Описание готовых интеграций по реагированию

> Весь актуальный и новый контент с описанием добавляется в GitHub - https://github.com/KUMA-Community

Реагирование из коробки KUMA

Реагирование на KES через KSC:

- Запуск задачи обновления баз KES
- Запуск задачи сканирования KES

Реагирование KEDR:

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути

Реагирование KICS Networks:

- Изменение статуса актива на Разрешенное
- Изменение статуса актива на Неразрешенное

Реагирование AD (с версии KUMA 2.1):

- Блокировка УЗ
- Сброс пароля УЗ
- Добавление УЗ в группу и исключение из группы

Реагирование Kaspersky Automated Security Awareness Platform (KASAP) – это платформа для онлайн-обучения:

- Изменять группы обучения пользователей
- Просматривать информацию о курсах, пройденных пользователями, и полученных ими сертификатах

Готовые скрипты (описание)

Telegram Response:

- Оповещения об алерте в телеграм канале

Telegram Response Advanced:

- Оповещения об алерте в телеграм канале
- Бот позволяет закрывать алерты по кнопке, создавать резервную копию и выполнять команды ssh на KUMA.

UserGate Response:

- Блокировка по IP
- Блокировка по URL
- Блокировка по Домену

KEDR Response (script):

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути
- Логирование реагирования в системном журнале

AD Response:

- Блокировка УЗ и разблокировка
- Выход пользователя из активных сессий
- Добавление УЗ в группу и исключение из группы

KWTS Response:

- Блокировка по URL
- Блокировка по IP
- Блокировка по DOMAIN

KSMG Response (по запросу):

- Блокировка по EMAIL
- Блокировка по IP

KUMA:

- Защита от брутфорса интерфейса KUMA

Cisco ASA Firewall:

- Блокировка по IP

BIFIT Mitigator:

- Временная блокировка трафика по src_ip, dst_ip, src_port, dst_port, protocol

---

Revision #8
Created 20 December 2023 13:57:03 by Boris Rzr
Updated 18 September 2024 07:43:34 by Boris Rzr