IBM Security

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

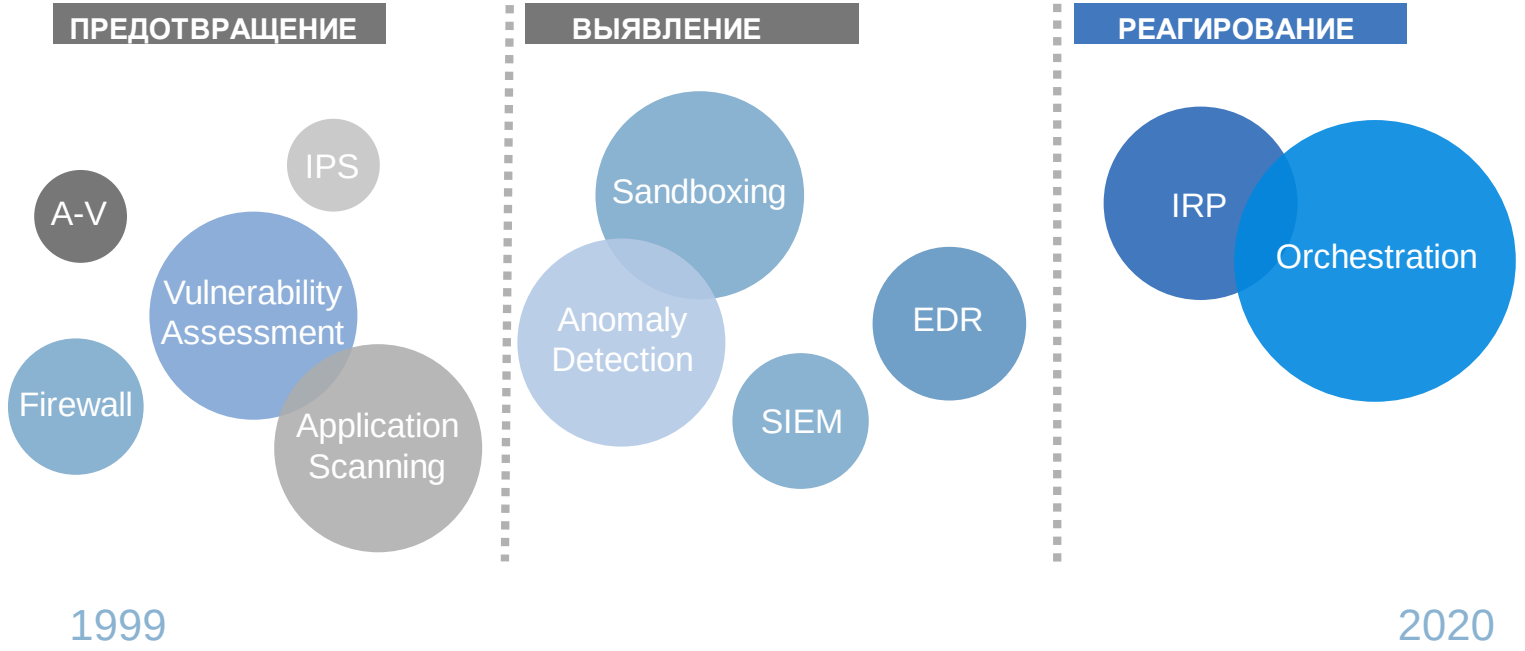
Как эффективно автоматизировать процессы реагирования на инциденты

Олег Бакшинский
Ведущий советник по вопросам информационной безопасности

19 сентября 2019 г.

IBM

Оркестрация как развитие платформы реагирования



Оркестрация как развитие платформы реагирования

Проблемы, возникающие в результате все более враждебного ландшафта угроз, в сочетании с нехваткой людей, опыта и бюджета побуждают организации к использованию технологий SOAR».

Gartner

SOAR = SOA + SIR + TIP

Реагирование на инциденты

Разбор инцидентов сегодня зачастую происходит вручную и без связи между отделами

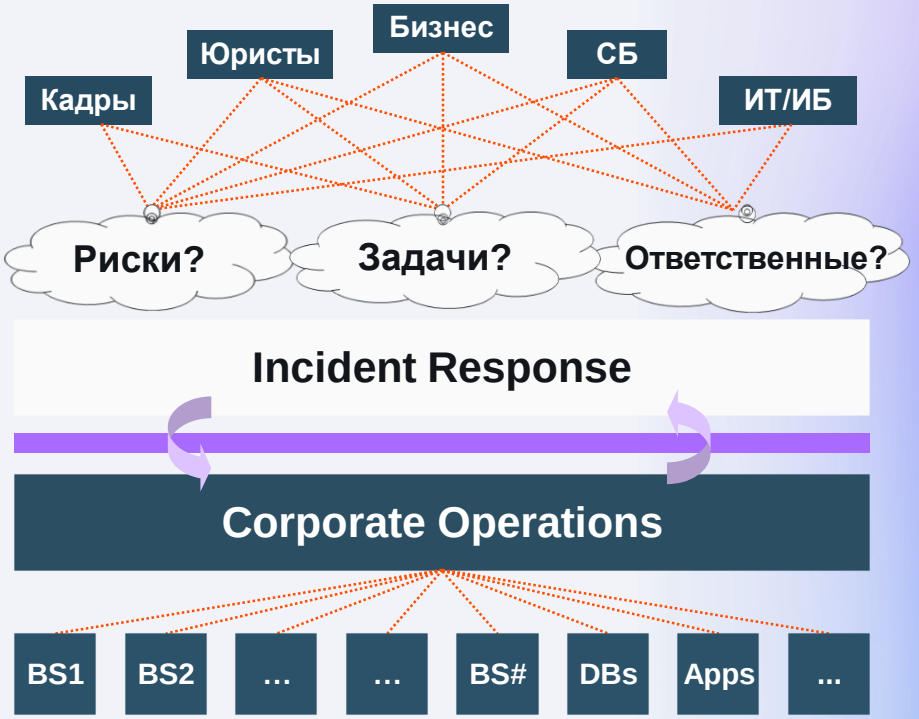
ПРОЦЕДУРЫ РЕАГИРОВАНИЯ НЕ ОПРЕДЕЛЕНЫ
возникают задержки и ненужная путаница

