ЕВРАЗ

Особенности внедрения и эксплуатации IRP/SOAR на промышленных предприятиях

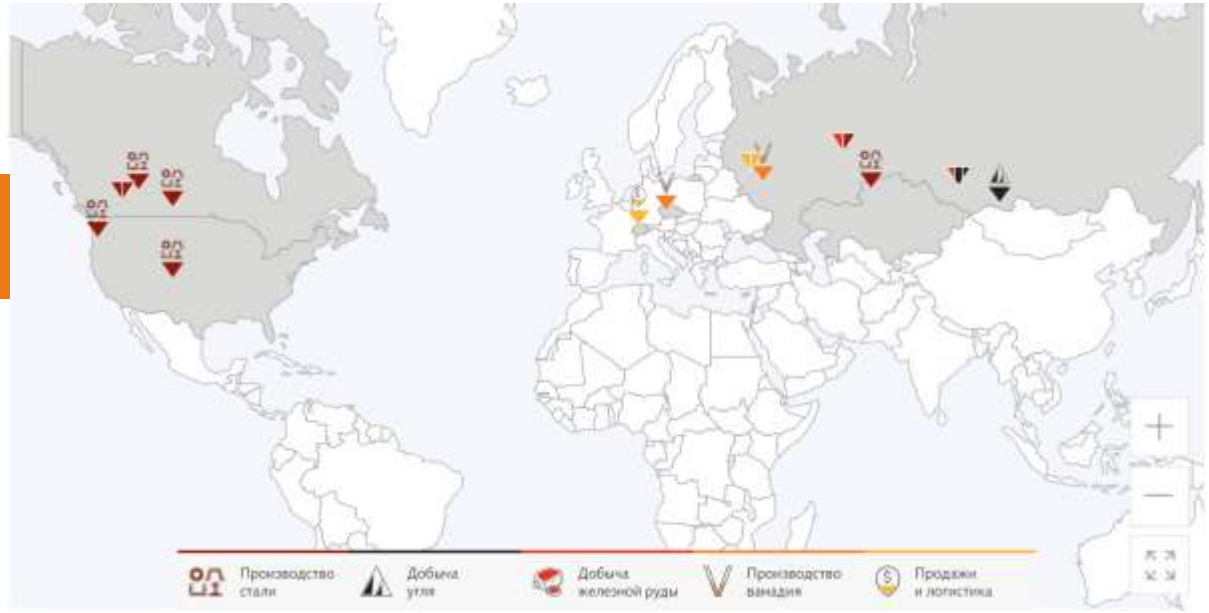
Нуйкин Андрей
CISM CISA АРСИБ
03.2022

Что такое ЕВРАЗ?

ЕВРАЗ

- ГЛОБАЛЬНАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа. Компания входит в ведущий индекс Лондонской Фондовой Биржи FTSE-100.



Создание SOC

ЕВРАЗ

На определенном этапе компании создают:

1. Систему мониторинга – видим что работает, а что не работает. Причину не знаем.

2. Систему мониторинга событий ИБ – видим, что не работает, понимаем почему.

3. Security Operations Center – видим что не работает, понимаем почему и можем управлять, реагировать и предотвращать.

Предпосылки внедрения IRP\SOAR

Со временем количество событий\инцидентов на оператора становится все больше.

Реагировать становится сложнее

Что делать?

ЕВРАЗ

В идеале нужна полная автоматизация.

В реальности нужно освободить операторов от рутинной ручной работы, в том числе и в части постановки задач ответственным на местах с дальнейшим отслеживанием их исполнения.

Предпосылки внедрения IRP\SOAR

ЕВРАЗ

В процессе реагирования возможны проблемы:

- SOC или администраторы работает по схеме 5\8.
  Ночью и в выходные никого нет.
- Ручной сбор информации по событиям\инцидентам.
- Много 1Click событий.
- У специалистов SOC нет возможности управлять всеми средствами защиты
- Нет единой среды постановки задач и контроля их в рамках процедур реагирования
- Недостаточная скорость реакции
- Потеря времени при расследовании инцидентов, вплоть до пропуска

Особенности внедрения и эксплуатации IRP/SOAR на промышленных предприятиях

ЕВРАЗ

По типу событий производственные компании **не сильно отличаются** от компаний других секторов. Среди основных событий:

- Фишинговые письма
- Вирусные заражения
- Брутфорс интернет-сервисов

Но некоторые отличия всё же есть:

Технологические сервисы обычно не имеют прямого доступа к корпоративной сети, а уж тем более к Интернет, поэтому, как правило злоумышленникам необходимо пройти сквозь Internet DMZ, корпоративную сеть и АСУТП DMZ. Пройти незамеченным весьма сложно.

