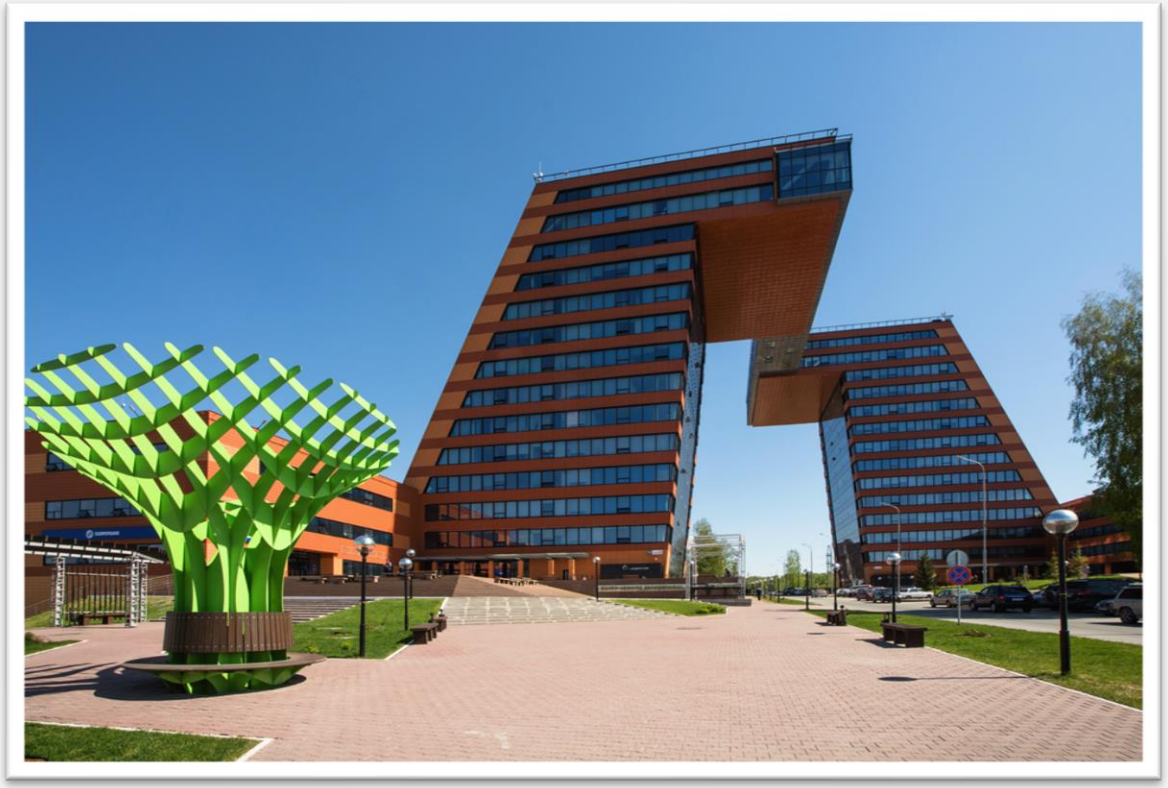
Новые продукты для защиты предприятия

Иван Чернов

Менеджер по развитию

ichernov@usergate.com

+7 983 129 13 06

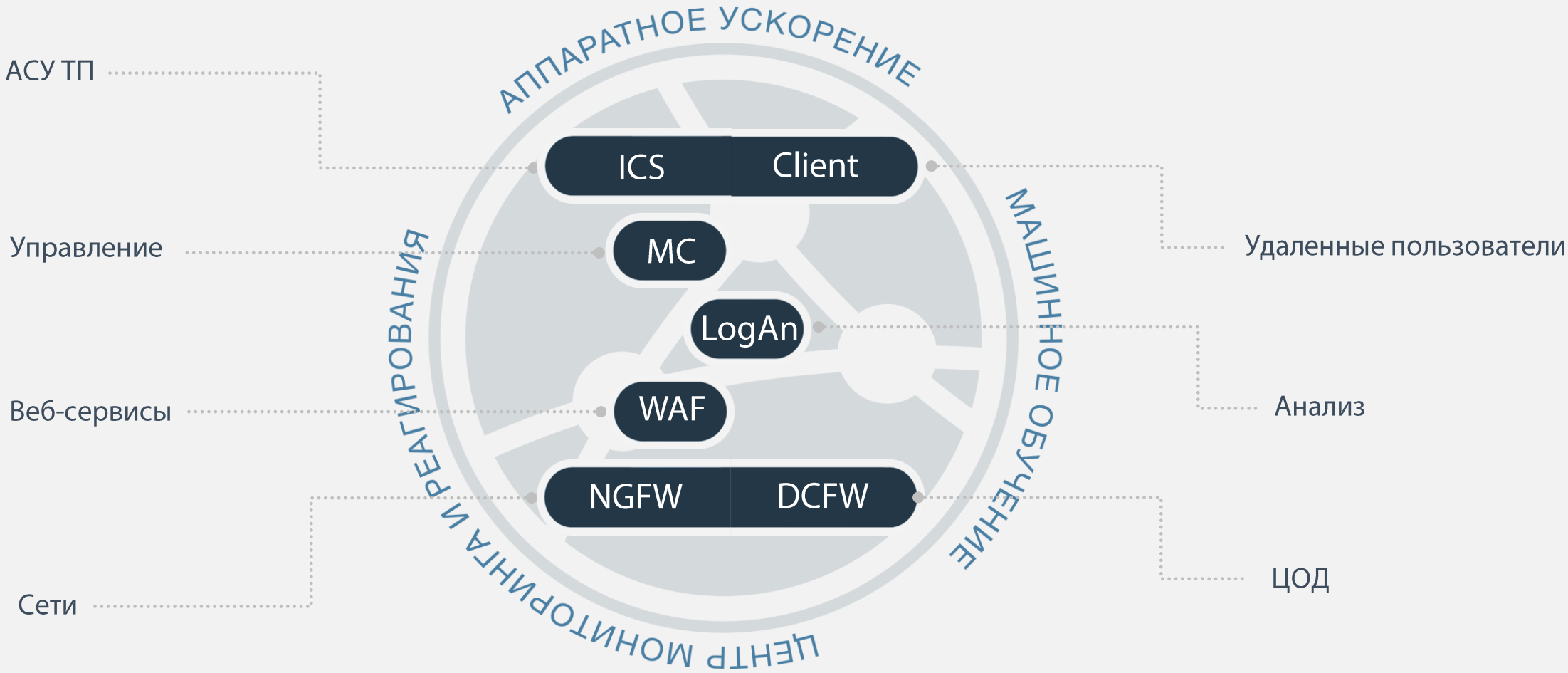


Наш офис разработки находится в Технопарке Новосибирского Академгородка, в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

Дополнительные офисы:
г. Москва, г. Санкт-Петербург, г. Хабаровск

UserGate

UserGate SUMMA



UserGate

Что нового?

