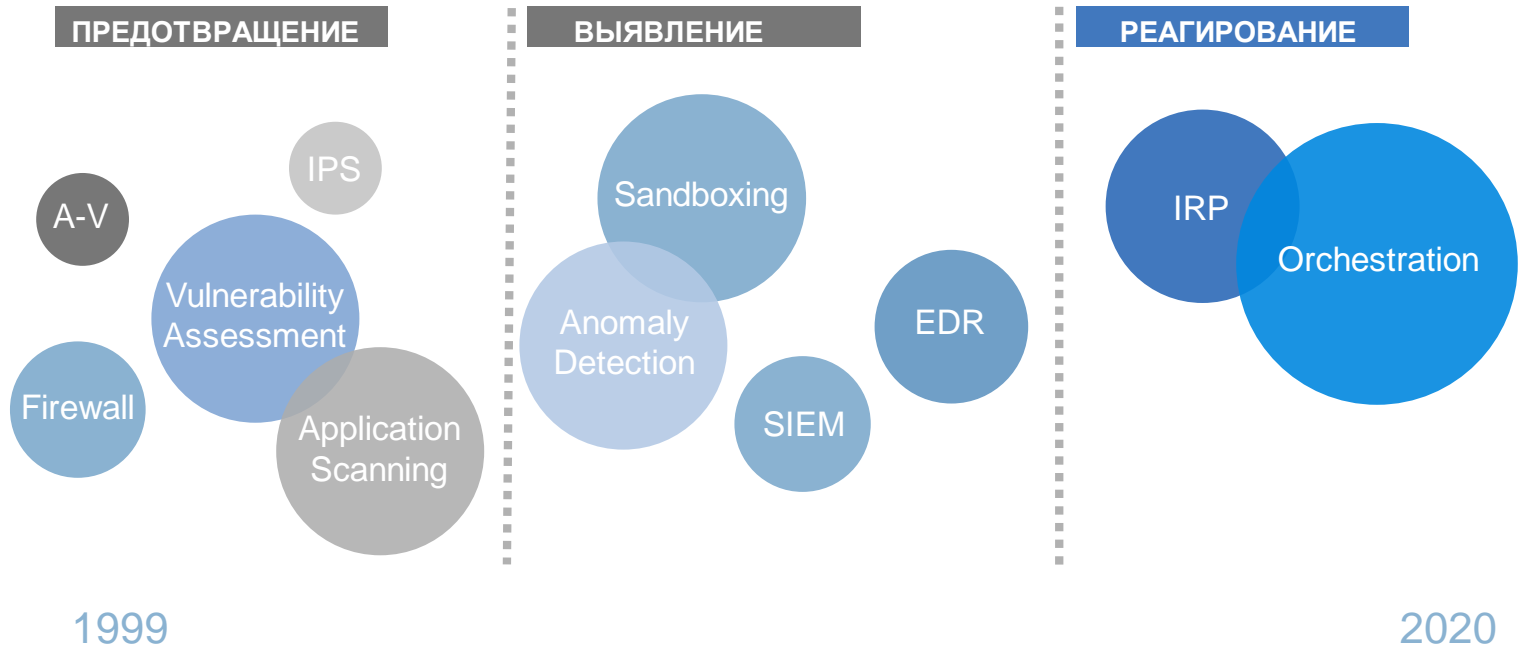


Как эффективно автоматизировать процессы реагирования на инциденты

Олег Бакшинский
Ведущий советник по вопросам информационной безопасности

19 сентября 2019 г.

