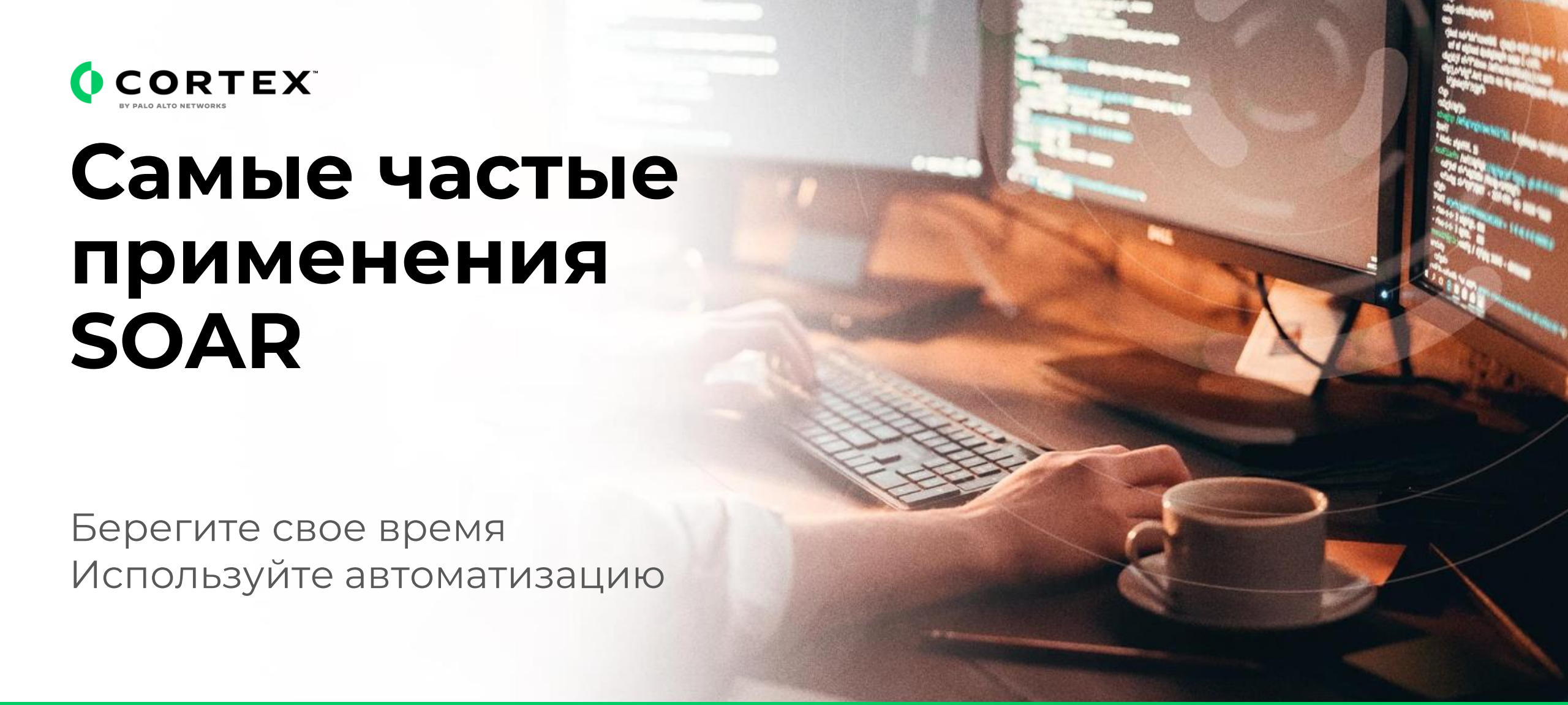
CORTEX
BY PALO ALTO NETWORKS

Самые частые применения SOAR



Берегите свое время
Используйте автоматизацию

paloalto NETWORKS

SOAR – основные примеры

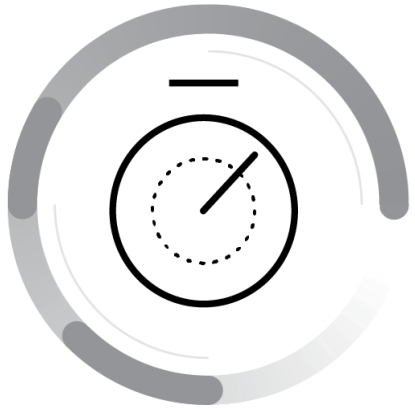
Сегодня расскажу	В записи: youtu.be/HBZptauuxSI
Фишинг	Cryptojacking
Защита рабочих станций	Управление уязвимостями
Невозможный путешественник	Облачная безопасность
Управление сертификатами SSL	Управление инцидентами
Белые списки приложений SaaS	Проактивно блокируем известные угрозы (TI)

Что мешает команде безопасников

Растущий поток событий

Очень много событий и мало людей на их анализ

10000/день



Недостаток времени

Однообразные ручные операции с продуктами мешают заняться чем-то более интеллектуальным

10+

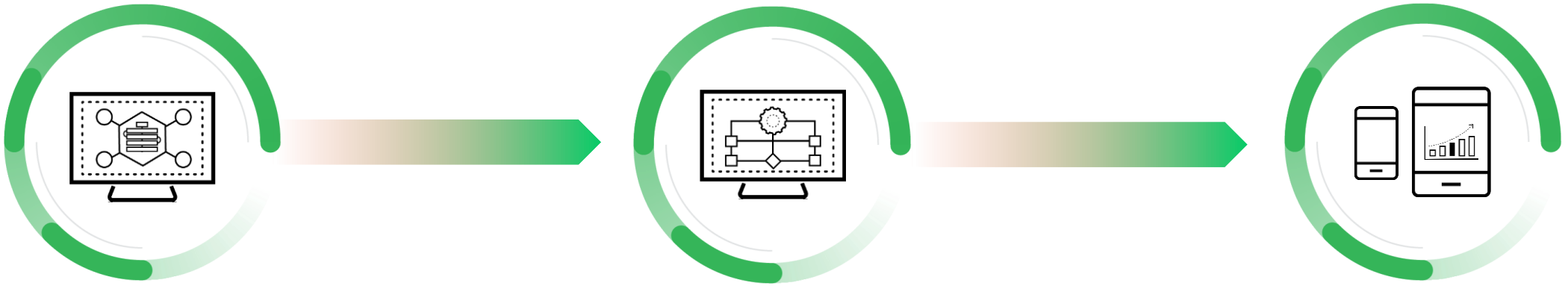
Узкий контекст

Несколько дней на сбор данных и расследование инцидента

4+ дня

Что делает SOAR?

