

Современная SIEM-система на примере UserGate SIEM



Алексей Афанасьев
Менеджер по развитию
UserGate SIEM

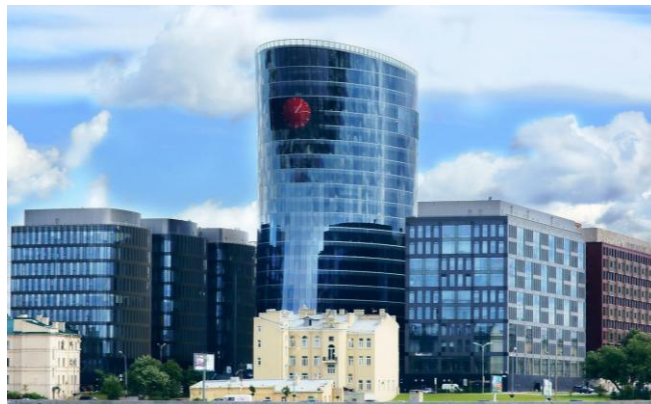


Мы в Telegram

О КОМПАНИИ USERGATE



Основной офис разработки в Технопарке
Новосибирского Академгородка



Офис разработки и сопровождения
в Санкт-Петербурге



Фронт-офис в Москве,
БЦ «ФилиГрад»

- + Минск
- + Томск
- + Хабаровск

25 лет

на ИБ-рынке России

600+ человек

в команде, и мы растем

70% штата

занимаются продуктами

SOC

и ИБ-услуги

500+ партнеров

вендорская модель бизнеса

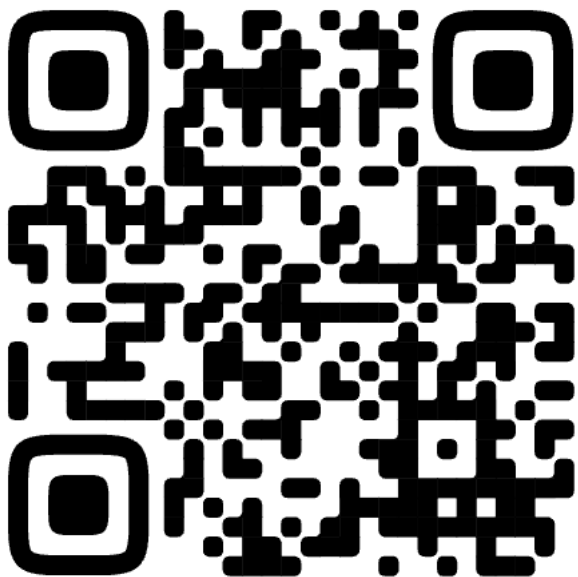
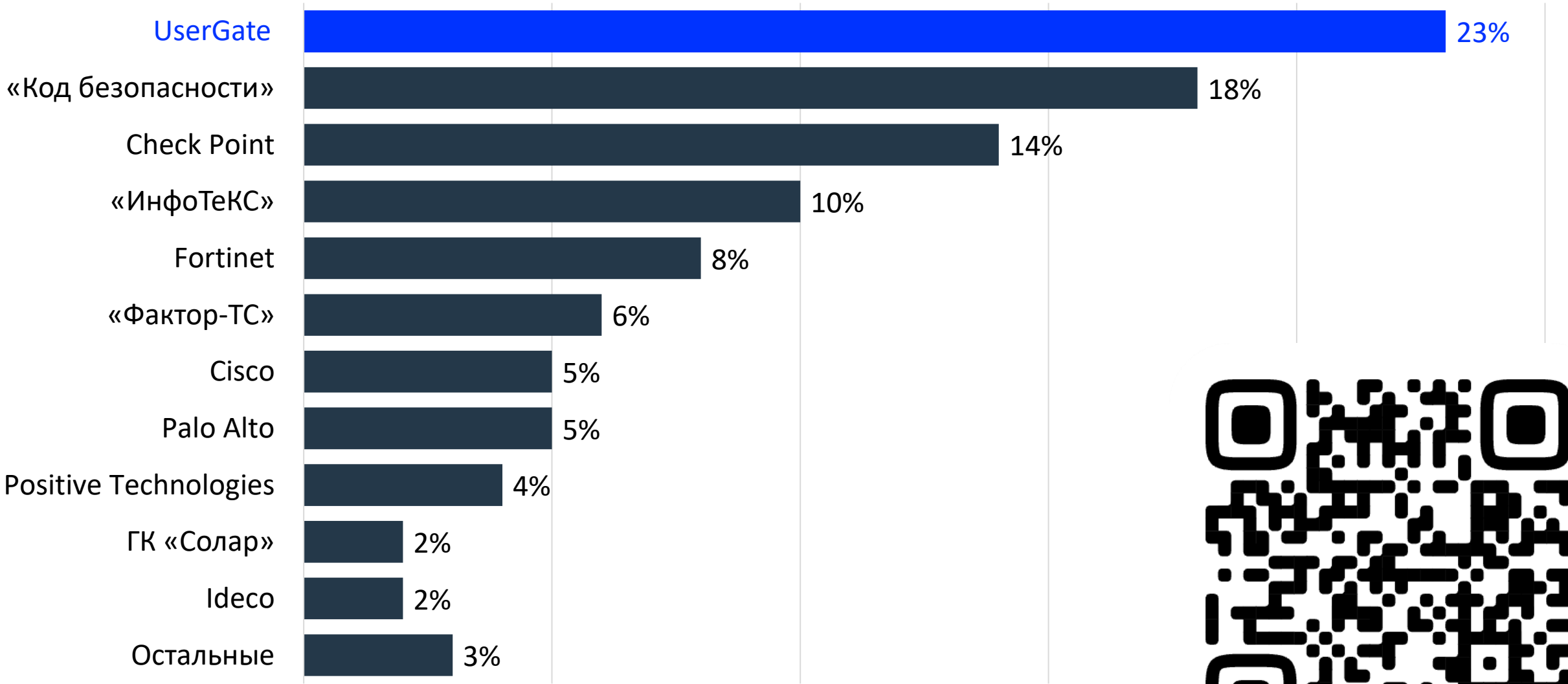
7 продуктов: NGFW +

DCFW, WAF, Client, SIEM, LogAn, MC

№1 по NGFW

в России, ЦСР, 2025

USERGATE – ЛИДЕР РЫНКА NGFW В 2024 ГОДУ (ЦСР, 2025)



Данные: «Рынок NGFW в Российской Федерации 2024-2030», Центр Стратегических Разработок, 3 апреля 2025



SUMMA = Security Unified Management and Monitoring Architecture - Единая Архитектура Управления и Мониторинга Безопасностью

Список наших продуктов:

NGFW

MC

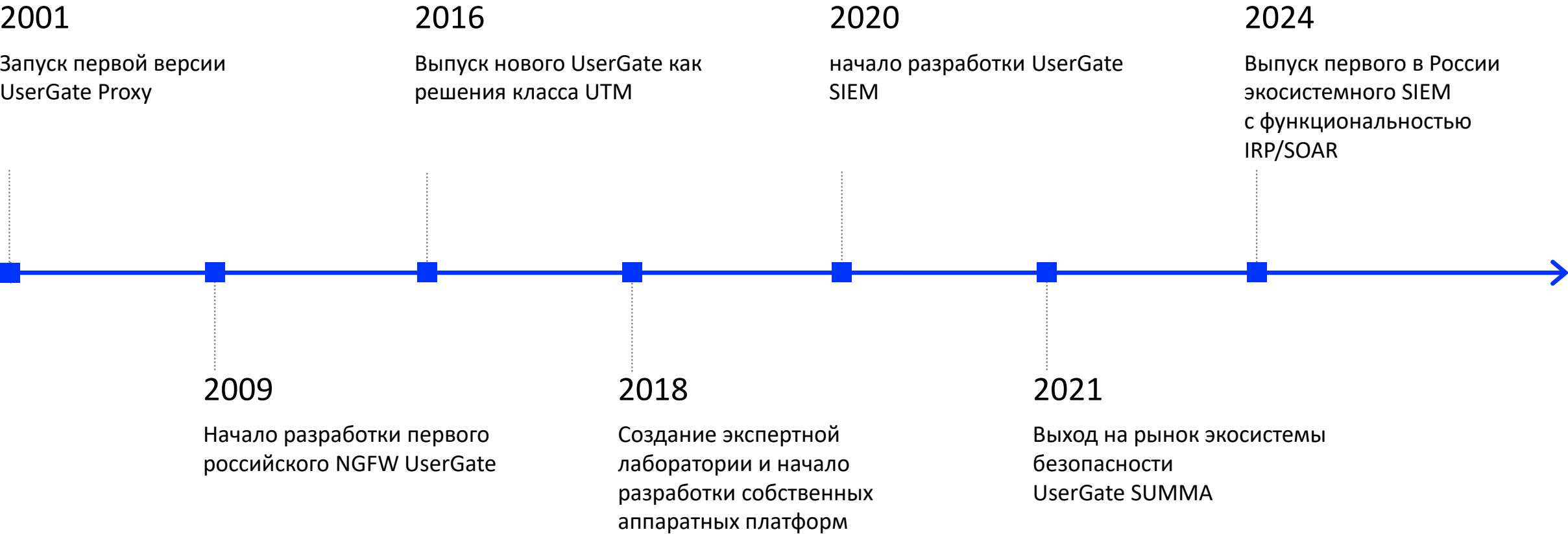
SIEM

LogAn

Client

DCFW

WAF



ЧТО ТАКОЕ SIEM?

SIEM

(Security Information and Event Management)

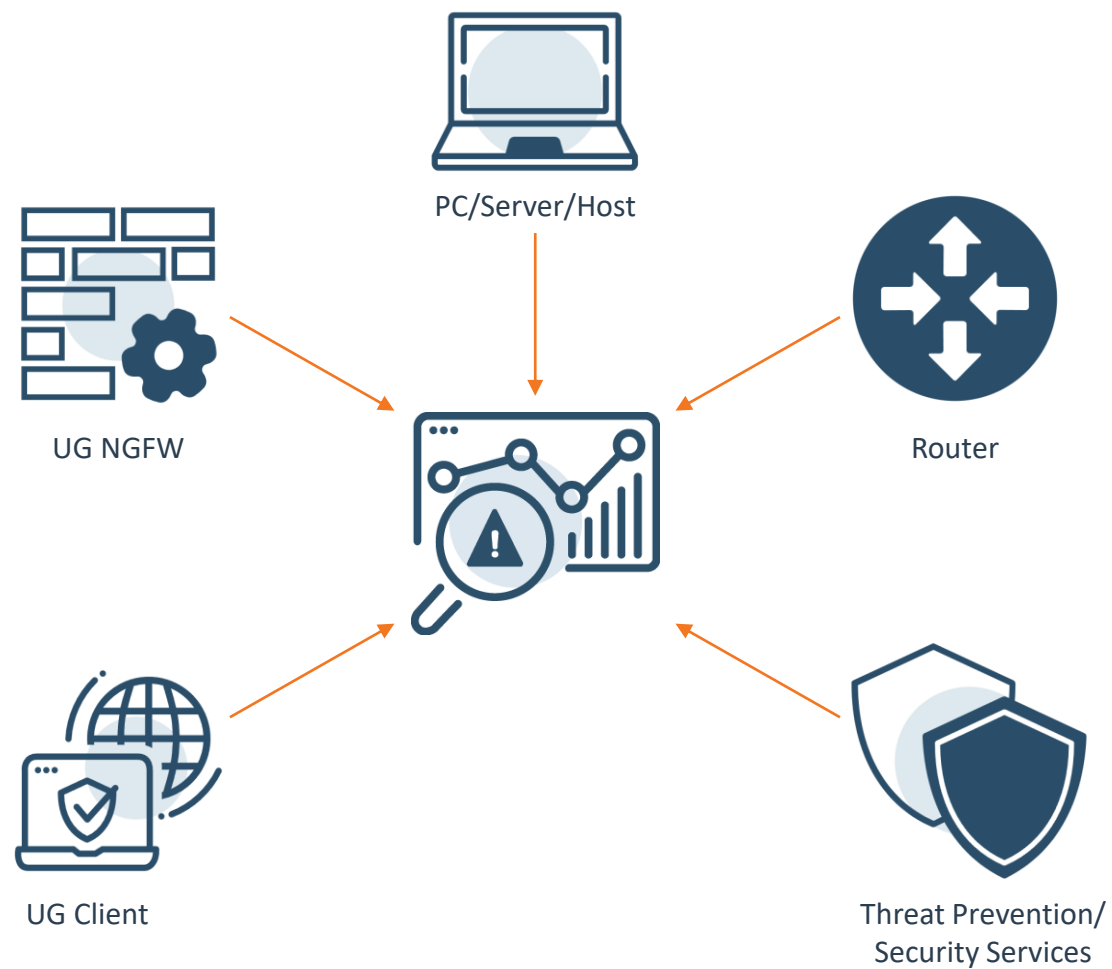
система управления событиями
информационной безопасности

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

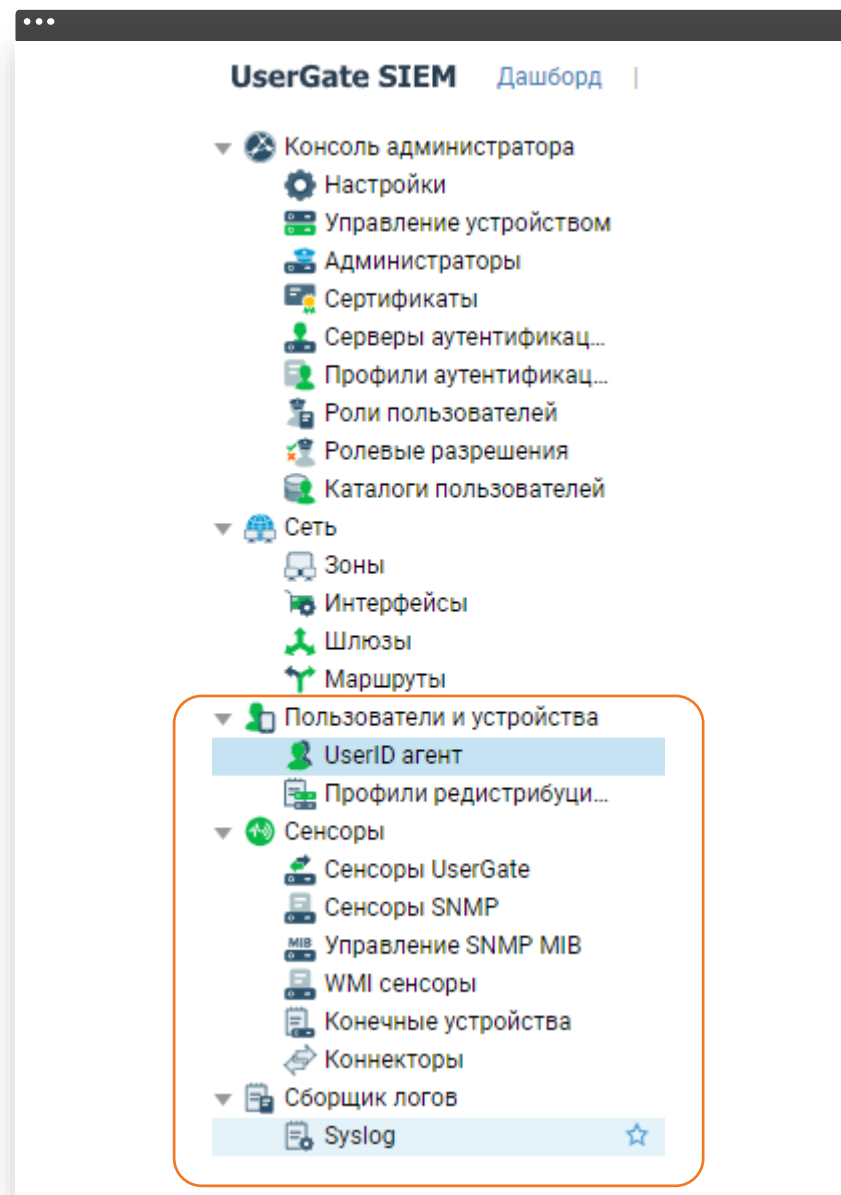
https://vkvideo.ru/video-211747929_456239139

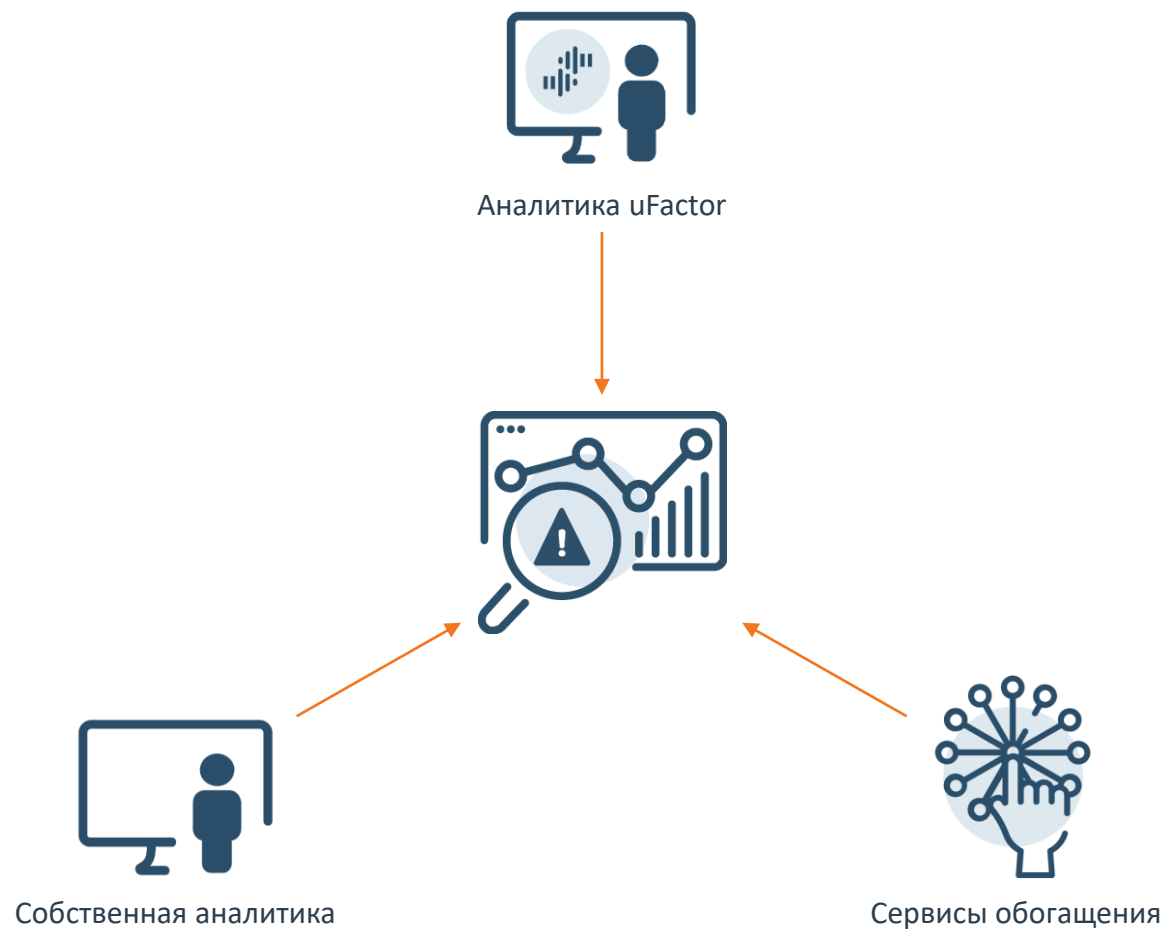
<https://rutube.ru/video/1d4c3321f002d531a6ef9cbd765fedf4/>





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





- Правила из библиотеки (более 1000 правил, подготовленных uFactor).
- 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 MSRT 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

»

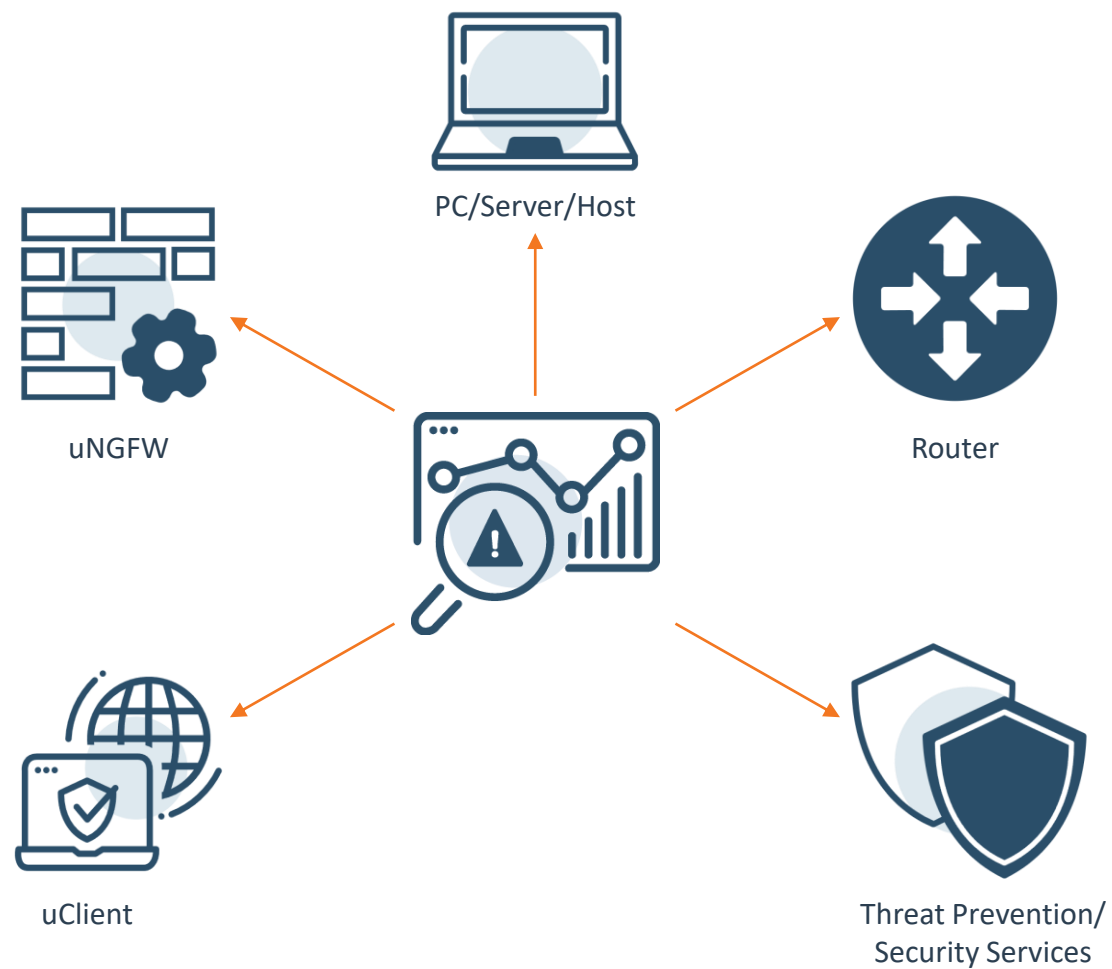
»

↺

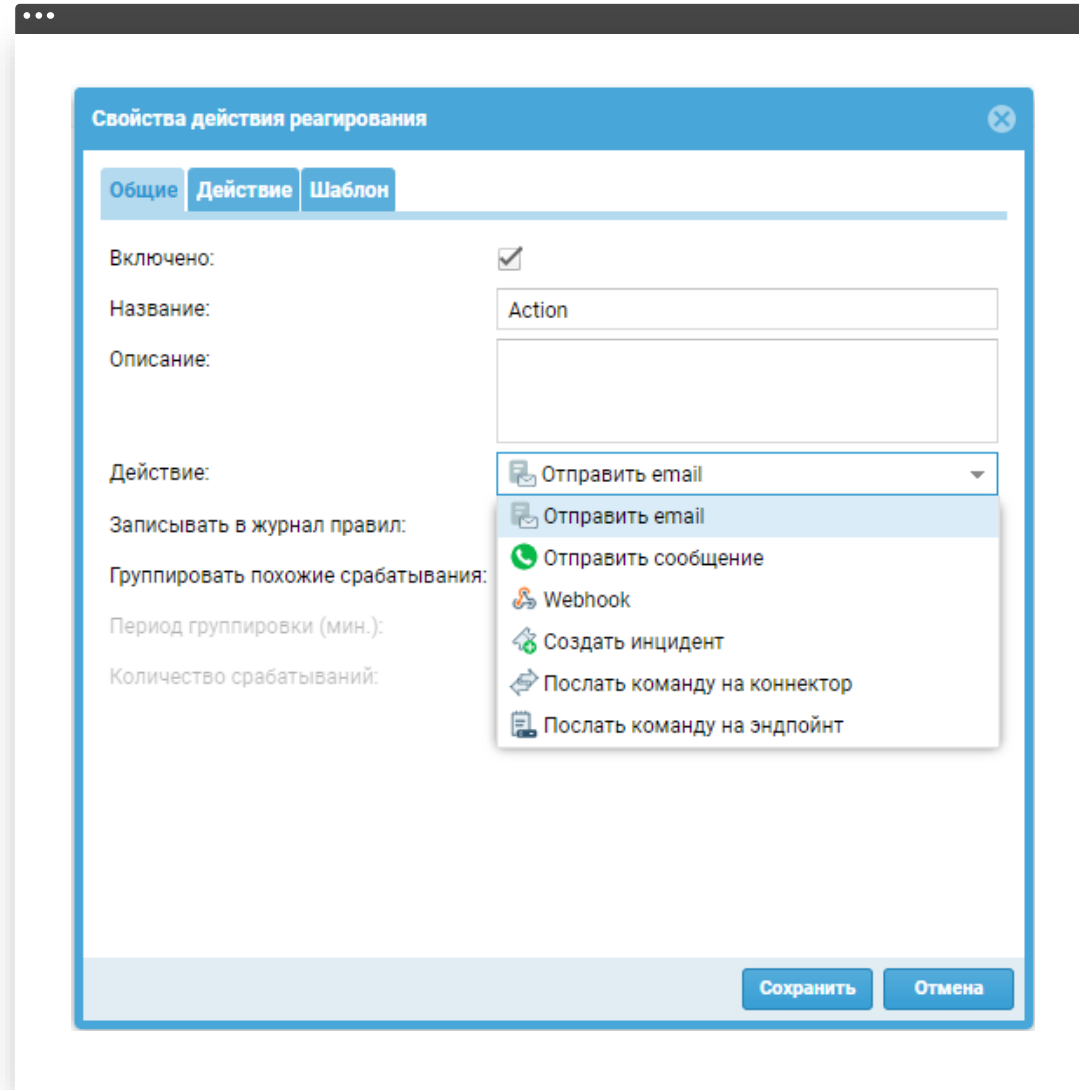
Найти:

Искать в имени и описании:

☐

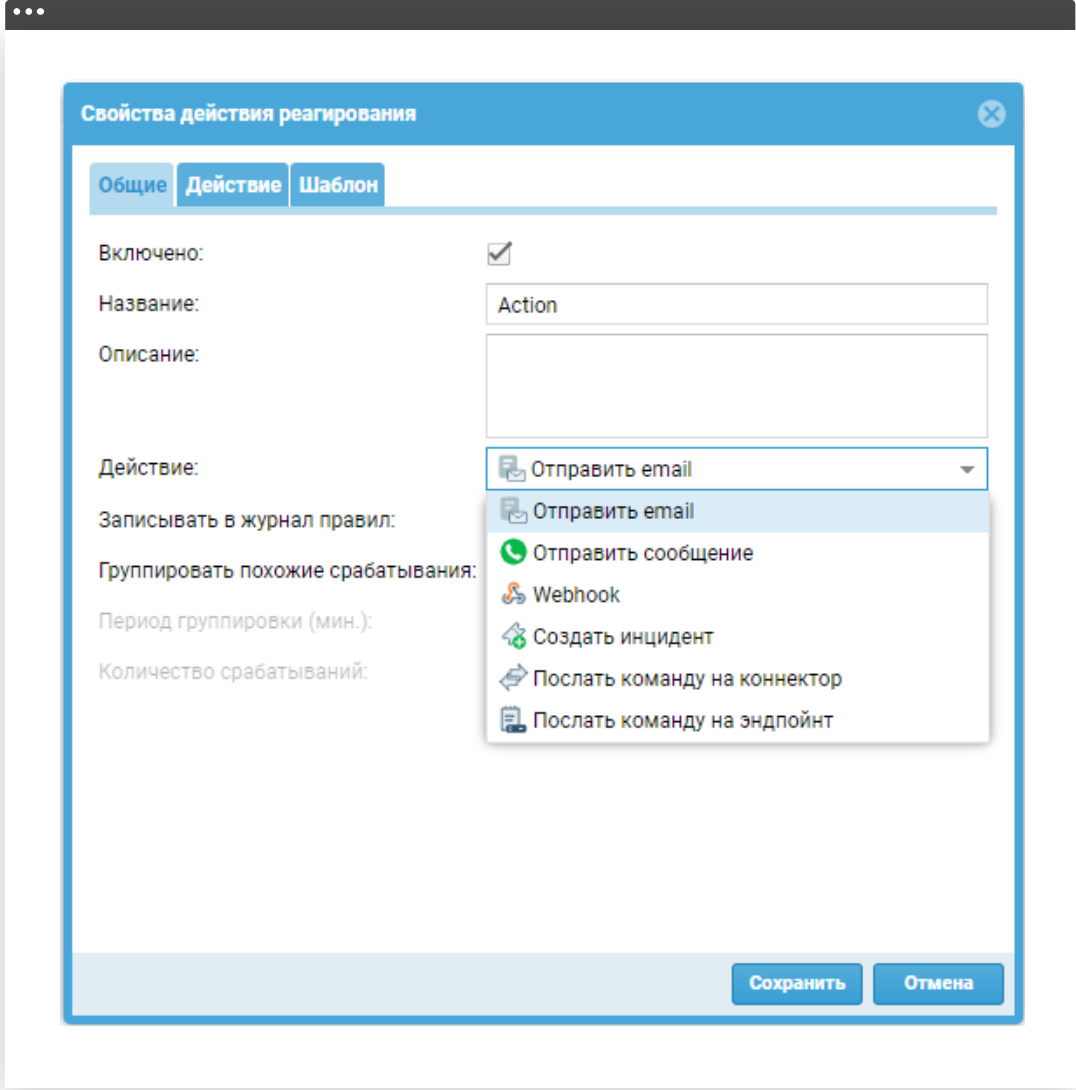


- Отправка команд через SSH/HTTP/HTTPS.
- Возможность передачи в команде артефактов, например IP-адресов.
- Возможность отправки команд на устройства других производителей (коммутаторы, маршрутизаторы и др.)



- Оповещение e-mail/CMC/ 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

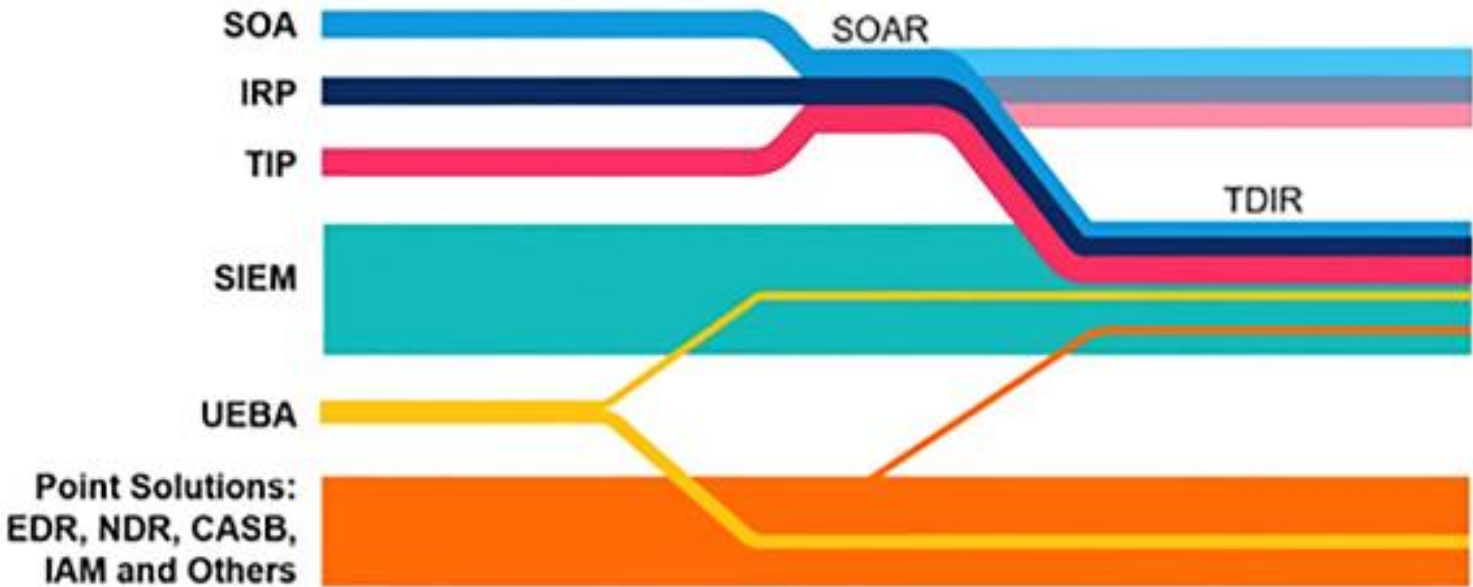
- улучшение логирования за счет экосистемных продуктов;
- увеличенный функционал системы.

03

Где взяли экспертизу?
Сами написали

SIEM-СИСТЕМЫ ДОЛЖНЫ ЭВОЛЮЦИОНИРОВАТЬ!

TDIR — An Evolution



Gartner

uFactor (ex. 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.

ЗАЧЕМ ВАМ SIEM?

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

Исключить

повторение инцидента

Получить

стабильно работающий продукт

Получить

быструю и качественную
техподдержку

Подготовить

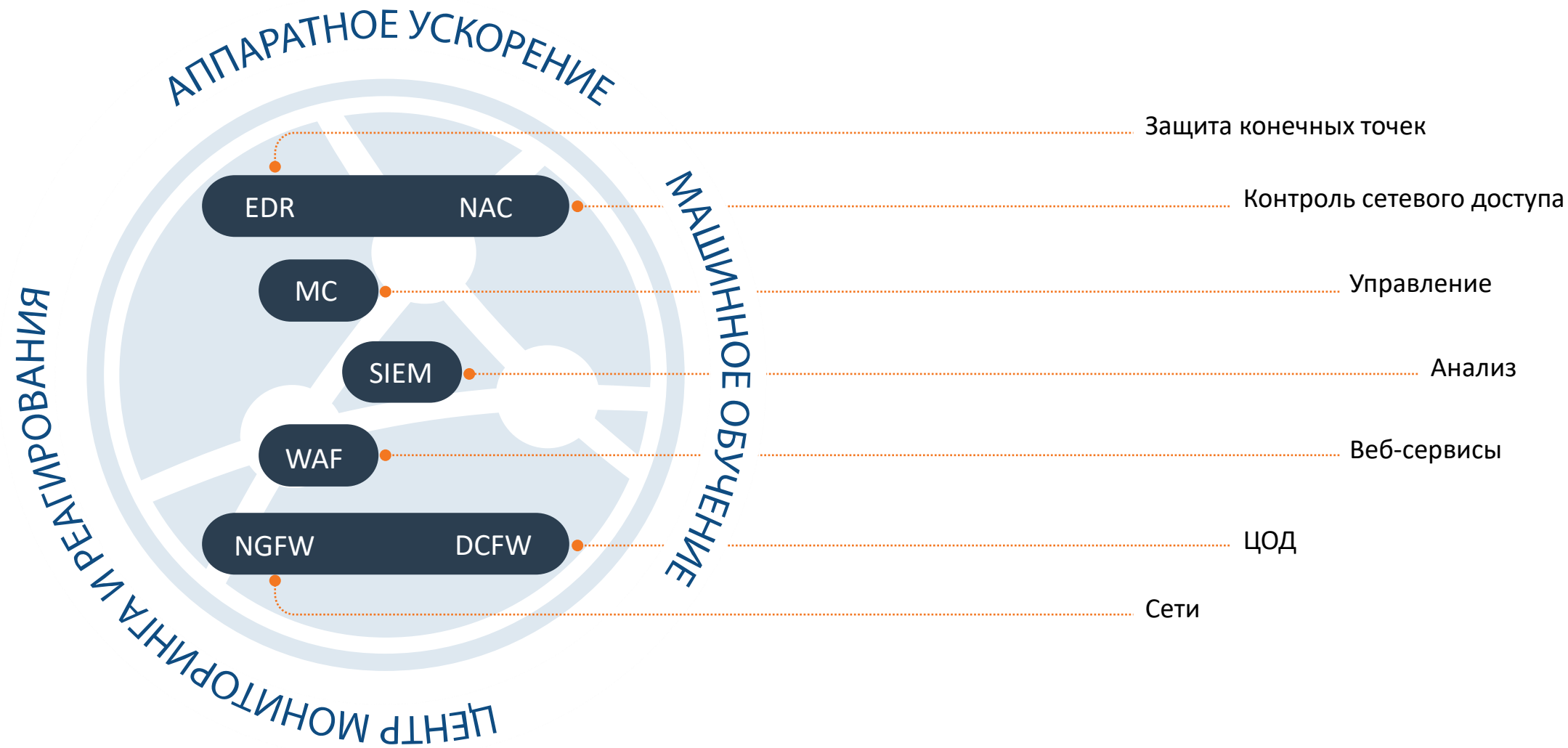
отчет для руководства

Произвести

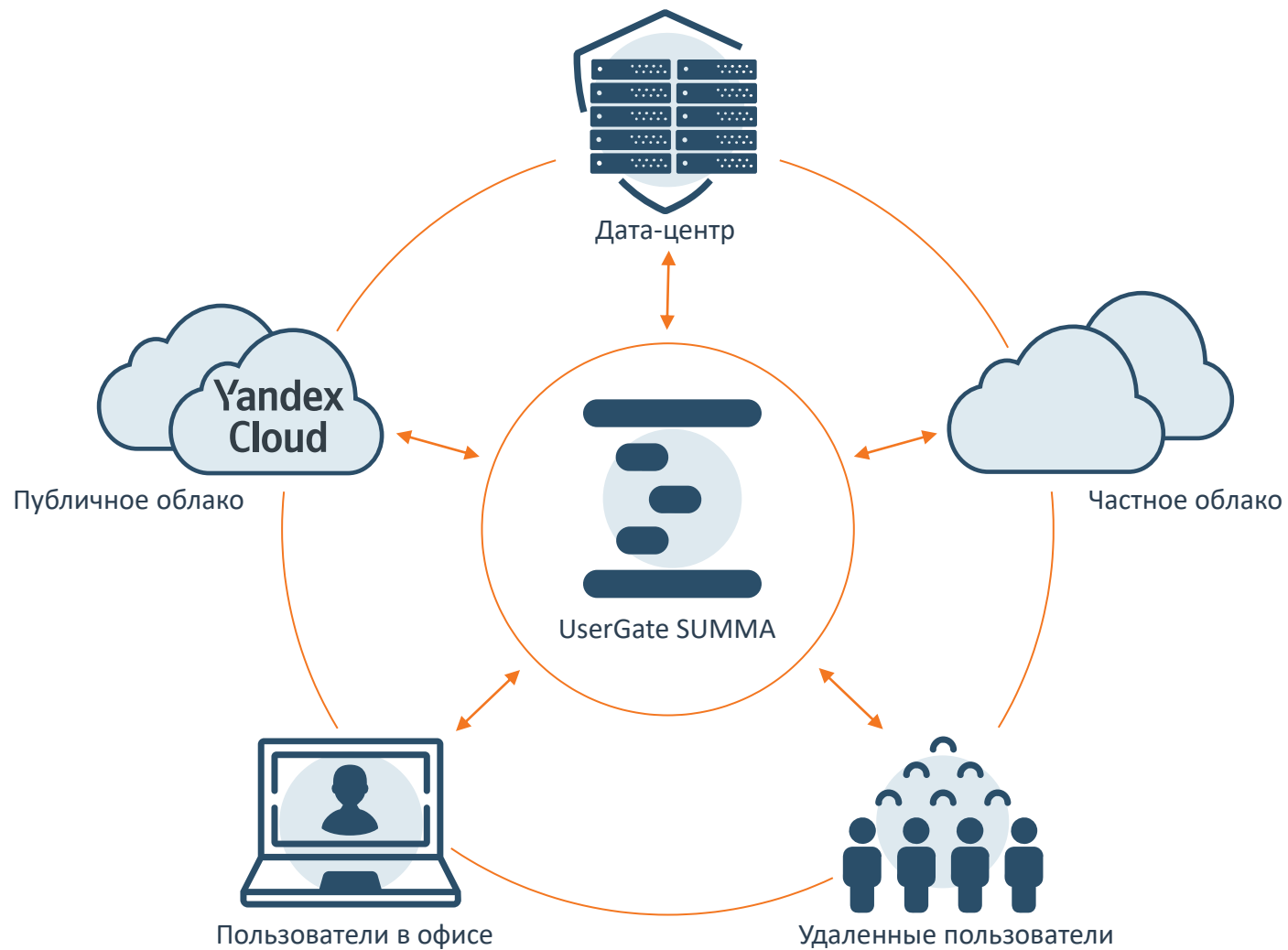
«безболезненные» обновления

- 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

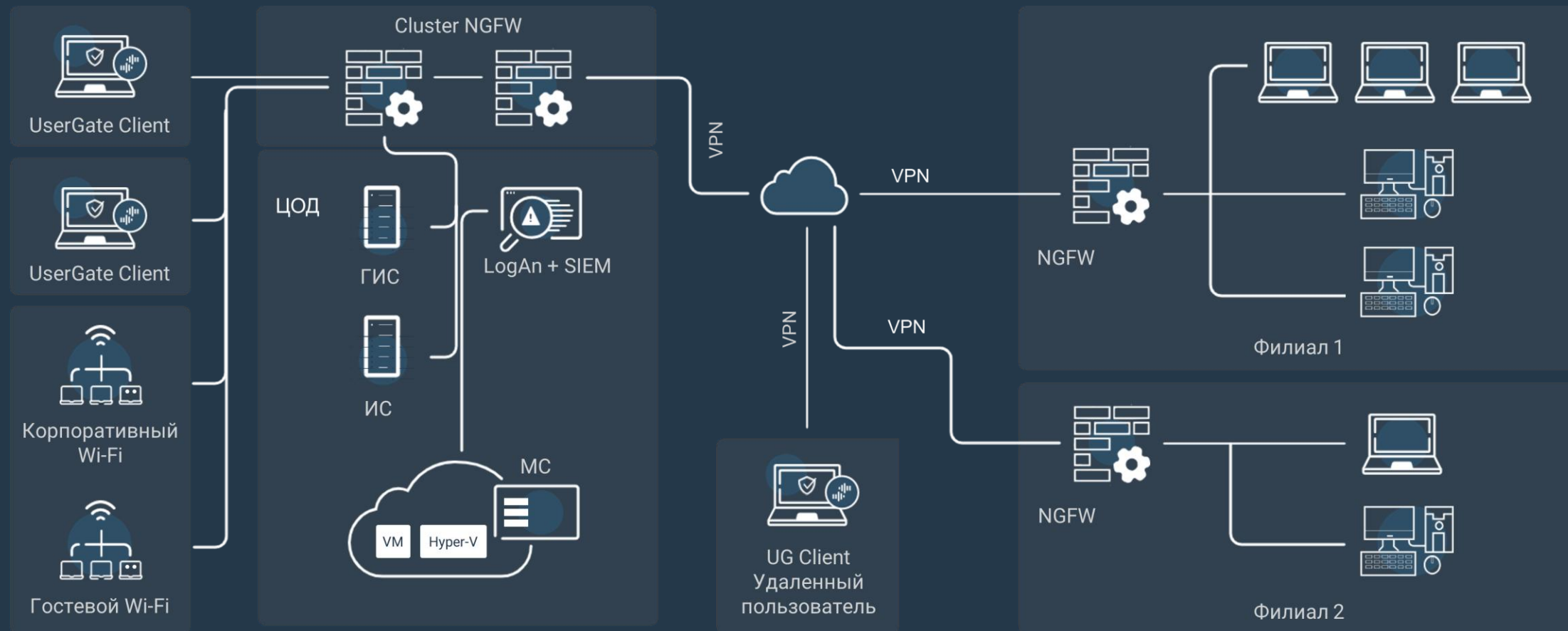
В ПАМКАХ USERGATE SUMMA



ZERO TRUST NETWORK ACCESS (ZTNA)

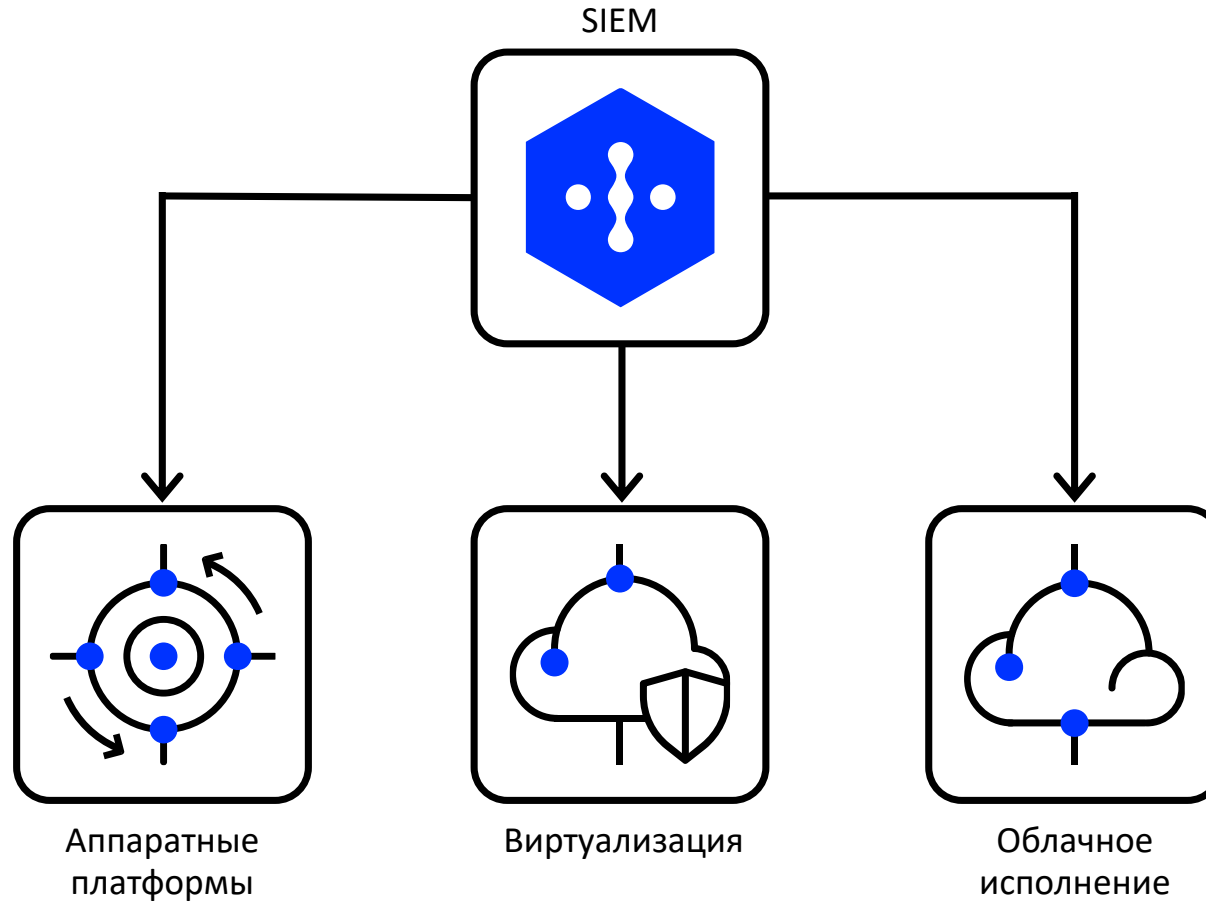


Экосистема продуктов безопасности UserGate SUMMA



ВАРИАНТЫ ПОСТАВКИ

USERGATE SIEM – SIEM ДЛЯ ГИБРИДНЫХ ИНФРАСТРУКТУР:



Аппаратные платформы

- модельный ряд, удовлетворяющий потребности каждого заказчика
- E6, E14, F25

01

Виртуализация

- поддержка всех популярных средств виртуализации
- VMware, Microsoft Hyper-V, KVM

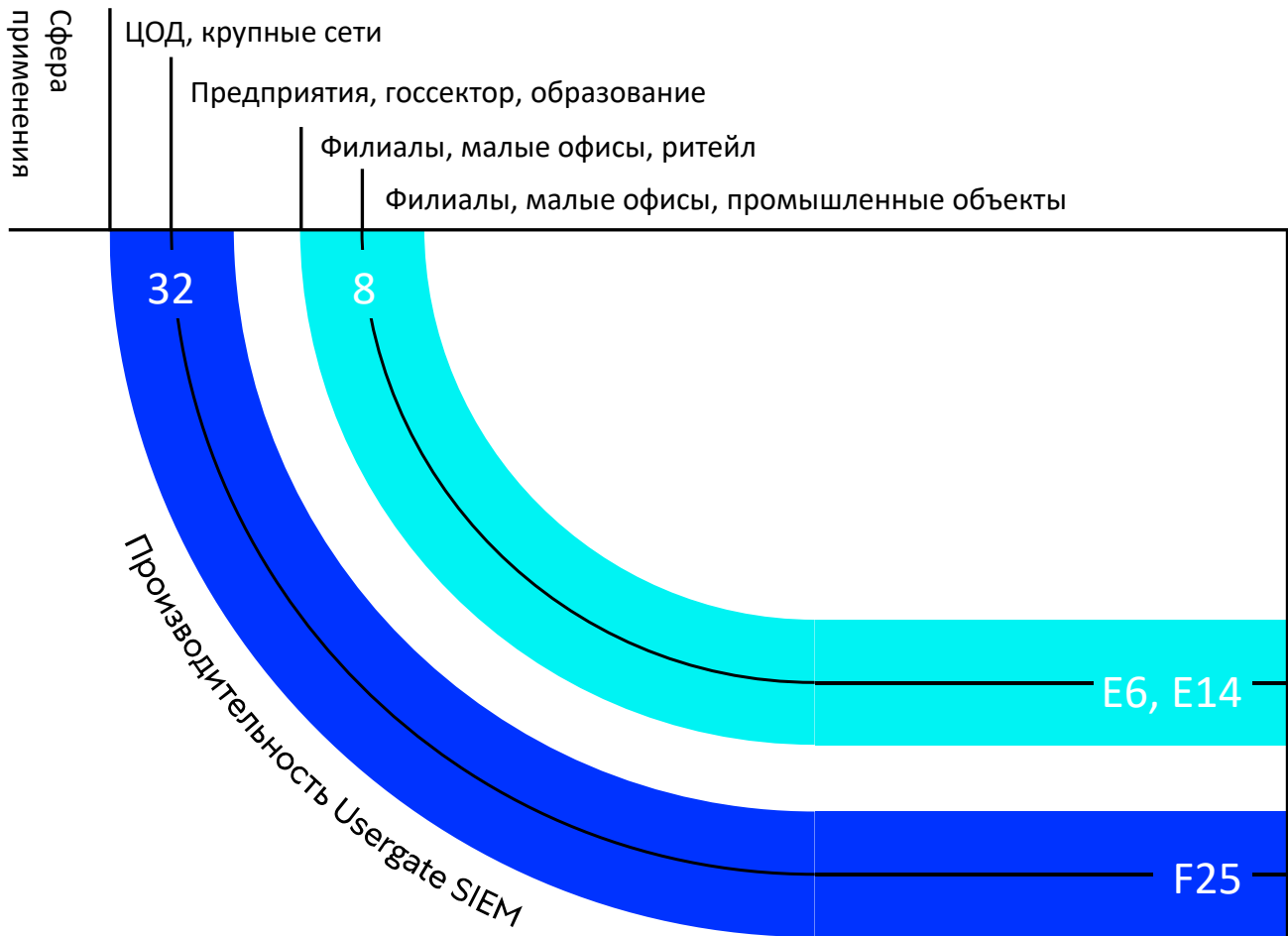
02

Облачное исполнение

- поддержка любых облаков, которые поддерживают стандартные реализации vmware и kvm (openstack)
- Yandex Cloud, Beeline cloud, MTC и VK

03

USERGATE SIEM. МОДЕЛЬНЫЙ РЯД АППАРАТНЫХ ПЛАТФОРМ



6 ТБ
14 ТБ

25 ТБ



Гибкость и масштабируемость

- быстрое развертывание
- горизонтальное масштабирование
- широкий выбор виртуализации

Снижение затрат

- отсутствие затрат на железо
- экономия на обслуживании

Отказоустойчивость и доступность

- встроенная геораспределенность
- автоматическое восстановление VM

Аппаратные платформы

- модельный ряд удовлетворяющий потребности каждого заказчика: E6, E14, F25.

01

Виртуализация

- поддержка всех популярных средств виртуализации.

02

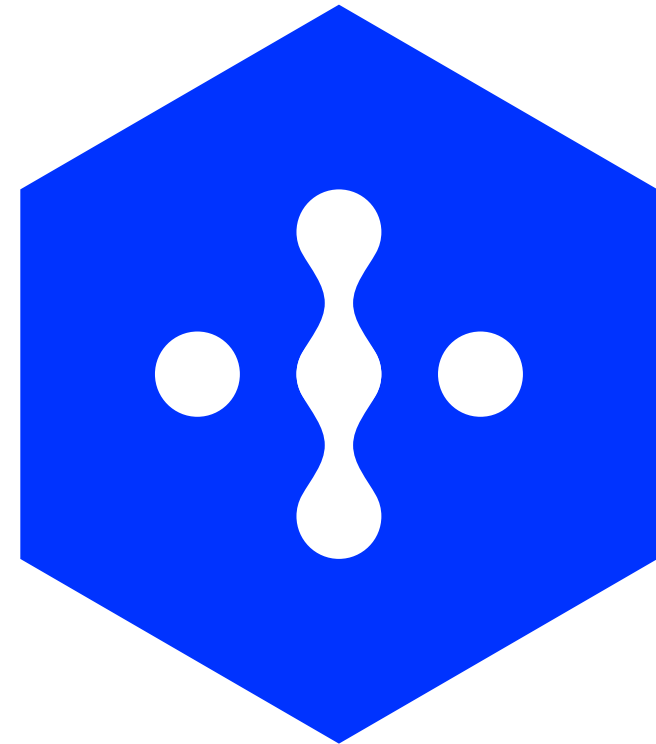
Облачное исполнение

- поддержка любых облаков, которые поддерживают стандартные реализации vmware и kvm (openstack);
- Yandex Cloud, Beeline cloud, МТС и VK.

03

ПРЕИМУЩЕСТВА

- **пользовательские правила** нормализации и корреляции
- **обогащение** инцидента дополнительной информацией
- **кастомизация** процесса обработки и **приоритезация** инцидентов
- возможность **автоматического реагирования** на инцидент
- хранение исторических данных и **ретроспективный анализ**
- формирование **отчетности** об инцидентах



IRP/SOAR

Возможности реагирования прямо из SIEM-системы. Как в автоматическом, так и в ручном режиме. При этом вам не нужно будет переключаться между различными продуктами ИБ, вся работа с инцидентом будет происходить в едином окне.

TI

Обогащения инцидента информацией из внешних сервисов, например, вы можете проверить адрес на предмет его чистоты на внешних базах данных, как платных, так и бесплатных.

Экспертиза

Собственная экспертиза от вендора на базе Центра мониторинга и реагирования UserGate (MRC UG);

Более 1'000 правил корреляции, отсортированных по матрице MITRE ATT&CK;

Различные способы реагирования.

НОРМАЛИЗАЦИЯ

Возможность создавать свои правила нормализации.

От того, как качественно вы выполните нормализацию, будет зависеть качество и скорость работы аналитиков.

ЭКОСИСТЕМА

Гибкость взаимодействия с продуктами из экосистемы;

Расширенное логирование за счет наличия экосистемных продуктов в инфраструктуре;

Удобство администрирования;

Единая точка тех. поддержки.

ОТКРЫТОСТЬ

Полноценная SIEM-система, которая может работать и в инфраструктуре, где нет других продуктов из экосистемы UserGate SUMMA.

ОСОБЕННОСТИ ПРОДУКТА



Гибкость развертывания

Железное исполнение;
Виртуальное исполнение;
Облачное исполнение.

Корреляция событий

Широкие возможности по выявлению и расследованию инцидентов.

Реагирование на инциденты

Автоматизация реагирования на инциденты прямо из SIEM-системы.

Простота и удобство

Система интуитивно понятна, не требует от сотрудников специфических знаний и навыком.

Отказоустойчивость

Возможность построения кластера для обеспечения поддержания работоспособности системы в случае сбоев, сохранности данных и безболезненных обновлений.

Требования законодательства

№ 152-ФЗ; № 187-ФЗ; приказ ФСТЭК № 21, 31; указ президента №250; ГОСТ Р 57580.1-2017; ГОСТ Р 57580.2-2018

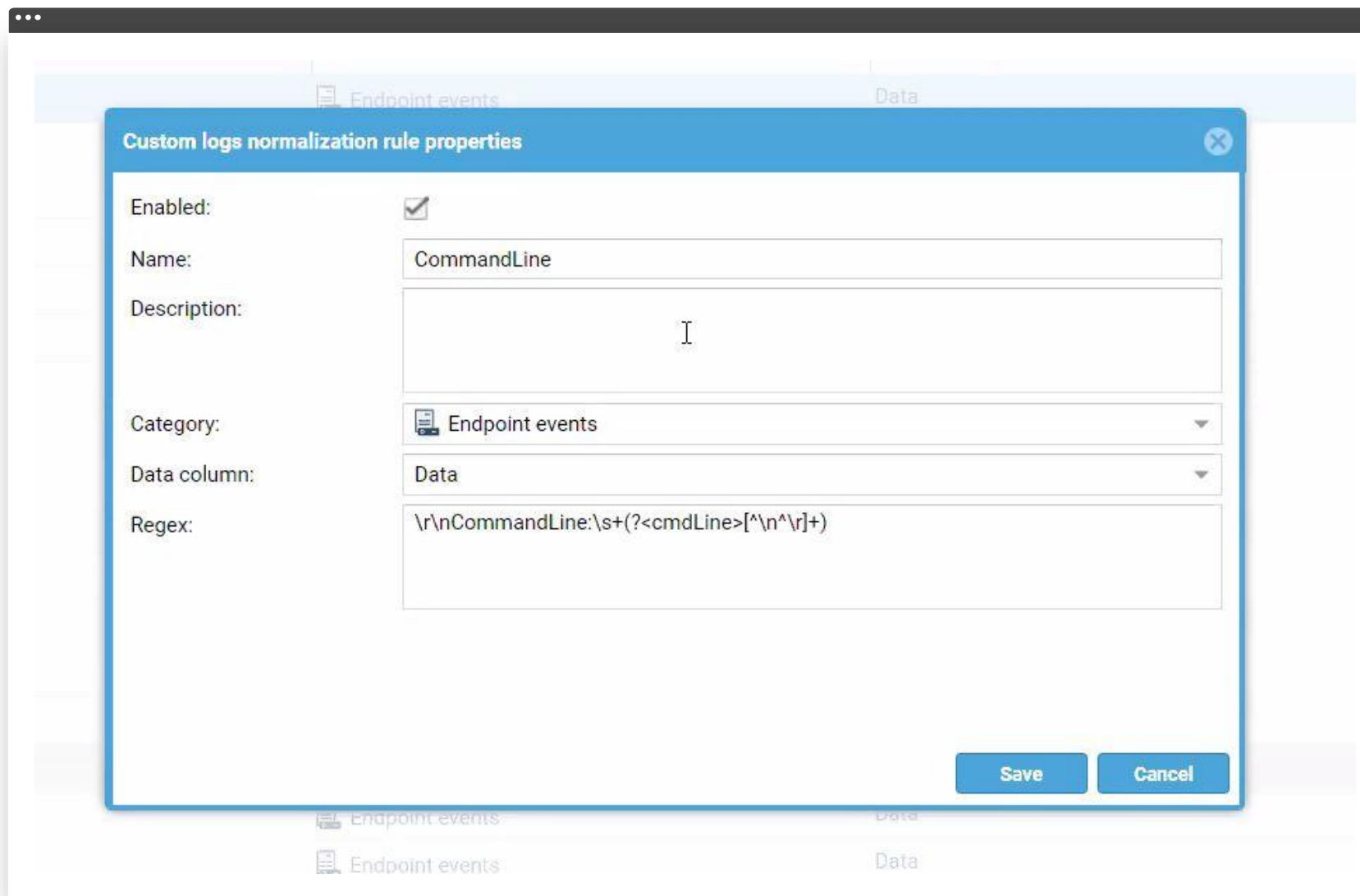
ГосСОПКА

Подготовка отчетов в формате ГосСОПКА. Отправка инцидентов в ГосСОПКу. Как в ручном режиме, так и в автоматическом.

Интеграция с экосистемой

Глубокая совместимость с другими продуктами из экосистемы UserGate SUMMA, что обеспечивает единую платформу для управления безопасностью.

- правила из библиотеки (более 1000 правил, подготовленных uFactor)
- правила добавленные пользователем
- возможность экспорта/импорта правил
- использование фильтров в качестве условий
- возможность загрузки правил в YAML-формате
- использование правил из библиотеки SIGMA



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 table with columns "Endpoint events" and "Data".

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 on the left and a downward arrow on the right.
- Data column:** A dropdown menu showing "Data" with a downward arrow on the right.
- 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".

В разделе аналитики добавлены журналы о процессах на конечных устройствах.

Вся информация о когда-то запущенных процессах хранится тут.

UserGate SIEM

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

Аналитика

Правила аналитики | Поиск | Действия реагирования | Срабатывания | Подробности срабатывания | Процессы конечных устройств

Лог процессов

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

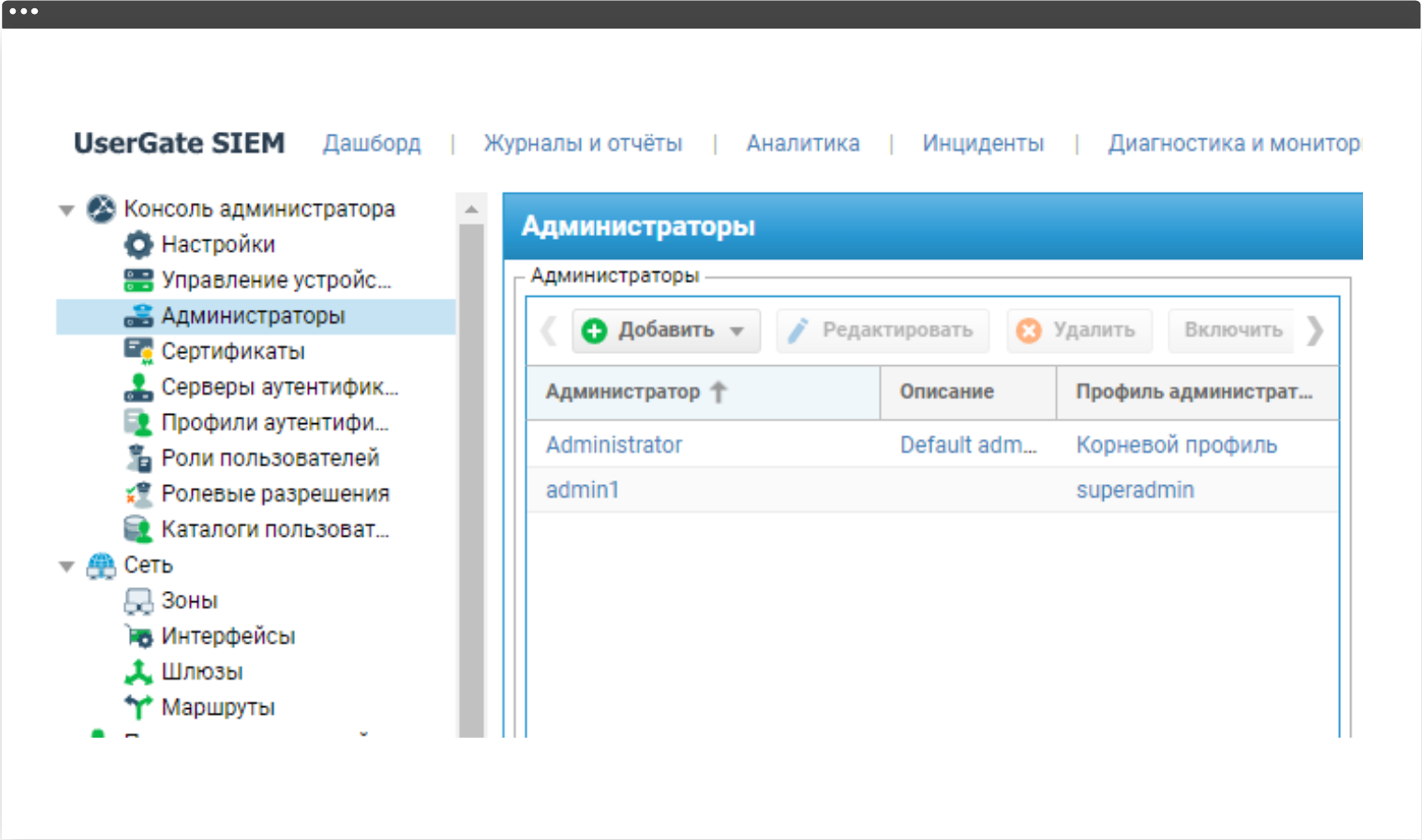
Время	Конечное устройство	Приложение	Идентификат...
19:31:38	MSEDGEWIN10	SearchProtocolHost.e...	1700
19:31:34	MSEDGEWIN10	DllHost.exe	6296
19:30:39	MSEDGEWIN10	DllHost.exe	1284
19:29:45	MSEDGEWIN10	DllHost.exe	2844
19:28:50	MSEDGEWIN10	DllHost.exe	5592
19:27:56	MSEDGEWIN10	DllHost.exe	3932
19:27:01	MSEDGEWIN10	DllHost.exe	3348
19:26:07	MSEDGEWIN10	DllHost.exe	2388
19:25:12	MSEDGEWIN10	DllHost.exe	4968
19:24:18	MSEDGEWIN10	DllHost.exe	4320
19:23:23	MSEDGEWIN10	DllHost.exe	8788
19:22:28	MSEDGEWIN10	DllHost.exe	8012
19:21:34	MSEDGEWIN10	DllHost.exe	6592
19:20:39	MSEDGEWIN10	DllHost.exe	3176
19:19:58	MSEDGEWIN10	svchost.exe	8908
19:19:45	MSEDGEWIN10	DllHost.exe	5560

Процесс: svchost.exe

Дерево процессов | Информация о процессе

Узел: 62a02caa-48d4-4ebf-b100-e1879e20353d
Время: 19:19:58
Конечное устройство: MSEDGEWIN10
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

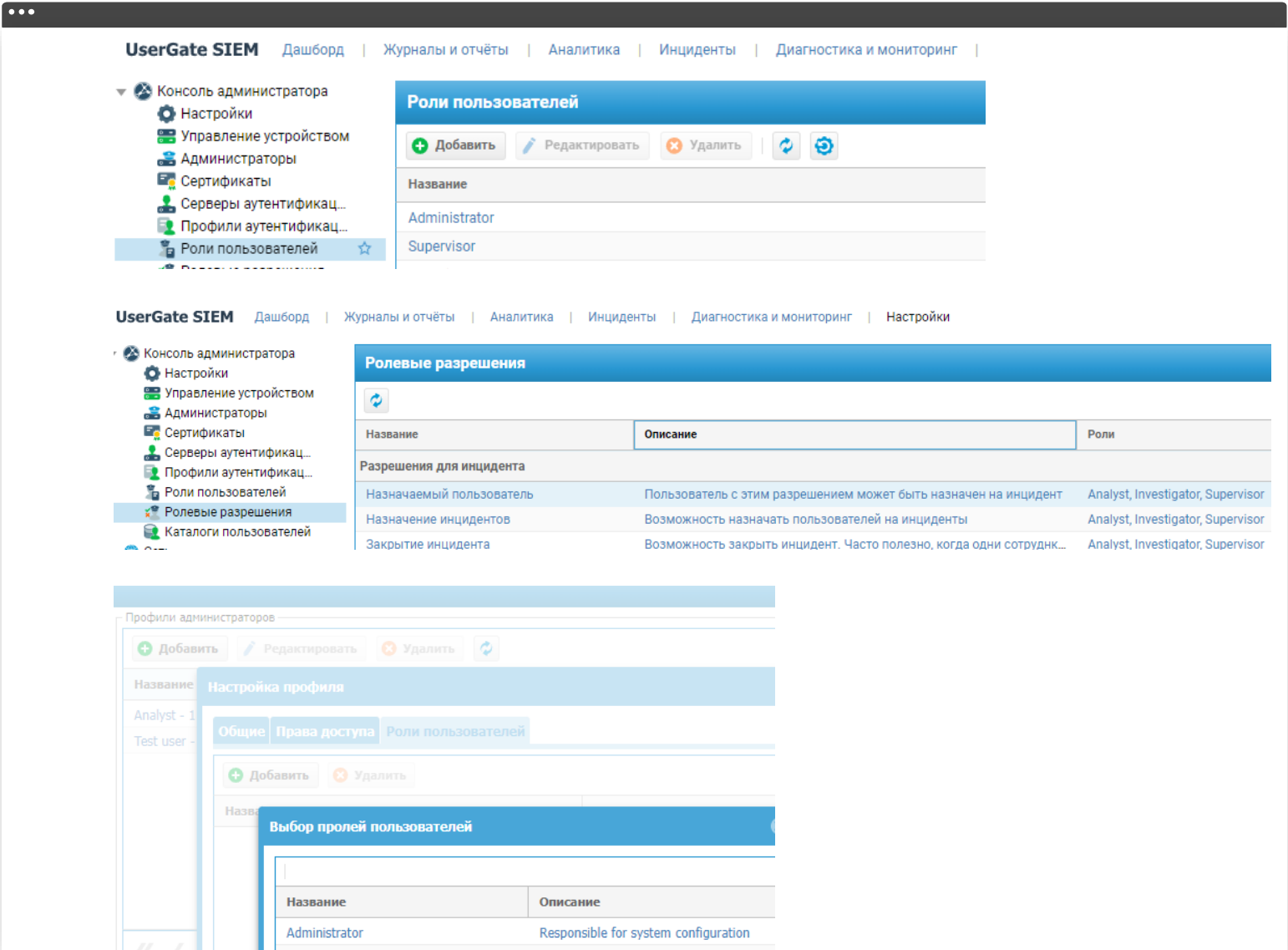
- Управление пользователями в системе.
- Добавление пользователей/ групп из LDAP.
- Отображение активных сессий пользователей.



01
Роли пользователей

02
Ролевые разрешения

03
Профиль пользователя



- Генерация отчета по инцидент
- 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

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

©2024 UserGate. Любое копирование и воспроизведение содержания (в том числе частичное) без разрешения правообладателя запрещено.

43

- Первый экосистемный SIEM в России с функциональностью IRP/SOAR.
- Реагирование прямо «из коробки».
- Экономия бюджета на стороннем IRP/SOAR-решении и дорогостоящем персонале.
- Обогащения инцидента информацией из сторонних баз и из нашей библиотеки.
- Готовое решение с простотой установки, настройки и эксплуатации.
- Простой язык создания правил корреляции. Меньше требований к знаниям.
- Возможность создавать пользовательские правила нормализации событий.
- Интеграция с ГосСОПКА.

СПАСИБО

По вопросам приобретения: sales@usergate.com



Алексей Афанасьев
Менеджер по развитию
UserGate SIEM



Записаться на пилот!