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 ОПРЕДЕЛЕННЫ

возникают задержки и ненужная путаница

ИНСТРУМЕНТЫ И ОТВЕТСТВЕННЫЕ НЕ СВЯЗАНЫ

действия вручную и потеря времени

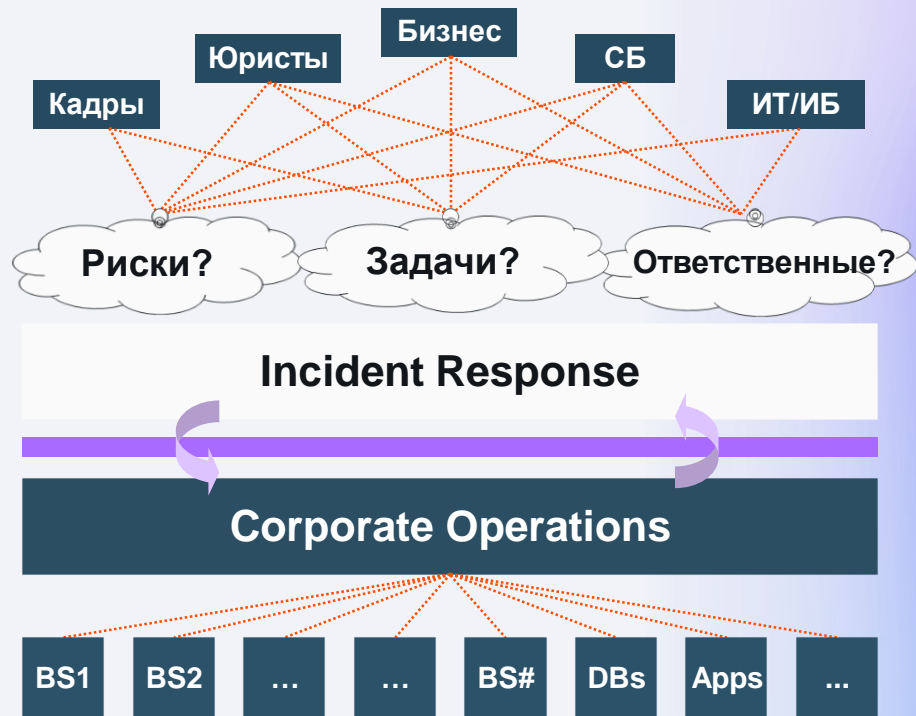
С РЕГЛАМЕНТАМИ НЕ ЗНАКОМЫ

требования и нормативные обязательства не выполняются

КВАЛИФИКАЦИИ НЕ ХВАТАЕТ

