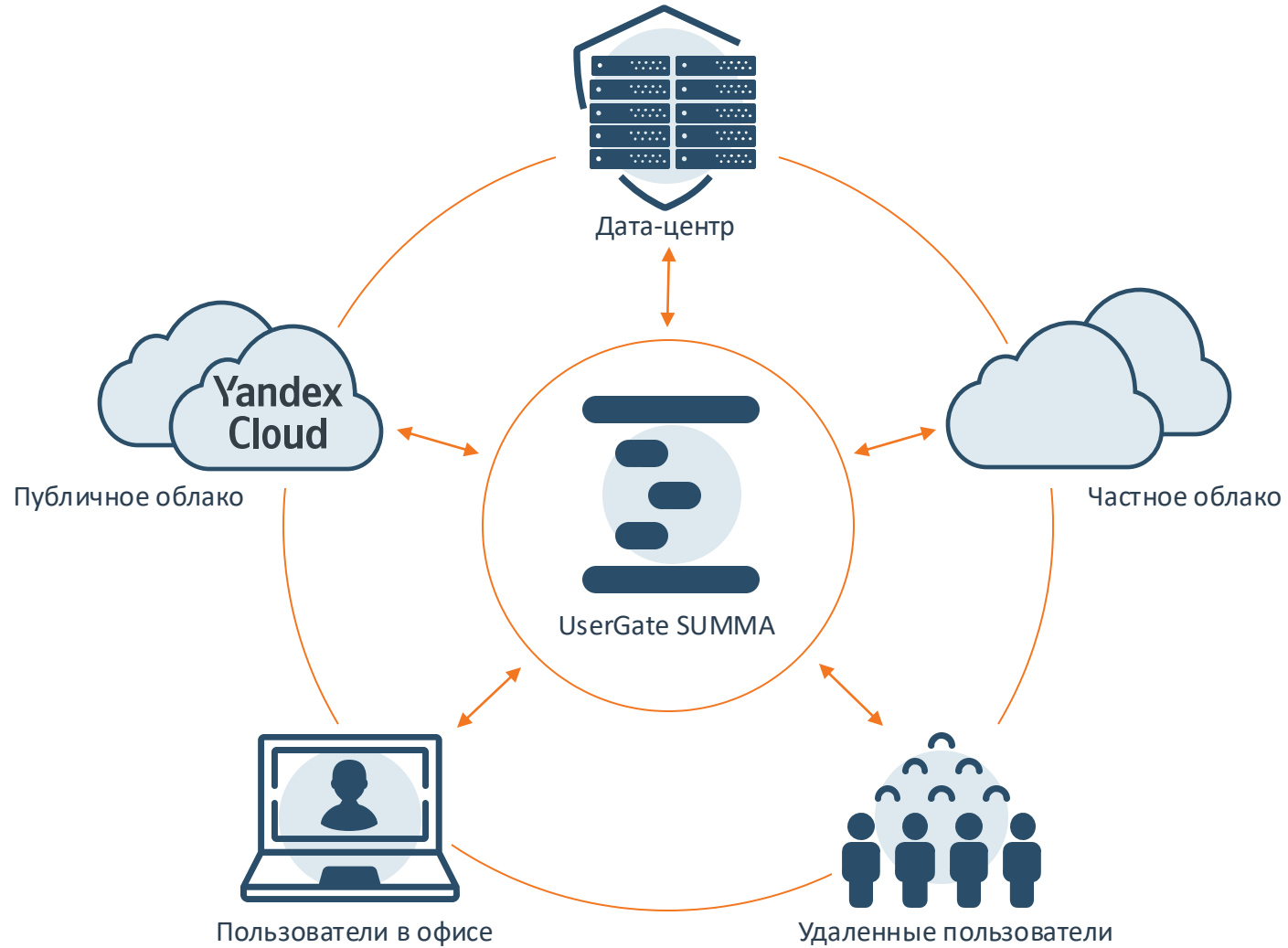
- Обезопасить свою компанию от сложных комплексных атак.
- Своевременно обнаружить инцидент.
- Оперативно реагировать на инцидент.
- Качественно расследовать инцидент.
- Не допустить повторения инцидента.



