



7.1

БОЛЬШОЕ ОБНОВЛЕНИЕ

Игорь Шефер  
Ведущий инженер UserGate



# IPSecv3



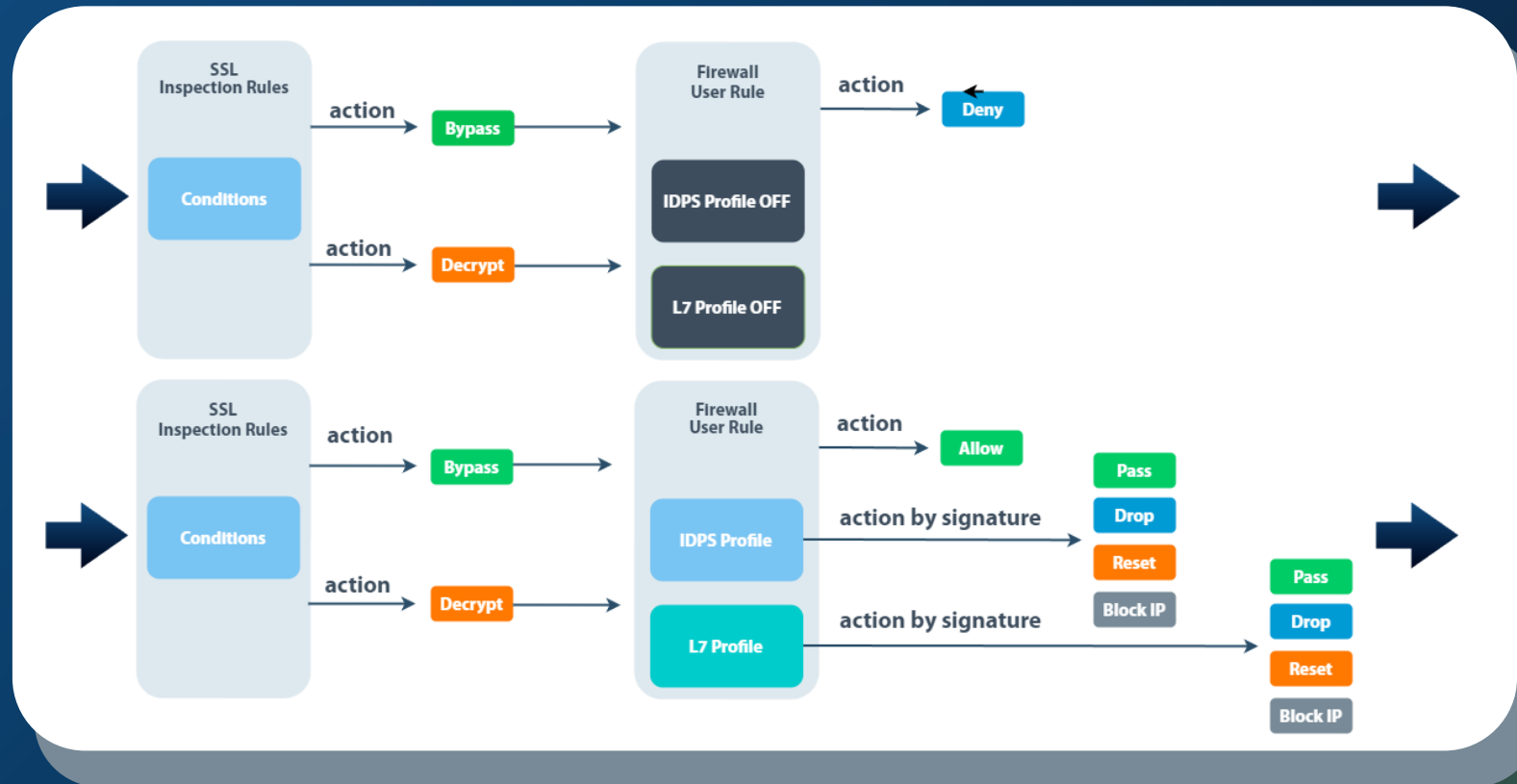
# ДВИЖОК

UserGate  
7.1

- 3 версия движка
- Поддержка обработки расшифрованного SSL
- Возможность описывать сигнатуры COB и L7-приложений (UASL)
- Верификация
- Интеграция в политики МЭ
- Расширение списка действий (action) при срабатывании
- Применение действия (action) по каждой сигнатуре
- Возможность захвата пакетов при сработке COB и L7-приложений
- Полноценное управление в CLI



# Action Flow





# Новые кейсы

UserGate  
7.1

- Детектирование и блокировка BruteForce сервисов
- Определение атак в зашифрованном трафике
- Сканирование пакетов на уровне протокольных диссекторов
- Белые списки приложений
- Обнаружение и блокировка туннелей
- Работа с метками в стриме



## GUI. IPS-сигнатуры

IPS signatures

Enable: All | All | Action: All | Owner: All | More | Reset | Search | Advanced

	Id	Status	Signature name	Action	Signature operating ...	Protocol	Class type	References	Category	Enable PCAP	Owner
5	20020090	Default settin...	(MS00-021)Microsoft NT / Windows 2000 ...	Pass	Windows	tcp	denial-of-service	CVE: 2000-0232	misc	Disabled	UserGate
5	20020052	Default settin...	(MS00-040)Microsoft Windows NT 4.0 Re...	Pass	Cisco	tcp	denial-of-service	CVE: 2000-0377	misc	Disabled	UserGate
5	22000124	Default settin...	(MS00-092)Microsoft SQL Server xp_displa...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2000-1081	sql	Disabled	UserGate
5	22000122	Default settin...	(MS00-092)Microsoft SQL Server xp_displa...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2000-1081	sql	Disabled	UserGate
5	22000170	Default settin...	(MS02-038)Microsoft SQL Server INSERT S...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2008-0106	sql	Disabled	UserGate
5	22000160	Default settin...	(MS02-039)Microsoft SQL Slammer worm ...	Pass	Windows	udp	arbitrary-code-exec...	CVE: 2002-0649	sql	Disabled	UserGate
5	22040024	Default settin...	(MS03-051)Microsoft FrontPage Server Ext...	Pass	Windows	tcp	arbitrary-code-exec...	None	misc	Disabled	UserGate
5	20020194	Default settin...	(MS04-007)LSASS.EXE Remote Denial-of-S...	Pass	Linux	tcp	denial-of-service	None	misc	Disabled	UserGate
5	20140538	Default settin...	(MS05-053)Internet Explorer WMF File Ren...	Pass	Windows	tcp	denial-of-service	CVE: 2005-2124	web client	Disabled	UserGate
5	20142804	Default settin...	(MS06-001)Windows Metafile SetAbortPro...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2005-4560	exploit	Disabled	UserGate
5	20142806	Default settin...	(MS06-001)Windows Metafile SetAbortPro...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2005-4560	exploit	Disabled	UserGate
5	20141458	Default settin...	(MS06-014)Internet Explorer MDAC RDS.D...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2006-0003	activex	Disabled	UserGate
5	20020490	Default settin...	(MS06-035)Microsoft Windows SMB PIPE ...	Pass	Windows	tcp	denial-of-service	CVE: 2006-3942	exploit	Disabled	UserGate
5	20020500	Default settin...	(MS06-035)Microsoft Windows SMB Rena...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2006-4696	misc	Disabled	UserGate
5	20020492	Default settin...	(MS06-063)Microsoft Windows SMB PIPE ...	Pass	Windows	tcp	denial-of-service	CVE: 2006-3942	exploit	Disabled	UserGate
5	20024	Default settin...	(MS07-003)Microsoft Outlook VEVENT Re...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-0033	exploit	Disabled	UserGate
5	20140380	Default settin...	(MS07-014)Microsoft Word 2000 Malform...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-0515	exploit	Disabled	UserGate
5	24040132	Default settin...	(MS07-017)Microsoft Windows Cursor And...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-0038	exploit	Disabled	UserGate
5	24040134	Default settin...	(MS07-017)Microsoft Windows Cursor And...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-0038	exploit	Disabled	UserGate
5	22444	Default settin...	(MS07-026)Microsoft Exchange Ical Reque...	Pass	Linux	tcp	denial-of-service	CVE: 2007-0039	exploit	Disabled	UserGate
5	20142726	Default settin...	(MS07-033)Internet Explorer COM Object L...	Pass	Linux MacOS Windows	tcp	arbitrary-code-exec...	CVE: 2007-0218	web client	Disabled	UserGate
5	20141462	Default settin...	(MS07-033)Internet Explorer COM Object L...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-0218	web client	Disabled	UserGate
5	20140472	Default settin...	(MS07-046)Windows GDI Malformed imag...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2007-3034	exploit	Disabled	UserGate
5	22000180	Default settin...	(MS08-040)Microsoft SQL Server CONVER...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2008-0086	sql	Disabled	UserGate

Page 1 of 435 | Total: 10871

- Security policies
  - Content filtering
  - Safe browsing
  - Tunnel inspection
  - SSL inspection
  - SSH inspection
  - Scenarios
  - Mail security
  - ICAP rules
  - ICAP servers
  - DoS rules
  - DoS profiles
- Global portal
- VPN
- Libraries
  - Morphology
  - Services
  - Services groups
  - IP addresses
  - Useragents
  - Content types
  - URL lists
  - Time sets
  - Bandwidth pools
  - Response pages
  - URL categories
  - Overridden URL categories
  - Applications
  - Application profiles
  - Applications groups
  - Emails
  - Phones
  - IPS signatures**
  - IPS profiles



## GUI. IPS профиль

IPS profile properties

General Signatures matched

Name: Default IPS profile

Description: Default UserGate IPS profile

Filters

Filters

threat > 3 AND owner = 'UserGate'

Save Cancel

IPS profile properties

General Signatures matched

Override Enable Disable Restore default Select all View All

Enable: All All Action: All Owner: All More Reset

	Id	Signature name ↑	Action	Signature ope...	Protocol	Class type	References	Category	Enable PCAP	Owner
5	20020090	(MS00-021)Microsoft NT / Win...	Pass	Windows	tcp	denial-of-ser...	CVE: 2000-02...	misc	Disabled	© UserGate
5	20020052	(MS00-040)Microsoft Windows ...	Pass	Cisco	tcp	denial-of-ser...	CVE: 2000-03...	misc	Disabled	© UserGate
5	22000124	(MS00-092)Microsoft SQL Serv...	Pass	Windows	tcp	arbitrary-cod...	CVE: 2000-10...	sql	Disabled	© UserGate
5	22000122	(MS00-092)Microsoft SQL Serv...	Pass	Windows	tcp	arbitrary-cod...	CVE: 2000-10...	sql	Disabled	© UserGate
5	22000170	(MS02-038)Microsoft SQL Serv...	Pass	Windows	tcp	arbitrary-cod...	CVE: 2008-01...	sql	Disabled	© UserGate

Page 1 of 202 Total: 10871 (filtered: 5044)

Save Cancel

- Security policies
  - Content filtering
  - Safe browsing
  - Tunnel inspection
  - SSL inspection
  - SSH inspection
  - Scenarios
  - Mail security
  - ICAP rules
  - ICAP servers
  - DoS rules
  - DoS profiles
- Global portal
- VPN
- Libraries
  - Morphology
  - Services
  - Services groups
  - IP addresses
  - Useragents
  - Content types
  - URL lists
  - Time sets
  - Bandwidth pools
  - Response pages
  - URL categories
  - Overridden URL categories
  - Applications
  - Application profiles
  - Applications groups
  - Emails
  - Phones
  - IPS signatures
  - IPS profiles



