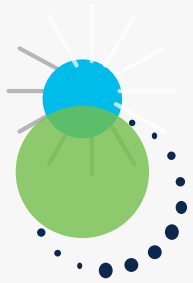
cisco SecureX

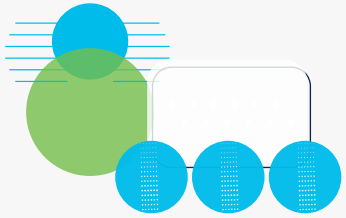
Облачные платформы безопасности – почему, что и как?

Михаил Кадер
Инженер

Команды ИБ пытаются идти в ногу с бизнесом разными путями

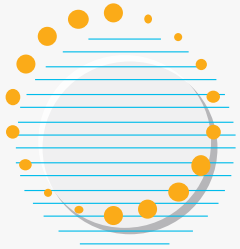


Нанимая и тренируя людей



Разрабатывая новые процедуры

Обновляя софт



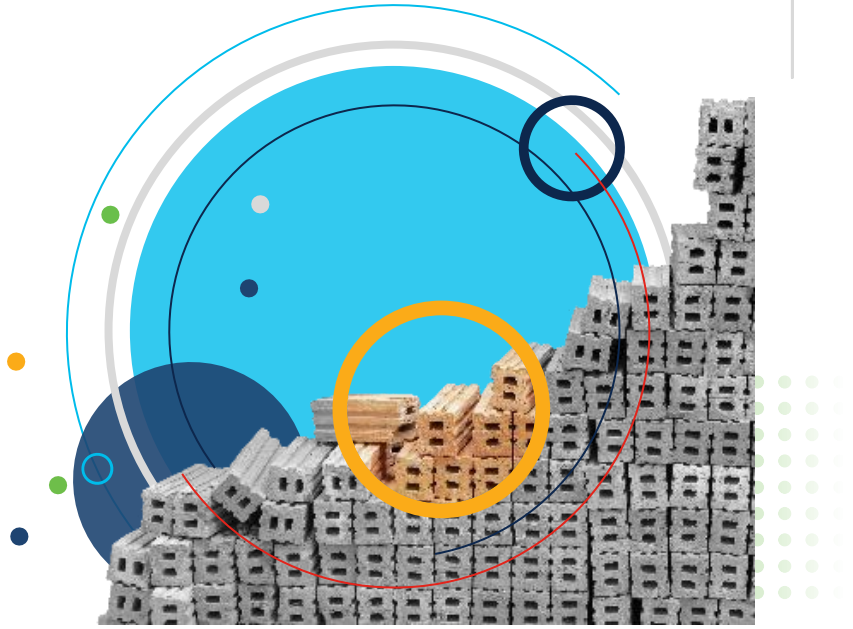
Добавляя новые технологии

Но просто добавлять новые технологии безопасности это обоюдно заточенный меч

Предоставляя новую функциональность, также добавляет много сложностей…

- Информация об угрозах и осведомленность разрознены
- Вы постоянно бегаете между разными интерфейсами
- Вы тратите слишком много времени на интеграции
- Ваши процессы разобщены

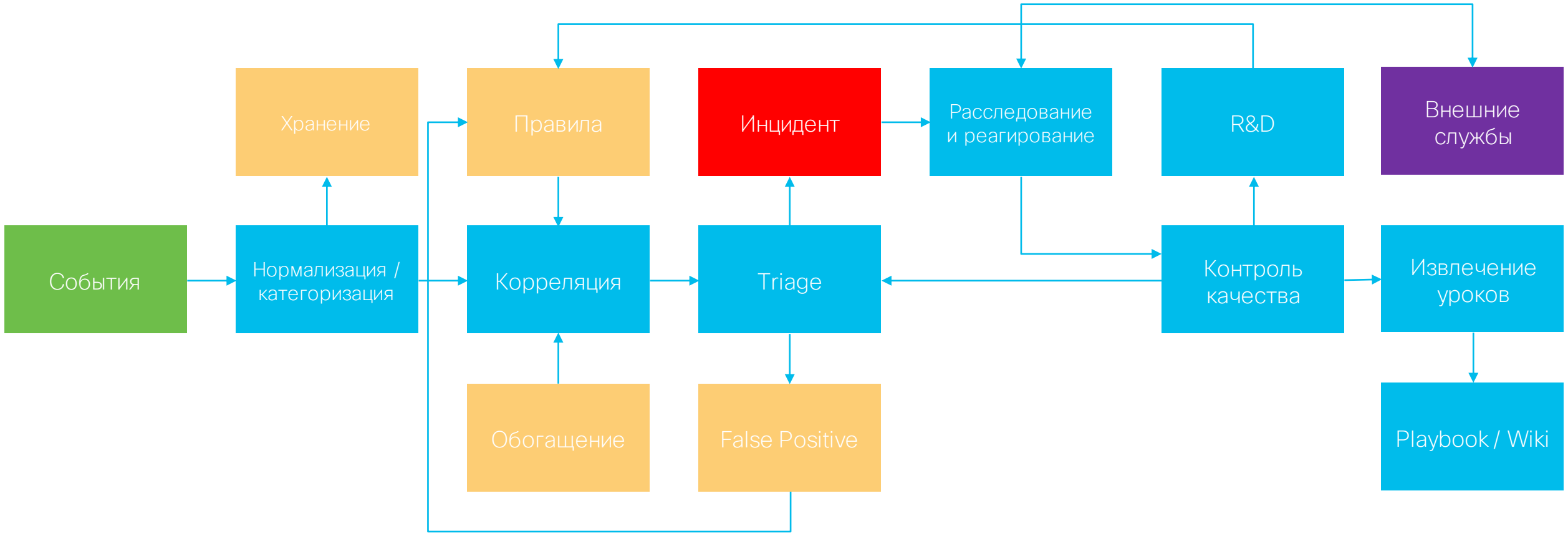
Это примерно как строить стену без раствора



