hoster.by

Автоматизация рутины аналитика в SOC

Никита Десятник

Начальник отдела аналитики центра кибербезопасноти

hoster.by

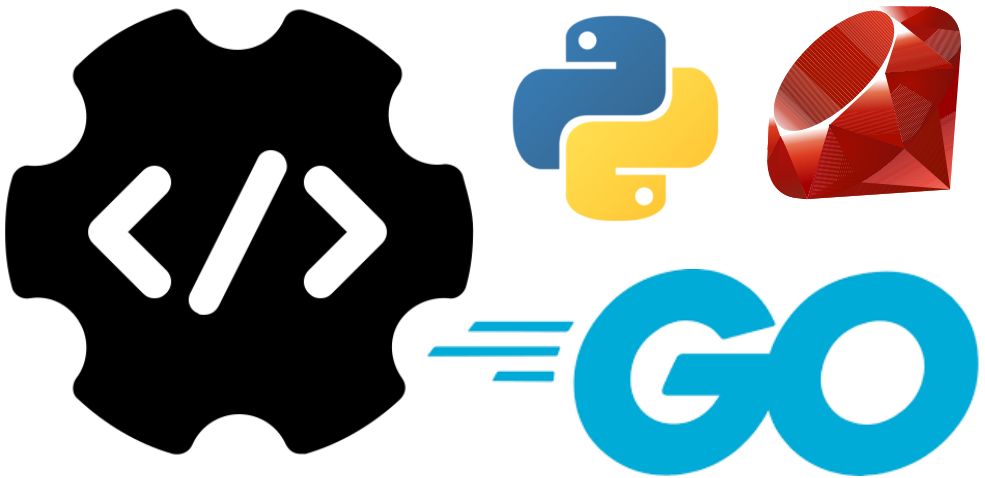
Зачем нужна автоматизация рутины аналитика в SOC?