# GUI. IPS профиль. Переопределение

IPS profile properties

General Signatures matched

Override Enable Disable Restore default Select all View All

Enable: All All Action: All Owner: All More Reset Search Advanced

	Id		Signature name ↑	Action	Signature ope...	Protocol	Class type	References	Category	Enable PCAP	Owner
S	20020090		(MS00-021)Microsoft NT / Win...	Pass	Windows	tcp	denial-of-ser...	CVE: 2000-02...	misc	Disabled	© UserGate
S	20020052		(MS00-040)Microsoft					2000-03...	misc	Disabled	© UserGate
S	22000124		(MS00-092)Microsoft S					2000-10...	sql	Disabled	© UserGate
S	22000122		(MS00-092)Microsoft S					2000-10...	sql	Disabled	© UserGate
S	22000170		(MS02-038)Microsoft S					2008-01...	sql	Disabled	© UserGate

Signature settings

Enabled: Enable

Action: Block IP

Enable logging: Enable

PCAP file: Enable

Apply to: Both

Duration: 0 / days

Save Cancel

Действия: None, Pass, Drop, Reset, Block IP  
Логирование: Enable, Disable  
Запись PCAP: Enable, Disable  
Применить к: Src, Dst, Both (активно при Reset и Block IP)  
Продолжительность: days, hours, minutes





# GUI. IPS сигнатура. Создание

Шаг 1

Custom signatures properties

General UASL and settings

Enabled:

Id: Automatic

Name:

Description:

Signature threat: 1 very low

Class type: Select value

Category: Select value

Signature operating system:

Windows  Linux  Mac OS  
 BSD  Solaris X  
 Android  iOS  Cisco  
 Other

CVE: 2000-0001

BDU: 2020-01000

URL: https://example.com

Save Cancel

Шаг 2

Custom signatures properties

General UASL and settings

UASL

```
UASL(name='brute.force',.protocol=tcp,.pattern='USER',.flow=from_server,.rate=3,60;.track=src_ip)
```

Settings

Action: Block IP

Enable logging: Enable

PCAP file: Disable

Apply to: Both

Duration: 5 minutes

Verify signature Save Cancel



# GUI.UASL

Фильтр по IP-адресам:

— src/dst (IPaddr/IPsubnet)

Фильтр по TCP/UDP-портам:

— src/dst (equal, less than, greater than, in range)

Поиск паттернов (packet payload):

— pattern (string)

Модификаторы области поиска:

— icmp, tcp, udp etc

Частота срабатывания:

— rate (count, period); track (src/dst IP)

Направление анализа:

— from\_client, from\_server, bi\_directional

Протокольные диссекторы:

— tcp dissector, udp dissector, icmp dissector etc

Матчинг бинарных данных

— byte\_test, byte\_jump

Пример:

```
UASL(.name='Scan';  
.flow=from_client;  
.tcp.flags = S;  
.dst_port=1:1024;  
.rate=100,10; .track=src_ip;)
```



## GUI. SCADA

The screenshot displays the UserGate GUI interface for managing IPS signatures. The main window shows a list of signatures with columns for ID, Status, Signature name, Action, Signature operating system, Protocol, Class type, References, Category, Enable PCAP, and Owner. A filter properties dialog is open, showing a list of signatures matched by the filter: category = scada and classtype = protocol-command. The filter is enabled, and the list shows 365 filtered signatures out of a total of 13480.

Id	Status	Signature name	Action	Signature operating ...	Protocol	Class type	References	Category	Enable PCAP	Owner
1378	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2012-4704	scada	Disabled	UserGate
1379	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1396	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1412	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1323	Default settin...	7T Interactive Graphical SCADA System Fil...	Pass	Windows						
162	Default settin...	7T Interactive Graphical SCADA System M...	Pass	Windows						
163	Default settin...	7T Interactive Graphical SCADA System Re...	Pass	Windows						
1371	Default settin...	ABB MicroSCADA Wserver Command Exec...	Pass	Windows						
24060948	Default settin...	ABB MicroSCADA wserver.exe CreateProce...	Pass	BSD Linux MacOS Windows						
1438	Default settin...	Advantech Studio NTWebServer.exe Create...	Pass	Windows						
1333	Default settin...	Advantech WebAccess AspVCObj ActiveX ...	Pass	Windows						
1364	Default settin...	Advantech WebAccess BwRpswd.exe Stac...	Pass	Windows						
1425	Default settin...	Advantech WebAccess Client bswwfcfg St...	Pass	Windows						
1400	Default settin...	Advantech WebAccess Dashboard openWl...	Pass	Windows						
1401	Default settin...	Advantech WebAccess Dashboard remove...	Pass	Windows						
1399	Default settin...	Advantech WebAccess Dashboard remove...	Pass	Windows						
165	Default settin...	Advantech WebAccess Dashboard Viewer ...	Pass	Windows						
1403	Default settin...	Advantech WebAccess Datacore DCE/RPC...	Pass	Windows						
1402	Default settin...	Advantech WebAccess DCE/RPC webnrc...	Pass	Windows						
1417	Default settin...	Advantech WebAccess HMI and SCADA So...	Pass	Windows						

Filter's properties dialog: Enabled, category = scada and classtype = protocol-command. Signatures matched table shows 365 filtered signatures out of 13480 total.



## GUI. Сигнатуры L7

The screenshot displays the UserGate GUI interface. On the left, a table lists various applications with columns for Id, Type, Name, Application categories, and Application technology. The 'Custom application properties' dialog box is open on the right, showing the 'UASL' tab. The dialog includes fields for Type, Id, Name, Description, Signature threat, Technology, and Categories. The 'Signature threat' is set to 'very low'. The 'Categories' section contains several checkboxes for different application types.

Id	Type	Name	Application categories	Application technology
8163	Application	Obin	<input type="checkbox"/> Web posting	Browser-based
731	Application	11st	<input type="checkbox"/> Web browsing	Browser-based
894	Application	123rf.com	<input type="checkbox"/> Web browsing	Browser-based
5810	Application	123VPN	<input type="checkbox"/> Proxies and anonymizers	Client-server
9074	Application	1337x.to	<input type="checkbox"/> Web browsing	Browser-based
188	Application	1C	<input type="checkbox"/> Business	Client-server
7855	Application	1C-Connect	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
7856	Application	1C-Connect audio	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
7858	Application	1C-Connect chat	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
7859	Application	1C-Connect file transfer	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
7860	Application	1C-Connect proxy	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
7857	Application	1C-Connect remote access	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
9025	Application	1clickVPN	<input type="checkbox"/> Proxies and anonymizers	Browser-based
9845	Application	1F Mobile	<input type="checkbox"/> Instant messaging	Client-server
9041	Application	2ch.hk	<input type="checkbox"/> Social networking	Browser-based
7696	Application	2GIS	<input type="checkbox"/> Web browsing	Browser-based
532	Application	360.com	<input type="checkbox"/> Web browsing	Browser-based
9666	Application	3DNews	<input type="checkbox"/> Web posting	Browser-based
9040	Application	4chan	<input type="checkbox"/> Social networking	Browser-based
811	Application	4PDA	<input type="checkbox"/> Web browsing	Browser-based
254	Application	4Shared	<input type="checkbox"/> File storage and backup	Browser-based
34	Application	6fndtrn	<input type="checkbox"/> Tunneling	Network protocol

**Custom application properties**

General | **UASL**

Type: Application  
Id: Automatic  
Name:   
Description:   
Signature threat: very low  
Technology: Select value  
Categories:  
 Media streaming  Email  Coin Miners  
 Tunneling  Games  Remote access  
 Conferencing  Trojan Horses  Business  
 Mobile  Proxies and anonymizers  Standard networks  
 VOIP  Web posting  Software update  
 File storage and backup  Web browsing  File sharing P2P  
 Instant messaging  Social networking

Save Cancel



# GUI. Правила МЭ

Rule properties

General Source Users Destination Service Time HIP profiles Usage History

Enabled:

Name: Rule

Description:

Action: **Deny**

Application profile: Do not use application profile

IPS profile: Do not use IPS profile

Reject with: Not selected

Scenario: Do not use scenario

Logging: None

Enable logging limit:

Limit logging events to: 3 / hour

Maximum number of packets per event: 5

Apply rule to: Any packets

Place to: End of the list

Rule properties

General Source Users Destination Service Time HIP profiles Usage History

Enabled:

Name: Rule

Description:

Action: **Allow**

Application profile: Test app profile

IPS profile: Test IPS profile

Reject with: Not selected

Scenario: Do not use scenario

Logging: None

Enable logging limit:

Limit logging events to: 3 / hour

Maximum number of packets per event: 5

Apply rule to: Any packets

Place to: End of the list

Save Cancel



# UserID



# UserID. Задачи

Прозрачная идентификация  
пользователей

Синхронизация групп пользователей

Сегментация на базе принадлежности к группе LDAP или имени  
пользователя (Identity Based Network Firewall)



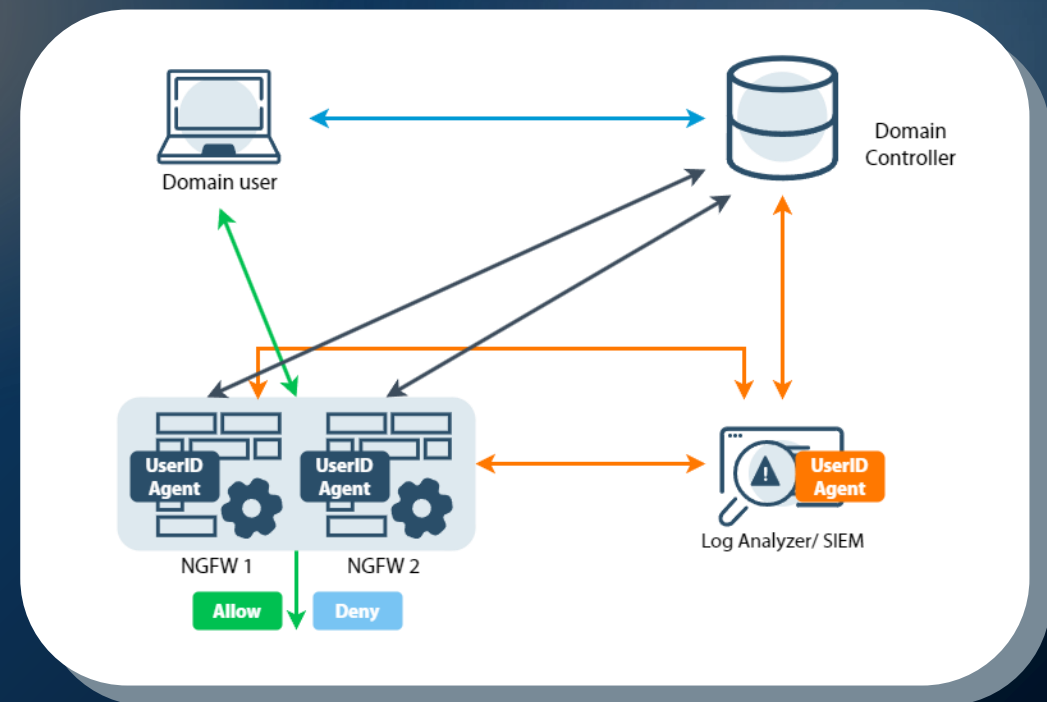
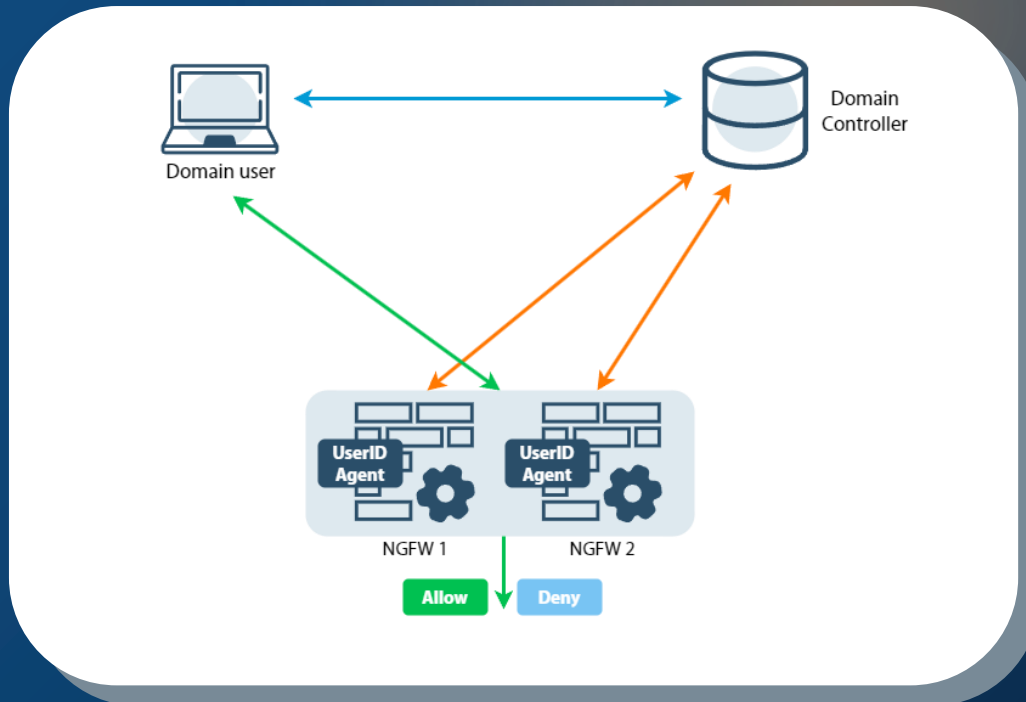
# UserID. Возможности