Различные цепочки действий в рамках жизненного цикла события ИБ

Захват	Расследование	Локализация	Уведомление	Документирование
Захват в режиме Poll	Анализ файла	Заблокировать пользователя	E-mail	Создать тикет
Захват в режиме Push	Анализ домена	Блокировать хэш	Задача для SOC	Обновить тикет
Установить статус	Анализ URL	Блокировать URL / домен	Чат	Закрыть тикет
Установить приоритет	Анализ IP	Блокировать IP / порт / MAC	Звонок	Передать тикет
Создать артефакт	Анализ хоста	Карантин	Сигнал тревоги	Запросить тикет
	Генерация запроса	Блокировать процесс	Эскалация	Обновить playbook
	Получение событий	Отключить сеть		Создать use case

Жизненный цикл Security Operations



Security Operations объединяет множество решений в единый комплекс!

платных и бесплатных

Проблемы Security Operations

Ресурсы

Нехватка более 1 миллиона специалистов

Продукты

Точечные продукты

Алерты

Рост объема числа сигналов тревоги

Статичность

Статические независимые средств защиты без оркестрации

Скорость

Скорость обнаружения, приоритезации и времени реагирования

Цена

Стоимость продолжает расти

Потребность в автоматизации и оркестрации

- В феврале 2021 года компания IDC опросила 1013 руководителей по ИБ в разных странах мира относительно их планов по инвестициям в автоматизацию и оркестрацию в ближайшие два года