Security **O**rchestration, **A**utomation, and **R**esponse



Оркестрация

Playbooks, runbooks, workflows

План действий в логическом порядке

Контроль и запуск продуктов безопасности из одной точки

Взаимодействие продуктов, технологий и людей

Автоматизация

Записанные действия сотрудников в виде скриптов

Интеграция со всеми продуктами

Компьютер исполняет готовые скрипты за сотрудника: ждет, напоминает, ищет

Готовый скрипт повышает квалификацию сотрудника

Реагирование

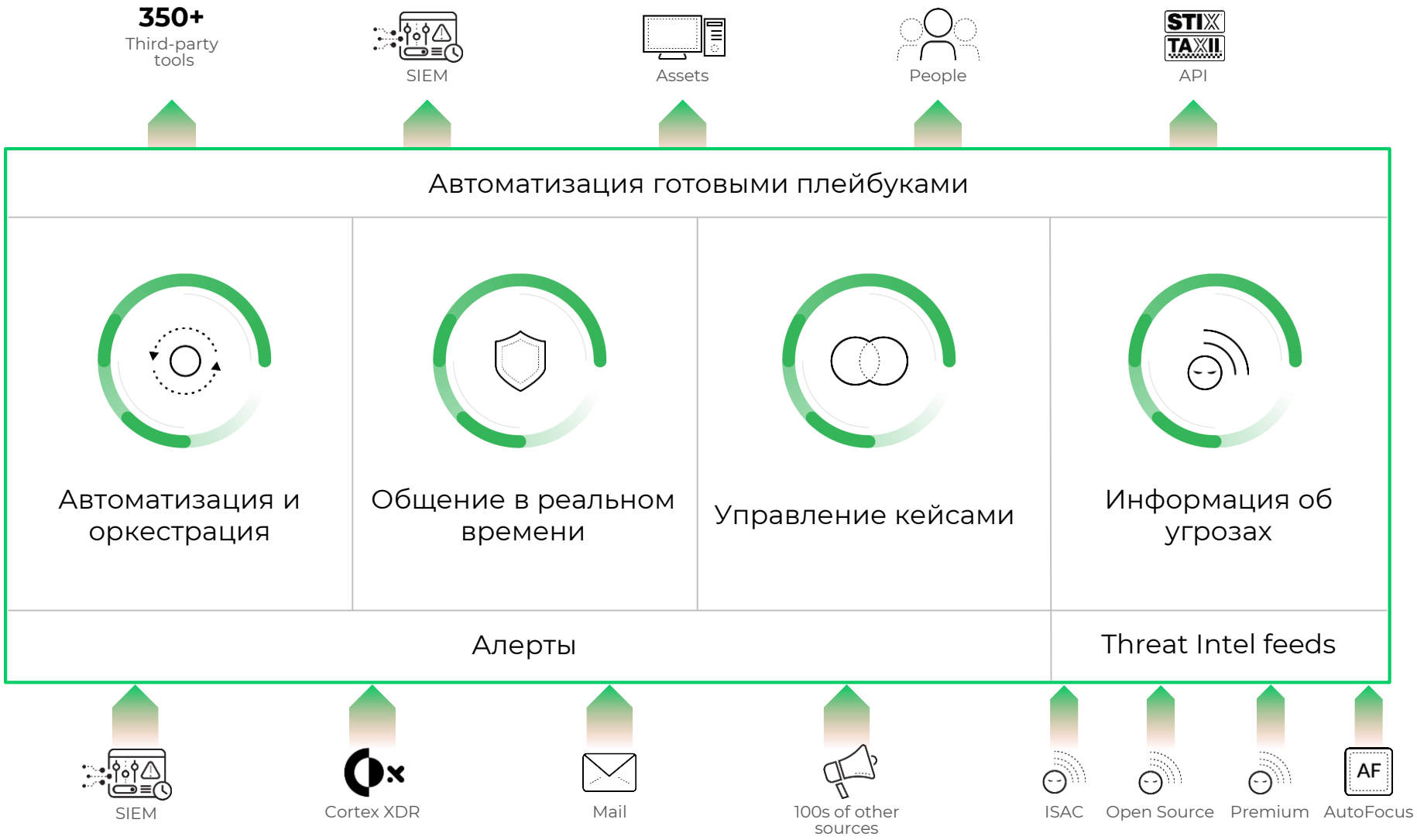
Управление кейсами

Аналитика и отчетность

Оповещение, совместная работа, контекст с другими кейсами

Подробно: youtu.be/BzB10GGQ8ms

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

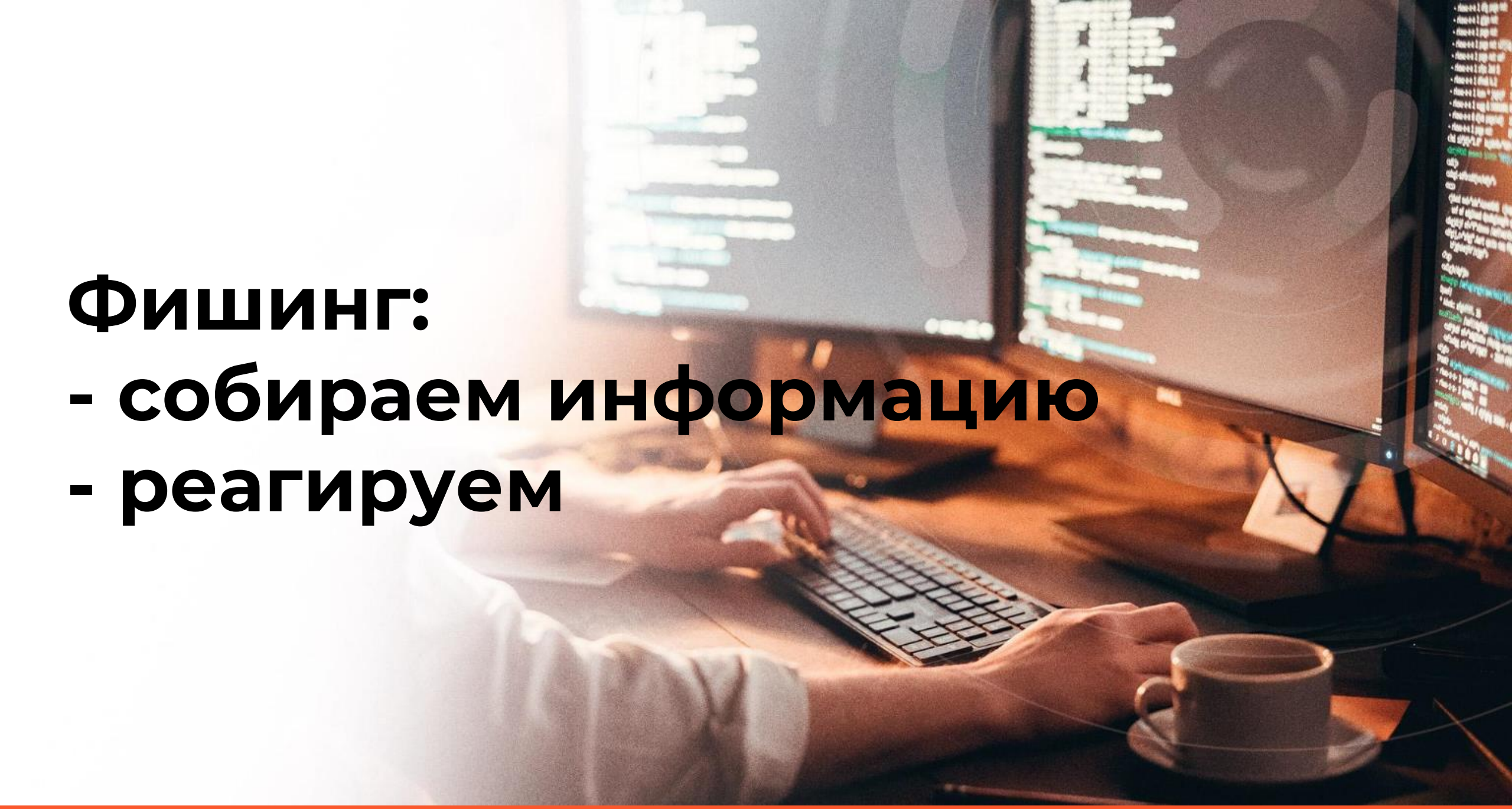


Cortex XSOAR применяется для многих задач