- Идентификация посредством использования журналов DC по WMI (коды событий 4624, 4634, 4768, 4769, 4770) и/или по Syslog (RFC 3164, RFC 5424, RFC 6587)
- Использование фильтров и таймеров в настройках агента
- Режимы работы:
  - a. Агент на борту NGFW
  - b. Агент на борту LogAn
  - c. Агенты на NGFW и LogAn
- Дистрибуция данных пользователей на NGFW



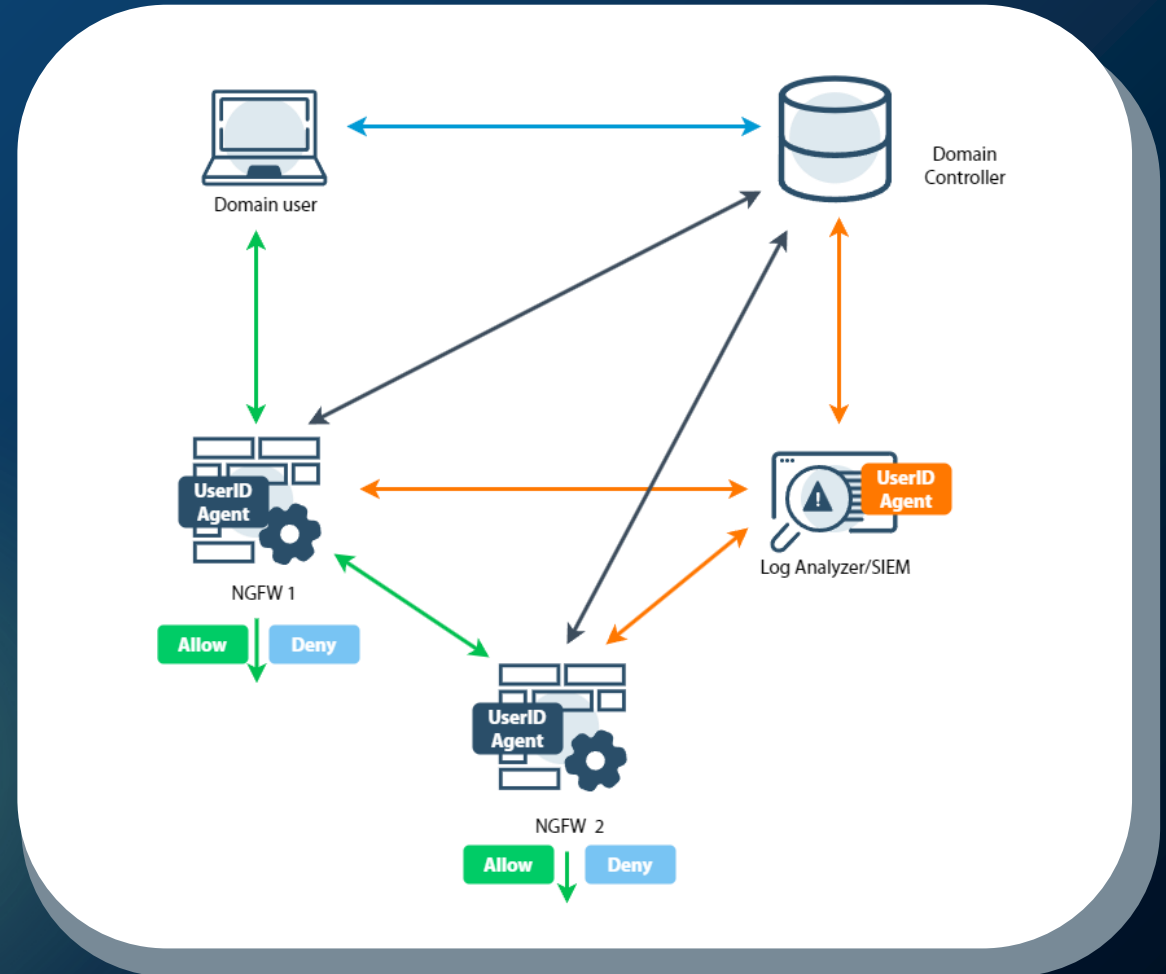


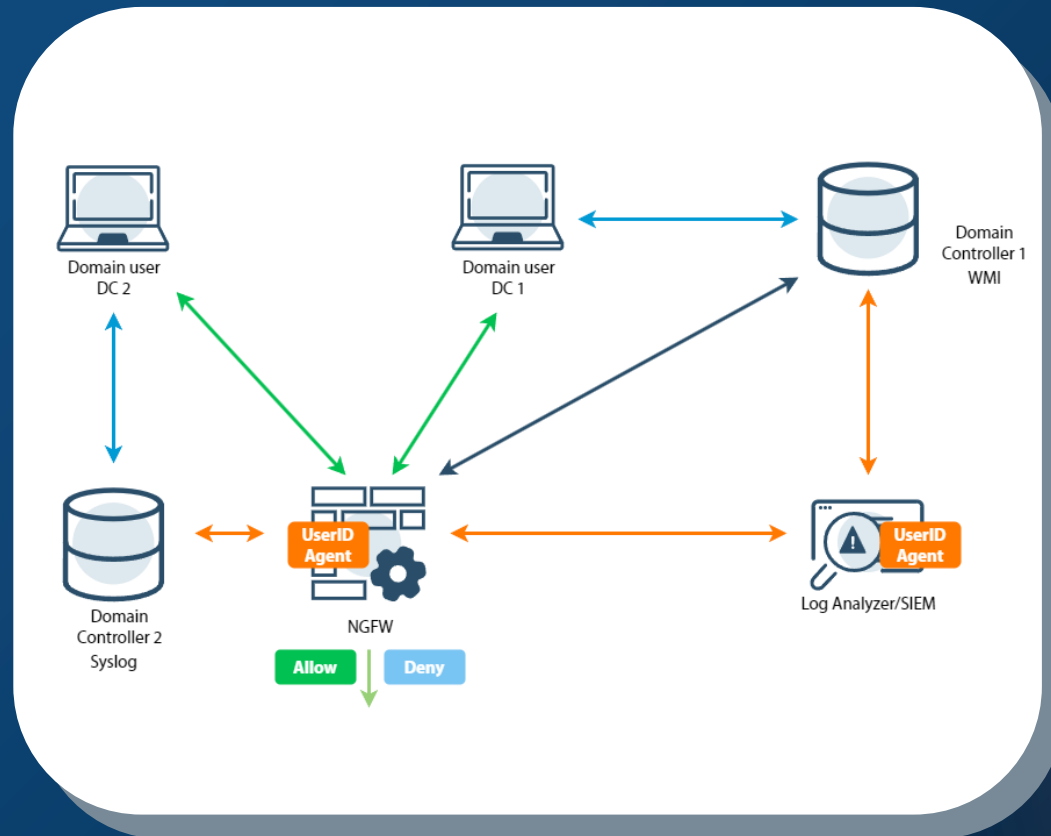
# Вариант исполнения: Cluster NGFW





## Вариант исполнения: NGFW + LogAn/ SIEM Дистрибуция





Вариант исполнения:  
NGFW + LogAn/SIEM  
с активными агентами



# GUI. Добавление агента

The screenshot displays the UserGate NGFW GUI interface. On the left, a sidebar menu is visible under the heading 'UserGate NGFW Dashboard'. The 'Users and devices' section is expanded, showing options like Groups, Users, Auth servers, Auth profiles, Captive portal, Captive profiles, Terminal servers, MFA profiles, and 'UserID agent' (which is highlighted with a star). Below this are Network policies, Security policies, Global portal, VPN, and Libraries.

Two configuration dialog boxes are shown in the foreground, connected to the sidebar by arrows:

- Microsoft Active Directory server properties:** This dialog has fields for 'Enabled' (checked), 'Name' (DC), 'Description', 'Address' (192.168.0.100), 'Protocol' (WMI), 'Name' (user), 'Password' (masked with dots), and 'Auth profile' (Example user auth profile). It includes 'Save' and 'Cancel' buttons at the bottom.
- Syslog sender properties:** This dialog has tabs for 'General' and 'Filters'. The 'General' tab is active, showing fields for 'Enabled' (checked), 'Name' (DC2), 'Description', 'Address' (192.168.0.200), 'Default domain' (domain.local), 'Timezone' (UTC), and 'Auth profile' (Example user auth profile). It also includes 'Save' and 'Cancel' buttons at the bottom.



# GUI. Конфигурирование агента



# Upstream Proxy



# GUI. Настройка. Лицензия и обновления

Product activation

Welcome to UserGate activation wizard! Please enter your pin code.

Pin code:

Use upstream proxy  
Configure

Back Next Cancel

Upstream proxy settings for licensing and updates

Enabled:

IP address:

Port:

Authentication:

Name:

Password:

Save Cancel



# GUI. Реконфигурация. Лицензия и обновления

- ▼ UserGate
  - ⚙️ General settings
  - 📱 Device management ★
  - 👤 Administrators
  - 📜 Certificates
  - 📄 User certificate profiles
  - ▶️ 🌐 Network
  - ▶️ 👤 Users and devices
  - ▶️ ↔️ Network policies
  - ▶️ 🛡️ Security policies
  - ▶️ 🌐 Global portal
  - ▶️ 🖥️ VPN
  - ▶️ 📚 Libraries