ИНСТРУМЕНТЫ И ОТВЕТСТВЕННЫЕ НЕ СВЯЗАНЫ
действия вручную и потеря времени

С РЕГЛАМЕНТАМИ НЕ ЗНАКОМЫ
требования и нормативные обязательства не выполняются

КВАЛИФИКАЦИИ НЕ ХВАТАЕТ
остановка процессов и неспособность к действию

затрагивает всю организацию

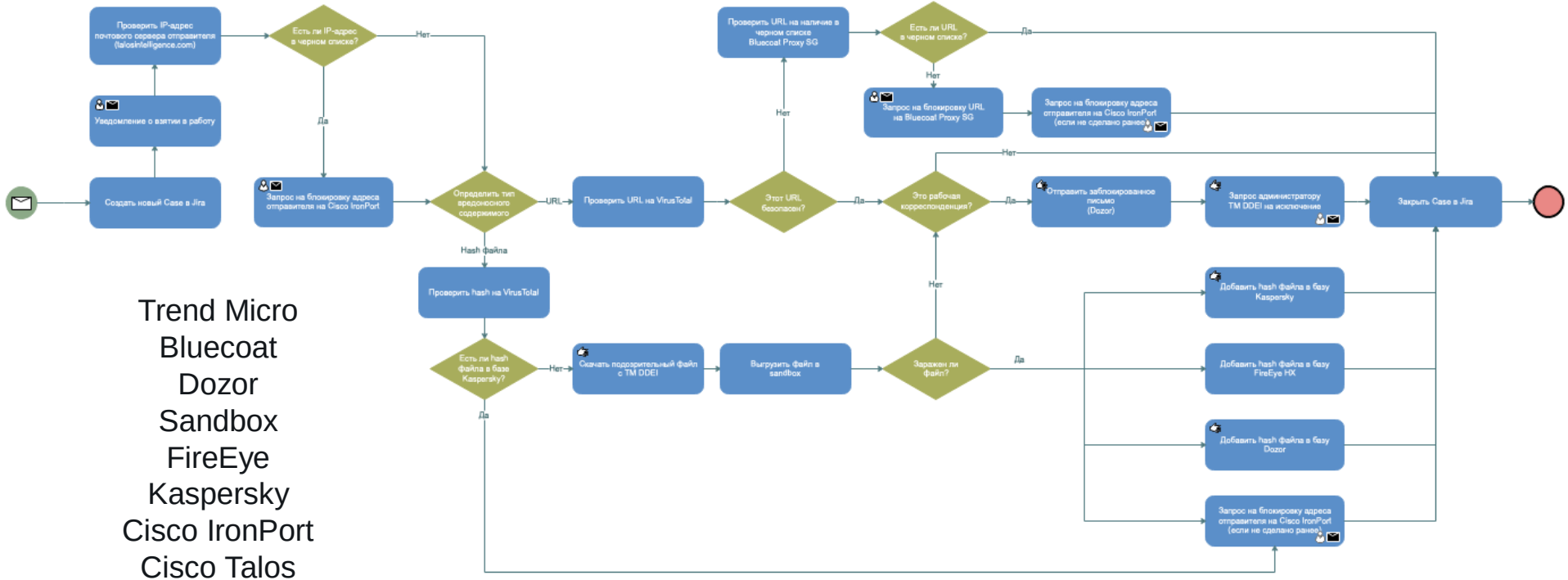


Сценарий инцидента: phishing

В соответствии с Verizon Data Breach Digest phishing атаки играют роль в 92% всех взломов систем защиты