NGFW

UG OS 7 – полностью новая OS

NGFW

Поддержка ARM – платформы C150 и X10

NGFW

Новый движок IDPS

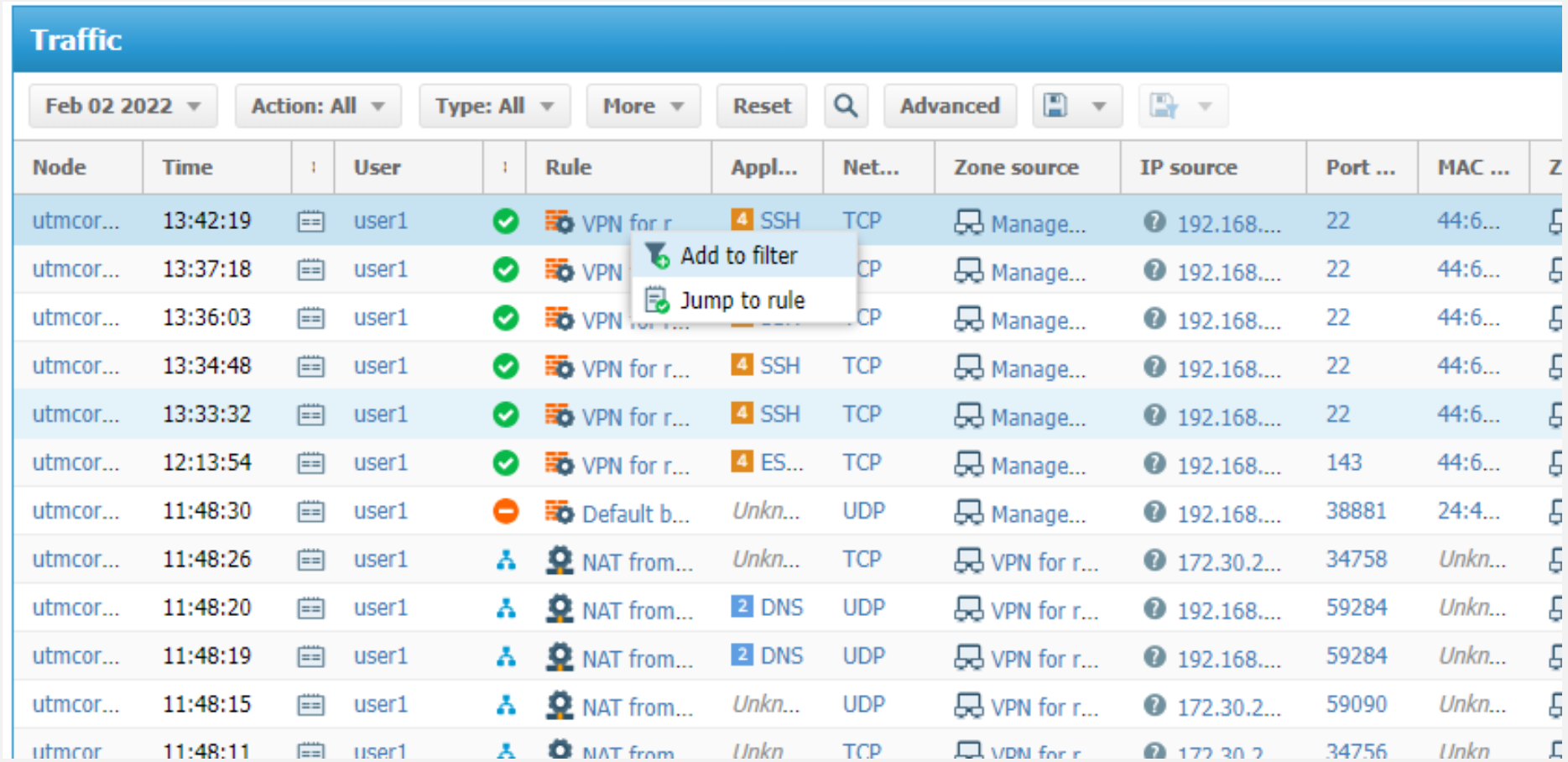
NGFW: работа с трафиком

- Добавлена возможность записи трафика в любых направлениях (входящий/исходящий).
- Добавлена возможность отправки расшифрованного SSL-трафика на внешние системы безопасности (SSL-tap).
- Добавлена возможность записи трафика при срабатывании сигнатур СОВ.
- Добавлена возможность проверки зашифрованного трафика SSL с помощью СОВ.

NGFW

- Обновление CLI
- Расширение API
- UPL
- Cloud init
- Live Backup

UserGate Log Analyzer


Traffic
Feb 02 2022
Action: All
Type: All
More
Reset
Advanced
Node
Time
User
Rule
Appl...
Net...
Zone source
IP source
Port ...
MAC ...
utmcor... 13:42:19 user1 VPN for r SSH TCP Manage... 192.168.... 22 44:6...
Add to filter
Jump to rule
utmcor... 13:37:18 user1 VPN CP Manage... 192.168.... 22 44:6...
utmcor... 13:36:03 user1 VPN CP Manage... 192.168.... 22 44:6...
utmcor... 13:34:48 user1 VPN for r... SSH TCP Manage... 192.168.... 22 44:6...
utmcor... 13:33:32 user1 VPN for r... SSH TCP Manage... 192.168.... 22 44:6...
utmcor... 12:13:54 user1 VPN for r... ES... TCP Manage... 192.168.... 143 44:6...
utmcor... 11:48:30 user1 Default b... Unkn... UDP Manage... 192.168.... 38881 24:4...
utmcor... 11:48:26 user1 NAT from... Unkn... TCP VPN for r... 172.30.2... 34758 Unkn...
utmcor... 11:48:20 user1 NAT from... DNS UDP VPN for r... 192.168.... 59284 Unkn...
utmcor... 11:48:19 user1 NAT from... DNS UDP VPN for r... 192.168.... 59284 Unkn...
utmcor... 11:48:15 user1 NAT from... Unkn... UDP VPN for r... 172.30.2... 59090 Unkn...
utmcor 11:48:11 user1 NAT from Unkn TCP VPN for r 172.30.2 34756 Unkn

LogAn

SIEM

Аналитика

Правила аналитики | Поиск | Правила действий | Срабатывания | Подробности срабатывания

01 Март 2021 г. 00:00 – 25 Май 2021 г. 23:59 | ID: Все | Правила: Все | Статус: Все | Приоритет: Все | Ещё | Расширенный | Сохранить как | Популярные фильтры | Редактировать | Показать по

Узел	Время	ID	Время первого со...	Время последнего...	Правило	Категория	Статус	Приоритет	Админи...	Пользов...	Сигнатуры
loganalyzer@ugutm	15:36:58	SEC-20	15:16:19	15:19:48	Download Mimikatz by Certutil.exe	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-19	15:24:35	15:24:35	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-18	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-17	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-16	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-15	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-14	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-13	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-12	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-11	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-10	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-9	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-8	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-7	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:36	SEC-6	15:19:48	15:19:48	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:11	SEC-5	15:05:51	15:16:09	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:11	SEC-4	15:05:43	15:06:07	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:11	SEC-3	15:05:35	15:06:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:11	SEC-2	15:05:19	15:06:05	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	Unknown	Нет
loganalyzer@ugutm	15:36:11	SEC-1	15:00:45	15:02:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	Unknown	Нет