остановка процессов и неспособность к действию

затрагивает всю организацию



Сценарий инцидента: phishing

ДО Автоматизации

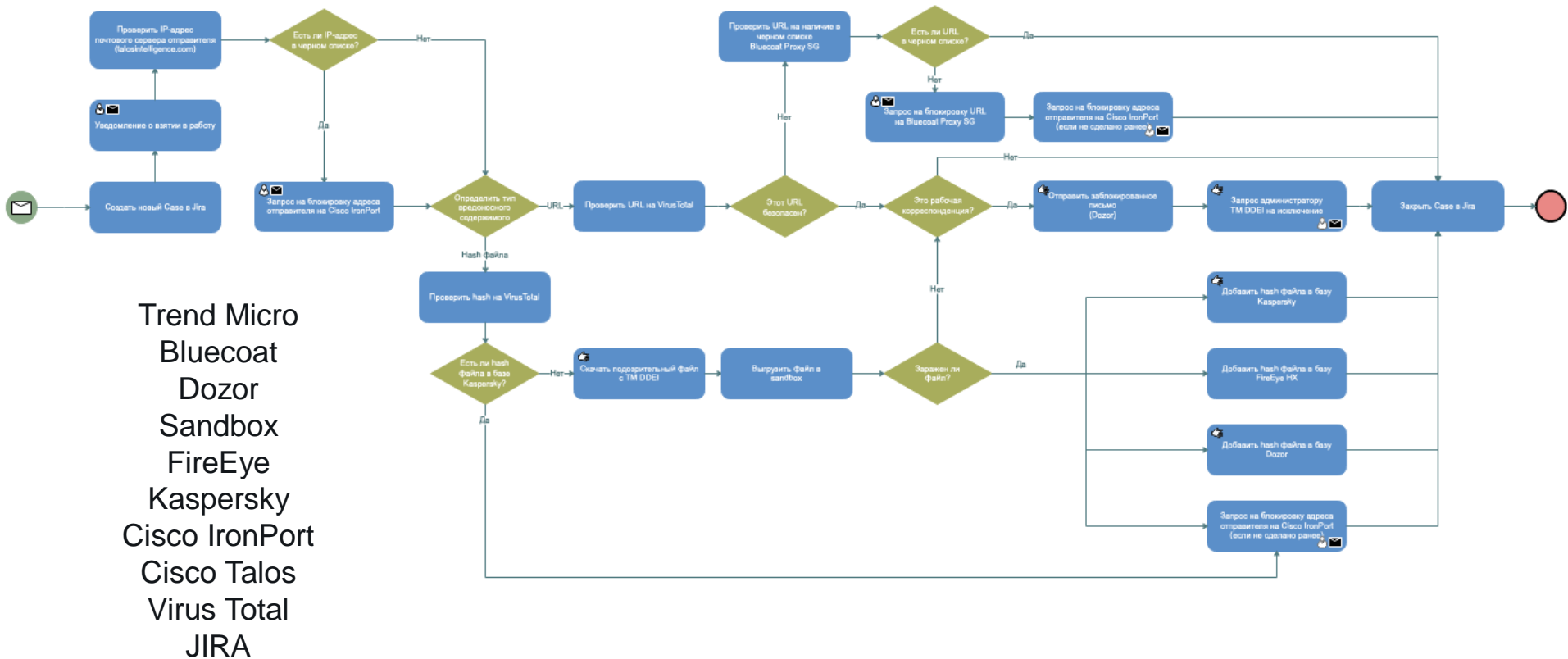


ПОСЛЕ
Автоматизации

Решение
человека

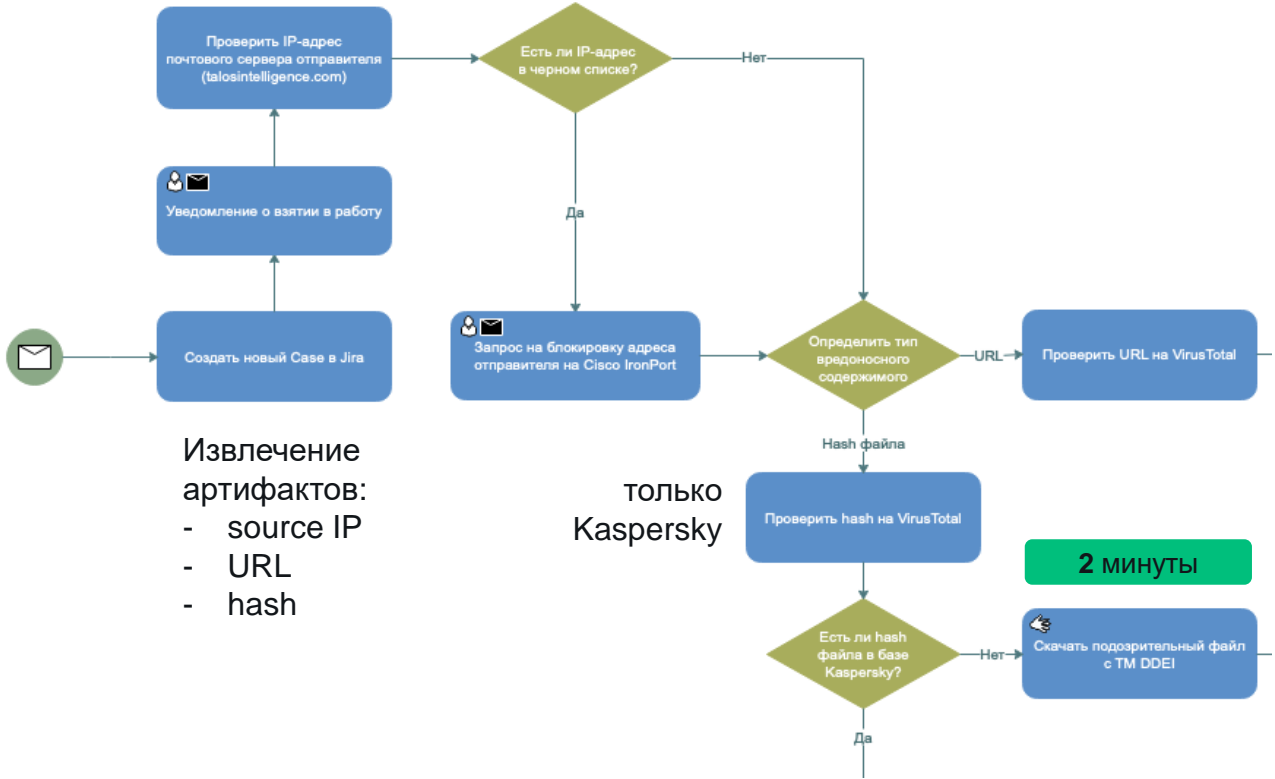
**В соответствии с Verizon Data Breach Digest
phishing атаки играют роль
в 92% всех взломов систем защиты**

