UserGate SUMMA:
Моновендорный подход к построению SOC

Александр Богданов
Партнерский отдел UserGate

abogdanov@usergate.com
+7 (800) 500 40 32 доб. 1033 | +7 (913) 792 61 48

Как созревает SOC?

Киберпреступники

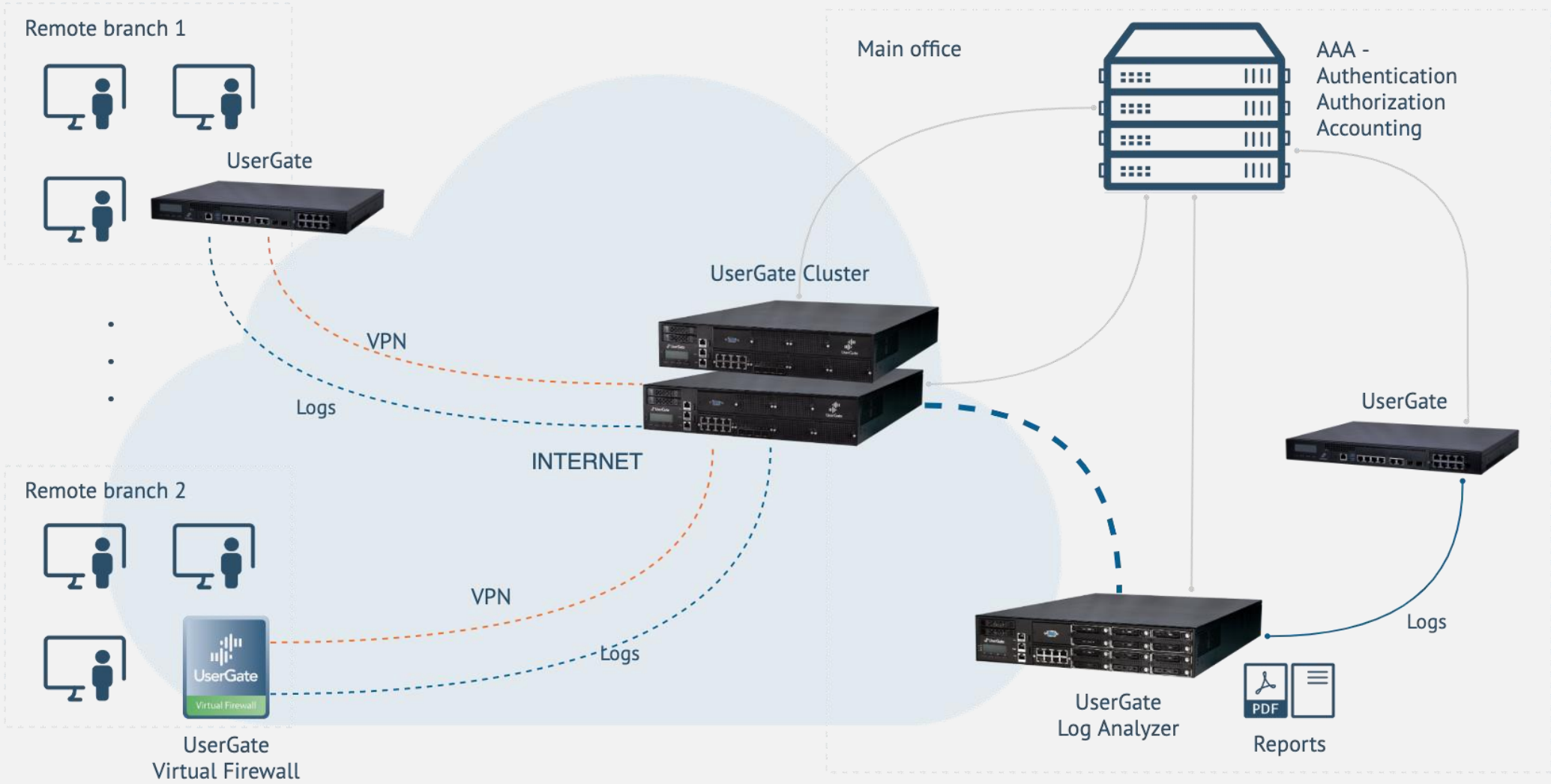
- Мультивекторный подход
- Социальная инженерия
- Горизонтальное перемещение по сети
- Широкая площадь атаки
- APT-атаки

Службы ИБ

- Набор базовых превентивных средств защиты
- Разные консоли управления
- Отсутствие корреляции событий
- Долгая реакция на инциденты
- Много статей расходов

1. Сбор и корреляция событий

Что делать?