Сортировать по возрастанию
Сортировать по убыванию
Столбцы

Правила аналитики | Поиск | Правила действий | Срабатывания | Подробности срабатывания

Срабатывание

SEC-15 Время: 15:36:36 Показать

Статус

Статус: Active Приоритет: Нормальны

Тикеты

Добавить в тикет

Время	Время п...	Время п...	Узел	Источ...	Важно...	Компонент	Тип события	Имя по	При...	Прот...	HTTP
15:20:35			logan_...	Журнал '				*Unknou*			

Страница 1 из 1

Display a menu

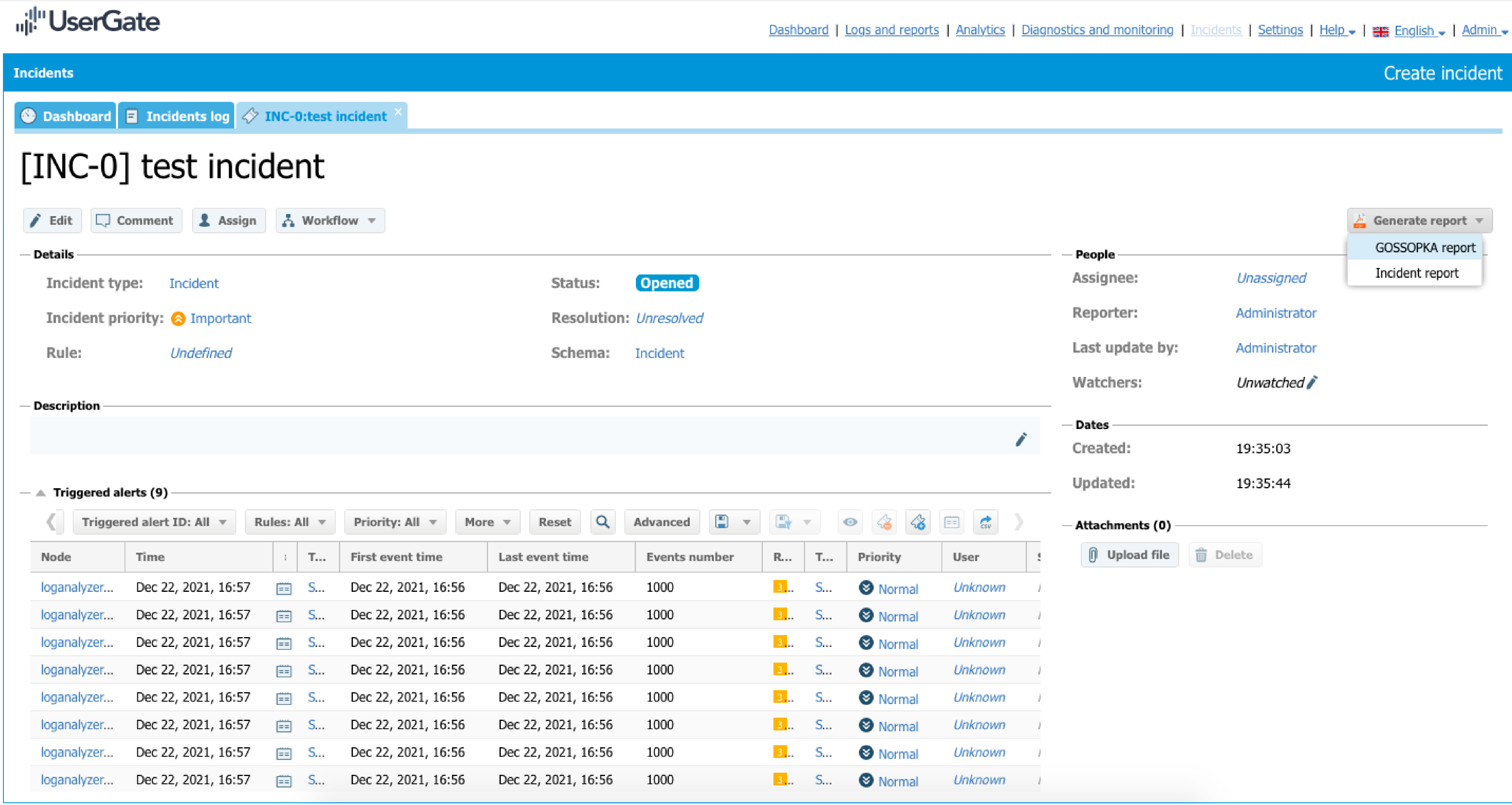
Запись журнала WMI

Узел:	logan_core@stiothhesese
Время:	15:20:35
Сенсор:	Win10
Счётчик:	Sysmon
Файл журнала лога:	Microsoft-Windows-Sysmon/Operational
Уровень лога:	Information
Источник журнала событий:	Microsoft-Windows-Sysmon
Категория лога:	2
Категория задачи:	File creation time changed (rule: FileCreateTime)
Имя компьютера:	MSEDGEWIN10.usergate.demo
Код события лога:	2
Идентификатор события лога:	2
Тип события лога:	3
Строка вставки:	T1099,2021-05-25 12:20:35.079,{43199d79-9603-60ac-8800-000000001200},2388,C:\Windows\Explorer.EXE,C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe,2021-05-18 14:08:42.000,2021-05-25 12:20:35.051
Данные:	File creation time changed: RuleName: T1099 UtcTime: 2021-05-25 12:20:35.079 ProcessGuid: {43199d79-9603-60ac-8800-000000001200} ProcessId: 2388 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe CreationUtcTime: 2021-05-18 14:08:42.000 PreviousCreationUtcTime: 2021-05-25 12:20:35.051