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ



Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

Инцидент
Trend
Micro
DDD



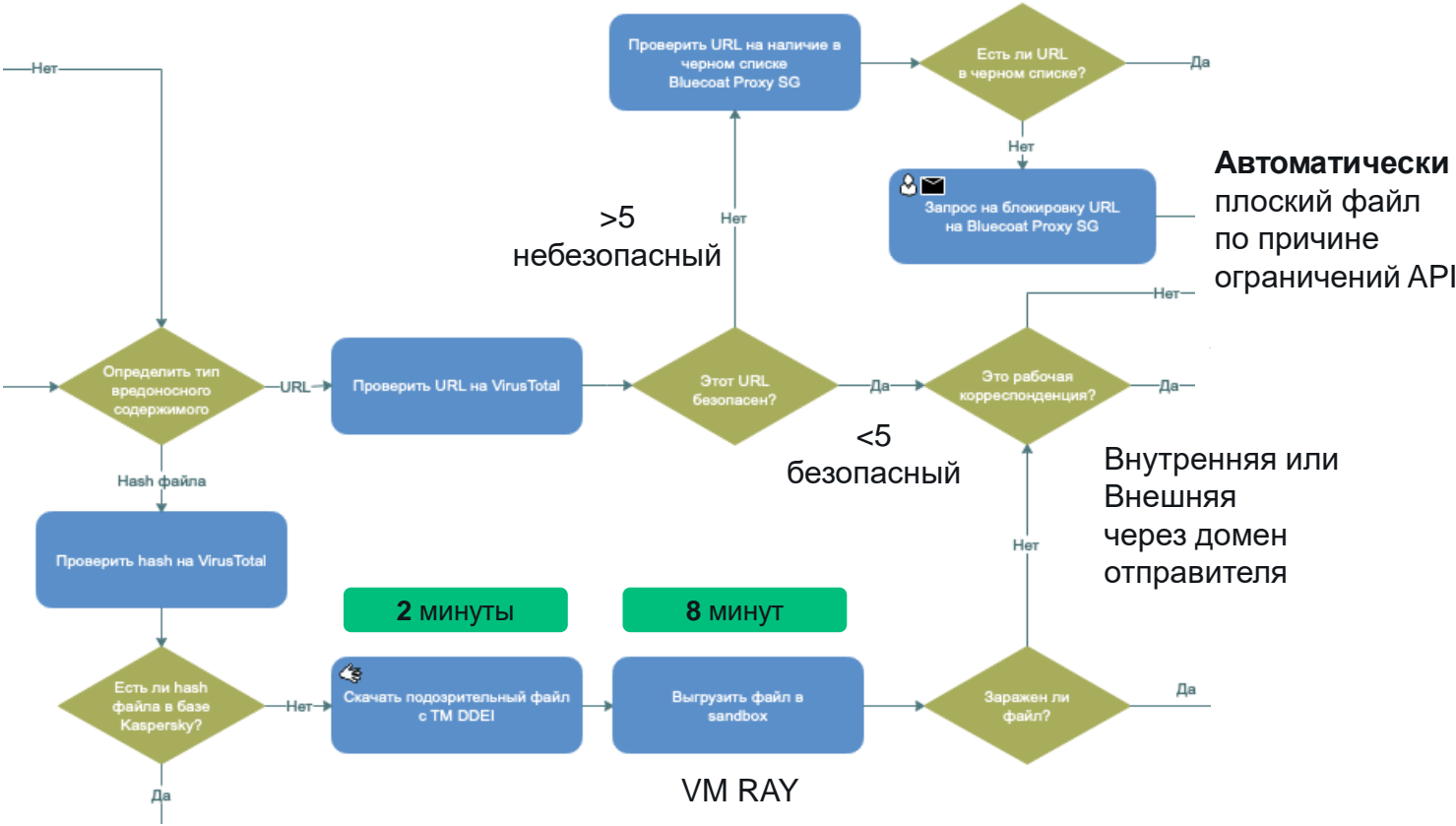
Извлечение артефактов:
- source IP
- URL
- hash