*Rapid7: Security Orchestration and Automation Playbook

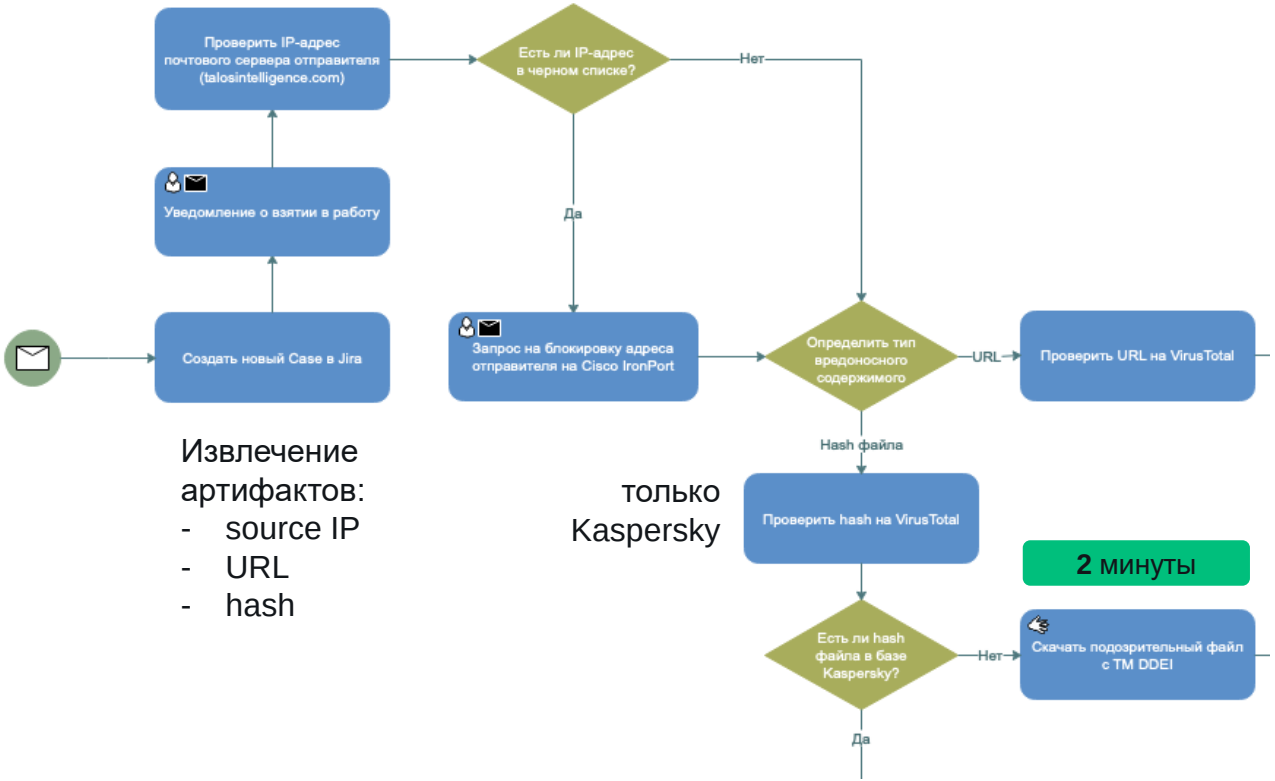
Сценарий инцидента: phishing - РЕАЛЬНОСТЬ



Trend Micro
Bluecoat
Dozor
Sandbox
FireEye
Kaspersky
Cisco IronPort
Cisco Talos
Virus Total
JIRA

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

Инцидент Trend Micro DDD



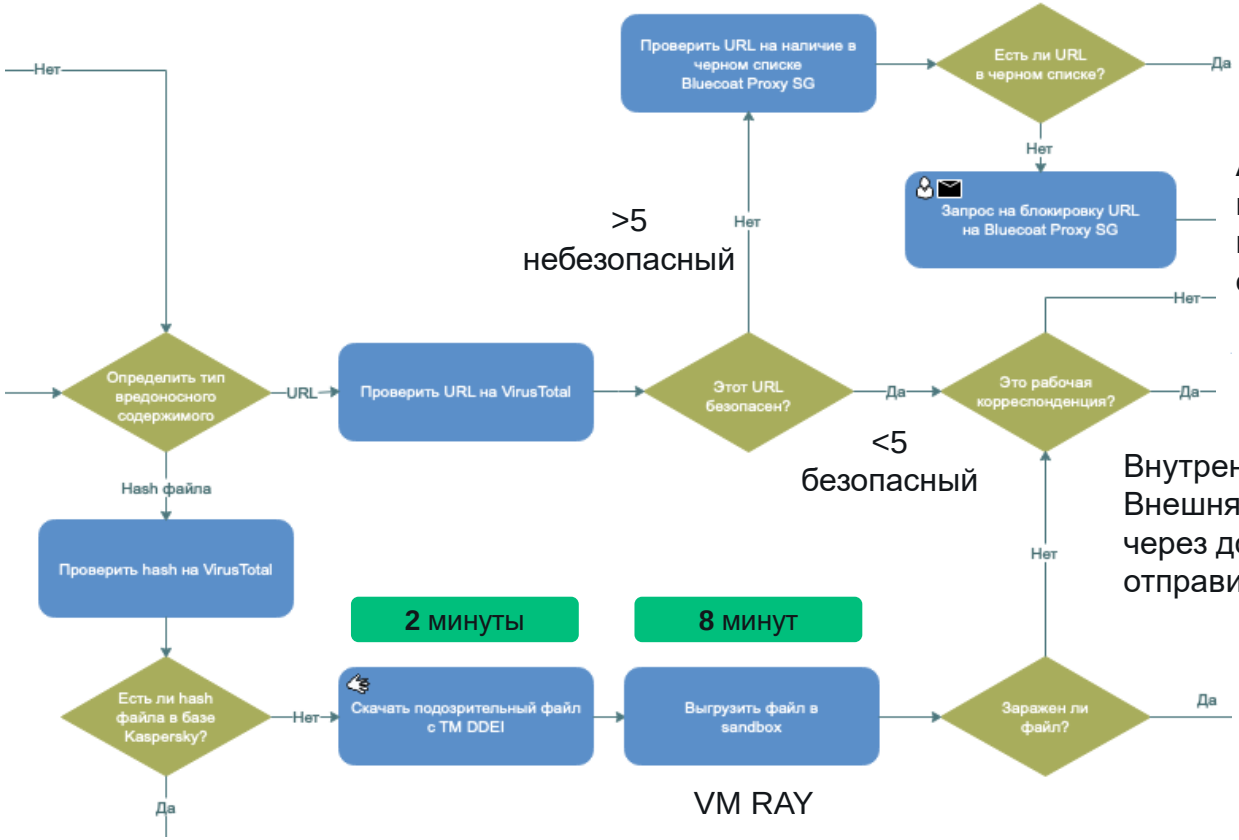
Извлечение артифактов:
- source IP
- URL
- hash