Закрыть

LogAn

IRP

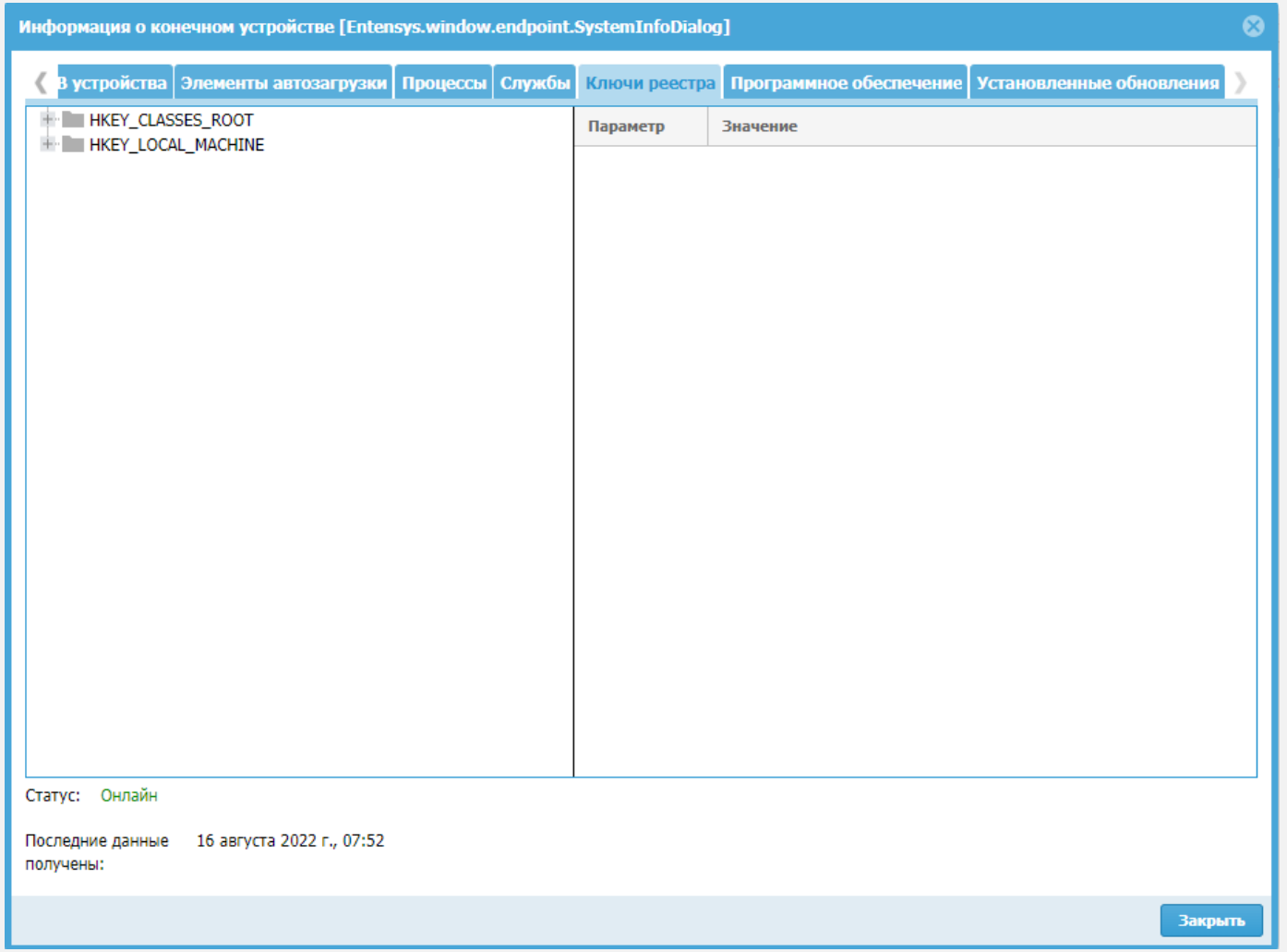

UserGate
Dashboard | Logs and reports | Analytics | Diagnostics and monitoring | Incidents | Settings | Help | English | Admin
Incidents
Create incident
Dashboard
Incidents log
INC-0:test incident
[INC-0] test incident
Edit
Comment
Assign
Workflow
Generate report
GOSSOPKA report
Incident report
Details
Incident type: Incident
Status: Opened
Incident priority: Important
Resolution: Unresolved
Rule: Undefined
Schema: Incident
People
Assignee: Unassigned
Reporter: Administrator
Last update by: Administrator
Watchers: Unwatched
Description
Dates
Created: 19:35:03
Updated: 19:35:44
Triggered alerts (9)
Triggered alert ID: All
Rules: All
Priority: All
More
Reset
Advanced
Attachments (0)
Upload file
Delete
Node
Time
T...
First event time
Last event time
Events number
R...
T...
Priority
User
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown
loganalyzer... Dec 22, 2021, 16:57 S... Dec 22, 2021, 16:56 Dec 22, 2021, 16:56 1000 3... S... Normal Unknown

UserGate Client

Client

- видимость событий безопасности;
- контроль устройства;
- доступ с нулевым доверием.