Платформенный подход уверенно решает наиболее неприятные проблемы ИБ

Простота

Интеграция технологий с **немедленным взаимодействием**

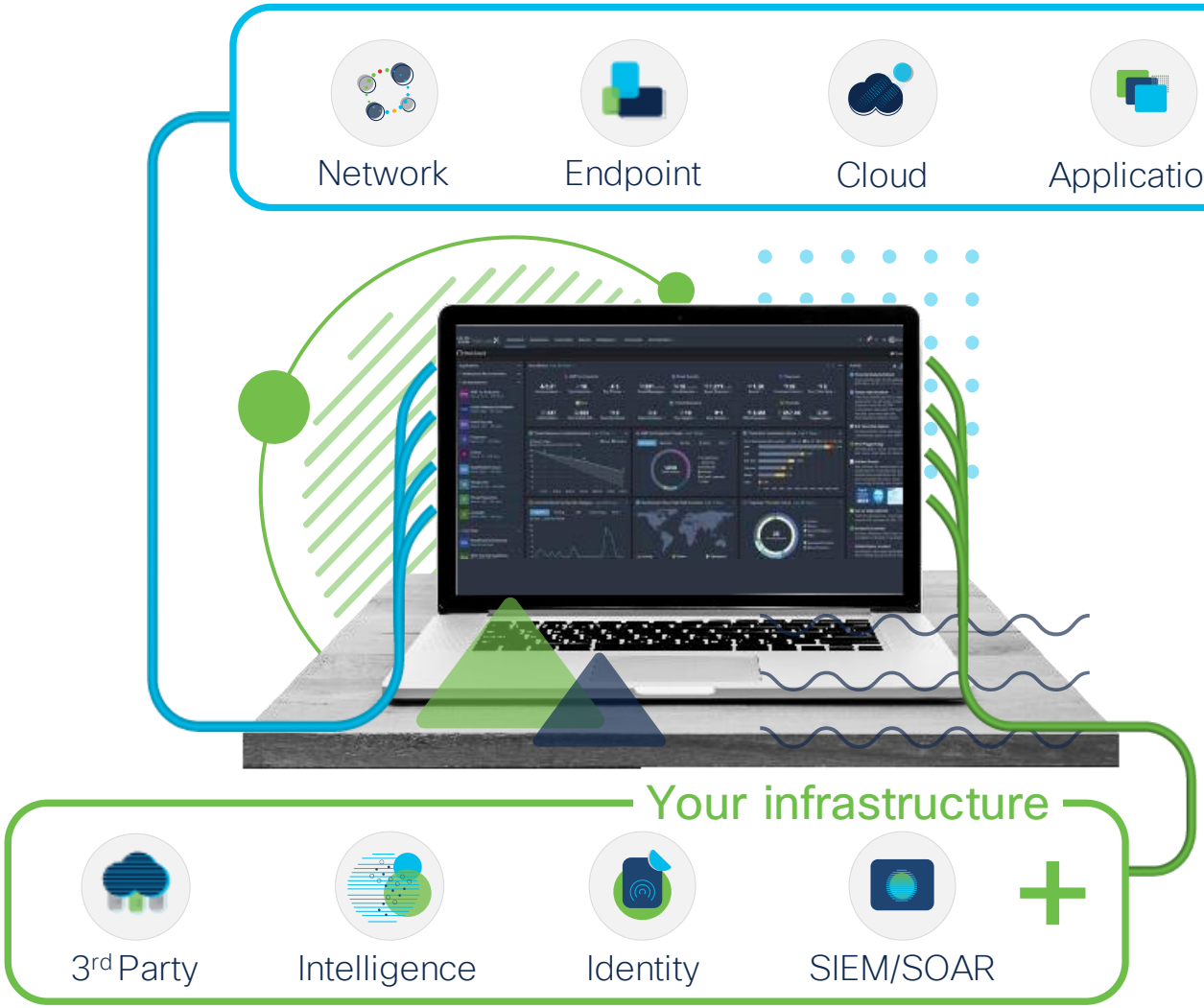
Видимость

Снижение **времени обнаружения и расследования** угроз и поддержка знания контекста

Эффективность

Ускорить **исправление и коррекцию** и автоматизировать рабочие процессы для усиления безопасности

Каждый соединен со **всей** инфраструктурой безопасности



Интегрируйте всё в своем окружении для получения унифицированного контекста, автоматизации и усиления безопасности