Выгорание аналитиков

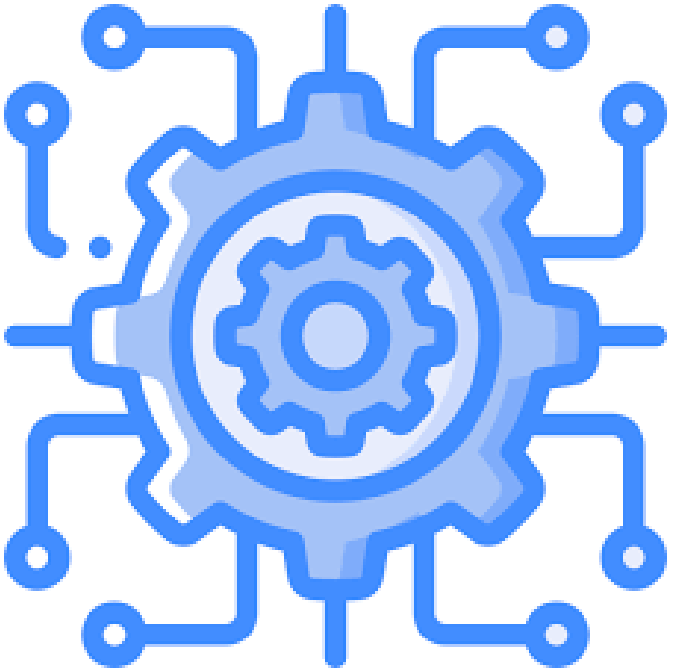
Улучшение метрик MTTD и MTTR

hoster.by

Способы автоматизации



Скрипты автоматизации на любом ЯП

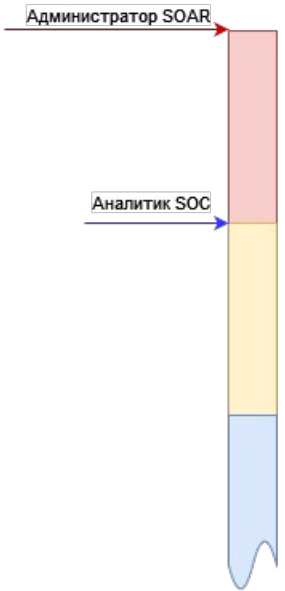


Решение SOAR

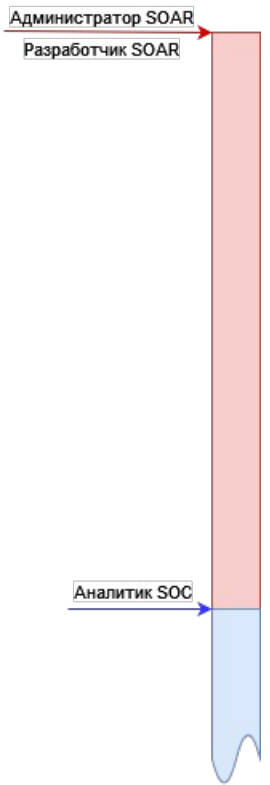
Виды SOAR

Коммерческие решения

Open source решения



Самописные системы



Этап разработки/внедрения

Этап автоматизации ключевых процессов

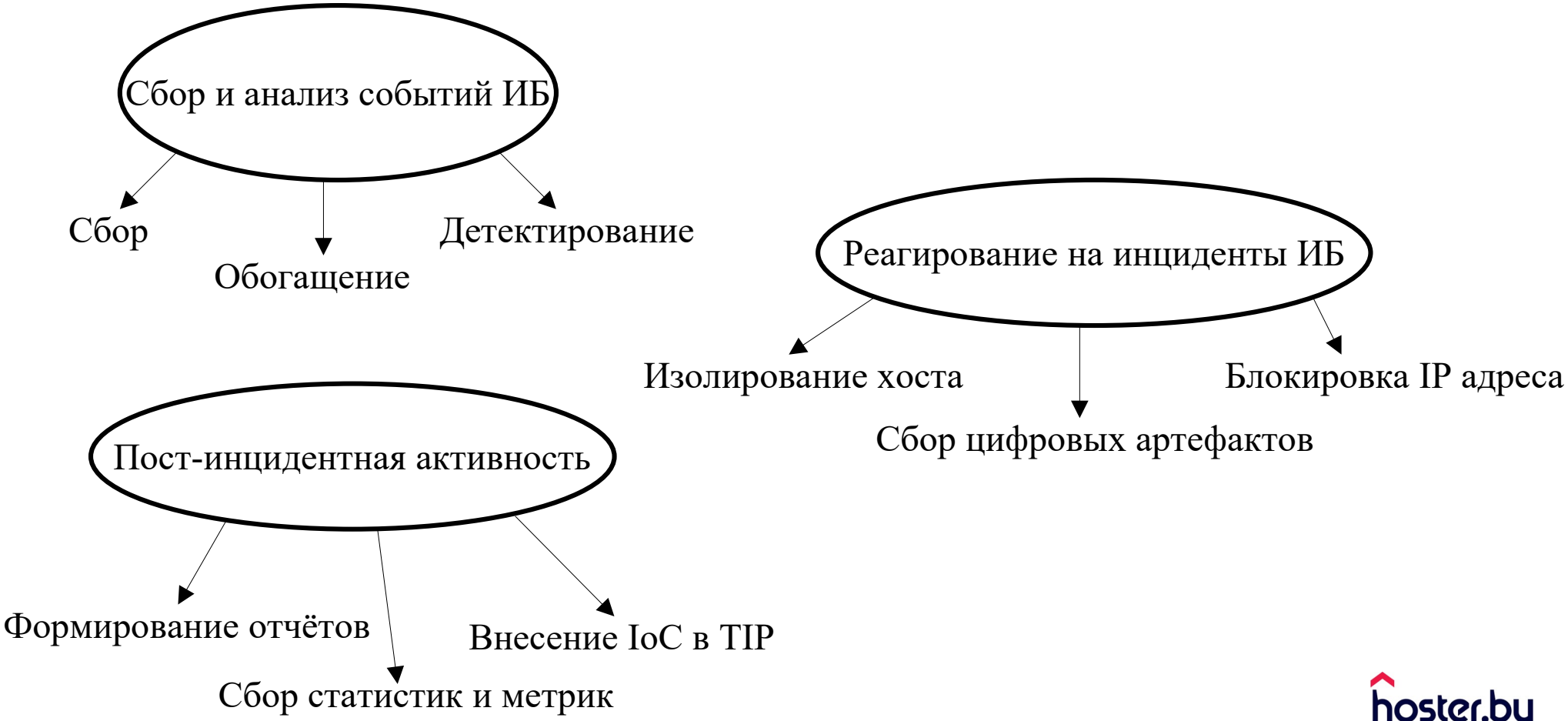
Этап эксплуатации и дальнейшего развития процессов