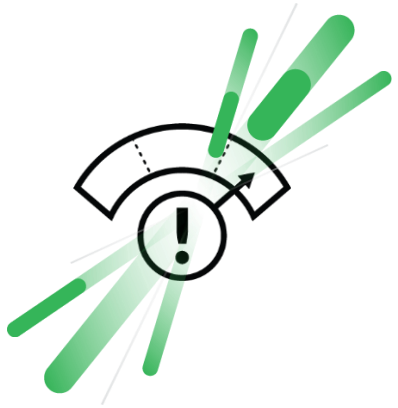
Источники событий
SIEM и аналитика
XDR (или EDR)
Облачные среды
Сканеры безопасности
Почта
Техподдержка
Данные расследований инцидентов

Разобраться и починить
Threat Intelligence
EDR
Анализ ВПО
Почта/ WEB
Техподдержка

Фишинг:
- собираем информацию
- реагируем

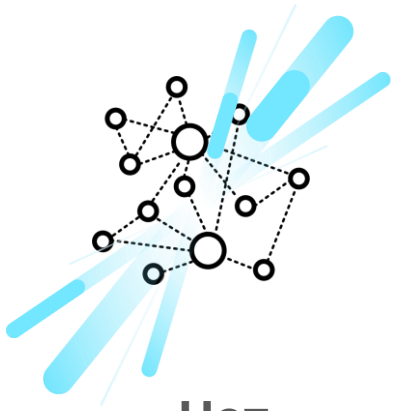


Проблема: **сложно реагировать на фишинг**



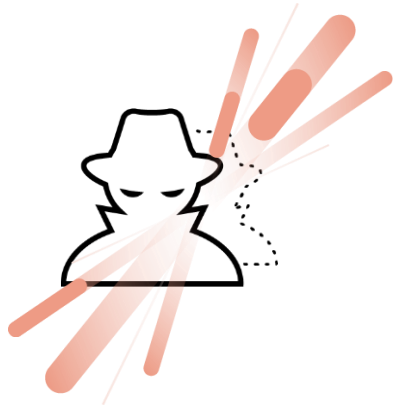
Очень много таких писем

Частая атака, легко проводится и с нее начинается большинство взломов



Нет согласованности

Нужно контролировать почтовые ящики, информацию об атаках, NGFW, хелпдеск и другие сервисы для защиты от фишинга



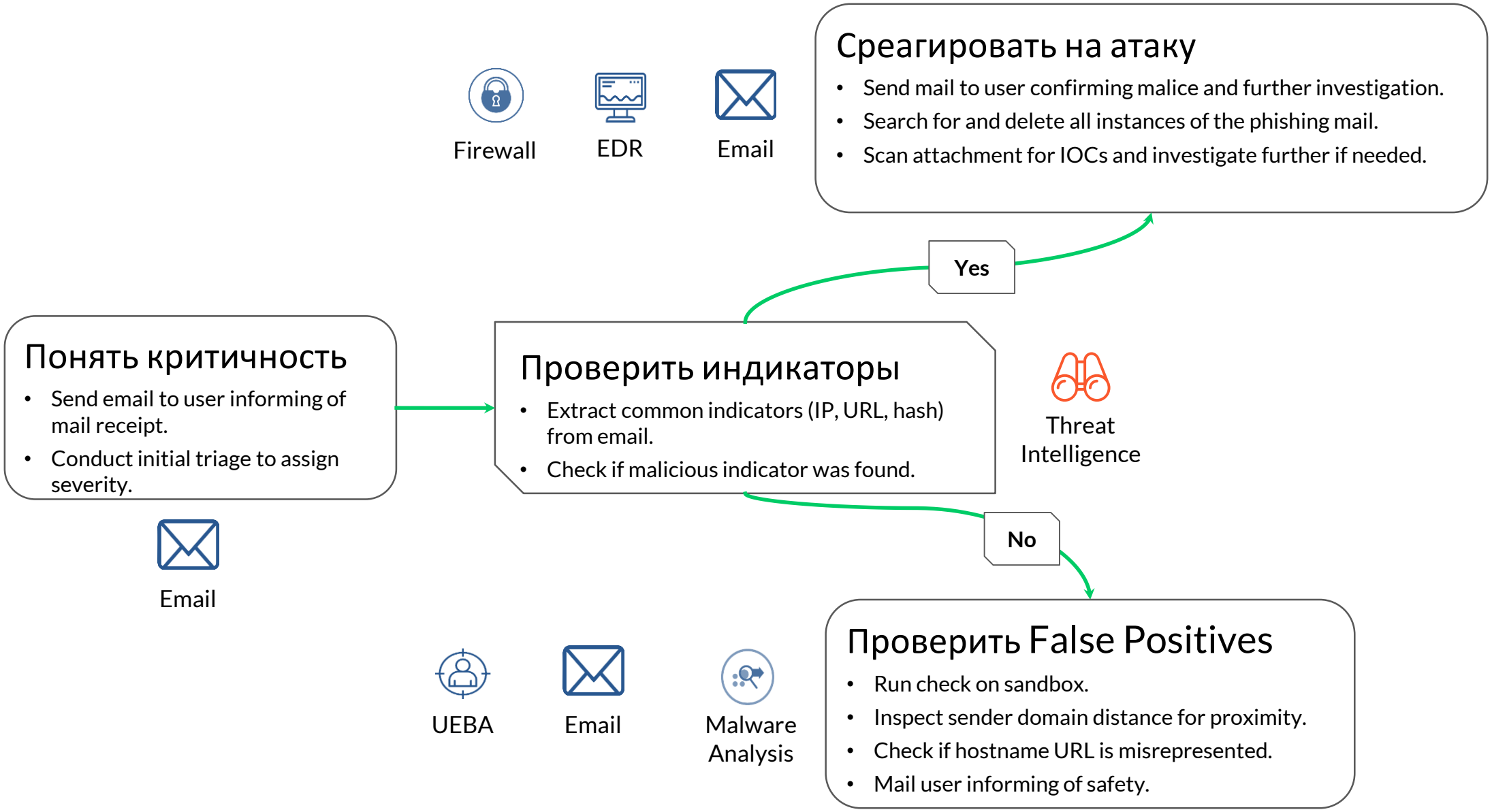
Есть всегда и растет

95% всех успешных атак на компании результат spear-phishing[1]