Унификация контекста и осведомленности во всей инфраструктуре

ДО

Ваши команды переключались между множеством консолей теряя понимание

ПОСЛЕ

Принимать решения на основании богатого контекста

Автоматизировать критические процессы

ДО

Ваши процедуры ручные и запутанные, и ведут к человеческим ошибкам

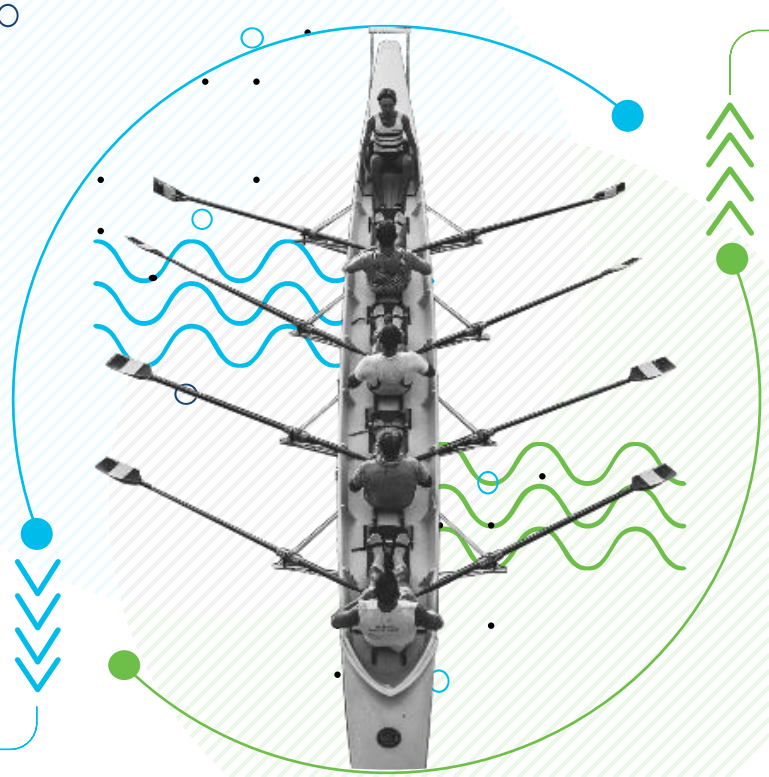
ПОСЛЕ

Поднять операционную эффективность и точность с усиления безопасности

Улучшая взаимодействие

ДО

У Ваших команд был разрозненный взгляд на угрозы, что ухудшало реагирование



ПОСЛЕ

Обмен контекстом между командами для ускорения процессов

Снизить сложность и получить преимущества

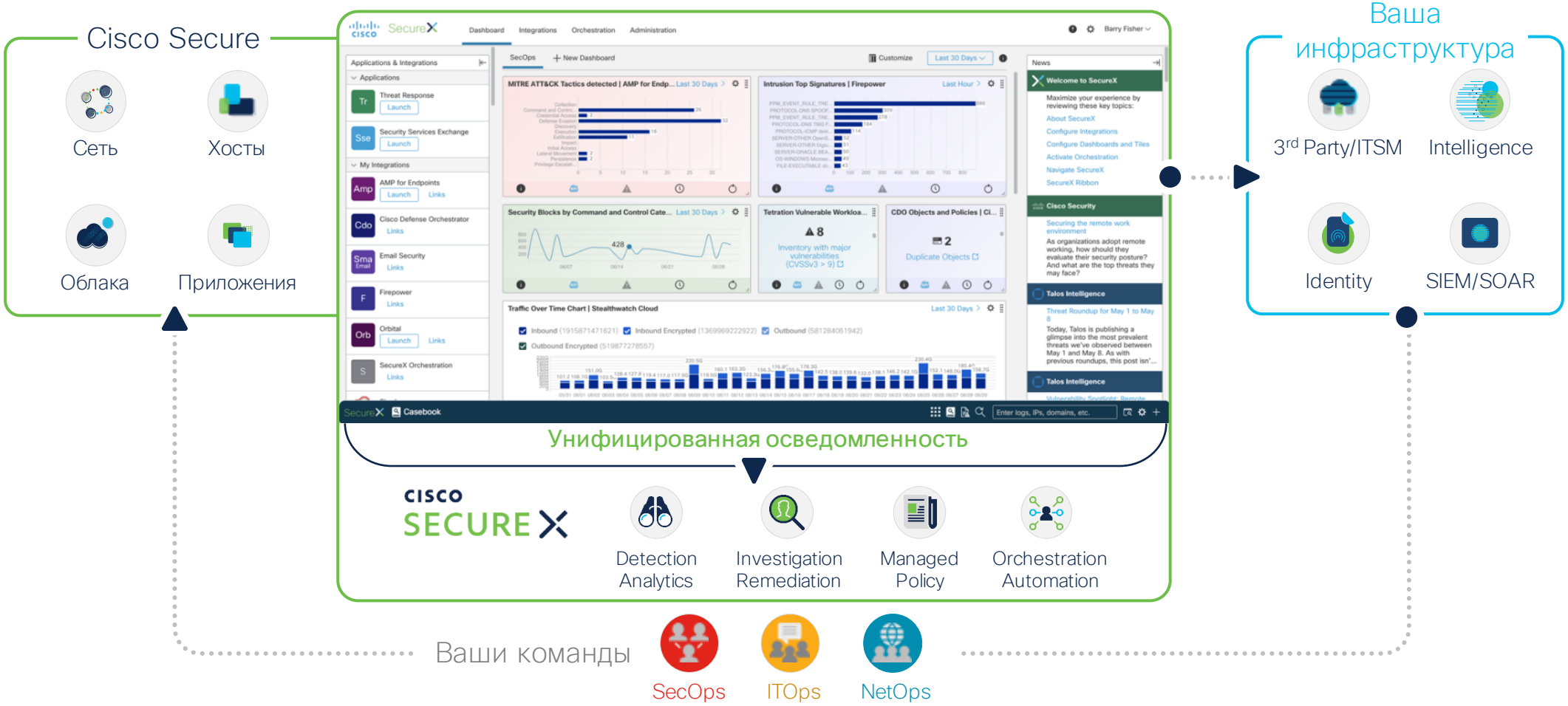
ДО

Отсутствие интеграции между инструментами снижает их ценность

ПОСЛЕ