Особенности внедрения и эксплуатации IRP/SOAR на промышленных предприятиях

ЕВРАЗ

Специфика производственных инфраструктур:

- Проприетарные системы/протоколы.
- Наличие критичных, но устаревших систем и приложений, разработанных без учета требований ИБ.
- Необходимость получать информацию с нестандартных, труднодоступных, географически распределенных источников.
- Приоритет непрерывности технологических процессов над требованиями ИБ.

Особенности внедрения и эксплуатации IRP/SOAR на промышленных предприятиях

ЕВРАЗ

Специфика ИБ и реагирования на киберинциденты в промышленности

- Географически распределенная инфраструктура с зачастую ограниченным/низкоскоростным сетевым доступом.
- Невозможность использования облачных систем ИБ, "приземление" всех сервисов.
- Замедленное реагирование на инциденты/сообщения из-за разницы часовых поясов, нехватки сотрудников на местах, работы в режиме 8х5.
- Специфические модели угроз и нарушителей: интересны APT-группировкам, киберармиям, профессиональным финансово-мотивированным хакерам, нацеленным на кражу информации, шантаж приостановкой деятельности, повреждение оборудования.
- Нормативные требования (КИИ, АСУТП).
- Регламентировано время реагирования на киберинцидент на объекте КИИ: время передачи информации об инциденте в НКЦКИ (систему ГосСОПКА) - не позднее 3 часов с момента обнаружения (для значимых объектов КИИ).
- Выполнение процедур реагирования в технологическом сегменте возможно только через постановку задач (ITSM/Эл.почта) ответственным специалистам на местах.

Особенности автоматизации реагирования с помощью IRP/SOAR в промышленности

ЕВРАЗ

Есть множество рутинных и типовых задач позволяющих их автоматизировать.

- Обогащение событий\инцидентов информацией из различных источников.
- Блокировка IP\URL на периметре.
- Изоляция ПК\Сервера
- Запуск сканирований на вирусы
- Поиск по базам TI
- Оповещение

Особенности автоматизации реагирования с помощью IRP/SOAR в промышленности

ЕВРАЗ

Как могут помочь IRP/SOAR-системы

- Роботизация и автоматизация ручных действий аналитиков на L1 в SOC: можно в нерабочее время (в случае SOC 8x5) включать "автопилот", в котором IRP/SOAR выполнит действия по реагированию в соответствии с playbook.
- Возможность автоматизации поиска признаков компрометации, например, путем сравнения значений хэш-сумм системных и исполняемых файлов с allow list.
- Применение технологий искусственного интеллекта, машинного обучения, Big Data для выявления аномалий, подсказок аналитикам SOC, автоматического немедленного реагирования на однозначно True Positive события.

Особенности автоматизации реагирования с помощью IRP/SOAR в промышленности

ЕВРАЗ

Как выбрать подходящую IRP/SOAR-систему для производственного предприятия

- Гибкость для взаимодействия с нестандартными/проприетарными системами и протоколами.
- Интеграция с разнообразными СЗИ, а также с зачастую устаревшими системами и взаимодействие со встроенными в них механизмами обеспечения кибербезопасности.
- Применение технологий искусственного интеллекта, машинного обучения, Big Data.
- Поддержка взаимодействия с системой ГосСОПКА (НКЦКИ) для выполнения законодательных норм.

Что же такое IRP\SOAR?

Incident Response Platform (IRP) – платформа, предназначенная для автоматизации процессов мониторинга, учета и реагирования на инциденты информационной безопасности

Security Orchestration, Automation and Response (SOAR) - класс программных продуктов, предназначенных для оркестровки систем безопасности, то есть их координации и управления ими.

Что делает оператор при инциденте

Пример: Получение фишингового письма

- Анализ заголовков и выявление имени и адреса почтового сервера
- Поиск в базах TI
- Выделение ссылок и вложений
- Анализ вложений в песочнице
- Анализ вложений во внешних системах (Virustotal и др.)
- Анализ ссылок в песочнице
- Анализ ссылок во внешних системах (Virustotal и др.)
- Создание IOC
- Получение списка пользователей получивших письмо
- Очистка ящиков от фишингового письма
- Запуск антивирусных проверок
- Блокировка URL и почтовых адресов
- И т.д.