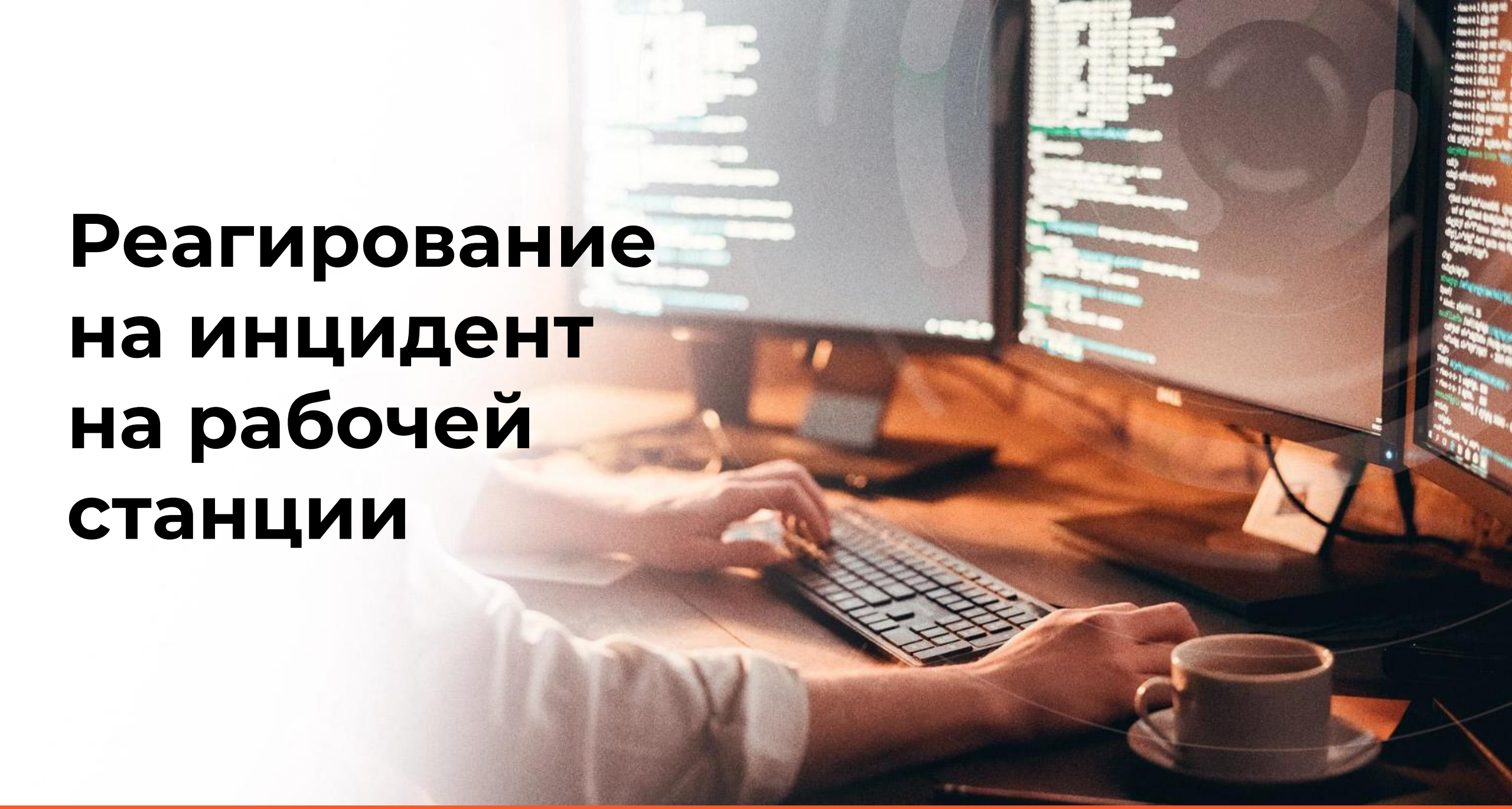
[1]Источник: https://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html