Remote branch 1
UserGate
Main office
AAA -
Authentication
Authorization
Accounting
UserGate Cluster
VPN
Logs
INTERNET
UserGate
Remote branch 2
VPN
Logs
UserGate
Virtual Firewall
UserGate
Log Analyzer
Logs
PDF
Reports
UserGate
Virtual Firewall

Аналитика

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

source='traffic log' AND dayOfWeek=2

Добавить правило | Добавить условие | Добавить в тикет

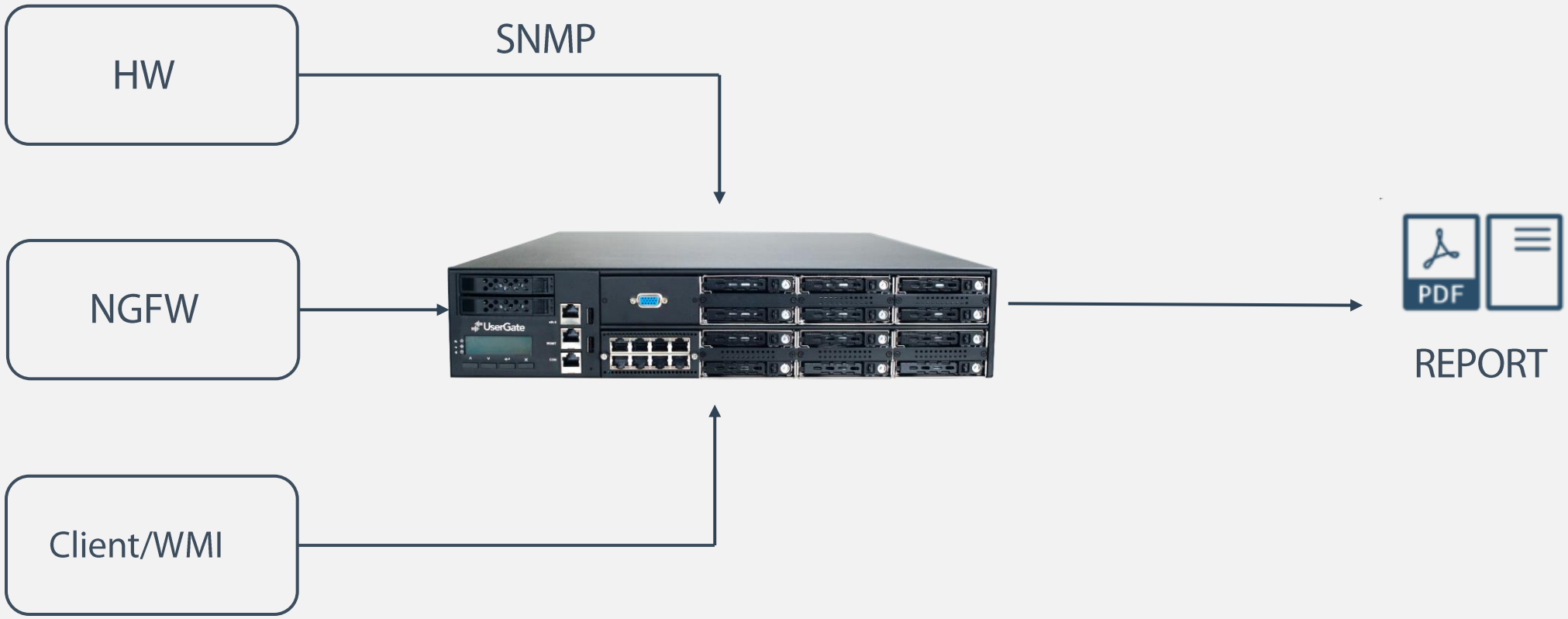
Время	Узел	Источ...	Имя пользо...	Правило	Действие	При...	Прот...	Зона источ...	IP источника	Порт...	Зона назна...	IP назначе...	Порт...	NAT адрес ...	NAT ...	NAT адрес ...	NAT ...	Б
17:08:29	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57036	Trusted	192.168....	80		0		0	6
17:08:29	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57042	Trusted	192.168....	80		0		0	6
17:08:28	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56132	Unknown	192.168....	8010	192.168.95.2...	56132	192.168.2.101	8010	6
17:08:24	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57040	Trusted	192.168....	80		0		0	6
17:08:23	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57034	Trusted	192.168....	80		0		0	6
17:08:16	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.116	60077	Trusted	192.168....	7680		0		0	5
17:08:16	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57032	Trusted	192.168....	80		0		0	6
17:08:14	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.129	62676	Trusted	192.168....	7680		0		0	5
17:08:14	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57036	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57034	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57030	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57028	Trusted	192.168....	80		0		0	6
17:08:00	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57032	Trusted	192.168....	80		0		0	6
17:08:00	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57026	Trusted	192.168....	80		0		0	6
17:07:54	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56128	Unknown	192.168....	8010	192.168.95.2...	56128	192.168.2.101	8010	6
17:07:54	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56127	Unknown	192.168....	8010	192.168.95.2...	56127	192.168.2.101	8010	6
17:07:53	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57024	Trusted	192.168....	80		0		0	6
17:07:52	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57030	Trusted	192.168....	80		0		0	6
17:07:51	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57028	Trusted	192.168....	80		0		0	6
17:07:45	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57026	Trusted	192.168....	80		0		0	6
17:07:44	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57018	Trusted	192.168....	80		0		0	6
17:07:38	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57016	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57024	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57022	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57020	Trusted	192.168....	80		0		0	6

