



ПРОГРАММНЫЙ КОМПЛЕКС  
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ  
«НОВЫЕ ТЕХНОЛОГИИ»  
Версия: 2.1.58

**Спецификация генерируемых сообщений в формате SEF**

**Листов 49**

## СОДЕРЖАНИЕ

1 CEF сообщения.....	3
1.1 Класс событий Web Service.....	3
SKDPUNT.WS.00001.....	4
SKDPUNT.WS.00002.....	5
SKDPUNT.WS.00003.....	8
SKDPUNT.WS.00004.....	8
SKDPUNT.WS.00005.....	15
SKDPUNT.WS.00006.....	16
SKDPUNT.WS.00007.....	33
SKDPUNT.WS.00008.....	33
SKDPUNT.WS.00009.....	34
1.2 Класс событий Authentication.....	34
SKDPUNT.AUTH.00002.....	35
SKDPUNT.AUTH.00003.....	35
SKDPUNT.AUTH.00004.....	36
SKDPUNT.AUTH.00005.....	36
1.3 Класс событий Report.....	37
SKDPUNT.REPORT.00001.....	37
SKDPUNT.REPORT.00002.....	38
SKDPUNT.REPORT.00003.....	38
1.4 Класс событий Session Control.....	39
SKDPUNT.SC.00001.....	40
SKDPUNT.SC.00002.....	40
SKDPUNT.SC.00003.....	40
SKDPUNT.SC.00004.....	40
SKDPUNT.SC.00005.....	41
1.5 Класс событий Incident.....	41
SKDPUNT.INCIDENT.00001.....	42
SKDPUNT.INCIDENT.00002.....	47
Перечень сокращений.....	48
История изменений.....	49


## 1 CEF СООБЩЕНИЯ

### Структура сообщения в формате CEF

Сообщение в формате CEF состоит из заголовка и тела сообщения.

В заголовке сообщения содержится версия формата CEF и общая информация о событии:

```
DATE HOST CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension
```

Имя поля	Описание
<i>DATE</i>	Дата и время события
<i>HOST</i>	Имя сервера СКДПУ НТ
<i>Version</i>	Версия формата CEF
<i>Device Vendor</i>	Производитель ( <i>IT-Bastion LLC</i> )
<i>Device Product</i>	Название программы ( <i>SKDPU-NT</i> )
<i>Device Version</i>	Версия программы
<i>Signature ID</i>	Уникальный идентификатор события
<i>Name</i>	Имя события
<i>Severity</i>	Важность (критичность) события     Возможные значения от 0 до 10
<i>Extension</i>	Тело сообщения представляет собой последовательность пар <i>ключ=значение</i> , которая определяется типом события

Подробнее по ссылке <https://github.com/kamushadenes/cefevent>

Тело сообщения, в зависимости от класса рассматриваемого события, может содержать различные пары *ключ=значение*

#### 1.1 Класс событий Web Service



##### Общее описание

СКДПУ НТ генерирует записи о следующих событиях рассматриваемого класса:

- успешная попытка авторизации пользователя СКДПУ НТ (*SKDPUNT.WS.00001*);
- неудачная попытка авторизации пользователя СКДПУ НТ (*SKDPUNT.WS.00002*);
- окончание сессии доступа к СКДПУ НТ (*SKDPUNT.WS.00003*);
- изменение настроек детекторов аномалий (*SKDPUNT.WS.00004*);

- управление сервисами СКДПУ НТ (**SKDPUNT.WS.00005**);
- управление ограничениями доступа к данным (**SKDPUNT.WS.00006**);
- управление настройками СКДПУ НТ (**SKDPUNT.WS.00006**);
- управление парольной политикой СКДПУ НТ (**SKDPUNT.WS.00006**);
- нарушение целостности данных пользовательских сессий целевых систем (**SKDPUNT.WS.00007**);
- нарушение целостности исполняемых модулей СКДПУ НТ (**SKDPUNT.WS.00008**);
- недостаток свободного места в хранилище (**SKDPUNT.WS.00009**).

Тело сообщения рассматриваемого класса событий содержит следующие пары *ключ=значение*

Ключ	Описание
<i>act</i>	Регистрируемое действие
<i>cat</i>	Категория действия
<i>dst</i>	URL, доменное имя или IP-адрес сервера СКДПУ НТ   Указывается в поле <b>IP-адрес хоста</b> в разделе <b>Настройки &gt; Основные настройки</b>
<i>dvchost</i>	URL, доменное имя или IP-адрес сервера СКДПУ НТ   Указывается в поле <b>Имя хоста</b> в разделе <b>Настройки &gt; Основные настройки</b>
<i>end</i>	Дата и время окончания сессии доступа к СКДПУ НТ
<i>rt</i>	Дата и время регистрации события
<i>src</i>	IP-адрес, с которого пользователь СКДПУ НТ осуществляет доступ к СКДПУ НТ
<i>start</i>	Дата и время начала сессии доступа к СКДПУ НТ
<i>suser</i>	Учетная запись пользователя СКДПУ НТ, который совершает рассматриваемое действие
<i>msg</i>	Дополнительная информация о совершаемом действии

## SKDPUNT.WS.00001

### Успешная авторизация пользователя через веб-интерфейс

```
Feb 20 13:09:52 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00001|LoginSuccessful|1|act>LoginSuccessful cat=WS.Auth
dst=https://skdpu-nt-cert.domain.local dvchost=https://skdpu-nt-
cert.domain.local rt=2022-02-20 13:09:52.510522 src=172.16.30.63
start=2022-02-20 13:09:52.510884 suser=admin
```

## SKDPUNT.WS.00002

Пользователь может не авторизоваться через веб-интерфейс СКДПУ НТ по следующим причинам:

- Авторизация завершилась с ошибкой
- Неизвестное имя пользователя
- Неправильный пароль
- Ассоциированная с пользователем роль не найдена
- Превышено допустимое количество попыток авторизации
- Срок действия учетной записи пользователя истек
- Срок действия пароля учетной записи пользователя истек
- Автоматическое блокирование учетной записи пользователя
- Попытка доступа к заблокированной учетной записи пользователя
- Идентификатор пользователя не найден
- Доменный пользователь не авторизовался
- Учетная запись доменного пользователя не найдена
- Роли, ассоциированные с доменным пользователем, не найдены
- Домен не найден

### Авторизация завершилась с ошибкой

Генерируется при неудачной попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя СКДПУ НТ.

```
Feb 20 13:08:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|LoginFailure|6|act>LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local dvchost=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:08:49.501324 src=172.16.30.63 suser=admin
```

### Неизвестное имя пользователя

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя СКДПУ НТ, которая отсутствует в базе данных.

```
Feb 21 00:22:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UnknownUserName|6|act>LoginFailure cat=WS.Auth dst=10.100.1.181 rt=2022-02-21 00:22:49.712196 src=172.16.30.63 suser=dfsfg
```

## Неправильный пароль

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ с неправильно введенным паролем.

```
Feb 20 13:08:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|InvalidPassword|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:08:49.168082 src=172.16.30.63 suser=admin
```

## Превышено допустимое количество попыток авторизации

Генерируется в момент превышения максимального количества неудачных попыток авторизации при попытке авторизоваться в веб-интерфейсе СКДПУ НТ.

```
Feb 20 13:25:34 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserLoginAttemptsExhausted|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:25:34.725603 src=172.16.30.63 suser=user
```

## Срок действия учетной записи пользователя истек

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ, используя учетную запись пользователя СКДПУ НТ с истекшим сроком действия.

```
Feb 20 13:34:33 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserAccountExpired|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:34:33.404097 src=172.16.30.63 suser=user
```

## Срок действия пароля учетной записи пользователя истек

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ, используя учетную запись пользователя СКДПУ НТ, с истекшим сроком действия пароля.

```
Feb 20 13:37:01 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserPasswordExpired|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:37:01.816555 src=172.16.30.63 suser=user
```

## Автоматическое блокирование учетной записи пользователя

Генерируется в момент блокирования учетной записи пользователя по следующим причинам:

- превышение допустимого количества попыток авторизации;
- попытка авторизации по истечении срока действия учетной записи пользователя;
- попытка авторизации по истечении срока действия пароля учетной записи пользователя.

```
Feb 20 13:25:34 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserAccountLock|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:25:34.725603 src=172.16.30.63 suser=user
```

## Попытка доступа к заблокированной учетной записи пользователя

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ, используя заблокированную ранее учетную запись пользователя СКДПУ НТ.

```
Feb 20 13:26:46 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|BlockedUserAccountAccess|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:26:46.399444 src=172.16.30.63 suser=user
```

## Ассоциированная с пользователем роль не найдена

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ по причине отсутствия привязки учетной записи пользователя СКДПУ НТ к роли СКДПУ НТ.

```
Feb 20 13:08:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|LoginFailure|6|act=UserRoleNotFound cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:08:49.168082 src=172.16.30.63 suser=user
```

## Идентификатор пользователя не найден

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ по причине отсутствия идентификатора пользователя СКДПУ НТ в базе данных.

```
Jun 1 11:07:00 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|LoginFailure|6|act=UserIdNotFound cat=WS.Auth dst=https://skdpu-nt-26.domain.local dvchost=https://skdpu-nt-26.domain.local rt=2022-06-01 11:07:00.203880 src=172.16.30.63 suser=leonid
```

## Доменный пользователь не авторизовался

Генерируется при неудачной попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя домена LDAP.

```
Feb 20 13:08:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserNotAuthenticated|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:08:49.501324 src=172.16.30.63 suser=domain.local\Администратор
```

## Учетная запись доменного пользователя не найдена

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя домена LDAP, информация о которой отсутствует в домене LDAP.

```
Jun 1 11:07:00 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00002|UserAccountNotFound|6|act=LoginFailure cat=WS.Auth dst=https://skdpu-nt-26.domain.local dvchost=https://skdpu-nt-26.domain.local rt=2022-06-01 11:07:00.203880 src=172.16.30.63 suser=leonid
```

## Роли, ассоциированные с доменным пользователем, не найдены

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя домена LDAP, для которой отсутствуют ассоциированные с ней роли.

```
Apr 16 18:58:40 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00002|UserRolesNotFound|6|act=LoginFailure cat=WS.Auth
dst=https://skdpu-nt-cert.domain.local rt=2022-04-16 18:58:40.998224
src=172.16.30.63 suser=domain.local\Администратор
```

## Домен не найден

Генерируется при попытке авторизоваться в веб-интерфейсе СКДПУ НТ с помощью учетной записи пользователя домена LDAP, при этом информация о домене LDAP отсутствует.

```
Feb 20 13:08:49 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00002|Domain not found|6|act=LoginFailure cat=WS.Auth
dst=https://skdpu-nt-cert.domain.local rt=2022-02-20 13:08:49.501324
src=172.16.30.63 suser=domain.local\Администратор
```

## SKDPUNT.WS.00003

## Успешное окончание сессии доступа к СКДПУ НТ

Генерируется при успешном окончании сессии доступа пользователя СКДПУ НТ.

```
Feb 20 13:08:23 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00003|Logout|1|act=Logout cat=WS.Auth dst=https://skdpu-
nt-cert.domain.local end=2022-02-20 13:08:23.678013 rt=2022-02-20
13:08:23.678013 src=172.16.30.63 suser=admin
```