Как XSOAR помогает

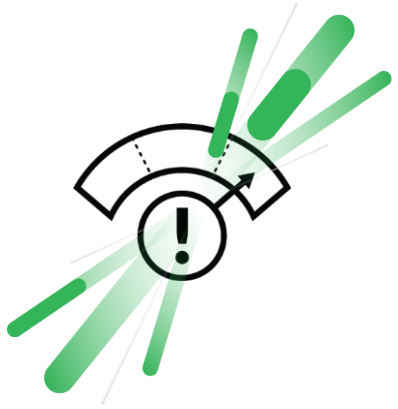
Существуют стандарты защиты от фишинга



Реагирование на инцидент на рабочей станции



Проблема: Сопоставление данных с SIEM и с хостов



Растущее число алертов

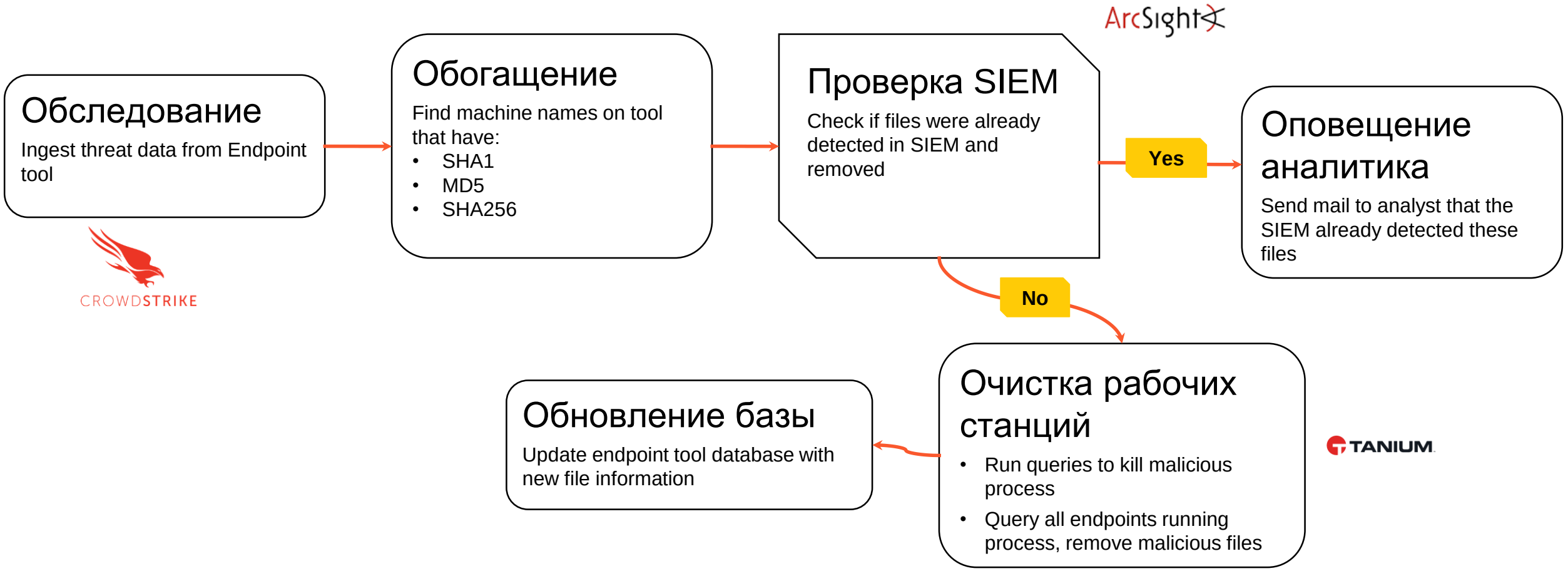
Сбор контекста вручную

Различные утилиты безопасности

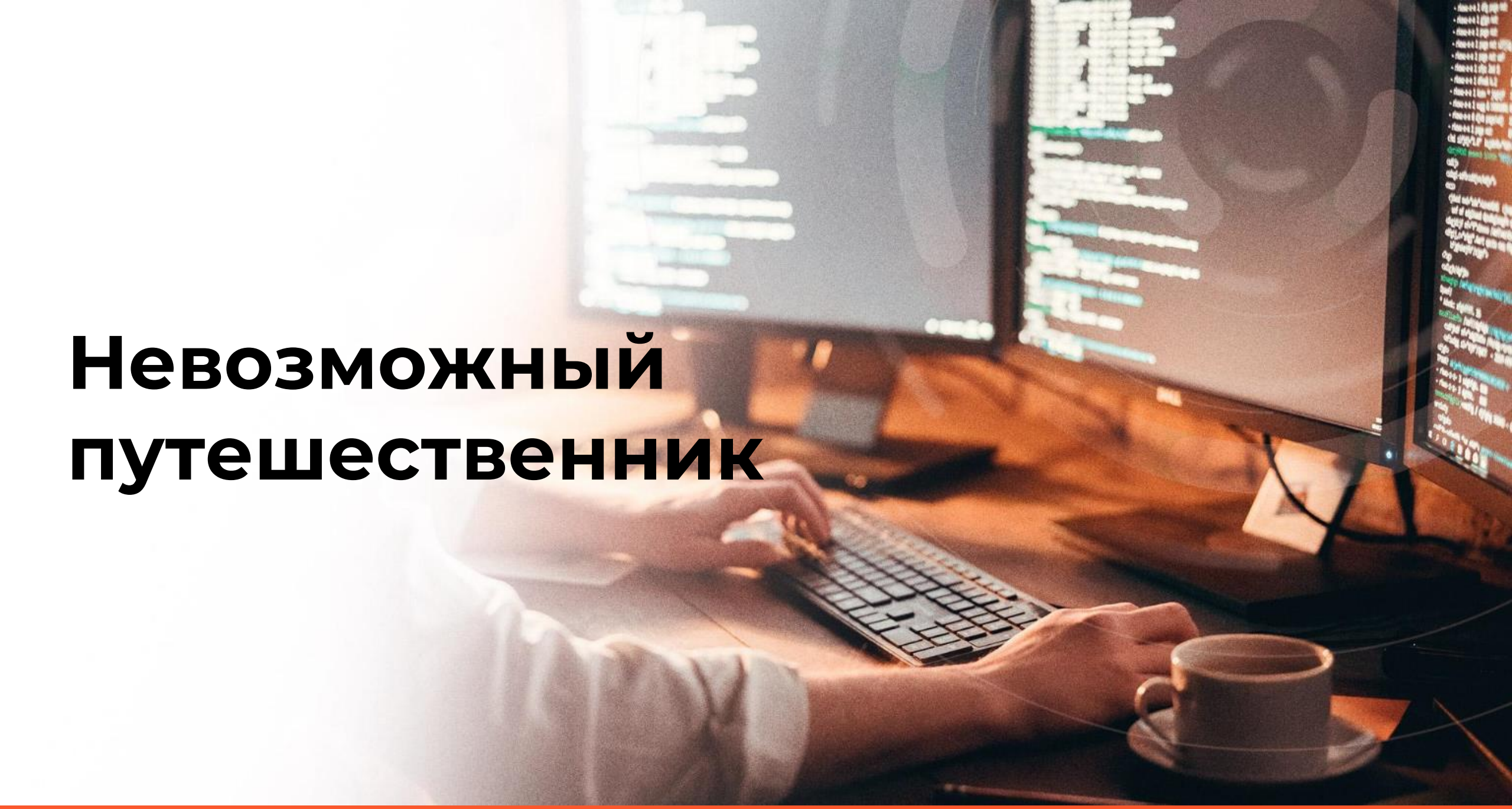
“Нашей сложностью стало сопоставление данных SIEM с полученными данными глобальных TI для активных действий. Аналитик проводил слишком много времени, имея огромное число открытых окошек и вручную проверял статус алертов. Это оставляло мало времени на реагирование. “**- Крупный консорциум технологических компаний**

Как SOAR помог – защита рабочих станций

Унификация процесса работы с SIEM и с консолью защиты рабочих станций



Невозможный путешественник



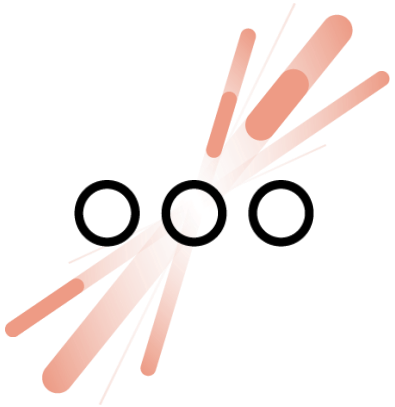
Проблема: **Найти подозрительные логины**

Поведение сложно контролировать

Вредоносные попытки логинов сложно контролировать, поскоку люди могут правда быть в другой стране