Страница 1 из 5104

Display a menu

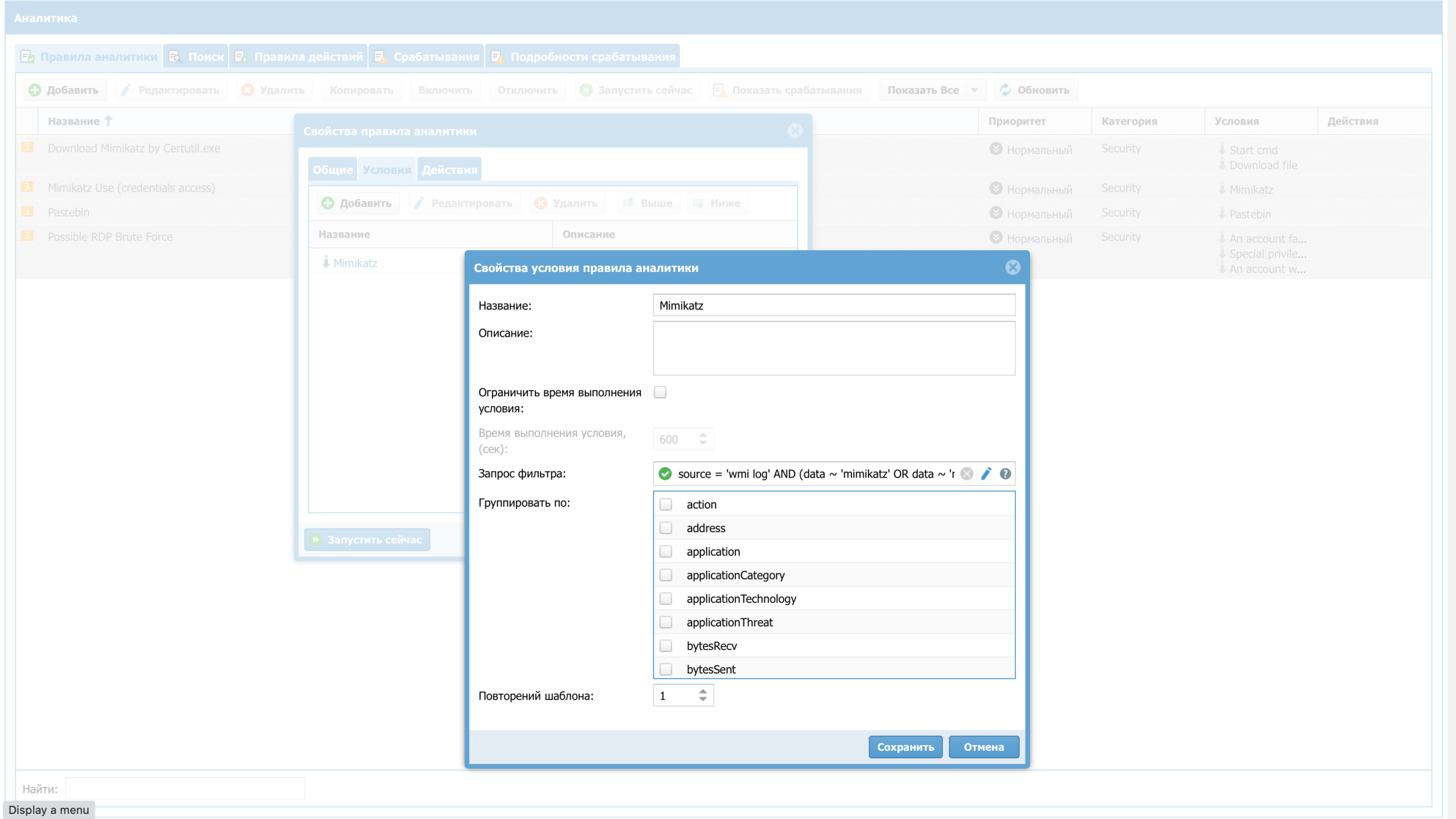
1. Сбор и корреляция событий
2. Глобальный мониторинг

Что делать?


HW
SNMP
NGFW
Client/WMI
PDF
REPORT

Что делать?

1. Сбор и корреляция событий
2. Глобальный мониторинг
3. Реагирование


Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Запустить сейчас
Показать срабатывания
Показать Все
Обновить
Название
Приоритет
Категория
Условия
Действия
Download Mimikatz by Certutil.exe
Нормальный
Security
Start cmd
Download file
Mimikatz Use (credentials access)
Нормальный
Security
Mimikatz
Pastebin
Нормальный
Security
Pastebin
Possible RDP Brute Force
Нормальный
Security
An account fa...
Special privile...
An account w...
Свойства правила аналитики
Общие
Условия
Действия
Добавить
Редактировать
Удалить
Выше
Ниже
Название
Описание
Mimikatz
Запустить сейчас
Свойства условия правила аналитики
Название:
Mimikatz
Описание:
Ограничить время выполнения условия:
Время выполнения условия, (сек):
600
Запрос фильтра:
source = 'wmi log' AND (data ~ 'mimikatz' OR data ~ 'r
Группировать по:
action
address
application
applicationCategory
applicationTechnology
applicationThreat
bytesRecv
bytesSent
Повторений шаблона:
1
Сохранить
Отмена
Найти:
Display a menu

