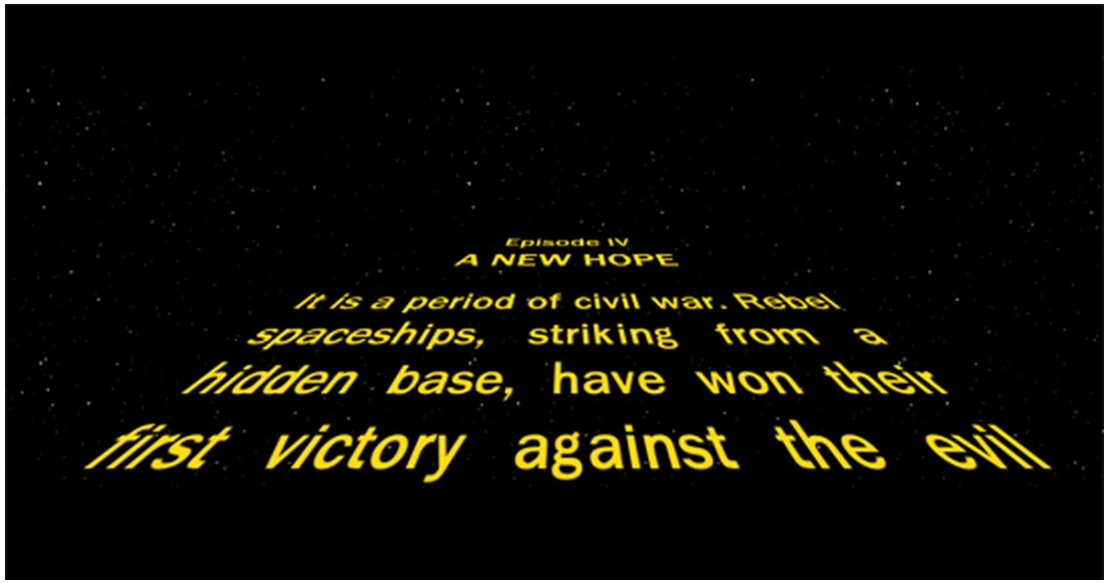
Постановка на мониторинг JSOC ИТ-ресурсов и технологического сегментов ГК «Содружество»

Баландин Евгений
Начальник отдела информационной безопасности

Предыстория



Территориальные особенности региона накладывают ограничения на кадровый потенциал, а именно на наличие местных квалифицированных и опытных ИБ-специалистов. Также общий дефицит специалистов в области ИБ на рынке труда не позволяли подобрать необходимый персонал, также длительный период на внедрение собственного SIEM и построение системы мониторинга 24/7, поэтому построение собственного SOC было не рациональным.

Было принято решение протестировать услуги MSSP-провайдеров по мониторингу и реагированию на события ИБ.

Пилот (старт)

В 2017 году выделили для себя двух основных MSSP-провайдеров:

JSOC от ООО «Солар Секьюрити» и RTK SOC от ПАО «Ростелеком».