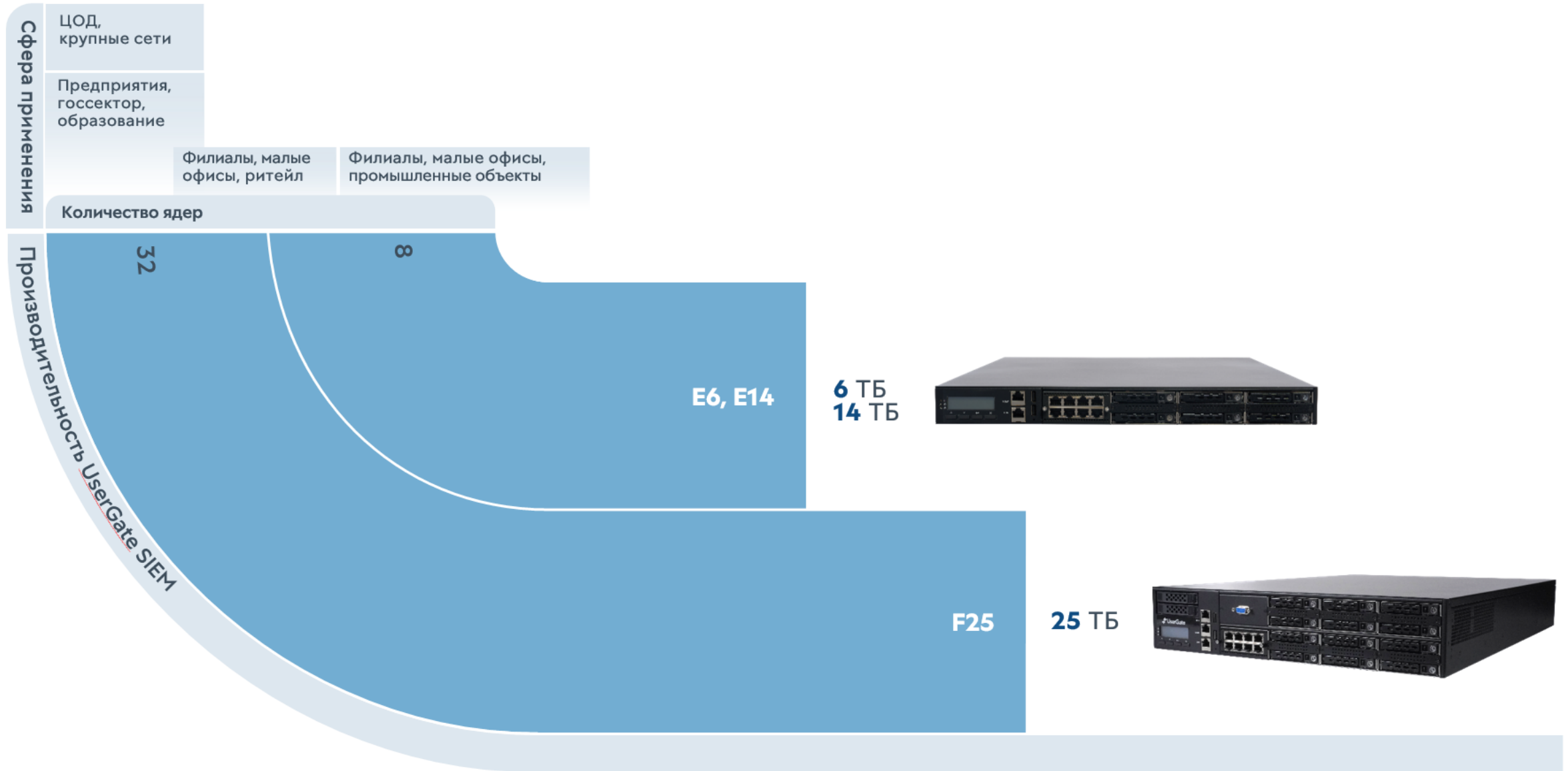
В ПАМКАХ USERGATE SUMMA



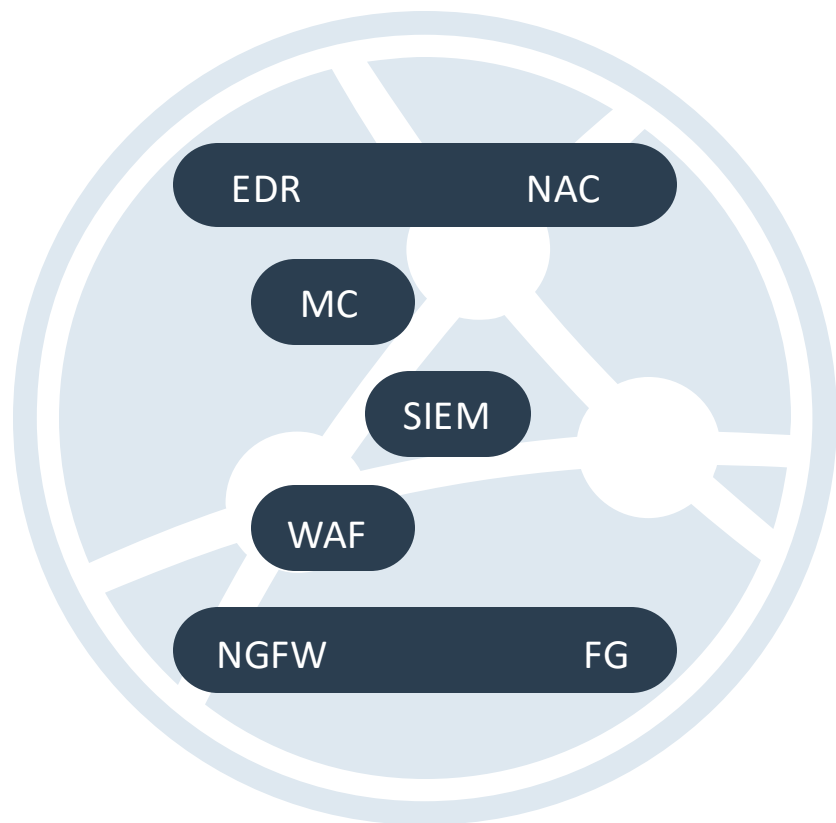
ZERO TRUST NETWORK ACCESS (ZTNA)



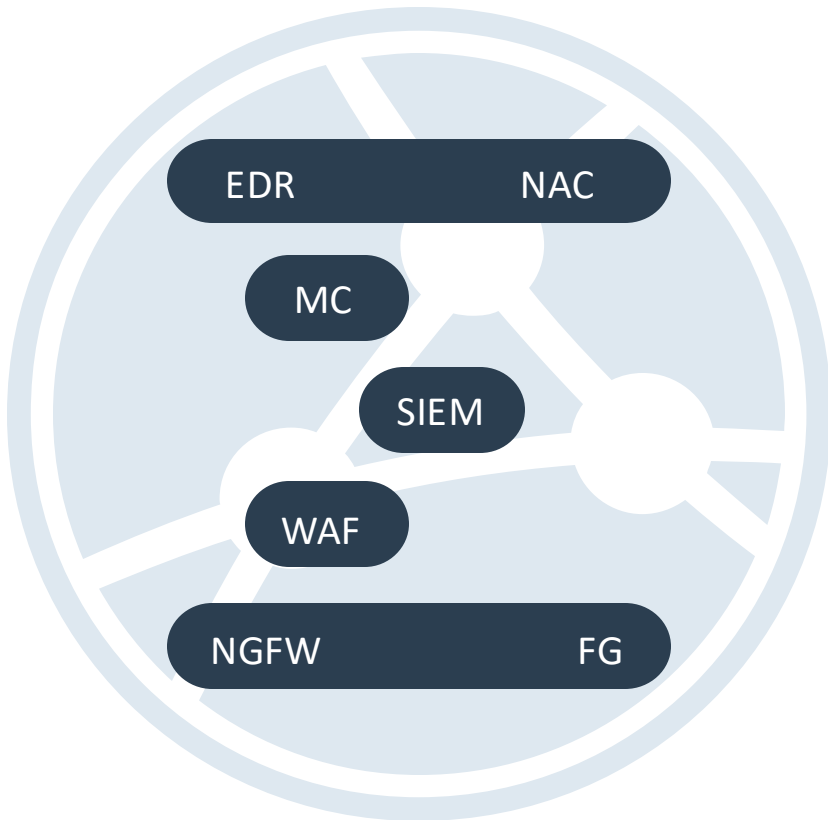
USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ВИРТУАЛЬНОМ ИСПОЛНЕНИИ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В
ОБЛАЧНОМ ИСПОЛНЕНИИ