Множество систем

С появлением облачных технологий число точек контроля возрастает



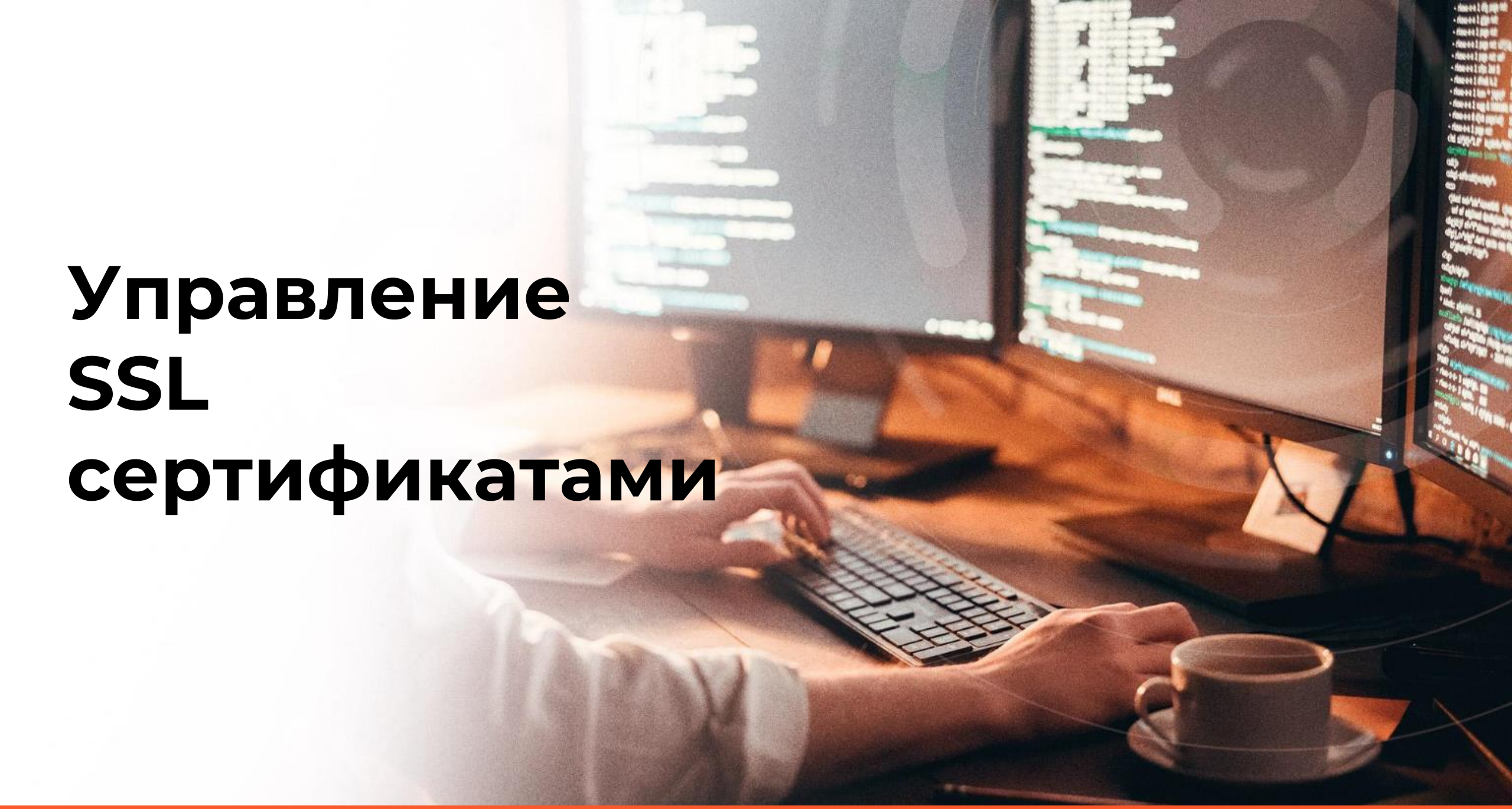
Постоянные задачи

Контроль подозрительных логинов слишком частая задача и отнимает время от более высокоуровневого анализа

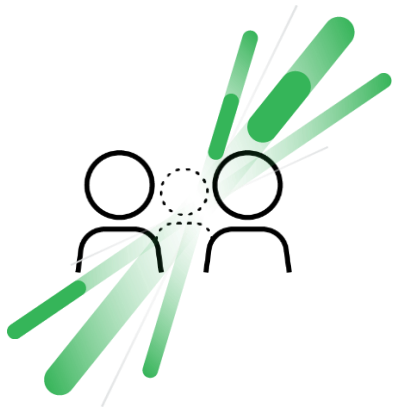
Как SOAR помог

Impossible time travel playbook - two IP addresses tied to same user are far apart

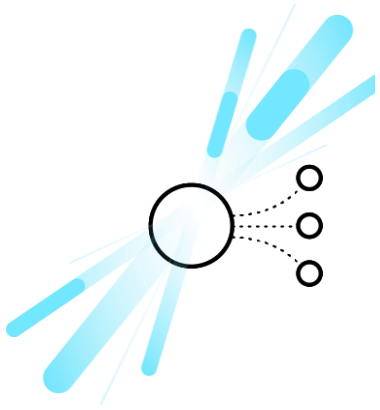
Управление SSL сертификатами



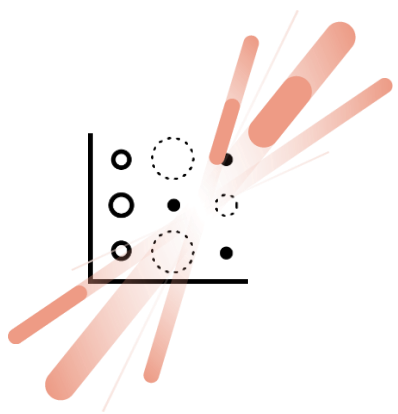
Проблема: Безопасники слишком загружены, чтобы проактивно делать проверки



