

СОВРЕМЕННЫЙ ПОДХОД К РАЗРАБОТКЕ SIEM-СИСТЕМЫ НА ПРИМЕРЕ USERGATE SIEM



Дмитрий Чеботарёв
Менеджер по развитию UserGate SIEM

Делаем безопасное настоящим





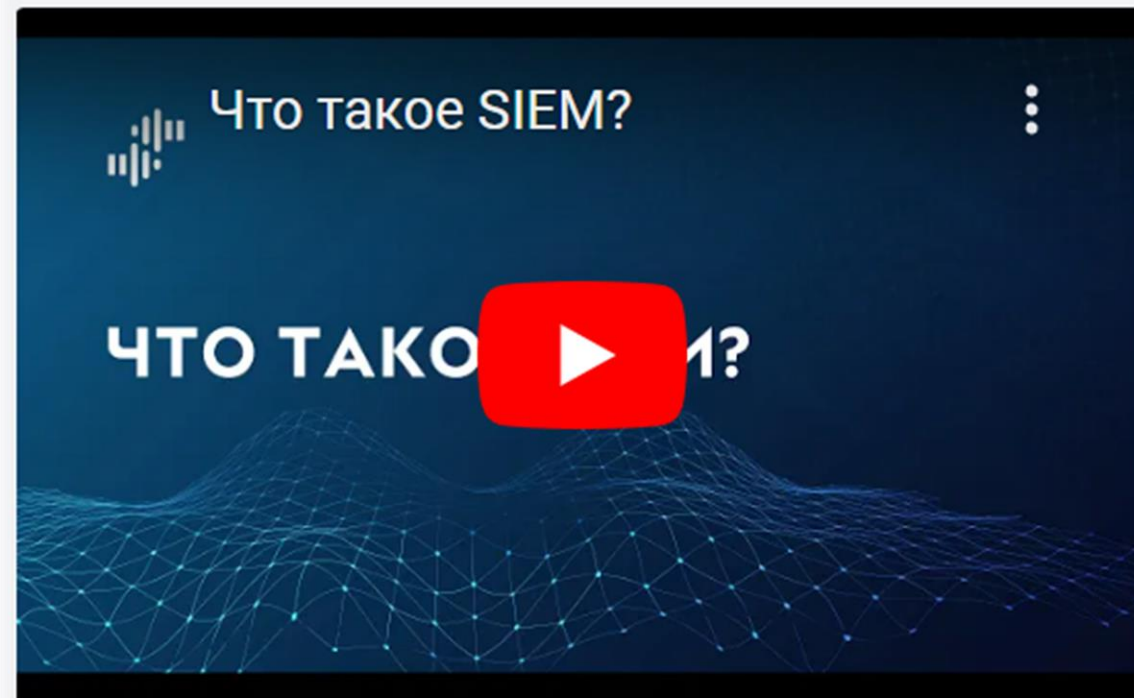
ЧТО ТАКОЕ SIEM?

ЧТО ТАКОЕ SIEM?

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

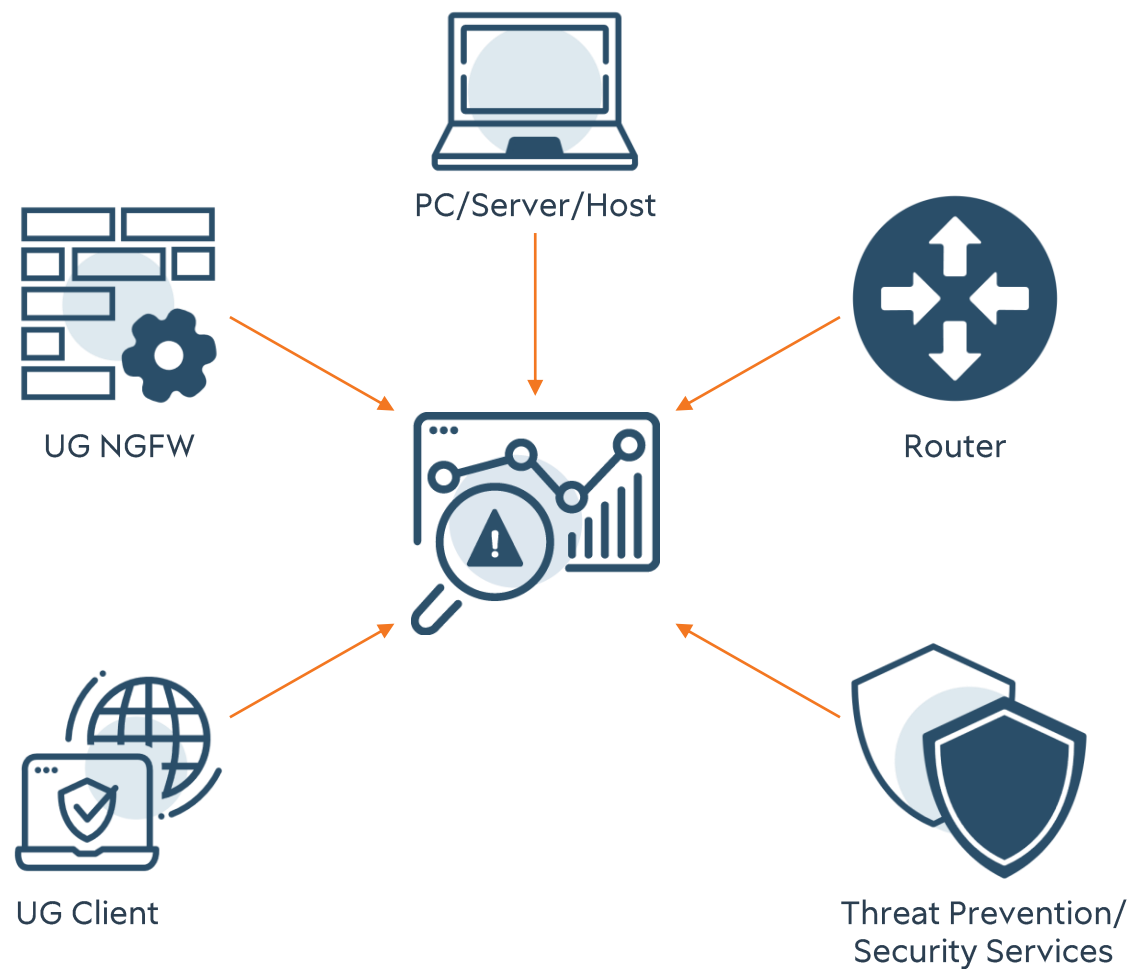
<https://www.youtube.com/watch?v=ddAzEN1iC5o>
https://vkvideo.ru/video-211747929_456239139
<https://rutube.ru/video/1d4c3321f002d531a6ef9cbd765fedf4/>