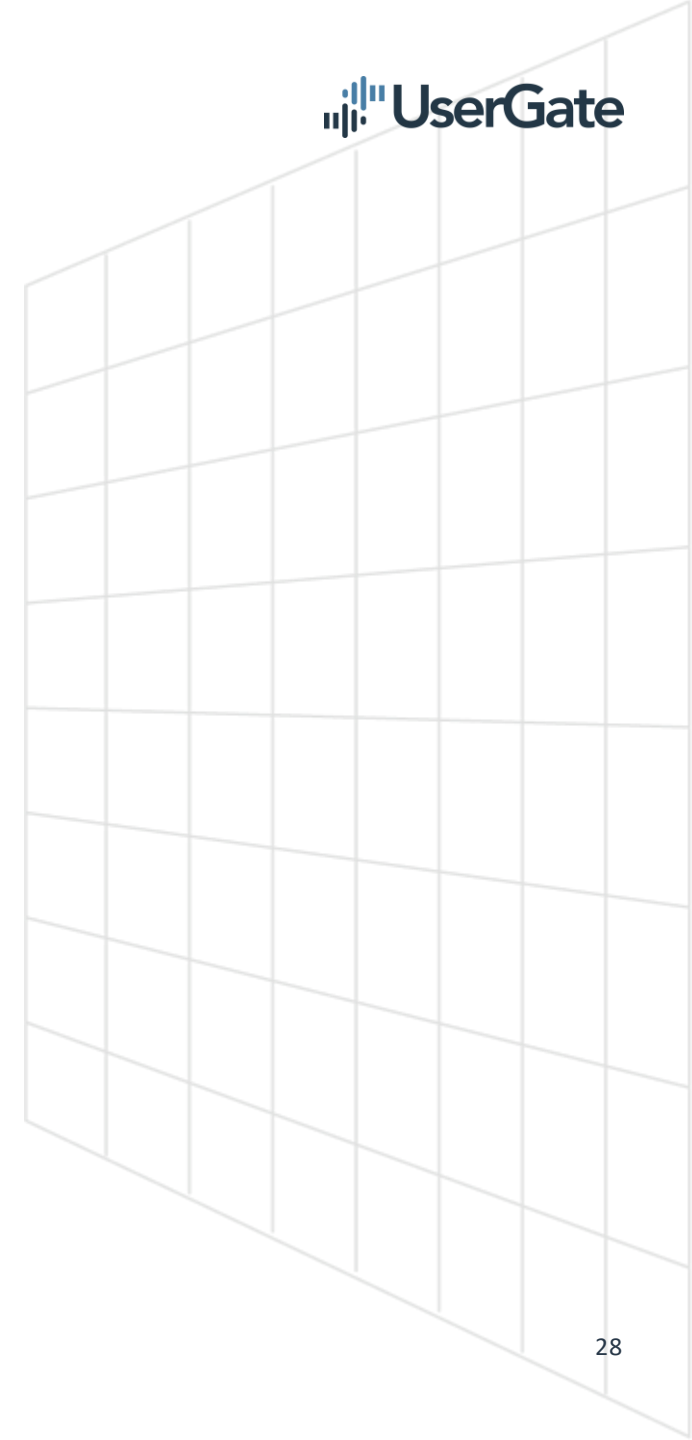
В любых облаках, которые поддерживают стандартные реализации vmware и kvm (openstack). Такие как **Yandex Cloud, Beeline cloud, МТС и VK.**