Приумножьте Ваши возможности соединив инфраструктуру безопасности

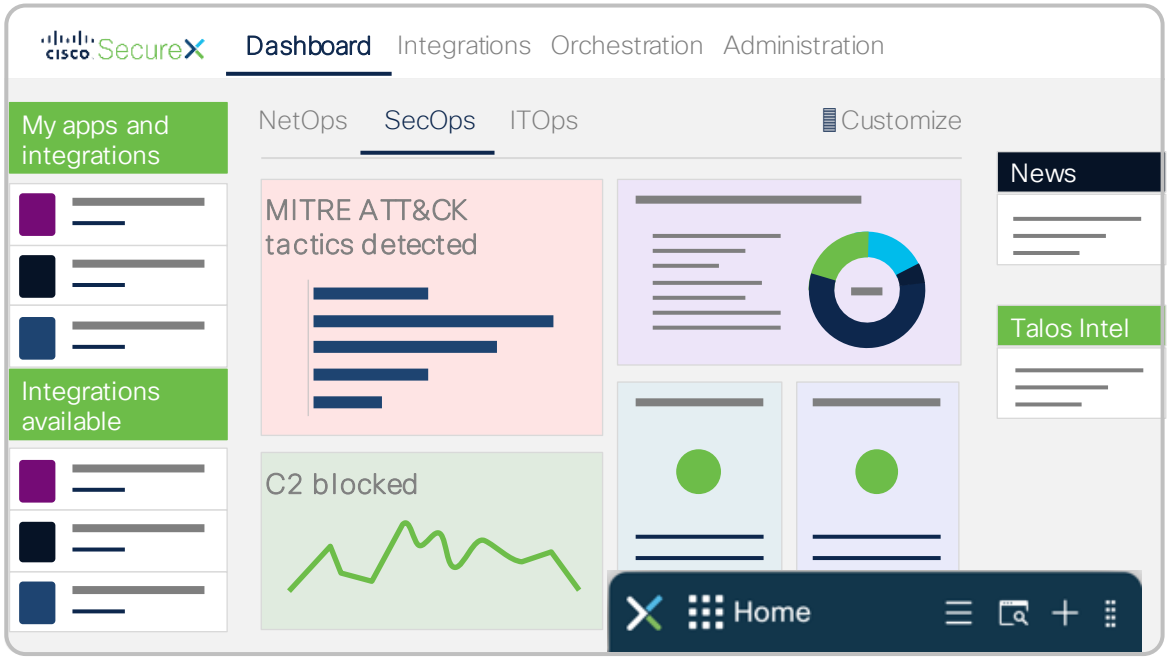
Облачная платформа безопасности



Как же выглядит унифицированная осведомленность

До: “Мы крутимся на стуле, чтобы увидеть как можно больше консолей”

После: “Мы моментально видим то, что для нас важно в едином окне”



“Мы можем видеть метрики ROI и операционные метрики по многим продуктам в **одном или нескольких дэшбордах**”

“Мы **никогда не теряем контекст** так как лента следует за нами везде где мы используем Cisco Secure portfolio”

“Мы можем протестировать интеграцию с другими платформами **одним щелчком** перед покупкой”

“Наш **SOC получает последние данные** от крупнейшей исследовательской команды по киберугрозам на планете”