только Kaspersky

2 минуты

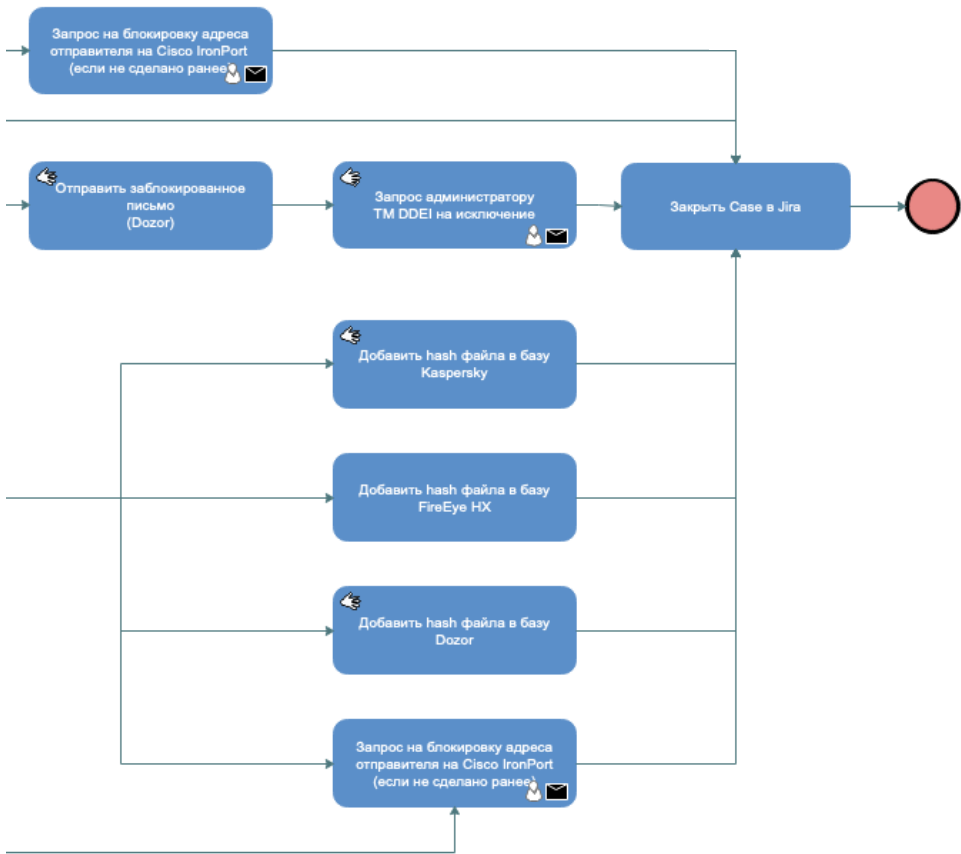
Вручную
по причине ограничений API

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

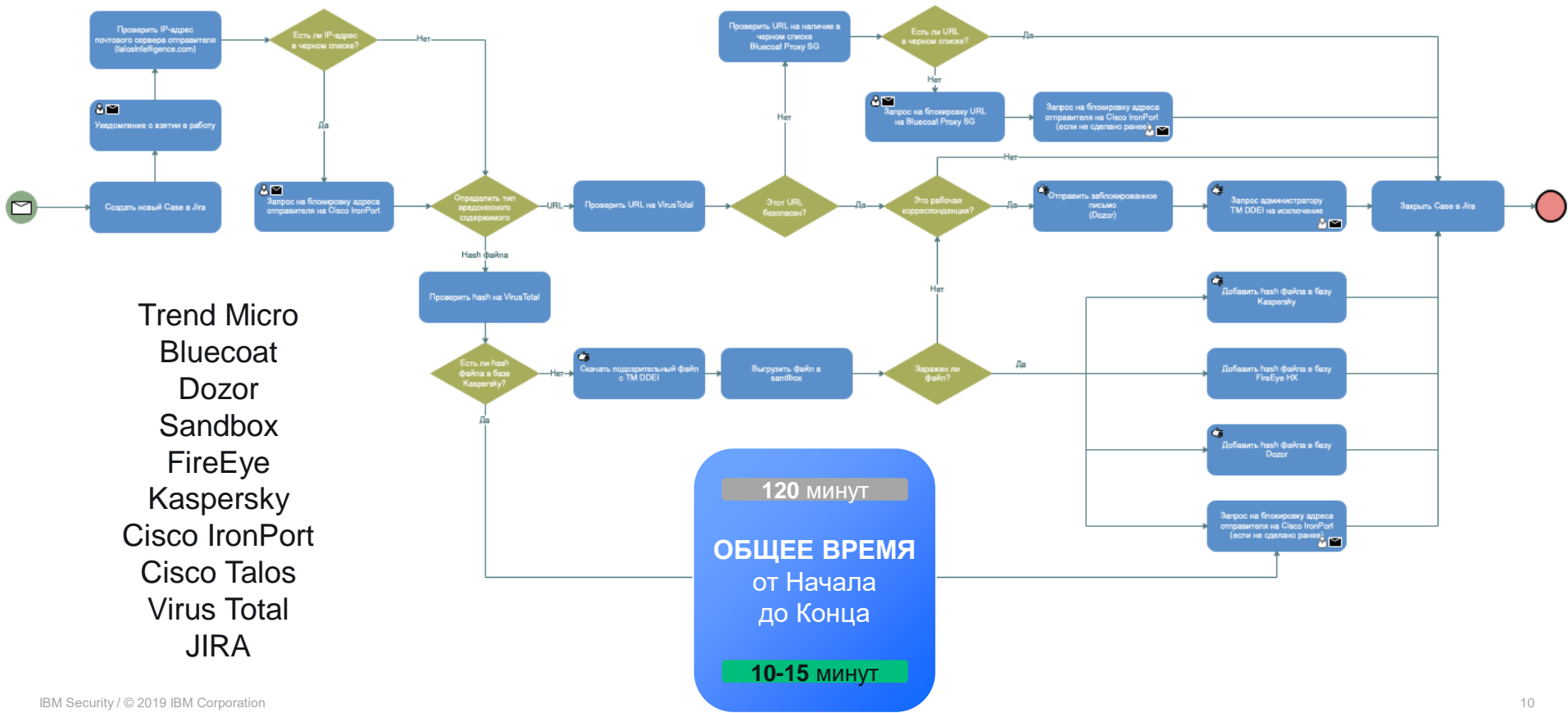


Сценарий инцидента: phishing - РЕАЛЬНОСТЬ

Вручную
по причине
ограничений
API



Сценарий инцидента: phishing - РЕАЛЬНОСТЬ



Преимущества и подводные камни автоматизации

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 трафик
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 проху 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