только Kaspersky

2 минуты

Вручную по причине ограничений API

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

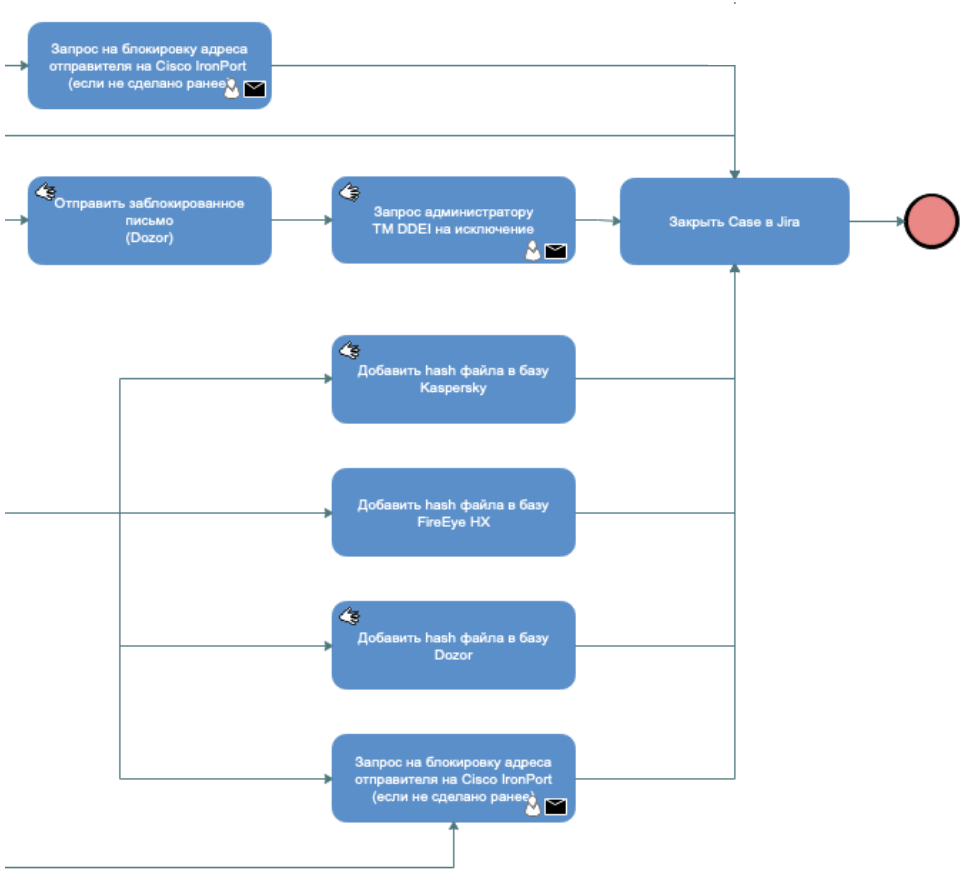


Автоматически
плоский файл
по причине
ограничений API

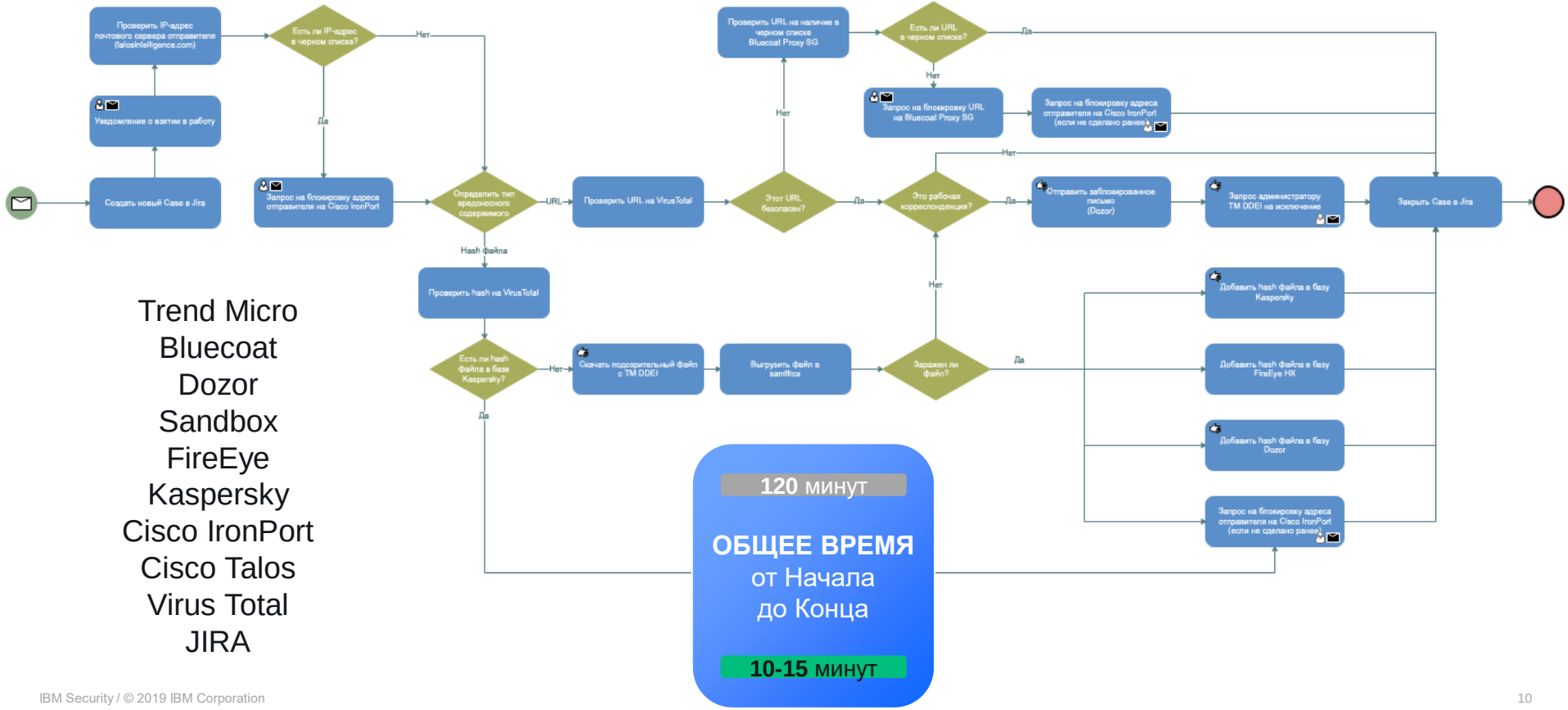
Внутренняя или
Внешняя
через домен
отправителя

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

Вручную
по причине
ограничений
API



Сценарий инцидента: phishing - РЕАЛЬНОСТЬ



Trend Micro
Bluecoat
Dozor
Sandbox
FireEye
Kaspersky
Cisco IronPort
Cisco Talos
Virus Total
JIRA

120 минут

ОБЩЕЕ ВРЕМЯ
от Начала
до Конца

10-15 минут

Преимущества и подводные камни автоматизации

IBM Security

Зачем так много средств защиты?
Механизм эшелонированной защиты никто не отменял
Нельзя надеяться на одно решение одного производителя

Наличие или отсутствие механизмов автоматизации (API, плоские файлы, скрипты)

Значительное сокращение времени и уровня квалификации сотрудников, валидация выполненных операций, обогащение черных списков

Минимизация ошибок переноса информации
(Ctrl-C / Ctrl-V)

Пример заказчика – глобальная фармацевтическая компания

Действие	ДО Resilient	С помощью Resilient	Пример
Эскалация через SIEM, EDR или NGFW	5 мин	10 сек	Эскалация инцидента из SIEM – подозрительная активность на рабочей станции