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*			

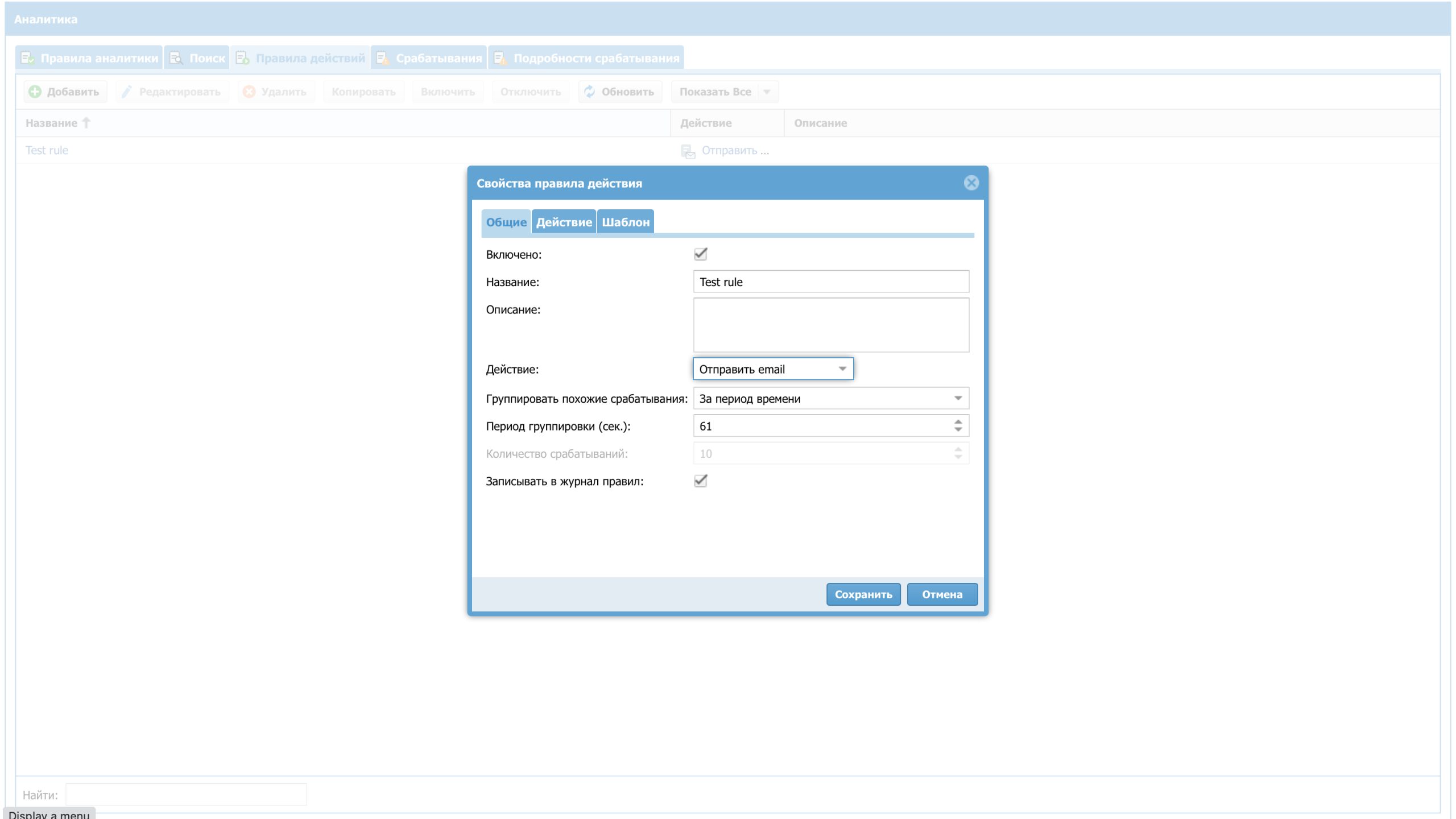
Страница 1 из 1

Display a menu

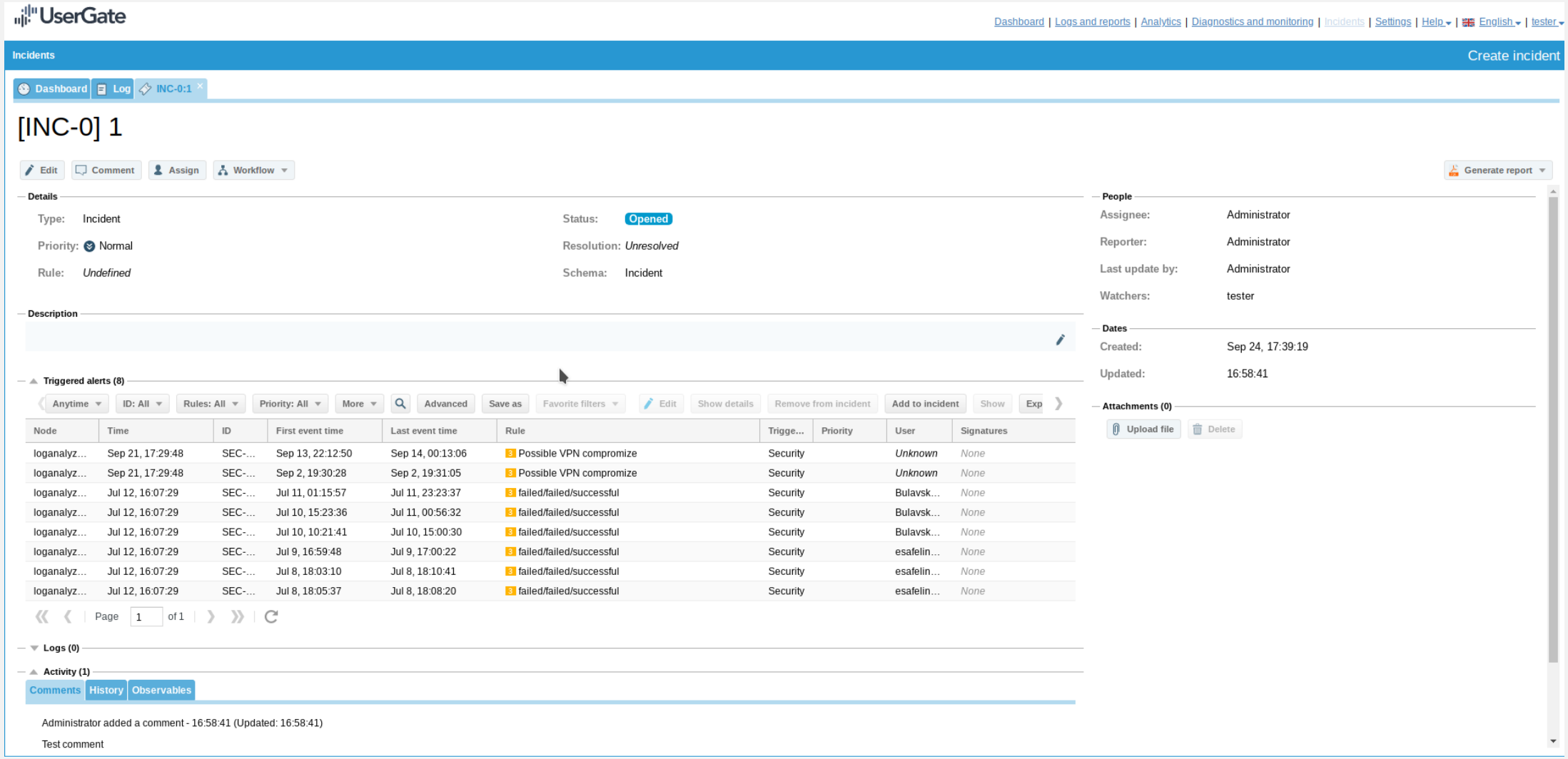
Запись журнала WMI

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


Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Обновить
Показать Все
Название
Действие
Описание
Test rule
Отправить ...
Свойства правила действия
Общие
Действие
Шаблон
Включено:
Название:
Test rule
Описание:
Действие:
Отправить email
Группировать похожие срабатывания:
За период времени
Период группировки (сек.):
61
Количество срабатываний:
10
Записывать в журнал правил:
Сохранить
Отмена
Найти:
Display a menu