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

ПРЕИМУЩЕСТВА

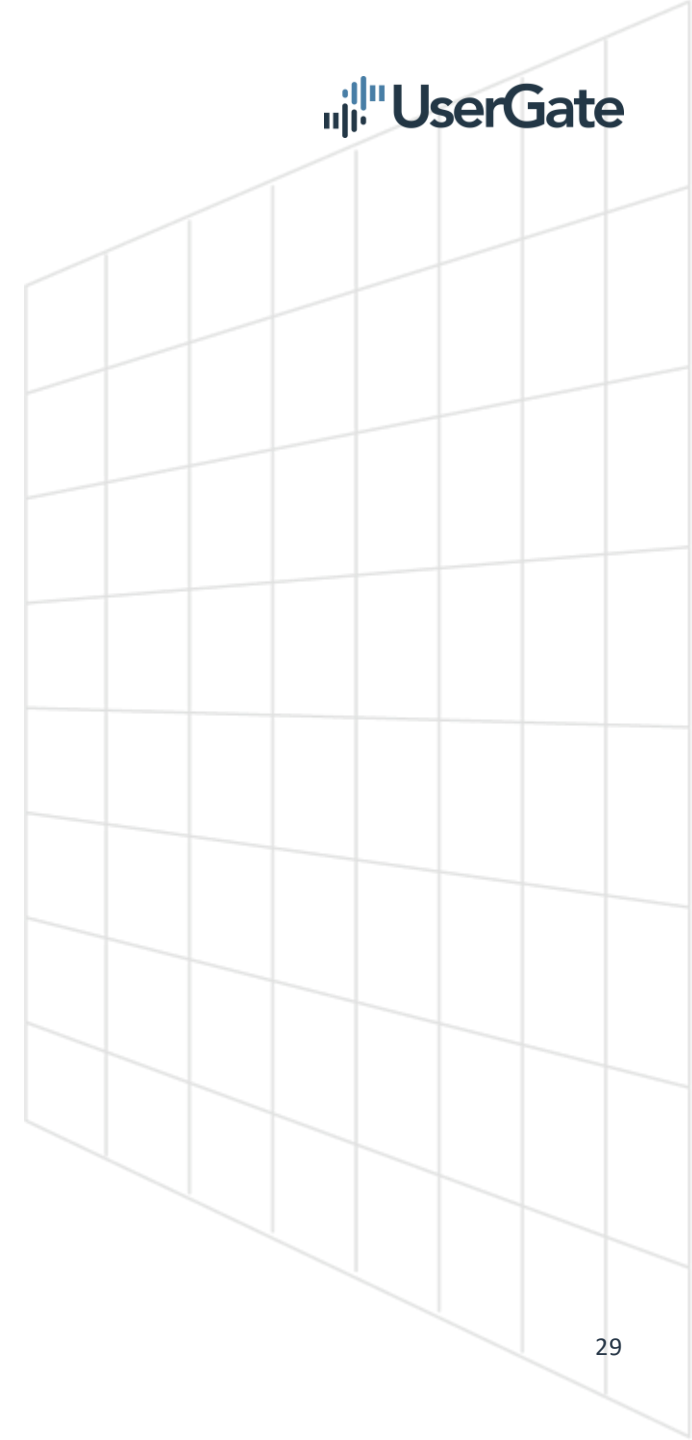
USERGATE SIEM

- 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.



