10 YEARS JETSECURITY CONFERENCE 2019

Практические примеры внедрения платформы реагирования на инциденты IBM Resilient

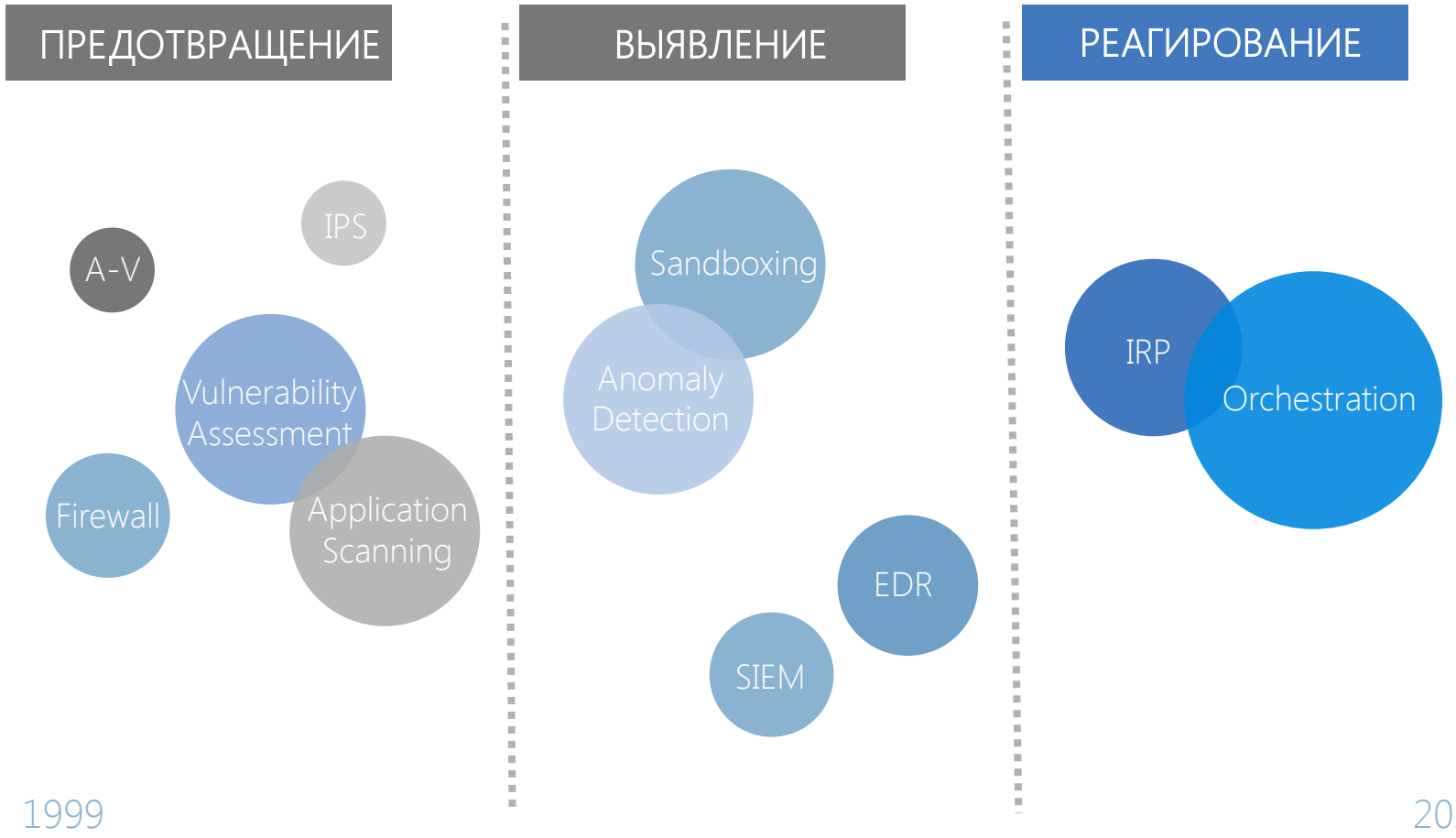
Олег Бакшинский

Ведущий советник по вопросам информационной безопасности IBM в России и странах СНГ

IBM Security

ОРКЕСТРАЦИЯ КАК РАЗВИТИЕ РЕАГИРОВАНИЯ

IBM Security



"Если собираетесь инвестировать во что-то одно, это должно быть реагирование на инциденты."

