



UserGate SIEM

Дмитрий Чеботарёв

Менеджер по развитию продукта



Что такое SIEM?

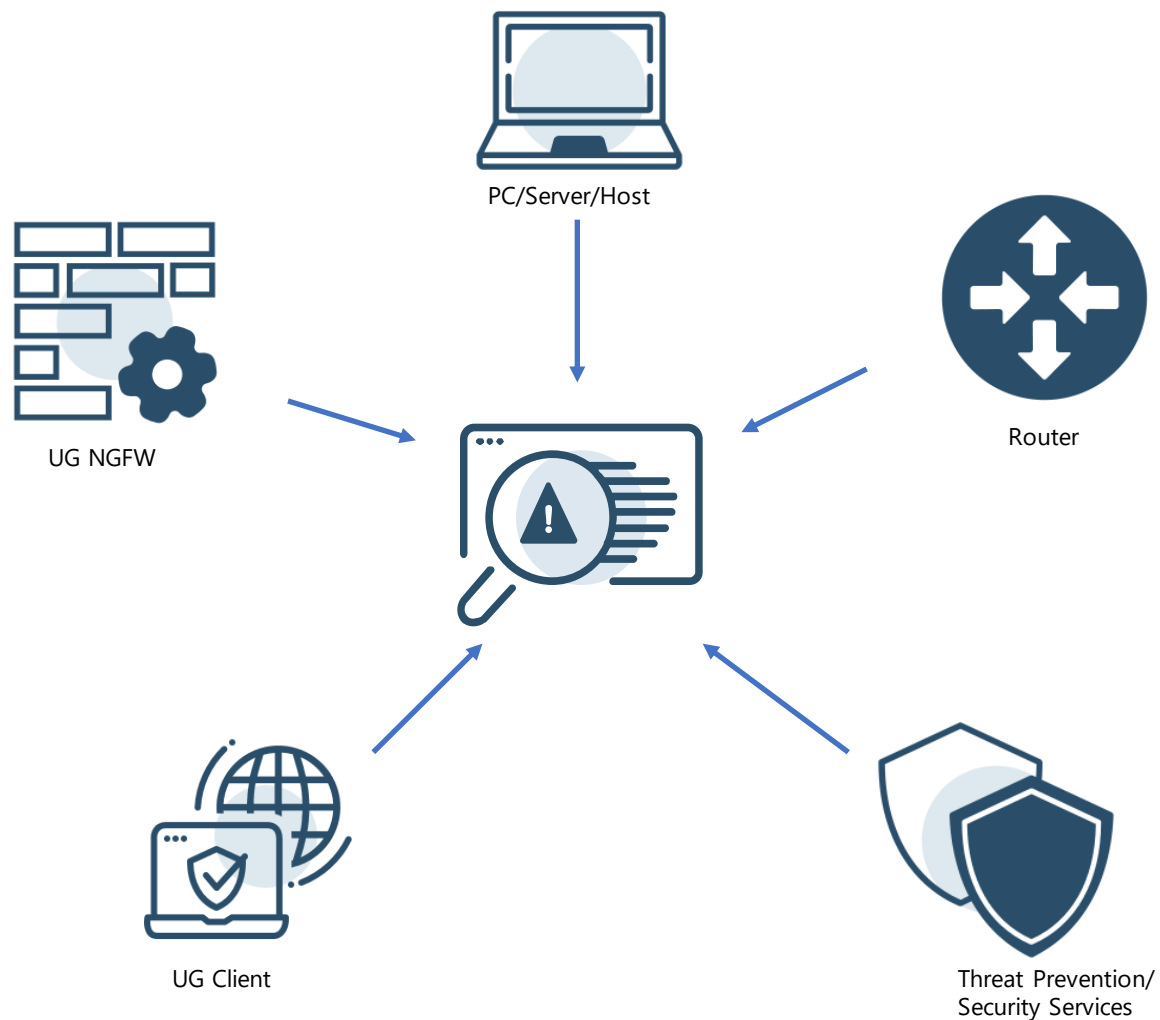
SIEM (Security Information and Event Management) - система управления событиями информационной безопасности.

