31/05/2018

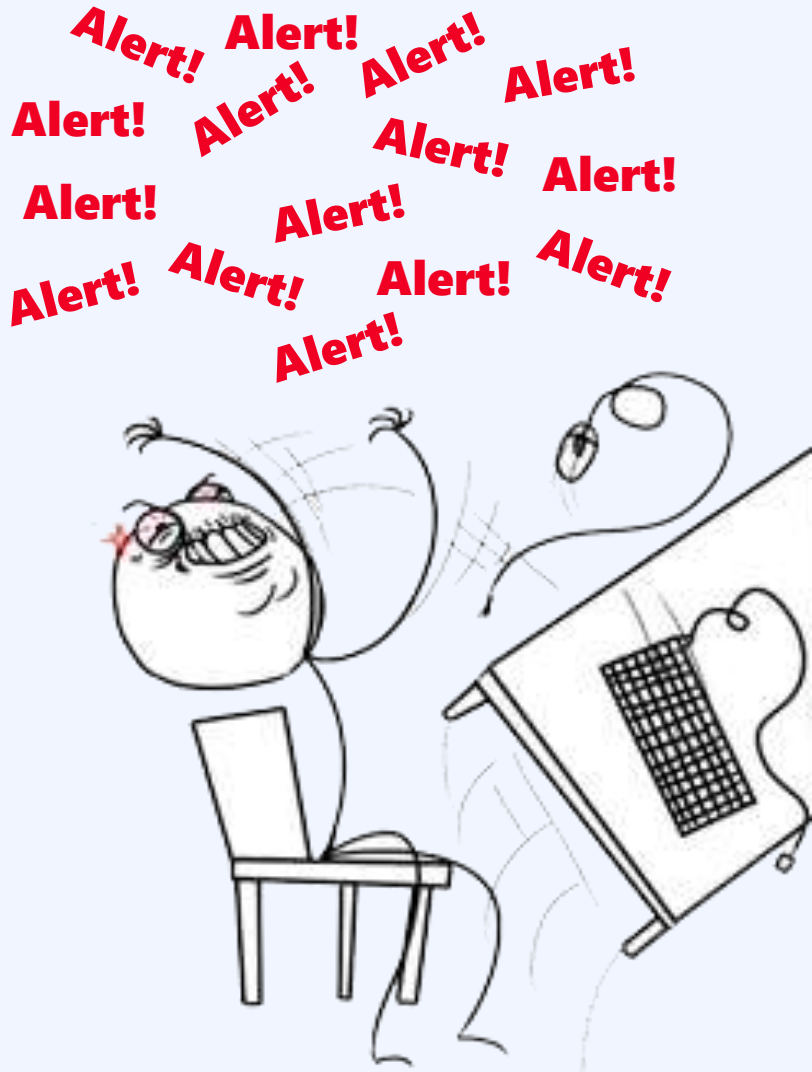
АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ

Анна Богданова

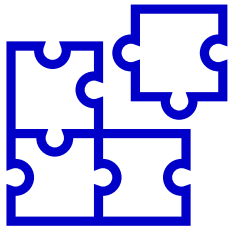
Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95

ПРОБЛЕМАТИКА

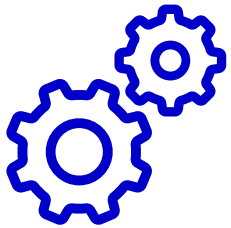
- Нет формализованного процесса
- Нет планов реагирования (play-books)
- Не автоматизирован ЖЦ инцидентов
- Нет единого информационного пространства
- Нет единой базы инцидентов
- Нет централизации
- Не хватает персонала



КАК АВТОМАТИЗИРОВАТЬ ПРОЦЕСС?