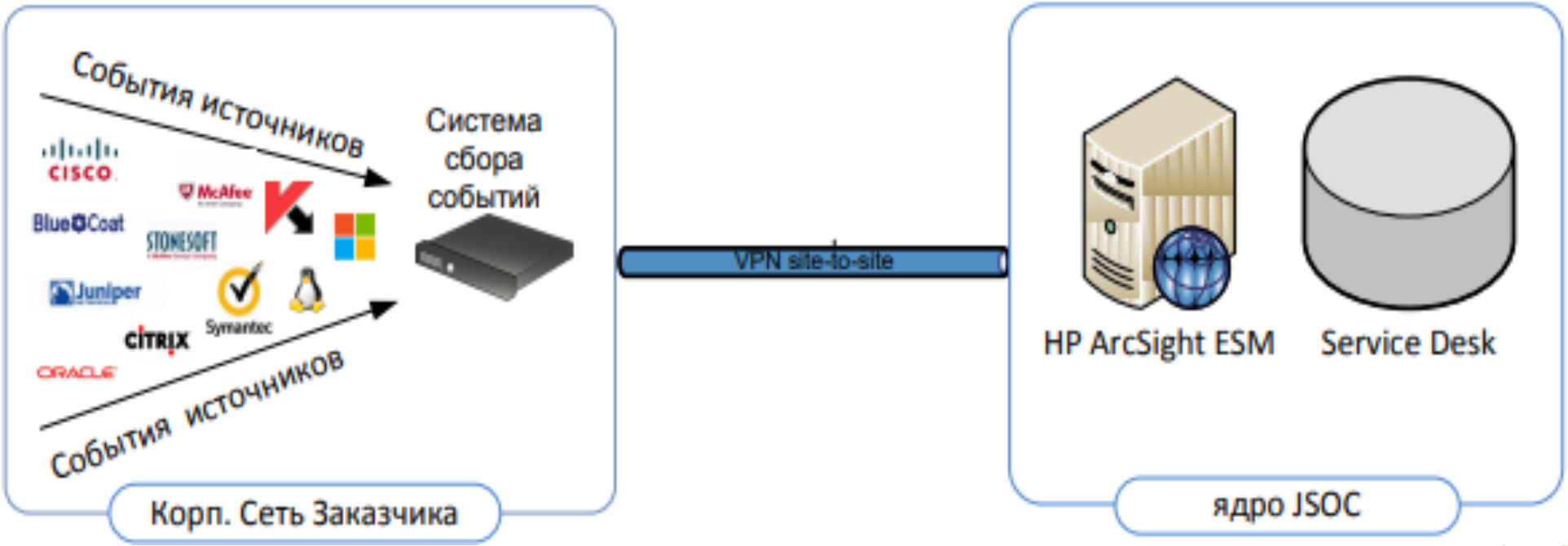
Пилот (финиш)

В конце такого параллельного пилота нам было сложно выявить победителя, т.к. задания на пилот выполнили оба MSSP-провайдера, уровень сервиса у обоих на должном уровне, явного перевеса в пользу одного из участников не было.

В итоге мы узнали о слиянии JSOC от ООО «Солар Секьюрити» и RTK SOC от ПАО «Ростелеком», и в результате мы получили два в одном - JSOC от ООО «Ростелеком Солар».

Этап 1

На первом этапе произведено подключение к JSOC ключевых ИТ-ресурсов и СЗИ в России, Европе и Латинской Америке по облачному типу.