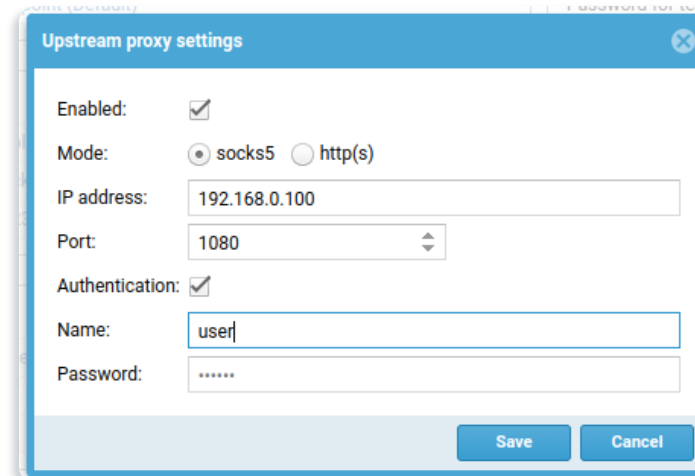
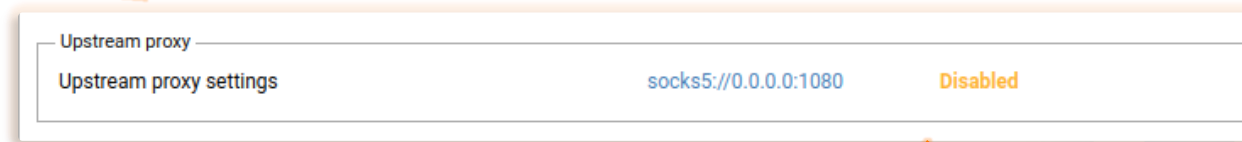
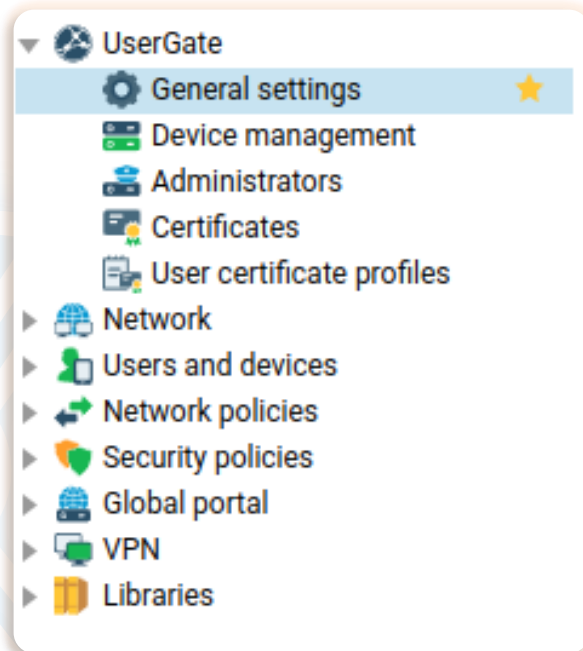
Server operations

Maintenance actions:	<a href="#">Reboot</a>   <a href="#">Shutdown</a>
Updates channel:	<a href="#">Stable</a>
Server updates:	<b>Updates are available!</b> <a href="#">Install now</a> <a href="#">View changelog</a>
Offline update:	<a href="#">Upload file</a>
Upstream proxy settings for licensing and updates:	<a href="#">Configure</a>



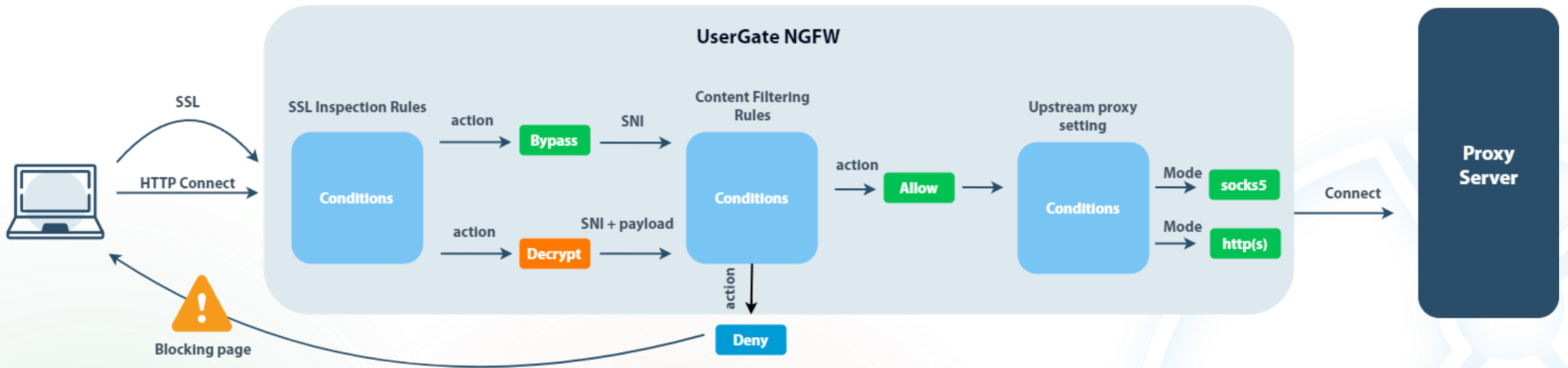


# GUI. Настройка. Пользовательский трафик





# Upstream Proxy flow





UserGate  
7.1

# UserGate Endpoint Client



# UserGate Client – агент SUMMA





# Режим NGFW

UserGate  
7.1

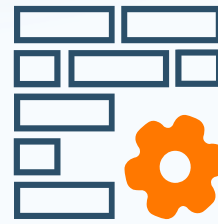
Внешние пользователи



VPN  
телеметрия



UserGate NGFW



Идентификация  
Политика доступа (Правила)  
Профили устройств HIP

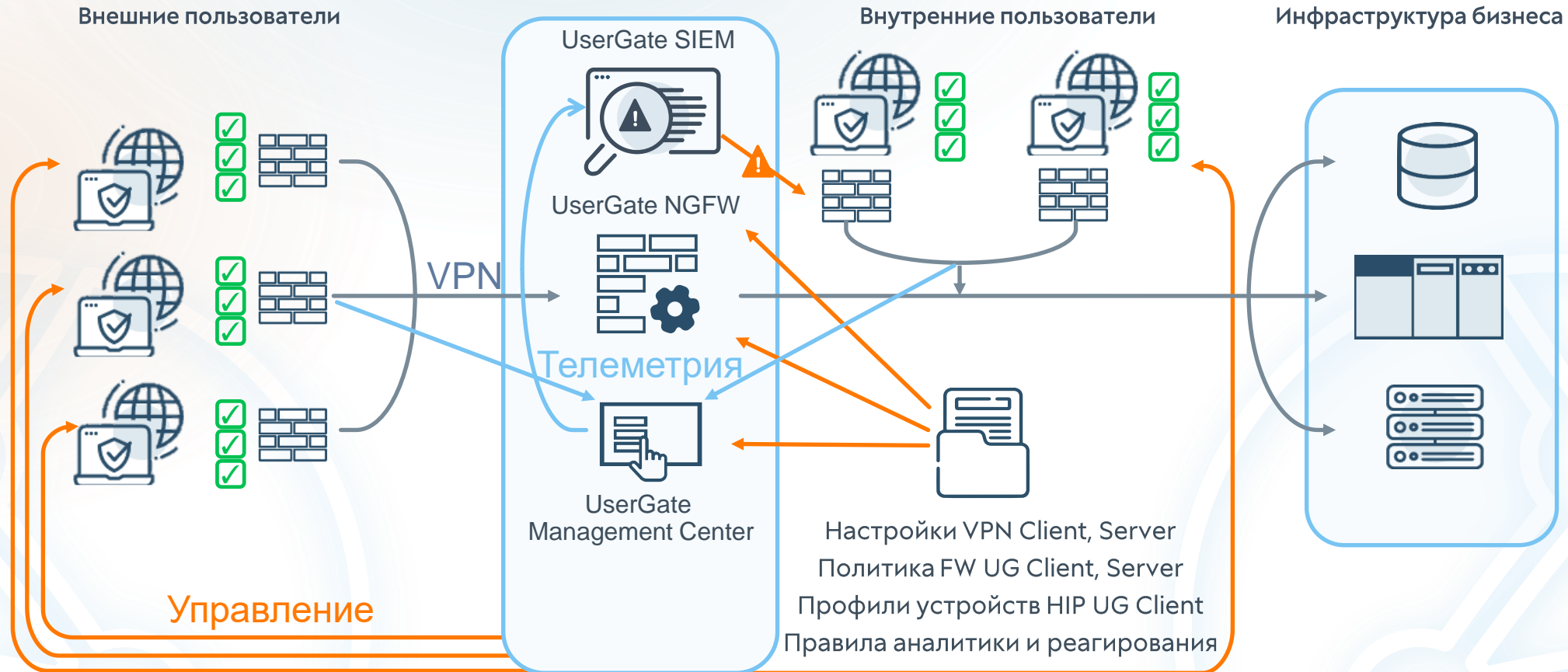
Инфраструктура бизнеса





# Режим МС

UserGate  
7.1





## VPN – процесс подключения

### NGFW-режим (автонастройка)

UserGate Endpoint Client 7. 1. 0. 621

"disconnected"

VPN server  
vpn.ug.local

Passphrase

Connect

UserGate Endpoint Client 7. 1. 0. 621

Select authorization type

Login and password  
 Certificate

Back Next

UserGate Endpoint Client 7. 1. 0. 621

Input credentials

Login  
user2@ug.local

Password  
.....

Back Next

UserGate Endpoint Client 7. 1. 0. 621

VPN connected

VPN server	192.168.0.1
VPN IP	172.30.250.2
Bytes in	0 KB
Bytes out	12 KB
Uptime	00:00:27

Disconnect

### MC-режим

UserGate MC

Выберите шаблон

Настройка VPN

Название: VPN-адрес: 10.10.5.33

Свойства VPN

Общие Файл 1 Файл 2

Включено:

Название: cert

Описание:

VPN-адрес: vpn.ug.local

Протокол: IKEV2 с сертификатом

Режимы: IPsec L2TP

UserGate Endpoint Client 7. 1. 0. 333

"disconnected"

VPN server

cert (vpn.ug.local)

cert (vpn.ug.local)

cert\_IP (10.10.5.33)

eap (vpn.ug.local)

eap\_IP (10.10.5.33)

Connect

UserGate Endpoint Client 7. 1. 0. 333

Confirm certificate selection

user2

QA

Back Next Change

UserGate Endpoint Client 7. 1. 0. 333

VPN connected

VPN server	192.168.0.1
VPN IP	172.30.250.2
Bytes in	0 KB
Bytes out	8 KB
Uptime	00:00:12

Disconnect



## VPN – Split tunneling

VPN network properties

General Network VPN routes UserGate Client routes

All routes

Include routes

+ Add Edit Delete

List name ↑	Owner
-------------	-------

Create and add new object

Exclude routes

+ Add Edit Delete

List name ↑	Owner
Google	you

Create and add new object

Restrict LAN access

Save Cancel

IPv4 таблица маршрута

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.3	281
0.0.0.0	0.0.0.0	172.30.250.1	172.30.250.2	1
8.8.8.8	255.255.255.255	192.168.0.1	192.168.0.3	281
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
169.254.1.100	255.255.255.252	On-link	169.254.1.101	281
169.254.1.100	255.255.255.252	172.30.250.1	172.30.250.2	1
169.254.1.101	255.255.255.255	On-link	169.254.1.101	281
169.254.1.103	255.255.255.255	On-link	169.254.1.101	281
169.254.1.103	255.255.255.255	172.30.250.1	172.30.250.2	1
172.30.250.0	255.255.255.0	On-link	172.30.250.2	257
172.30.250.2	255.255.255.255	On-link	172.30.250.2	257
172.30.250.255	255.255.255.255	On-link	172.30.250.2	257
192.168.0.0	255.255.255.0	On-link	192.168.0.3	281
192.168.0.0	255.255.255.0	172.30.250.1	172.30.250.2	1
192.168.0.3	255.255.255.255	On-link	192.168.0.3	281
192.168.0.255	255.255.255.255	On-link	192.168.0.3	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	172.30.250.2	257
224.0.0.0	240.0.0.0	On-link	192.168.0.3	281
224.0.0.0	240.0.0.0	On-link	169.254.1.101	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	172.30.250.2	257
255.255.255.255	255.255.255.255	On-link	192.168.0.3	281
255.255.255.255	255.255.255.255	On-link	169.254.1.101	281

Постоянные маршруты:

Сетевой адрес	Маска	Адрес шлюза	Метрика
0.0.0.0	0.0.0.0	192.168.0.1	По умолчанию





## НIP– сбор информации с устройства

- Состояние, производительность
- Безопасность
- USB-устройства
- Элементы автозагрузки
- Процессы
- Службы
- Ключи реестра
- Программное обеспечение
- Установленные обновления

Информация о конечном устройстве

Общие Производительность Безопасность USB устройства Элементы автозагрузки Процессы Службы Ключи реестра

Пользователи

Фотография	Пользоват...	Статус	Аккаунт	Имя поль...	Фамилия	Электронн...	Телефон
	user2@ug...	Локальный	Доменный	user2	ug.local	user2@ug...	111111

Информация о хосте

Netbios имя: PC10

Версия ОС: Майкрософт Windows 10 Корпоратив LTSC сборка 17763

Тип системы: x64-based PC

Версия UserGate Client: 7.1.0.333

IP-адрес: 10.10.5.33

Время загрузки системы: 24 октября 2023 г., 08:45 GMT+07:00

Время: 10 ноября 2023 г., 12:53 GMT+07:00

Статус: **Онлайн**

Последние данные получены: 10 ноября 2023 г., 08:53

Имя службы	Описание	Статус
AssignedAccessManagerSvc	Служба AssignedAccessManager	Остановлен
AudioEndpointBuilder	Средство построения конечных точек Windows Au...	Запущен
AudioSrv	Windows Audio	Запущен
AxInstSV	Установщик ActiveX (AxInstSV)	Остановлен
BFE	Служба базовой фильтрации	Запущен
BITS	Фоновая интеллектуальная служба передачи (BITS)	Остановлен
BrokerInfrastructure	Служба инфраструктуры фоновых задач	Запущен
BTAGService	Служба звукового шлюза Bluetooth	Остановлен
BthAvctpSvc	Служба AVCTP	Запущен
bthserv	Служба поддержки Bluetooth	Остановлен
camsvc	Служба диспетчера доступа к возможностям	Остановлен
CDPSvc	Служба платформы подключенных устройств	Запущен
CertProcSvc	Распространение сертификата	Запущен

Безопасность

Компонент	Статус
Межсетевой экран	Выключен
Автоматическое обновление	Включен
Антивирус	Выключен
Центр обеспечения безопасности Windo...	Выключен

Имя компонента	Имя производителя	Версия
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29...	Microsoft Corporat...	14.28.29913.0
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29...	Microsoft Corporat...	14.28.29913.0
Mozilla Firefox (x64 ru)	Mozilla	118.0.2
Mozilla Maintenance Service	Mozilla	117.0
UserGate Client	UserGate	7.1.0.333
VMware Tools	VMware, Inc.	11.3.5.18557794
WinRAR 6.11 (64-разрядная)	win.rar GmbH	6.11.0
Пакет драйверов Windows - UserGate kgdrv ActivityMonitor (0...	UserGate	06/08/2022 1.0.0.552



## HIP – настройка

В проверке установленных продуктов доступно:

- антивирус (более 500)
- межсетевой экран (более 250)
- резервное копирование (более 220)
- шифрование диска (более 100)
- DLP (более 25)
- управление обновлениями

The screenshot displays the HIP configuration interface with several panels for selecting security products:

- Выберите антивирус:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Нет), a dropdown for 'Базы антивируса обновлены' (Да), and a dropdown for 'Версия' (ANY).
- Выберите продукт межсетевого экрана:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Не проверять), and a dropdown for 'Версия' (ANY).
- Выберите продукт резервного копирования:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Не проверять), and a dropdown for 'Версия' (ANY).
- Выберите продукт шифрования дисков:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Не проверять), and a dropdown for 'Версия' (ANY).
- Выберите продукт DLP:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Не проверять), and a dropdown for 'Версия' (ANY).
- Выберите продукт управления обновлениями:** Includes checkboxes for 'Установлен' (checked) and 'Включено' (Не проверять), and a dropdown for 'Версия' (ANY).

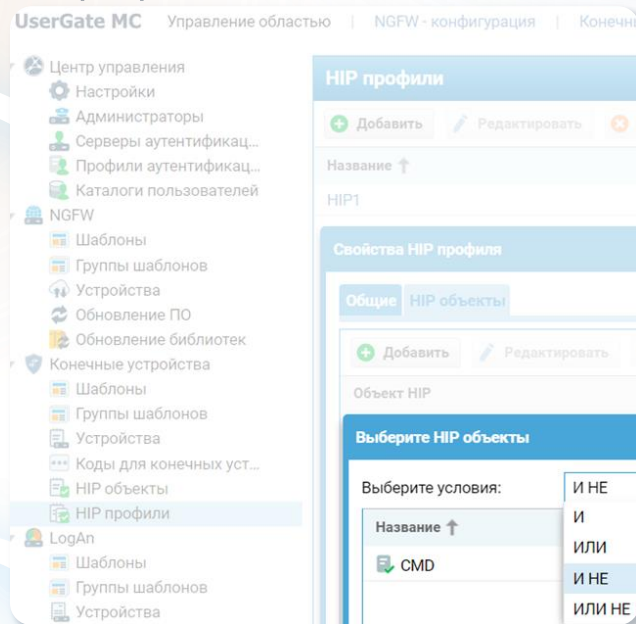
On the right, a 'Выберите продукт' panel shows a list of vendors and products:

- Вендор: Все вендоры
- Название продукта ↑
- Products listed: K7 Total Security, K7 Ultimate Security, K7 Virus Security ZERO, K7VirusSecurity Plus, KV Antivirus, Kapha Anti-Malware, Kaspersky Anti-Virus, Kaspersky Endpoint Security, Kaspersky Free, Kaspersky Internet Security.
- Page navigation: Страница 5 из 10

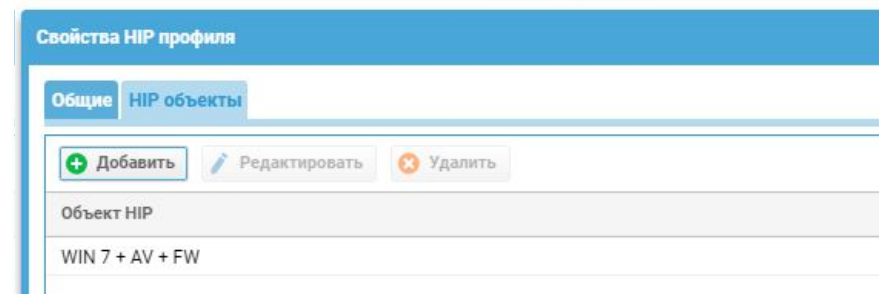
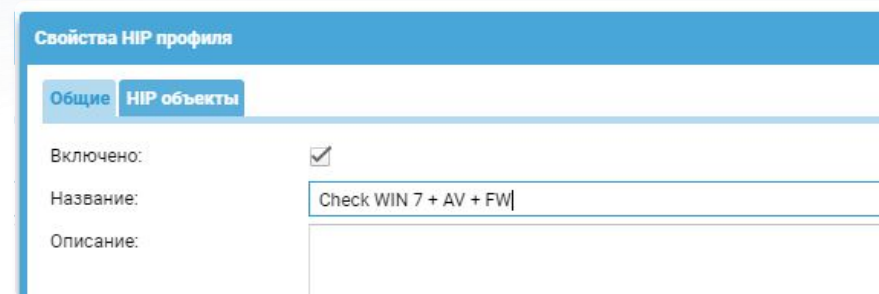


# НIP – настройка

В НIP-профиле агрегируем всю информацию по объектам



В одном НIP-профиле может быть несколько объектов НIP





## НIP – правила FW

UserGate MC Управление областью | NGFW - конфигурация | Конечные устройства - конфигурация | LogAn - конфигурация | Журналы и отчёты | ex\_admin | Py

Выберите шаблон: ер

- UserGate
  - Настройки
  - Настройка VPN
  - Политики сети
    - Межсетевой экран
  - Библиотеки
    - Сервисы
      - Группы сервисов
    - IP-адреса
      - Группы приложений
      - Профили прокси
      - Списки URL
      - Категории URL
      - Типы контента
      - Календари

### Межсетевой экран

Добавить | Редактировать | Удалить | Переместить | Копировать | Включить | Отключить | Скопировать ID правила | Все

#	Название	Действие	Область примен...	Пользователи	Адрес источника	Адрес назначения	Сервис	Приложения	Списки URL	Категории URL	Тип контента	Время	НIP профили
1	НIP	Запретить	Везде	Любой	Любой	Любой	Любой	Любое	Любой	Любая	Любой	Любое	НIP1
2	deny webmail	Запретить	Везде	Любой	Любой	Любой	http https	Любое	Любой	Веб-почта	Любой	Любое	Любой
3	Allow any	Разрешить	Снаружи перим...	Domain User...	Любой	Любой	Любой	<input type="checkbox"/> Chrome <input type="checkbox"/> CMD <input type="checkbox"/> FAR	Любой	Любая	Любой	Любое	Любой
4	Allow inside	Разрешить	Везде	Любой	Любой	Любой	Любой	Любое	Любой	Любая	Любой	Любое	Любой
5	Deny any	Запретить	Везде	Любой	Любой	Любой	Любой	Любое	Любой	Любая	Любой	Любое	Любой

Выберите шаблон: ер

- UserGate
  - Настройки
  - Настройка VPN
  - Политики сети
    - Межсетевой экран
  - Библиотеки
    - Сервисы
      - Группы сервисов
    - IP-адреса
      - Группы приложений

### Группы приложений

Добавить | Редактировать | Удалить

Группы приложений	Название	Версия
2	Chrome	2
2	CMD	3
2	FAR	2
1	test	1

### Приложения

Добавить | Редактировать | Удалить

Приложение	Хэш
Chrome v. 115.0.5790.110	BA2C5BB8A228C0BD739B043094597F614B4C01F0

### Свойства приложения

Название: Chrome v. 115.0.5790.110  
Хэш: BA2C5BB8A228C0BD739B043094597F614B4C01F0

Сохранить | Отмена



## HIP – нотификация

The screenshot displays the UserGate management console interface. On the left is a navigation menu with categories like 'Центр управления', 'NGFW', and 'Конечные устройства'. The main area shows the 'Устройства' (Devices) section with a table of endpoints. A table with 9 columns (Name, OS, Version, Last connection, Telemetry, Monitoring, Template groups, HIP profiles, Device) lists an 'Autogenerated endpoint'. Below the table, two 'Отчет несоответствия требованиям' (Compliance report) windows are shown. The first report is for 'HIP1' and lists 'CMD' as a non-compliant element. The second report is for 'CMD' and lists 'cmd.exe' as a prohibited object. A settings window for 'Оповещения' (Notifications) is also visible, showing options for displaying icons, tooltips, and messages for device quarantine. At the bottom right, a Windows taskbar shows a notification from 'UserGate Endpoint Client' stating 'UserGate Endpoint Agent Resource blocked'.

Название ↑	Версия ОС	Версия	Последнее подключение	Телеметрия	Мониторинг	Группы шаблонов	HIP профили	Устройство
✓ Autogenerated endpoi...	Майкрософт...	7.1.0.333	10 ноября 2023 г., 09:31	IP Address: 10.10.5.33 Netbios имя: PC10	Синхронизация конечного устройства завершилась успешно Информация о конечном у...	eps1	Не соответствует комплаенсу Посмотреть отчет	Log

**Отчет несоответствия требованиям**  
Дата: 10 ноября 2023 г., 09:34

Объект HIP	Несоответствующие элементы
HIP1	
CMD	Не соответствует комплаенсу Посмотреть отчет

**Отчет несоответствия требованиям**  
Дата: 10 ноября 2023 г., 09:35

Найдены следующие запрещенные объекты

Тип объекта	Несоответствующие элементы
Процесс	cmd.exe

**Оповещения**

Показывать иконку в трее	Да
Показывать тултипы оповещений	Да
Сообщение о добавлении устройства в карантин	Тип: всплывающее окно Сообщение: "Device added to quarantine"
Сообщение об удалении устройства из карантина	Тип: всплывающее окно Сообщение: "Device removed from quarantine"
Сообщение о блокировке ресурса	Тип: всплывающее окно Сообщение: "Resource blocked"

UserGate Endpoint Client  
UserGate Endpoint Agent  
Resource blocked



## Мониторинг событий

### Журнал событий:

В журнале событий конечных устройств отражены события, получаемые от конечных устройств, контролируемых с использованием программного обеспечения UserGate Client.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, важность, тип события и т.п.

Узел	Время	Коне...	Уровень лога	Данные
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:31:57	PC10	Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:31:57	PC10	Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	PC10	Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	PC10	Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	PC10	Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	PC10	Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	PC10	Аудит успеха	Выполнен выход учетной записи из системы. Субъект: ИД безопасности: S-1-5-21-144772055-15890
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	PC10	Сведения	Окончание транзакции установщика Windows: C:\Users\user2\Downloads\utlmauthclient_6.2.0.17.msi.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	PC10	Сведения	Product: UserGate Domain Authorization Agent – Installation completed successfully.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	PC10	Сведения	Установщик Windows выполнил установку продукта. Продукт: UserGate Domain Authorization Agent.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	PC10	Сведения	Завершение сеанса 0, запущенного 2023-10-03T06:27:27.083644900Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	PC10	Сведения	Запуск сеанса 0 - 2023-10-03T06:27:27.083644900Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	PC10	Аудит успеха	Новому сеансу входа назначены специальные привилегии. Субъект: ИД безопасности: S-1-5-21-144
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	PC10	Аудит успеха	Вход в учетную запись выполнен успешно. Субъект: ИД безопасности: S-1-5-18 Имя учетной записи
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	PC10	Аудит успеха	Выполнена попытка входа в систему с явным указанием учетных данных. Субъект: ИД безопаснос
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:16	PC10	Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:16	PC10	Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:15	PC10	Сведения	Начало транзакции установщика Windows: C:\Users\user2\Downloads\utlmauthclient_6.2.0.17.msi. ИД
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	PC10	Сведения	Окончание транзакции установщика Windows: {38BA81AB-5A22-4BC5-84C9-9DDCCABB2E13}. ИД кли
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	PC10	Сведения	Завершение сеанса 0, запущенного 2023-10-03T06:26:30.029325000Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	PC10	Сведения	Product: UserGate Domain Authorization Agent – Removal completed successfully.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	PC10	Сведения	Установщик Windows выполнил удаление продукта. Продукт: UserGate Domain Authorization Agent. B
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	PC10	Аудит успеха	Новому сеансу входа назначены специальные привилегии. Субъект: ИД безопасности: S-1-5-21-144
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	PC10	Аудит успеха	Вход в учетную запись выполнен успешно. Субъект: ИД безопасности: S-1-5-18 Имя учетной записи
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	PC10	Аудит успеха	Выполнена попытка входа в систему с явным указанием учетных данных. Субъект: ИД безопаснос



## Мониторинг событий

Узел	Время	Конечное устрой...	Правило	Приложение
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:07	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:07	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:07	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:02	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:02	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:02	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:02	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:32:02	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:31:48	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:31:48	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:55	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:55	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:55	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:06	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:01	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:30:01	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:56	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:56	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:56	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:56	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:56	PC10	NIP	PID 1092
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:08	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:29:08	PC10	NIP	PID 600
be63e2c2-0195-4573-989c-ad09b626f463	03 октября, 09:28:14	PC10	NIP	PID 600

## Журнал правил конечных устройств

отображает события срабатывания правил межсетевых экранов конечных устройств, в настройках которых включена функция **ЖУРНАЛИРОВАНИЕ**



## Мониторинг событий

Приложения конечных устройств:

отображает приложения, которые запускались на конечных устройствах

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

Журналы

- Журнал событий
- Журнал веб-доступа
- Журнал DNS
- Журнал трафика
- Журнал СОВ
- Журнал АСУ ТП
- Журнал инспектирован...
- История поиска
- Конечные устройства
  - Журнал событий
  - Журнал правил
  - Приложения
- Аппаратура
- Syslog
- Защита почтового траф...
- UserID
- Экспорт журналов
- Пользовательская нор...

Отчёты

- Шаблоны
- Пользовательские шаб...
- Правила отчётов
- Созданные отчёты

Отчёты инцидентов

- Шаблоны отчётов инци...
- Правила отчётов инцид...
- Созданные отчёты инци...

Журналы Log Analyzer

- Журнал событий

### Приложения

01 Авг 2023 г. 00:00 – 05 Окт 2023 г. 23:59 | Конечное устройство: Все | Действие: Все | Приложение: Все | Ещё | Сброс | Поиск | Расширенный | [Иконки]

Узел	Время	Конечное устройство	Хэш	Приложение	Версия	Субъект подписи	Подписано
be63e2c2...	03 октябр...	PC10	B8F00586870C42957EC5408B2C39CEEF9026F56A	consent.exe	6.2.17763.1697	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	5BE67DAD56E33CDBD1C327948EE70D43E69ED106	NOTEPAD.EXE	6.2.17763.1697		
be63e2c2...	03 октябр...	PC10	5BE67DAD56E33CDBD1C327948EE70D43E69ED106	NOTEPAD.EXE	6.2.17763.1697		
be63e2c2...	03 октябр...	PC10	4B8BF0359C6208468C9A55D9483E417729DB9C2C	utmclient.exe	6.2.0.17		
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	2FA92AF18B877319E660F8A152FAF386C33E2F3C	taskmgr.exe	6.2.17763.1697	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	B54CE57731B58A49800EFA31894DDF6AB6B6A4F4	MsiExec.exe	5.0.17763.404		





## Мониторинг событий

Аппаратура конечных устройств:

данный журнал содержит информацию об устройствах, подключаемых к конечным устройствам с установленным UserGate Client

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

Журналы

- Журнал событий
- Журнал веб-доступа
- Журнал DNS
- Журнал трафика
- Журнал СОВ
- Журнал АСУ ТП
- Журнал инспектирован...
- История поиска
- Конечные устройства
  - Журнал событий
  - Журнал правил
  - Приложения
  - Аппаратура**
- Syslog
- Защита почтового траф...
- UserID
- Экспорт журналов
- Пользовательская нор...

Отчёты

- Шаблоны
- Пользовательские шаб...
- Правила отчётов
- Созданные отчёты
- Отчёты инцидентов
- Шаблоны отчётов инци...
- Правила отчётов инцид...
- Созданные отчёты инц...

Журналы Log Analyzer

- Журнал событий

### Аппаратура

01 Авг 2023 г. 00:00 – 05 Окт 2023 г. 23:59 | Конечное устройство: Все | Действие: Все | Устройство: Все | Ещё | Сброс | Поиск | Расшир...

Узел	Время	□	Конечное устройство	+	Устройство	Идентификатор уст
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	☰	PC10	+	USB Root Hub	USB\ROOT_HUB\48
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	☰	PC10	+	USB Input Device	USB\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	☰	PC10	+	HID-compliant mouse	HID\VID_0627&PID
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	☰	PC11	+	USB Root Hub	USB\ROOT_HUB\48
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	☰	PC11	+	USB Input Device	USB\VID_0627&PID
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	☰	PC11	+	HID-compliant mouse	HID\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	☰	HOME-PC	+	USB Root Hub	USB\ROOT_HUB\48
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	☰	HOME-PC	+	USB Input Device	USB\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	☰	HOME-PC	+	HID-compliant mouse	HID\VID_0627&PID



## Аналитика

The screenshot displays the 'Rules of Analytics' (Правила аналитики) configuration page. A modal window titled 'Properties of the analytics rule' (Свойства правила аналитики) is open, showing the 'Conditions' (Условия) tab. The condition is defined as:

```
((logEventId = 5140) AND (data ~ &#39;\\*\ADMIN$&#39;)) OR ((logEventId = 5145) AND (data ~ &#39;\\*\ADMIN$&#39;) AND ((data ~ &#39;\pwsh.exe&#39;) OR (data ~ &#39;\powershell.exe&#39;) OR (data ~ &#39;\cmd.exe&#39;)))
```

The background shows a table of rules with columns: Name (Название), Priority (Приоритет), Category (Категория), Conditions (Условия), and Action (Действия). The 'SMB admin share accessed' rule is highlighted.

Below the modal, a list of rules is shown:

Группы аналитики	Правила аналитики
Название	Правила аналитики
Воздействие	Добавить в аналитику
Выполнение	Название
Закрепление	Описание
Исследование	SMB admin share accessed
Первоначальный доступ	Detects scenarios where an attacker attempts to connect to the administrative SMB share. References: <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.002%20-SMB%20Windows%20Admin%20Shares">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.002%20-SMB%20Windows%20Admin%20Shares</a> Tags:...
Перемещение внутри периметра	RDP hijacking via tscon
Повышение привилегий	An attempt to hijack RDP session with the Microsoft Windows 'tscon' utility is detected Tags: attack.lateral_movement
Получение учётных данных	Logon process then pass the hash
Предотвращение обнаружения	Detects logon process then pass the hash References: <a href="https://blog.netrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/#~:text=In%20particular%2C%20one%20common%20technique,move%20laterally%20within%20the">https://blog.netrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/#~:text=In%20particular%2C%20one%20common%20technique,move%20laterally%20within%20the</a> Tags:...
Разведка	Impacket DCOMexec privilege abuse via MMC
Сбор данных	Detects scenarios where an attacker execute the Impacket DCOMexec tool in order to abuse DCOM services. References: <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.003-Distributed%20Component%20Object%20Model%20(DCOM)">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.003-Distributed%20Component%20Object%20Model%20(DCOM)</a> <a href="https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/">https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/...</a>
Управление и контроль	Enabling RDP via Registry
Экранирование данных	Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of



## Реагирование

### Свойства действия реагирования

**Общие** Действие Шаблон

Включено:

Название:

Описание:

Действие:

- Послать команду на эндпойнт
- Отправить email
- Отправить сообщение
- Webhook
- Создать инцидент
- Послать команду на коннектор
- Послать команду на эндпойнт

Записывать в журнал правил:

Группировать похожие срабатывания:

Период группировки (мин.):

Количество срабатываний:

### Конечные устройства

Показать Все  10 секунд  Послать команду

Название ↑	Версия	Последнее подключение
✔ Autogenerated end...	7.1.0.333	10 ноября 2023 г., 10:24

### Команда к конечному устройству

Команда: Отключить от сети

Служба: Отключить от сети

ИД процесса: Разрешить передачу данных по сети

- Завершить процесс
- Запустить службу
- Остановить службу

### Свойства действия реагирования

**Общие** Действие Шаблон

Команда:

- Отключить от сети
- Завершить процесс



# SIEM



UGOS 6.X: Log Analyzer

UGOS 7.0: Log Analyzer + SIEM

UGOS 7.1: Log Analyzer или SIEM



## Изменения в UserGate SIEM

- » UserGate LogAnalyzer – продукт с базовой лицензией
- » UserGate SIEM – полноценная лицензируемая SIEM-система
- » UserGate SIEM Expert – подписка на обновляемые правила аналитики от вендора



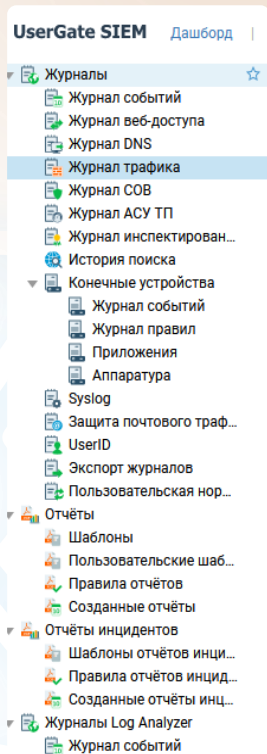
# UserGate LogAnalyzer 6.X

## ЖУРНАЛЫ:

- событий
- веб-доступа
- трафика
- COB
- АСУ ТП
- инспектирования SSH



# Журналы UserGate SIEM:



- Журналы UserGate NGFW
- APM Windows – UG Client
- Серверы Windows – протокол WMI
- Syslog-журналы
- Почтовый трафик
- UserID