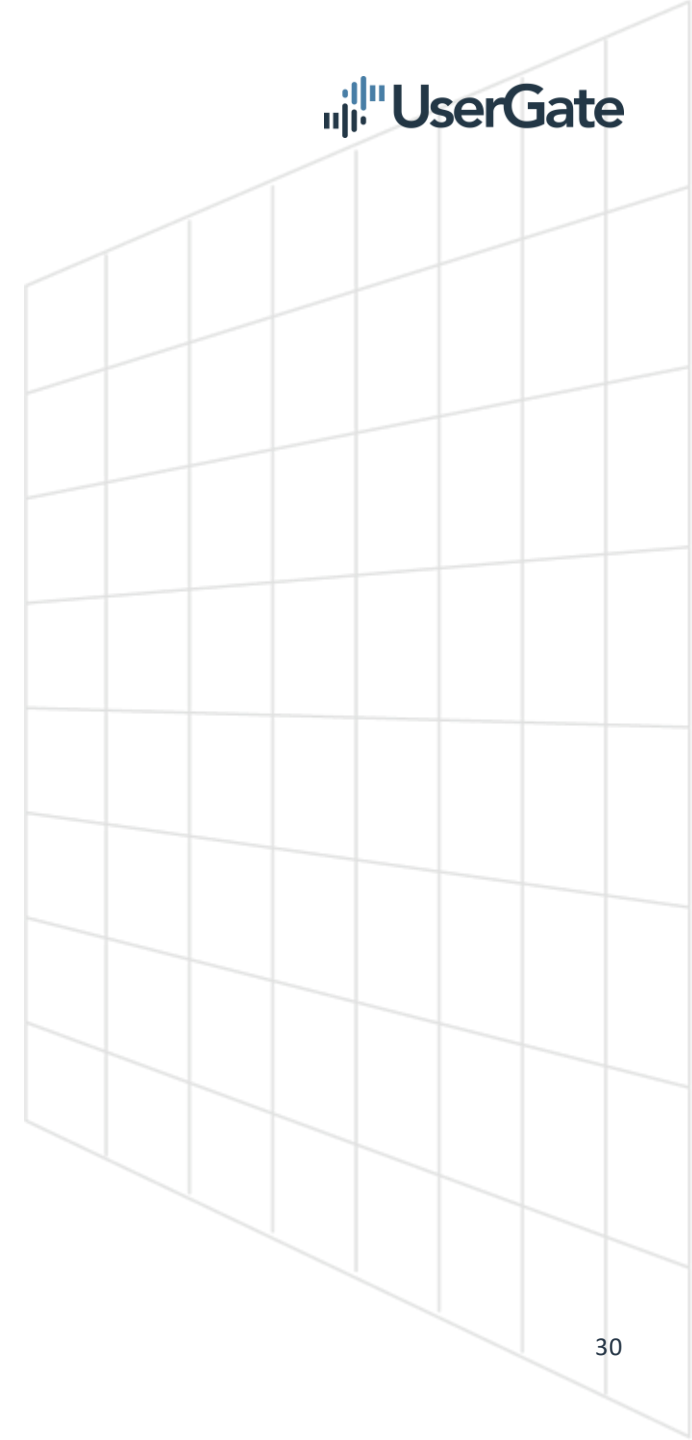
USERGATE SIEM

- 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.



Endpoint events Data

Custom logs normalization rule properties

Enabled:

Name:

Description:

Category:

Data column:

Regex:

Save Cancel

Endpoint events Data

Endpoint events Data

В разделе аналитики добавлены журналы о процессах на конечных устройствах.

Вся информация о когда-то запущенных процессах хранится тут.

The screenshot displays the UserGate SIEM interface. The top navigation bar includes 'UserGate SIEM' and menu items: 'Дашборд', 'Журналы и отчёты', 'Аналитика', 'Инциденты', 'Диагностика и мониторинг', and 'Настройки'. The 'Аналитика' section is active, with sub-menus for 'Правила аналитики', 'Поиск', 'Действия реагирования', 'Срабатывания', 'Подробности срабатывания', and 'Процессы конечных устройств'. The 'Процессы конечных устройств' sub-menu is selected, showing a 'Лог процессов' table and a 'Процесс: svchost.exe' details panel.

Лог процессов

08 Нояб 2023 г. | Конечное устройство: Все | Приложение: Все | Сброс

Время	Конечное устройство	Приложение	Идентификат...
19:31:38	MSEEDGEWIN10	SearchProtocolHost.e...	1700
19:31:34	MSEEDGEWIN10	DllHost.exe	6296
19:30:39	MSEEDGEWIN10	DllHost.exe	1284
19:29:45	MSEEDGEWIN10	DllHost.exe	2844
19:28:50	MSEEDGEWIN10	DllHost.exe	5592
19:27:56	MSEEDGEWIN10	DllHost.exe	3932
19:27:01	MSEEDGEWIN10	DllHost.exe	3348
19:26:07	MSEEDGEWIN10	DllHost.exe	2388
19:25:12	MSEEDGEWIN10	DllHost.exe	4968
19:24:18	MSEEDGEWIN10	DllHost.exe	4320
19:23:23	MSEEDGEWIN10	DllHost.exe	8788
19:22:28	MSEEDGEWIN10	DllHost.exe	8012
19:21:34	MSEEDGEWIN10	DllHost.exe	6592
19:20:39	MSEEDGEWIN10	DllHost.exe	3176
19:19:58	MSEEDGEWIN10	svchost.exe	8908
19:19:45	MSEEDGEWIN10	DllHost.exe	5560

Процесс: svchost.exe

Дерево процессов | Информация о процессе

Узел: 62a02caa-48d4-4ebf-b100-e1879e20353d
Время: 19:19:58
Конечное устройство: MSEEDGEWIN10
Хэш: A1385CE20AD79F55DF235EFFD9780C31442AA234
Приложение: C:\Windows\system32\svchost.exe
Версия: 6.2.17763.1
Субъект подписи: Microsoft Windows Publisher
Подписано: Microsoft Windows Production PCA 2011
Идентификатор процесса: 8908
Идентификатор родительского процесса: 552
Пользователь: SYSTEM
Командная строка: C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc

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

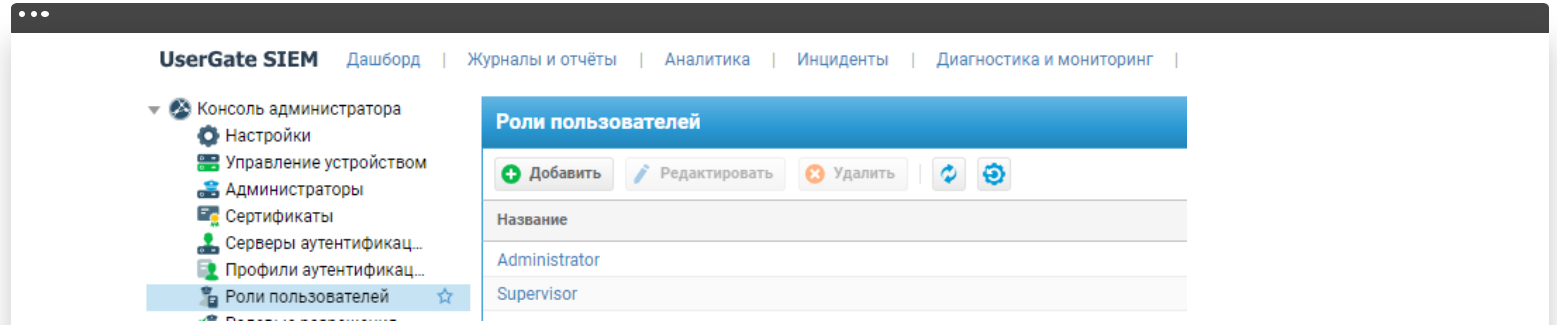
UserGate SIEM Дашборд | Журналы и отчёты | Аналитика | Инциденты | Диагностика и мониторинг

Администраторы

Администратор ↑	Описание	Профиль администрат...
Administrator	Default adm...	Корневой профиль
admin1		superadmin

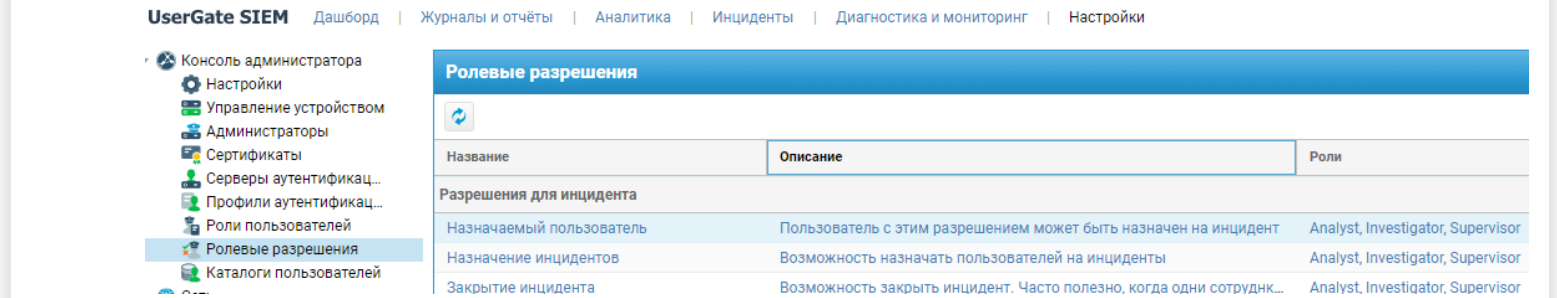
01

Роли пользователей



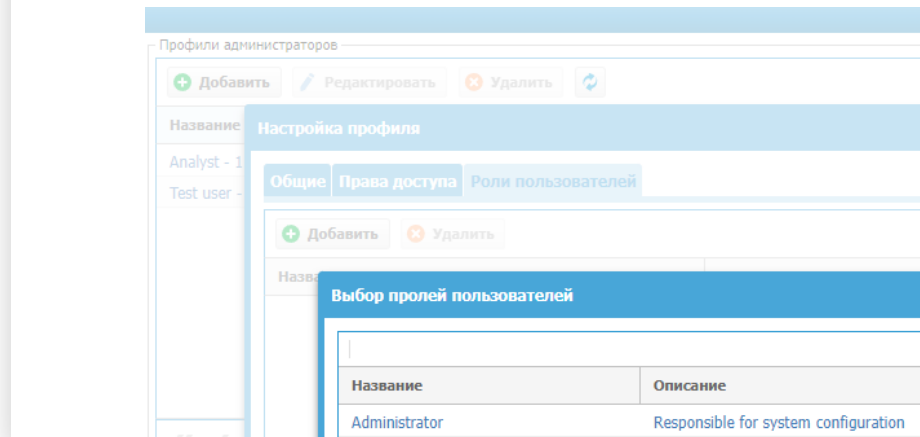
02

Ролевые разрешения



03

Профиль пользователя



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

UserGate SIEM Dashboard

Incidents | Dashboard | Logs and reports | Analytics | Incidents | Diagnostics and | admin | En |