– Основное послание Worldwide Security Summit

Gartner

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING

IBM Security

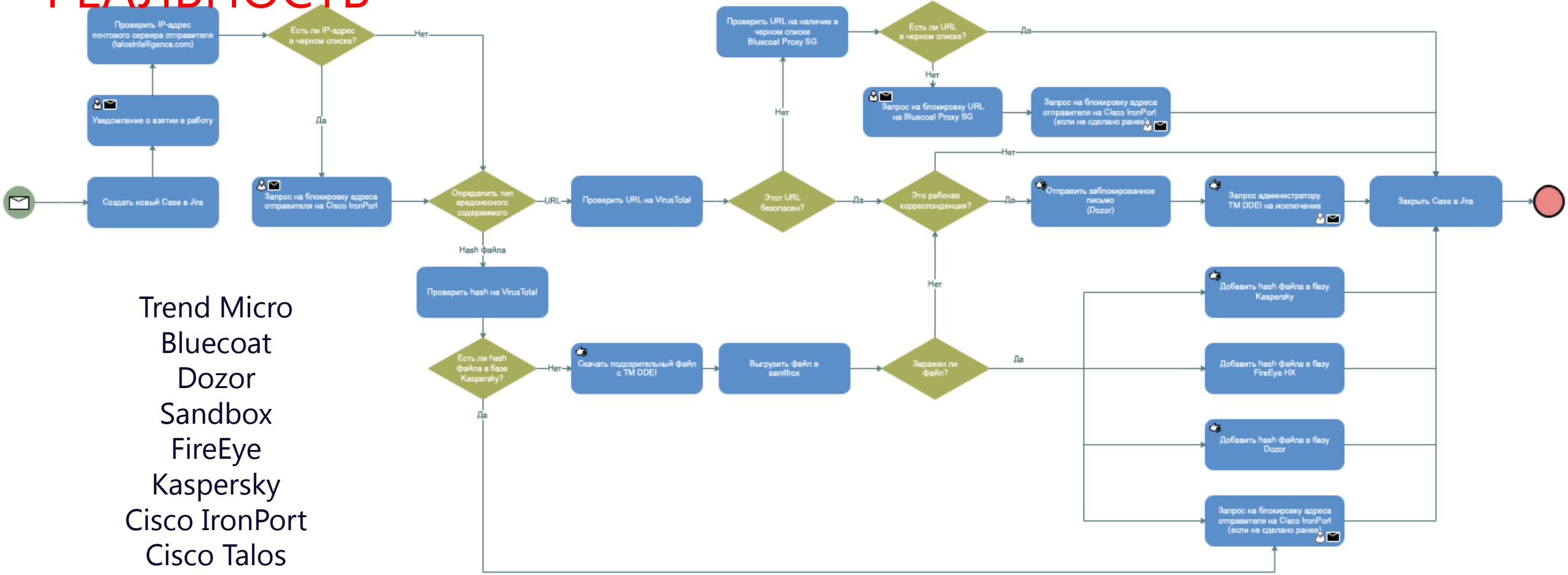
В соответствии с Verizon Data Breach Digest
phishing атаки играют роль
в 92% всех взломов систем защиты