# UserGate SIEM

## Основные функции:

- функционал LogAnalyzer 6.x
- Дополнительные источники журналов
- Правила аналитики
- Правила нормализации событий
- Экспертиза вендора в создании правил аналитики
- Автоматическая реакция на срабатывания правил аналитики
- Работа с инцидентами информационной безопасности



# UserGate SIEM: АНАЛИТИКА

Правила  
аналитики:  
настройки  
по любому  
полю журналов

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

Аналитика

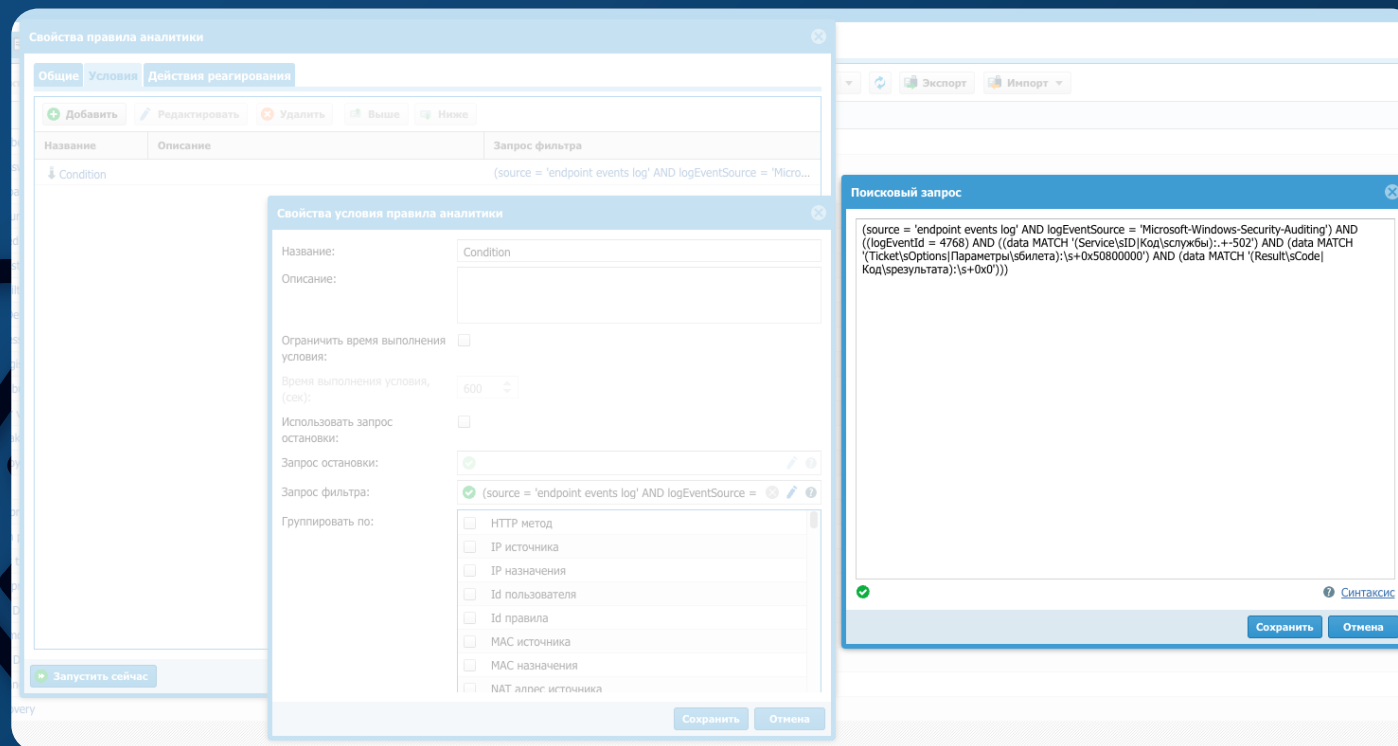
Правила аналитики | Поиск | Действия реагирования | Срабатывания | Подробности срабатывания | Процессы конечных устройств

+ Добавить | Редактировать | Копировать | Удалить | Включить | Отключить | Запустить сейчас | Показать срабатывания | Показать Все

	Название ↑	Приоритет	Действия реагирования	Условия	Категория срабатывания
5	rule Block EndPoint (IDPS and not Russia)	Критический	Block network (endpoint)	Signature ID Not Russian Federation	Security
3	rule block ip (user test and site anekdot.ru)	Низкий	Block Network (NGFW)	User test Anekdot.ru	Security
2	rule create incident (ipSource 10.55.65.1)	Нормальный	Create incident	ipSource 10.55.65.1	Security
1	rule send e-mail (url mail.ru)	Низкий	send email	Url mail.ru	Performance
3	rule send SMS (natIpSource 10.10.10.1)	Нормальный	Send message	natIpSource 10.10.10.1	Availability
4	rule send webhook (computer ivanov.test.local)	Нормальный	Send Webhook	computerName ivanov.test.local	Security



# UserGate SIEM: АНАЛИТИКА



Условия срабатывания: произвольная логика запросов



## UserGate SIEM: АНАЛИТИКА

Правила аналитики:  
база правил  
аналитики  
по подписке

Правила аналитики		Правила аналитики	
<b>Группы аналитики</b>		<b>Правила аналитики</b>	
Название		Добавить в аналитику	
● Взадействие		Название	
● Выполнение		Persistence via TelemetryController Scheduled Task Hijack	
● Закрытие		Detects the successful hijack of Microsoft Compatibility Appraiser scheduled task to establish persistence with an integrity level of system.	
● Исследование		References: <a href="https://attack.mitre.org/techniques/T1953/">https://attack.mitre.org/techniques/T1953/</a> ...	
● Персональный доступ		Potential Persistence via Time Provider Modification	
● Передача внутри периметра		Identifies modification of the Time Provider. Adversaries may establish persistence by registering and enabling a malicious DLL as a time provider. Windows uses the time provider architecture to obtain accurate time stamps from other network devices or clients in the network. Time providers are implemented in the form of a DLL file which resides in the System32 folder. The service W32Time initiates during the startup of Windows and loads w32time.dll.	
● Повышение привилегий		Creation or Modification of a new GPO Scheduled Task or Service	
● Получение учебных данных		Detects the creation or modification of a new Group Policy based scheduled task or service. These methods are used for legitimate system administration, but can also be abused by an attacker with domain admin permissions to execute a malicious payload remotely on all or a subset of the domain joined machines.	
● Подтверждение обнаружения		Computer account created with privileges	
● Разведка		Detects scenarios where an attacker creates a computer account with privileges for later exploitation.	
● Сбор данных		Tags: attack_persistence attack_t1099 ...	
● Управление и контроль		New member added to an Exchange administration group (medium risk)	
● Эксплуатация данных		Detects scenarios where a new member is added to a sensitive group related to Exchange server	
		Reference: <a href="https://msrc.microsoft.com/details/CVE-2016-3016">https://msrc.microsoft.com/details/CVE-2016-3016</a> <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1098.xxx-Account%20manipulation...">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1098.xxx-Account%20manipulation...</a>	
		High risk Active Directory group membership change	
		Detects scenarios where a suspicious group membership is changed.	
		References: <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1098.xxx-Account%20manipulation">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1098.xxx-Account%20manipulation</a> <a href="https://i666.com/ty/syntax-groups.html">https://i666.com/ty/syntax-groups.html</a>	
		DSRM password changed (log via command)	
		Detects scenarios where an attacker reset or synchronize with another domain account the DSRM (Directory Services Restore Mode) password in order to escalate privileges.	
		References: <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0006-Credential%20Access/T1003-Credential%20dumping">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0006-Credential%20Access/T1003-Credential%20dumping</a> <a href="https://idsecrity.org/?p=1714">https://idsecrity.org/?p=1714</a> ...	
		Scheduled task was created	
		Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The "code-schtasks-<code> can be run directly on the command line, or the Task Scheduler can be.	
		Persistence via BITS Job Notify Cmdline	
		An adversary can use the Background Intelligent Transfer Service (BITS) SetNotifyCmdLine method to execute a program that runs after a job finishes transferring data or after a job enters a specified state in order to persist on a system.	
		Persistence via WMI Event Subscription	
		An adversary can use Windows Management Instrumentation (WMI) to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.	
		Exchange transport agent injection via configuration file	
		Detects scenarios where an attacker attempts to load an artifact in the Exchange transport agent.	
		References: <a href="https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1505-Server%20Software%20Component">https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0003-Persistence/T1505-Server%20Software%20Component</a> <a href="https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook...">https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook...</a>	
		Webserver IIS configuration edited (SYSMON)	
		Detects scenarios where an attacker attempts to edit IIS configuration file in order to load a module.	
		Tags: attack_persistence attack_t1505.004	
		Component Object Model Hijacking	
		Identifies Component Object Model (COM) hijacking via registry modification. Adversaries may establish persistence by executing malicious content triggered by hijacked references to COM objects.	
		References: <a href="https://pentestlab.blog/tag/ingreserver32/">https://pentestlab.blog/tag/ingreserver32/</a> ...	
		Image File Execution Options Injection	
		Image File Execution Options is a Windows registry key which enables developers to attach a debugger to an application and to enable "stepping" for application debugging. This behavior of Windows opens the door for persistence since an arbitrary executable can be used as a debugger of a specific process or as a "MonitorProcess".	
		Add autorun task	
		Detects suspicious command line reg.exe tool adding key to RUN key in Registry	
		Tags: attack_persistence attack_t1547.003	
		Suspicious ImagePath Service Creation	
		Identifies the creation of a suspicious ImagePath value. This could be an indication of an adversary attempting to stealthily persist or escalate privileges through abnormal service creation.	
		Tags: attack_persistence ...	
		Suspicious change default file association	
		Identifies hijack a file extension and make it execute a malicious application before the actual file is opened.	
		References: <a href="https://www.rid.team/offensive-security/persistence/hijacking-default-file-extension">https://www.rid.team/offensive-security/persistence/hijacking-default-file-extension</a> <a href="https://attack.mitre.org/techniques/T1544/">https://attack.mitre.org/techniques/T1544/</a> ...	