Link Preview ▾

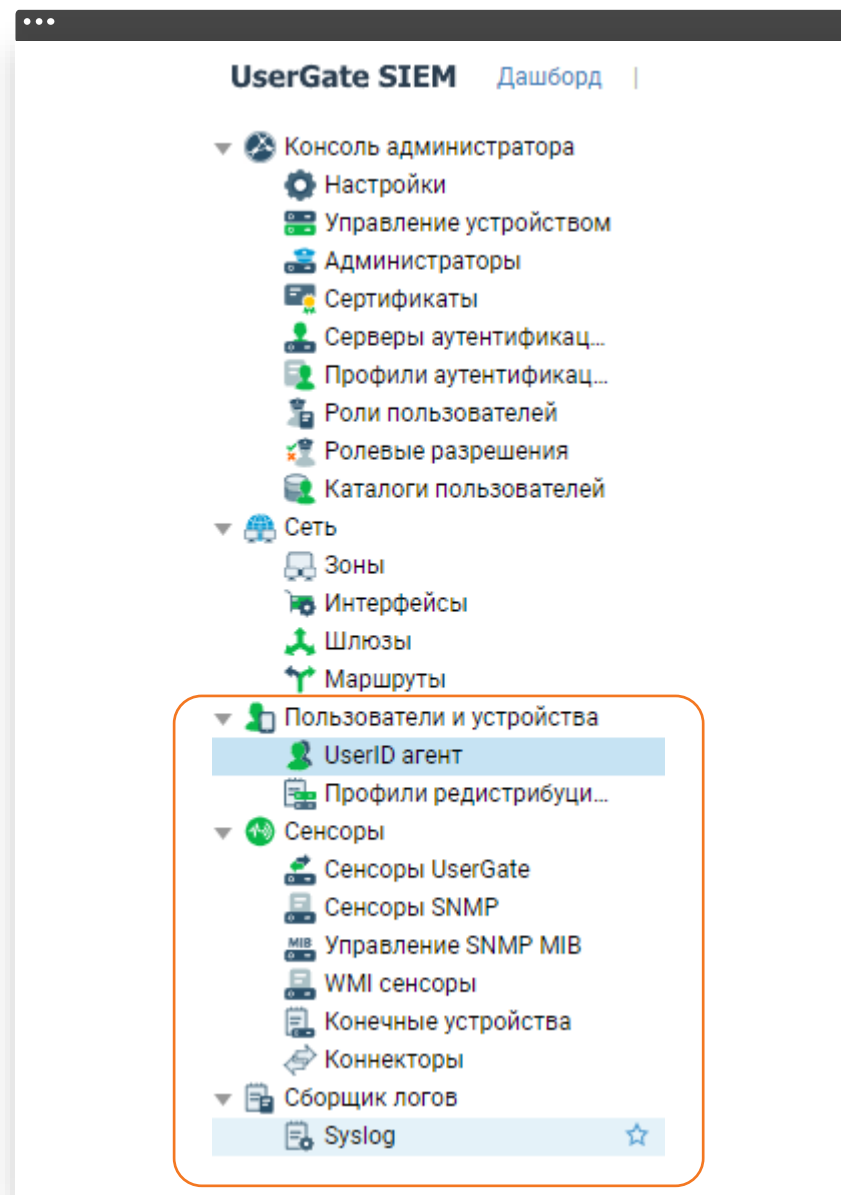


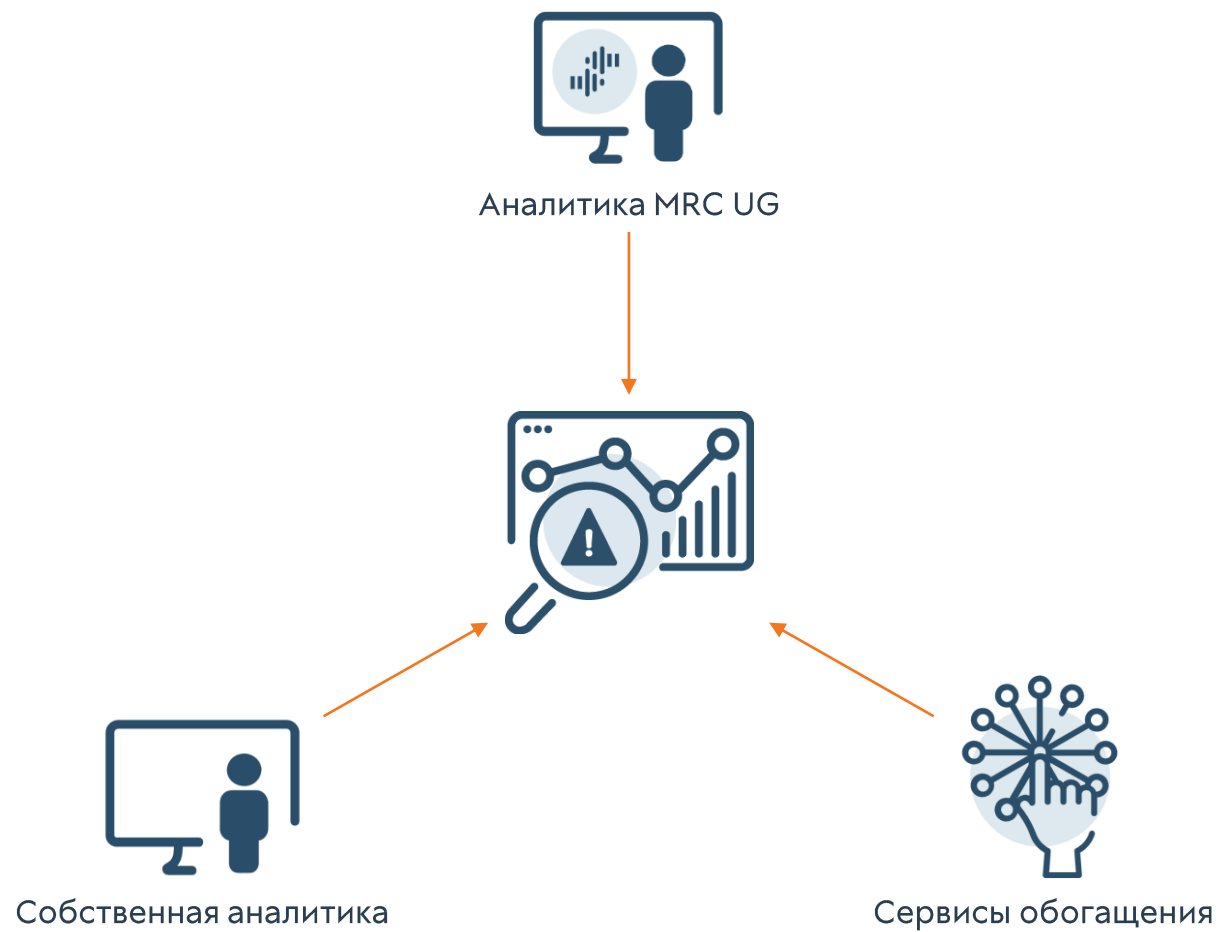
Что такое SIEM?

