ЕВРАЗ

SOAR, IRP: зачем внедрять

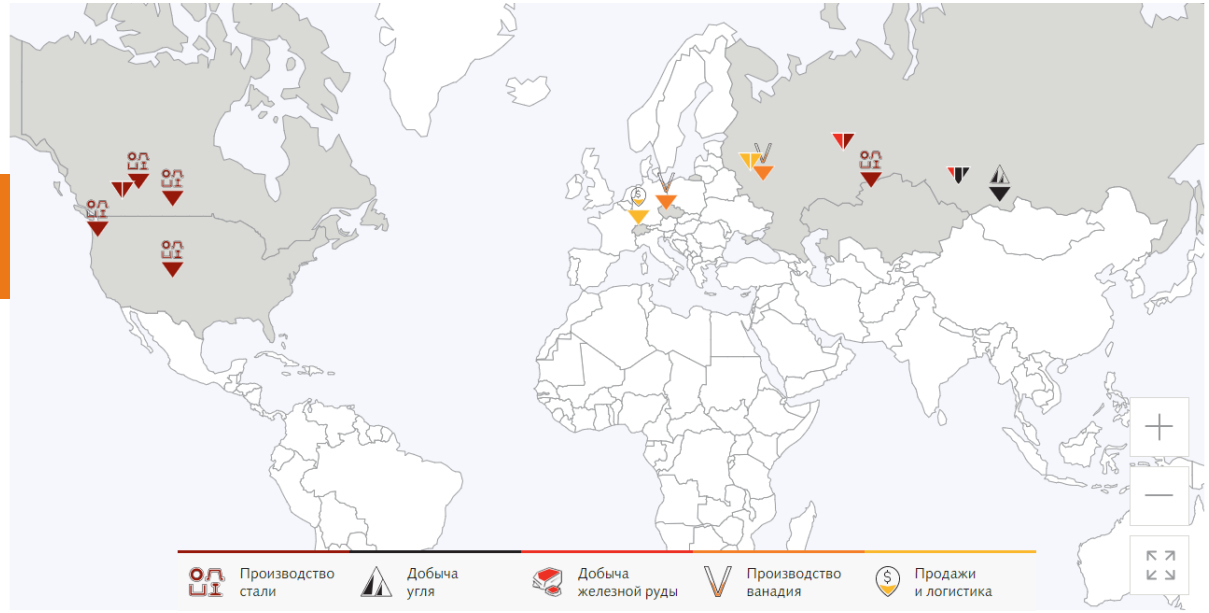
Нуйкин Андрей
CISM CISA АРСИБ
10.2020

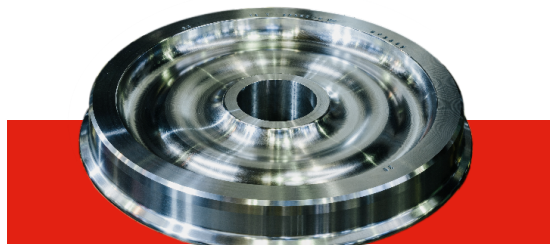
Что такое ЕВРАЗ?

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

ЕВРАЗ

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

Реагировать становится сложнее

Предпосылки внедрения IRP\SOAR

ЕВРАЗ

В процессе реагирования возможны проблемы:

- SOC 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
- Недостаточная скорость реакции
- Потеря времени при расследовании инцидентов, вплоть до пропуска

Что делать?

ЕВРАЗ

В идеале нужна полная автоматизация.

В реальности нужно освободить операторов от рутинной ручной работы.

Автоматизация

ЕВРАЗ

Есть множество 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

Что же такое IRP\SOAR?

ЕВРАЗ

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

ЕВРАЗ

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.

IRP

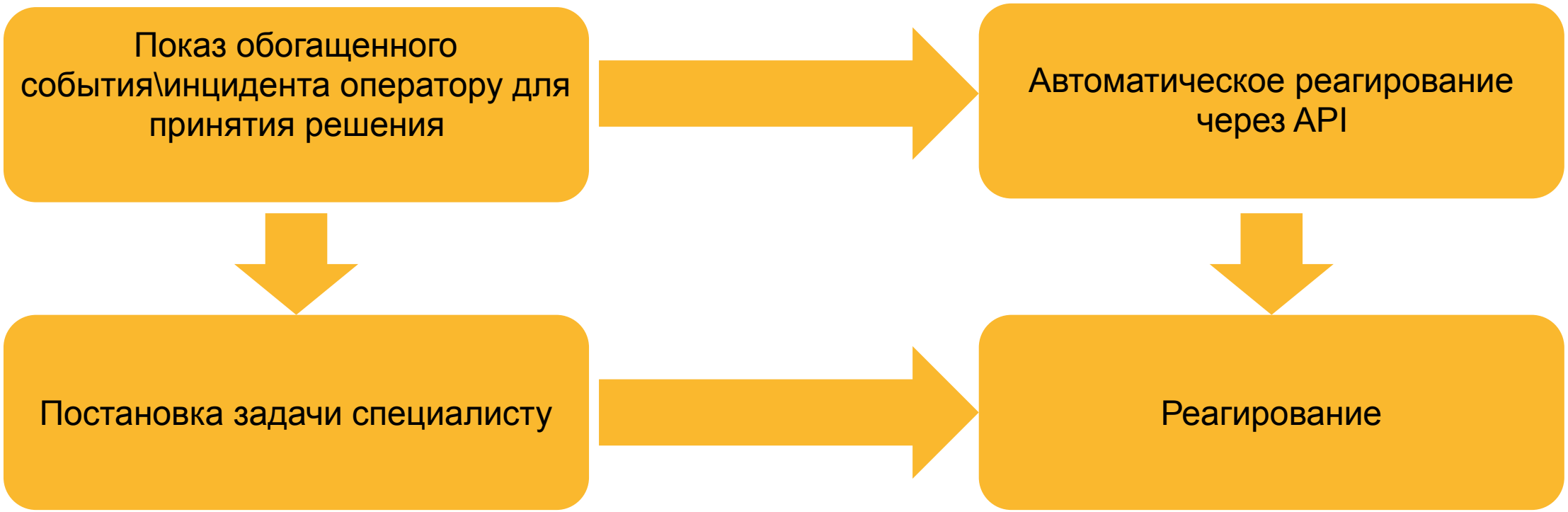
ЕВРАЗ

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

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

ЕВРАЗ

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
- И много других

ЕВРАЗ

Спасибо за внимание

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com