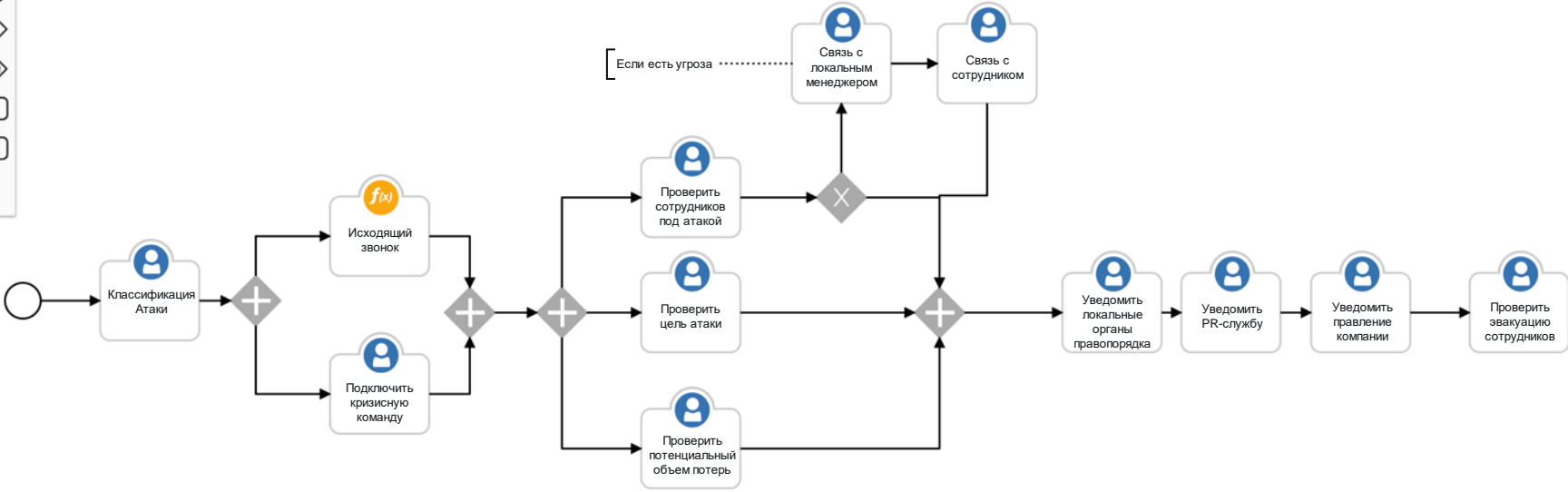
Armed intruder in the office complex

Kidnap on exec

Natural disaster impacting an office

ATM Ram Raid

Автоматизация реагирования на любой тип инцидента



Поддержка планшетов для работы в полях

Workspace Cyber

ID 2124

Phase Engage

Severity Medium

Date Created 05/06/2018

Date Occurred 29/05/2018

Date Discovered 05/06/2018

Was personal information or personal data involved? Yes

Incident Type Lost storage device...

Description

USB device reported lost to Helpdesk.
User believes that it contains a number of personal files, an excel spreadsheet with approx. 10,000 potential cust Device discovered lost 4th June, user believes that it may have been lost on 29th May.

Tasks Details Breach Notes Members News Feed **Attachments** Timeline

Artifacts Users & Systems

Attachments

Take Photo or Video

Photo Library

Browse

1 File
Size: 25 MB

Uploaded By: All
Date Created: All

Search... Show Task Attachments


Контекстная информация для разных типов инцидентов

News Feed | Tasks | Members | Notes | Timeline | Evidence | Details | **Location**