[INC-1] Login to critical system attempt

Incidents log | INC-1: Login to critical system attempt

Generate report

Details

Incident type:	Incident	Status:	Opened
Incident priority:	Important	Resolution:	Unresolved
Rule:		Schema:	Incident

People

Assignee:	Administrat
Reporter:	Administrat
Last update by:	Administrat
Watchers:	Unwatched

Dates

Created:	Oct 12, 10:5
----------	--------------

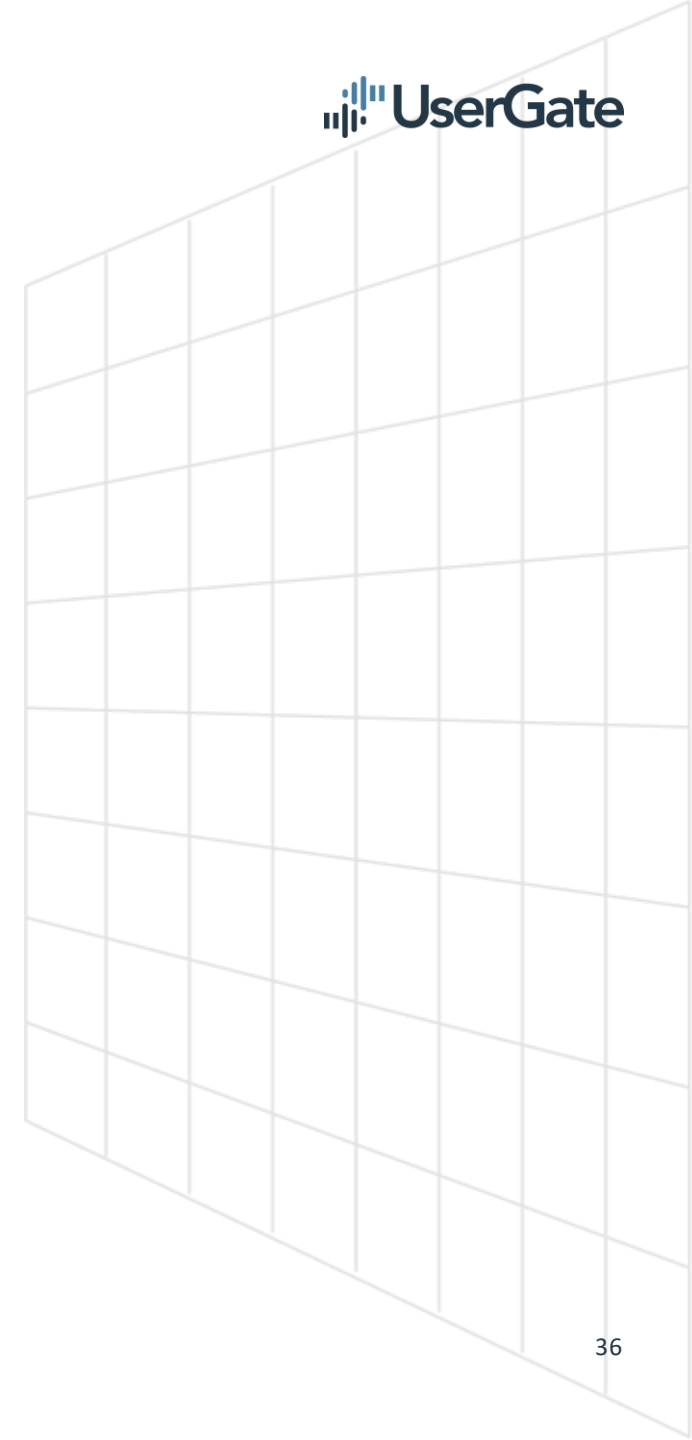
Форма для ГОССОПКА

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

- **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