Идентификация активов – CMDB/AD/IAM	5-10 мин	10 сек	Запросы в CMDB по рабочей станции и в Active Directory по пользователю
Проверка IOC в Threat Intelligence базах	5 мин	10 сек	В инциденте есть hash связанный с ВПО
Историческая корреляция инцидентов	10-20 мин	мгновенно	2 других инцидента за последний месяц имеют тот же hash и исходящий траффик
Ручное обогащение – активности с рабочих станций, внутренней сети, логи VPN, DNS записи, сетевая инфраструктура	30-55 мин	30 сек	Используем EDR решение чтобы получить всю информацию с рабочей станции, DNS с web proxy для выявления сервера управления
Записи по инциденту – детальные записи и задачи на протяжении всего инцидента	неизвестно	мгновенно	Resilient автоматически сохраняет все выполненные задачи и действия по реагированию, все записи аналитиков хранятся на платформе
Эскалация через SIEM, EDR или NGFW	неизвестно	мгновенно	Все действия логируются в Resilient и не могут быть модифицированы. При разборе инцидента руководство может анализировать отчеты
Отчет по статусу инцидента и визуализация для руководства	неизвестно	мгновенно	Встроенные консоли для руководства и внешние уведомления предоставляют всю информацию в режиме реального времени без лишней работы
ИТОГО	**85 мин**	**1 мин**	