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

































Сбор данных и нормализация



Источники

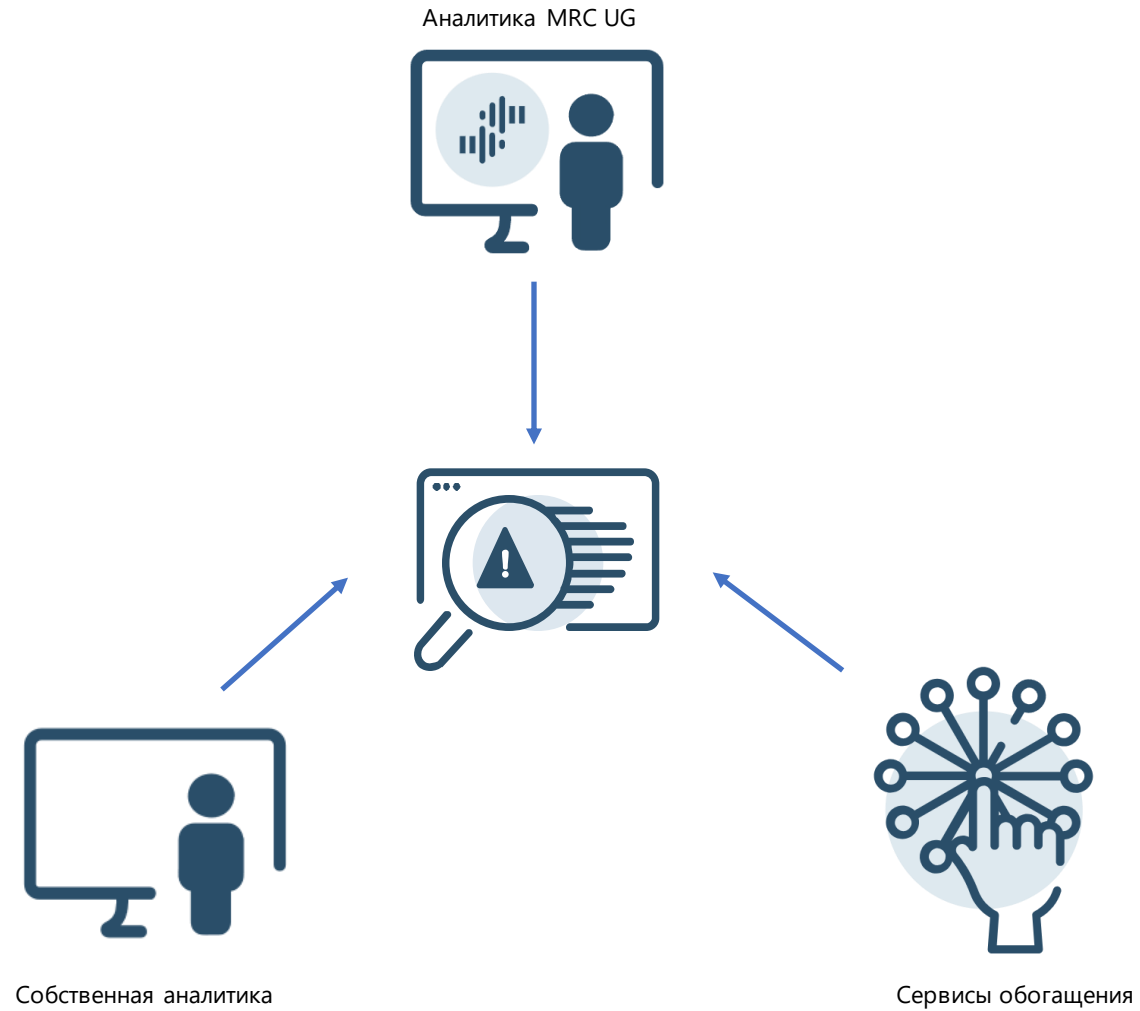
- Межсетевые экраны UserGate
- Устройства SNMP
- Рабочие станции и сервера с WMI
- Агенты UserID
- UserGate Client
- Хосты Syslog

UserGate SIEM [Дашборд](#) |

- ▼  Консоль администратора
 -  Настройки
 -  Управление устройством
 -  Администраторы
 -  Сертификаты
 -  Серверы аутентификац...
 -  Профили аутентификац...
 -  Роли пользователей
 -  Ролевые разрешения
 -  Каталоги пользователей
- ▼  Сеть
 -  Зоны
 -  Интерфейсы
 -  Шлюзы
 -  Маршруты
- ▼  Пользователи и устройства
 -  UserID агент
 -  Профили редистрибуци...
- ▼  Сенсоры
 -  Сенсоры UserGate
 -  Сенсоры SNMP
 -  Управление SNMP MIB
 -  WMI сенсоры
 -  Конечные устройства
 -  Коннекторы
- ▼  Сборщик логов
 -  Syslog 



Анализ и корреляция





Правила аналитики

- Правила из библиотеки
- 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

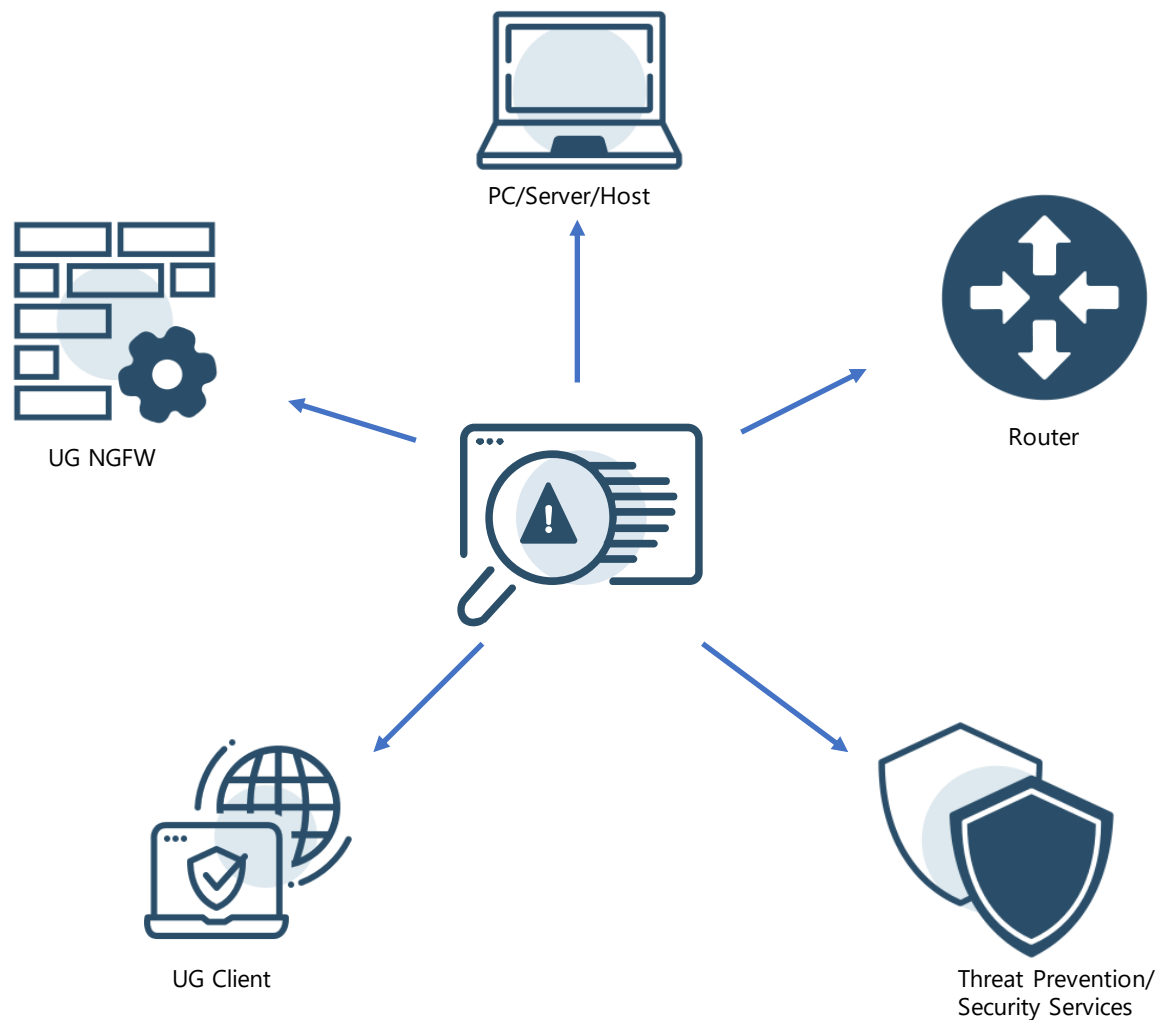
+ Добавить | ✎ Редактировать | 📄 Копировать | ✖ Удалить | 🗑 Включить | 🚫 Отключить | ▶ Запустить сейчас | 📄 Показать срабатывания | 📄 Показать Все | 🔄 | 📄 Экспорт | 📄 Импорт

	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 MSDT 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 dpg.exe	🔴 Важный	Performance	↓ Condition	

« | < | Страница 1 из 2 | > | » | 🔄 | Найти: | Искать в имени и описании:



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.)

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:

Сохранить Отмена



Варианты реагирования

- 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

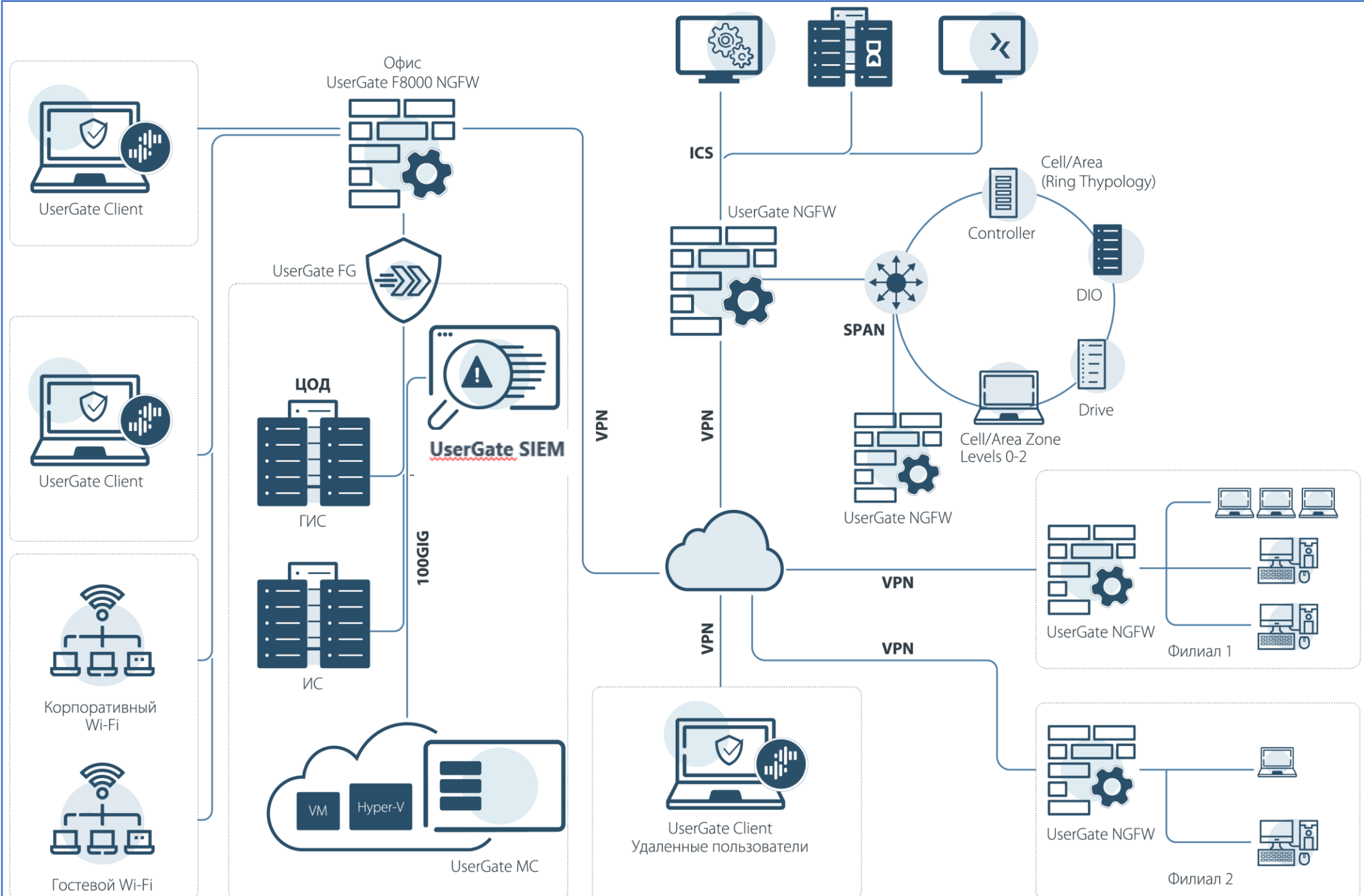
Webhook

Создать инцидент

Послать команду на коннектор

Послать команду на эндпойнт

Сохранить Отмена





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;

A decorative graphic on the right side of the slide, consisting of a network of light blue lines and dots, resembling a molecular or data network structure.

В рамках UserGate SUMMA



SIEM-системы должны эволюционировать!

TDIR — An Evolution



11 © 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner.



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 SIEM | Dashboard | Logs and reports | Analytics | Incidents | Diagnostics and monitoring | | admin ▾

- ▶ Admin console
- ▶ Network
- ▶ Users and devices
- ▶ Sensors
- ▶ Log collector
- ▼ Incident settings
 - Incident schema
 - Incident states
 - Incident types
 - Incident resolutions
- ▼ Libraries
 - IP addresses
 - Emails
 - Phones
 - Commands
 - Analytics rules
 - Notification profiles
 - Triggered alert categories
 - External enrichment services
 - Syslog applications
 - UserID agent syslog filters

External enrichment services

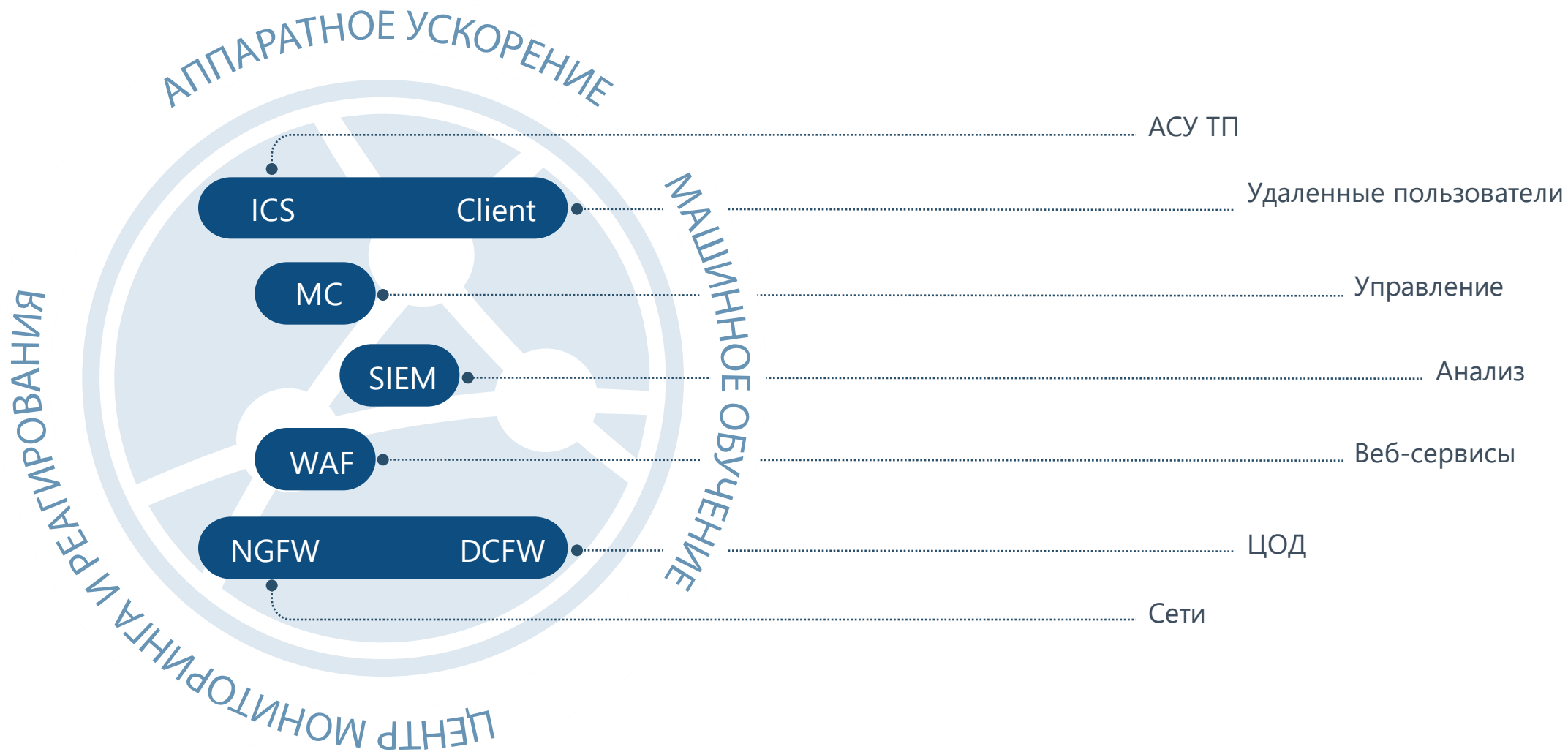
Edit | |

ID	Credentials	Creden...	Types of observables
dnsgoogle	Not set	No	IP
urlhaus	Not set	No	Domain, Hash, Host name, IP, URL
dshield	Not set	No	Domain, FQDN, IP
fortiguard	Not set	No	Domain, FQDN, URL
cybercrime	Not set	No	Domain, FQDN, IP, URL, Other
cyberprotect	Not set	No	Domain, Hash, IP, URL, User agent
unshorten	Not set	No	URL
ipwhois	Not set	No	IP
ipinfo	Token: Undefined	No	IP
hashdd	Key: Undefined	No	Hash
urlscan	Key: Undefined	No	Domain, FQDN, Hash, IP, URL
emailrep	Key: Undefined	No	Mail
greynoise	Key: Undefined	No	IP
abuseip	Key: Undefined	Yes	IP
hybridanalysis	Key: Undefined	Yes	Hash



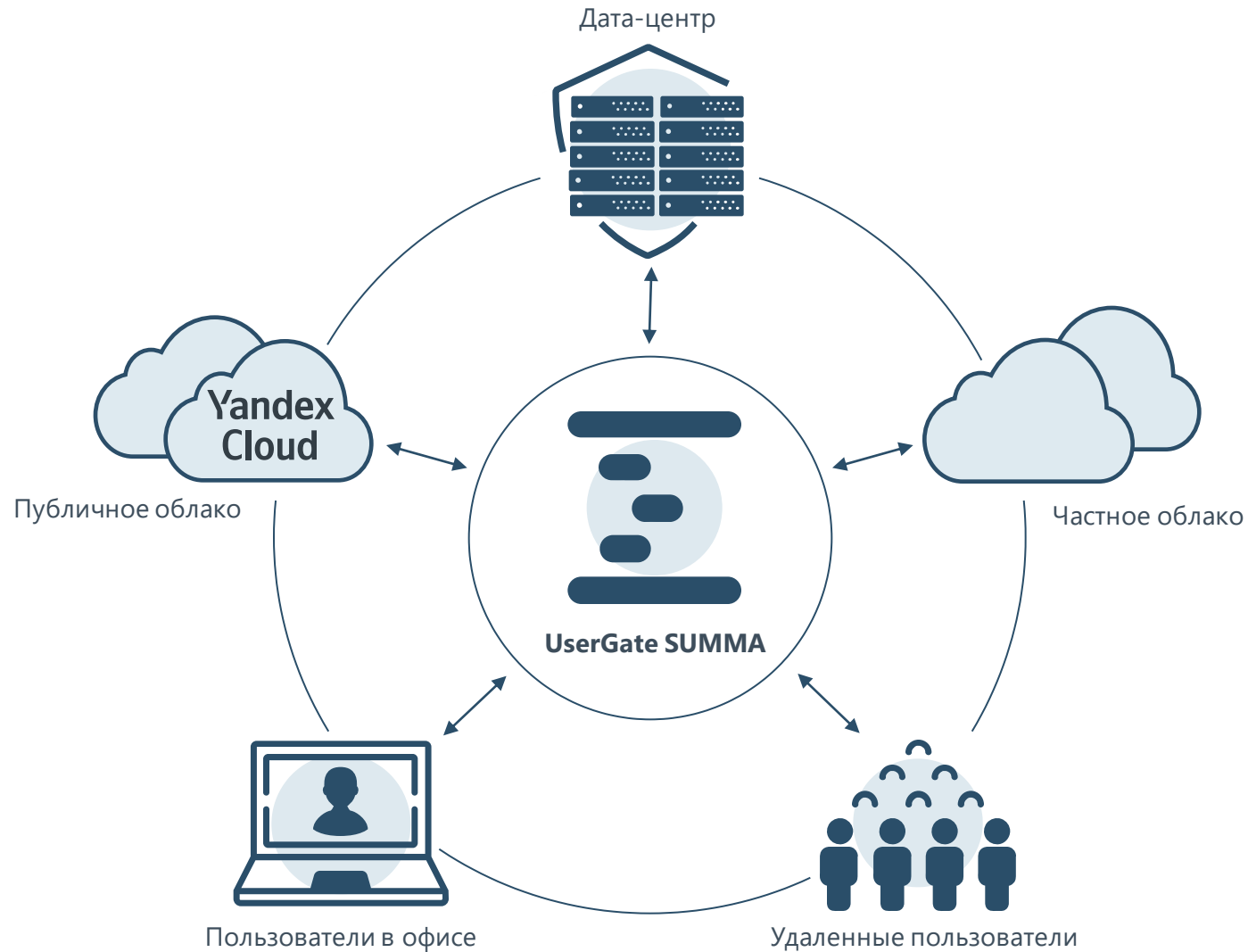
UserGate SUMMA

100% видимость событий безопасности



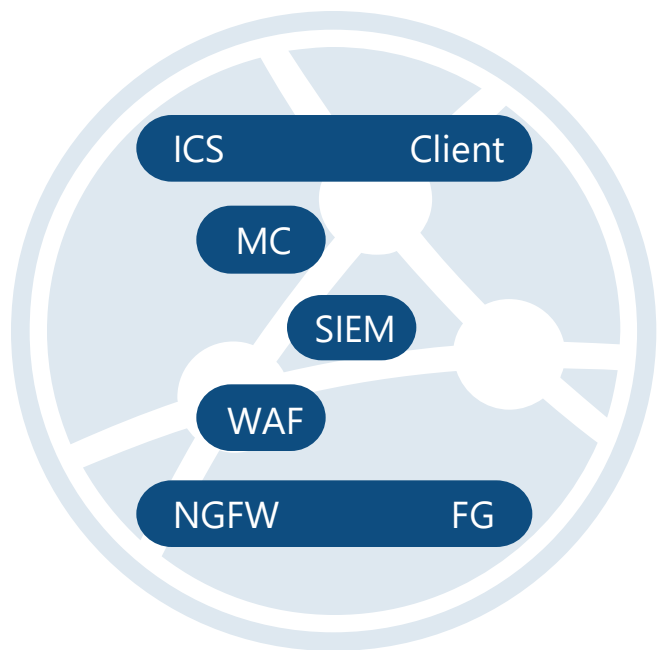


Zero Trust Network Access (ZTNA)