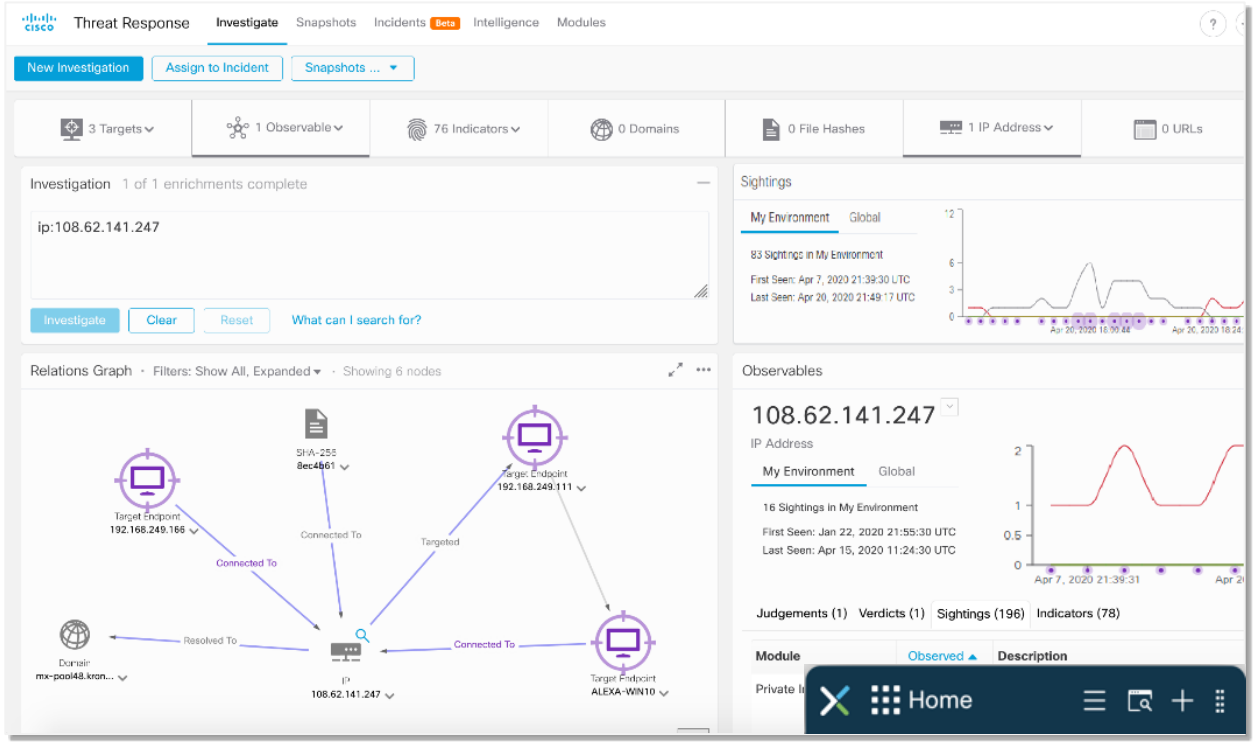
Ускорение расследований

Агрегирование и запросы глобальным базам угроз сведенные с локальным контекстом в унифицированном виде

Визуализация распространения угрозы в Вашем окружении

Принятие мгновенных решений по изоляции хостов и блокировании доменов и файлов

Автоматизация процессов с подтверждением для лучшего взаимодействия



Расследуйте с диспозицией, контекстом и реагированием

Диспозиция

Безопасность хостов
Данные о Malware
Данные о Internet

VirusTotal и другие

Эти объекты подозрительные или вредоносные?

Локальный контекст безопасности

Безопасность хостов

Безопасность почты

Аналитика (StealthWatch)

Облачная безопасность

Межсетевой экран

Безопасность Веб

Видели ли мы данные объекты? Где?

Какие хосты подключались к этим доменам/URL?

Реагирование

Блокирование доменов

Блокирование файлов

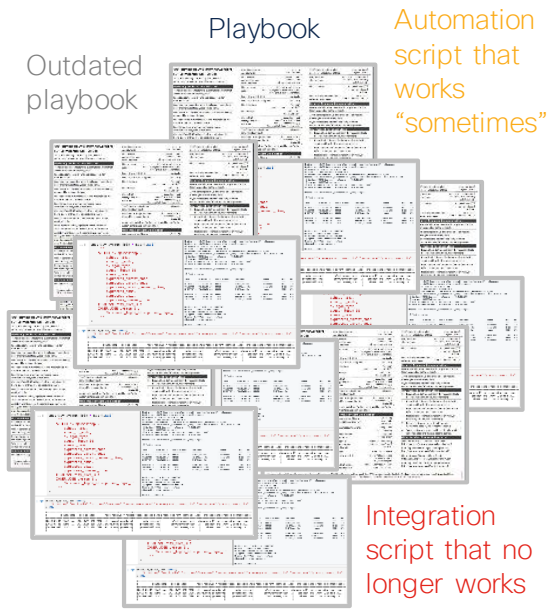
Изоляция хостов

Что я могу с этим сделать прямо сейчас?

Объекты: 1) Хэш файла, 2) IP адрес, 3) Домен, 4) URL, 5) Email адрес, и др.

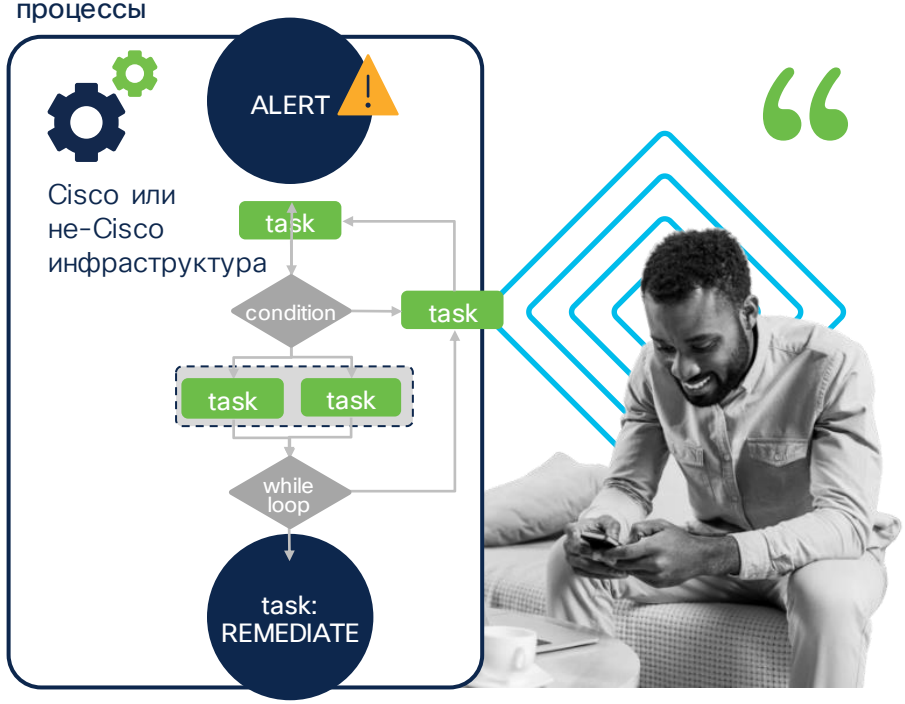
Максимизировать операционную эффективность