SOAR – Совсем не про ИБ

Bomb threat

Gun threat

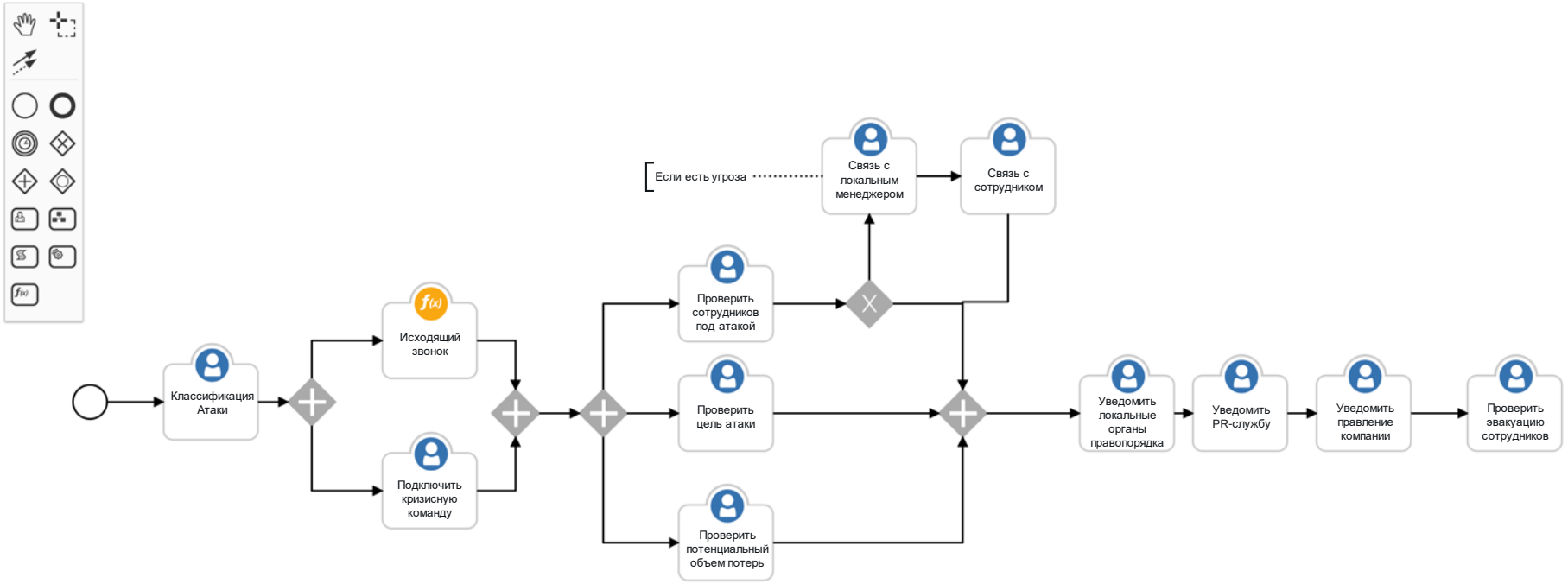
Armed intruder in the office complex

Kidnap on exec

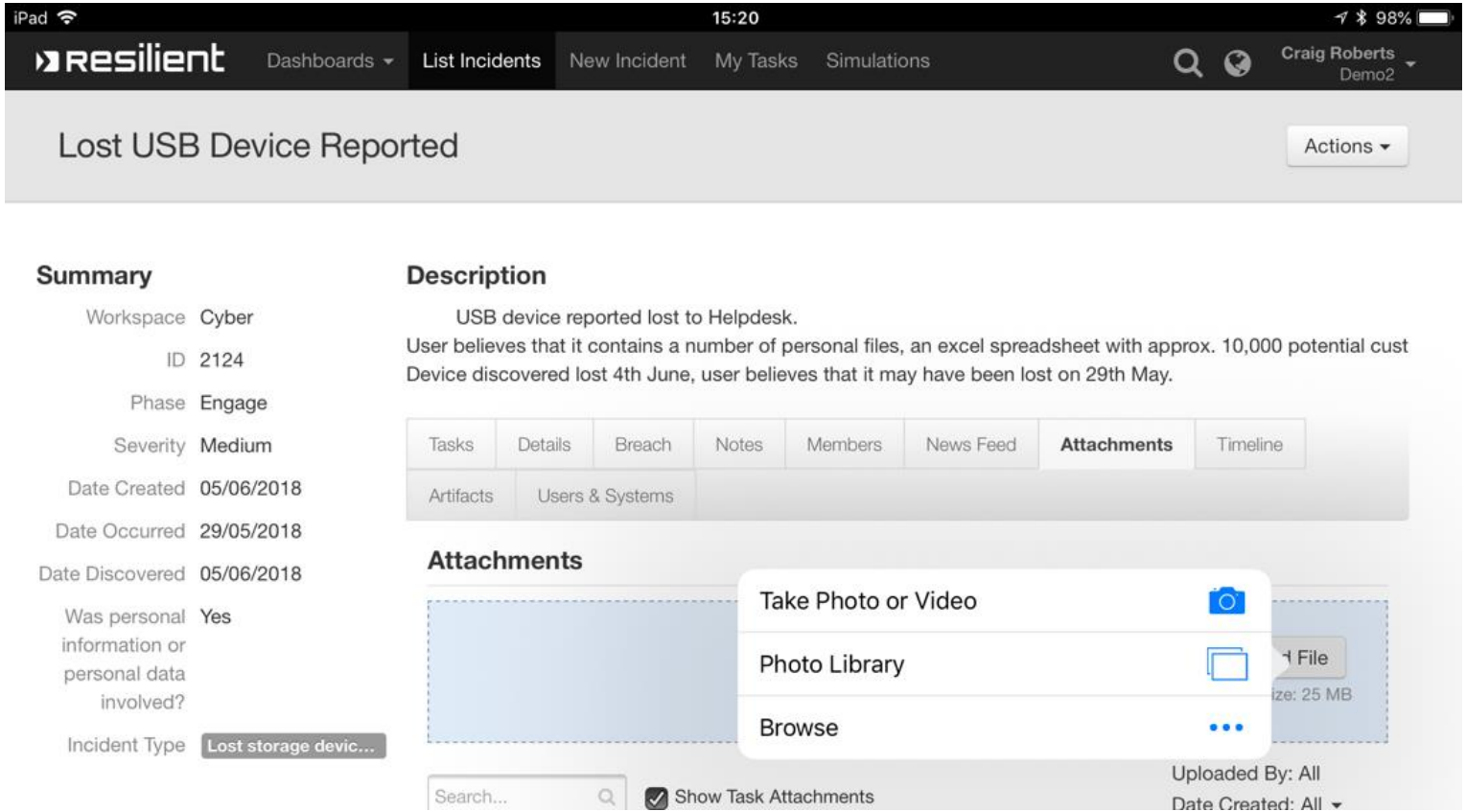