## SKDPUNT.WS.00004

При изменении настроек детекторов аномалий поле *msg* будет содержать перечень изменяющихся свойств детектора и имеет следующий формат:

```
root.<detector_name>.<feature>: <old_value> \=> <new_value>
```

**<detector\_name>**

имя детектора аномалий

Имя детектора	Наименование детектора
<i>color_list_match</i>	Детектирование потенциально опасных команд
<i>kill_pattern_event</i>	Детектирование принудительного блокирования сессий
<i>time_frame</i>	Контроль привычного времени работы
<i>trust_level</i>	Контроль изменения уровня доверия
<i>commands_resemblance</i>	Контроль стандартных команд

Имя детектора	Наименование детектора
<i>source_address</i>	Контроль привычных сетевых адресов
<i>activity_level</i>	Индикаторы взрывной активности
<i>new_access</i>	Детектор новых доступов
<i>permission_denied</i>	Детектор проблем с правами доступа к файлам
<i>remote_jump</i>	Детектор туннелей и прыжков
<i>direct_login</i>	Детектор входов помимо бастиона
<i>authentication_failure</i>	Анализатор ошибок авторизации
<i>forgotten_person</i>	Детектор забытых персон
<i>file_transfer</i>	Количество переданных файлов
<i>no_login</i>	Детектор сканеров

**<feature>**

изменяемое свойство детектора аномалий

Свойство	Описание	Формат
<i>active</i>	Состояние детектора	True False
<i>agents</i>	Перечень имен сервисов удаленного доступа	List[str]  Пример:  ['ssh', 'mstsc', 'vnc', 'scp']
<i>cases</i>	Пороговые значения количества дней, при достижении которых происходит генерирование инцидента с соответствующим уровнем критичности	List[Dict{'severity': severity, 'days': int, 'factor': decimal}, Dict{'severity': severity, 'days': int, 'factor': decimal}, Dict{'severity': severity, 'days': int, 'factor': decimal}]  Пример:  [{'severity': 'LOW', 'days': 91, 'factor': 1.0}, {'severity': 'MEDIUM', 'days': 182, 'factor': 1.0}, {'severity': 'HIGH', 'days': 365, 'factor': 1.0}]
<i>factor</i>	Весовой коэффициент инцидента	Число с плавающей точкой  Пример: 10.1

Свойство	Описание	Формат
<i>high_loads</i>	Количество переданных файлов для закрепления высокого уровня нагрузки	Целое число Пример: 10
<i>history_depth</i>	Количество дней, использующихся при анализе	Целое число Пример: 10
<i>ignoretime</i>	Количество дней, в течение которых учет статистики данных не ведется	Целое число Пример: 10
<i>include_localhost</i>	Необходимость учитывать прямые и обратные подключения к целевому устройству по адресам localhost, 127.0.0.1, 127.1	True False

Свойство	Описание	Формат
<i>interval</i>	Ширина временного окна	Целое число Пример: 10
<i>levels</i>	Пороговые значения уровней доверия, при достижении которых происходит генерирование инцидента с соответствующим уровнем критичности	<pre>List[   Dict{'severity': 'LOW',     'level': int,     'factor': decimal},   Dict{'severity': 'MEDIUM',     'level': int,     'factor': decimal},   Dict{'severity': 'HIGH',     'level': int,     'factor': decimal},   Dict{'severity': 'CRITICAL',     'level': int,     'factor': decimal} ]</pre> <p>Пример:</p> <pre>[{'severity': 'LOW', 'level': 450,   'factor': 1}, {'severity': 'MEDIUM',   'level': 300, 'factor': 1},   {'severity': 'HIGH', 'level':   200, 'factor': 1}, {'severity':   'CRITICAL', 'level': 1, 'factor': 1}]</pre>
<i>lists</i>	Перечень списков потенциально опасных команд	<pre>List[   Dict{'patterns': List[str],     'name': str,     'factor': decimal},   Dict{'patterns': List[str],     'name': str,     'factor': decimal} ]</pre> <p>Пример:</p> <pre>[{'patterns': ['^rm -r1'],   'name': 'black', 'factor': 2.0},   {'patterns': ['ls /etc.*'], 'name':   'gray', 'factor': 0.2}]</pre>
<i>low_loads</i>	Количество переданных файлов для закрепления низкого уровня нагрузки	Целое число Пример: 10
<i>medium_loads</i>	Количество переданных файлов для закрепления среднего уровня нагрузки	Целое число Пример: 10
<i>params</i>	Параметры, использующиеся при ручной настройке	<pre>List[int, int, int, int]</pre> <p>Пример:</p> <pre>[10, 50, 40, 0]</pre>

Свойство	Описание	Формат
<i>percentage</i>	Максимальный процент отличия	Целое число Пример: 1
<i>period</i>	Количество дней, в течение которых фиксируется активность персон	Целое число Пример: 10
<i>severity</i>	Уровень критичности инцидента	LOW MEDIUM HIGH CRITICAL
<i>truncated</i>	Режим учета пользовательских сессий целевых систем	True False
<i>tuned</i>	Режим контроля потока команд	AUTO MANUAL

**<old\_value>**

старое значение свойства детектора аномалий

**<new\_value>**

новое значение свойства детектора аномалий

### Детектирование потенциально опасных команд

```
Apr 27 10:05:44 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.color_list_match.active: True \=>
False root.color_list_match.severity: MEDIUM \=> HIGH,
root.color_list_match_lists: [{'patterns': ['^rm -r1', '*.crypt.*',
'*.hyena.*', '*.mimikatz.*', '*.mimilove.', '*/etc/passwd', '*/etc/
shadow', '*.fstab.*', '*.wget.*-O-.*sh', '*.curl.*sh', '*.shred.*', '*.dd.*
dev.*', '*.mkfs.*', '*.mv.*dev/null', '*.airbase-ng.*', '*.airdecap-ng.*',
'*.airdecloak-ng.*', '*.airreplay-ng.*', '*.airodump-ng.*', '*.airolib-
ng.*', '*.airserv-ng.*', '*.airtun-ng.*', '*.airventriloquist-ng.*',
'*.besside-ng.*', '*.buddy-ng.*', '*.easside-ng.*', '*.ivstools.*',
'*.packetforge-ng.*', '*.triptun-ng.*', '*.wesside-ng.*', '*.wpaclean.*',
'*.Ghidra.*', '*.ghidraSvr.*', '*.nmap.*', '*.wireshark.*', '*.nikto.*',
'*.sqlmap.*', '*.sqlninja.*', '*.wapiti.*', '*.maltego.*', '*.reaver.*',
'*.ettercap.*', '*.setoolkit.*', '*.seproxy.*', '*.seautomate.*',
'*.grendel.*', '*.enCase.*', '*.Autopsy.*', '*.UnicornsCan.*',
'*.ngrep.*', '*.argus.*', '*.ida pro.*', '*.windbg.*', '*.gdb.*',
'*.dumpsec.*', '*.ollydbg.*', '*.johny.*', '*.ophcrack.*', '*.hashcat.*',
'*.msfconsole.*', '*.msfvenom.*', '*.msfpayload.*', '*.msfcli.*',
'*.msfgui.*', '*.msfweb.*', '*.msfencode.*', '*.shell_bind_*',
'*.shell_reverse_*', '*.metsvc.*', '*.meterpreter.*', '*.searchsploit.*',
'*.exploitdb.*', '*.shellfire.*', '*.Burp.*', '*.armitage.*'], 'name':
'black1', 'factor': 2.01}, {'patterns': ['ls /etc.*1', '*.passwd.*',
'*.Delete.*', '*.conf.t.*', '*.alter.table.*', '*.Server.*Management.*',
'*.reboot.*', '*.Restart.*', '*.KMS.*', '*.monero.*', '*.itcoin.*',
'*.terium.*', '*.xmr-stak.*', '*.xmrig.*', '*.miner.*', '*.setfacl.*',
'*.chattr.*', '*.mkfs.*', '*.mimi.*', '*.ps1.*', '*.xls.*', '*.pdf.*',
```

```

'.*.docx.*', '*.chmod.*777', '*.corkscrew.*', '*.polipo.*', '*.tor-.*',
'.*i2p.*', '*.torrent.*'], 'name': 'gray1', 'factor': 0.21}] \=>
[{'patterns': ['^rm -r', '*.crypt.*', '*.hyena.*', '*.mimikatz.*',
'.*mimilove.*', '*/etc/passwd', '*/etc/shadow', '*.fstab.*', '*.wget.*-
O-*.sh', '*.curl.*sh', '*.shred.*', '*.dd.*dev.*', '*.mkfs.*', '*.mv.*dev/
null', '*.airbase-ng.*', '*.airdecap-ng.*', '*.airdecloak-ng.*',
'.*airreplay-ng.*', '*.airodump-ng.*', '*.airolib-ng.*', '*.airserv-
ng.*', '*.airtun-ng.*', '*.airventriloquist-ng.*', '*.besside-ng.*',
'.*buddy-ng.*', '*.easside-ng.*', '*.ivstools.*', '*.packetforge-ng.*',
'.*triptun-ng.*', '*.wesside-ng.*', '*.wpaclean.*', '*.Ghidra.*',
'.*ghidraSvr.*', '*.nmap.*', '*.wireshark.*', '*.nikto.*', '*.sqlmap.*',
'.*sqlninja.*', '*.wapiti.*', '*.maltego.*', '*.reaver.*', '*.ettercap.*',
'.*setoolkit.*', '*.seproxy.*', '*.seautomate.*', '*.grendel.*',
'.*enCase.*', '*.Autopsy.*', '*.UnicornsCan.*', '*.ngrep.*', '*.argus.*',
'.*ida pro.*', '*.windbg.*', '*.gdb.*', '*.dumpsec.*', '*.ollydbg.*',
'.*johny.*', '*.ophcrack.*', '*.hashcat.*', '*.msfconsole.*',
'.*msfvenom.*', '*.msfpayload.*', '*.msfcli.*', '*.msfgui.*', '*.msfweb.*',
'.*msfencode.*', '*.shell_bind.*', '*.shell_reverse.*', '*.metsvc.*',
'.*meterpreter.*', '*.searchsploit.*', '*.exploitdb.*', '*.shellfire.*',
'.*Burp.*', '*.armitage.*'], 'name': 'black', 'factor': 2.0}, {'patterns':
['ls /etc.*', '*.passwd.*', '*.Delete.*', '*.conf.t.*', '*.alter.table.*',
'.*Server.*Management.*', '*.reboot.*', '*.Restart.*', '*.KMS.*',
'.*monero.*', '*.itcoin.*', '*.tereum.*', '*.xmr-stak.*', '*.xmrig.*',
'.*miner.*', '*.setfacl.*', '*.chattr.*', '*.mkfs.*', '*.mimi.*',
'.*.ps1.*', '*.xls.*', '*.pdf.*', '*.docx.*', '*.chmod.*777',
'.*corkscrew.*', '*.polipo.*', '*.tor-.*', '*.i2p.*', '*.torrent.*'],
'name': 'gray', 'factor': 0.2}] rt=2023-04-27 10:05:44.807282
src=172.16.30.63 suser=admin

```

## Детектирование принудительного блокирования сессий

```

Apr 27 10:05:58 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.kill_pattern_event.active: True \=> False
root.kill_pattern_event.factor: 1.5 \=> 1.51 rt=2023-04-27 10:05:58.237722
src=172.16.30.63 suser=admin