Карточка инцидента

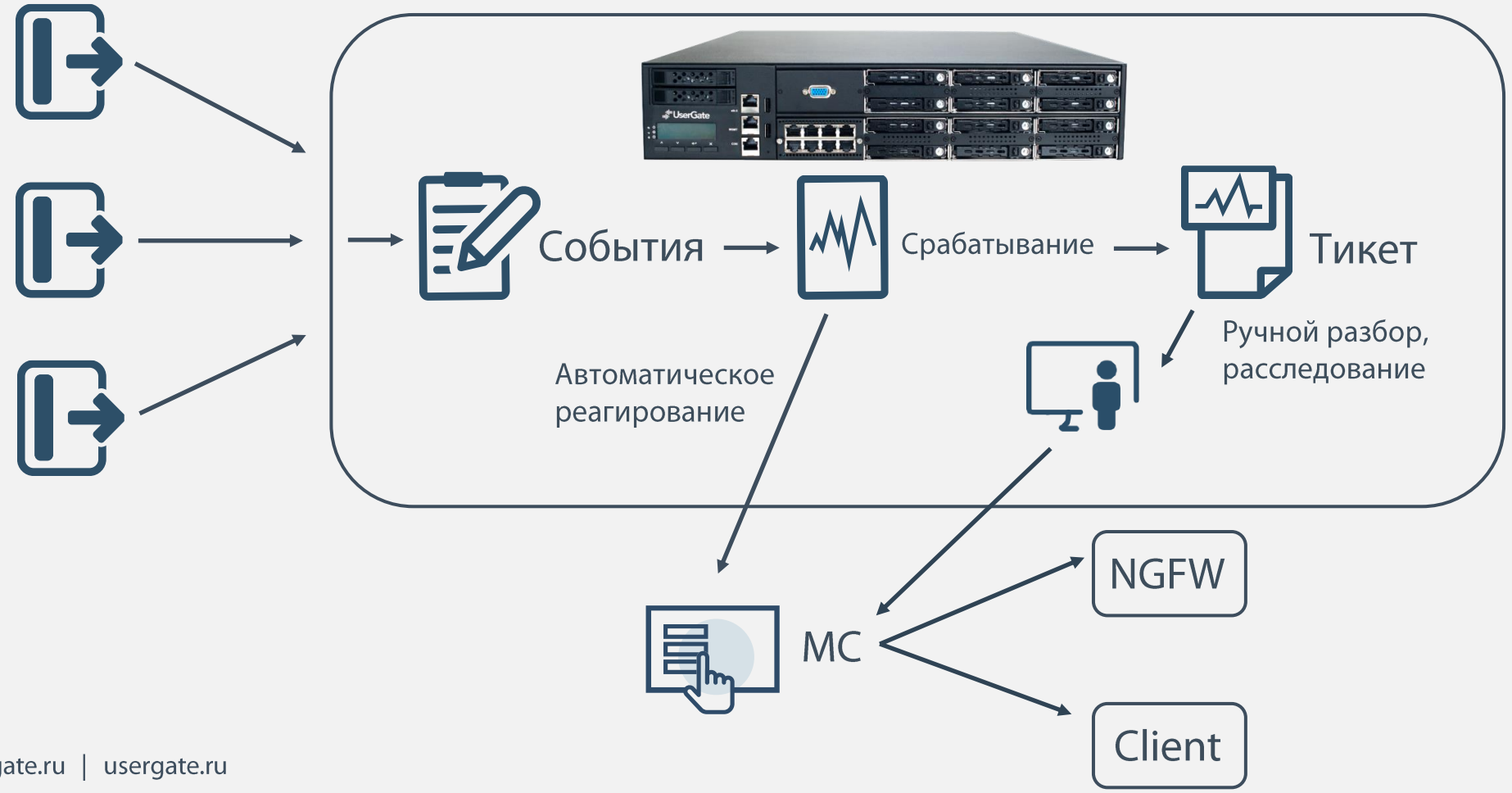


Что делать?

1. Сбор и корреляция событий
2. Глобальный мониторинг
3. Реагирование
4. Унифицированная платформа

