КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Регистрация событий в частном облаке

Редакция: 20.04.2026

Содержание

Заявление об авторских правах

1 Введение

В настоящем документе описаны технические меры по регистрации событий информационной безопасности, а также событий, связанных с изменением конфигурации.

2 Регистрация событий

Кибер Бэкап Облачный поддерживает возможность передачи событий из журнала аудита в SIEM-систему. В Руководстве администратора компании приведены более подробные сведения о журнале аудита и инструкции по настройке отправления записей журнала аудита на удаленный Syslog-сервер. Перечень регистрируемых событий приведён в разделе "Регистрируемые события" (стр. 6).

Примечание
Регистрация событий Кибер Инфраструктуры не поддерживается.

На уровне операционной системы регистрация событий обеспечивается стандартным пакетом auditd для РЕД ОС. Правила устанавливаются в конфигурационном файле (см. "Приложение 1. Применяемые правила аудита" (стр. 34)).

Для передачи данных в централизованное хранилище или SIEM-систему на виртуальных машинах настроен анализатор сетевых пакетов Auditbeat, который пересылает данные в СУБД Redis. Данные из неё получает серверный конвейер обработки данных Logstash, на уровне которого можно настроить правила выгрузки событий безопасности во внешнюю систему.

Например, для выгрузки событий во внешние системы по стандарту Syslog необходимо добавить в блок output конфигурации Logstash следующие строки:

```
if "auditd" in [service][type] {
  udp {
    <параметры_подключения>
  }
}
```

Где <параметры_подключения> – это параметры подключения ко внешней системе по стандарту Syslog.

3 Регистрируемые события

В журнале аудита Кибер Бэкапа Облачного фиксируются события следующих категорий:

- оповещения;
- действия с планами защиты;
- действия с устройствами и их группами;
- аутентификация и авторизация;
- действия с тенантами;
- резервное копирование;
- лицензирование;
- регистрация агентов.

Более подробная информация о записываемых в журнал событиях приведена в таблицах ниже.

3.1 События оповещений

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Оповещение создано (Alert created)	Информация (info)	AlertManagement	Alert	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount	-	Создать (Create)	200	Имя отдела	<IP-адрес инициатора>:<порт>
Оповещени	Информаци	AlertManageme	Alert	Имя	• Plan и имя	ServiceAccou	-	Обновит	200	Имя	<IP-адрес

е обновлено (Alert updated)	я (info)	nt		ресурса	(идентификатор) плана; • resource и имя (идентификатор) ресурса.	nt		ь (Update)		отдела	инициатора>:<порт>
Оповещение отменено (Alert reset)*	Информация (info)	AlertManagement	Alert	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или user	Имя пользователя	Удалить (Delete)	204	Имя отдела	<IP-адрес инициатора>:<порт>

* При использовании массового действия с оповещениями, например, **Очистить всё**, для каждого оповещения будет создана отдельная запись в журнале аудита.

3.2 События действий с планами защиты

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
План защиты создан (Backup plan created)	Информация (info)	PolicyManagement	Policy	Имя плана	Location и имя хранилища	User	Имя пользователя	Создать (Create)	20x	Имя тенанта	<IP-адрес инициатора>:<порт>
План защиты	Информация (info)	PolicyManagement	Policy	Имя плана	• Resource и имя	User	Имя пользовате	Обновить (Update)	20x	Имя тенанта	<IP-адрес инициатора>:<п

обновлён (Backup plan updated)					(идентификатор) ресурса; • location и имя хранилища.		ля				орт>
План защиты удалён (Backup plan deleted)	Информация (info)	PolicyManagement	Policy	Имя плана	• Resource и имя (идентификатор) ресурса; • location и имя хранилища.	User	Имя пользователя	Удалить (Delete)	204	Имя тенанта	<IP-адрес инициатора>:<порт>
Статус установки плана (Plan deployment state)	Информация (info)	PolicyManagement	Policy	Имя плана	• Location и имя хранилища; • DeploymentState и идентификатор статуса.	User	-	Применить (Apply)	200	Имя пользователя **Примечание** Если действие выполняется на уровне тенанта типа **Клиент**, то в поле **Имя тенанта** будет указано имя учётной записи администратора отдела.	-
Политика примене	Информация (info)	PolicyManagement	PolicyApplication	Имя плана	• Resource и имя	User	Имя пользовате	Обновить (Update)	20x	Имя тенанта	<IP-адрес инициатора>:<п

на к устройст ву (Policy applied to workload)					(идентифика тор) ресурса; • location и имя хранилища.		ля				орт>

3.3 События действий с устройствами и их группами

Событие	Серьёзнос ть	Категория (домен)	Тип объекта события	Назван ие объекта	Связанные объекты	Тип инициато ра	Инициатор события	Действ ие	Результ ат действи я	Тенант	IP-адрес инициатора
Устройство создано (Workload created)	Информац ия (info)	WorkloadManage ment	Workload	Имя ресурса	Agent и имя (идентификат ор) агента	User	-	Создать (Create)	200	Имя пользовате ля	-
Устройство обновлено (Workload updated)	Информац ия (info)	WorkloadManage ment	Workload	Имя ресурса	Agent и имя (идентификат ор) агента	User	-	Обнови ть (Update)	200	Имя пользовате ля	-
Устройство удалено (Workload deleted)	Информац ия (info)	WorkloadManage ment	Workload	Имя ресурса	Agent и имя (идентификат ор) агента	User	-	Удалить (Delete)	200	Имя пользовате ля	-
Группа устройств создана (Workload group	Информац ия (info)	WorkloadManage ment	GroupMember ship	Имя группы	Нет	User	Имя пользовате ля	Создать (Create)	201	Имя тенанта	<IP-адрес инициатора>:<п орт>

created)											
Участники добавлены в статическую группу устройств (Workload static group member added)	Информация (info)	WorkloadManagement	GroupMembership	Имя группы	Resource и имя (идентификатор) ресурса	User	-	Добавить (Add)	200	Имя тенанта	-
Участники добавлены в динамическую группу устройств (Workload dynamic group member added)	Информация (info)	WorkloadManagement	GroupMembership	Имя группы	Resource и имя (идентификатор) ресурса	User	-	Добавить (Add)	200	Имя тенанта	-
Участники удалены из статической группы устройств (Workload static group member	Информация (info)	WorkloadManagement	GroupMembership	Имя группы	Resource и имя (идентификатор) ресурса	User	-	Удалить (Remove)	200	Имя тенанта	-

removed)											
Участники удалены из динамической группы устройств (Workload dynamic group member removed)	Информация (info)	WorkloadManagement	GroupMembership	Имя группы	Resource и имя (идентификатор) ресурса	User	-	Удалить (Remove)	200	Имя тенанта	-
Группа устройств удалена (Workload group deleted)	Информация (info)	WorkloadManagement	GroupMembership	Имя группы	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	<IP-адрес инициатора>:<порт>

3.4 События аутентификации и авторизации

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Успешный вход в систему (Logged in)	Информация (info)	Auth	Session	Имя пользователя	User и имя (идентификатор) пользователя	User	Имя пользователя	Вход в систему (Login)	200	Имя учётной записи	IP-адрес машины, с которой был выполнен вход

Превышено число попыток войти в систему (Exceeded the number of login attempts)	Критично (critical)	Auth	Session	Имя пользователя	User и имя (идентификатор) пользователя	ServiceAccount	Имя пользователя	Вход в систему временно заблокирован (Login::TemporaryLock)	429	Имя тенанта, имя отдела	IP-адрес машины, с которой был выполнен вход
Успешный выход из системы (Logged out)	Информация (info)	Auth	Session	Имя пользователя	User и имя (идентификатор) пользователя	User	Имя пользователя	Выход из системы (Logout)	200	Имя учётной записи	IP-адрес машины, с которой был выполнен выход
Документ был подписан (Legal document signed)	Информация (info)	Auth	LegalDocument	-	User и имя (идентификатор) пользователя	User	Имя пользователя	Подписать (Sign)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Токен доступа выписан (Access token issued)	Информация (info)	Auth	Token	-	User и имя (идентификатор) пользователя	ServiceAccount	-	Выписать (Issue)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

3.5 События действий с тенантами

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Тенант создан (Tenant created)	Информация (info)	IAM	Tenant	Имя созданного тенанта	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант обновлён (Tenant updated) **Примечание** При обновлении тенанта типа **Клиент**.	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант обновлён (Tenant updated)	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	User и имя пользователя	User	-	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено

Примечание При обновлении родительского тенанта.											действие
Тенант обновлён (Tenant updated) **Примечание** При обновлении имени тенанта или при включении тенанта.	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант отключён (Tenant disabled)	Предупреждение (warning)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант удалён (Tenant deleted)	Предупреждение (warning)	IAM	Tenant	Имя удалённого тенанта	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено

											действие
Изменение привилегий пользователя (User privileges updated) **Примечание** При назначении привилегий пользователю.	Информация (info)	IAM	UserPrivileges	-	User и имя (идентификатор) пользователя, для которого назначаются привилегии	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Изменение привилегий пользователя (User privileges updated) **Примечание** При отзыве привилегий пользователя.	Информация (info)	IAM	UserPrivileges	-	User и имя (идентификатор) пользователя, у которого отзываются привилегии	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя пользователя	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя создана (User created)	Информация (info)	IAM	User	Имя пользователя	Нет	User	Имя пользователя	Создать (Create)	200	Имя пользователя	IP-адрес машины, с которой было совершено действие

Учётная запись пользователя обновлена (User updated)	Информация (info)	IAM	User	Имя (логин) обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя отключена (User disabled)	Предупреждение (warning)	IAM	User	Имя обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя включена (User enabled)	Предупреждение (warning)	IAM	User	Имя изменённого пользователя	Нет	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Пароль сброшен (User reset)	Предупреждение (warning)	IAM	User	Имя обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Учётная	Критично (critical)	IAM	User	Имя пользоват	Нет	User	Имя пользовате	Удалить (Delete)	200	Имя тенанта	IP-адрес

запись пользователя удалена (User deleted)				еля			ля				машины, с которой было совершено действие
Служебная учётная запись создана (Account created) **Примечание** При работе с API-клиентами.	Информация (info)	IAM	ServiceAccount	Имя API-клиента	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служебная учётная запись обновлена (Account updated) **Примечание** При работе с API-клиентами.	Информация (info)	IAM	ServiceAccount	Имя API-клиента	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служебная учётная запись удалена (Account	Информация (info)	IAM	ServiceAccount	Имя API-клиента	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было

deleted) **Примечание** При работе с API-клиентами.											совершено действие
Секрет служебной учётной записи сброшен (Account secret reset) **Примечание** При работе с API-клиентами.	Информация (info)	IAM	ServiceAccount	Имя API-клиента	Нет	User	Имя пользователя	Сбросить (Reset)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Юридический документ добавлен (Legal document created) **Примечание** При работе с лицензионными документами.	Информация (info)	Auth	LegalDocument	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Юридический	Информация	Auth	LegalDocum	Версия	Нет	User	Имя	Опубликов	200	Имя	IP-адрес

документ опубликован (Legal document published) **Примечание** При работе с лицензионными документами.	(info)		ent	документа (например, Version 2024-04-03)			пользователя	ать (Publish)		тенанта	машины, с которой было совершено действие
Юридический документ удалён (Legal document deleted) **Примечание** При работе с лицензионными документами.	Информация (info)	Auth	LegalDocument	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Документ был подписан (Legal document signed)	Информация (info)	Auth	LegalDocument	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Подписать (Sign)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служба	Информация	LicenseManage	Application	Cyber	Нет	User	Имя	Включение	200	Имя	IP-адрес

добавлена для тенанта (Service added for tenant) **Примечание** При добавлении функциональности Кибер Инфраструктуры.	(info)	ment		Infrastructure			пользователя	(Enable)		тенанта	машины, с которой было совершено действие
Служба удалена для тенанта (Service removed from tenant) **Примечание** При отключении функциональности Кибер Инфраструктуры.	Информация (info)	LicenseManagement	Application	Cyber Infrastructure	Нет	User	Имя пользователя	Отключение (Disable)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служба добавлена для тенанта (Service added for tenant)	Информация (info)	LicenseManagement	Application	Cyber Protection	Нет	User	Имя пользователя	Включение (Enable)	200	Имя тенанта	IP-адрес машины, с которой было совершен

Примечание При включении у тенанта прочих консолей (Cyber Protection).											о действие
Служба удалена для тенанта (Service removed from tenant) **Примечание** При отключении у тенанта прочих консолей (Cyber Protection).	Информация (info)	LicenseManagement	Application	Cyber Protection	Нет	User	Имя пользователя	Отключение (Disable)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

3.6 События резервного копирования

Событие	Серьёзность	Категория (домен)	Тип объекта событи	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора

			я								
Резервное копирование помещено в очередь (Backup queued)	Информация (info)	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или User	• Имя пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	Создать (Create)	200	Имя пользователя	-
Резервное копирование назначено агенту (Backup assigned to agent)	Информация (info)	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или User	• Имя пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	Назначить (Assign)	200	Имя пользователя	-
Ошибка при назначении резервного копирования агенту (Error assigning backup to agent)	Критично (critical)*	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или User	• Имя пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	Назначить (Assign)	500	Имя пользователя	-
Резервное	Информация	TaskManagem	Task	Имя	• Plan и имя	ServiceAcco	• Имя	Начать	200	Имя	-

копирование начато (Backup started)	(info)	ent		ресурса	(идентификатор) плана; • resource и имя (идентификатор) ресурса.	unt или User	пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	(Start)		пользователя	
Резервное копирование выполнено (Backup completed)	Информация (info)	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или User	• Имя пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	Завершить (Complete)	200	Имя пользователя	-
Резервное копирование завершилось с предупреждением (Backup finished with warning)	Предупреждение (warning)*	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	ServiceAccount или User	• Имя пользователя (если тип инициатора **User**); • '-' (если тип инициатора **ServiceAccount**).	Завершить (Complete)	200	Имя пользователя	-
Резервное копирование завершилось с ошибкой	Критично (critical)*	TaskManagement	Task	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и	ServiceAccount или User	• Имя пользователя (если тип инициатора	Завершить (Complete)	500	Имя пользователя	-

(Backup failed)					имя (идентификатор) ресурса.		**User**); • '-' (если тип инициатора **ServiceAccount**).				
Задача на восстановление создана (Recovery task created)	Информация (info)	TaskManagement	Activity	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	User	Имя пользователя	Создать (Create)	200	Имя пользователя	-
Задача на восстановление запущена (Recovery task started)	Информация (info)	TaskManagement	Activity	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	User	Имя пользователя	Начать (Start)	200	Имя пользователя	-
Задача на восстановление выполнена (Recovery task completed)	Информация (info)	TaskManagement	Activity	Имя ресурса	• Plan и имя (идентификатор) плана; • resource и имя (идентификатор) ресурса.	User	Имя пользователя	Завершать (Complete)	200	Имя пользователя	-

* Серьёзность зависит от кода задачи: если она завершена с кодом **warning**, то Серьёзность – **предупреждение** (**warning**); если с кодом **error**, то Серьёзность – **критично** (**critical**).

3.7 События лицензирования

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Лицензия для тенанта включена (Tenant license enabled)	Информация (info)	LicenseManagement	OfferingItemCount	pw_pack... или pg_pack...	Нет	User	Имя тенанта	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Лицензия для тенанта включена (Tenant license enabled)	Информация (info)	LicenseManagement	OfferingItemCount	local_storage	Нет	User	Имя тенанта	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Успешное выключение лицензии для тенанта (Tenant license disabled)	Предупреждение (warning)	LicenseManagement	OfferingItemCount	pw_pack... или pg_pack...	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Квота для тенанта установлена (Tenant	Информация (info)	LicenseManagement	TenantQuota	pw_base... или pg_base...	Application, tenant	User	Имя тенанта	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было

quota set)											совершено действие

3.8 События регистрации агентов

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Регистрация агента завершена (Agent registered)	Информация (info)	SoftwareManagement	Agent	Имя агента (имя хоста)	Нет	ServiceAccount	-	Зарегистрировать (Register)	200	Имя отдела, в котором регистрируется агент	IP-адрес машины с агентом
Регистрация агента отозвана (Agent unregistered)	Информация (info)	SoftwareManagement	Agent	Имя агента (имя хоста)	Нет	ServiceAccount	-	Отменить регистрацию (Unregister)	200	Имя отдела, в котором отменяется регистрация агента	IP-адрес машины с агентом

Примечание При удалении агента с помощью интерфейса командной строки.											
Регистрация агента отозвана (Agent unregistered) **Примечание** При удалении агента с помощью консоли службы.	Информация (info)	SoftwareManagement	Agent	Имя агента (имя хоста)	Нет	User	Имя пользователя, инициировавшего удаление	Отменить регистрацию (Unregister)	200	Имя отдела, в котором отменяется регистрация агента	IP-адрес машины с агентом

4 Описание формата сообщений Syslog

4.1 Сообщения CEF (RFC 3164)

Сообщение состоит из Syslog-заголовка (Syslog RFC 3164 header) и CEF-сообщения (CEF msg) и имеет следующую структуру:

```
<PRI> TIMESTAMP HOSTNAME TAG: CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class Id|Name|Severity|[Extension]
```

Ниже приведено описание компонентов сообщения.

К Syslog-заголовку относятся:

- <PRI> – приоритет сообщения, значение которого определяется формулой:

  ```
  <PRI> = <Facility> x 8 + <Severity>
  ```

  Где:

  - <Facility> – параметр, который может принимать следующие значения:

Значение	Назначение
0	Kernel
1	User-level
2	Mail
3	Daemon
4	Security
5	Syslog
6	Printer
7	News
16–23	Local0–local7 (прикладное ПО)

  - <Severity> – параметр, который может принимать следующие значения:

Значение	Уровень	Условия использования
0	Emergency	Аварийное состояние
1	Alert	Необходимо срочное вмешательство
2	Critical	Критическая ошибка

3	Error	Ошибка
4	Warning	Предупреждение
5	Notice	Значимое событие
6	Info	Информационное сообщение
7	Debug	Отладочная информация

Например, если <Facility> = 16 (local0), <Severity> = 6 (info), то <PRI> = <Facility> x 8 + <Severity> = 16 x 8 + 6 = 134.

- TIMESTAMP – временная метка в формате BSD без указания года и часового пояса, имеющая вид: <MMM> <ДД> <чч>:<мм>:<сс>.

  В этом выражении:
  - <MMM> – первые три буквы названия месяца на английском языке, первая буква является заглавной.
  - <ДД> – день месяца одной или двумя цифрами. Если значение меньше 10, то день отделяется от месяца двумя пробелами, при этом ноль перед днём месяца не указывается.
  - <чч> – часы двумя цифрами (если значение меньше 10, то перед ним указывается ноль).
  - <мм> – минуты двумя цифрами (если значение меньше 10, то перед ним указывается ноль).
  - <сс> – секунды двумя цифрами (если значение меньше 10, то перед ним указывается ноль).

  Примеры значений TIMESTAMP: Jan 29 03:09:27, Nov 7 11:15:17.
- HOSTNAME – имя хоста (например, cp1).
- TAG – источник процесса. В его качестве может быть app[pid] (например, event-store[3924]).

Примечание
После TAG обязательно двоеточие.

К CEF-сообщению относятся:

- CEF:Version – номер версии формата CEF (например, CEF:1).
- Device Vendor – вендор продукта (например, Cyberprotect).
- Device Product – название продукта (например, CyberBackupCloud).
- Device Version – версия продукта (например, 18.5).
- Device Event Class Id – идентификатор типа события (например, BackupStart).
- Name – название события в человекочитаемом формате (например, Backup job started).
- Severity – параметр CEF-severity, принимающий значения, приведённые в таблице.

Значение	Уровень серьёзности
0–3	Low

4–6	Medium
7–8	High
9–10	Critical

- [Extension] (необязательно) – параметры сообщения в формате key=value (например, src=10.0.0.1 dst=10.0.0.5 suser=admin msg=Backup started).

  Более подробное описание параметров сообщений приведено в документе Implementing ArcSight Common Event Format (CEF).

Пример сообщения:

```
<134> Feb 24 06:31:14 dev01-cloud-event-store-744996bf97-5sp5r event-store[1]:
CEF:1|Cyberprotect|CyberBackupCloud|25.11|Session|Logged in|3|cat=Command
flexString1=2c448d4d-876d-432f-ab2d-e1e2973a76c5 flexString1Label=eventTenantUUID
flexString2=S_admin flexString2Label=eventTenantName src= requestClientApplication= act=Login
cn1=200 cn1Label=eventStatus end=2026-02-24 06:31:14.376999 +0000 UTC outcome=success
msg=Logged in dvc= dvchost=dev01-cloud-event-store-744996bf97-5sp5r dvcExternalId=
reportedResourceID= reportedResourceName=user cs6=Auth cs6Label=objectDomain
reportedResourceType=Session cs4= cs4Label=objectSubtype dst= cs7=00000000-0000-0000-
0000-000000000000 cs7Label=localityID sourceServiceName=management suid=d7638075-ad65-
4378-83a5-d32d568453bb cs3=User cs3Label=principalType suser=user spid=00000000-0000-
0000-0000-000000000000 cs1= cs1Label=oldValue cs2= cs2Label=newValue cs5=
cs5Label=changedField
```

4.2 Сообщения Syslog (RFC 5424)

Сообщение Syslog (SYSLOG-MSG) состоит из заголовка (header), параметров сообщения (structured-data) и самого сообщения (MSG). Оно имеет следующую структуру:

```
HEADER STRUCTURED-DATA MSG
```

Где:

- HEADER – компонент, включающий в себя:
  - <PRI> – приоритет сообщения, значение которого определяется формулой:

    ```
    <PRI> = <Facility> x 8 + <Severity>
    ```

    В этом выражении:

- <Facility> – параметр, который может принимать следующие значения:

Значение	Назначение
0	Kernel
1	User-level
2	Mail
3	Daemon
4	Security
5	Syslog
6	Printer
7	News
16–23	Local0–local7 (прикладное ПО)

- <Severity> – параметр, который может принимать следующие значения:

Значение	Уровень	Условия использования
0	Emergency	Аварийное состояние
1	Alert	Необходимо срочное вмешательство
2	Critical	Критическая ошибка
3	Error	Ошибка
4	Warning	Предупреждение
5	Notice	Значимое событие
6	Info	Информационное сообщение
7	Debug	Отладочная информация

- VERSION – версия (например, 1).
- TIMESTAMP – временная метка в соответствии с RFC3339 или ISO 8601, имеющая вид: <ГГГГ>-<ММ>-<ДД>T<чч>:<мм>:<сс><ЧАСОВОЙ ПОЯС>.

  Где:

  - <ГГГГ> – год четырьмя цифрами (например, 2026).
  - <ММ> – месяц двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 01).
  - <ДД> – день месяца двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 02).
  - T – разделитель времени.

- <чч> – часы двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 03).
- <мм> – минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 04).
- <сс> – секунды двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 05).
- <ЧАСОВОЙ ПОЯС> – смещение времени, которое может быть указано в виде символа Z (для формата UTC) или в виде ±<чч>:<мм> (например, +03:00 или -02:00).

Примеры значений TIMESTAMP:

- 2026-01-29T03:09:23-08:00;
- 2026-01-29T11:09:23Z.

- HOSTNAME – имя узла (например, cp1).
- APP-NAME – название приложения (например, CyberBackupCloud).
- PROCID – идентификатор процесса (PID), например, 3924.
- MSGID – тип или идентификатор события (например, BackupStarted).

- STRUCTURED-DATA – параметры события в формате key=value (например, [backup@32473 job="daily" status="started"]).

Примечание
Параметры определяются на уровне приложения.

Описание полей Syslog-сообщений приведено в таблице.

Категория	Ключ	SourceField	Описание
event	id	event.ID	Уникальный идентификатор события
event	category	event.Category	Категория события
event	version	event.Version	Версия
event	tenant_id	event.TenantUUID	Идентификатор тенанта
event	tracing_id	event.TracingUUID	Идентификатор трассировки
event	src_ip	event.SrcIP	IP-адрес инициатора действия
event	dst_ip	event.DstIP	IP-адрес цели воздействия
event	user_ agent	event.UserAgent	User-Agent клиента или приложения, выполнившего запрос
event	status	event.Status	Статус
object	id	object.ID	Уникальный идентификатор объекта

object	name	object.Name	Имя объекта в человекочитаемом формате
object	domain	object.Domain	Логический домен или пространство объекта
object	type	object.Type	Тип объекта
object	subtype	object.Subtype	Подтип и уточняющая классификация объекта
object	expr	object.Expr	Выражение, условие или фильтр, описывающие объект или набор объектов
object	scope_path	object.ScopePath	Расположение объекта в структуре
object	scope_expr	object.ScopeExpr	Выражение области действия (scope), определяющее группу объектов
principal	id	principal.ID	Уникальный идентификатор субъекта
principal	type	principal.Type	Тип субъекта (пользователь, сервис, роль и т. п.)
principal	name	principal.Name	Имя или логин субъекта
principal	session	principal.SessionUUID	Идентификатор сессии субъекта
locality	id	locality.ID	Идентификатор узла или локации выполнения события
locality	type	locality.Type	Тип локации (агент, сервер, кластер, узел и т. п.)
locality	version	locality.Version	Версия ПО или компонента, где произошло событие

- HEADER — описание события в человекочитаемом формате (например, Backup started).