[YouTube](#) | [UserGate](#)



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





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

UserGate SIEM

Дашборд | Журналы и отчёты | **Аналитика** | Инциденты | Диагностика и мониторинг | Настройки

Аналитика

Правила аналитики

Поиск

Действия реагирования

Срабатывания

Подробности срабатывания

Процессы конечных устройств

Добавить

Редактировать

Копировать

Удалить

Включить

Отключить

Запустить сейчас

Показать срабатывания

Показать Все

Экспорт

Импорт

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

«

«

Страница

1

из 2

»

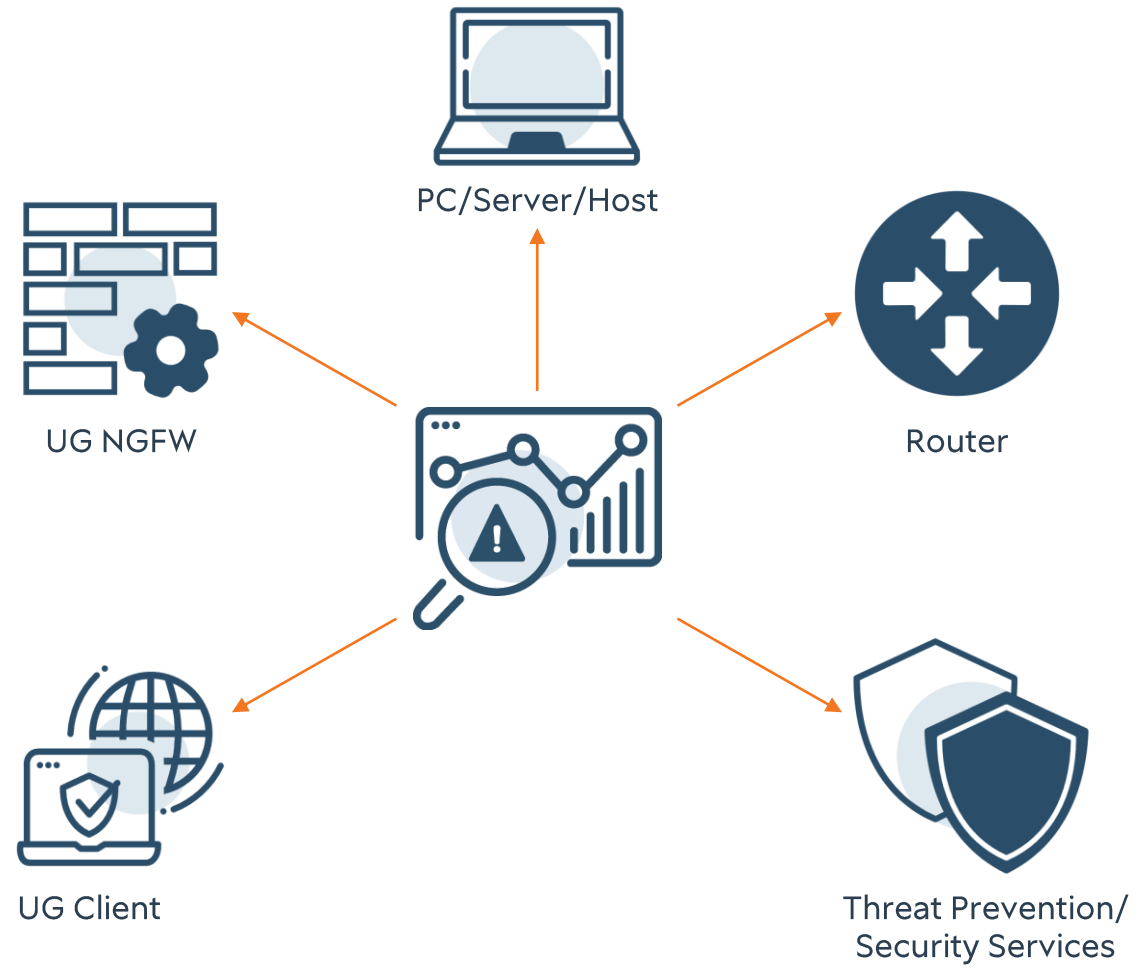
»

↺

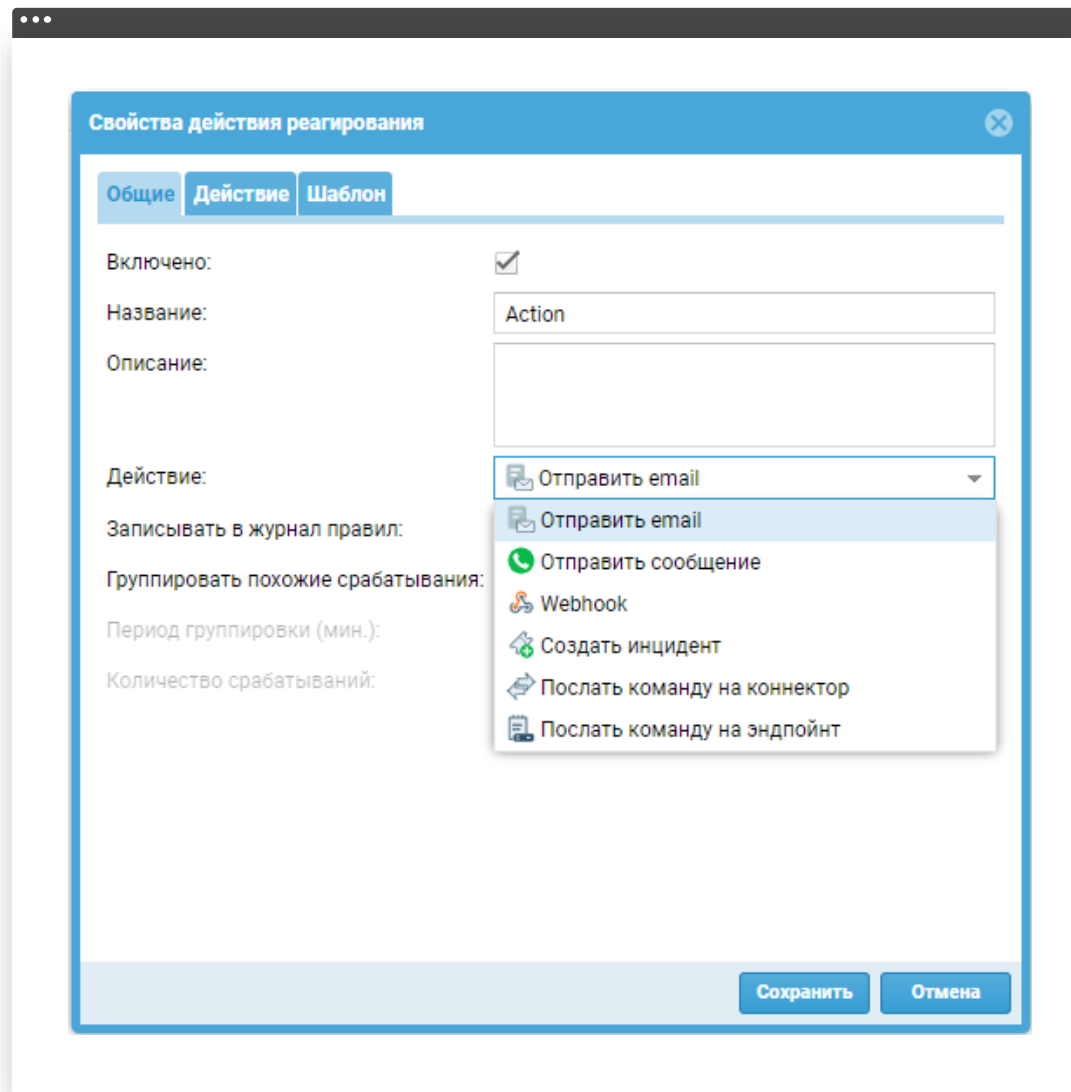
Найти:

Искать в имени и описании:

☐



- 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.)