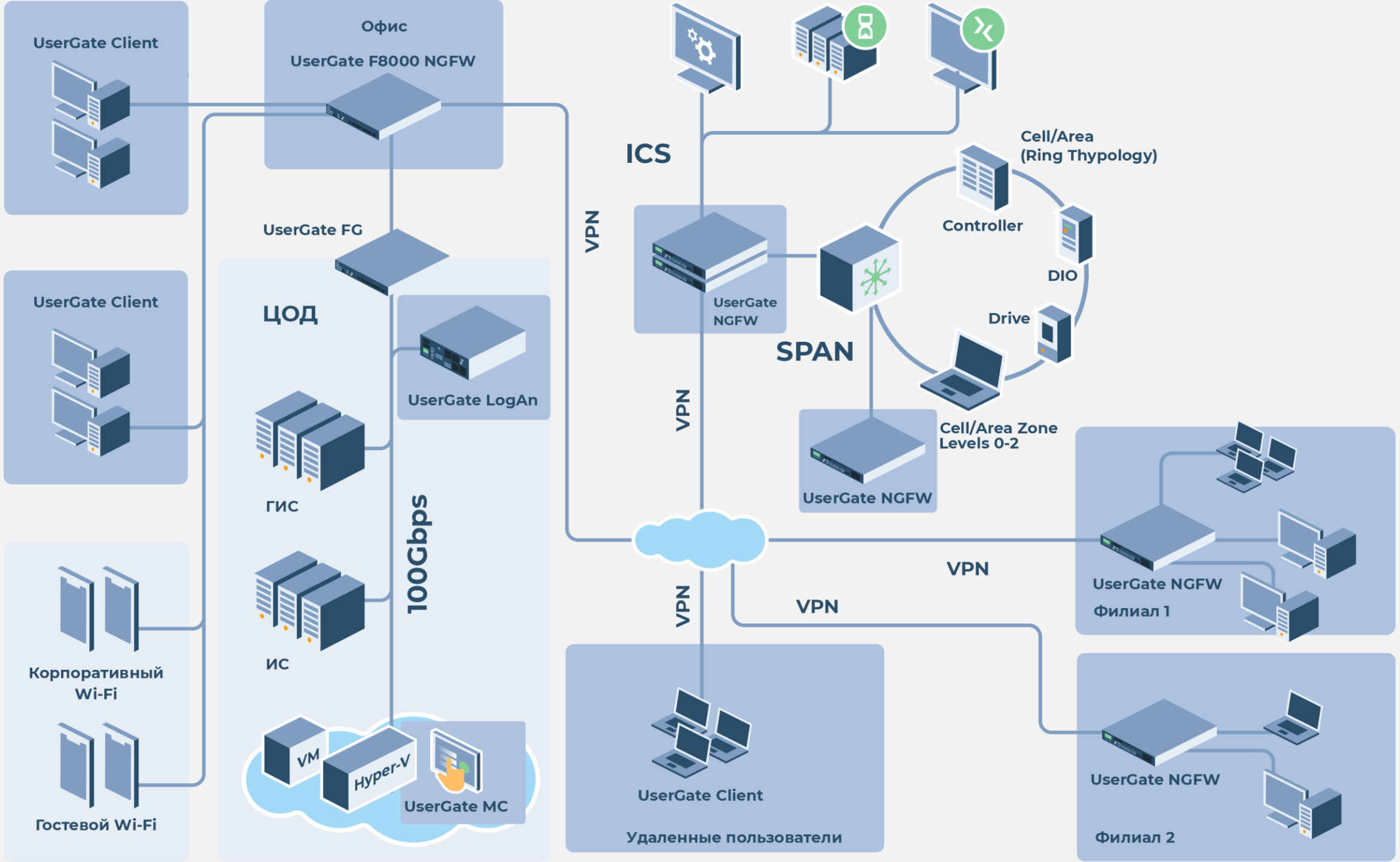
LogAn сейчас

SIEM + IRP


События
Срабатывание
Тикет
Автоматическое
реагирование
Ручной разбор,
расследование
MC
NGFW
Client

В составе UserGate SUMMA:

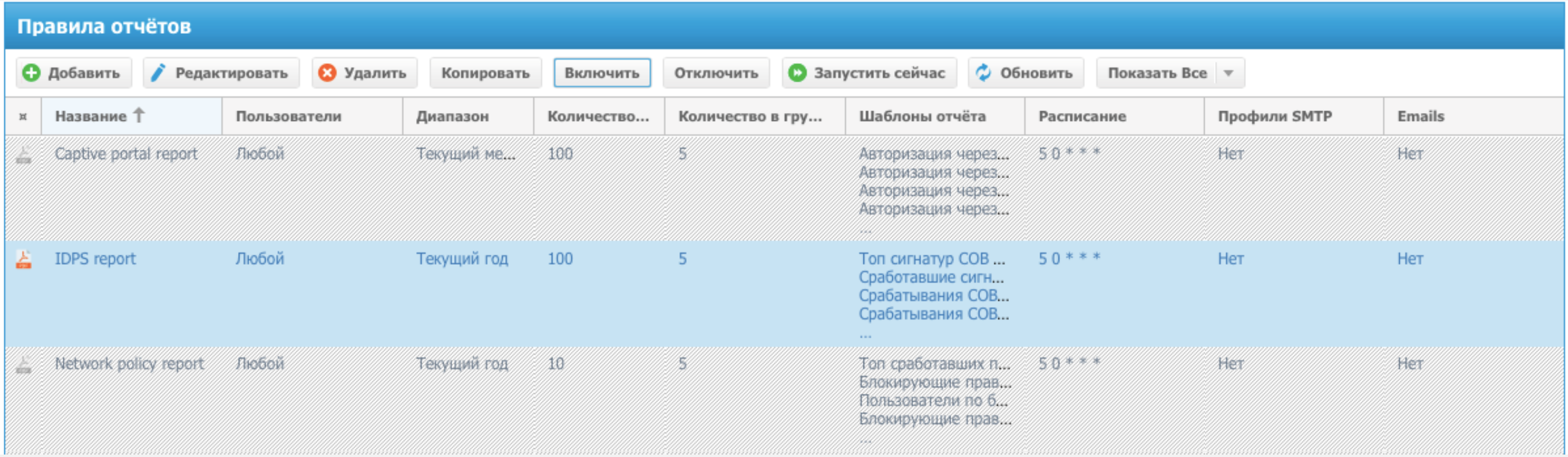
LogAn + MC = SOAR


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

Что делать?

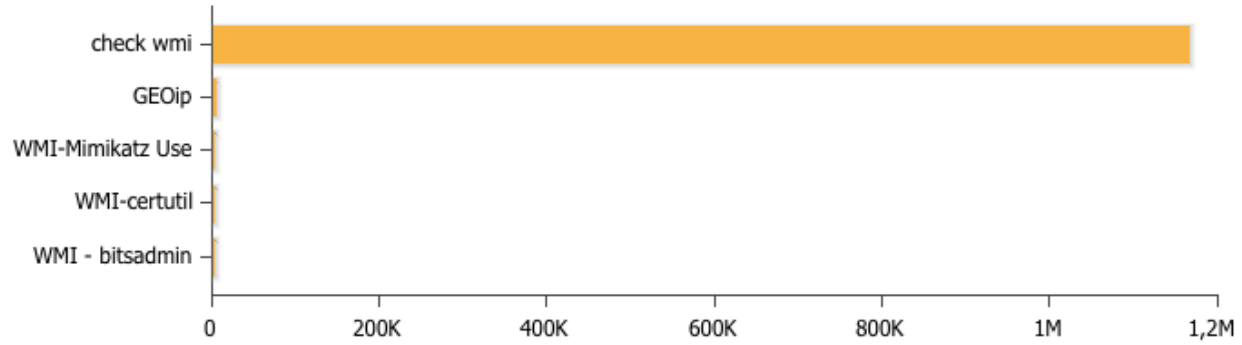
1. Сбор и корреляция событий
2. Глобальный мониторинг
3. Реагирование
4. Унифицированная платформа
5. Систематизация