Много команд



Много задач

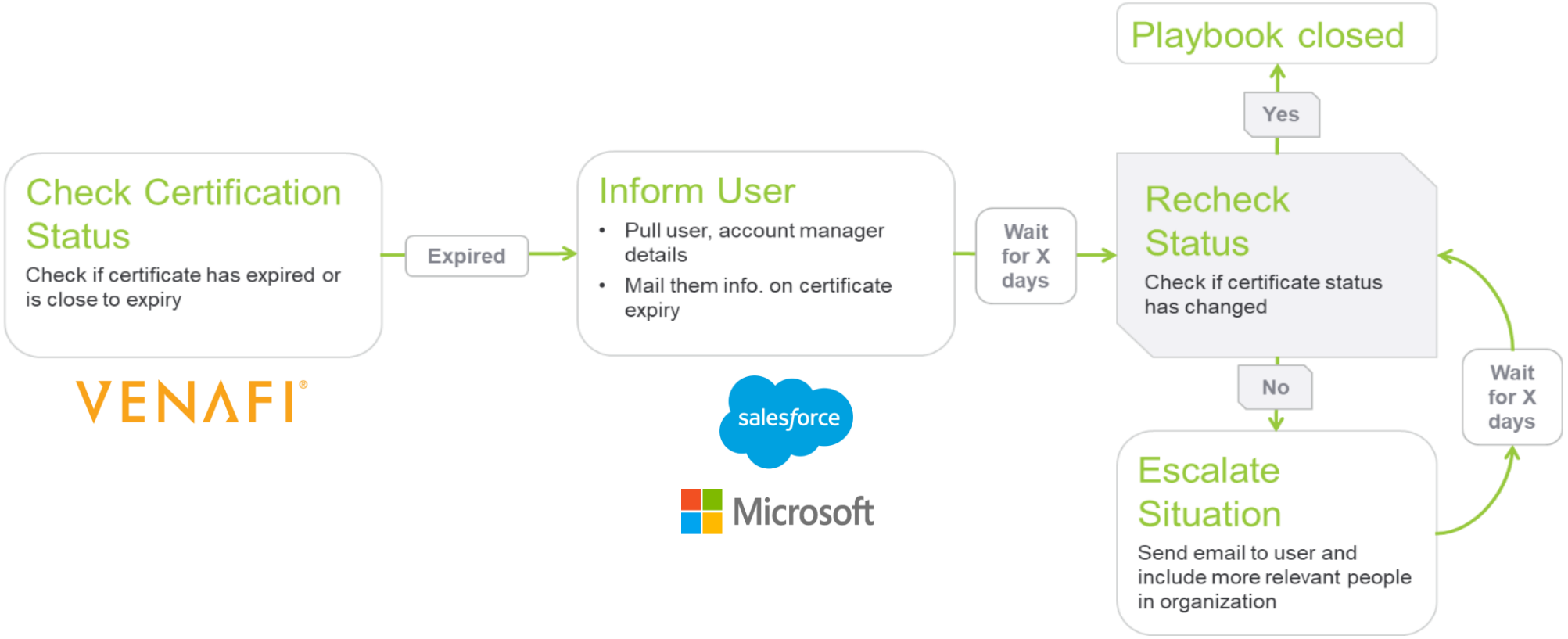


Задачи теряются в цепочках

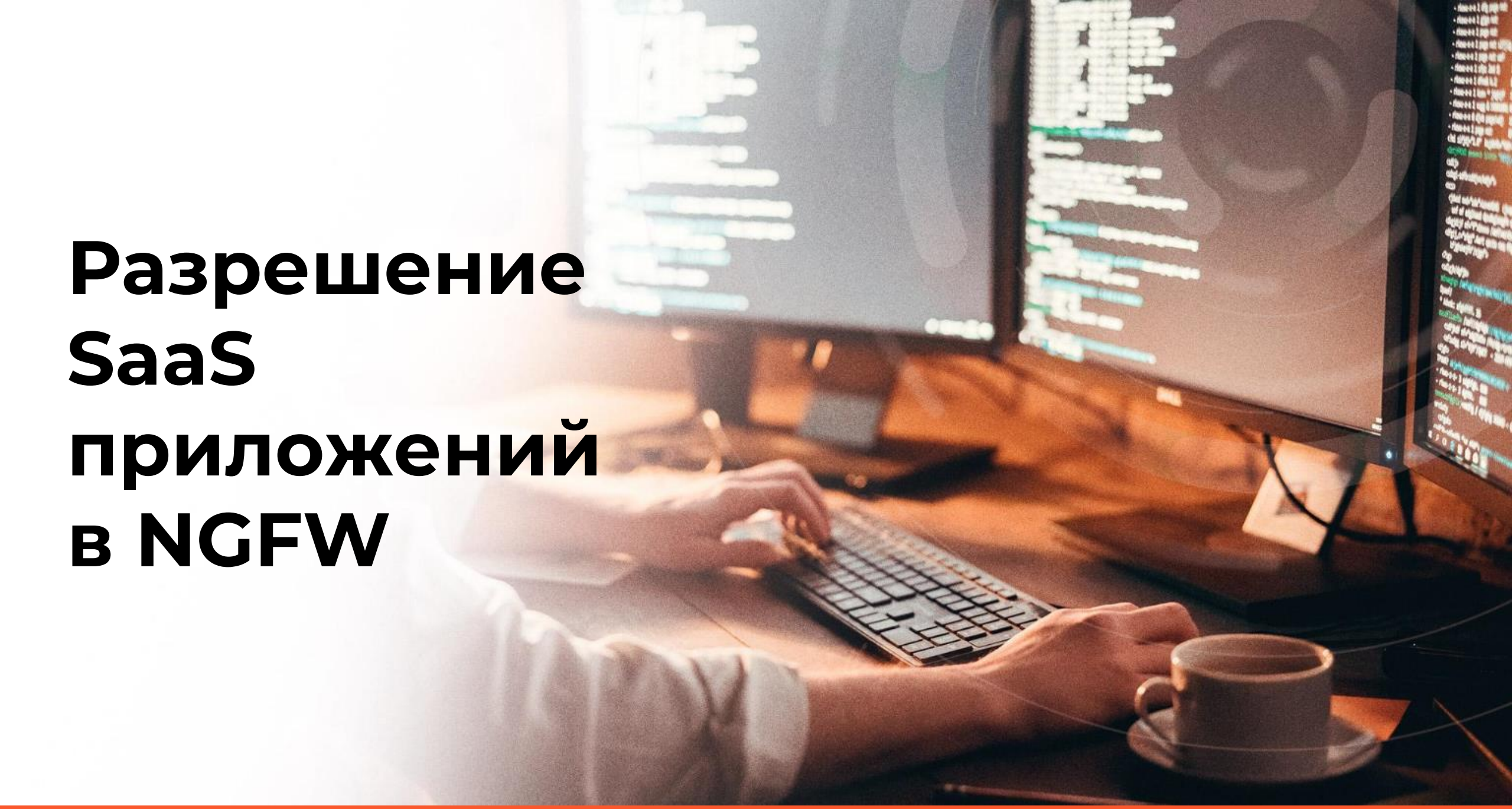
“Нам было сложно поддерживать SSL сертификаты в актуальном состоянии на рабочих станциях. Мы использовали Cortex XSOAR и периодически запускали playbook, который проверял SSL сертификаты на рабочих станциях, которые скоро истекут, что избавило от ручной проверки и от проблем с тем, что сертификаты истекают.” **- медицинская компания**

Как SOAR помог – управление SSL сертификатами

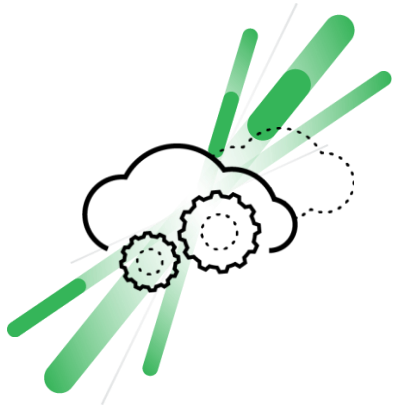
Операционные задачи регулярно сами запускаются и проактивно помогают ИТ



Разрешение SaaS приложений в NGFW

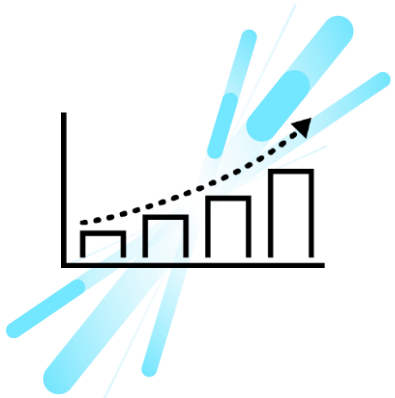


Проблема: Разрешить приложения, которые используют сотрудники



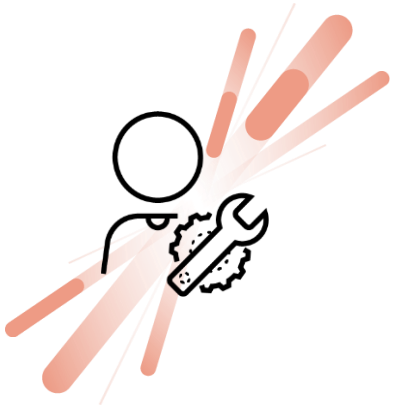
Облачные приложения динамические

Приложения могут перемещаться по миру, меняя адреса и нужно вовремя давать им доступ