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

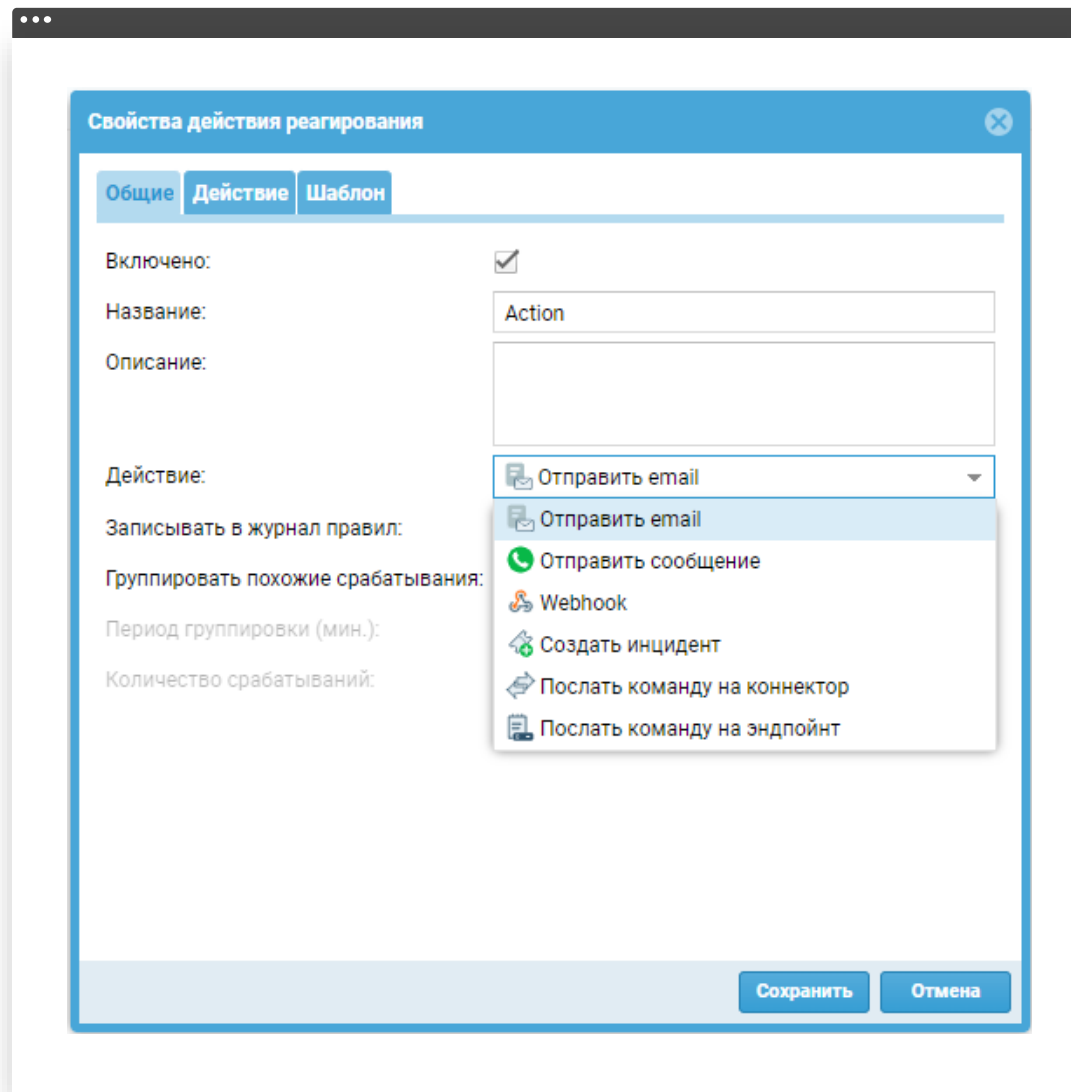
Послать команду на коннектор

Послать команду на эндпойнт

Сохранить Отмена

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

Настройки группировки
похожих событий



ПУТИ ЭВОЛЮЦИИ SIEM

Log Manager

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

Классический SIEM

- правила корреляции;
- анализ.

Экосистемный SIEM

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

01

02

03

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.

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!

TDIR — An Evolution



Gartner.

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.

- 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.

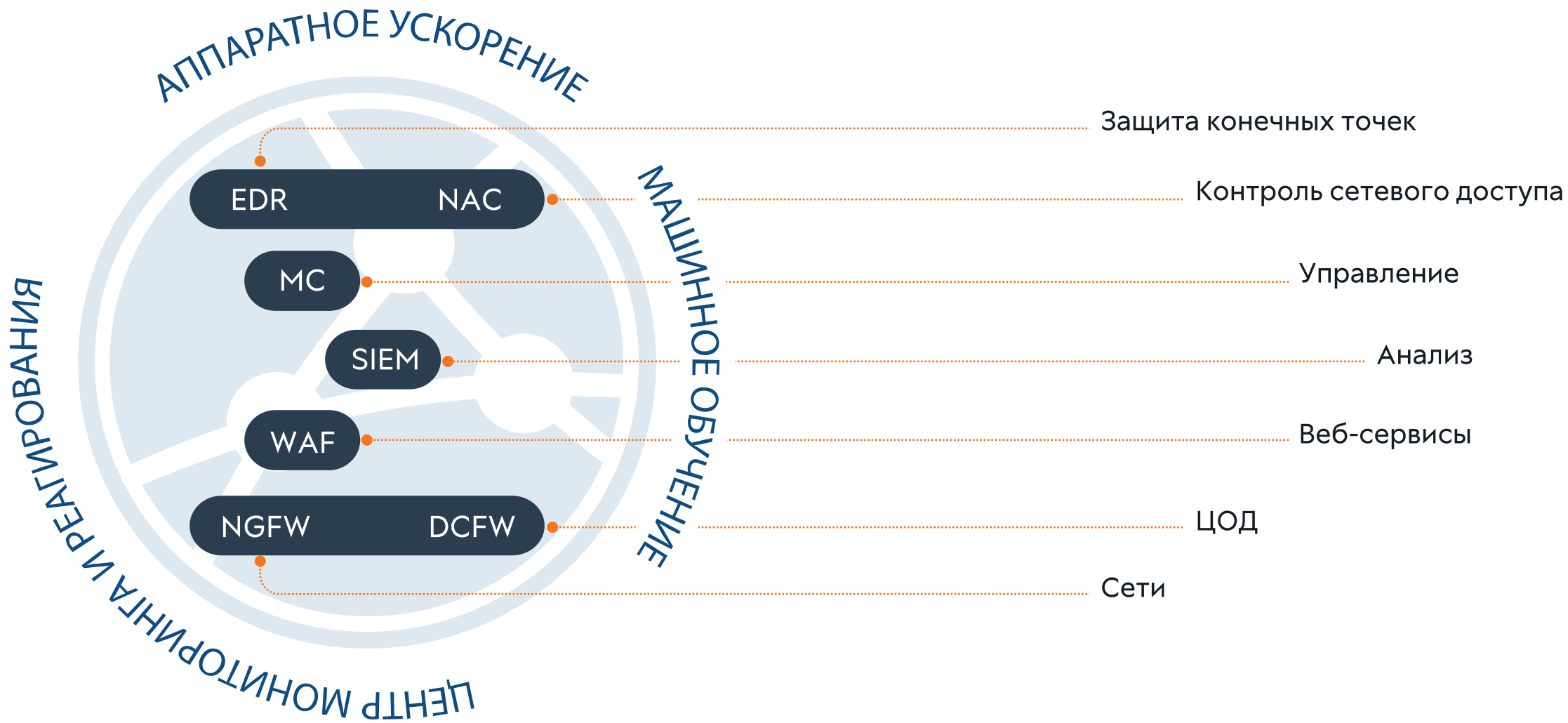
- Обезопасить свою компанию от сложных комплексных атак.
- Своевременно обнаружить инцидент.
- Оперативно реагировать на инцидент.
- Качественно расследовать инцидент.
- Не допустить повторения инцидента.