До: Повторяющиеся задачи, исполняемые человеком



Решение: Полный цикл оркестрации безопасности

Встроенные и настраиваемые процессы



После: Я собрал **9 задач** в 3-х инструментах безопасности, 2-х инфраструктурных системах и 3 команды **в один клик!**

“ Я создал автоматизированный playbook с помощью интерфейса drag and drop

Мы никогда не взаимодействовали быстрее: Наши подтверждения автоматизированы

Мои ТОП 5 наиболее раздражающих задач были автоматизированы

Оркестрация

Простой процесс автоматизации с интерфейсом drag & drop без программирования

Расследование

Снизить время на расследование и реагирование с помощью процессов и playbook, исполняемых со скоростью компьютера

Автоматизация

Исключить повторяющиеся задачи и снизить время реагирования для повышения производительности и концентрации на критичных задачах

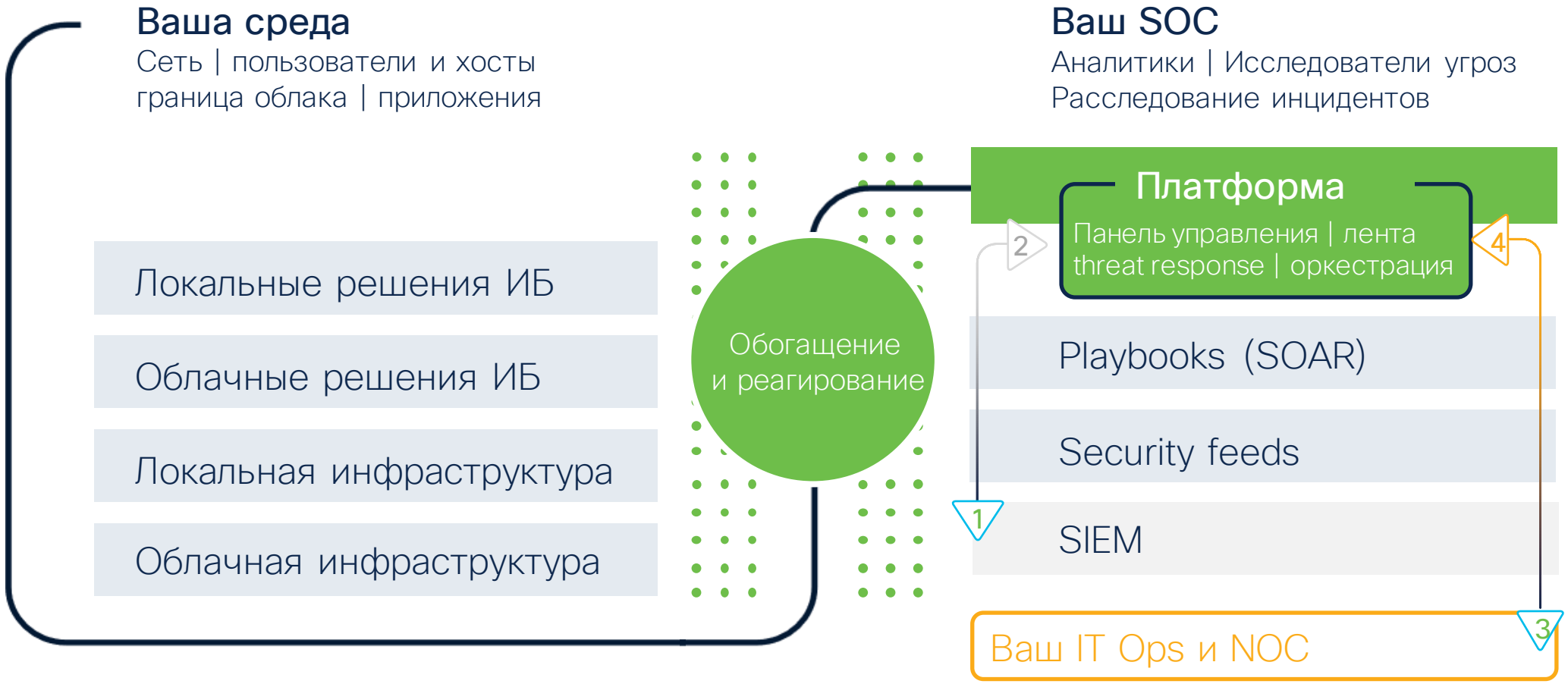
Интеграция

Уникальный подход для быстрой интеграции с другими системами и решениями для расширения инструментария