Что делает оператор при инциденте

Пример: Брутфорс внешнего сервиса

- Получение IP атакующих
- Проверка адреса
- Занесение в лист блокировки
- NGFW по таймеру или API применяет лист блокировки

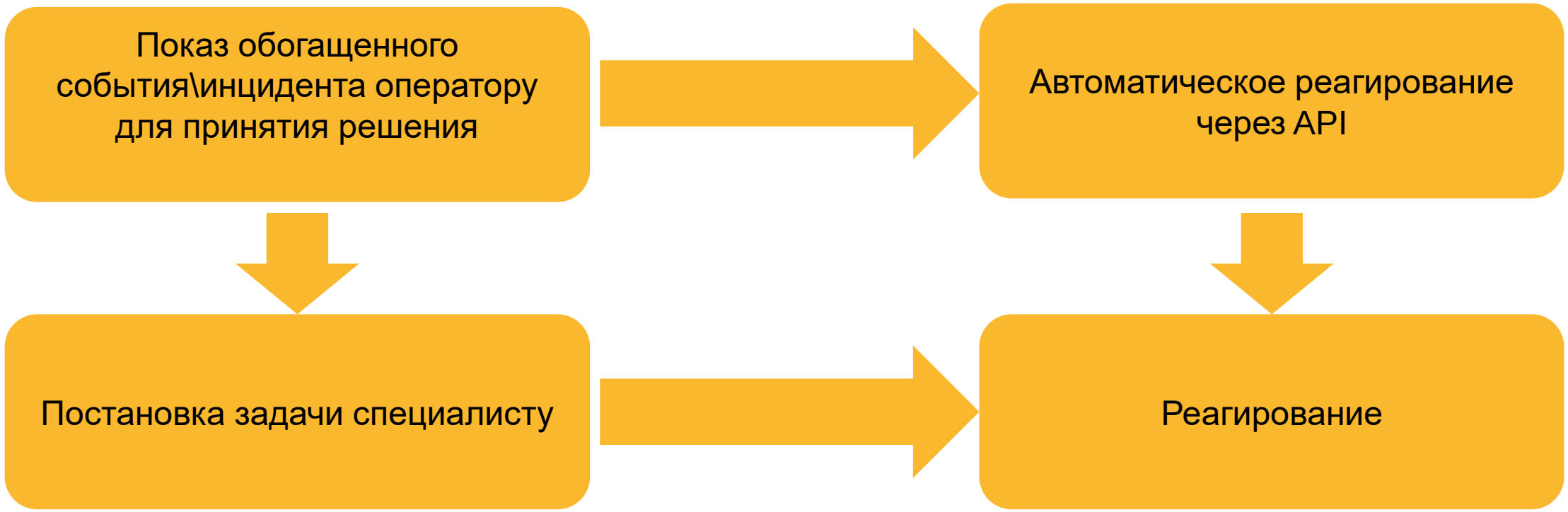
IRP

ЕВРАЗ

При получении информации о событии/инциденте запускается определенная процедура (playbook), которая автоматически делает большую часть рутинной работы:

- Собирает дополнительные данные по участникам события\инцидента из различных источников.
- Ищет по базам TI
- Проверяет IOC
- Запрашивает внешние источники
- И т.д.

По результатам сбора информации происходит:



Выводы

ЕВРАЗ

Внедряя IRP\SOAR мы:

- Снижаем рутинную нагрузку на операторов SOC
- Уменьшаем количество операторов SOC
- Снижаем показатели MTTD (Mean Time To Detect, среднее время обнаружения инцидента)
- Снижаем показатели MTTR (Mean Time To Respond, среднее время реагирования на инцидент)
- Снижаем зависимость от специалистов по управлению средствами защиты
- Улучшаем контекст инцидента за счет обогащения информацией
- Четко описываем и фиксируем сценарий реагирования
- Объединяем различные средства защиты в единый организм
- И много других

Выводы

ЕВРАЗ

Внедряя IRP\SOAR мы:

- Снижаем рутинную нагрузку на операторов SOC
- Уменьшаем количество операторов SOC
- Снижаем показатели MTTD (Mean Time To Detect, среднее время обнаружения инцидента)
- Снижаем показатели MTTR (Mean Time To Respond, среднее время реагирования на инцидент)
- Снижаем зависимость от специалистов по управлению средствами защиты
- Улучшаем контекст инцидента за счет обогащения информацией
- Четко описываем и фиксируем сценарий реагирования
- Объединяем различные средства защиты в единый организм
- И много других

ЕВРАЗ

Спасибо за внимание

Андрей Нуйкин
CISA, CISM
АРСИБ
RuSCADASec Coin #29

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com