# UserGate SIEM: АНАЛИТИКА

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 | Показать Все

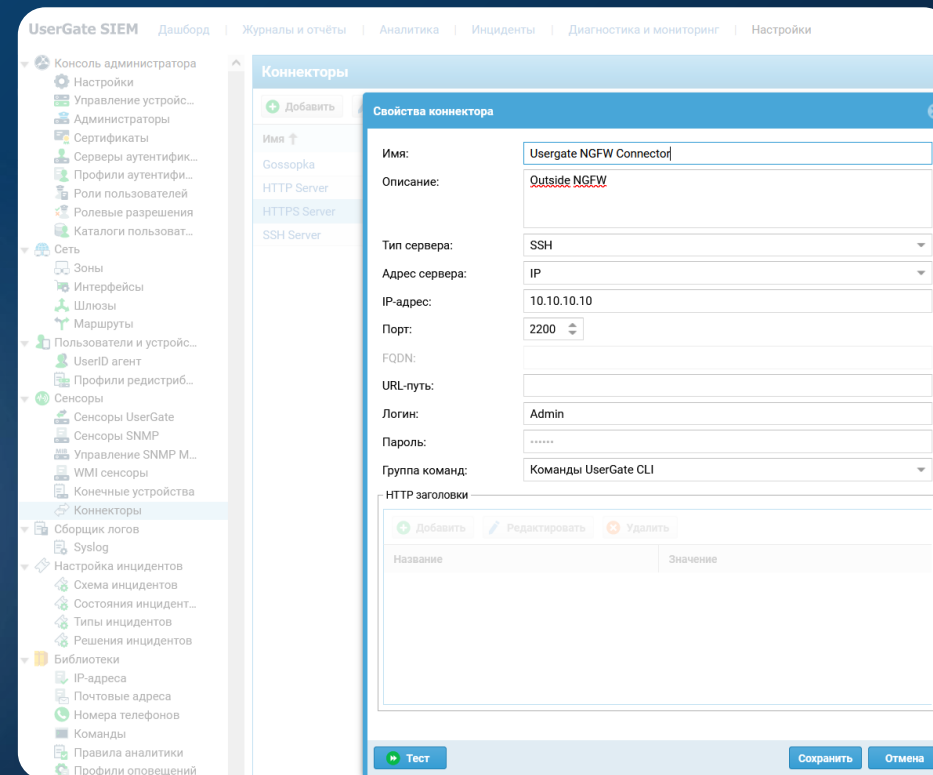
Название ↑	Действие	Описание
Block network (endpoint)	Послать команду на эндпойнт	
Block Network (NGFW)	Послать команду на коннектор	
Create firewall rule (NGFW)	Послать команду на коннектор	
Create incident	Создать инцидент	
Kill Process (Endpoint)	Послать команду на эндпойнт	
send email	Отправить email	
Send SMS message	Отправить сообщение	
Send Webhook	Webhook	
Stop process (Linux)	Послать команду на коннектор	

Действия  
реагирования:  
информирование  
инженеров  
и команды  
управляемым  
устройствам



# UserGate SIEM: КОННЕКТОРЫ

Поддержка устройств по протоколам SSH, HTTP, HTTPS





## UserGate SIEM: АНАЛИТИКА

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

Аналитика

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

08 Ноеб 2023 г. | Идентификатор срабатывания: Все | Правила: Все | Приоритет: Все | Ещё | Сброс | Поиск | Расширенный

Узел	Время	Идентификатор	Время первого со...	Время последнего с...	Колличеств...	П...	Категория сраба...	Приоритет	Пользова...	Сигнатуры COB	Конечное устройсто/...	Имя комп...
loganalyzer...	18:32:52	SEC-8731	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8730	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8729	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8728	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8727	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8726	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8725	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8724	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8723	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8722	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8721	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8720	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8719	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8718	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8717	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8716	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8715	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8714	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8713	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8712	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8711	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8710	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет
loganalyzer...	18:32:52	SEC-8709	18:24:52	18:24:52	1	1	Security	Нормальный	Unknown	Нет	Нет	Нет

« | < | Страница 1906 из 2255 | > | » | ↻

Срабатывания  
правил аналитики:  
ничто не останется  
вне внимания



## UserGate SIEM: АНАЛИТИКА

Процессы конечных устройств: полная информация

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: A1385CE20AD79F55DF235EFFF9780C31442AA234  
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





# UserGate SIEM: ИНЦИДЕНТЫ

Журнал инцидентов: информация обо всех инцидентах

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

Инциденты | Создать инцидент

02bc1-ca44-47d7-918f-f5e6296c0498 OR statusid = ddafd388-549a-416c-9fdd-a6a83ef85eaa OR statusid = 52bc84fb-0b23-4885-a82e-c745970c6a8f ))) AND ruleid = 'a21a7d9a-c5c1-4d4a-bcf0-3b02a3d1c659'

Создан	Изменён	Индекс	Имя инцидента	Правило	Статус	Решение	Тип инцидента	Приоритет инци...	Инициатор	Последнее изме...	Ответственный	Активность
25 октября, 14:50:17	25 октября, 14:51:33	INC-7	test1	test	Opened	Не завершён	Incident	Критический	Unknown	Administrator (...)	Administrator	Комментарии: 1 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-6	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-5	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-4	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-3	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-2	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-1	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0
25 октября, 14:50:17	25 октября, 14:50:17	INC-0	test1	test	Opened	Не завершён	Incident	Критический	Unknown	System	Administrator	Комментарии: 0 Срабатывания... Журналы: 0



UserGate  
7.1

# UserGate SIEM: **ЗАЧЕМ?**



# UserGate SIEM: ИНЦИДЕНТЫ

The screenshot displays the UserGate SIEM interface for incident management. The main header shows the incident title "[INC-7] test1" and a toolbar with actions like "Редактировать", "Комментировать", "Назначить", and "Рабочий процесс". Below this, there are sections for "Журналы (1)", "Улики (2)", and "Активность (1)".

**Журналы (1)**

Узел	Конечное устройство/...	Идентификат...	Хэш	Действие	Информация	Пользователь	Источник
62a02cav-48...	MSEDEGEWIN10	7720	F1ADA921FB6D2A7C...	Журналиро...		SYSTEM	Приложени...

**Улики (2)**

Тип ул...	Значение	Тип атаки	TLP	Инд...	Сервисы	Обнов...
Хэш	3345434ferv435t43444tqbrdzds95f6gb...	Другое	AMBER	Нет	-	01 янв...
Автон...	65556	Угон трафика	RED	Нет	-	01 янв...

**Активность (1)**

Комментарии История

Administrator (Admin) добавил комментарий - 25 октября, 14:51:33 (Изменён: 19:51:36)  
Подозрение на взлом прокси сервера squid.

Работа  
с инцидентом:  
одновременная  
работа  
с инцидентом  
множества  
участников



# UserGate SIEM: ЗАЧЕМ?

- Анализ и реагирование
- Рекомендации UserGate: применять UserGate SIEM при наличии 5-ти и более сетевых устройств



## UserGate SIEM: ИНЦИДЕНТЫ События ИТ

Журнал событий

21 Июнь 2023 г. Конечное устройство/сенсор: Все Файл журнала лога: Все Уровень лога: Все Источник журнала событий: Все Ещё Сброс

Узел	Время	Конечное устр...	Уровень...	Данные	Источни...	Кате...	Категория инц...	Имя компьютера	Пользовате...	Код ...	Иде...	Тип ...	Файл журнала ...
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-1664 Account Name: Health...	Microsoft...	12545	Logoff	exchange.pentes...	HealthMailbo...	4242	4634	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Log...	Microsoft...	12544	Logon	exchange.pentes...	HealthMailbo...	4241	4624	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domai...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4240	4648	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-1656 Account Name: Health...	Microsoft...	12545	Logoff	exchange.pentes...	HealthMailbo...	4239	4634	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domain: PENTE...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4238	4624	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domai...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4237	4648	4	Security
3d5d3c...	21 июня...	WINDOWS-10-O...	Ауди...	Учетные данные диспетчера учетных данных прочитаны. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетно...	Microsoft...	13824	User Account Ma...	Windows-10-off...		59030	5379	4	Security
3d5d3c...	21 июня...	WINDOWS-10-O...	Ауди...	Учетные данные диспетчера учетных данных прочитаны. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетно...	Microsoft...	13824	User Account Ma...	Windows-10-off...		59029	5379	4	Security
3d5d3c...	21 июня...	WINDOWS-10-O...	Ауди...	Учетные данные диспетчера учетных данных прочитаны. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетно...	Microsoft...	13824	User Account Ma...	Windows-10-off...		59028	5379	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-1656 Account Name: Health...	Microsoft...	12545	Logoff	exchange.pentes...	HealthMailbo...	4236	4634	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domain: PENTE...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4235	4624	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domai...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4234	4648	4	Security
1c9f30...	21 июня...	EXCHANGE	Audit...	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: EXCHANGES Account Domai...	Microsoft...	12544	Logon	exchange.pentes...	EXCHANGE	4233	4648	4	Security
3d5d3c...	21 июня...	WINDOWS-10-O...	Свед...	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2023-06-21 23:...	Microsoft...	11	File created (rule...	Windows-10-off...	NT AUTHORI...	54098	11	3	Microsoft-Windo...
3d5d3c...	21 июня...	WINDOWS-10-O...	Свед...	Process terminated: RuleName: - UtcTime: 2023-06-21 23:59:53.037 ProcessGuid: {289a599c-8ef0-6493-9fb2-000000002b0...	Microsoft...	5	Process terminat...	Windows-10-off...	NT AUTHORI...	54097	5	3	Microsoft-Windo...
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14428	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14429	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14430	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14431	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14432	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was logged off. Subject: Security ID: S-1-5-21-2282938710-1989567394-2605000726-500 Account Name: Admin...	Microsoft...	12545	Logoff	AD.pentest.net	Administrator	14433	4634	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Log...	Microsoft...	12544	Logon	AD.pentest.net	Administrator	14427	4624	4	Security
44f6b3...	21 июня...	AD	Audit...	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION...	Microsoft...	14336	Credential Validat...	AD.pentest.net		14426	4776	4	Security
44f6b3...	21 июня...	AD	Audit...	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Log...	Microsoft...	12544	Logon	AD.pentest.net	Administrator	14425	4624	4	Security
44f6b3...	21 июня...	AD	Audit...	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION...	Microsoft...	14336	Credential Validat...	AD.pentest.net		14424	4776	4	Security



## UserGate SIEM: ИНЦИДЕНТЫ События ИТ

### Журнал событий

Узел	Время	Конечное устройство/сенсор	Уровень	Диагн.
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
3d543c...	21 июня...	WINDOWS-10-O...	Учет...	Учет
3d543c...	21 июня...	WINDOWS-10-O...	Учет...	Учет
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
1c9f30...	21 июня...	EXCHANGE	Audit...	An 2
3d543c...	21 июня...	WINDOWS-10-O...	Смел...	Proc
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	The
44f6b3...	21 июня...	AD	Audit...	An 2
44f6b3...	21 июня...	AD	Audit...	The

### Аппаратура

Узел	Время	Конечное устройство	Устройство
a62f3c96-e0c7-4...	05 апреля, 03:37:56	USERWIN	VMware USI
a62f3c96-e0c7-4...	05 апреля, 03:37:56	USERWIN	HID-compli
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	USB Root H
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	Generic USE
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	USB Compo
c5118051-db1b-...	27 февраля, 15:55:46	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	Generic USE
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	USB Root H
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	USB Compo
c5118051-db1b-...	27 февраля, 15:45:43	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	HID-compli
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	USB Compo
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	USB Input E
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	USB Root H
c5118051-db1b-...	27 февраля, 15:35:41	EXCHANGE	Generic USE
c5118051-db1b-...	27 февраля, 15:25:40	EXCHANGE	Generic USE
c5118051-db1b-...	27 февраля, 15:25:40	EXCHANGE	USB Root H

### Приложения

Узел	Время	Конечное устройство	Хэш	Приложение	Версия	Субъект по...	Подписано	Идентифик...	Пользов...	Командная ...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			3976	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			5100	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			6284	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			6552	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			4740	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			836	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	6D9D0BE989C8383C06B279A71...	taskhostw.exe	6.2.14393.32...	Microsoft Wi...	Microsoft Wi...	4800	SYSTEM	taskhostw.ex...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			3024	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			2480	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			4740	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			380	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			5876	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			1520	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			6460	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			6448	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			2980	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			1196	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			80	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			1668	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			1504	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			3208	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			6136	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			5516	SYSTEM	"rellog.exe" "...
75365105-...	30 апреля,...	EXCHANGE	00667A0F0C0D5E9DA697E9FF5...	Conhost.exe	6.2.14393.0			3144	SYSTEM	{??C:\Windo...
75365105-...	30 апреля,...	EXCHANGE	AFCFF85A1610F4569C3442FAA...	rellog.exe	6.2.14393.0			5592	SYSTEM	"rellog.exe" "...



## UserGate SIEM: ЗАЧЕМ

Мы позволяем:

- » сократить время реакции на событие ИБ
- » расследовать инцидент
- » выполнить автоматическую реакцию на инцидент



# UserGate SIEM: ЗАЧЕМ

Мы позволяем:

**не допустить  
последствий инцидента:**

- утечка данных;
- потеря доступа к данным;
- остановка процессов  
и многое-многое другое





# Регистрация на конференцию

Оффлайн



Онлайн



7.1

Спасибо за внимание!

**Игорь Шефер**  
Ведущий инженер UserGate