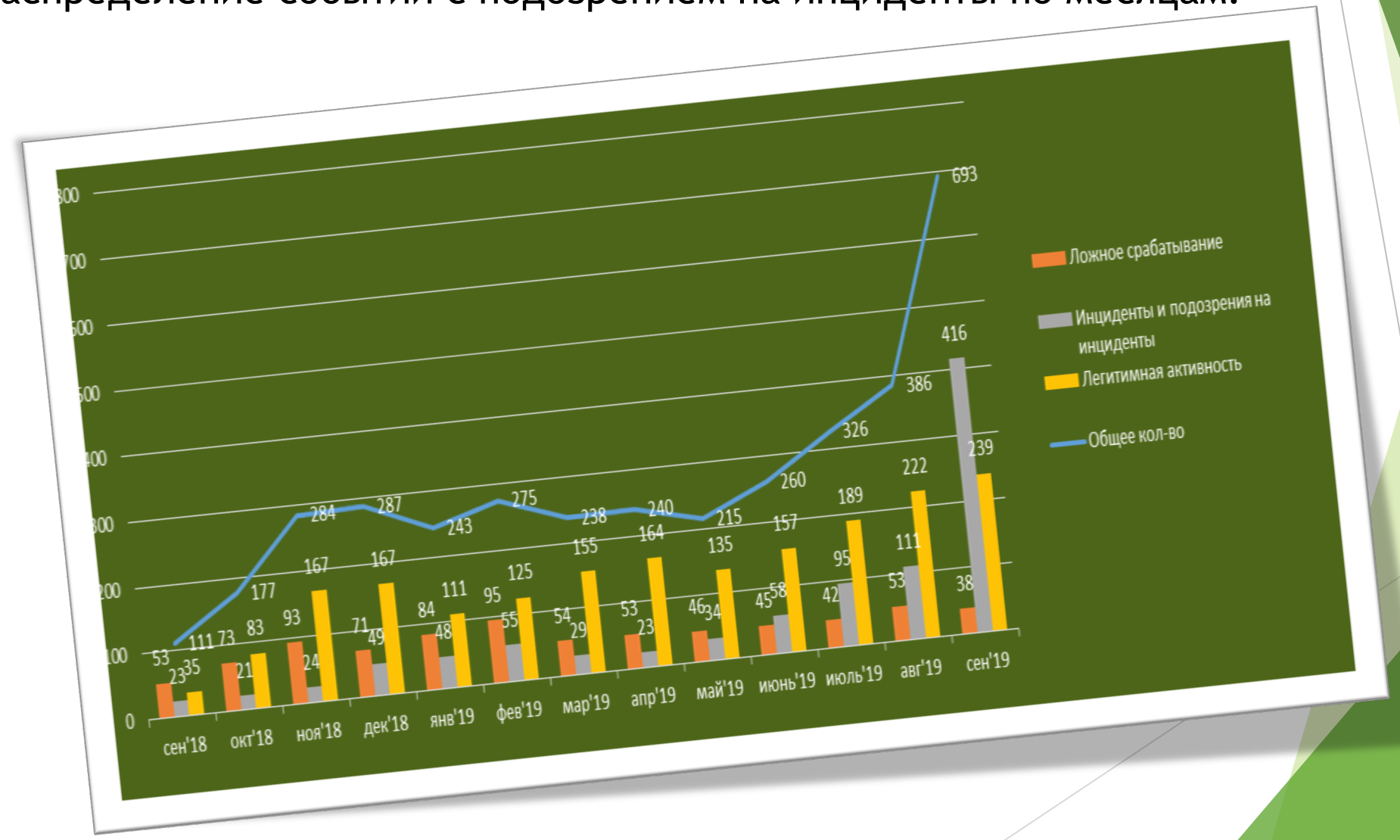
Этап 1

За первый год:

- подключено более 130 источников событий;
- запущено 55 сценариев мониторинга;
- достигнут поток в 1522 EPS;
- ежеквартально обрабатывается около 3,7 млрд. событий от всех источников;
- средний поток – 75 ГБ в день;

Этап 1

Распределение событий с подозрением на инциденты по месяцам:



Этап 2

Как у любой производственной компании, основные риски и угрозы связаны с АСУ ТП, поэтому следующим этапом стал переход к мониторингу событий из технологического сегмента.

Производственные предприятия расположены в 4-х странах мира:

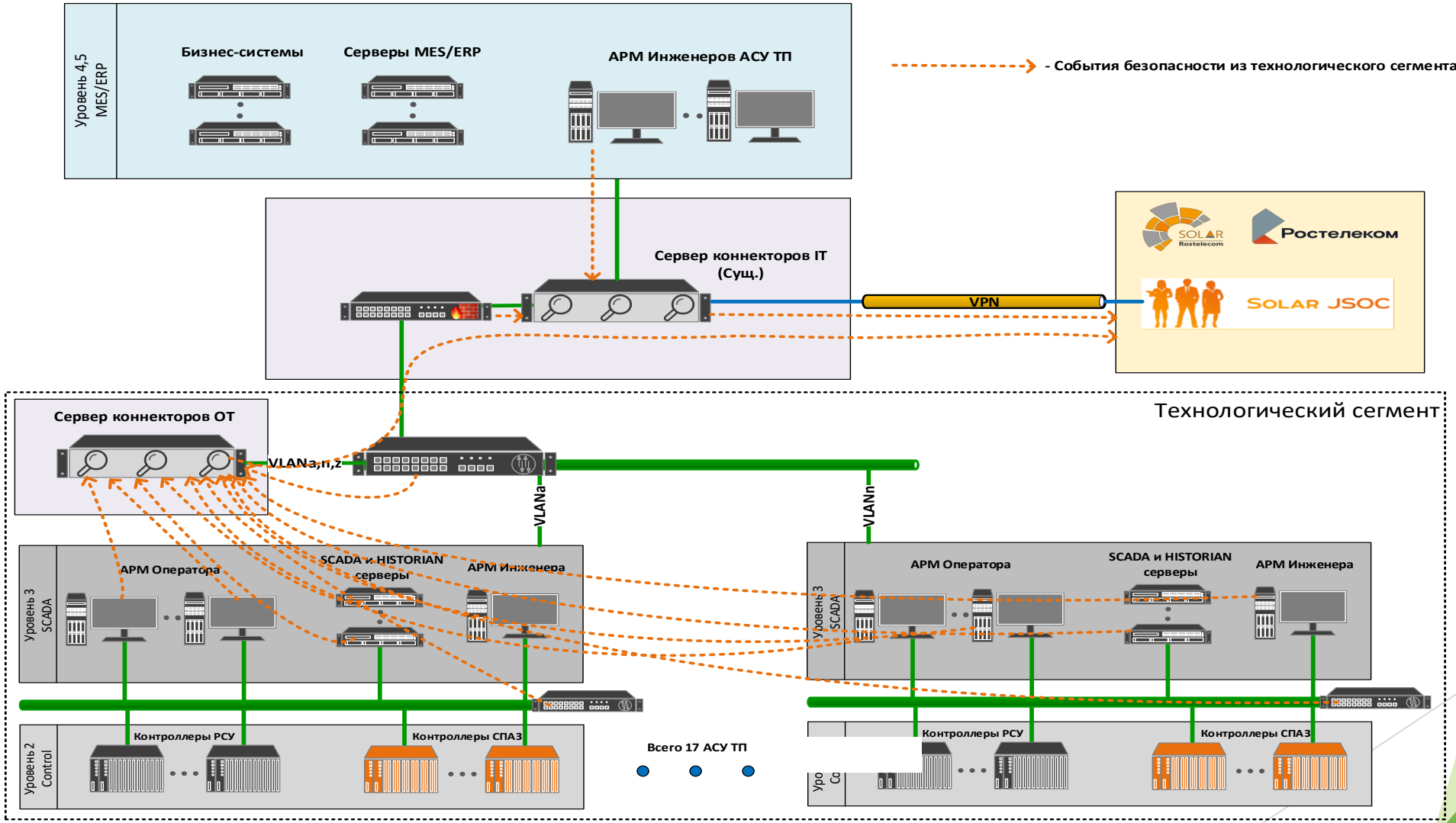
- Россия, Калининградская область, г.Светлый;
- Республика Беларусь, г.Сморгонь;
- Бразилия, муниципалитет Сан-Жуаким-да-Барра;
- Турция, г.Измир.

Более десяти производителей программируемых логических контроллеров.

Более десяти производителей прикладного ПО.

Полный перечень операционных систем Win-семейства.

Этап 2
Возможная схема подключения к JSOC



Этап 2
Проведение тестирования

В качестве области проведения тестирования выбран один из действующих заводов в г.Светлый:

- подключены АРМ инженеров АСУ ТП, расположенных в корпоративном сегменте;
- подключены АРМ операторов АСУ ТП, расположенных в производственной зоне.

На этапе тестирования осуществлялся мониторинг следующих событий:

- логи безопасности;
- системные логи;
- SQL Server;
- Powershell;
- планировщики задач;
- наложенные СЗИ.

Сформирован перечень сценариев реагирования на инциденты ИБ в сегменте АСУ

Период проведения тестирования составил 1,5 месяца

Этап 2. Итоги тестирования

- Написаны парсеры для ряда наложенных средств защиты;
- Переформированы маршруты уведомлений: информация об инцидентах ИБ в сегменте АСУ поступает в профильного специалиста по информационной безопасности;
- Пересчитаны уровни критичности для каждого из сценариев и подключенных источников технологического сегмента;
- Запущены сценарии по 5 категориям угроз для АСУ:
  - компрометация сегмента АСУ;
  - критическая атака в сегменте АСУ;
  - нарушение технологических процессов;
  - нарушение целостности сегмента АСУ;
  - нарушение изоляции сегмента АСУ.