Location Edit

Address ⓘ 75 Binney Street, Cambridge, MA

Google Map



Google Streetview

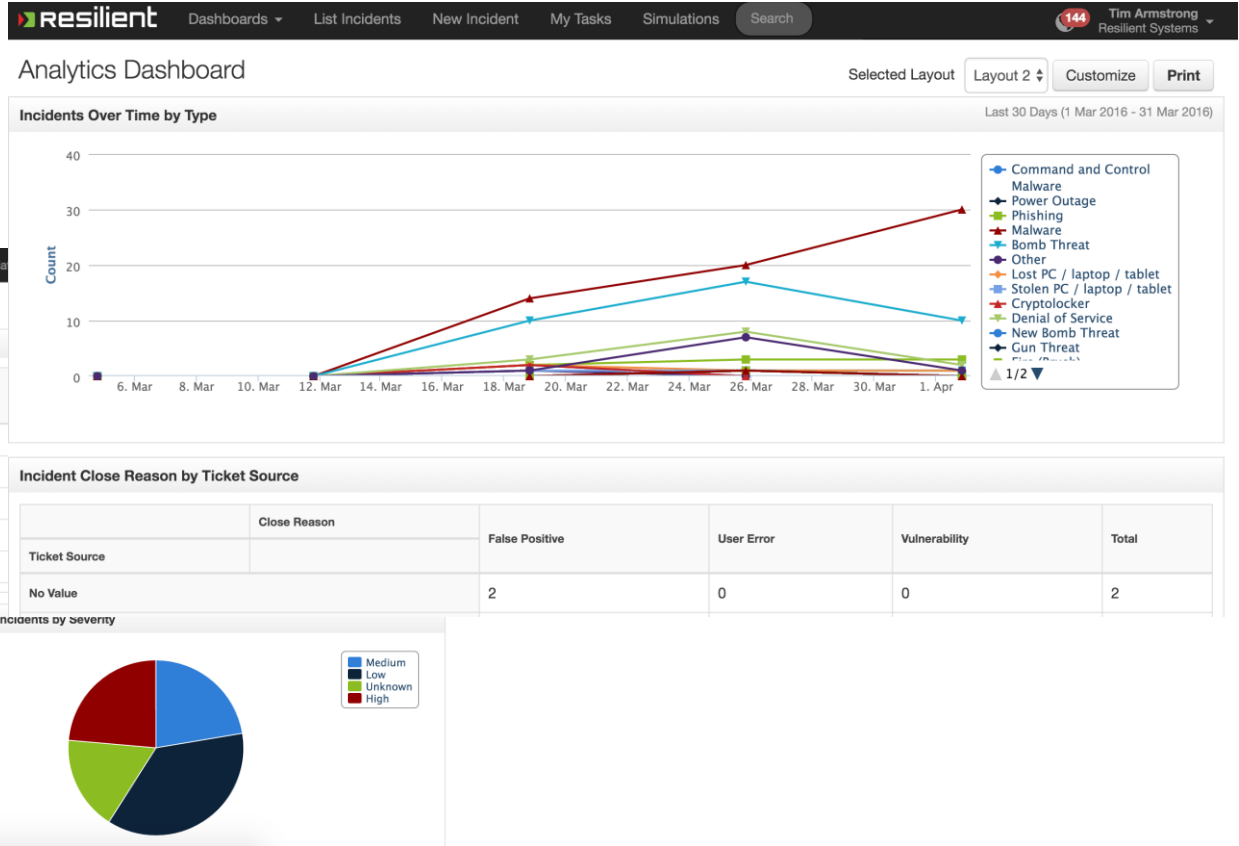


Map data ©2017 Google

© 2017 Google

Аналитика по всем инцидентам в организации

- Ключевые метрики инцидента всегда под рукой



Как эффективно внедрять

ОЦЕНИТЬ ПОТЕНЦИАЛЬНУЮ ЭФФЕКТИВНОСТЬ

Анализ существующих 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







реагирование на инциденты



ВОПРОСЫ?

СПАСИБО

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  ibm.com/security/community
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

МОИ КОНТАКТЫ:



© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM Security / © 2019 IBM Corporation