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

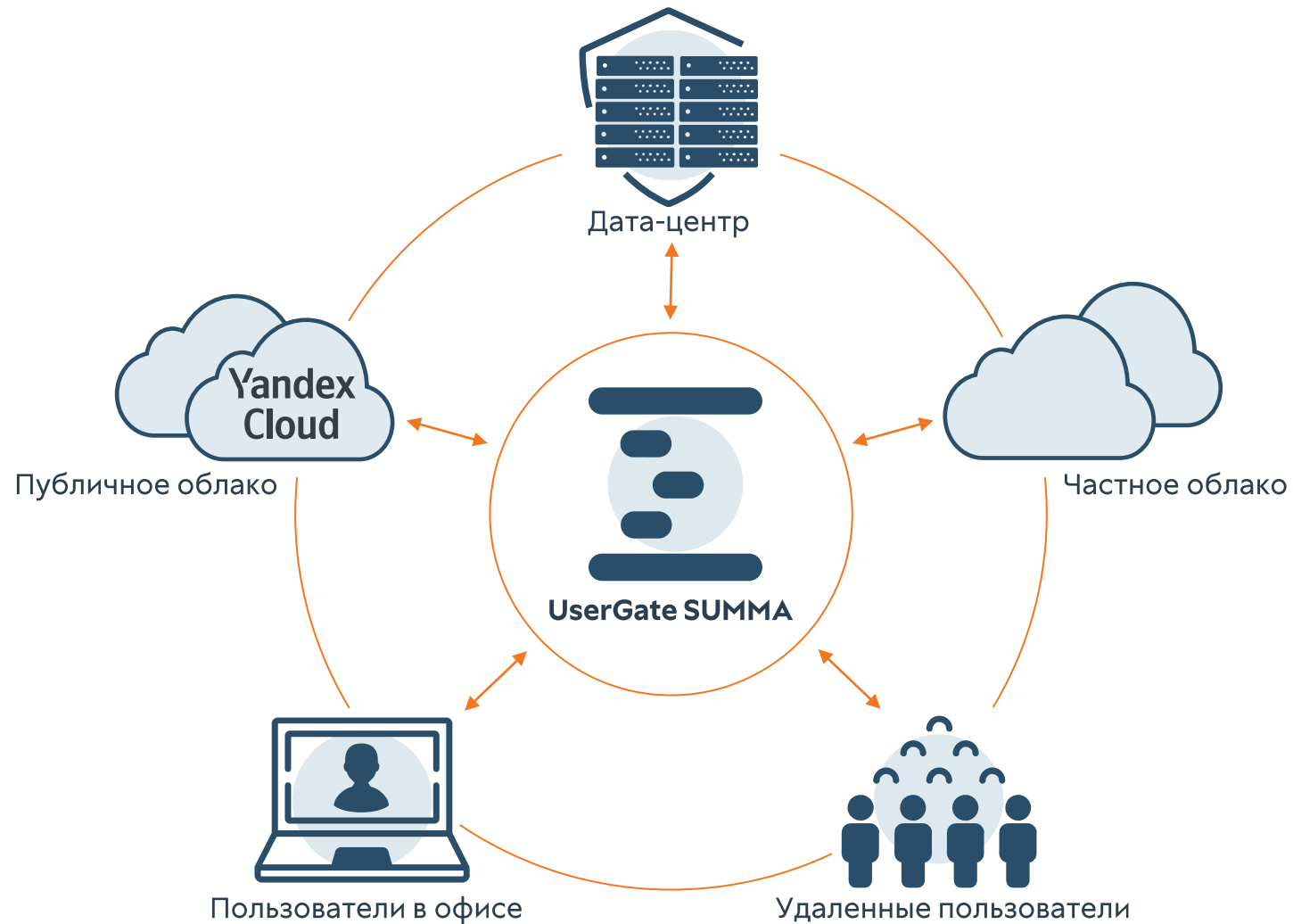
Защита цифрового мира технологиями, которым доверяют без границ



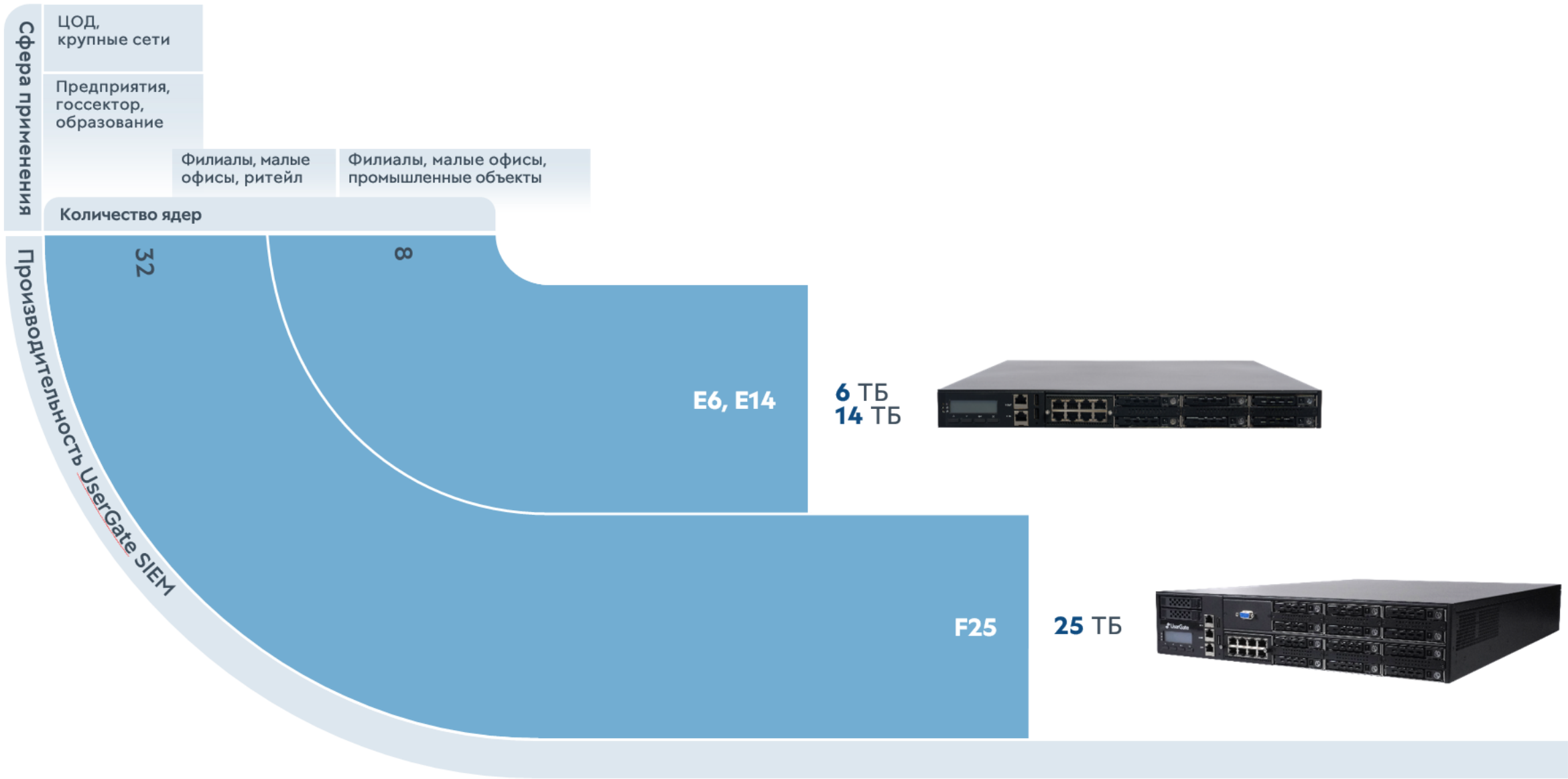
В ПАМКАХ USERGATE SUMMA



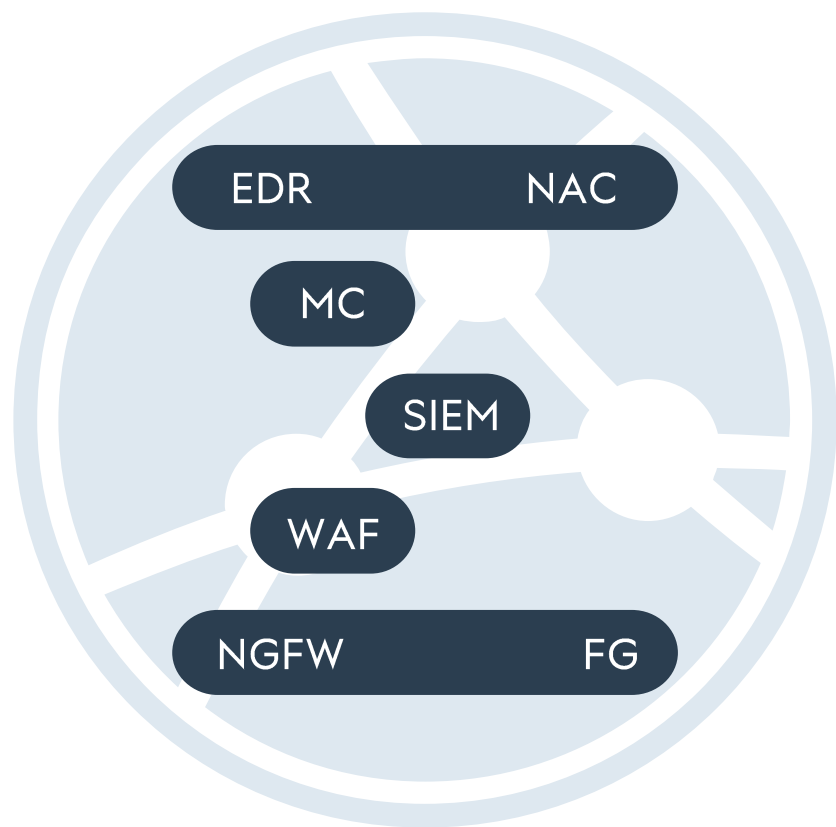
ZERO TRUST NETWORK ACCESS (ZTNA)



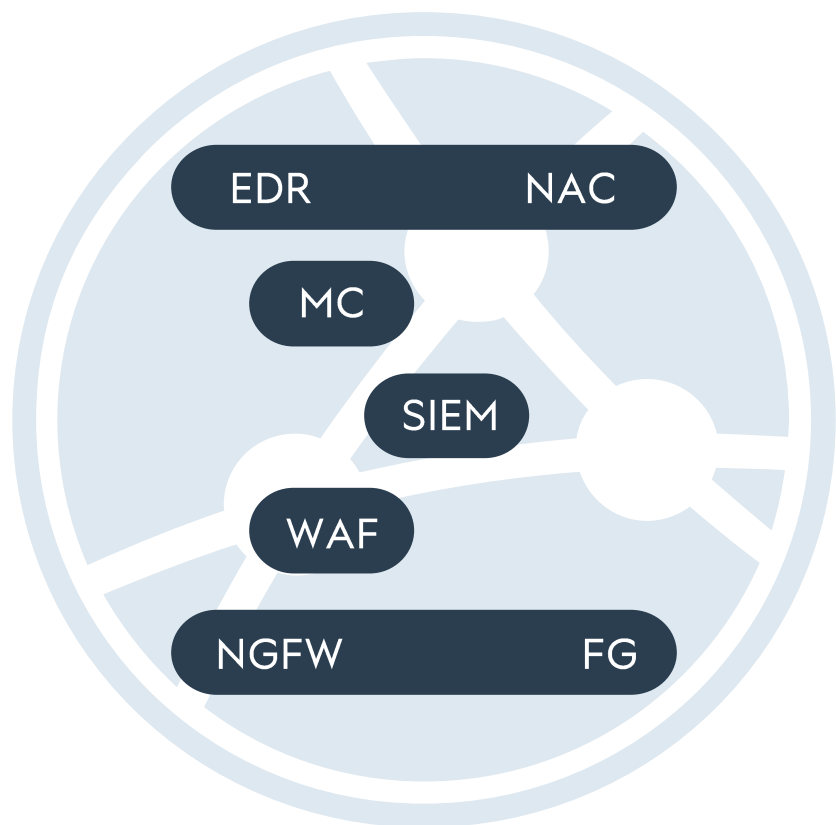
USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В ВИРТУАЛЬНОМ ИСПОЛНЕНИИ