Этап 2. Итоги тестирования

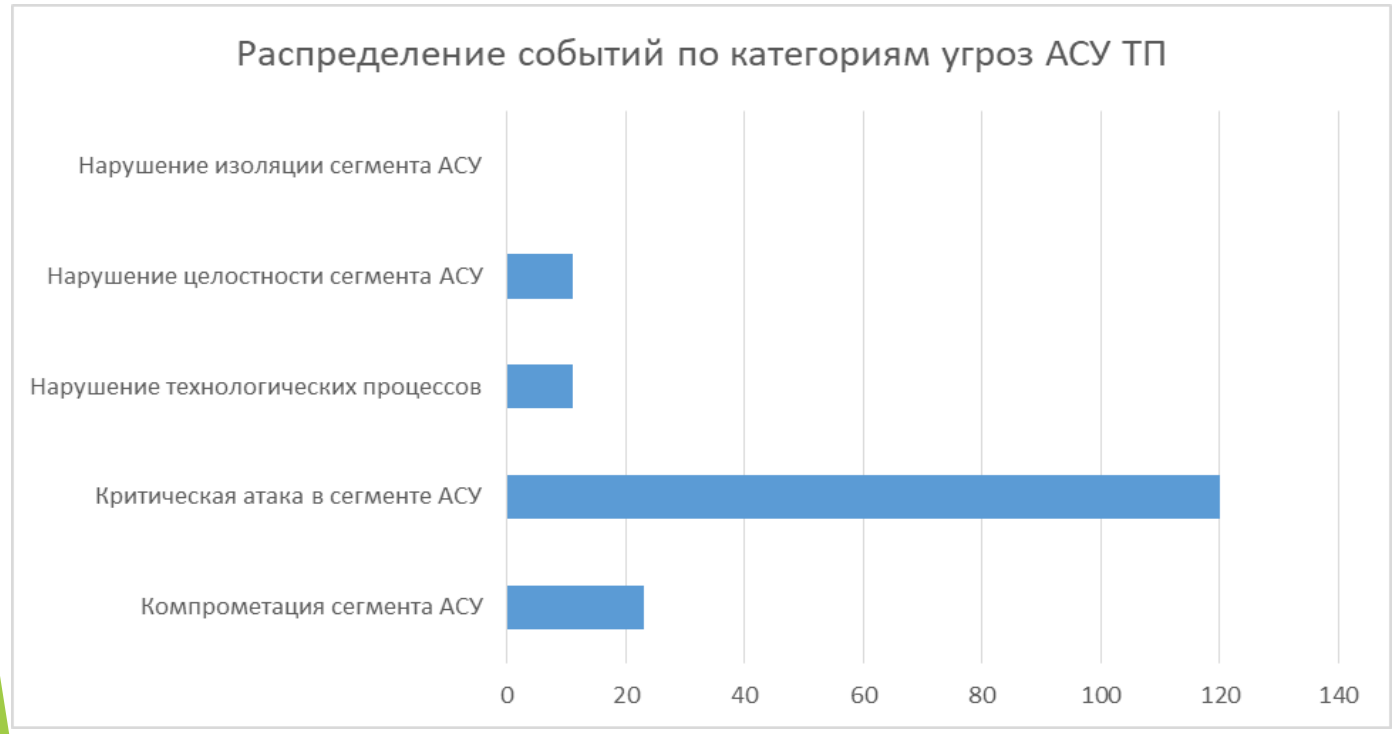
Группы запущенных сценариев:

- Компрометация сегмента АСУ – 13
- Критическая атака в сегменте АСУ – 13
- Нарушение технологических процессов – 11
- Нарушение целостности сегмента АСУ – 9
- Нарушение изоляции сегмента АСУ - 8

Этап 2. Итоги тестирования

Всего было зафиксировано 165 событий информационной безопасности.

Было получено 25 уведомлений от специалистов JSOC, все были проанализированы и квалифицированы как легитимные.



Группы запущенных сценариев

- Компрометация сегмента АСУ – 23
- Критическая атака в сегменте АСУ – 120
- Нарушение технологических процессов – 11
- Нарушение целостности сегмента АСУ – 11
- Нарушение изоляции сегмента АСУ - 0

В итоге

На текущий момент:

- Текущий этап тестирования завершен и выбранная схема переведена в промышленную эксплуатацию;

Что надо сделать на тестовой площадке:

- Осуществить подключение активного сетевого оборудования;
- Осуществить подключение SCADA систем и ПЛК;
- Провести еще один этап тестирования после подключения дополнительных источников;
- Осуществить масштабирование на иные заводы данного типа, расположенных на других площадках.

Благодарю за внимание!