Правила отчетов



Дашборд

Top 10 analytics rules Год | Месяц | Неделя | День | Сейчас

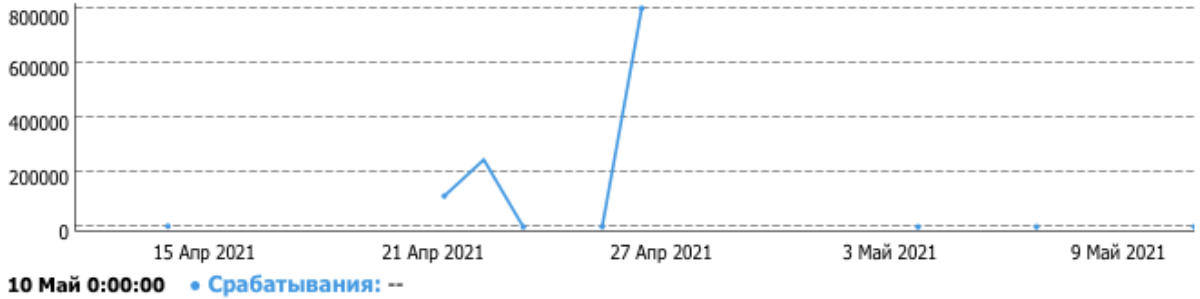


Last 10 triggered alerts Год | Месяц | Неделя | **День** | Сейчас

Время	ID	Правило	Статус	Приоритет	Админи...
14:15:28	SEC-297...	WMI-cert...	Active	Норма...	Anna
14:15:28	SEC-297...	WMI-cert...	Active	Норма...	Anna
14:15:28	SEC-297...	WMI-cert...	Active	Норма...	Anna
14:15:28	SEC-297...	WMI-cert...	Active	Норма...	Anna
13:41:00	SEC-297...	WMI-cert...	Active	Норма...	Anna
13:41:00	SEC-297...	WMI-cert...	Active	Норма...	Anna
13:41:00	SEC-297...	WMI-cert...	Active	Норма...	Anna

Top 10 triggered alerts source countries Год | Месяц | Неделя | День | Сейчас

Triggered alerts graph Год | Месяц | Неделя | День | Сейчас



Что делать?

1. Сбор и корреляция событий
2. Глобальный мониторинг
3. Реагирование
4. Унифицированная платформа
5. Систематизация
6. SOC – это система и люди

SOC UserGate

Центр мониторинга и реагирования UserGate добавил в Систему обнаружения вторжений UserGate (IDPS) новую сигнатуру, позволяющую детектировать атаки, использующие уязвимость CVE-2021-41773 в сервере Apache.

Уязвимость возникает из-за ошибок в процессе нормализации URL (конвертация сервером Apache схем пути URL) и позволяет злоумышленникам осуществить path traversal атаку, сопоставив URL-адреса с файлами за пределами ожидаемого корня документа. Подобная атака может привести к утечке CGI-скриптов. Уязвимость получила рейтинг 7,5 по шкале CVSS v3.1.

Уязвимые продукты:

- Apache HTTP Server версии 2.4.49.

Система обнаружения вторжений (СОВ) в составе UserGate NGFW детектирует и блокирует сеансы, связанные с этой уязвимостью, автоматически.

Специалисты Центра мониторинга и реагирования UserGate рекомендуют пользователям Apache одно из следующих действий:

- проверить актуальность подписки на модуль Security Updates. При использовании профиля сигнатур UserGate, все новые сигнатуры начинают работать автоматически;
- создать правило СОВ с новой сигнатурой Path traversal and file disclosure vulnerability in Apache 2.4.49, если используется собственный профиль сигнатур;
- обновить Apache до последней версии;
- включить настройку "`require all denied`" в httpd.conf.

Центр мониторинга и реагирования UserGate добавил в Систему Обнаружения Вторжений (СОВ) UserGate новую сигнатуру, позволяющую детектировать атаки с использованием уязвимости нулевого дня CVE-2021-22005 в продукте vCenter компании Vmware.

21 сентября Vmware объявила пользователям о необходимости обновить ПО до последний версии, в которой были исправлены опасные уязвимости. Уязвимость CVE-2021-22005 в подключаемом модуле Virtual SAN Health Check, включенном в состав vCenter по умолчанию, оценивается в 9,8 балла по шкале CVSS v3. Уязвимость позволяет неаутентифицированному пользователю загрузить любой файл и исполнить произвольную команду операционной системы.

Уязвимые продукты:

- Vmware vCenter Server версий 6.7, 7.0;
- Vmware Cloud Foundation версий 3.x и 4.x.

Система Обнаружения Вторжений (СОВ) в составе UserGate NGFW детектирует и блокирует сеансы, связанные с этой уязвимостью автоматически.

Специалисты центра мониторинга и реагирования на киберугрозы UserGate рекомендуют пользователям следующие действия:

- Установить последнюю версию ПО с сайта производителя.
- Проверить актуальность подписки на модуль Security Updates. При использовании профиля сигнатур UserGate, все новые сигнатуры начинают работать автоматически.
- При использовании собственного профиля сигнатур, необходимо создать правило СОВ с новой сигнатурой «VMWare vCenter 6.7/7.0 Arbitrary File Upload».

UserGate

Спасибо за внимание!

Александр Богданов
Партнерский отдел UserGate

abogdanov@usergate.com
+7 (800) 500 40 32 доб. 1033 | +7 (913) 792 61 48