*Rapid7: Security Orchestration and Automation Playbook

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING - РЕАЛЬНОСТЬ

IBM Security



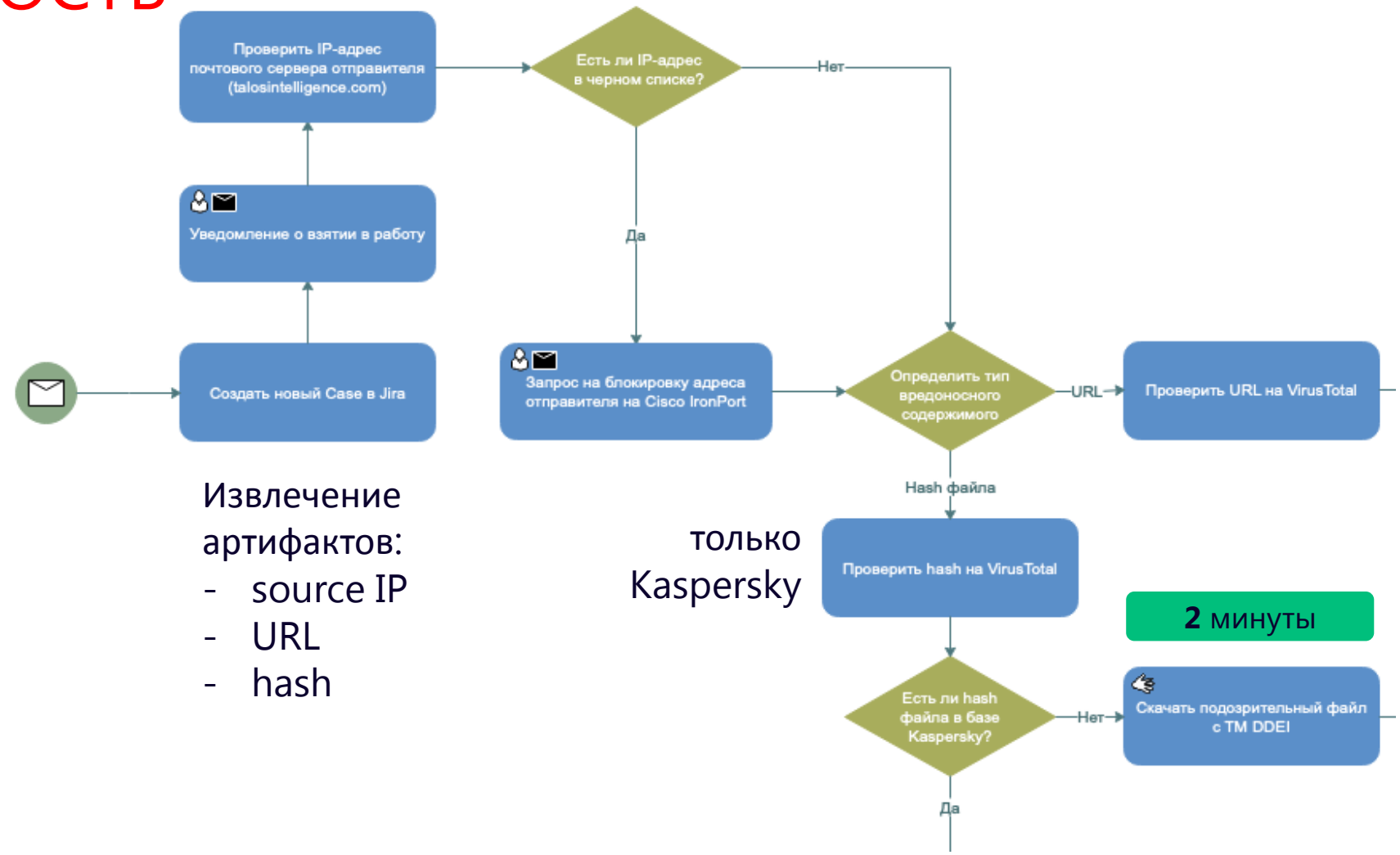
Trend Micro
Bluecoat
Dozor
Sandbox
FireEye
Kaspersky
Cisco IronPort
Cisco Talos
Virus Total
JIRA

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING - РЕАЛЬНОСТЬ

IBM Security

Инцидент Trend Micro DDD



Извлечение артифактов:
- source IP
- URL
- hash

только Kaspersky

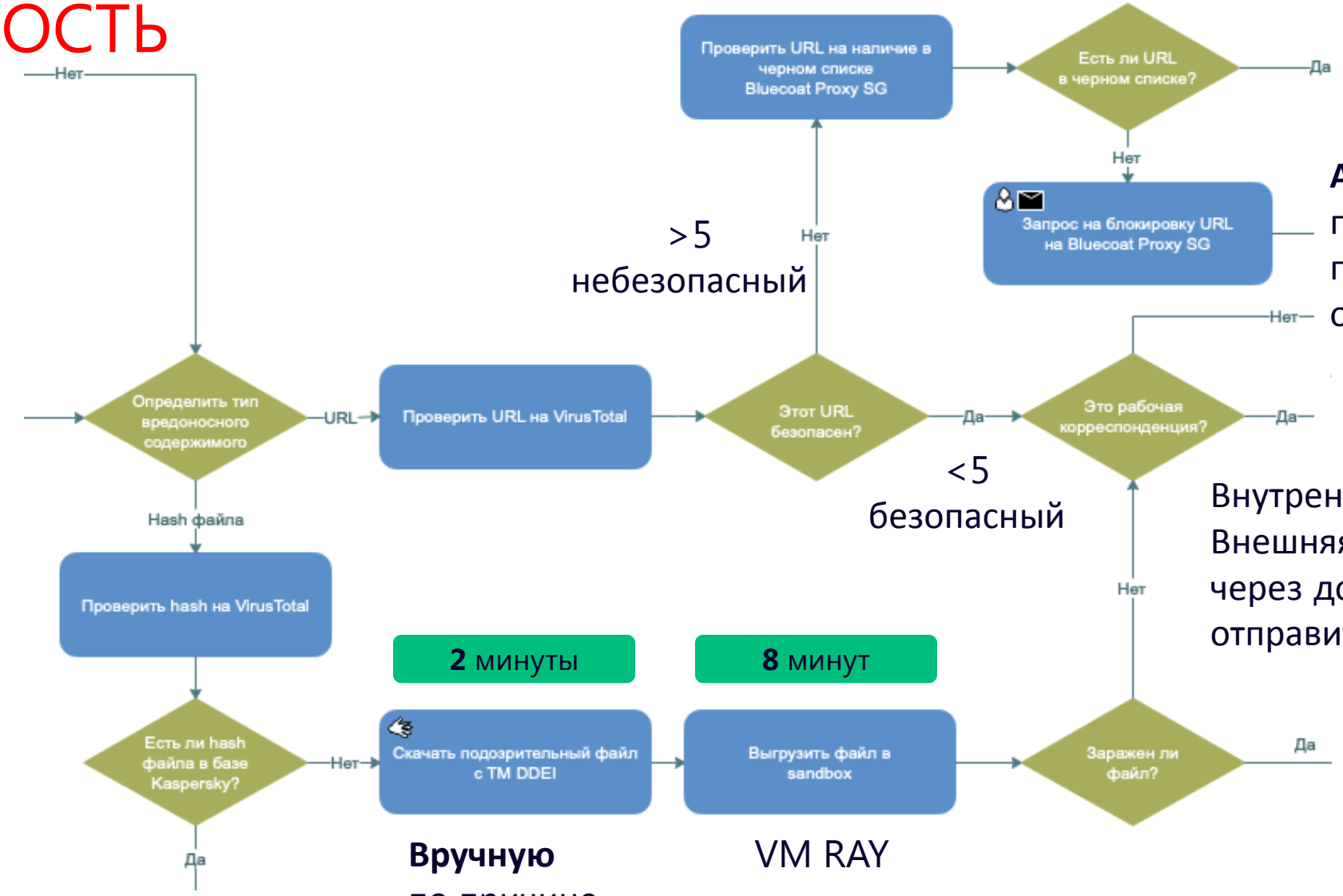
2 минуты

Вручную по причине ограничений API

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING - РЕАЛЬНОСТЬ

IBM Security



Автоматически
плоский файл
по причине
ограничений API

Внутренняя или
Внешняя
через домен
отправителя

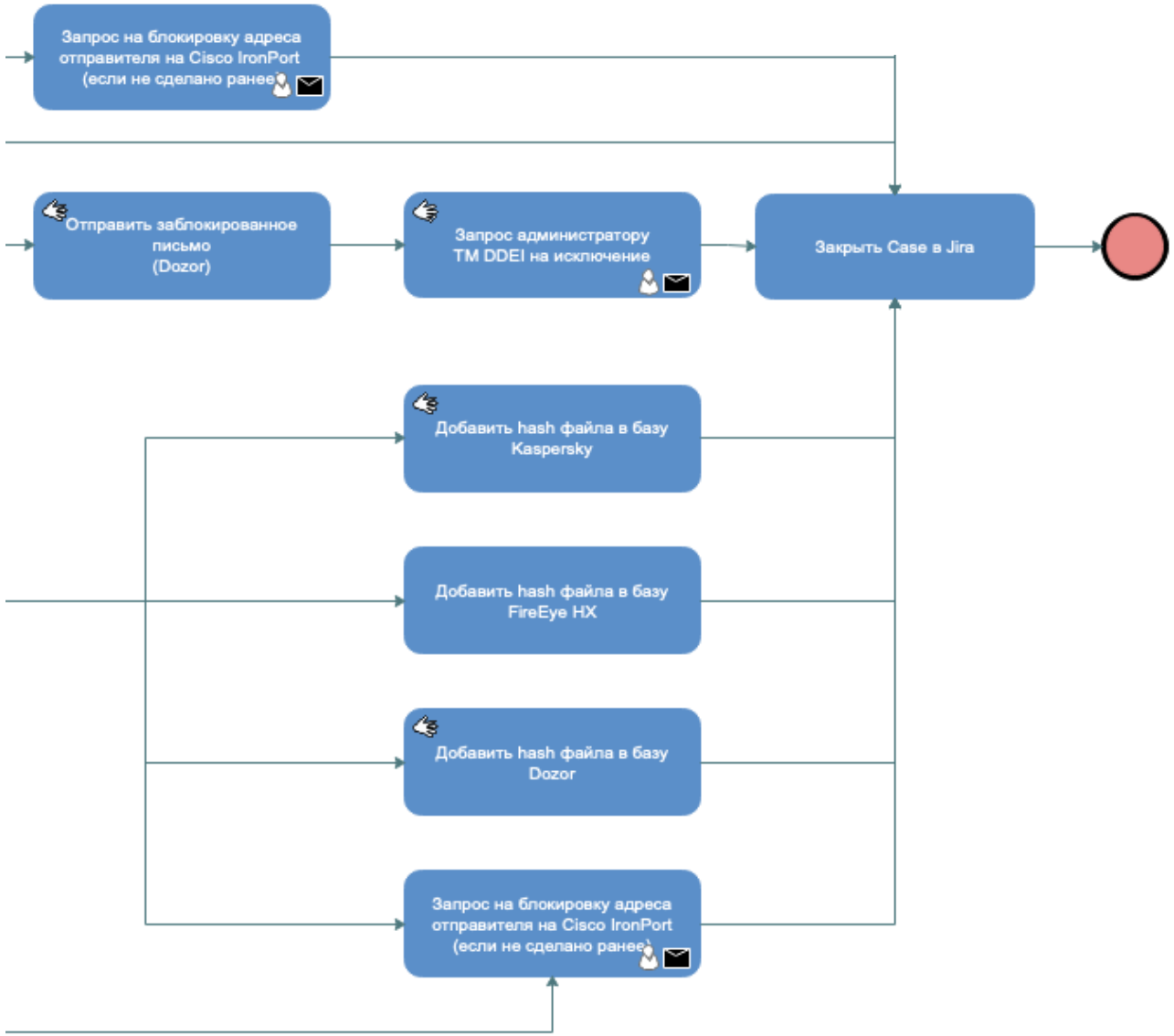
Вручную
по причине
ограничений API

VM RAY

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING - РЕАЛЬНОСТЬ

IBM Security

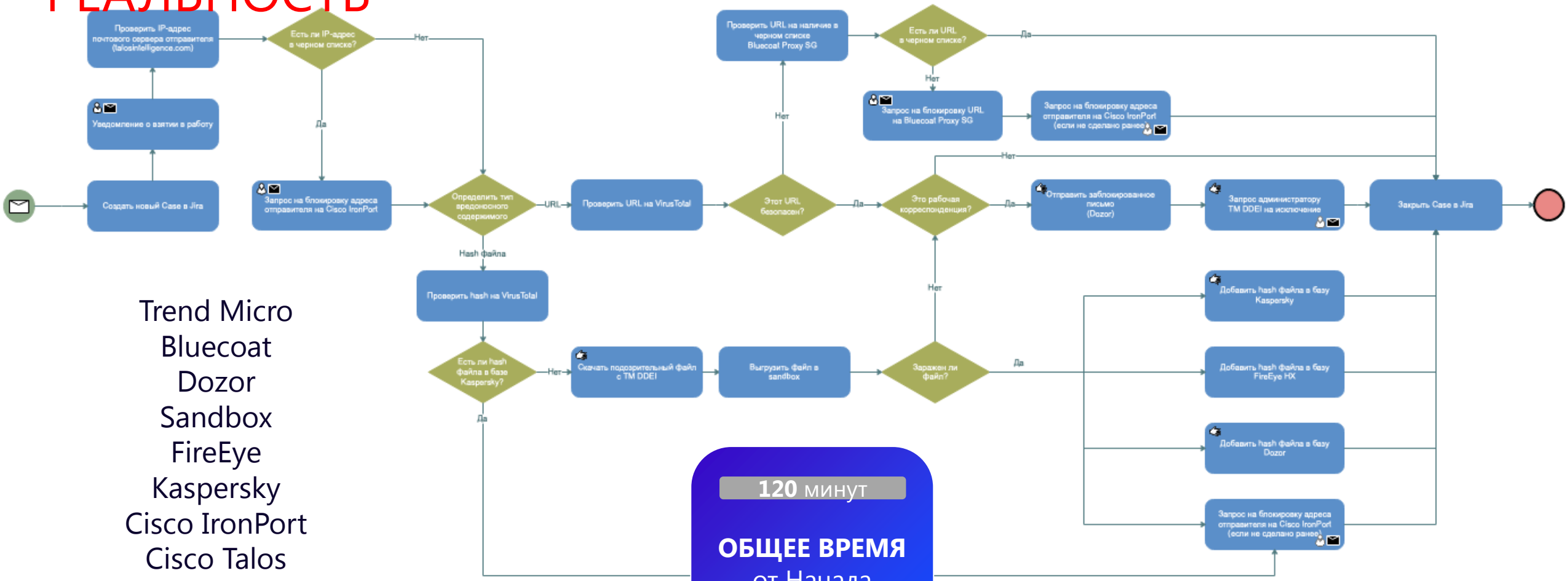


Вручную
по причине ограничений API

10 YEARS JETSECURITY CONFERENCE 2019

СЦЕНАРИЙ ИНЦИДЕНТА: PHISHING - РЕАЛЬНОСТЬ

IBM Security



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

10 YEARS JETSECURITY CONFERENCE 2019

SOAR - ВЫВОДЫ

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)

SOAR – СОВСЕМ НЕ ПРО ИБ

IBM Security

Bomb threat

Gun threat

Armed intruder in the office complex

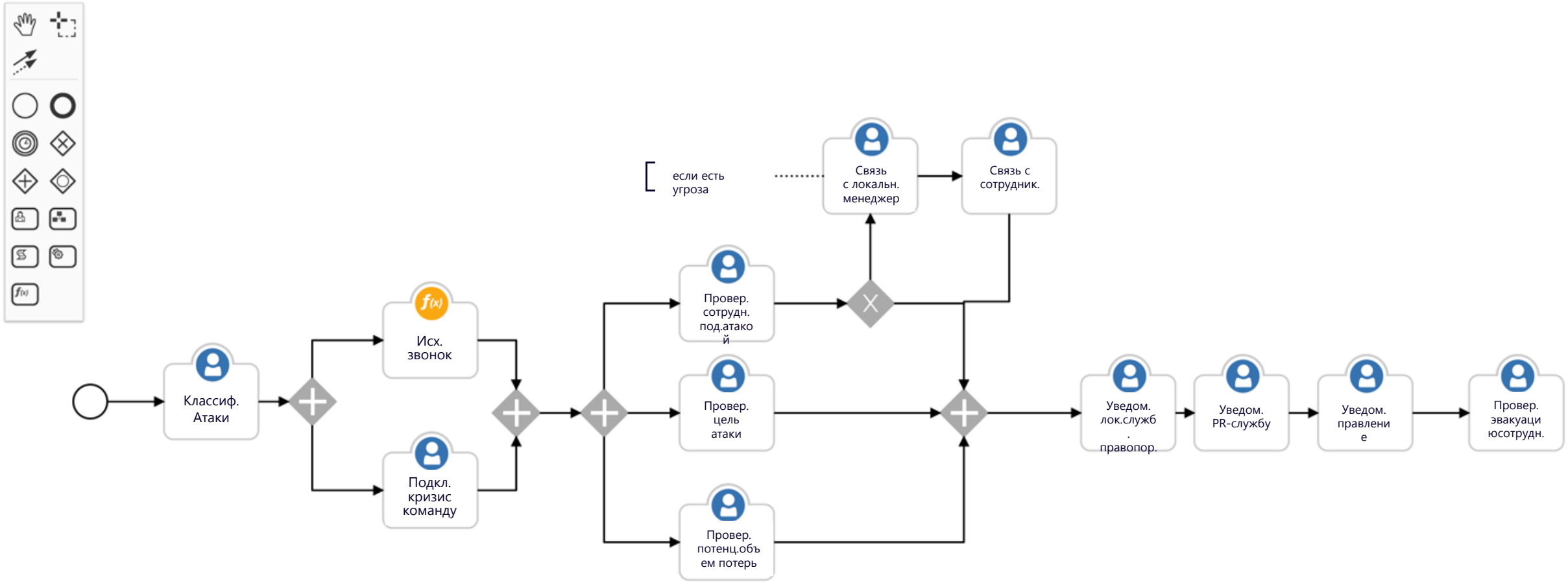
Kidnap on exec

Natural disaster impacting an office

ATM Ram Raid

SOAR – СОВСЕМ НЕ ПРО ИБ

IBM Security



10 YEARS JETSECURITY CONFERENCE 2019

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Олег Бакшинский

Ведущий советник по вопросам информационной безопасности IBM в России и странах СНГ

IBM Security