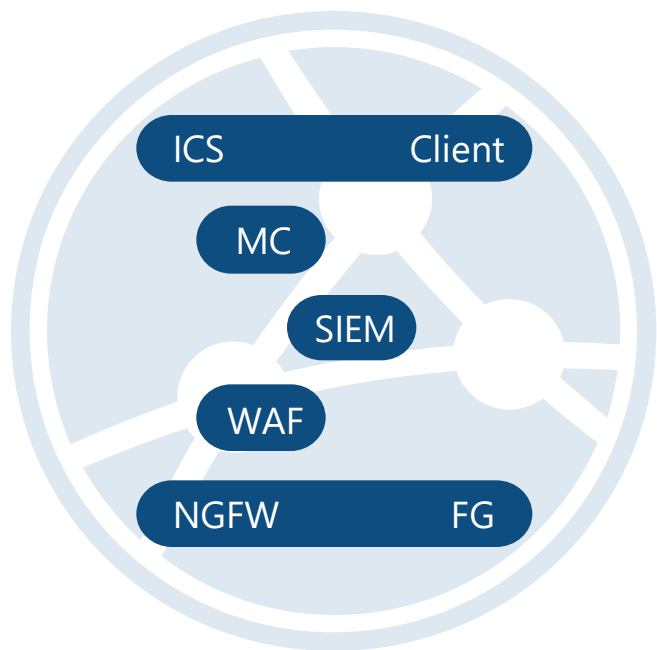


Все продукты UserGate SUMMA доступны в виртуальном исполнении





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

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 Нояб 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



Пользовательская нормализация

The image shows a dialog box titled "Custom logs normalization rule properties" with a close button (X) in the top right corner. The dialog contains the following fields:

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

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



Администраторы

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

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

Консоль администратора

- Настройки
- Управление устройс...
- Администраторы**
- Сертификаты
- Серверы аутентифик...
- Профили аутентифи...
- Роли пользователей
- Ролевые разрешения
- Каталоги пользоват...

Сеть

- Зоны
- Интерфейсы
- Шлюзы
- Маршруты

Администраторы

Администраторы

[+ Добавить](#) [Редактировать](#) [Удалить](#) [Включить](#)

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



Ролевой доступ SIEM

Роли пользователей



Ролевые разрешения



Профиль пользователя

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

- Консоль администратора
 - Настройки
 - Управление устройством
 - Администраторы
 - Сертификаты
 - Серверы аутентификац...
 - Профили аутентификац...
 - Роли пользователей**

Роли пользователей

+ Добавить | ✎ Редактировать | ✖ Удалить | ↻ | ⚙

Название
Administrator
Supervisor

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

- Консоль администратора
 - Настройки
 - Управление устройством
 - Администраторы
 - Сертификаты
 - Серверы аутентификац...
 - Профили аутентификац...
 - Роли пользователей
 - Ролевые разрешения**
 - Каталоги пользователей

Ролевые разрешения

↻

Название	Описание	Роли
Разрешения для инцидента		
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент	Analyst, Investigator, Supervisor
Назначение инцидентов	Возможность назначать пользователей на инциденты	Analyst, Investigator, Supervisor
Закрытие инцидента	Возможность закрыть инцидент. Часто полезно, когда одни сотруднк...	Analyst, Investigator, Supervisor

Профили администраторов

+ Добавить | ✎ Редактировать | ✖ Удалить | ↻

Название
Analyst - 1
Test user -

Настройка профиля

Общие | **Права доступа** | Роли пользователей

+ Добавить | ✖ Удалить

Выбор ролей пользователей

Название	Описание
Administrator	Responsible for system configuration

Отчеты

- 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 (highlighted)
 - 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 ...

Incidents Create incident

[INC-1] Login to critical system attempt

Edit Comment Assign Workflow Generate report

Details

Incident type: Incident	Status: Opened	Assignee: Administrat
Incident priority: Important	Resolution: Unresolved	Reporter: Administrat
Rule:	Schema: Incident	Last update by: Administrat
Description		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



**Спасибо
за внимание!**

Дмитрий Чеботарев

Менеджер по развитию продукта