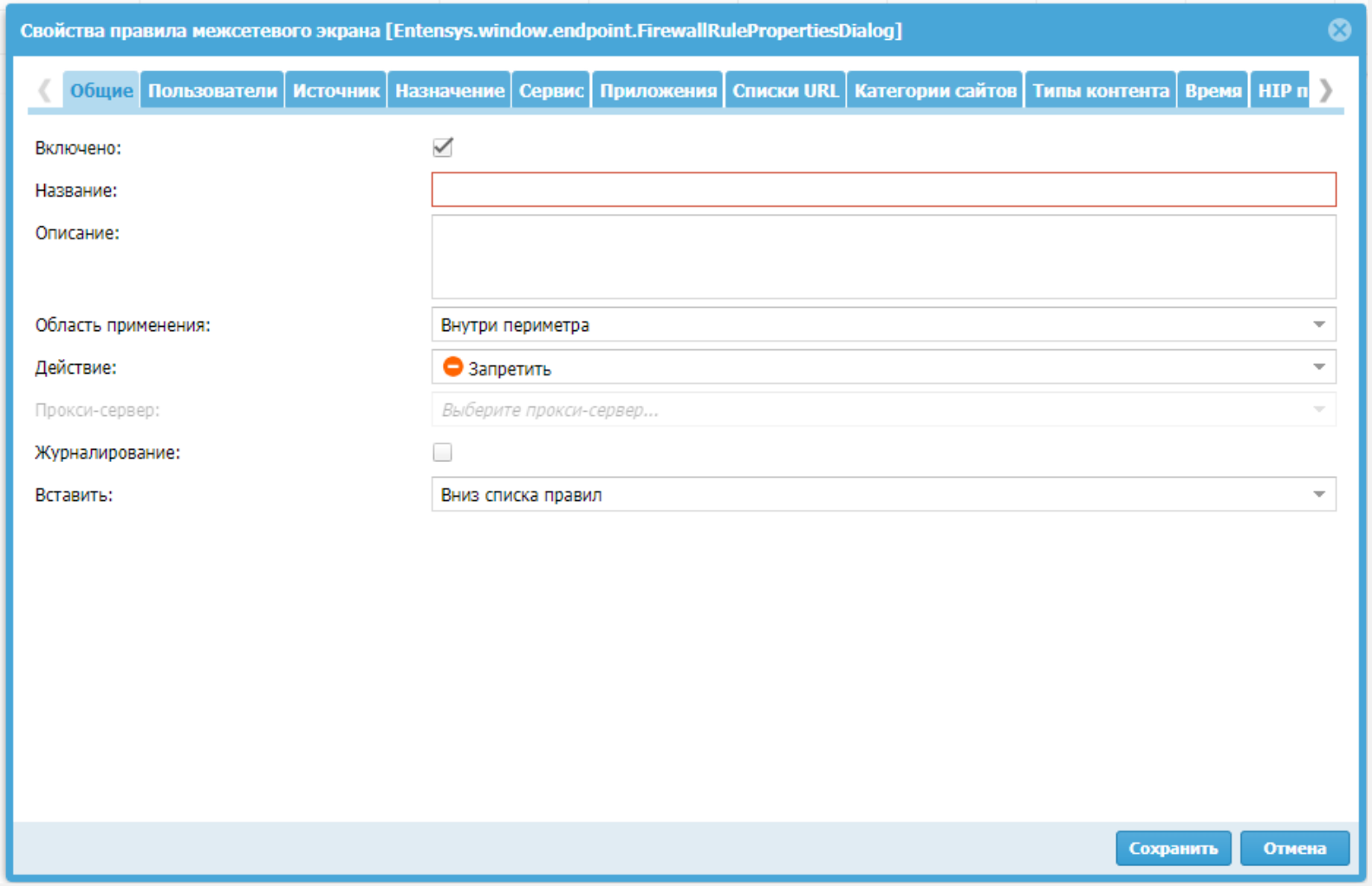
Сбор информации



Сбор информации

- состояние, память и производительность;
- безопасность;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- службы;
- ключи реестра;
- программное обеспечение;
- установленные обновления.

Персональный МЭ



NAC