```

## Контроль привычного времени работы

```

Apr 27 10:06:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU NT
msg=root.time_frame.active: True \=> False root.time_frame.ignoretime: 60
\=> 61, root.time_frame.factor: 1.0 \=> 1.01, root.time_frame.interval: 60
\=> 61 rt=2023-04-27 10:06:53.005273 src=172.16.30.63 suser=admin

```

## Контроль изменения уровня доверия

```

Apr 27 10:20:17 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU
NT msg=root.trust_level.active: True \=> False root.trust_level.levels:
[{'severity': 'LOW', 'level': 450, 'factor': 1}, {'severity': 'MEDIUM',
'level': 300, 'factor': 1}, {'severity': 'HIGH', 'level': 200, 'factor':
1}, {'severity': 'CRITICAL', 'level': 1, 'factor': 1}] \=> [{'severity':
'MEDIUM', 'level': 451, 'factor': 1.1}, {'severity': 'LOW', 'level':
301, 'factor': 1.1}, {'severity': 'MEDIUM', 'level': 200, 'factor':
1.1}, {'severity': 'HIGH', 'level': 1, 'factor': 1.1}] rt=2023-04-27
10:20:17.940949 src=172.16.30.63 suser=admin

```

## Контроль стандартных команд

```
Apr 27 10:11:15 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.commands_resemblance.active: True
\=> False root.commands_resemblance.params: [10, 50, 40,
0] \=> [11, 51, 41, 1], root.commands_resemblance.tuned:
AUTO \=> MANUAL, root.commands_resemblance.truncated: False
\=> True, root.commands_resemblance.percentage: 50 \=> 51,
root.commands_resemblance.history_depth: 30 \=> 301 rt=2023-04-27
10:11:15.660210 src=172.16.30.63 suser=admin
```

## Контроль привычных сетевых адресов

```
Apr 27 10:16:42 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.source_address.active: True \=> False
root.source_address.ignoretime: 7 \=> 6 rt=2023-04-27 10:16:42.175022
src=172.16.30.63 suser=admin
```

## Индикаторы взрывной активности

```
Apr 27 10:17:27 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU NT
msg=root.activity_level.active: True \=> False root.activity_level.period:
32 \=> 321 rt=2023-04-27 10:17:27.459475 src=172.16.30.63 suser=admin
```

## Детектор новых доступов

```
Apr 27 10:06:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU NT
msg=root.new_access.active: True \=> False root.new_access.ignoretime: 7
\=> 8, root.new_access.factor: 1.0 \=> 1.01 rt=2023-04-27 10:06:53.005273
src=172.16.30.63 suser=admin
```

## Детектор проблем с правами доступа к файлам

```
Apr 27 22:26:08 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.permission_denied.severity: LOW \=> MEDIUM,
root.permission_denied.factor: 0.2 \=> 0.21 rt=2023-04-27 22:26:08.895228
src=192.168.20.124 suser=admin
```

## Детектор туннелей и прыжков

```
Apr 27 10:21:35 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU
NT msg=root.remote_jump.active: True \=> False root.remote_jump.agents:
['ssh', 'mstsc', 'vnc', 'rdesktop', 'scp'] \=> ['ssh', 'mstsc', 'vnc',
'rdesktop', 'scp1'], root.remote_jump.include_localhost: False \=> True
rt=2023-04-27 10:21:35.578511 src=172.16.30.63 suser=admin
```

## Детектор входов помимо бастиона

```
Apr 27 22:27:42 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU NT
```

```
msg=root.direct_login.severity: HIGH \=> MEDIUM, root.direct_login.factor:
1 \=> 1.01, root.direct_login.active: True \=> False rt=2023-04-27
22:27:42.708755 src=192.168.20.124 suser=admin
```

## Анализатор ошибок авторизации

```
Apr 27 22:29:30 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.authentication_failure.severity: LOW
\=> MEDIUM, root.authentication_failure.factor: 1 \=> 1.01,
root.authentication_failure.active: True \=> False rt=2023-04-27
22:29:30.161502 src=192.168.20.124 suser=admin
```

## Детектор забытых персон

```
Apr 27 10:23:33 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy
dst=SKDPU NT msg=root.forgotten_person.active: True \=> False
root.forgotten_person.cases: [{'severity': 'LOW', 'days': 91, 'factor':
1.0}, {'severity': 'MEDIUM', 'days': 182, 'factor': 1.0}, {'severity':
'HIGH', 'days': 365, 'factor': 1.0}] \=> [{'severity': 'LOW', 'days':
911, 'factor': 1.01}, {'severity': 'MEDIUM', 'days': 1821, 'factor':
1.01}, {'severity': 'HIGH', 'days': 3651, 'factor': 1.01}] rt=2023-04-27
10:23:33.603685 src=172.16.30.63 suser=admin
```

## Количество переданных файлов

```
Apr 27 10:24:27 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-
NT|2.1.58|SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange
cat=WS.Policy dst=SKDPU NT msg=root.file_transfer.active:
True \=> False root.file_transfer.high_loads: 30000 \=>
300001, root.file_transfer.medium_loads: 10000 \=> 100001,
root.file_transfer.period: 32 \=> 321, root.file_transfer.low_loads: 2000
\=> 20001 rt=2023-04-27 10:24:27.374637 src=172.16.30.63 suser=admin
```

## Детектор сканеров

```
Apr 27 22:28:46 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00004|PolicyChange|3|act=PolicyChange cat=WS.Policy dst=SKDPU
NT msg=root.no_login.severity: LOW \=> MEDIUM, root.no_login.factor: 1 \=>
1.01 rt=2023-04-27 22:28:46.404905 src=192.168.20.124 suser=admin
```

## SKDPUNT.WS.00005

Управление сервисами:

- Сервис перезапущен

## Сервис перезапущен

```
Feb 20 23:20:52 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00005|ServiceRestart|3|act=ServiceRestart cat=Internal
dst=10.100.1.181 msg=analysed rt=2022-02-20 23:20:52.396277 suser=admin$
```

msg

название сервиса

## SKDPUNT.WS.00006

Записи данного типа генерируются при регистрации следующих событий:

- Управление группами ограничений доступа на просмотр данных;
- Управление настройками LDAP;
- Управление настройками СКДПУ НТ;
- Изменение парольной политики СКДПУ НТ.

### Управление группами ограничений доступа на просмотр данных

В СКДПУ НТ фиксируются факты создания, изменения и удаления групп ограничений доступа на просмотр данных. В зависимости от произведенного действия поле *msg* содержит следующие сведения:

- при создании группы ограничений

```
msg=Group added: group\<=<group_name>, roles\<=<list_roles>
```

**<group\_name>**

имя группы ограничения;

**<list\_roles>**

перечень ролей, с которыми ассоциируется группа ограничений.

```
Apr 27 22:36:31 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group added: group\<=Test_group, roles\<=['Operator']
rt=2023-04-27 22:36:31.698346 suser=admin
```

- при изменении группы ограничений

```
msg=Group changed: group\<=<group_name>, roles\<=<new_list_roles>
```

**<group\_name>**

имя группы ограничения;

**<new\_list\_roles>**

новый перечень ролей, с которыми ассоциируется группа ограничений.

```
Apr 27 22:37:37 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group changed: group\<=Test_group, roles
\<=['Administrator'] rt=2023-04-27 22:37:37.357614 suser=admin
```

- при удалении группы ограничений

```
msg=Group deleted: group\<>=<group_name>
```

**<group\_name>**

имя группы ограничения;

```
Apr 27 22:45:16 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group deleted: group\<>=Test_group rt=2023-04-27
22:45:16.119999 suser=admin
```

В зависимости от добавления или удаления ограничений в группу ограничений доступа на просмотр данных поле *msg* содержит следующие сведения:

- при добавлении ограничения на персону

```
msg=Group person added: group\<>=<group_name>, person\<>=<person_name>
```

**<group\_name>**

имя группы ограничения;

**<person\_name>**

имя персоны.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group person added: group\<>=Test_group, person
\<>=webmaster rt=2023-04-27 22:38:53.785637 suser=admin
```

- при добавлении ограничения на систему

```
msg=Group system added: group\<>=<group_name>, proxy\<>=<proxy_name>,
target\<>=<target_name>
```

**<group\_name>**

имя группы ограничения;

**<proxy\_name>**

имя шлюза доступа;

**<target\_name>**

целевое устройство.



Если целевое устройство не указано в ограничении, то `target\<>=None`.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group system added: group\<>=Test_group, proxy
\<>=basion7, target\<>=win1 rt=2023-04-27 22:38:53.785637 suser=admin
```

- при добавлении ограничения на группу персон LDAP

```
msg=Group ldap persons added: group\<>=<group_name>, domain\  
\= <domain_name>, name\<>=<person_group_name>
```

**<group\_name>**

имя группы ограничения;

**<domain\_name>**

имя домена LDAP;

**<person\_group\_name>**

имя группы персон.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|  
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings  
dst=SKDPU NT msg=Group ldap persons added: group\<>=Test_group,  
domain\<>=domain.local, name\<>=operators rt=2023-04-27 22:38:53.785637  
suser=admin
```

- при добавлении ограничения на группу систем LDAP

```
msg=Group ldap systems added: group\<>=<group_name>, domain\  
\= <domain_name>, name\<>=<system_group_name>
```

**<group\_name>**

имя группы ограничения;

**<domain\_name>**

имя домена LDAP;

**<system\_group\_name>**

имя группы устройств.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|  
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings  
dst=SKDPU NT msg=Group ldap systems added: group\<>=Test_group,  
domain\<>=domain.local, name\<>=printers rt=2023-04-27 22:38:53.785637  
suser=admin
```

- при удалении ограничения на персону

```
msg=msg=Group person deleted: group\<=<group_name>, person
\<=<person_name>
```

**<group\_name>**

имя группы ограничения;

**<person\_name>**

имя персоны.

```
Apr 27 22:39:50 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group person deleted: group\=Test_group, person
\<=webmaster rt=2023-04-27 22:39:50.834723 suser=admin
```

- при удалении ограничения на систему

```
msg=msg=Group system deleted: group\<=<group_name>, proxy
\<=<proxy_name>, target\<=<target_name>
```

**<group\_name>**

имя группы ограничения;

**<proxy\_name>**

имя шлюза доступа;

**<target\_name>**

целевое устройство.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group system deleted: group\=Test_group, proxy
\<=basion7, target\<=win1 rt=2023-04-27 22:38:53.785637 suser=admin
```

- при удалении ограничения на группу персон LDAP

```
msg=msg=Group ldap persons deleted: group\<=<group_name>, domain
\<=<domain_name>, name\<=<person_group_name>
```

**<group\_name>**

имя группы ограничения;

**<domain\_name>**

имя домена LDAP;

**<person\_group\_name>**

имя группы персон.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group ldap persons deleted: group\=Test_group,
```

```
domain\=domain.local, name\=operators rt=2023-04-27 22:38:53.785637
suser=admin
```

- при удалении ограничения на группу систем LDAP

```
msg=msg=Group ldap systems deleted: group\<=<group_name>, domain
\<=<domain_name>, name\<=<system_group_name>
```

**<group\_name>**

имя группы ограничения;

**<domain\_name>**

имя домена LDAP;

**<system\_group\_name>**

имя группы устройств.

```
Apr 27 22:38:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Group ldap systems deleted: group\=Test_group,
domain\=domain.local, name\=printers rt=2023-04-27 22:38:53.785637
suser=admin
```

## Управление настройками LDAP

Регистрируются следующие события:

- управление привязкой групп LDAP к ролям СКДПУ НТ;
- управление подключением доменов и серверов LDAP.

При возникновении указанных событий в поле *msg* указывается тип совершенного действия *<operation>*, а также перечень сущностей *<Ldap\_class>*, которые были изменены в результате совершенного действия, в формате

```
<operation>:[<Ldap_class>(<options>)]
```

**<operation>**

типы совершенных действий:

- *Added enrties* - добавлены сущности из перечня *<Ldap\_class>*;
- *Modified enrties* - свойства *<options>* сущностей из перечня *<Ldap\_class>* изменены;
- *Removed enrties* - сущности из перечня *<Ldap\_class>* удалены.



В поле *msg* могут быть указано несколько событий через запятую

**<Ldap\_class>**

перечень сущностей

Имя изменяемой сущности	Описание
<i>LdapDomain</i>	Настройки домена LDAP

Имя изменяемой сущности	Описание
<i>LdapServer</i>	Настройки сервера LDAP
<i>LdapGroup</i>	Настройки привязки группы LDAP

**<options>**

свойства у соответствующей сущности *<Ldap\_class>*

Таблица 1 – *LdapDomain*

Свойство	Описание	Формат
<i>authentication</i>	Тип проверки подлинности	Одно из строковых значений:  <pre>'SIMPLE'</pre> <pre>'SASL'</pre> <pre>'ANONYMOUS'</pre> <pre>'NTLM'</pre>
<i>base_dn</i>	Базовое уникальное имя	Строка Пример:  <pre>'CN</pre> <pre> \=Administrators,CN</pre> <pre> \=Builtin,DC\=test,DC</pre> <pre> \=local'</pre>
<i>computer_container</i>	Контейнер компьютеров	Строка Пример:  <pre>'OU\=Computers,CN</pre> <pre> \=Builtin,DC\=test,DC</pre> <pre> \=local'</pre>
<i>default</i>	Домен является доменом по умолчанию	True False
<i>group_container</i>	Контейнер групп	Строка Пример:  <pre>'OU\=Group,CN</pre> <pre> \=Builtin,DC\=test,DC</pre> <pre> \=local'</pre>
<i>id</i>	Идентификатор домена	128-битный уникальный идентификатор Пример:  <pre>'3f64ac10-e5f5-4bdb-</pre> <pre> a570-9f1832fb325b'</pre>

Свойство	Описание	Формат
<i>mapping_schema</i>	Схема соответствия	Одно из строковых значений:  <pre>'AD001'</pre> <pre>'AD002'</pre> <pre>'LDAP001'</pre> <pre>'POSIX001'</pre>
<i>name</i>	Имя домена	Строка
<i>ntlm_login</i>	Логин при проверке подлинности NTLM	Строка
<i>ntlm_password</i>	Пароль при проверке подлинности NTLM	Строка
<i>sasl_mechanism</i>	Механизм SASL	Одно из строковых значений:  <pre>'EXTERNAL'</pre> <pre>'DIGEST-MD5'</pre> <pre>'GSSAPI'</pre> <pre>'PLAIN'</pre>
<i>sasl_digest_md5_user</i>	Идентификатор пользователя при проверке подлинности SASL с механизмом DIGEST-MD5	Строка
<i>sasl_digest_md5_password</i>	Пароль при проверке подлинности SASL с механизмом DIGEST-MD5	Строка
<i>sasl_digest_md5_realm</i>	Область действия при проверке подлинности SASL с механизмом DIGEST-MD5	Строка
<i>sasl_digest_md5_authz_id</i>	Идентификатор авторизации при проверке подлинности SASL с механизмом DIGEST-MD5	Строка
<i>sasl_external_authorization_id</i>	Идентификатор авторизации при проверке подлинности SASL с механизмом EXTERNAL	Строка

Свойство	Описание	Формат
<i>sasl_gssapi_principal</i>	Субъект доступа Kerberos при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_gssapi_server_hostname</i>	Имя сервера Kerberos при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_gssapi_credential_store</i>	Хранилище учетных данных при проверке подлинности SASL с механизмом GSSAPI	Одно из строковых значений:  'DEFAULT' 'ALTERNATIVE'
<i>sasl_gssapi_cs_keytab</i>	Путь к файлу таблицы ключей при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_gssapi_cs_client_keytab</i>	Путь к файлу таблицы ключей клиента при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_gssapi_cs_ccache</i>	Путь к файлу кэш учетных данных при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_gssapi_cs_rcache</i>	Путь к файлу кэш повторов при проверке подлинности SASL с механизмом GSSAPI	Строка
<i>sasl_plain_authorization_id</i>	Идентификатор авторизации при проверке подлинности SASL с механизмом PLAIN	Строка
<i>sasl_plain_authentication_id</i>	Идентификатор аутентификации при проверке подлинности SASL с механизмом PLAIN	Строка

Свойство	Описание	Формат
<i>sasl_plain_password</i>	Пароль при проверке подлинности SASL с механизмом PLAIN	Строка
<i>simple_login</i>	Логин при проверке подлинности SIMPLE	Строка
<i>simple_password</i>	Пароль при проверке подлинности SIMPLE	Строка
<i>user_container</i>	Контейнер пользователей	Строковое представление Пример: <pre>'OU\=users,CN \=Builtin,DC\=test,DC \=local'</pre>

```
LdapDomain(authentication\='SIMPLE',sasl_gssapi_server_hostname
\='None',ntlm_login\='root',sasl_gssapi_cs_ccache\='None',base_dn
\='DC\=test, DC\=local',sasl_plain_authentication_id
\='None',sasl_digest_md5_realm\='None',sasl_plain_authorization_id
\='None',sasl_digest_md5_authz_id\='None',sasl_gssapi_cs_keytab
\='None',id\='7749e548-e93f-42bb-b76d-7a6c8c5890b3',name
\='test.local',ntlm_password\='*****',sasl_plain_password
\='*****',sasl_digest_md5_user\='None',sasl_external_authorization_id
\='None',sasl_gssapi_cs_rcache\='None',sasl_mechanism
\='PLAIN',computer_container\='None',default
\='True',group_container\='None',simple_password
\='*****',sasl_gssapi_cs_client_keytab\='None',user_container
\='None',sasl_gssapi_principal\='None',sasl_digest_md5_password
\='*****',sasl_gssapi_credential_store\='DEFAULT',simple_login
\='root',mapping_schema\='AD001')
```

Таблица 2 – LdapServer

Свойство	Описание	Формат
<i>address</i>	IP-адрес сервера	Строка IP-адреса Пример: <pre>'10.100.1.50'</pre>
<i>domain_id</i>	Идентификатор домена	128-битный уникальный идентификатор Пример: <pre>'3f64ac10-e5f5-4bdb- a570-9f1832fb325b'</pre>

Свойство	Описание	Формат
<i>encryption</i>	Контейнер компьютеров	Одно из строковых значений:  'NONE' 'SSL_TLS'
<i>id</i>	Идентификатор сервера	128-битный уникальный идентификатор  Пример:  '3f64ac10-e5f5-4bdb-a570-9f1832fb325b'
<i>poll_order</i>		Целое число  По умолчанию '0'
<i>port</i>	Номер порта	Целое число
<i>ssl_client_certificate</i>	Имя загруженного файла сертификата клиента	Строка
<i>ssl_client_private_key</i>	Имя загруженного файла закрытого ключа клиента	Строка
<i>ssl_client_private_key_password</i>	Пароль закрытого ключа (при наличии)	Строка
<i>ssl_ca_certificate_store</i>	Тип хранилища сертификатов СА при выбранном режиме шифрования	Одно из строковых значений:  'DEFAULT' 'FILE' 'FOLDER'
<i>ssl_ca_certificate_file</i>	Имя загруженного файла сертификата при выбранном типе хранилища FILE	Строка
<i>ssl_ca_certificate_folder</i>	Путь к директории файла сертификата при выбранном типе хранилища FOLDER	Строка
<i>ssl_validate_server_certificate</i>	Необходимость проверки сертификата сервера при выбранном режиме шифрования	Одно из строковых значений:  'ALWAYS' 'OPTIONALLY' 'NEVER'

Свойство	Описание	Формат
<i>timeout</i>	Время ожидания	Целое число

```
LdapServer(ssl_ca_certificate_folder\='None',encryption\='NONE',port
\='389',ssl_client_certificate\='*****',ssl_client_private_key
\='*****',address\='10.100.1.50',ssl_ca_certificate_file
\='*****',ssl_client_private_key_password\='*****',id
\='c2a5216b-8039-415e-98b1-6a80137bb408',poll_order
\='0',ssl_validate_server_certificate
\='ALWAYS',ssl_ca_certificate_store\='DEFAULT',timeout\='5',domain_id
\='3f64ac10-e5f5-4bdb-a570-9f1832fb325b')
```

Таблица 3 – *LdapGroup*

Свойство	Описание	Формат
<i>description</i>	Описание группы домена	Строка
<i>domain_id</i>	Идентификатор домена	128-битный уникальный идентификатор Пример: <pre>'3f64ac10-e5f5-4bdb-a570-9f1832fb325b'</pre>
<i>id</i>	Идентификатор сервера	128-битный уникальный идентификатор Пример: <pre>'3f64ac10-e5f5-4bdb-a570-9f1832fb325b'</pre>
<i>identifier</i>	Путь к группе пользователей домена	Строка Пример: <pre>'CN\=Administrators,CN\=Builtin,DC\=test,DC\=local'</pre>
<i>name</i>	Имя группы пользователей домена	Строка
<i>role_id</i>	Идентификатор роли	128-битный уникальный идентификатор Пример: <pre>'3f64ac10-e5f5-4bdb-a570-9f1832fb325b'</pre>

```
LdapGroup(identifier\='CN\=Administrators,CN\=Builtin,DC\=test,DC
\=local',domain_id\='8c12cf5a-7d19-4df8-b1a2-6b2bd48e428f',id
\='4ec7d0df-7872-465c-a529-cac9c8188da5',description\='Administrators
have complete and unrestricted access to the computer/domain',name
\='Administrators',role_id\='0a5b3c22-43c2-488f-8bc2-0be09148c453')
```

## Изменение настроек подключения к домену LDAP

```
May 7 11:47:14 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=Modified enrties: [LdapDomain(authentication
\'SIMPLE',sasl_gssapi_server_hostname=\'None',ntlm_login
\'root',sasl_gssapi_cs_ccache=\'None',base_dn=\'DC\=test, DC
\'local',sasl_plain_authentication_id=\'None',sasl_digest_md5_realm
\'None',sasl_plain_authorization_id=\'None',sasl_digest_md5_authz_id
\'None',sasl_gssapi_cs_keytab=\'None',id=\'7749e548-
e93f-42bb-b76d-7a6c8c5890b3',name=\'test.local',ntlm_password
\'*****',sasl_plain_password=\'*****',sasl_digest_md5_user
\'None',sasl_external_authorization_id=\'None',sasl_gssapi_cs_rcache
\'None',sasl_mechanism=\'PLAIN',computer_container
\'None',default=\'True',group_container=\'None',simple_password
\'*****',sasl_gssapi_cs_client_keytab=\'None',user_container
\'None',sasl_gssapi_principal=\'None',sasl_digest_md5_password
\'*****',sasl_gssapi_credential_store=\'DEFAULT',simple_login
\'root',mapping_schema=\'AD001')] rt=2023-05-07 11:47:14.227284
src=172.16.30.63 suser=admin
```

## Удаление сервера LDAP

```
Apr 27 22:49:10 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange
cat=WS.Settings dst=SKDPU NT msg=Removed enrties:
[LdapServer(ssl_ca_certificate_folder=\'None',encryption=\'NONE',port
\'389',ssl_client_certificate=\'*****',ssl_client_private_key
\'*****',address=\'10.100.1.50',ssl_ca_certificate_file
\'*****',ssl_client_private_key_password=\'*****',id
\'c2a5216b-8039-415e-98b1-6a80137bb408',poll_order
\'0',ssl_validate_server_certificate=\'ALWAYS',ssl_ca_certificate_store
\'DEFAULT',timeout=\'5',domain_id=\'3f64ac10-e5f5-4bdb-a570-9f1832fb325b')]
rt=2023-04-27 22:49:10.324659 src=192.168.20.124 suser=admin
```

## Изменение привязки группы LDAP к роли

```
May 2 16:04:53 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange
cat=WS.Settings dst=SKDPU NT msg=Modified enrties:
[LdapGroup(identifier=\'CN\=Администраторы,CN\=Builtin,DC\=domain,DC
\'local',domain_id=\'b3328ede-6143-48bf-b8e6-8bb47eb6a677',id
\'7d9f5e25-97c2-4c3e-a744-c641d9788d63',description
\'Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру и
\'Администраторы',role_id=\'a0964a74-a8dc-4cf5-bb31-e6240a31e22d')]
rt=2023-05-02 16:04:53.463755 src=172.16.30.63 suser=admin
```

## Управление настройками СКДПУ НТ

Регистрируются следующие события:

- изменение основных настроек СКДПУ НТ;
- изменение системных настроек СКДПУ НТ.

При изменении настроек СКДПУ НТ поле *msg* будет содержать перечень изменяющихся настроек и имеет следующий формат:

```
root.<setting_group>.<option>: <old_value> \=> <new_value>
```

**<setting\_group>**

имя группы настроек

Группа настроек	Описание
<i>system</i>	Настройки системы
<i>system.data_retention_defaults</i>	Стандарты хранения данных по умолчанию
<i>system.reports</i>	Настройка отчетов
<i>verbose</i>	Отладочная информация
<i>mail</i>	Настройка подключения к почтовому серверу
<i>webapp</i>	Настройка веб-интерфейса СКДПУ НТ

**<option>**

изменяемое свойство настроек

Таблица 4 – *system*

Свойство	Описание	Формат
<i>gc_session_timeout</i>	Максимальная продолжительность пользовательских сессий целевых систем	Целое число часов
<i>keep_tl_events</i>	Количество последних значений уровня доверия персон, которые учитываются в статистике изменения	Целое число

```
Apr 27 22:57:59 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings dst=SKDPU NT msg=root.system.gc_session_timeout: 251 \=> 250, root.system.keep_tl_events: 501 \=> 500 rt=2023-04-27 22:57:59.091406 src=192.168.20.124 suser=admin
```

Таблица 5 – *system.data\_retention\_defaults*

Свойство	Описание	Формат
<i>sessions</i>	Время хранения (месяцев) информации о пользовательских сессиях целевых систем, по истечении которого вся информация о них будет удалена	Целое число

Свойство	Описание	Формат
<i>persons</i>	Время бездействия персон (месяцев), по истечении которого вся информация о них будет удалена	Целое число
<i>targets</i>	Время отсутствия подключений к целевым устройствам (месяцев), по истечении которого вся информация о них будет удалена	Целое число
<i>incidents</i>	Время хранения информации об инцидентах (месяцев), по истечении которого вся информация о них будет удалена	Целое число
<i>keep_data</i>	Время хранения наборов данных для профилирования действий персон (месяцев), по истечении которого наборы данных будут удалены	Целое число
<i>keep_export</i>	Время хранения архивов пользовательских сессий целевых систем (месяцев), по истечении которого они будут удалены	Целое число

```
Apr 27 22:58:12 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=root.system.data_retention_defaults.sessions:
61 \=> 60, root.system.data_retention_defaults.persons: 181
\=> 180, root.system.data_retention_defaults.targets: 121 \=>
120, root.system.data_retention_defaults.incidents: 61 \=>
60, root.system.data_retention_defaults.keep_export: 31 \=>
30, root.system.data_retention_defaults.keep_data: 61 \=> 60
rt=2023-04-27 22:58:12.911604 src=192.168.20.124 suser=admin
```

Таблица 6 – *system.reports*

Свойство	Описание	Формат
<i>max_preview_lines</i>	Максимальное количество строк в отчете, доступных для предпросмотра перед печатью	Целое число
<i>reports.max_lines</i>	Максимальное количество строк в отчете, доступных для печати	Целое число

Свойство	Описание	Формат
<i>keep_period</i>	Время хранения отчетов (месяцев), по истечении которого они будут удалены	Целое число

```
Apr 27 22:56:32 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=root.system.reports.max_preview_lines:
51 \=> 50, root.system.reports.max_lines: 2001 \=> 2000,
root.system.reports.keep_period: 4 \=> 3 rt=2023-04-27
22:56:32.236371 src=192.168.20.124 suser=admin
```

Таблица 7 – *verbose*

Свойство	Описание	Формат
<i>level</i>	Уровень отладочной информации	Целое число, лежащее в диапазоне 0-4

```
Apr 27 22:55:15 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=root.verbose.level: 1 \=> 0 rt=2023-04-27
22:55:15.947652 src=192.168.20.124 suser=admin
```

Таблица 8 – *mail*

Свойство	Описание	Формат
<i>server</i>	Доменное имя или IP-адрес почтового сервера	Строка
<i>from_addr</i>	Электронный адрес отправителя	Строка
<i>from_name</i>	Имя отправителя	Строка
<i>protocol</i>	Протокол передачи сообщений	Одно из строковых значений:  'SMTP' 'SMTPS' 'SMTP+STARTTLS'
<i>port</i>	Номер порта	Целое число
<i>password</i>	Пароль пользователя	Строка
<i>username</i>	Имя пользователя	Строка

```
Apr 27 22:56:04 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=root.mail.server: smtp.gmail.com1 \=>
smtp.gmail.com, root.mail.from_addr: ro4dale@gmail.com1 \=>
ro4dale@gmail.com, root.mail.from_name: SKDPU NT \=> SKDPU
NT1, root.mail.protocol: smtps \=> starttls, root.mail.port:
4651 \=> 465, root.mail.password: changed, root.mail.username:
```

```
ro4dale@gmail.com \=> ro4dale@gmail.com1 rt=2023-04-27
22:56:04.862584 src=192.168.20.124 suser=admin
```

Таблица 9 – *webapp*

Свойство	Описание	Формат
<i>default_language</i>	Язык страницы авторизации веб-интерфейса	Одно из строковых значений:  <div style="border: 1px solid black; padding: 5px; width: fit-content;">                     'en' 'ru' 'fr' 'de'                 </div>
<i>max_print_list</i>	Максимальное количество строк таблиц при печати из веб-интерфейса СКДПУ НТ	Целое число
<i>hostip</i>	IP-адрес сервера СКДПУ НТ	Строка
<i>per_page</i>	Количество строк таблиц, отображаемых в веб-интерфейсе СКДПУ НТ на одной странице	Целое число
<i>autologout_interval</i>	Время бездействия (минут), после которого происходит прерывание сессии доступа к веб-интерфейсу СКДПУ НТ	Целое число
<i>max_session_lifetime</i>	Максимальное время (минут) сессии доступа к веб-интерфейсу СКДПУ НТ	Целое число
<i>new_incident_interval</i>	Интервал поиска новых инцидентов (минут)	Целое число
<i>hostname</i>	Имя сервера СКДПУ НТ	Строка

```
Apr 27 22:56:21 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange
cat=WS.Settings dst=SKDPU NT msg=root.webapp.default_language:
en \=> ru, root.webapp.max_print_list: 1001 \=> 1000,
root.webapp.hostip: SKDPU NT \=> SKDPU NT1, root.webapp.per_page:
11 \=> 10, root.webapp.autologout_interval: 16 \=>
15, root.webapp.max_session_lifetime: 1441 \=> 1440,
root.webapp.new_incident_interval: 6 \=> 5, root.webapp.hostname:
skdpu nt \=> skdpu nt1 rt=2023-04-27 22:56:21.864372
src=192.168.20.124 suser=admin
```

**<old\_value>**

старое значение свойства

**<new\_value>**

новое значение свойства

## Изменение парольной политики СКДПУ НТ

При изменении парольной политики СКДПУ НТ поле *msg* будет содержать перечень изменяющихся настроек и имеет следующий формат:

```
root.<setting_group>.<option>: <old_value> \=> <new_value>
```

### <setting\_group>

имя группы настроек

Группа настроек	Описание
<i>webapp.password_policy</i>	Настройка парольной политики СКДПУ НТ

### <option>

изменяемое свойство настроек

Таблица 10 – *webapp.password\_policy*

Свойство	Описание	Формат
<i>max_login_attempts</i>	Максимальное количество попыток авторизации через веб-интерфейс СКДПУ НТ	Целое число
<i>not_equal_to_user_name</i>	Пароль не должен совпадать с именем пользователя	True False
<i>min_lowercase</i>	Минимальное количество строчных букв	Целое число
<i>last_passwords_denied</i>	Количество последних использованных паролей, которые запрещены для повторного использования	Целое число
<i>min_length</i>	Минимальная длина пароля	Целое число
<i>min_uppercase</i>	Минимальное количество заглавных букв	Целое число
<i>days_to_warn</i>	Количество дней, по истечении которого будет выдано оповещение об окончании действия пароля	Целое число
<i>max_length</i>	Максимальная длина пароля	Целое число

Свойство	Описание	Формат
<i>min_special</i>	Минимальное количество специальных символов	Целое число

```
Apr 27 23:01:54 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00006|SettingsChange|3|act=SettingsChange cat=WS.Settings
dst=SKDPU NT msg=root.webapp.password_policy.max_login_attempts:
6 \=> 5, root.webapp.password_policy.not_equal_to_user_name:
False \=> True, root.webapp.password_policy.min_lowercase:
2 \=> 1, root.webapp.password_policy.days_to_expire: 366
\=> 365, root.webapp.password_policy.min_digits: 2 \=>
1, root.webapp.password_policy.last_passwords_denied:
6 \=> 5, root.webapp.password_policy.min_length: 7
\=> 6, root.webapp.password_policy.min_uppercase: 2
\=> 1, root.webapp.password_policy.days_to_warn: 4 \=>
3, root.webapp.password_policy.max_length: 33 \=> 32,
root.webapp.password_policy.min_special: 2 \=> 1 rt=2023-04-27
23:01:54.311323 src=192.168.20.124 suser=admin
```

**<old\_value>**

старое значение свойства

**<new\_value>**

новое значение свойства

### SKDPUNT.WS.00007

Несоответствие отпечатка данных сессии сохраненному (нарушение целостности данных).

### Нарушение целостности записей сессий

```
Feb 20 13:14:30 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00007|SessionIntegrityError|3|cat=Internal msg=Stored session
integrity error rt=2022-02-20 13:14:30.918732 src=skdpu-nt
```

### SKDPUNT.WS.00008

Нарушение целостности собственных исполняемых файлов:

- Отсутствие исполняемых модулей СКДПУ НТ
- Несовпадают контрольные суммы модулей СКДПУ НТ

### Отсутствие исполняемых модулей СКДПУ НТ

```
Jun 1 11:53:28 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00008|ExecutableIntegrityError|8|cat=Internal fname=/opt/skdpu-
nt/bin/nt-oem msg=Executable integrity error rt=2022-06-01 11:53:28.123016
src=skdpu-nt
```

### Несовпадают контрольные суммы модулей СКДПУ НТ

```
Jun 1 11:53:27 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00008|ChecksumMismatch|8|cat=Internal fname=/opt/skdpu-nt/
```

```
bin/whisper-auto-resize.py msg=Executable integrity error rt=2022-06-01
11:53:27.124416 src=skdpu-nt
```

## SKDPUNT.WS.00009

Достижение критического уровня свободной памяти для хранения данных пользовательских сессий целевых систем.

### Уменьшение объема свободного места

```
Jun 1 11:53:27 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.WS.00009|LowFreeSpace|8|cat=Internal msg=Storage space < 10% free
rt=2022-06-01 11:53:27.124416 src=skdpu-nt
```



## 1.2 Класс событий Authentication

### Общее описание

СКДПУ НТ генерирует записи о следующих событиях рассматриваемого класса:

- управление блокированием пользователей через веб-интерфейс СКДПУ НТ (SKDPUNT.AUTH.00002);
- управление учетными записями пользователей через веб-интерфейс СКДПУ НТ (SKDPUNT.AUTH.00003);
- управление ролями пользователей через веб-интерфейс СКДПУ НТ (SKDPUNT.AUTH.00004);
- управление паролем пользователя через веб-интерфейс СКДПУ НТ (SKDPUNT.AUTH.00005).

Тело сообщения рассматриваемого класса событий содержит следующие пары *ключ=значение*

Ключ	Описание
<i>act</i>	Регистрируемое действие
<i>cat</i>	Категория действия
<i>dst</i>	URL, доменное имя или IP-адрес сервера СКДПУ НТ   Указывается в поле <b>IP-адрес хоста</b> в разделе <b>Настройки &gt; Основные настройки</b>
<i>dvchost</i>	URL, доменное имя или IP-адрес сервера СКДПУ НТ   Указывается в поле <b>Имя хоста</b> в разделе <b>Настройки &gt; Основные настройки</b>

Ключ	Описание
<i>duser</i>	Учетная запись пользователя СКДПУ НТ, по отношению к которому совершается рассматриваемое действие
<i>rt</i>	Дата и время регистрации события
<i>src</i>	IP-адрес, с которого пользователь СКДПУ НТ осуществляет доступ к СКДПУ НТ
<i>start</i>	Дата и время начала сессии доступа к СКДПУ НТ
<i>suser</i>	Учетная запись пользователя СКДПУ НТ, который совершает рассматриваемое действие
<i>msg</i>	Дополнительная информация о совершаемом действии

Каждое событие располагает своим набором параметров описания.

### SKDPUNT.AUTH.00002

Блокировка\разблокировка пользователя.

#### Для учетной записи пользователя было изменено состояние блокировки

```
Feb 20 13:23:38 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00002|UserAccountPassword|6|act=('UserAccountLock',) cat=Auth
dst=https://skdpu-nt-cert.domain.local duser=user msg=user@testmail.com
rt=2022-02-20 13:23:38.692790 suser=admin$
```

### SKDPUNT.AUTH.00003

Создание, удаление и изменение пользователя:

- Создана учетная запись пользователя
- Учетная запись пользователя удалена
- Роль, ассоциированная с учетной записью пользователя, изменена
- Адрес электронной почты, привязанный к учетной записи пользователя, изменен

#### Создана учетная запись пользователя

```
Feb 20 13:11:01 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00003|UserAccountCreate|3|act=UserAccountCreate cat=Auth
dst=https://skdpu-nt-cert.domain.local duser=user rt=2022-02-20
13:11:01.556386 suser=admin$
```

#### Учетная запись пользователя удалена

```
Feb 20 13:13:19 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00003|UserAccountDelete|3|act=UserAccountDelete cat=Auth
dst=https://skdpu-nt-cert.domain.local duser=user rt=2022-02-20
13:13:19.920668 suser=admin$
```

## Роль, ассоциированная с учетной записью пользователя, изменена

```
Feb 20 13:11:21 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00003|UserRoleChange|3|act=UserRoleChange cat=Auth dst=https://
skdpu-nt-cert.domain.local duser=user msg=Operator rt=2022-02-20
13:11:21.819801 suser=admin$
```

## Адрес электронной почты, привязанный к учетной записи пользователя, изменен

```
Feb 20 13:11:21 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00003|UserEmailChange|3|act=UserEmailChange cat=Auth
dst=https://skdpu-nt-cert.domain.local duser=user msg=user1@testmail.com
rt=2022-02-20 13:11:21.821026 suser=admin$
```

### SKDPUNT.AUTH.00004

Создание, удаление и изменение роли в веб-интерфейсе СКДПУ НТ:

- Создана новая роль
- Роль изменена
- Роль удалена

## Создана новая роль

```
Feb 20 13:14:01 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00004|RoleCreate|3|act=RoleCreate cat=Auth dst=https://
skdpu-nt-cert.domain.local name=Test_role rt=2022-02-20 13:14:01.963456
suser=admin$
```

## Роль изменена

```
Feb 20 13:15:55 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00004|RoleChange|3|act=RoleChange cat=Auth dst=https://
skdpu-nt-cert.domain.local name=Test_role rt=2022-02-20 13:15:55.707783
suser=admin$
```

## Роль удалена

```
Feb 20 13:19:59 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00004|RoleDelete|3|act=RoleDelete cat=Auth dst=https://skdpu-
nt-cert.domain.local msg=Test_role rt=2022-02-20 13:19:59.184977 suser=admin
$
```

### SKDPUNT.AUTH.00005

Изменение пароля учетной записи пользователя СКДПУ НТ.

## Пароль учетной записи пользователя изменен

```
Feb 20 13:12:37 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.AUTH.00005|UserAccountPassword|3|act=UserAccountPassword cat=Auth
dst=https://skdpu-nt-cert.domain.local duser=user msg=user1@testmail.com
rt=2022-02-20 13:12:37.768734 suser=admin$
```


### 1.3 Класс событий Report

#### Общее описание

СКДПУ НТ генерирует записи о следующих событиях рассматриваемого класса:

- управление отчетами СКДПУ НТ (**SKDPUNT.REPORT.00001**);
- отправка отчетов адресатам (**SKDPUNT.REPORT.00002**);
- просмотр пользовательских сессий целевых систем через веб-интерфейс СКДПУ НТ (**SKDPUNT.REPORT.00003**).

Тело сообщения рассматриваемого класса событий содержит следующие пары *ключ=значение*

Ключ	Описание
<i>act</i>	действие
<i>cat</i>	категория действия
<i>dst</i>	URL, доменное имя или IP-адрес сервера СКДПУ НТ   Указывается в поле <b>IP-адрес хоста</b> в разделе <b>Настройки &gt; Основные настройки</b>
<i>duser</i>	учетная запись пользователя шлюза доступа, сессия которого просматривается
<i>rt</i>	дата и время регистрации события
<i>suser</i>	учетная запись пользователя СКДПУ НТ, который совершает рассматриваемое действие
<i>msg</i>	дополнительная информация о совершаемом действии

#### SKDPUNT.REPORT.00001

Работа с отчетами в веб-интерфейсе СКДПУ НТ:

- **Отчет создан**
- **Отчет изменен**
- **Отчет удален**

## Отчет создан

```
Feb 20 18:18:18 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00001|Test_report|3|act=ReportCreate cat=Reporting dst=10.100.1.181 rt=2022-02-20 18:18:18.667654 suser=admin$
```

## Отчет изменен

```
Feb 20 18:19:38 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00001|Test_report|3|act=ReportChange cat=Reporting dst=10.100.1.181 rt=2022-02-20 18:19:38.736502 suser=admin$
```

## Отчет удален

```
Feb 20 18:25:25 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00001|Test_report|3|act=ReportDelete cat=Reporting dst=10.100.1.181 rt=2022-02-20 18:25:25.622205 suser=admin$
```

## SKDPUNT.REPORT.00002

Выгрузка отчета в веб-интерфейсе СКДПУ НТ.

## Отчет отправлен по электронной почте/ Скачивание отчета

```
Feb 20 18:23:13 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00002|Test_report|3|act=ReportAccess cat=Reporting rt=2022-02-20 18:23:13.814517 suser=CyberNova Operation center mailbot <skdpunt01@it-bastion.com>$
```

## SKDPUNT.REPORT.00003

Генерирование отчета и просмотр пользовательской сессии целевой системы в веб-интерфейсе СКДПУ НТ:

- Отчет сгенерирован
- Произведен просмотр пользовательских сессий целевых систем

## Отчет сгенерирован

```
Feb 20 18:23:12 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00003|Report built|3|cat=Reporting rt=2022-02-20 18:23:12.869666 suser=admin$
```

## Произведен просмотр пользовательских сессий целевых систем

```
Feb 20 18:04:09 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.REPORT.00003|17f0d1478c8aa207000c29b8a9a2|3|act=SessionView cat=Reporting dst=10.100.1.181 duser=admin msg=17f0d1478c8aa207000c29b8a9a2 rt=2022-02-20 18:04:09.518000 suser=admin$
```

msg

идентификатор просматриваемой пользовательской сессии целевой системы

## 1.4 Класс событий Session Control

### Общее описание

Рассматриваемый класс включает в себя события, которые были зарегистрированы на стороне шлюза доступа при взаимодействии с целевым устройством:

- Успешное подключение к целевому ресурсу (**SKDPUNT.SC.00001**);
- Успешное окончание сессии подключения к целевому ресурсу (**SKDPUNT.SC.00002**);
- Передача файлов в рамках сессии подключения к целевому ресурсу (**SKDPUNT.SC.00003**);
- Ошибка авторизации при подключении к целевому ресурсу (**SKDPUNT.SC.00004**);
- Прекращение доступа к целевому ресурсу (**SKDPUNT.SC.00005**).

Система должна сигнализировать следующим сообщением о действиях в интерфейсе. Тело сообщения рассматриваемого класса событий содержит следующие пары *ключ=значение*

Ключ	Описание
<i>act</i>	Регистрируемое действие
<i>app</i>	Тип пользовательской сессии целевой системы. Возможные значения: RDP, SSH, APP
<i>cat</i>	Категория события
<i>destinationServiceName</i>	Тип протокола пользовательской сессии целевой системы. Возможные значения: SSH, RDP, TELNET, RLOGIN, VNC, RAWTCP.
<i>dhost</i>	Имя целевого устройства
<i>dst</i>	IP-адрес целевого устройства
<i>duid</i>	Целевая учетная запись
<i>dvchost</i>	Имя шлюза доступа
<i>end</i>	Дата и время окончания пользовательской сессии целевой системы
<i>externalId</i>	Идентификатор пользовательской сессии целевой системы
<i>fileHash</i>	Хеш-сумма передаваемого файла
<i>fname</i>	Имя передаваемого файла
<i>fsize</i>	Размер передаваемого файла в байтах
<i>msg</i>	Дополнительная информация о событии
<i>rt</i>	Дата и время регистрации события в СКДПУ НТ
<i>src</i>	IP-адрес персоны

Ключ	Описание
<i>start</i>	Дата и время начала пользовательской сессии целевой системы
<i>suser</i>	Имя персоны

### SKDPUNT.SC.00001

Начало сессии через шлюз.

### Сессия установлена успешно

```
Mar 18 22:11:24 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.SC.00001|SESSION_ESTABLISHED_SUCCESSFULLY|1|act=SESSION_ESTABLISHED_SUCCESSFULLY app=SSH cat=SessionControl destinationServiceName=SSH dhost=ssh dst=10.100.50.71 duid=M-PM-0M-PM-4M-PM-<M-PM-8M-PM-=M-PM-8M-QM-^AM-QM-^BM-QM-^@M-PM-0M-QM-^BM-PM->M-QM-^@_1 dvchost=avs externalId=17f9e70665f663d8000c29b8a9a2 rt=2022-03-18 22:11:24.712241 src=172.16.30.63 start=2022-03-18 22:10:41 suser=admin$
```

### SKDPUNT.SC.00002

Окончание сессии через шлюз.

### Отключение сессии

```
Mar 18 22:16:12 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.SC.00002|SESSION_DISCONNECTION|1|act=SESSION_DISCONNECTION app=SSH cat=SessionControl destinationServiceName=SSH dhost=ssh dst=10.100.50.71 duid=M-PM-0M-PM-4M-PM-<M-PM-8M-PM-=M-PM-8M-QM-^AM-QM-^BM-QM-^@M-PM-0M-QM-^BM-PM->M-QM-^@_1 dvchost=avs externalId=17f9e70665f663d8000c29b8a9a2 rt=2022-03-18 22:16:12.846567 src=172.16.30.63 start=2022-03-18 22:10:41 suser=admin$
```

### SKDPUNT.SC.00003

Факты передачи файлов в рамках сессии (направление, имена файлов).

### Передача файлов в рамках сессии

```
Mar 25 14:42:37 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|SKDPUNT.SC.00003|SFTP_EVENT|1|act=SFTP_EVENT app=SSH cat=SessionFileTransfer destinationServiceName=SSH dhost=dnd-30.179 dst=172.16.30.179 duid=dnd dvchost=skdpuprod externalId=17fc0e18a6f9e82e000c29318b8d fileHash=b51d76991b07374d2dad69cb697e088c97c2bf412d75e076e1f89071126a842d fname=/home/dnd/gop/OKBM.conf fsize=205 rt=2022-03-25 14:42:37.646004 src=192.168.20.64 suser=p.garbar
```

### SKDPUNT.SC.00004

Ошибка авторизации в рамках сессии.

## Ошибка аутентификации

```
Mar 23 15:33:35 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.SC.00004|LoginFailure|6|act=LoginFailure app=rdpproxy cat=Auth
destinationServiceName=rdpproxy dvchost=avs msg=AUTHENTICATION_FAILURE by
password or pubkey rt=2022-03-23 15:33:35.714973 src=avs suser=$
```

### SKDPUNT.SC.00005

Прерывание пользовательской сессии целевой системы.

## Прекращение доступа к целевой системе

```
Mar 25 14:42:37 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.SC.00005|CONNECTION_FAILED|1|act=CONNECTION_FAILED app=SSH
cat=SessionControl destinationServiceName=SSH dhost=dnd-30.179
dst=172.16.30.179 duid=dnd dvchost=skdpuprod end=2022-03-25 16:42:37.646004
externalId=17fc0e18a6f9e82e000c29318b8d rt=2022-03-25 14:42:37.646004
src=192.168.20.64 suser=p.garbar
```

## 1.5 Класс событий Incident

### Общее описание

СКДПУ НТ генерирует записи об инцидентах при срабатывании детекторов аномалий.

Тело сообщения рассматриваемого класса событий содержит следующие пары *ключ=значение*

Ключ	Описание
<i>act</i>	Регистрируемое действие
<i>app</i>	Тип пользовательской сессии целевой системы. Возможные значения: RDP, SSH, APP
<i>cat</i>	Категория инцидента
<i>cnt</i>	Влияние инцидента
<i>destinationServiceName</i>	Тип протокола пользовательской сессии целевой системы. Возможные значения: RDP, SSH, TELNET, RLOGIN, VNC, RAWTCP.
<i>dhost</i>	Имя целевого устройства
<i>dst</i>	IP-адрес целевого ресурса
<i>duid</i>	Целевая учетная запись
<i>dvchost</i>	Имя шлюза доступа
<i>externalId</i>	Идентификатор пользовательской сессии целевой системы
<i>reason</i>	Причина возникновения инцидента. Состоит из пар <i>ключ: значение</i> .

Ключ	Описание
<i>rt</i>	Дата и время регистрации инцидента
<i>src</i>	IP-адрес персоны
<i>suser</i>	Имя персоны

Значение ключа *reason* представляет собой JSON-структуру со следующими ключами:

- *event\_data* - данные события, которое инициировало инцидент;
- *event\_hash* - хеш-сумма события;
- *wabsession\_id* - идентификатор, который имеет пользовательская сессия целевой системы, хранящаяся в СКДПУ НТ;
- *recorded\_at* - дата и время фиксирования события;
- *session\_id* - идентификатор, который имеет пользовательская сессия целевой системы, хранящаяся на шлюзе доступа;
- *event\_type* - тип события.

## SKDPUNT.INCIDENT.00001

Создание инцидента, инициированного вследствие срабатывания соответствующего детектора аномалий:

- Детектирование потенциально опасных команд;
- Детектирование принудительного блокирования сессий;
- Контроль привычного времени работы;
- Контроль привычных сетевых адресов;
- Контроль привычного времени работы;
- Детектор новых доступов;
- Детектор проблем с правами доступа к файлам;
- Детектор туннелей и прыжков;
- Анализатор ошибок авторизации;
- Детектор входов помимо бастиона;
- Детектор забытых персон;
- Контроль стандартных команд;
- Детектор сканеров;
- Индикаторы взрывной активности;
- Количество переданных файлов;
- Создание инцидента вручную.

## Детектирование потенциально опасных команд

Генерирование инцидента при обнаружении потенциально опасных команд.

```
Apr 3 11:52:19 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|CLM-1001453|3|act=SKDPUNT.INCIDENT.NEW
app=RDP cat=COLOR_LIST_MATCH cnt=2.0 destinationServiceName=RDP
dhost=win1 dst=10.100.1.50 duid=root dvchost=wab-7-0-7
externalId=187465097d2a5524000c2904ee49 reason={'recorded_at': '2023-04-03
11:52:18', 'session_id': '187465097d2a5524000c2904ee49', 'event_type':
'KBD_INPUT', 'wabsession_id': '897f8bac-9630-459e-9b45-02eb9e6f4d98',
'event_hash': '2728028e7ff564e07d21e3226c910a07', 'event_data': {'data':
'bitcoin/<enter>'}, } rt=2022-04-03 11:52:18 src=172.16.129.142 suser=user
```

## Детектирование принудительного блокирования сессий

Генерирование инцидента при обнаружении фактов принудительного прерывания пользовательских сессий целевых систем при обнаружении команд из черных списков, заданных в политике безопасности шлюзов доступа.

```
Apr 7 17:01:38 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|KPE-846576|3|act=SKDPUNT.INCIDENT.NEW
app=RDP cat=KILL_PATTERN_EVENT cnt=16.0 destinationServiceName=RDP
dhost=rdp_wallix dst=10.100.164.51 duid=Administrator dvchost=wab-7-0-14
externalId=180044e1718eb1a9000c29b77bfc reason={'recorded_at': '2022-04-07
17:02:04', 'session_id': '180044e1718eb1a9000c29b77bfc', 'event_type':
'KILL_PATTERN_DETECTED', 'wabsession_id': 'cbc51836-b5de-4de6-9ceb-
eeae7629db2b', 'event_hash': '65c154afafd0ed38d15a57d745768a4d',
'event_data': {'pattern': '$ocr:.*\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\cmd.exe|Administrator: C:
\\\\\\\\\\\\\\\\Windows\\\\\\\\\\\\\\\\system32\\\\\\\\\\\\\\\\cmd.exe'}, } rt=2022-04-07 17:02:04
src=192.168.20.225 suser=user
```

## Контроль привычного времени работы

Генерирование инцидента при выходе за пределы характерного для пользователя целевой системы времени работы.

```
Apr 10 10:58:40 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|TF-1001464|3|act=SKDPUNT.INCIDENT.NEW
app=RDP cat=TIME_FRAME cnt=10.0 destinationServiceName=RDP
dhost=rdp dst=10.100.50.16 duid=Administrator dvchost=wab-7-0-14
externalId=1876a2c808463328000c295a01e8 reason={'recorded_at': '2023-04-10
10:58:39', 'session_id': '1876a2c808463328000c295a01e8', 'event_type':
'SESSION_ESTABLISHED_SUCCESSFULLY', 'wabsession_id': '0621e4c0-5466-41b9-
b461-4e1e04fab769', 'event_hash': '844f48b067d2eb38b41144flebbf1aae',
'event_data': {}} rt=2022-04-10 10:58:39 src=192.168.50.195 suser=user
```

## Контроль привычных сетевых адресов

Генерирование инцидента при пользовательском запросе на доступ к целевой системе из другой подсети.

```
Apr 5 13:51 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|SA-1001462|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=SOURCE_ADDRESS cnt=10 destinationServiceName=SSH
```

```
dhost=netlinux-10.100.1.195 dst=10.100.1.195 duid=wabadmin
dvchost=wab-7-0-7 externalId=187510b1a41b6fb3000c2904ee49
reason={'recorded_at': '2023-04-05 13:51:35',
'session_id': '187510b1a41b6fb3000c2904ee49', 'event_type':
'SESSION_ESTABLISHED_SUCCESSFULLY', 'wabsession_id':
'35a3d6ca-831d-4fbe-8633-aabdb6c19c71', 'event_hash':
'04109b87f4c7281bf3f4e20ab84cac3b', 'event_data': {}} rt=2023-04-05
13:51:35 src=192.168.50.128 suser=mds@test.local
```

## Контроль привычного времени работы

Генерирование инцидента при достижении установленных пороговых значений Уровня доверия.

## Детектор новых доступов

Генерирование инцидента при выявлении попыток доступа пользователей к нехарактерным целевым учетным записям или целевым системам.

```
Mar 23 13:04:17 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|NA-846559|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=NEW_ACCESS cnt=1.0 destinationServiceName=SSH
dhost=ssh dst=10.100.50.71 duid=wabadmin dvchost=avs
externalId=17fb63acd787a008000c29b8a9a2 reason={'recorded_at':
'2022-03-23 13:03:01', 'session_id': '17fb63acd787a008000c29b8a9a2',
'event_type': 'SESSION_ESTABLISHED_SUCCESSFULLY', 'wabsession_id':
'bbcdba7b-7181-48a3-9532-116f11b208d1', 'event_hash':
'd08fbc47ab5f7f47e01db631f7a95fa8', 'event_data': {}} rt=2022-03-23
13:03:01 src=192.168.20.60 suser=admin$
```

## Детектор проблем с правами доступа к файлам

Генерирование инцидента при обнаружении ошибок доступа на осуществление операций чтения или записи файлов по протоколу SFTP.

```
Apr 25 16:27:32 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|PD-1000019|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=PERMISSION_DENIED cnt=2.0 destinationServiceName=SSH
dhost=websrv-01 dst=172.16.1.129 duid=webmaster dvchost=basion7
externalId=ad8190ab519fa8a24d0fafa2e287 reason={'wabsession_id':
'016efa11-9e08-4103-bb6c-4a06fb2bfa9e', 'session_id':
'ad8190ab519fa8a24d0fafa2e287', 'event_type': 'SFTP_EVENT', 'event_hash':
'24d678fdc3e6fcb77336651db45ceddc', 'recorded_at': '2023-04-25 16:22:23',
'event_data': {'data': "setstat '/data3/dev.kultura.local/htdocs/bitrix/
php_interface/init.php' uid=\"0\" gid=\"0\"", 'status': 'Permission denied'}}
rt=2023-04-25 16:27:32 src=192.168.0.8 suser=webmaster
```

## Детектор туннелей и прыжков

Генерирование инцидента, когда персона выполняет команды или другие действия с целью открытия дополнительных сетевых каналов для инфраструктуры в рамках рассматриваемой пользовательской сессии целевой системы.

### Выполнение команды:

```
Apr 25 16:22:11 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|RJ-1000007|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=REMOTE_JUMP cnt=10 destinationServiceName=SSH
dhost=jenkins-01 dst=172.16.1.3 duid=adm@test.local dvchost=basion7
externalId=51fa6c2d0ef2d9ce31f05fae548f reason={'wabsession_id':
'98ae768a-d033-4845-b56c-c10a470e81e1', 'session_id':
'51fa6c2d0ef2d9ce31f05fae548f', 'event_type': 'KBD_INPUT', 'event_hash':
'0500dcalbc9fe25a458043d609ef4673', 'recorded_at': '2023-04-25 16:25:40',
'event_data': {'data': 'sudo ssh 10.15.42.17'}} rt=2023-04-25 16:25:40
src=192.168.0.52 suser=adm@test.local
```

### Окончание сессии доступа:

```
Apr 25 16:22:12 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|RJ-1000010|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=REMOTE_JUMP cnt=10 destinationServiceName=SSH
dhost=jenkins-01 dst=172.16.1.3 duid=adm@test.local dvchost=basion7
externalId=51fa6c2d0ef2d9ce31f05fae548f reason={'wabsession_id':
'98ae768a-d033-4845-b56c-c10a470e81e1', 'session_id':
'51fa6c2d0ef2d9ce31f05fae548f', 'event_type': 'SESSION_DISCONNECTION',
'event_hash': '6ad4d03ae507ce72fa05f6baea706647', 'recorded_at':
'2023-04-25 17:13:16', 'event_data': {'duration': '0:51:05'}} rt=2023-04-25
17:13:16 src=192.168.0.52 suser=adm@test.local
```

## Анализатор ошибок авторизации

Генерирование инцидента при обнаружении ошибок авторизации на целевой системе.

```
Apr 7 17:19:24 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|AF-846580|3|act=SKDPUNT.INCIDENT.NEW
cat=AUTHENTICATION_FAILURE cnt=1.0 reason=None rt=2022-04-07 17:19:49
suser=wabadmin
```

## Детектор входов помимо бастиона

Генерирование инцидента при обнаружении системами сторонних производителей попыток доступа к целевой системе в обход шлюза доступа (СКДПУ).

```
Apr 7 18:23:24 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|TF-1000030|3|act=SKDPUNT.INCIDENT.NEW
app=RDP cat=TIME_FRAME cnt=10.0 destinationServiceName=RDP
dhost=MJ-874.481.91.0 dst=822.4.2.2 duid=tester dvchost=skdpu70
externalId=eb6476279cb7c1103884b93c1c87 reason={'session_id':
'eb6476279cb7c1103884b93c1c87', 'wabsession_id': 'eda82722-6504-4ff4-9d93-
f20a89fb0f58', 'event_hash': 'bdfebc3500e322619b0235c3fa6a3abd',
'event_type': 'SESSION_ESTABLISHED_SUCCESSFULLY', 'recorded_at':
'2023-04-07 18:23:24', 'event_data': {}} rt=2023-04-07 18:23:24
src=73.8.011.47 suser=JoPo4ka
```

## Детектор забытых персон

Генерирование инцидента при обнаружении активности целевых учетных записей, которые оставались продолжительное время неактивными.

```
Apr 7 15:37:22 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|FP-846566|3|act=SKDPUNT.INCIDENT.NEW app=RDP
cat=FORGOTTEN_PERSON cnt=10.0 destinationServiceName=RDP dhost=rdp_wallix
dst=10.100.164.51 duid=PAVLOV\\Administrators dvchost=wab-7-0-14
externalId=180040732c3540e2000c29b77bfc reason={'recorded_at':
'2022-04-07 15:37:04', 'session_id': '180040732c3540e2000c29b77bfc',
'event_type': 'SESSION_ESTABLISHED_SUCCESSFULLY', 'wabsession_id':
'7aa5547f-3cd6-4489-9ee2-e8acd08c5aaa', 'event_hash':
'bleacae779c47aa49b940aflacd98ae6', 'event_data': {}} rt=2022-04-07
15:37:04 src=192.168.20.225 suser=user
```

## Контроль стандартных команд

Генерирование инцидента при обнаружении несвойственных шаблонов команд выбранной целевой учетной записи.

```
Apr 7 18:33:28 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|CR-1000031|3|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=COMMANDS_RESEMBLANCE cnt=10 destinationServiceName=SSH
dhost=TVCC-1.827.856.785 dst=8.30.36.0 duid=commander
dvchost=skdpu_test externalId=a3d78e84d97284d31d51044779a9
reason={'session_id': 'a3d78e84d97284d31d51044779a9', 'wabsession_id':
'b0f3ea36-be72-42ab-9081-7a3faa01f818', 'event_hash':
'0165a105b59ac11331e460b3c211ff0b', 'event_type': 'SESSION_DISCONNECTION',
'recorded_at': '2023-04-07 18:33:30', 'event_data': {'duration':
'0:00:01'}} rt=2023-04-07 18:33:30 src=5.676.120.935 suser=JoPo4ka
```

## Детектор сканеров

Генерирование инцидента при обнаружении множественных попыток доступа к целевой системе без дальнейшей авторизации в течение короткого времени.

```
Apr 7 17:30:54 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|NL-846581|3|act=SKDPUNT.INCIDENT.NEW cat=NO_LOGIN
cnt=0.5 reason=None rt=2022-04-07 17:31:19 suser=None
```

## Индикаторы взрывной активности

Генерирование инцидента при обнаружении высокого уровня активности целевой учетной записи:

- превышение порога максимального количества событий в рамках пользовательской сессии целевой системы;
- превышение порога максимального количества соединений с целевыми системами в течение дня;

- превышение порога максимального количества переданных и полученных файлов в рамках пользовательской сессии целевой системы.

```
Apr 25 18:16:13 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|AL-1000028|8|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=ACTIVITY_LEVEL cnt=30 destinationServiceName=SSH
dhost=IETJSG-99.608.7.86 dst=8.09.80.4 duid=connections dvchost=skdpu_test
externalId=6cec02ba9f374c04005056b7712f reason={'session_id':
'6cec02ba9f374c04005056b7712f', 'wabsession_id': '3d804f7a-468b-484d-8a8a-
d56d58867877', 'event_hash': '4cfe971ca0f66d1ca2f9704918c0a7e3',
'event_type': 'SESSION_DISCONNECTION', 'recorded_at': '2023-06-08
08:15:04', 'event_data': {'duration': '0:00:00'}} rt=2023-04-25 08:15:04
src=55.763.331.55 suser=burstperson
```

## Количество переданных файлов

Генерирование инцидента при обнаружении передачи большого количества файлов в рамках пользовательской сессии целевых систем.

```
Apr 25 16:37:07 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|FT-1000021|6|act=SKDPUNT.INCIDENT.NEW
app=SSH cat=FILE_TRANSFER cnt=20 destinationServiceName=SSH
dhost=GIS-13 dst=172.16.1.13 duid=svc10101 dvchost=basion7
externalId=f7f791f8c0f4aec1536c11a5d0d8 reason={'wabsession_id':
'a8693c22-e194-46bd-aab6-2a9c87b4d0fb', 'session_id':
'f7f791f8c0f4aec1536c11a5d0d8', 'event_type': 'SESSION_DISCONNECTION',
'event_hash': '05ad238b3a26aa380489d2637553af27', 'recorded_at':
'2023-04-25 17:40:24', 'event_data': {'duration': '1:11:53'}} rt=2023-04-25
17:40:24 src=192.168.0.113 suser=b.dylan
```

## Создание инцидента вручную

Создание вручную инцидента, обнаруженного в рамках анализа пользовательских сессий целевых систем.

```
Feb 20 18:06:27 skdpu-nt CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00001|MAN-846546|3|act=SKDPUNT.INCIDENT.NEW app=RDP
cat=MANUAL cnt=10 destinationServiceName=RDP dhost=rdp dst=10.100.50.16
duid=usr dvchost=avs externalId=17f0d1478c8aa207000c29b8a9a2 reason=None
rt=2022-02-18 16:45:25 src=192.168.20.60 suser=admin$
```

## SKDPUNT.INCIDENT.00002

## Изменение инцидента

Изменение параметров обнаруженного инцидента.

```
Feb 20 18:00:27 skdpunt-test CEF:0|IT-Bastion LLC|SKDPU-NT|2.1.58|
SKDPUNT.INCIDENT.00002|KPE-846544|3|act=IncidentChange cat=Incident
dst=10.100.1.181 rt=2022-02-20 18:00:27.606572 src=172.16.30.63 suser=admin
```

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

<b>APP</b>	Remote APP — Удаленное приложение.
<b>CEF</b>	Common Event Format разработан для унификации событий от разных технических средств. В качестве транспортного механизма CEF использует стандарт syslog-сообщения.
<b>IP</b>	Internet Protocol (межсетевой протокол) — маршрутизируемый протокол сетевого уровня стека TCP/IP.
<b>JSON</b>	JavaScript Object Notation — текстовый формат обмена данными, основанный на JavaScript.
<b>LDAP</b>	Lightweight Directory Access Protocol (легковесный протокол доступа к каталогам) — протокол прикладного уровня для доступа к службе каталогов X.500
<b>RDP</b>	Remote Desktop Protocol — протокол удаленного рабочего стола
<b>RLOGIN</b>	Remote LOGIN — удалённый вход в систему.
<b>SSH</b>	Secure SHell (безопасная оболочка) — протокол защищенной передачи данных.
<b>TELNET</b>	TErminaL NETwork — сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP).
<b>URL</b>	Uniform Resource Locator (унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов.
<b>VNC</b>	Virtual Network Computing — система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).