Пример сообщения:

```
<134>1 2026-02-24T06:23:48Z dev01-cloud-event-store-744996bf97-5sp5r CyberBackupCloud 1 77261 [event category="Command" dst_ip="" id="019c8e51-7172-7da7-b304-b13add75c9dc" src_ip="" status="200" tenant_id="2c448d4d-876d-432f-ab2d-e1e2973a76c5" tracing_id="90128efb-6f51-df4a-42ec-9c65e86dfd17" user_agent="" version="1"][locality id="00000000-0000-0000-0000-000000000000" type="management" version=""][object domain="Auth" expr="" id="" name="user" scope_expr="" scope_path="" subtype="" type="Session"][principal id="d7638075-ad65-4378-83a5-d32d568453bb" name="user" session="00000000-0000-0000-0000-000000000000" type="User"] Session.Login.200
```

5 Приложение 1. Применяемые правила аудита

```
## ---------------------------- FILTERS ----------------------------
## Ignore SELinux AVC records
-a always,exclude -F msgtype=AVC
## Ignore current working directory records
-a always,exclude -F msgtype=CWD
## This is not very interesting and wastes a lot of space if the server is public
#facing
-a always,exclude -F msgtype=CRYPTO_KEY_USER
##Kaspersky
-a never,exit -S all -F dir=/opt/kaspersky/ -k soc_spam_filter
-a never,exit -S all -F dir=/etc/opt/kaspersky/ -k soc_spam_filter
-a never,exit -S all -F dir=/var/opt/kaspersky/ -k soc_spam_filter
-a never,exit -S all -F dir=/opt/kaspersky/klnagent64/sbin/ -k soc_spam_filter
#UNKNOWN
-a always,exclude -F msgtype=UNKNOWN[1332]
-a always,exclude -F msgtype=UNKNOWN[1333]
-a always,exclude -F msgtype=UNKNOWN[1334]
-a always,exclude -F msgtype=CAPSET
-a never,exit -F path=/sbin/consoletype -F perm=x -k soc_auditd2_sbin_exe
-a never,exit -F path=/sbin/ethtool -F perm=x -k soc_auditd2_sbin_exe
-a never,exit -F path=/sbin/lsmod -F perm=x -k soc_auditd2_sbin_exe
-a never,exit -F arch=b32 -S open,openat -F path=/proc/filesystems -k soc_auditd2_fs
-a never,exit -F arch=b64 -S open,openat -F path=/proc/filesystems -k soc_auditd2_fs
#Ignore cron events
-a never,user -F subj_type=crond_t
-a never,exit -S all -F subj_type=crond_t
# Vector
-a never,exit -F arch=b64 -S openat -F exe=/usr/bin/vector
-a never,exit -F arch=b32 -S openat -F exe=/usr/bin/vector
# exim4/logcheck
#-a never,exit -F arch=b32 -S execve -F exe=/usr/sbin/exim4 -F auid=logcheck
#-a never,exit -F arch=b64 -S execve -F exe=/usr/sbin/exim4 -F auid=logcheck
#lsattr
-a never,exit -F arch=b32 -S lstat,openat -F exe=/usr/bin/lsattr
-a never,exit -F arch=b64 -S lstat,openat -F exe=/usr/bin/lsattr
# stat lstat
-a never,exit -F arch=b64 -S lstat,stat -F exe=/usr/bin/bash
# duplicate with soc_auditd2_RootCMD
-a never,exit -F arch=b64 -S stat
# These executable files may produce a large amount of events.
# exclude bins (x64)
-a never,exit -F arch=b64 -S capset,setxattr,lsetxattr,fsetxattr,settimeofday,adjtimex,clock_
settime,socket,connect,accept4,accept,listen,execve,execveat,ptrace,setuid,setgid,setreuid,setregi
d -F exe=/usr/bin/vmtoolsd
-a never,exit -F arch=b64 -S capset,setxattr,lsetxattr,fsetxattr,settimeofday,adjtimex,clock_
settime,socket,connect,accept4,accept,listen,execve,execveat,ptrace,setuid,setgid,setreuid,setregi
d -F exe=/usr/sbin/haproxy
# exclude bins (x32)
-a never,exit -F arch=b32 -S capset,setxattr,lsetxattr,fsetxattr,settimeofday,adjtimex,clock_
```

```
settime,socket,connect,accept4,listen,execve,execveat,ptrace,setuid,setgid,setreuid,setregid -F
exe=/usr/bin/vmtoolsd
-a never,exit -F arch=b32 -S capset,setxattr,lsetxattr,fsetxattr,settimeofday,adjtimex,clock_
settime,socket,connect,accept4,listen,execve,execveat,setuid,setgid,setreuid,setregid -F
exe=/usr/sbin/haproxy
# reduce all find foundings
-a never,exit -F arch=b64 -S open,openat,newfstatat -F exe=/usr/bin/find
-a never,exit -F arch=b64 -S open,openat,newfstatat -F exe=/bin/find
-a never,exit -F arch=b64 -S execve -F exe=/usr/bin/sort
-a never,exit -F arch=b64 -S execve -F exe=/usr/bin/uniq
-a never,exit -F arch=b64 -S execve -F exe=/usr/bin/xargs
# because they read /etc/passwd
-a never,exit -F arch=b64 -S open,openat -F exe=/usr/bin/ps
-a never,exit -F arch=b64 -S open,openat -F exe=/usr/bin/top
-a never,exit -F arch=b64 -S open,openat -F exe=/usr/bin/htop
-a never,exit -F arch=b64 -S open,openat -F exe=/usr/bin/id
-a never,exit -F arch=b64 -S open,openat -F exe=/usr/bin/w.procps
## ------------------------------- MAIN RULES ------------------------------
##Changes to .bash_profile or .bashrc
-w /root/.bashrc -p wa -k soc_auditd_Profile
-w /root/.profile -p wa -k soc_auditd_Profile
-w /etc/profile -p wa -k soc_auditd_Profile
-w /etc/shells -p wa -k soc_auditd_Profile
-w /etc/bash.bashrc -p wa -k soc_auditd_Profile
-w /home/ -p x -k soc_auditd_Profile
-w /etc/profile.d/ -p wa -k soc_auditd2_T1546.004_shell_profiles
-a always,exit -F path=/etc/profile.d -F perm=wa -k soc_auditd2_Profile6
-w /root/.bash_profile -p wa -k soc_auditd2_T1546_Event_Triggered_Execution
-w /root/.bash_login -p wa -k soc_auditd2_Profile7
-w /root/.bash_logout -p wa -k soc_auditd2_Profile8
-w /etc/bash.bash_logout -p wa -k soc_auditd2_Profile9
-w /root/ -p x -k soc_auditd2_Profile10
##AuditD change config
-w /etc/audit/ -p wa -k soc_auditd_Changeconfig1
-w /etc/libaudit.conf -p wa -k soc_auditd_Changeconfig2
-w /etc/audisp/ -p wa -k soc_auditd_Changeconfig3
-w /sbin/auditctl -p x -k soc_auditd_Changeconfig4
-w /sbin/auditd -p x -k soc_auditd_Changeconfig5
-w /usr/sbin/augenrules -p x -k soc_auditd_Changeconfig6
-w /var/log/audit -p rwxa -k soc_auditd2_Changeconfig7
-w /sbin/augenrules -p x -k soc_auditd_Changeconfig8
-w /etc/audit/rules.d/ -p wa -k soc_auditd2_Changeconfig9
##Binary Padding
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k soc_auditd_Binarypadding1
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k soc_auditd_Binarypadding2
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k soc_auditd_Binarypadding3
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k soc_auditd_Binarypadding4
##IPTabbles execution
```

```
-w /usr/sbin/iptables -p x -k soc_auditd_Firewall1
-w /usr/sbin/xtables-nft-multi -p x -k soc_auditd_Firewall2
-w /usr/sbin/xtables-legacy-multi -p x -k soc_auditd_Firewall3
-w /usr/sbin/arptables -p x -k soc_auditd_Firewall4
-w /usr/sbin/ebtables -p x -k soc_auditd_Firewall5
-w /sbin/xtables-nft-multi -p x -k soc_auditd_Firewall6
-w /usr/sbin/xtables-multi -p x -k soc_auditd2_iptables_xtables7
-w /usr/sbin/nft -p x -k soc_auditd_Firewall8
-w /sbin/ip6tables -p x -k soc_auditd_Firewall9
-w /sbin/iptables -p x -k soc_auditd_Firewall0
-w /sbin/xtables-nft-multi -p x -k soc_auditd2_Firewall
-w /sbin/xtables-legacy-multi -p x -k soc_auditd2_Firewall2
-w /sbin/arptables -p x -k soc_auditd2_Firewall3
-w /sbin/ebtables -p x -k soc_auditd2_Firewall7
-w /sbin/ipset -p x -k soc_auditd2_Firewall18
-w /sbin/efw -p x -k soc_auditd2_Firewall19
##Sudo and Sudo Caching
-w /bin/su -p x -k soc_auditd_Sudo1
-w /usr/bin/sudo -p x -k soc_auditd_Sudo2
-w /usr/bin/visudo -p x -k soc_auditd_Sudo3
-w /etc/sudoers -p wa -k soc_auditd2_T1078.003_1_sudo_actions
-w /etc/sudoers.d -p rwa -k soc_auditd2_Sudo3
-a always,exit -F arch=b64 -F dir=/home -F uid=0 -F auid>=1000 -F auid!=-1 -C auid!=obj_uid -k soc_
auditd_Sudo4
-a always,exit -F arch=b32 -F dir=/home -F uid=0 -F auid>=1000 -F auid!=-1 -C auid!=obj_uid -k soc_
auditd_Sudo5
-a always,exit -S all -F path=/etc/sudoers -F perm=r -F auid!=-1 -k soc_auditd2_sudoers_read
-a always,exit -F arch=b32 -F path=/etc/sudoers -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd2_ACCOUNT_DISC
-a always,exit -F arch=b64 -F path=/etc/sudoers -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd2_ACCOUNT_DISC
##Data Edit
-w /usr/bin/mv -p x -k soc_auditd_DataEdit1
-w /usr/bin/cp -p x -k soc_auditd_DataEdit2
-w /usr/bin/dd -p x -k soc_auditd_DataEdit3
-w /bin/mv -p x -k soc_auditd_DataEdit4
-w /bin/cp -p x -k soc_auditd_DataEdit5
-w /bin/dd -p x -k soc_auditd_DataEdit6
##Suspicious actions: Ptrace System Calls
##-a always,exit -F arch=b64 -S ptrace -k soc_auditd_Ptrace
##-a always,exit -F arch=b32 -S ptrace -k soc_auditd_Ptrace
-a always,exit -F arch=b32 -S ptrace -F a0=0x4 -F key=soc_auditd_Ptrace1
-a always,exit -F arch=b64 -S ptrace -F a0=0x4 -F key=soc_auditd_Ptrace2
-a always,exit -F arch=b32 -S ptrace -F a0=0x5 -F key=soc_auditd_Ptrace3
-a always,exit -F arch=b64 -S ptrace -F a0=0x5 -F key=soc_auditd_Ptrace4
-a always,exit -F arch=b32 -S ptrace -F a0=0x6 -F key=soc_auditd_Ptrace5
-a always,exit -F arch=b64 -S ptrace -F a0=0x6 -F key=soc_auditd_Ptrace6
-a always,exit -F arch=b64 -S ptrace -F a0=0x0 -k soc_auditd2_api_ptrace7
-a always,exit -F arch=b64 -S ptrace -F a0=0x10 -k soc_auditd2_api_ptrace8
-a always,exit -F arch=b64 -S ptrace -F a0=0x11 -k soc_auditd2_api_ptrace9
-a always,exit -F arch=b64 -S ptrace -F a0=0x13 -k soc_auditd2_api_ptrace10
-a always,exit -F arch=b64 -S ptrace -F a0=0x4203 -k soc_auditd2_api_ptrace11
```

```
-a always,exit -F arch=b64 -S ptrace -F a0=0x4205 -k soc_auditd2_api_ptrace12
-a always,exit -F arch=b64 -S ptrace -F a0=0x4206 -k soc_auditd2_api_ptrace13
-a always,exit -F arch=b64 -S ptrace -F a0=0x4207 -k soc_auditd2_api_ptrace14
-a always,exit -F arch=b64 -S ptrace -F a0=0xd -k soc_auditd2_api_ptrace15
-a always,exit -F arch=b64 -S ptrace -F a0=0xf -k soc_auditd2_api_ptrace16
-a always,exit -F arch=b32 -S ptrace -F a0=0x0 -k soc_auditd2_api_ptrace16
-a always,exit -F arch=b32 -S ptrace -F a0=0x10 -k soc_auditd2_api_ptrace17
-a always,exit -F arch=b32 -S ptrace -F a0=0x11 -k soc_auditd2_api_ptrace18
-a always,exit -F arch=b32 -S ptrace -F a0=0x13 -k soc_auditd2_api_ptrace19
-a always,exit -F arch=b32 -S ptrace -F a0=0x4203 -k soc_auditd2_api_ptrace20
-a always,exit -F arch=b32 -S ptrace -F a0=0x4205 -k soc_auditd2_api_ptrace21
-a always,exit -F arch=b32 -S ptrace -F a0=0x4206 -k soc_auditd2_api_ptrace22
-a always,exit -F arch=b32 -S ptrace -F a0=0x4207 -k soc_auditd2_api_ptrace23
-a always,exit -F arch=b32 -S ptrace -F a0=0xd -k soc_auditd2_api_ptrace24
-a always,exit -F arch=b32 -S ptrace -F a0=0xf -k soc_auditd2_api_ptrace25
##Network share discovery
-w /usr/bin/showmount -p x -k soc_auditd_Network1
-w /usr/bin/exportfs -p x -k soc_auditd_Network2
-w /usr/bin/nmblookup -p x -k soc_auditd_Network3
-w /usr/sbin/showmount -p x -k soc_auditd_Network4
-w /usr/sbin/exportfs -p x -k soc_auditd_Network5
-w /usr/sbin/nmblookup -p x -k soc_auditd_Network6
-w /etc/exports -p wa -k soc_auditd_Network7
-w /etc/fstab -p wa -k soc_auditd_Network8
-w /usr/sbin/arp -p x -k soc_auditd_Network9
-w /bin/arp -p x -k soc_auditd_Network10
##System Information Discovery
-w /bin/uname -p x -k soc_auditd_SysDiscovery14
-w /bin/lsblk -p x -k soc_auditd_SysDiscovery15
-w /sbin/fdisk -p x -k soc_auditd_SysDiscovery16
-w /usr/bin/uname -p x -k soc_auditd_SysDiscovery1
-w /usr/bin/lscpu -p x -k soc_auditd_SysDiscovery2
-w /usr/bin/lsblk -p x -k soc_auditd_SysDiscovery3
-w /usr/bin/fdisk -p x -k soc_auditd_SysDiscovery4
-w /usr/bin/lsb_release -p x -k soc_auditd_SysDiscovery5
-w /usr/sbin/uname -p x -k soc_auditd_SysDiscovery6
-w /usr/sbin/lscpu -p x -k soc_auditd_SysDiscovery7
-w /usr/sbin/lsblk -p x -k soc_auditd_SysDiscovery8
-w /usr/sbin/fdisk -p x -k soc_auditd_SysDiscovery9
-w /usr/sbin/lsb_release -p x -k soc_auditd_SysDiscovery10
-w /etc/os-release -p rwxa -k soc_auditd_SysDiscovery11
-a always,exit -F arch=b32 -F path=/etc/hostname -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd_SysDiscovery12
-a always,exit -F arch=b64 -F path=/etc/hostname -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd_SysDiscovery13
##Valid Accounts
-w /usr/sbin/usermod -p x -k soc_auditd_ValidAccounts1
-w /usr/bin/passwd -p x -k soc_auditd_ValidAccounts2
##Process Discovery
-w /bin/ps -p x -k soc_auditd_ProcDiscovery8
-w /bin/grep -p x -k soc_auditd_ProcDiscovery9
-w /bin/pidof -p wxa -k soc_auditd_ProcDiscovery10
```

```
-w /sbin/pidof -p wxa -k soc_auditd_ProcDiscovery11
-a always,exit -F arch=b32 -F path=/sbin/killall5 -F auid>=1000 -F auid!=-1 -F perm=x -k soc_auditd_
SysDiscovery13
-a always,exit -F arch=b64 -F path=/sbin/killall5 -F auid>=1000 -F auid!=-1 -F perm=x -k soc_auditd_
SysDiscovery14
-w /usr/bin/ps -p x -k soc_auditd_ProcDiscovery1
-w /usr/bin/top -p x -k soc_auditd_ProcDiscovery2
-w /usr/sbin/lsof -p x -k soc_auditd_ProcDiscovery3
-w /usr/bin/lsof -p x -k soc_auditd_ProcDiscovery4
-w /usr/bin/grep -p x -k soc_auditd_ProcDiscovery5
-w /usr/bin/pidof -p wxa -k soc_auditd_ProcDiscovery6
-a always,exit -F arch=b32 -F path=/usr/sbin/killall5 -F auid>=1000 -F auid!=-1 -F perm=x -k soc_
auditd_SysDiscovery15
-a always,exit -F arch=b64 -F path=/usr/sbin/killall5 -F auid>=1000 -F auid!=-1 -F perm=x -k soc_
auditd_SysDiscovery16
##Data Compressed
-w /usr/bin/zip -p x -k soc_auditd_DataCompress1
-w /usr/bin/gzip -p x -k soc_auditd_DataCompress2
-w /usr/bin/tar -p x -k soc_auditd_DataCompress3
-w /bin/gzip -p x -k soc_auditd_DataCompress4
-w /bin/tar -p x -k soc_auditd_DataCompress5
##System Network Configuration Discovery
-a always,exit -F dir=/etc/NetworkManager/ -F perm=wa -k soc_auditd2_system_locale_network_
modifications
-a always,exit -F arch=b64 -F path=/proc/net/arp -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd2_T1018_Remote_system_Discovery1
-a always,exit -F arch=b64 -F path=/proc/net/tcp -S open -S openat -F auid>=1000 -F auid!=-1 -k
soc_auditd2_T1018_Remote_system_Discovery2
-w /bin/route -p x -k soc_auditd_NetDiscovery18
-w /sbin/ifconfig -p x -k soc_auditd_NetDiscovery19
-w /bin/ifconfig -p x -k soc_auditd_NetDiscovery20
-w /usr/sbin/route -p x -k soc_auditd_NetDiscovery1
-w /usr/sbin/ifconfig -p x -k soc_auditd_NetDiscovery2
-w /etc/resolv.conf -p wa -k soc_auditd_NetDiscovery3
-w /etc/hosts.allow -p wa -k soc_auditd_NetDiscovery4
-w /etc/hosts.deny -p wa -k soc_auditd_NetDiscovery5
-w /etc/hosts -p wa -k soc_auditd_NetDiscovery6
-w /bin/sysctl -p x -k soc_auditd_NetDiscovery7
-w /sbin/sysctl -p x -k soc_auditd_NetDiscovery8
-w /bin/traceroute.db -p x -k soc_auditd_NetDiscovery9
-w /usr/bin/traceroute.db -p x -k soc_auditd_NetDiscovery10
-w /bin/tracepath -p x -k soc_auditd_NetDiscovery11
-w /usr/bin/sysctl -p x -k soc_auditd_NetDiscovery12
-w /usr/sbin/sysctl -p x -k soc_auditd_NetDiscovery13
-w /usr/bin/traceroute -p x -k soc_auditd_NetDiscovery14
-w /usr/bin/tracepath -p x -k soc_auditd_NetDiscovery15
-w /proc/sys/net/ipv4/ip_forward -p wa -k soc_auditd_NetDiscovery16
-w /bin/traceroute -p x -k soc_auditd_NetDiscovery21
-w /etc/sysconfig/network -p wa -k soc_auditd_NetDiscovery22
-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
NetDiscoveryubip
-a always,exit -F arch=b32 -S execve -F exe=/usr/sbin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
```

```
NetDiscoveryusbinip
-a always,exit -F arch=b32 -S execve -F exe=/bin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
NetDiscoverybip
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
NetDiscoveryubip
-a always,exit -F arch=b64 -S execve -F exe=/usr/sbin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
NetDiscoveryusbinip
-a always,exit -F arch=b64 -S execve -F exe=/bin/ip -F auid!=-1 -F perm=x -k soc_auditd2_
NetDiscoverybip
##System Network Connection Discovery
-w /usr/bin/netstat -p x -k soc_auditd_ConnDiscovery1
-w /bin/netstat -p x -k soc_auditd_ConnDiscovery2
##Password Policy Discovery
-w /etc/pam.d/common-password -p wa -k soc_auditd_PwdDiscovery1
-w /etc/passwdqc.conf -p wa -k soc_auditd_PwdDiscovery2
##Account Discovery
-a always,exit -F arch=b64 -F path=/etc/group -S open -S openat -F auid>=1000 -F auid!=-1 -k soc_
auditd_AccountDiscovery1
# because many legal utilites ask /etc/passwd
-a always,exit -F path=/etc/passwd -F perm=wa -k soc_auditd2_T1087.001_etc_passwd_change
-a always,exit -F arch=b32 -F path=/etc/shadow -S all -F auid>=1000 -F auid!=-1 -F perm=rwa -k
soc_auditd2_AccountDiscovery
-a always,exit -F arch=b64 -F path=/etc/shadow -S all -F auid>=1000 -F auid!=-1 -F perm=rwa -k
soc_auditd2_AccountDiscovery
-w /usr/bin/getent -p x -k soc_auditd_AccountDiscovery1
-w /usr/bin/who -p x -k soc_auditd_AccountDiscovery2
-w /usr/bin/whoami -p x -k soc_auditd_AccountDiscovery3
-w /usr/bin/groups -p x -k soc_auditd_AccountDiscovery4
-w /usr/bin/users -p x -k soc_auditd_AccountDiscovery5
-w /usr/bin/ldapsearch -p x -k soc_auditd_AccountDiscovery6
-w /etc/security/opasswd -p wa -k soc_auditd_AccountDiscovery7
-w /etc/tcb/ -p w -k soc_auditd_AccountDiscovery8
##File And Directory Discovery
-w /usr/bin/ls -p x -k soc_auditd_FileDiscovery1
-w /usr/bin/dir -p x -k soc_auditd_FileDiscovery2
-w /usr/bin/tree -p x -k soc_auditd_FileDiscovery3
-w /usr/bin/find -p x -k soc_auditd_FileDiscovery4
-w /usr/bin/locate -p x -k soc_auditd_FileDiscovery5
-w /usr/bin/pwd -p x -k soc_auditd_FileDiscovery6
-w /bin/ls -p x -k soc_auditd_FileDiscovery7
-w /bin/find -p x -k soc_auditd_FileDiscovery8
-w /bin/pwd -p x -k soc_auditd_FileDiscovery9
##Sandbox Evasion System Checks
-w /usr/bin/dmidecode -p x -k soc_auditd_Sandbox1
-w /usr/bin/facter -p x -k soc_auditd_Sandbox2
-w /usr/bin/lshw -p x -k soc_auditd_Sandbox3
-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/dmesg -F auid!=-1 -k soc_auditd2_Sandbox5
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/dmesg -F auid!=-1 -k soc_auditd2_Sandbox6
-w /usr/bin/hostnamectl -p x -k soc_auditd_Sandbox7
-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/systemd-detect-virt -F auid!=-1 -F perm=x -k
soc_auditd2_Sandbox10
-a always,exit -F arch=b32 -S execve -F exe=/usr/sbin/systemd-detect-virt -F auid!=-1 -F perm=x -k
```

```
soc_auditd2_Sandbox11
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/systemd-detect-virt -F auid!=-1 -F perm=x -k
soc_auditd2_Sandbox12
-a always,exit -F arch=b64 -S execve -F exe=/usr/sbin/systemd-detect-virt -F auid!=-1 -F perm=x -k
soc_auditd2_Sandbox13
-w /usr/sbin/dmidecode -p x -k soc_auditd_Sandbox14
-w /usr/sbin/lshw -p x -k soc_auditd_Sandbox15
-a always,exit -F arch=b32 -S execve -F exe=/bin/dmesg -F auid!=-1 -k soc_auditd2_Sandbox17
-a always,exit -F arch=b64 -S execve -F exe=/bin/dmesg -F auid!=-1 -k soc_auditd2_Sandbox18
-w /usr/bin/imvirt -p x -k soc_auditd_Sandbox14
-w /usr/sbin/facter -p x -k soc_auditd_Sandbox15
-w /usr/sbin/dmesg -p x -k soc_auditd_Sandbox16
-w /usr/sbin/hostnamectl -p x -k soc_auditd_Sandbox17
-w /usr/sbin/imvirt -p x -k soc_auditd_Sandbox18
##Security Software Discovery
-w /usr/bin/ufw -p x -k soc_auditd_SecuritySoftDIscovery1
-w /usr/bin/pfctl -p x -k soc_auditd_SecuritySoftDIscovery2
-w /usr/bin/pf -p x -k soc_auditd_SecuritySoftDIscovery3
-w /usr/bin/getenforce -p x -k soc_auditd_SecuritySoftDIscovery4
-w /usr/sbin/ufw -p x -k soc_auditd_SecuritySoftDIscovery5
-w /usr/sbin/pfctl -p x -k soc_auditd_SecuritySoftDIscovery6
-w /usr/sbin/pf -p x -k soc_auditd_SecuritySoftDIscovery7
-w /usr/sbin/getenforce -p x -k soc_auditd_SecuritySoftDIscovery8
-w /usr/bin/getfacl -p x -k soc_auditd_SecuritySoftDIscovery9
-w /usr/bin/setfacl -p x -k soc_auditd_SecuritySoftDIscovery10
-w /usr/bin/control++ -p x -k soc_auditd_SecuritySoftDIscovery11
-w /etc/control++/ -p wa -k soc_auditd_SecuritySoftDIscovery12
##Network Sniffing
-w /usr/bin/bettercap -p x -k soc_auditd_Sniff1
-w /usr/bin/dsniff -p x -k soc_auditd_Sniff2
-w /usr/bin/eigrp-tools -p x -k soc_auditd_Sniff3
-w /usr/bin/ettercap -p x -k soc_auditd_Sniff4
-w /usr/bin/httpsniff -p x -k soc_auditd_Sniff5
-w /usr/bin/netsniff-ng -p x -k soc_auditd_Sniff6
-w /usr/bin/sslsniff -p x -k soc_auditd_Sniff7
-w /usr/bin/ssldump -p x -k soc_auditd_Sniff8
-w /usr/bin/tcpick -p x -k soc_auditd_Sniff9
-w /usr/bin/wireshark-cli -p x -k soc_auditd_Sniff10
-w /usr/bin/wireshark-qt -p x -k soc_auditd_Sniff11
-w /usr/bin/wifi-monitor -p x -k soc_auditd_Sniff12
-w /usr/bin/tcpdump -p x -k soc_auditd_Sniff13
-w /usr/sbin/bettercap -p x -k soc_auditd_Sniff14
-w /usr/sbin/dsniff -p x -k soc_auditd_Sniff15
-w /usr/sbin/eigrp-tools -p x -k soc_auditd_Sniff16
-w /usr/sbin/ettercap -p x -k soc_auditd_Sniff17
-w /usr/sbin/httpsniff -p x -k soc_auditd_Sniff18
-w /usr/sbin/netsniff-ng -p x -k soc_auditd_Sniff19
-w /usr/sbin/sslsniff -p x -k soc_auditd_Sniff20
-w /usr/sbin/ssldump -p x -k soc_auditd_Sniff21
-w /usr/sbin/tcpick -p x -k soc_auditd_Sniff22
-w /usr/sbin/wireshark-cli -p x -k soc_auditd_Sniff23
-w /usr/sbin/wireshark-qt -p x -k soc_auditd_Sniff24
```

```
-w /usr/sbin/wifi-monitor -p x -k soc_auditd_Sniff25
-w /usr/sbin/tcpdump -p x -k soc_auditd_Sniff26
-w /usr/bin/wireshark -p x -k soc_auditd_Sniff27
-w /usr/bin/wireshark-qt5 -p x -k soc_auditd_Sniff28
##Acccount Modification
-w /usr/sbin/useradd -p x -k soc_auditd_AccountModification1
-w /usr/sbin/userdel -p x -k soc_auditd_AccountModification2
-w /usr/sbin/usermod -p x -k soc_auditd_AccountModification3
-w /usr/sbin/adduser -p x -k soc_auditd_AccountModification4
##Group Modification
-w /usr/sbin/groupadd -p x -k soc_auditd_GroupModification1
-w /usr/sbin/groupmod -p x -k soc_auditd_GroupModification2
-w /usr/sbin/addgroup -p x -k soc_auditd_GroupModification3
-w /usr/sbin/roleadd -p x -k soc_auditd_GroupModification4
##Power Management
-w /sbin/shutdown -p x -k soc_auditd_Power1
-w /sbin/poweroff -p x -k soc_auditd_Power2
-w /sbin/reboot -p x -k soc_auditd_Power3
-w /sbin/halt -p x -k soc_auditd_Power4
##Discretionary Access Control (DAC) modifications
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights1
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights2
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights3
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights4
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights5
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights6
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights7
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights8
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights9
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights10
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights11
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights12
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights13
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights14
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights15
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights16
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights17
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights18
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights19
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights20
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights21
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights22
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights23
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights24
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights25
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=-1 -k soc_auditd_FileRights26
-w /usr/bin/chattr -p x -k soc_auditd_FileRights27
##Cron configuration & scheduled jobs
-w /etc/cron.allow -p wa -k soc_auditd_Cron1
-w /etc/cron.deny -p wa -k soc_auditd_Cron2
-w /etc/cron.d/ -p wa -k soc_auditd_Cron3
-w /etc/cron.daily/ -p wa -k soc_auditd_Cron4
```

```
-w /etc/cron.hourly/ -p wa -k soc_auditd_Cron5
-w /etc/cron.monthly/ -p wa -k soc_auditd_Cron6
-w /etc/cron.weekly/ -p wa -k soc_auditd_Cron7
-w /etc/crontab -p wa -k soc_auditd_Cron8
-w /var/spool/cron/ -p wa -k soc_auditd_Cron9
-a always,exit -F path=/var/spool/anacron -F perm=wa -k soc_auditd2_anacron
-w /var/spool/at -p wa -k soc_auditd2_cron_modify1
-w /var/spool/cron -p wa -k soc_auditd2_cron_modify2
-w /var/spool/cron/ -k soc_auditd2_T1053.003_cron_change_cron
-w /var/spool/cron/crontabs/ -k soc_auditd2_cron
-w /var/spool/at/ -p wa -k soc_auditd2_T1053.001_at_change
-w /var/spool/at/spool -p wa -k soc_auditd2_at_spool_change
-w /etc/anacrontab -p wa -k soc_auditd2_T1053.003_anacron
-w /etc/at.allow -p wa -k soc_auditd2_T1053.001_at-allow_change_Scheduled_Task
-w /etc/at.deny -p wa -k soc_auditd2_T1053.001_at-deny_change_Scheduled_Task
##Login configuration and information
-w /etc/login.defs -p wa -k soc_auditd_Login1
-w /etc/securetty -p wa -k soc_auditd_Login2
-w /var/log/faillog -p wa -k soc_auditd_Login3
-w /var/log/lastlog -p wa -k soc_auditd_Login4
-w /var/log/tallylog -p wa -k soc_auditd_Login5
-w /var/run/faillock/ -p wa -k soc_auditd_Login6
-w /var/log/secure -p wa -k soc_auditd2_T1078.001_4
##Changes to hostname
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k soc_auditd_Hostname1
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k soc_auditd_Hostname2
##Detect Remote Shell Use
-a always,exit -F arch=b32 -F exe=/bin/bash -F success=1 -S connect -k soc_auditd_RemoteShell1
-a always,exit -F arch=b64 -F exe=/bin/bash -F success=1 -S connect -k soc_auditd_RemoteShell2
-a always,exit -F arch=b32 -F exe=/usr/bin/bash -F success=1 -S connect -k soc_auditd_
RemoteShell3
-a always,exit -F arch=b64 -F exe=/usr/bin/bash -F success=1 -S connect -k soc_auditd_
RemoteShell4
##Changes to issue
-w /etc/issue -p wa -k soc_auditd_Issue1
-w /etc/issue.net -p wa -k soc_auditd_Issue2
##PAM configuration
-w /etc/security/limits.conf -p wa -k soc_auditd_PAM1
-w /etc/security/limits.d -p wa -k soc_auditd_PAM2
-w /etc/security/pam_env.conf -p wa -k soc_auditd_PAM3
-w /etc/security/namespace.conf -p wa -k soc_auditd_PAM4
-w /etc/security/namespace.d -p wa -k soc_auditd_PAM5
-w /etc/security/namespace.init -p wa -k soc_auditd_PAM6
-w /etc/pam.d -p wa -k soc_auditd_PAM7
##Suspicious activity: Remote Access
-w /usr/bin/wget -p x -k soc_auditd_SuspTools1
-w /usr/bin/curl -p x -k soc_auditd_SuspTools2
-w /usr/bin/base64 -p x -k soc_auditd_SuspTools3
-w /bin/nc -p x -k soc_auditd_SuspTools4
-w /bin/netcat -p x -k soc_auditd_SuspTools5
-w /usr/bin/ncat -p x -k soc_auditd_SuspTools6
#-w /usr/bin/ss -p x -k soc_auditd_SuspTools7
```

```
-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/ss -F auid!=-1 -F perm=x -k soc_auditd2_
SuspTools8
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/ss -F auid!=-1 -F perm=x -k soc_auditd2_
SuspTools9
#-w /usr/sbin/ss -p x -k soc_auditd_SuspTools24
-a always,exit -F arch=b32 -S execve -F exe=/usr/sbin/ss -F auid!=-1 -F perm=x -k soc_auditd2_
SuspTools25
-a always,exit -F arch=b64 -S execve -F exe=/usr/sbin/ss -F auid!=-1 -F perm=x -k soc_auditd2_
SuspTools26
-w /usr/bin/ssh -p x -k soc_auditd_SuspTools10
-w /usr/bin/scp -p x -k soc_auditd_SuspTools11
-w /usr/bin/sftp -p x -k soc_auditd_SuspTools12
-w /usr/bin/ftp -p x -k soc_auditd_SuspTools13
-w /usr/bin/socat -p x -k soc_auditd_SuspTools14
-w /usr/bin/wireshark -p x -k soc_auditd_SuspTools15
-w /usr/bin/tshark -p x -k soc_auditd_SuspTools16
-w /usr/bin/rawshark -p x -k soc_auditd_SuspTools17
-w /usr/bin/rdesktop -p x -k soc_auditd_SuspTools18
-w /usr/local/bin/rdesktop -p x -k soc_auditd_SuspTools19
-w /usr/bin/wlfreerdp -p x -k soc_auditd_SuspTools20
-w /usr/bin/xfreerdp -p x -k soc_auditd_SuspTools21
-w /usr/local/bin/xfreerdp -p x -k soc_auditd_SuspTools22
-w /usr/bin/nmap -p x -k soc_auditd_SuspTools23
##Software Configuration
-w /usr/bin/dnet -p x -k soc_auditd_apt1
#-w /usr/bin/dpkg -p x -k soc_auditd_apt2
-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/dpkg -F auid!=-1 -F perm=x -k soc_auditd2_apt
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/dpkg -F auid!=-1 -F perm=x -k soc_auditd2_apt
-w /usr/bin/apt -p x -k soc_auditd_apt3
-w /usr/bin/apt-add-repository -p x -k soc_auditd_apt4
-w /usr/bin/apt-get -p x -k soc_auditd_apt5
-w /usr/bin/aptitude -p x -k soc_auditd_apt6
-w /usr/bin/wajig -p x -k soc_auditd_apt7
-w /usr/bin/snap -p x -k soc_auditd_apt8
-w /usr/bin/apt-repo -p x -k soc_auditd_apt9
-w /bin/rpm -p x -k soc_auditd_apt10
-w /usr/bin/rpm -p x -k soc_auditd_apt11
-w /usr/bin/epm -p x -k soc_auditd_apt12
-w /usr/bin/wajig -p x -k soc_auditd_apt13
-w /usr/bin/snap -p x -k soc_auditd_apt14
##PIP
-w /usr/bin/pip -p x -k soc_auditd_PIP1
-w /usr/local/bin/pip -p x -k soc_auditd_PIP2
-w /usr/bin/pip3 -p x -k soc_auditd_PIP3
-w /usr/local/bin/pip3 -p x -k soc_auditd_PIP4
##File Deletion Events by User
##-a always,exit -F arch=b32 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F
auid!=-1 -k soc_auditd_FileDelete1
##-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F
auid!=-1 -k soc_auditd_FileDelete2
##Unsuccessful Creation
-a always,exit -F arch=b32 -S creat,link,mknod,mkdir,symlink,mknodat,linkat,symlinkat -F exit=-
```

```
EACCES -k soc_auditd_UnsuccessfulCreation1
-a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -F exit=-
EACCES -k soc_auditd_UnsuccessfulCreation2
-a always,exit -F arch=b32 -S link,mkdir,symlink,mkdirat -F exit=-EPERM -k soc_auditd_
UnsuccessfulCreation3
-a always,exit -F arch=b64 -S mkdir,link,symlink,mkdirat -F exit=-EPERM -k soc_auditd_
UnsuccessfulCreation4
##Unsuccessful Modification
-a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S
removexattr -S lremovexattr -F exit=-EACCES -k soc_auditd_UnsuccessfulModification1
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S
removexattr -S lremovexattr -F exit=-EACCES -k soc_auditd_UnsuccessfulModification2
-a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S
removexattr -S lremovexattr -F exit=-EPERM -k soc_auditd_UnsuccessfulModification3
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S
removexattr -S lremovexattr -F exit=-EPERM -k soc_auditd_UnsuccessfulModification4
##Session info
-w /var/run/utmp -p wa -k soc_auditd_SessionInfo1
-w /var/log/btmp -p wa -k soc_auditd_SessionInfo2
-w /var/log/wtmp -p wa -k soc_auditd_SessionInfo3
##Mount, unmount
-a always,exit -F arch=b64 -S mount -S umount2 -F auid!=-1 -k soc_auditd_MountUnmount1
-a always,exit -F arch=b32 -S mount -S umount2 -F auid!=-1 -k soc_auditd_MountUnmount2
##External device conneting to server
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=soc_auditd_ExternalDevice1
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=soc_auditd_ExternalDevice2
##Time Change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F key=soc_auditd_TimeChange1
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F key=soc_auditd_TimeChange2
-a always,exit -F arch=b32 -S adjtimex,settimeofday,stime,clock_settime -F key=soc_auditd2_
TimeChange1
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F key=soc_auditd2_
TimeChange2
-w /etc/localtime -p wa -k soc_auditd_TimeChange3
##Module Change
-a always,exit -F arch=b32 -S create_module -k soc_auditd_Module1
-a always,exit -F arch=b64 -S create_module -k soc_auditd_Module2
-a always,exit -F arch=b32 -S finit_module -k soc_auditd_Module3
-a always,exit -F arch=b64 -S finit_module -k soc_auditd_Module4
-w /sbin/insmod -p x -k soc_auditd_Module5
-w /sbin/rmmod -p x -k soc_auditd_Module6
-w /sbin/modprobe -p x -k soc_auditd_Module7
-a always,exit -F arch=b32 -S init_module -k soc_auditd_Module8
-a always,exit -F arch=b64 -S init_module -k soc_auditd_Module9
-a always,exit -F arch=b32 -S delete_module -k soc_auditd_Module10
-a always,exit -F arch=b64 -S delete_module -k soc_auditd_Module11
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -k soc_auditd_
Module12
##Priveleged User Control
-a always,exit -F path=/bin/ping -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser1
-a always,exit -F path=/bin/umount -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
```

```
PrivelegedUser2
-a always,exit -F path=/bin/chgrp -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser3
-a always,exit -F path=/bin/ping6 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser4
-a always,exit -F path=/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd_PrivelegedUser5
-a always,exit -F path=/bin/at -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_PrivelegedUser6
-a always,exit -F path=/bin/chage -F auid>=1000 -F auid!=-1 -k soc_auditd_PrivelegedUser7
-a always,exit -F path=/bin/ssh-agent -F auid>=1000 -F auid!=-1 -k soc_auditd_PrivelegedUser8
-a always,exit -F path=/bin/wall -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser9
-a always,exit -F path=/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser10
-a always,exit -F path=/sbin/pwck -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser11
-a always,exit -F path=/usr/bin/wall -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser12
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser13
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser14
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser15
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser16
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F auid!=-1 -k
soc_auditd_PrivelegedUser1
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser18
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=unset -k soc_
auditd_PrivelegedUser19
-a always,exit -F path=/usr/bin/ping6 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser20
-a always,exit -F path=/usr/lib/chkpwd/tcb_chkpwd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd_PrivelegedUser21
-a always,exit -F path=/usr/sbin/pwck -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd_
PrivelegedUser22
-a always,exit -F path=/lib/dbus-1/dbus-daemon-launch-helper -F perm=x -F auid>=1000 -F auid!=-1
-k soc_auditd2_PrivelegedUser23
-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser24
-a always,exit -F path=/bin/mount -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser25
-a always,exit -F path=/usr/lib/screen/tcb_chkpwd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd2_PrivelegedUser26
-a always,exit -F path=/usr/lib/screen/utempter -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd2_PrivelegedUser27
-a always,exit -F path=/usr/lib/utempter/utempter -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd2_PrivelegedUser28
-a always,exit -F path=/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper -F perm=x -F
auid>=1000 -F auid!=-1 -k soc_auditd2_PrivelegedUser29
```

```
-a always,exit -F path=/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper -F perm=x -F
auid>=1000 -F auid!=-1 -k soc_auditd2_PrivelegedUser30
-a always,exit -F path=/usr/bin/ping -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser31
-a always,exit -F path=/usr/libexec/polkit-1/polkit-agent-helper-1 -F perm=x -F auid>=1000 -F auid!=-
1 -k soc_auditd2_PrivelegedUser32
-a always,exit -F path=/usr/libexec/postfix/postqueue/postqueue -F perm=x -F auid>=1000 -F auid!=-
1 -k soc_auditd2_PrivelegedUser33
-a always,exit -F path=/usr/bin/gpg -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser34
-a always,exit -F path=/usr/bin/screen -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser35
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser36
-a always,exit -F path=/usr/bin/write -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser37
-a always,exit -F path=/usr/bin/cgexec -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser38
-a always,exit -F path=/usr/bin/vlock -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser39
-a always,exit -F path=/usr/bin/sudoreplay -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser40
-a always,exit -F path=/usr/bin/netlist -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser41
-a always,exit -F path=/usr/bin/fusermount3 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser42
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser43
-a always,exit -F path=/usr/bin/fusermount -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser44
-a always,exit -F path=/usr/bin/cgclassify -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser45
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
PrivelegedUser46
##MAC Policy
-w /etc/selinux/ -p wa -k soc_auditd_MACPolicy1
-w /etc/apparmor/ -p wa -k soc_auditd_MACPolicy2
-w /etc/apparmor.d/ -p wa -k soc_auditd_MACPolicy3
-w /etc/osec/ -p wa -k soc_auditd_MACPolicy4
-w /sbin/integalert -p x вЂ“k soc_auditd_MACPolicy5
-w /usr/bin/osec -p x вЂ“k soc_auditd_MACPolicy6
##Core
-w /etc/sysctl.conf -p wa -k soc_auditd_Core
##Sources.list
-w /etc/apt/sources.list -p wa -k soc_auditd_SourcesList_apt
-w /etc/apt/sources.list.d -p wa -k soc_auditd2_SourcesList_dir
##Collection attack
-w /usr/sbin/getcap -p x -k soc_auditd_attack_collection1
-w /usr/bin/chmod -p x -k soc_auditd_attack_collection2
-w /sbin/getcap -p x -k soc_auditd_attack_collection3
-w /bin/chmod -p x -k soc_auditd_attack_collection4
##----------------------Additional Rules-------------------------
```

```
-w /etc/krb5.conf -p wa -k soc_kerberos_configure
-w /etc/sssd/ -p wa -k soc_sssd_configure
# KUMA pack
-w /etc/update-motd.d/ -p wa -k soc_auditd2_motd
-w /etc/udev/rules.d/ -p wa -k soc_auditd2_udev
-w /etc/xdg/autostart/ -p wa -k soc_auditd2_xdg1
-w /usr/share/autostart/ -p wa -k soc_auditd2_xdg2
-w /lib/systemd/ -p wa -k soc_auditd2_systemd3
-w /usr/local/lib/systemd/ -p wa -k soc_auditd2_systemd4
-w /usr/local/share/systemd/user -p wa -k soc_auditd2_systemd_user1
-w /usr/share/systemd/user -p wa -k soc_auditd2_systemd_user2
-w /usr/sbin/setcap -p x -k soc_auditd2_setcap
-w /root/.ssh/authorized_keys -p wa -k soc_auditd2_root_key_change_rootkey1
-w /boot/grub2/grub.cfg -p wa -k soc_auditd2_T1542.003_PreS_Boot
-w /run/systemd/system/ -k soc_auditd2_T1543.002_systemd_change
-w /root/.ssh -p wa -k soc_auditd2_root_key_change_rootkey2
-a always,exit -F arch=b32 -C auid!=uid -S execve -k soc_auditd2_T1548.001_28
-a always,exit -F arch=b32 -S execve,execveat -C uid!=euid -F euid=0 -k soc_audit2_setuid1
-a always,exit -F arch=b64 -S execve,execveat -C uid!=euid -F euid=0 -k soc_audit2_setuid2
-a always,exit -F arch=b32 -S execve,execveat -C gid!=egid -F egid=0 -k soc_audit2_setgid1
-a always,exit -F arch=b64 -S execve,execveat -C gid!=egid -F egid=0 -k soc_audit2_setgid2
-a always,exit -F path=/usr/bin/mount -F auid>=1000 -F auid!=-1 -k soc_audit_privileged_mount
# suspicious renaming
-a always,exit -F dir=/bin -F arch=b32 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002
-a always,exit -F dir=/bin -F arch=b64 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002
-w /usr/bin/mount -p x -k soc_auditd_MountUnmount
-w /var/lib/afick/afick -p wa -k soc_audit_change_bd_afick
-w /boot/ -p wa -k soc_system_obj_modification1
-w /bin/ -p wa -k soc_system_obj_modification2
-w /sbin/ -p wa -k soc_system_obj_modification3
-w /usr/bin/ -p wa -k soc_system_obj_modification4
-w /usr/sbin/ -p wa -k soc_system_obj_modification5
##----------------------Rules v2 Addendum-------------------------
## Postgresql
-w /usr/local/pgsql/bin/pg_ctl -p x -k soc_auditd2_pg_ctl
-w /usr/local/pgsql/bin/psql -p x -k soc_auditd2_psql
-w /usr/local/pgsql/bin/pg_dump -p x -k soc_auditd2_pgdump
-w /usr/local/pgsql/bin/pg_dumpall -p x -k soc_auditd2_pgdumpall
-w /usr/local/pgsql/bin/createuser -p x -k soc_auditd2_createuser
-w /usr/local/pgsql/bin/dropuser -p x -k soc_auditd2_dropuser
-w /usr/local/pgsql/bin/pg_basebackup -p x -k soc_auditd2_pgbasebackup
-w /usr/local/pgsql/data/pg_hba.conf -p wa -k soc_auditd2_pghba
-w /usr/local/pgsql/data/postgresql.conf -p wa -k soc_auditd2_pgconfig
## Init or another persistent places
-w /etc/rc.d/ -p wa -k soc_auditd2_T1037_init_dir_change1
-w /etc/rc.d/init.d/ -p wa -k soc_auditd2_T1037_init_dir_change2
-w /etc/rc.local -p wa -k soc_auditd2_T1037_init_dir_change_T1546_Event_Triggered_Execution
-w /etc/rc0.d -p wa -k soc_auditd2_soc_auditd2_T1037_init_dir_change
-w /etc/rc1.d -p wa -k soc_auditd2_T1037_init_dir_change3
-w /etc/rc2.d -p wa -k soc_auditd2_T1037_init_dir_change4
```

```
-w /etc/rc3.d -p wa -k soc_auditd2_T1037_init_dir_change5
-w /etc/rc4.d -p wa -k soc_auditd2_T1037_init_dir_change6
-w /etc/rc5.d -p wa -k soc_auditd2_T1037_init_dir_change7
-w /etc/rc6.d -p wa -k soc_auditd2_T1037_init_dir_change8
## Directory Access Errors
-a always,exit -F arch=b64 -S open -F dir=/bin -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068bin
-a always,exit -F arch=b64 -S open -F dir=/etc -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068etc
-a always,exit -F arch=b64 -S open -F dir=/sbin -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068sbin
-a always,exit -F arch=b64 -S open -F dir=/srv -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068srv
-a always,exit -F arch=b64 -S open -F dir=/usr/bin -F success=0 -k soc_auditd2_
unauthedfileaccess_T1068ubin
-a always,exit -F arch=b64 -S open -F dir=/usr/sbin -F success=0 -k soc_auditd2_
unauthedfileaccess_T1068usbin
-a always,exit -F arch=b64 -S open -F dir=/var -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068var
-a always,exit -F arch=b64 -S open -F dir=/tmp -F success=0 -k soc_auditd2_unauthedfileaccess_
T1068tmp
-a always,exit -F arch=b64 -S open -F dir=/var/tmp/ -F success=0 -k soc_auditd2_
unauthedfileaccess_T1068vartmp
## Network Connection Establishing
-a always,exit -F arch=b32 -S socket -F a0=0x11 -k soc_auditd2_api_socket11
-a always,exit -F arch=b32 -S socket -F a0=0xA -k soc_auditd2_api_socket10
-a always,exit -F arch=b32 -S socket -F a0=10 -k soc_auditd2_Exfiltration_Over_Other_Network_
Medium
-a always,exit -F arch=b64 -S socket -F a0=0x11 -k soc_auditd2_api_socket1
-a always,exit -F arch=b64 -S socket -F a0=0x2 -F a1=0x3 -k soc_auditd2_api_socket2
-a always,exit -F arch=b64 -S socket -F a0=0x2 -F a1=0xA -k soc_auditd2_api_socket3
-a always,exit -F arch=b64 -S socket -F a0=0xA -F a1=0x3 -k soc_auditd2_api_socket4
-a always,exit -F arch=b64 -S socket -F a0=0xA -F a1=0xA -k soc_auditd2_api_socket5
-a always,exit -F arch=b64 -S socket -F a0=0xA -k soc_auditd2_api_socket6
-a always,exit -F arch=b64 -S socket -F a0=10 -k soc_auditd2_Exfiltration_Over_Other_Network_
Medium
-a always,exit -F arch=b64 -S socket -F a0=14 -k soc_auditd2_net_socket1
-a always,exit -F arch=b64 -S socket -F a0=15 -k soc_auditd2_net_socket2
-a always,exit -F arch=b64 -S socket -F a0=17 -k soc_auditd2_net_socket3
-a always,exit -F arch=b64 -S socket -F a0=26 -k soc_auditd2_net_socket4
-a always,exit -F arch=b64 -S socket -F a0=44 -k soc_auditd2_net_socket5
-a always,exit -F arch=b32 -S connect -F a2=0x1C -k soc_auditd2_api_connect1
-a always,exit -F arch=b32 -S connect -F a2=28 -F success=1 -k soc_auditd2_network_connect_6
-a always,exit -F arch=b64 -S connect -F a2=0x1C -k soc_auditd2_api_connect2
-a always,exit -F arch=b64 -S connect -F a2=28 -F success=1 -k soc_auditd2_network_connect_6
## Binaries Monitoring
-w /usr/local/bin -p wa -k soc_auditd2_bin_modify
-w /usr/local/bin/xonsh -p x -k soc_auditd2_susp_shell_xonsh
## Suspicious actions
-a always,exit -F dir=/var/log -F arch=b32 -S unlink -S unlinkat -S rmdir -F auid>=1000 -F auid!=-1 -F
exit=0 -k soc_auditd2_T1070_002log
-a always,exit -F dir=/var/log -F arch=b64 -S unlink -S unlinkat -S rmdir -F auid>=1000 -F auid!=-1 -F
```

```
exit=0 -k soc_auditd2_T1070_002log
## /usr/sbin executables
-a always,exit -F path=/usr/sbin/aulast -F perm=x -k soc_auditd2_auditreport1
-a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k soc_auditd2_aulastlogin
-a always,exit -F path=/usr/sbin/aureport -F perm=x -k soc_auditd2_auditreport2
-a always,exit -F path=/usr/sbin/ausearch -F perm=x -k soc_auditd2_auditreport3
-a always,exit -F path=/usr/sbin/auvirt -F perm=x -k soc_auditd2_auditreport4
-a always,exit -F path=/usr/sbin/ccreds_validate -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd2_T1078.003_27
-a always,exit -F path=/usr/sbin/groupdel -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_24
-a always,exit -F path=/usr/sbin/newusers -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_23
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_25
-a always,exit -F path=/usr/sbin/suexec -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_21
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_19
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_28
-a always,exit -F path=/usr/sbin/usernetctl -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_26
-w /usr/sbin/aa-complain -p x -k soc_auditd2_apparmor_tools1
-w /usr/sbin/aa-disable -p x -k soc_auditd2_apparmor_tools2
-w /usr/sbin/aa-enforce -p x -k soc_auditd2_apparmor_tools3
-w /usr/sbin/chkconfig -p x -k soc_auditd2_chkconfig_T1562
-w /usr/sbin/dig -p x -k soc_auditd2_T1018_Remote_system_Discovery1
-w /usr/sbin/ftpd -p x -k soc_auditd2_T1133_External_Remote_Services1
-w /usr/sbin/insmod -p x -k soc_auditd2_T1547_Boot_or_Logon_Autostart_Execution1
-w /usr/sbin/lsmod -p x -k soc_auditd2_T1547_Boot_or_Logon_Autostart_Execution2
-w /usr/sbin/modinfo -p x -k soc_auditd2_T1547_Boot_or_Logon_Autostart_Execution3
-w /usr/sbin/modprobe -p x -k soc_auditd2_T1547_Boot_or_Logon_Autostart_Execution4
-w /usr/sbin/nologin -k soc_auditd2_T1087.001_6
-w /usr/sbin/nslookup -p x -k soc_auditd2_T1018_Remote_system_Discovery2
-w /usr/sbin/realm -p x -k soc_auditd2_T1136.002_realm_change_Create_Account_Domain_
Account
-w /usr/sbin/rmmod -p x -k soc_auditd2_T1547_Boot_or_Logon_Autostart_Execution5
-w /usr/sbin/sshd -p x -k soc_auditd2_T1133_External_Remote_Services2
-w /usr/sbin/stunnel -p x -k soc_auditd2_T1573.002_1_stunnel
-w /usr/sbin/traceroute -p x -k soc_auditd2_T1049_2_sbin_susp
-w /usr/sbin/update-ca-certificates -p x -k soc_auditd2_update-ca-certificates
-w /usr/sbin/vsftpd -p x -k soc_auditd2_T1133_External_Remote_Services3
-a always,exit -F dir=/usr/bin -F arch=b32 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002_rename_exe1
-a always,exit -F dir=/usr/bin -F arch=b64 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002_rename_exe2
## /sbin/ executables
-w /sbin/apparmor_parser -p x -k soc_auditd2_apparmor_tools
-w /sbin/init -k soc_auditd2_T1037_4
-w /sbin/init -p wa -k soc_auditd2_T1037_init_change
-w /sbin/nologin -k soc_auditd2_T1087.001_7
```

```
-w /sbin/yast -p x -k soc_auditd2_T1072_3_yast
-w /sbin/yast2 -p x -k soc_auditd2_T1072_4_yast
-a always,exit -F dir=/sbin -F arch=b32 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002_rename_exe3
-a always,exit -F dir=/sbin -F arch=b64 -S rename -F auid>=1000 -F auid!=-1 -F exit=0 -k soc_
auditd2_T1070_002_rename_exe4
## /usr/bin executables
-a always,exit -F path=/usr/bin/Xorg -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_30
-a always,exit -F path=/usr/bin/at -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_
33
-a always,exit -F path=/usr/bin/awk -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_63
-a always,exit -F path=/usr/bin/bash -F perm=x -F auid=0 -F auid!=-1 -k soc_auditd2_T1059.004_2
# our standart shell from non-privileged users
#-a always,exit -F path=/usr/bin/bash -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1059.004_1
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_46
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_44
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_47
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_43
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_42
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_37
-a always,exit -F path=/usr/bin/findmnt -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_59
-a always,exit -F path=/usr/bin/gawk -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_62
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_35
-a always,exit -F path=/usr/bin/kgrantpty -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_36
-a always,exit -F path=/usr/bin/kpac_dhcp_helper -F perm=x -F auid>=1000 -F auid!=-1 -k soc_
auditd2_T1078.003_50
-a always,exit -F path=/usr/bin/lspci -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_56
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_48
-a always,exit -F path=/usr/bin/newrole -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_49
-a always,exit -F path=/usr/bin/pgrep -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_54
-a always,exit -F path=/usr/bin/pkla -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_61
-a always,exit -F path=/usr/bin/python -F perm=x -F auid=0 -F auid!=-1 -k soc_auditd2_T1059.006_2
-a always,exit -F path=/usr/bin/python -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1059.006_1
```

```
-a always,exit -F path=/usr/bin/python2 -F perm=x -F auid=0 -F auid!=-1 -k soc_auditd2_T1059.006_
4
-a always,exit -F path=/usr/bin/python2 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1059.006_3
-a always,exit -F path=/usr/bin/python3 -F perm=x -F auid=0 -F auid!=-1 -k soc_auditd2_T1059.006_
4
-a always,exit -F path=/usr/bin/python3 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1059.006_3
-a always,exit -F path=/usr/bin/rcp -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_
40
-a always,exit -F path=/usr/bin/rlogin -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_31
-a always,exit -F path=/usr/bin/rsh -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_
34
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_45
-a always,exit -F path=/usr/bin/sleep -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_52
-a always,exit -F path=/usr/bin/staprun -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_39
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_32
-a always,exit -F path=/usr/bin/udevadm -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_58
-w /usr/bin/LogMein -p x -k soc_auditd2_T1219_Remote_Access_Tools
-w /usr/bin/VBoxManage -p x -k soc_auditd2_VBoxManage
-w /usr/bin/at -p x -k soc_auditd2_T1053_Scheduled_Task
-w /usr/bin/bzip2 -p x -k soc_auditd2_Data_Compressed11
-w /usr/bin/certutil -p x -k soc_auditd2_Deobfuscate_T1140
-w /usr/bin/chown -p x -k soc_auditd2_chown
-w /usr/bin/cpan -p x -k soc_auditd2_third_party_software1
-w /usr/bin/dbus-send -p x -k soc_auditd2_T1068_CVE_2021_3560_dbus_send
-w /usr/bin/dig -p x -k soc_auditd2_T1018_Remote_system_Discovery
-w /usr/bin/dnf -p x -k soc_auditd2_software_mgmt
-w /usr/bin/egrep -p x -k soc_auditd2_T1081_Credentials_In_Files_T1552.001_2
-w /usr/bin/gcc -p x -k soc_auditd2_gcc
-w /usr/bin/gdbus -p x -k soc_auditd2_gdubs_call
-w /usr/bin/gem -p x -k soc_auditd2_third_party_software2
-w /usr/bin/hostname -p x -k soc_auditd2_T1033_System_Owner_User_Discovery
-w /usr/bin/kubelet -k soc_auditd2_kubelet
-w /usr/bin/lbzip2 -p x -k soc_auditd2_Data_Compressed12
-w /usr/bin/luarocks -p x -k soc_auditd2_third_party_software3
-w /usr/bin/lz4 -p x -k soc_auditd2_Data_Compressed13
-w /usr/bin/lzip -p x -k soc_auditd2_Data_Compressed14
-w /usr/bin/lzop -p x -k soc_auditd2_Data_Compressed15
-w /usr/bin/npm -p x -k soc_auditd2_third_party_software4
-w /usr/bin/nslookup -p x -k soc_auditd2_T1018_Remote_system_Discovery
-w /usr/bin/openssl -p x -k soc_auditd2_Deobfuscate_T1140
-w /usr/bin/pbzip2 -p x -k soc_auditd2_Data_Compressed16
-w /usr/bin/pgrep -p x -k soc_auditd2_T1057_Process_Discovery
-w /usr/bin/pigz -p x -k soc_auditd2_Data_Compressed17
-w /usr/bin/pixz -p x -k soc_auditd2_Data_Compressed18
```

```
-w /usr/bin/pkexec -p x -k soc_auditd2_T1068_CVE_2021_4034_pkexec
-w /usr/bin/pkill -p x -k soc_auditd2_pkill
-w /usr/bin/plzip -p x -k soc_auditd2_Data_Compressed19
-w /usr/bin/postfix -p x -k soc_auditd2_T1505_Server_Software_Component1
-w /usr/bin/qemu -p x -k soc_auditd2_qemu
-w /usr/bin/qemu-img -p x -k soc_auditd2_qemu-img
-w /usr/bin/qemu -p x -k soc_auditd2_vm
-w /usr/bin/qemu-system-x86_64 -p x -k soc_auditd2_qemu-system-x86_64
-w /usr/bin/realm -p x -k soc_auditd2_T1136.002_realm_change_Create_Account_Domain_Account
-w /usr/bin/rpm -p x -k soc_auditd2_T1072_software_mgmt1
-w /usr/bin/rsync -p x -k soc_auditd2_T1105_remote_file_copy
-w /usr/bin/sendmail -p x -k soc_auditd2_T1505_Server_Software_Component2
-w /usr/bin/stunnel -p x -k soc_auditd2_stunnel
-w /usr/bin/svcadm -p x -k soc_auditd2_svcadm
-w /usr/bin/teamviewer -p x -k soc_auditd2_T1219_Remote_Access_Tools
-w /usr/bin/trap -p x -k soc_auditd2_T1546_Event_Triggered_Execution
-w /usr/bin/ugrep -p x -k soc_auditd2_T1081_Credentials_In_Files
-w /usr/bin/unpigz -p x -k soc_auditd2_Data_Compressed20
-w /usr/bin/unshadow -p x -k soc_auditd2_T1003_Credential_Dumping
-w /usr/bin/unzip -p x -k soc_auditd2_Deobfuscate_T1140
-w /usr/bin/update-ca-trust -p x -k soc_auditd2_update-ca-trust
-w /usr/bin/vi -p x -k soc_auditd2_T1552_Unsecured_Credentials1
-w /usr/bin/vim -p x -k soc_auditd2_T1552_Unsecured_Credentials2
-w /usr/bin/virt-manager -p x -k soc_auditd2_virt-manager
-w /usr/bin/virtualbox -p x -k soc_auditd2_virtualbox
-w /usr/bin/zstd -p x -k soc_auditd2_Data_Compressed21
-w /usr/bin/zypper -k soc_auditd2_T1072_software_mgmt2
## Web-server home files change
-w /var/www -p wa -k soc_auditd2_www_home_access
## Home catalogs accesses
-a always,exit -F arch=b32 -S open -F dir=/root -F success=0 -k soc_auditd2_unauthedfileaccess1
-a always,exit -F arch=b64 -S open -F dir=/root -F success=0 -k soc_auditd2_unauthedfileaccess2
-a always,exit -F arch=b64 -S open -F dir=/home -F success=0 -k soc_auditd2_T1068_7_
unauthedfileaccess1
-a always,exit -F arch=b32 -S open -F dir=/home -F success=0 -k soc_auditd2_T1068_7_
unauthedfileaccess2
## Library paths
-a always,exit -F dir=/usr/lib64 -F perm=wa -k soc_auditd2_lib64
-w /lib -p wa -k soc_auditd2_lib_modify
-w /lib/security/ -p wa -k soc_auditd2_T1071_pam_dir_change
-w /lib/systemd/ -p wa -k soc_auditd2_systemd1
-w /lib32/ -p wa -k soc_auditd2_binaries
-w /lib64 -p wa -k soc_auditd2_lib_modify
-w /usr/lib -p wa -k soc_auditd2_lib_modify
-w /usr/lib/systemd -p wa -k soc_auditd2_systemd2
-w /usr/lib/systemd/system/ -k soc_auditd2_T1543.002_systemd_change
-w /usr/lib/systemd/system/ -p wa -k soc_auditd2_T1543_Create_or_Modify_System_Process
## /bin executables
-a always,exit -F exe=/bin/ps -F perm=x -k soc_auditd2_T1057_2
-a always,exit -F path=/bin/chgrp -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_
16
-a always,exit -F path=/bin/ping -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_12
```

```
-a always,exit -F path=/bin/ping6 -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_T1078.003_
17
-a always,exit -F path=/bin/umount -F perm=x -F auid>=1000 -F auid!=-1 -k soc_auditd2_
T1078.003_13
-w /bin/ash -p x -k soc_auditd2_susp_shell1
-w /bin/busybox -p x -k soc_auditd2_susp_shell2
-w /bin/csh -p x -k soc_auditd2_susp_shell3
-w /bin/dash -p x -k soc_auditd2_susp_shell4
-w /bin/fish -p x -k soc_auditd2_susp_shell5
-w /bin/hostname -p x -k soc_auditd2_recon
-w /bin/journalctl -p x -k soc_auditd2_systemd_tools
-w /bin/ksh -p x -k soc_auditd2_susp_shell6
-w /bin/nc.openbsd -p x -k soc_auditd2_T1219_10_susp_activity
-w /bin/nc.traditional -p x -k soc_auditd2_T1219_4_susp_activity
-w /bin/rbash -p x -k soc_auditd2_susp_shell7
-w /bin/rpm -p x -k soc_auditd2_T1072_5_software_mgmt
-w /bin/tclsh -p x -k soc_auditd2_susp_shell8
-w /bin/tcsh -p x -k soc_auditd2_susp_shell9
-w /bin/traceroute -p x -k soc_auditd2_T1016_System_Network_Configuration_Discovery
-w /bin/xonsh -p x -k soc_auditd2_susp_shell10
-w /bin/zsh -p x -k soc_auditd2_susp_shell11
## /etc/ executables
-a always,exit -F dir=/etc/security -F perm=wa -k soc_auditd2_T1071_pam_dir_change
-a always,exit -F dir=/etc/sysconfig -F perm=wa -k soc_auditd2_sysconfig
-a always,exit -F dir=/etc/yum -F perm=wa -k soc_auditd2_yum
-a always,exit -F dir=/etc/yum.repos.d -F perm=wa -k soc_auditd2_yum_repo
-w /etc/sysconfig/network-scripts -p w -k soc_auditd2_network_modifications
-a always,exit -F path=/etc/aliases -F perm=wa -k soc_auditd2_mail
-a always,exit -F path=/etc/bashrc -F perm=wa -k soc_auditd2_T1546.004_shell_profiles
-a always,exit -F path=/etc/krb5.conf.d -F perm=wa -k soc_auditd2_krb5
-a always,exit -F path=/etc/krb5.keytab -F perm=wa -k soc_auditd2_krb5
-a always,exit -F path=/etc/ld.so.conf -F perm=wa -k soc_auditd2_ld_so
-a always,exit -F path=/etc/ld.so.conf.d -F perm=wa -k soc_auditd2_ld_so
-a always,exit -F path=/etc/libaudit.conf -F perm=wa -k soc_auditd2_libaudit
-a always,exit -F path=/etc/logrotate.conf -F perm=wa -k soc_auditd2_logrotate1
-a always,exit -F path=/etc/logrotate.d -F perm=wa -k soc_auditd2_logrotate2
-a always,exit -F path=/etc/modprobe.d -F perm=wa -k soc_auditd2_modprobe
-a always,exit -F path=/etc/nsswitch.conf -F perm=wa -k soc_auditd2_nss
-a always,exit -F path=/etc/ntp.conf -F perm=wa -k soc_auditd2_ntp
-a always,exit -F path=/etc/pki/ca-trust -F perm=wa -k soc_auditd2_ca_trust
-a always,exit -F path=/etc/postfix -F perm=wa -k soc_auditd2_postfix
-a always,exit -F path=/etc/rsyslog.conf -F perm=wa -k soc_auditd2_rsyslog
-a always,exit -F path=/etc/rsyslog.d -F perm=wa -k soc_auditd2_rsyslog
-a always,exit -F path=/etc/securetty -F perm=wa -k soc_auditd2_securetty
-a always,exit -F path=/etc/selinux/config -F perm=wa -k soc_auditd2_selinux
-a always,exit -F path=/etc/skel -F perm=wa -k soc_auditd2_skel
-a always,exit -F path=/etc/sssd/sssd.conf -F perm=wa -k soc_auditd2_sssd
-a always,exit -F path=/etc/sudo-ldap.conf -F perm=wa -k soc_auditd2_ldap
-a always,exit -F path=/etc/sudo.conf -F perm=wa -k soc_auditd2_sudo
-a always,exit -F path=/etc/sysctl.conf -F perm=wa -k soc_auditd2_sysctl
-a always,exit -F path=/etc/sysctl.d -F perm=wa -k soc_auditd2_sysctl
-a always,exit -S all -F path=/etc/gshadow -F perm=r -F auid!=-1 -k soc_auditd2__etc_read_T1087_
```

```
Account_Discovery
-a always,exit -F path=/etc/gshadow -F perm=wa -k soc_auditd2_AccountDiscovery
-a always,exit -S all -F path=/etc/master.passwd -F perm=r -F auid!=-1 -k soc_auditd2__etc_read
-a always,exit -S all -F path=/etc/security/opasswd -F perm=r -F auid!=-1 -k soc_auditd2__etc_read
-a always,exit -S all -F path=/etc/spwd.db -F perm=r -F auid!=-1 -k soc_auditd2_etc_read
-w /etc/chef -p wa -k soc_auditd2_soft_chef
-w /etc/csh.cshrc -k soc_auditd2_T1546.004_5
-w /etc/csh.cshrc -p wa -k soc_auditd2_shell_profiles1
-w /etc/csh.login -k soc_auditd2_T1546.004_6
-w /etc/csh.login -p wa -k soc_auditd2_shell_profiles2
-w /etc/exim4/ -p wa -k soc_auditd2_mail
-w /etc/fish/ -p wa -k soc_auditd2_shell_profiles3
-w /etc/fluent/ -p wa -k soc_auditd2_fluentd_dir_change
-w /etc/fluent/fluent.conf -p wa -k soc_auditd2_fluentd_config_change
-w /etc/init.d/ -p wa -k soc_auditd2_T1037_2_init
-w /etc/init/ -p wa -k soc_auditd2_T1037_3_init
-w /etc/inittab -p wa -k soc_auditd2_T1037_init_change_init
-w /etc/ld.so.preload -p wa -k soc_auditd2_systemwide_preloads
-w /etc/modprobe.conf -p wa -k soc_auditd2_T1547.006_modprobe_config_change_modprobe
-w /etc/modules -p wa -k soc_auditd2_modprobe
-w /etc/network/ -p wa -k soc_auditd2_network_network_dir_change
-w /etc/otter -p wa -k soc_auditd2_soft_otter
-w /etc/pam.d/password-auth-ac -p wa -k soc_auditd2_T1201_pam_config_change
-w /etc/pam.d/system-auth-ac -p wa -k soc_auditd2_T1201_pam_config_change
-w /etc/puppet/ssl -p wa -k soc_auditd2_puppet_ssl
-w /etc/rsyslog.d/ -p wa -k soc_auditd2_rsyslog_dir_change
-w /etc/security/limits.d/ -p wa -k soc_auditd2_T1078.001_pam_dir_change
-w /etc/security/namespace.d/ -p wa -k soc_auditd2_T1078.001_pam_config_change
-w /etc/ssh/sshd_config -p wa -k soc_auditd2_T1098_Account_Manipulation_SSH_Authorized_
Keys
-w /etc/ssh/sshd_config.d -k soc_auditd2_sshd_config_change
-w /etc/sysconfig/network-scripts/ifcfg-device -p wa -k soc_auditd2_T1016_System_Network_
Configuration_Discovery
-w /etc/syslog-ng.conf -p wa -k soc_auditd2_syslog-ng_config_change
-w /etc/syslog-ng/ -p wa -k soc_auditd2_syslog-ng_dir_change
-w /etc/syslog-ng/security-config-omsagent.conf -p wa -k soc_auditd2_oms-agent_bin_change
-w /etc/syslog.conf -p wa -k soc_auditd2_syslog_config_change
-w /etc/syslog/ -p wa -k soc_auditd2_syslog_dir_change
-w /etc/systemd -p wa -k soc_auditd2_T1543.002_systemd_change
-w /etc/systemd/system -p wa -k soc_auditd2_T1543.002_systemd_change_create_or_Modify_
System_Process
-w /etc/timezone -p wa -k soc_auditd2_timezone
-w /etc/zsh/ -p wa -k soc_auditd2_shell_profiles
## Typical SYSCALLs
-a always,exit -F arch=b32 -S accept4 -k soc_auditd2_api_accept
-a always,exit -F arch=b32 -S listen -k soc_auditd2_api_listen
# excluded with msgtype=CAPSET upwards
#-a always,exit -F arch=b32 -S capset -k soc_auditd2_api_caps
-a always,exit -F arch=b64 -S accept4 -k soc_auditd2_api_accept
-a always,exit -F arch=b64 -S listen -k soc_auditd2_api_listen
#-a always,exit -F arch=b64 -S capset -k soc_auditd2_api_caps
# maybe huge events:
```

```
-a always,exit -F arch=b32 -S setuid,setgid,setreuid,setregid -F exit=EPERM -k soc_auditd2_api_
setuid
-a always,exit -F arch=b64 -S setuid,setgid,setreuid,setregid -F exit=EPERM -k soc_auditd2_api_
setuid
-a always,exit -F arch=b32 -S clock_adjtime -k soc_auditd2_time-change
-a always,exit -F arch=b64 -S clock_adjtime -k soc_auditd2_T1070.006_time-change
-a always,exit -F arch=b32 -S memfd_create -k soc_auditd2_anon_file_create
-a always,exit -F arch=b64 -S memfd_create -k soc_auditd2_anon_file_create
-a always,exit -F arch=b32 -S swapon -S swapoff -F auid!=-1 -k soc_auditd2_swap_change
-a always,exit -F arch=b64 -S swapon -S swapoff -F auid!=-1 -k soc_auditd2_swap_change
-a always,exit -F arch=b32 -S utimensat -k soc_auditd2_T1070.006_time_change
-a always,exit -F arch=b64 -S utimensat -k soc_auditd2_T1070.006_time_change
-a always,exit -F arch=b32 -S utimes -k soc_auditd2_T1070.006_time_change
-a always,exit -F arch=b64 -S utimes -k soc_auditd2_T1070.006_time_change
-a always,exit -F arch=b64 -S kexec_load -k soc_auditd2_T1014_kernel_swap_detected
-a always,exit -F arch=b32 -S sys_kexec_load -k soc_auditd2_T1014_kernel_swap_detected
##User Commands
-a always,exit -F arch=b64 -F auid>=1000 -F auid!=4294967295 -S execve -k soc_auditd_
UserCommands
##Root command executions
-a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k soc_auditd_
RootCMD
-a always,exit -F arch=b32 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k soc_auditd_
RootCMD
##-a always,exit -F arch=b64 -S all -F euid=0 -F perm=awx -k soc_auditd_RootCMD
```

Указатель