ВСЕ ПРОДУКТЫ USERGATE SUMMA ДОСТУПНЫ В
ВИРТУАЛЬНОМ ИСПОЛНЕНИИ

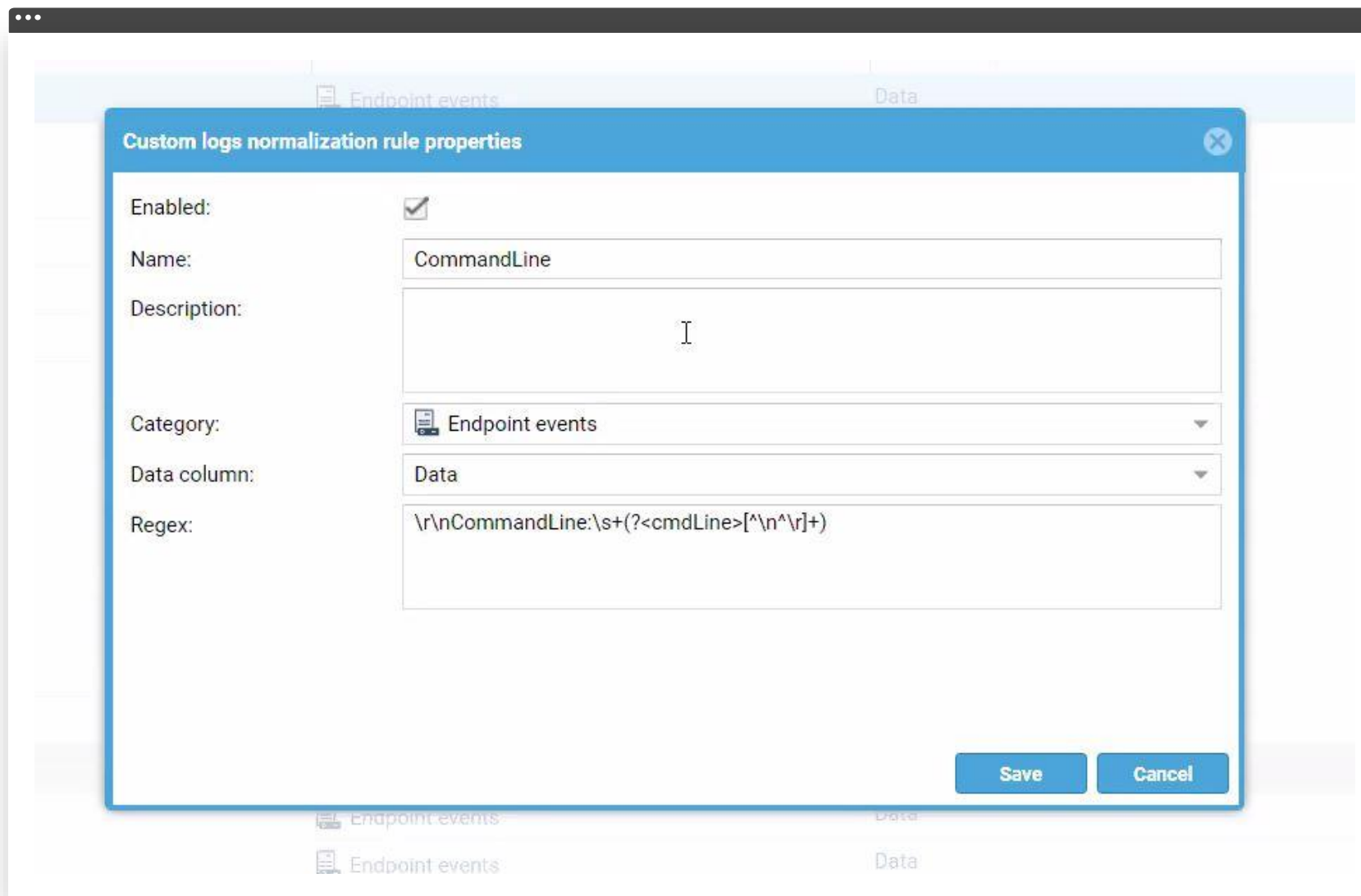


В любых облаках, которые поддерживают стандартные реализации vmware и kvm (openstack). Такие как **Yandex Cloud, Beeline cloud, МТС и VK.**