Natural disaster impacting an office

ATM Ram Raid

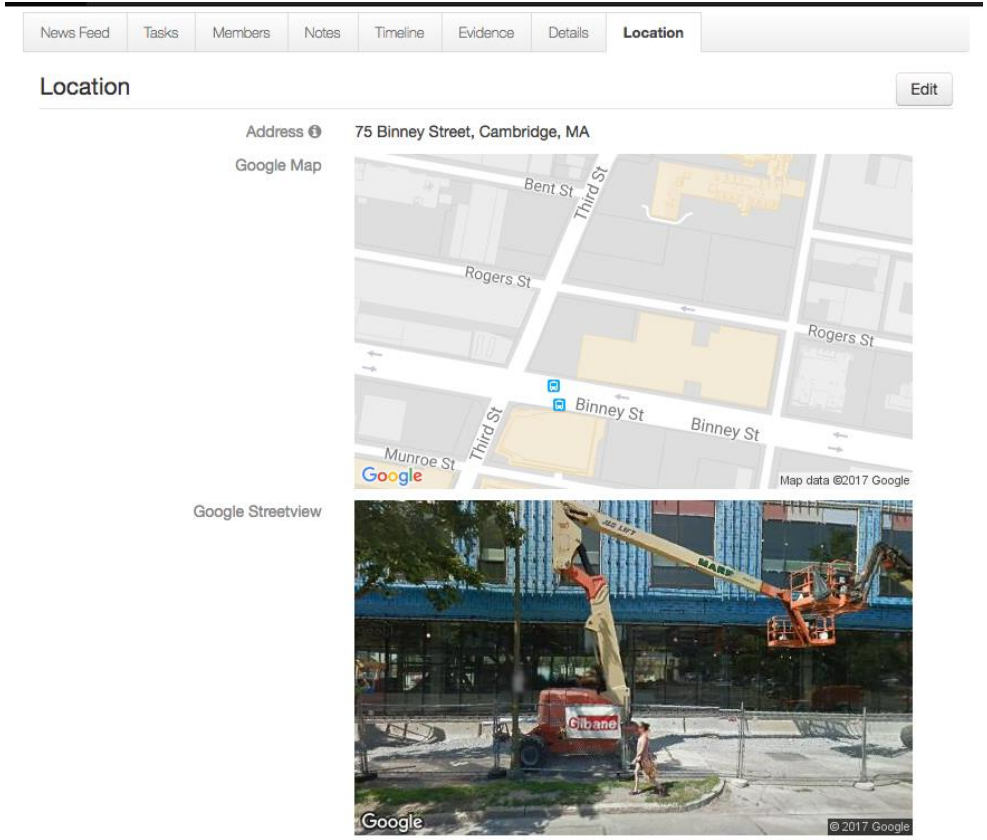
Автоматизация реагирования на любой тип инцидента