Профили устройства:

- продукт;
- процесс;
- запущенная служба;
- ключи реестра;
- установленные обновления.

VPN

- Client2Site – IPSec/L2TP, IKEv2;
- SSL VPN;
- «Принудительный» VPN.

Экспертиза

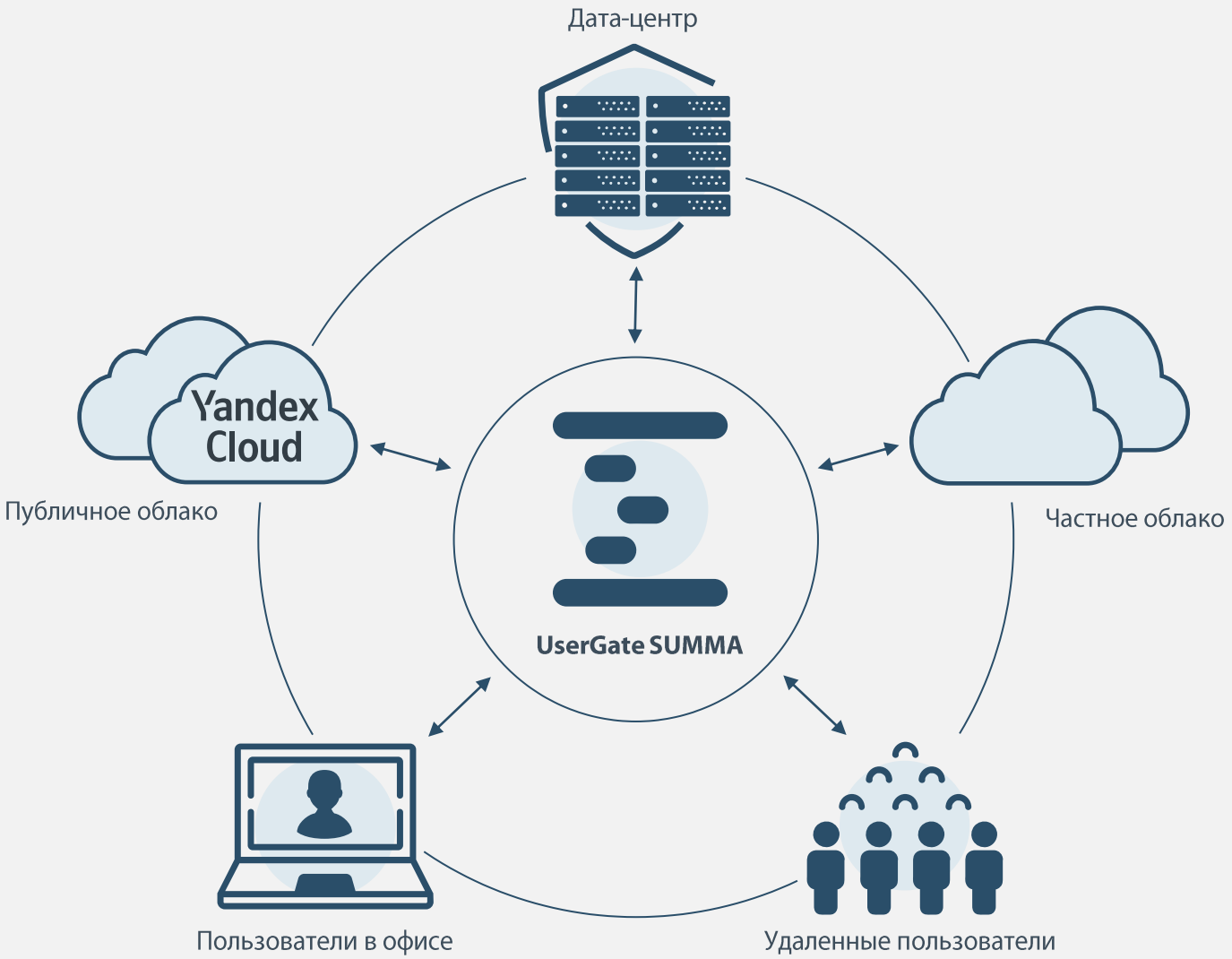
Данные из логов, которые можно обогатить и найти следы компрометации:

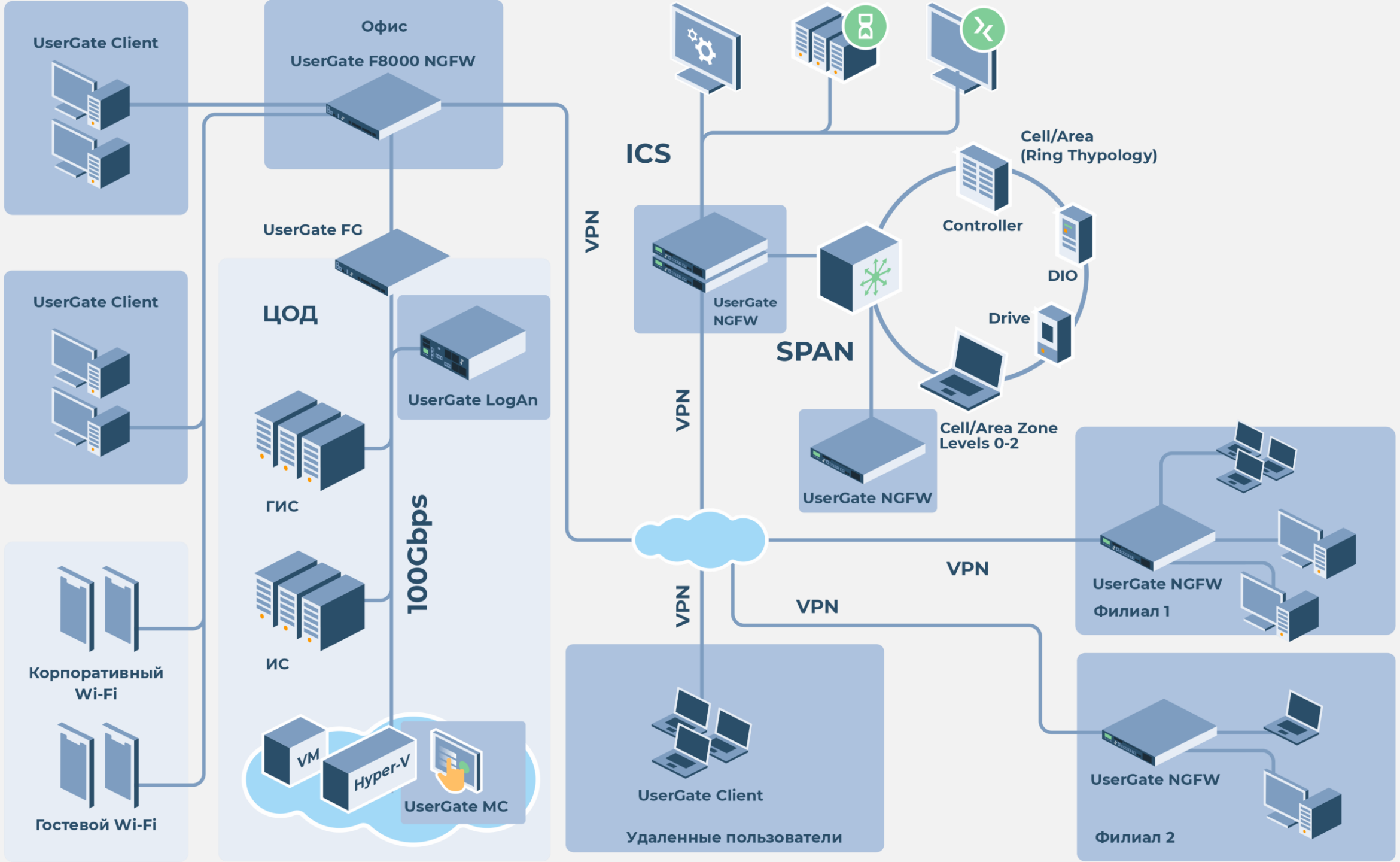
- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

XDR


Extended
Detection
Response
Сети
Облака
Устройства
UserGate Log Analyzer
SOC
Cloud Protection
Client
Proxy
NGFW
WAF

ZTNA


Дата-центр
Yandex Cloud
Публичное облако
UserGate SUMMA
Частное облако
Пользователи в офисе
Удаленные пользователи


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

Новые продукты для защиты предприятия

Иван Чернов

Менеджер по развитию

ichernov@usergate.com

+7 983 129 13 06