SIEM

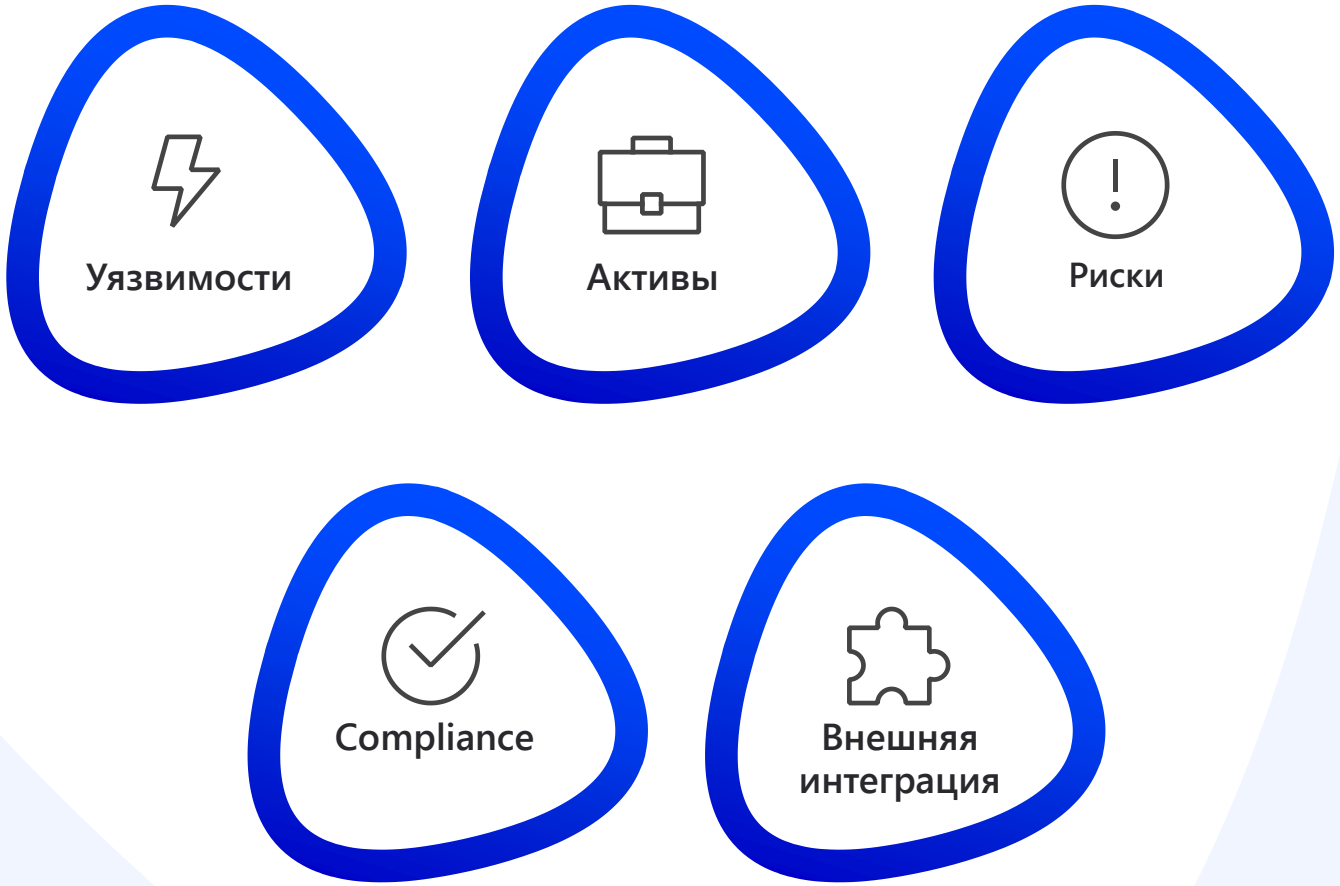


Service Desk

IRP

INCIDENT RESPONSE PLATFORM

ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ IRP-СИСТЕМ



ОСОБЕННОСТИ IRP-СИСТЕМ

- Снижение нагрузки на персонал
- Организация процесса управления инцидентами ИБ
- Совершенствование ИБ в целом

IRP — катализатор перемен в ИБ

- Не работают «из коробки»!
- Полноценные процессы ~ 1 год

IRP — технологическая платформа для построения процессов, а не готовый инструмент для расследования инцидентов

КАК ВЫБРАТЬ IRP-СИСТЕМУ?

Функционал

- IRP
- SGRC
- BI
- CMDB
- VM
- Compliance

Интеграция

Источники данных

SIEM | DLP | IDM | IDS

Внешние системы

Help Desk | TIP | FinCERT | ГосСОПКА

Реагирование

AD | FW | Endpoint | SCCM

РЫНОК IRP-СИСТЕМ

RVision

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

resilient

CYBERBIT

eplatform

JET SIGNAL


Интеграция
Дежурные смены
Планы мероприятий
Профили пользователей
Ролевая Модель
Аналитика
Активы
Новостная лента
Инциденты
JET SIGNAL
Поручения
Распорядительные документы
Уязвимости
Веб-чат
База знаний
Журналирование
Справочники
Информационные кампании
Рабочие столы

31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

Анна Богданова

Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95