Бизнес непрерывный

Доступ к Office 365, Dropbox и другим бизнес-приложениям должен быть постоянно

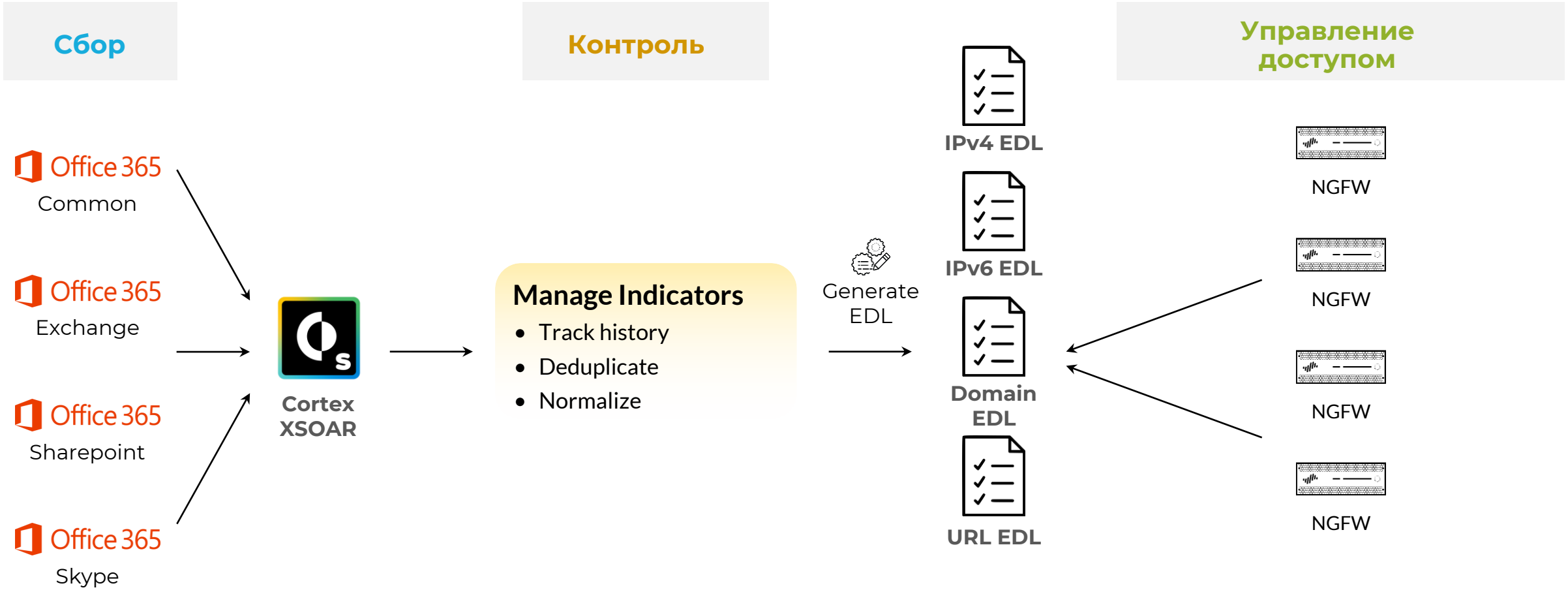


Процессы ручные

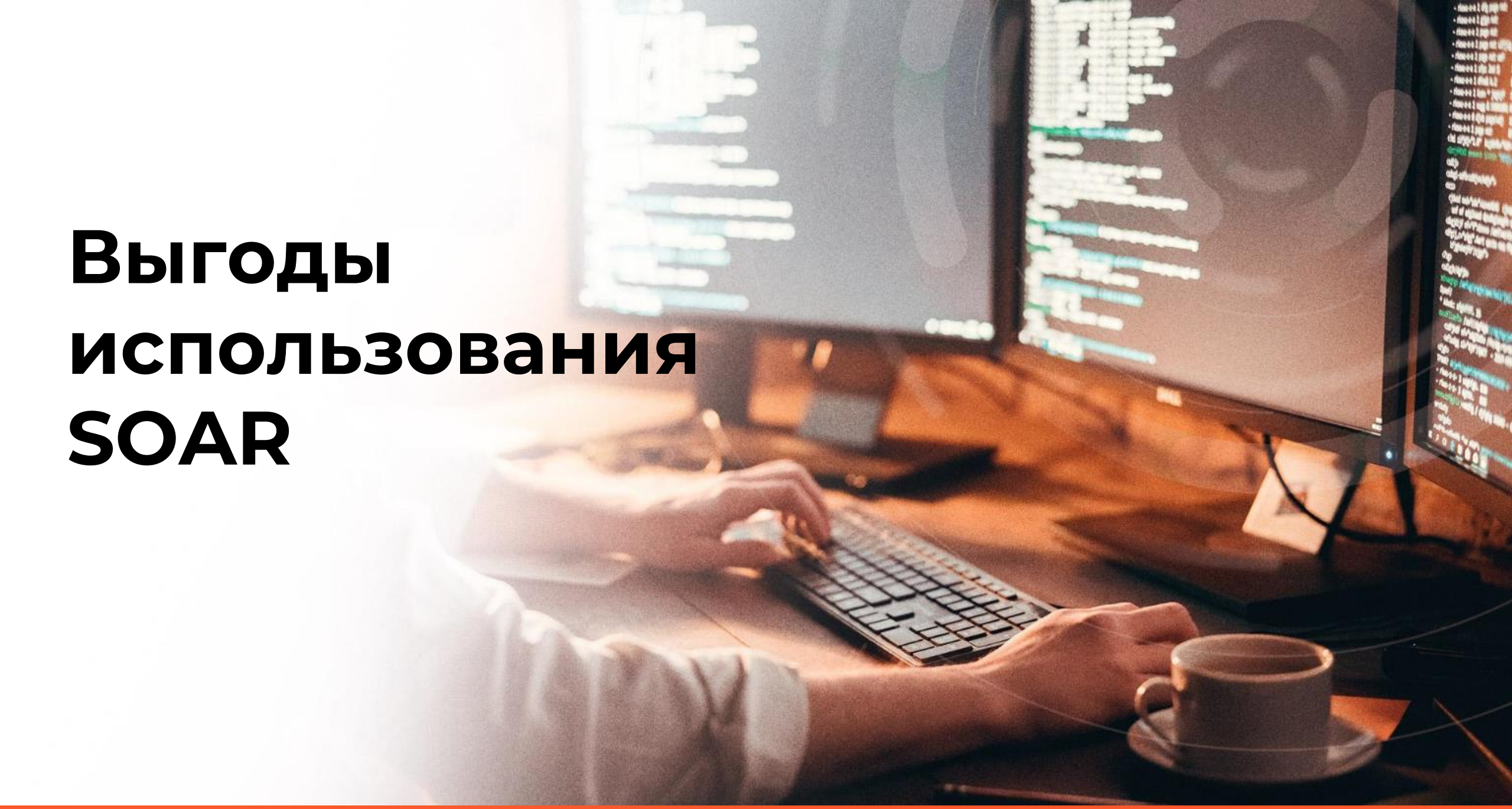
Создание единого белого списка доступа позволяет использовать его во многих устройствах компании

Как SOAR помог: Список доступа для SaaS приложений в NGFW

Как бы SaaS приложения не менялись – доступ всегда есть



Выгоды использования SOAR



SOAR позволил

Снизить поток алертов

Уменьшили число алертов
с 10000 до 500

Enterprise Software*

Быстрее реагировать

Снизили время реагирования
с 3 дней до 25 минут

Financial Services*

Эффективно управлять

Автоматизировали 30% инцидентов
1 FTE экономии

Energy/Utilities*

*Реальная статистика заказчиковCortex XSOAR

Запишите ссылки

- Самые частые use case реализованные в SOAR
  https://start.paloaltonetworks.com/whitepaper-top-security-orchestration-use-cases

- Что такое SOAR: Dummies Book:

  https://start.paloaltonetworks.com/your-guide-to-security-orchestration

- Gartner пишет про SOAR | Руководство Gartner по рынку SOAR

  https://start.paloaltonetworks.com/the-hitchhikers-guide-to-soar

- Попробуйте Free Community Edition!

  https://start.paloaltonetworks.com/sign-up-for-community-edition.html
- GitHub | Ссылка на сотни готовых playbook для Cortex XSOAR

  https://github.com/demisto/content/tree/master/TestPlaybooks

CORTEX™
BY PALO ALTO NETWORKS

Thank you

paloaltonetworks.com

paloalto® NETWORKS