Подключение аналитика SOC к работе

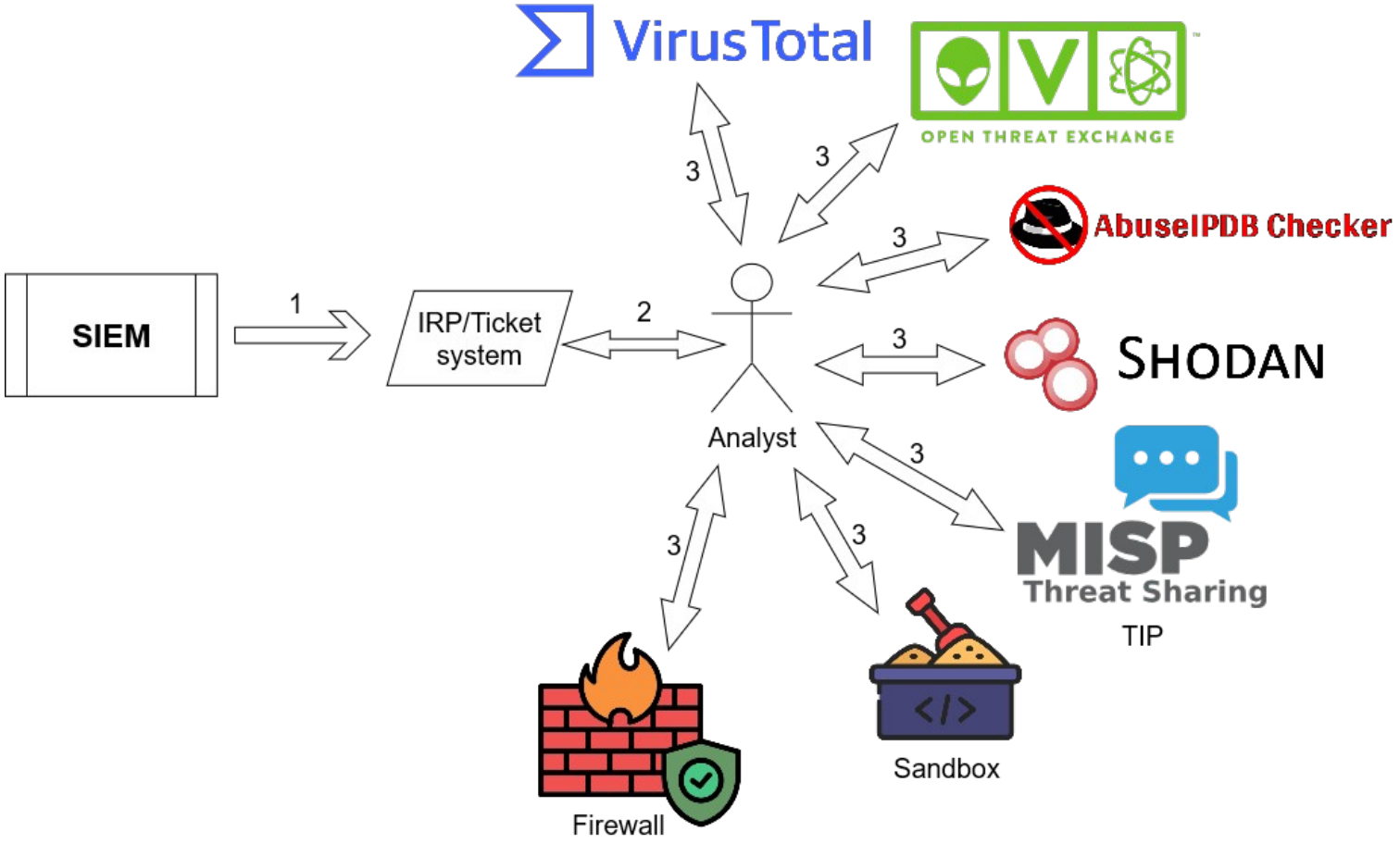
Подключение администратора(разработчика) системы SOAR из штата SOC к работе

hoster.by

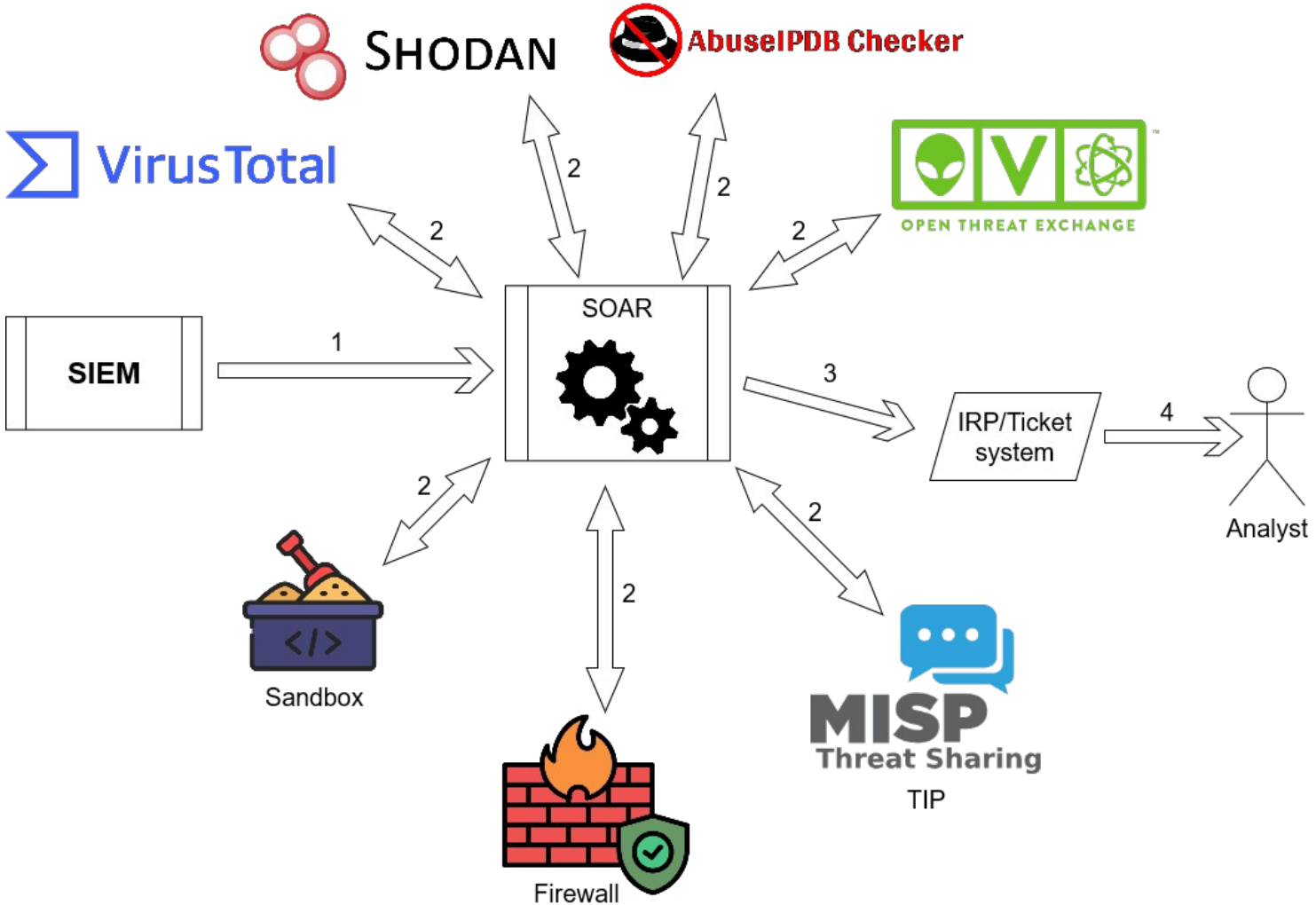
Что можно автоматизировать?



Сбор информации из дополнительных источников

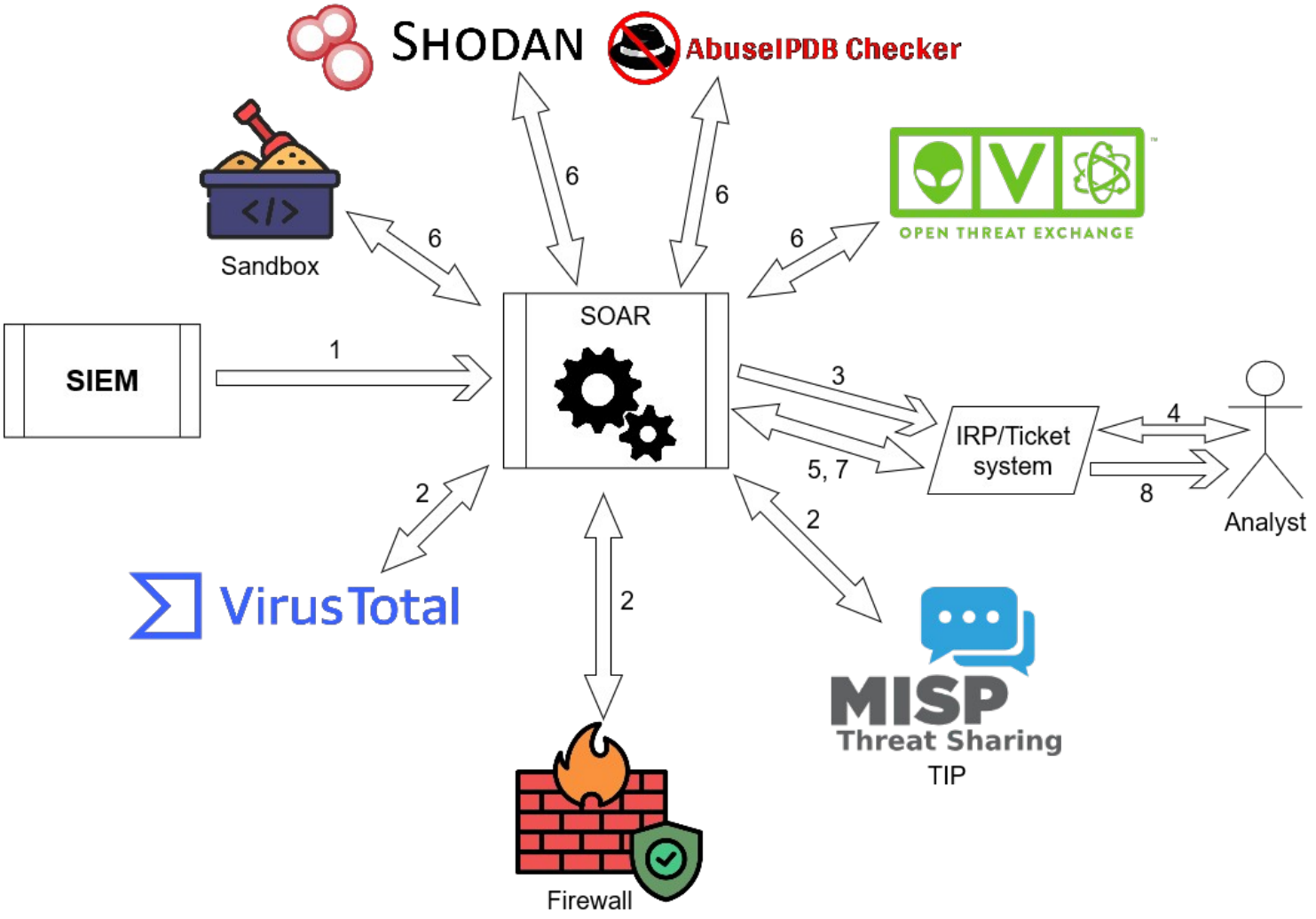


Сбор информации из дополнительных источников



hoster.by

Сбор информации из дополнительных источников



hoster.by

Что еще можно автоматизировать?

- Процессы управления активами
- Процессы управления уязвимостями
- Процессы разворачивания и управления Deception систем
- Процессы сбора и расчета статистики

Спасибо за внимание!

220006, г.Минск, ул. Аранская, 8, блок 1, 4 этаж
Почта info@hoster.by

hoster.by