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

ПРЕИМУЩЕСТВА

- **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.**

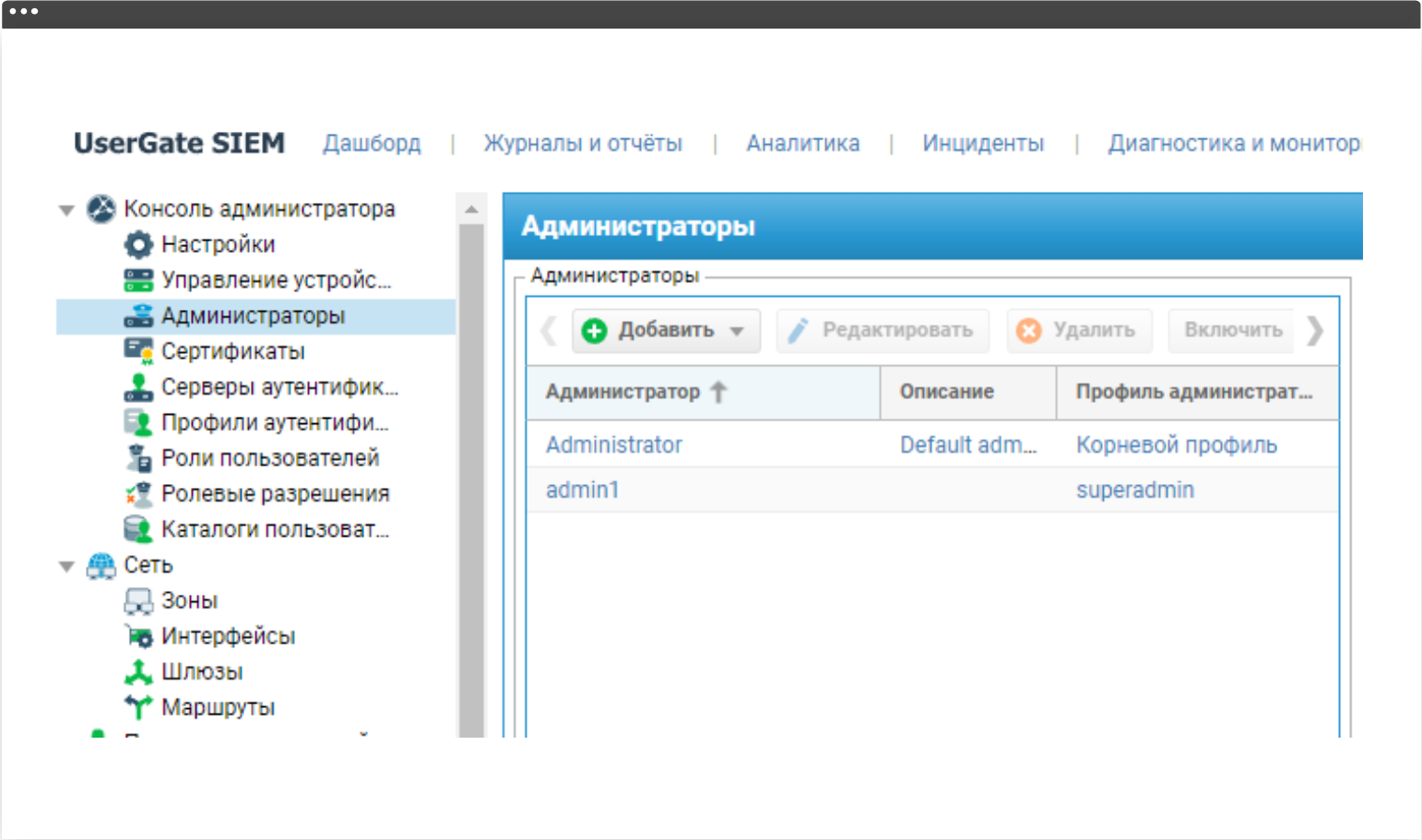


The screenshot shows a web application interface with a modal dialog box titled "Custom logs normalization rule properties". The dialog has a blue header bar with a close button (X) in the top right corner. The background interface shows a sidebar with a tree view containing "Endpoint events" and "Data", and a main content area with a table. The dialog contains the following fields:

- Enabled:** A checkbox that is checked.
- Name:** A text input field containing "CommandLine".
- Description:** A large text area with a cursor, currently empty.
- Category:** A dropdown menu showing "Endpoint events" with a folder icon.
- Data column:** A dropdown menu showing "Data".
- Regex:** A text input field containing the regex pattern: `\r\nCommandLine:\s+(?<cmdLine>[^\n\r]+)`

At the bottom right of the dialog are two buttons: "Save" and "Cancel".

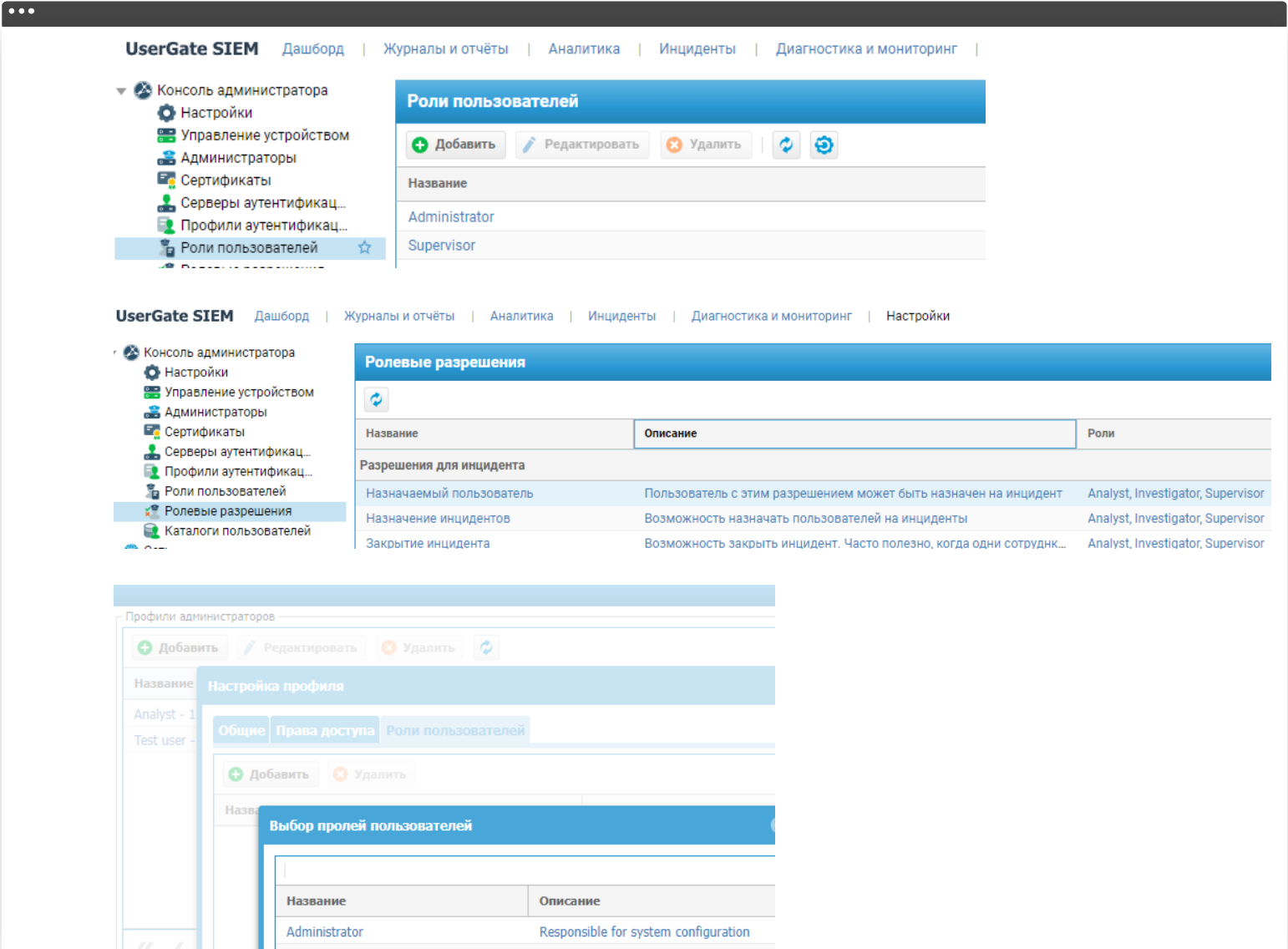
- Управление пользователями в системе.
- Добавление пользователей/ групп из LDAP.
- Отображение активных сессий пользователей.



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

▼ Logs

Events

Web access

DNS

Traffic

IDPS

SCADA

SSH inspection

Search history

▼ Endpoints

Endpoint events

Endpoint rules

Endpoint applications

Endpoint hardware

Syslog

Mail security

UserID

Logs export

Custom logs normalization

▼ Reports

Report templates

Custom report templates

Report rules

Generated reports

▼ Incident reports

Incident report templates

Incident report rules

Generated incident reports

▼ Log Analyzer logs

Events

UserGate SIEM | Dashboard | Logs and reports | Analytics | Incidents | Diagnostics and

admin | En |

Incidents

Create incident

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

[INC-1] Login to critical system attempt

Edit | Comment | Assign | Workflow | 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

Description

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

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

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.

ЧТО НУЖНО ПРЕДПРИНЯТЬ БИЗНЕСУ ДЛЯ ВЫПОЛНЕНИЯ **ТРЕБОВАНИЙ** **ЗАКОНОДАТЕЛЬСТВА**

**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 реагирование 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

**Мы защищаем вас,
пока вы делаете мир лучше**



СПАСИБО ЗА ВНИМАНИЕ



Дмитрий Чеботарёв
Менеджер по развитию UserGate SIEM