Легенда

Основная деятельность УК City в Государстве F связана с ЖКХ и государственными услугами. Управляющая компания отвечает за освещение улиц, работу систем видеонаблюдения, рекламных экранов и общественного транспорта. В ее ведении также находятся торговые и бизнес-центры, парковки, МФЦ и информационные общественные табло. УК City ответственна за оснащение квартир жителей IoT-устройствами и подключение к сети городского радиовещания.

Хакеры могут подпортить жизнь горожанам, например оставить их без онлайн-заказов из аптеки, уличного освещения, заблокировать жителей в квартирах и лишить их доступа к государственным услугам.

Совет:

Если вы плохо знакомы с языком запросов PDQL для MP SIEM, то советую ознакомиться с официальным справочником.

Выполните Задания 2.1

Задание

Руководитель отдела информационной безопасности City в бешенстве: несколько часов назад, в момент, когда он докладывал начальству о достижении высокого уровня защищенности городских систем, злоумышленники взломали рекламный экран в центре столицы и включили горожанам неприятные для просмотра ролики.

Восстановите последовательность действий нарушителей. Укажите FQDN атакуемого актива.

Атака проходила 22 ноября 2022 года — с 12:10:00 по 12:20:00 (UTC: 09:10:00–09:20:00).

Тактики, техники и подтехники атак по MITRE ATT&CK

1. 1.TA0001. Первоначальный доступ | T1190. Недостатки в общедоступном приложении