Поддержка планшетов для работы в полях

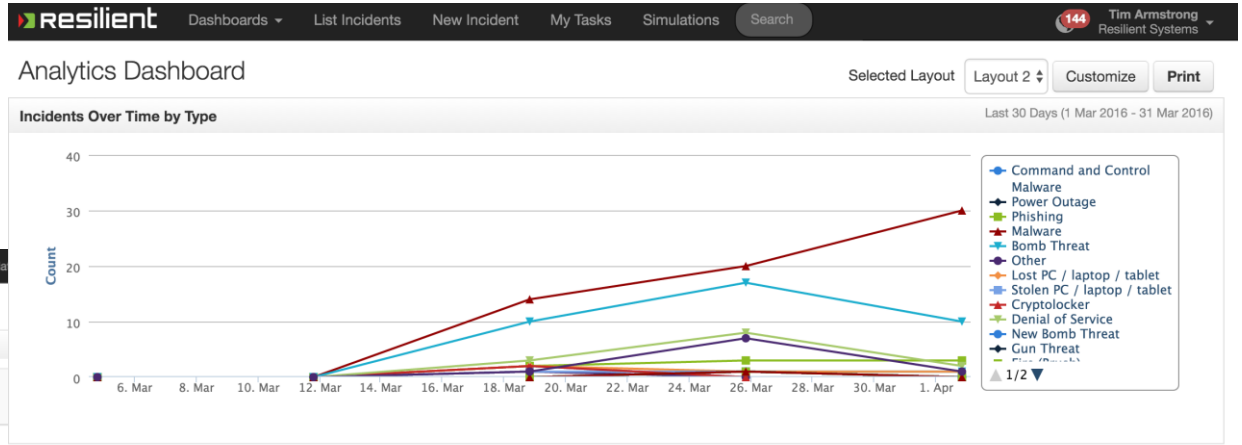


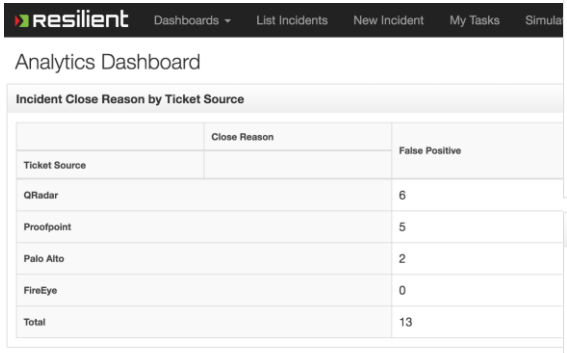
Контекстная информация для разных типов инцидентов

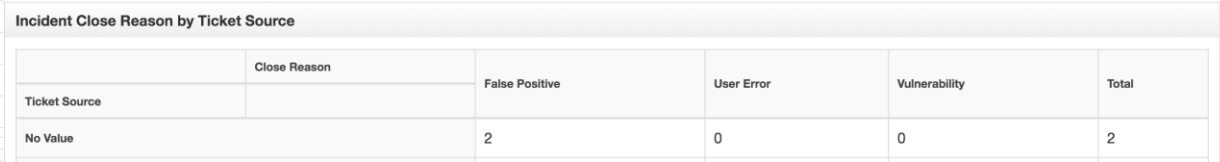


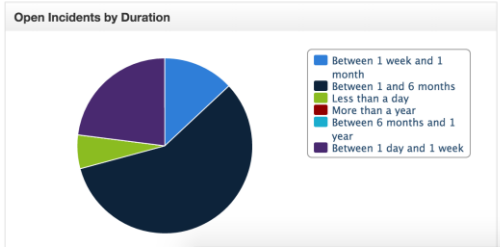
Аналитика по всем инцидентам в организации

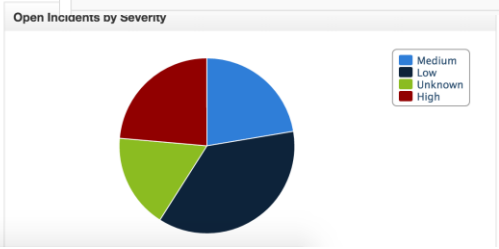
- Ключевые метрики инцидента всегда под рукой











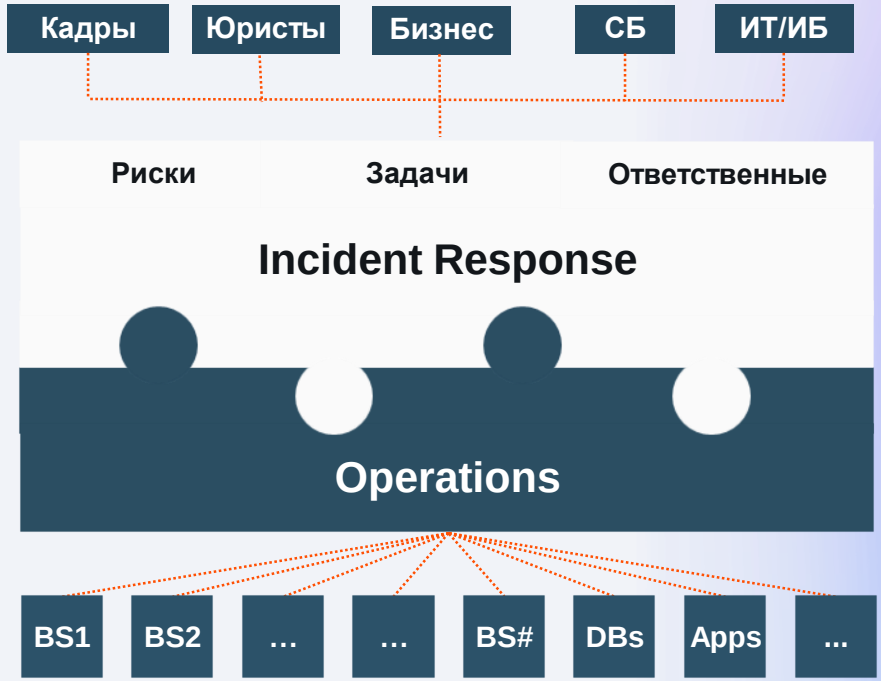
Как эффективно внедрять реагирование на инциденты

ОЦЕНИТЬ ПОТЕНЦИАЛЬНУЮ ЭФФЕКТИВНОСТЬ
Анализ существующий процессов реагирования

ОПРЕДЕЛИТЬ СИСТЕМЫ ДЛЯ ИНТЕГРАЦИИ
Для демонстрации оптимально до 5 систем интегрированных в процесс реагирования

ОПРЕДЕЛИТЬ СЦЕНАРИИ РЕАГИРОВАНИЯ
Необходимо зафиксировать процесс реагирования который принят в организации (1-2 процесса)

АВТОМАТИЗИРОВАТЬ СУЩЕСТВУЮЩИЕ РУТИННЫЕ ЗАДАЧИ
Показать ценность автоматизированных процессов



ВОПРОСЫ?

IBM Security

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СПАСИБО

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

МОИ КОНТАКТЫ: