События безопасности

Описание применяемых технических мер, обеспечивающих регистрацию событий ИБ.

Для регистрации событий ИБ:

(а) определён перечень регистрируемых событий

(б) в базе данных Postgres задана отдельная схема **evtlog**, в которой определена таблица **security_event** для хранения событий ИБ

(в) на уроне операционной системы используется syslog для трансляции событий во внешние SIEM и/или хранения выделенного текстового лог-файла в /var/log/cloudmaster-secevent.log

(г) в исполняемых компонентах cm-idm.jar и cm-broker.jar встроен механизм создания и отправки события ИБ одновременно в базу данных (evtlog.security_event) и в syslog операционной системы

(д) события ИБ записываются в Common Event Format (CEF) виде

CEF-формат записи события ИБ

CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]

Перечень регистрируемых событий

Запись о любом событии информационной безопасности выполняется в соответствии с форматом CEF:

- начальный заголовок записи (CEF:Version) - CEF:0
- поле Device Vendor содержит "GPN"
- поле Device Product содержит "InferitCloudMaster"
- поле Device Version содержит номер версии Cloudmaster - "0.0.1"

последующие поля Device Event Class ID, Name, Severity и Extension содержат значения в соответствии с таблицей событий

Описание события.	**Идентификатор события/ DeviceEventClassID**	**Наименование события/ Name**	**Уровень важности события/ Severity**	**Регистрируемые параметры/ Extension**
Успешный вход пользователя в систему.	CM-00010	Пользователь прошёл аутентификацию	3	• **end**={Дата время (epoch in ms)} • **suser**={sAMAccountName пользователя из LDAP} • **suid**={GUID пользователя в LDAP} • **cs1**={Внутренний идентификатор сессии пользователя} • **dproc**={Useragent HTTP-запроса пользователя} • **src**={IP v4 пользователя - источника запроса} • **dst**={IP v4 API-сервера Cloudmaster} • **dhost**={FQDN (имя хоста) API-сервера Cloudmaster} • **outcome**="Success"
Ошибка при попытке аутентификации.	CM-00011	Пользователь не прошёл аутентификацию	7	• **end**={Дата время (epoch in ms)} • **suser**={sAMAccountName пользователя из LDAP} • **dproc**={UserAgent HTTP-запроса пользователя} • **reason**="Ошибка аутентификации на стороне LDAP-сервера" • **src**={IP v4 пользователя - источника запроса} • **dst**={IP v4 API-сервера Cloudmaster} • **dhost**={FQDN (имя хоста) API-сервера Cloudmaster} • **outcome**="Failure"
Завершение сеанса работы пользователя.	CM-00020	Сеанс пользователя завершён	3	• **end**={Дата время (epoch in ms)} • **src**={IP v4 пользователя - источника запроса} ○ Может отсутствовать, если сеанс был завершён автоматически по истечении установленного периода времени. • **suser**={sAMAccountName пользователя из LDAP} • **suid**={GUID пользователя в LDAP}

				• **outcome**=Success
Создан новый пользователь.	CM-00030	Создан новый пользователь	3	• **end**={Дата время (epoch in ms)} • **duid**={GUID пользователя в LDAP} • **duser**={sAMAccountName пользователя из LDAP} ○ IP источника запроса не фиксируется, т.к. пользователи создаются автоматически при первой успешной аутентификации • **outcome**="Success"
Изменены параметры пользователя.	CM-00040	Изменены параметры пользователя	4	• **end**={Дата время (epoch in ms)} • **duid**={GUID пользователя в LDAP} • **duser**={sAMAccountName пользователя из LDAP} ○ IP источника запроса не фиксируется, т.к. параметры пользователя изменяются автоматически при успешной аутентификации на основе данных из LDAP • **outcome**="Success"

Изменены роли пользователя.	CM-00050	Изменены роли пользователя	4	• **end**={Дата время (epoch in ms)}
				• **duid**={GUID пользователя в LDAP}
				• **duser**={sAMAccountName пользователя из LDAP}
				  ○ IP источника запроса не фиксируется, т.к. параметры пользователя изменяются автоматически при успешной аутентификации на основе данных из LDAP
				• **cs1Label**="Старый список ролей"
				  ○ **cs1**={Старый список ролей}
				• **cs2Label**="Новый список ролей"
				  ○ **cs2**={Новый список ролей}
				• **outcome**="Success"

Изменены группы	CM-00060	Изменены группы	5	• **end**={Дата время (epoch in ms)}

безопасности ролей.		безопасности ролей		• **src**={IP v4 пользователя - источника запроса} • **suser**={sAMAccountName пользователя из LDAP - кто меняет} • **suid**={GUID пользователя в LDAP} • **cs1Label**="JSON запроса" ○ **cs1**={JSON с новыми группами для ролей} • **outcome**="Success"
Изменены параметры интеграции с LDAP.	CM-00070	Изменена интеграция с LDAP	7	• **end**={Дата время (epoch in ms)} • **src**={IP v4 пользователя - источника запроса} • **suser**={sAMAccountName пользователя из LDAP - кто меняет} • **suid**={GUID пользователя в LDAP} • **cs1Label**="JSON запроса" ○ **cs1**={JSON с новыми параметрами для LDAP} • **outcome**="Success"
Попытка выполнить неразрешённую операцию.	CM-00080	Недостаточно прав для операции	7	• **end**={Дата время (epoch in ms)} • **src**={IP v4 пользователя - источника запроса} • **suser**={sAMAccountName пользователя из LDAP} • **suid**={GUID пользователя в LDAP} • **dst**={IP v4 API-сервера Cloudmaster} • **dhost**={FQDN (имя хоста) API-сервера Cloudmaster} • **request**={Идентификатор ресурса URI - endpoint API-метода} • **requestMethod**={Тип HTTP запроса (GET, POST…)} • **reason**="Пользователь не имеет прав на данную операцию" • **outcome**="Failure"
Обнаружен проблемный SSL-сертификат.	CM-00090	Проблемный SSL-сертификат	5	• **end**={Дата время (epoch in ms)} • **dst**={IP v4 сервера с проблемным сертификатом} • **dhost**={FQDN (имя хоста) сервера с проблемным сертификатом} • **app**="HTTPS" *или* "LDAPS"

				• **reason**="Истекла дата действия сертификата" *или* "Сертификат отозван" • **outcome**="Failure"
Пользователь создал новую сущность.	CM-00100	Создана новая сущность	2	• **end**={Дата время (epoch in ms)} • **src**={IP v4 пользователя - источника запроса} • **suser**={sAMAccountName пользователя из LDAP} • **suid**={GUID пользователя в LDAP} • **dst**={IP v4 API-сервера Cloudmaster} • **dhost**={FQDN (имя хоста) API-сервера Cloudmaster} • **request**={Идентификатор ресурса URI - endpoint API-метода} • **requestMethod**="POST" • **cs1Label**="JSON запроса" ○ **cs1**={JSON с параметрами новой сущности} • **outcome**="Success"
Изменён программный компонент или файл конфигурации	CM-00110	Изменён компонент системы	5	• **end**={Дата время (epoch in ms)} • **dst**={IP v4 API-сервера Cloudmaster} • **dhost**={FQDN (имя хоста) API-сервера Cloudmaster} • **filePath**={ПОЛНЫЙ ПУТЬ К ИЗМЕНЁННОМУ ФАЙЛУ} • **oldFileHash**={СТАРЫЙ КОНТРОЛЬНЫЙ ХЭШ-КОД ФАЙЛА} • **fileHash**={НОВЫЙ КОНТРОЛЬНЫЙ ХЭШ-КОД ФАЙЛА} • **outcome**="Success"

Настройка интеграции с внешней SEIM-системой

На уровне операционной системы от имени суперпользователя в каталоге /etc/rsyslog.d/ необходимо создать простой текстовый конфигурационный файл siem.conf с таким содержимым

```
:msg, contains, "InferitCloudMaster" @10.10.10.11
```

где вместо "10.10.10.11" необходимо указать IP-адрес SIEM-системы, принимающей сообщения syslog

Перезапустить сервис rsyslog командой

```
service rsyslog restart
```

Пример записей событий из лог-файла:

Nov 8 15:07:00 dev java[462298]: 08-11-2024 15:07:00.819 [http-nio-1999-exec-3] INFO ru.cloudmaster.seclog.SyslogSender.log - CEF:0|GPN|InferitCloudMaster|0.0.1|CM-00010|Пользователь прошёл аутентификацию|3|end=1731067620819 suser=budget.owner suid=S-1-5-21-1007706797-3498080564-133587131-25605 cs1Label=Внутренний идентификатор сессии пользователя cs1=b63c9410-a289-480f-ab4b-5cc23710d3e2 dproc=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 src=172.22.100.8 dst=172.22.100.222 dhost=adm.broker.inferit outcome=Success

Nov 8 15:06:35 dev java[480293]: 08-11-2024 15:06:35.391 [http-nio-8081-exec-6] INFO ru.cloudmaster.seclog.SyslogSender.log - CEF:0|GPN|InferitCloudMaster|0.0.1|CM-00080|Недостаточно прав для операции|7|end=1731067595391 src=172.22.100.8 suser=budget.owner suid=S-1-5-21-1007706797-3498080564-133587131-25605 dst=172.22.100.222 dhost=adm.broker.inferit request=/data/broker/api/v1/products/35337cfd-4a82-4740-889d-d2de4a0f1cc3 requestMethod=GET reason=Пользователь не имеет прав на данную операцию outcome=Failure

Nov 7 15:49:47 dev java[462298]: 07-11-2024 15:49:47.322 [http-nio-1999-exec-6] INFO ru.cloudmaster.seclog.SyslogSender.log - CEF:0|GPN|InferitCloudMaster|0.0.1|CM-00040|Изменены параметры пользователя|4|end=1730983787321 duid=S--84-91488718 duser=hfLpgPYKQi8eyNor/VDPQ3gFKzxK+mGWATZkyjWxqLA= outcome=Success