Масштабирование

Бесконечно масштабируемая автоматизация, которая не нуждается в отдыхе, предоставляет целостный SLA круглые сутки

Интеграция в Ваш SOC



Платформа открывает новые возможности для вашей организации

Интегрирована и открыта для **простоты**

Унификация в одном месте для **видимости**

Максимальная операционная **эффективность**

Множество продуктов по информационной безопасности

за 15 минут, Вы получаете реальные преимущества в использовании того что уже приобрели

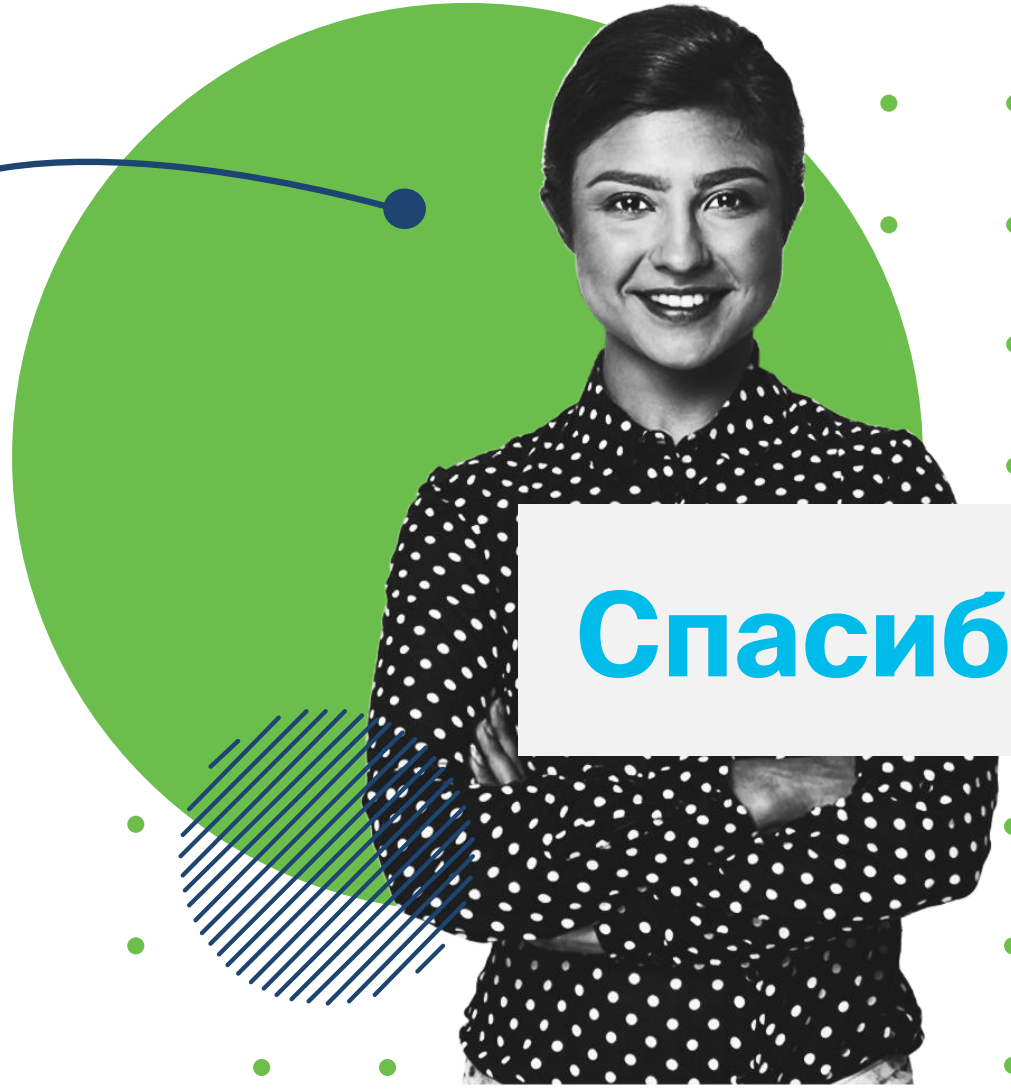
В два раза быстрее, заказчики визуализируют угрозы в своей сети[1]

Сохраняет сотни часов унифицируя и автоматизируя операции

85% снижение времени реагирования на атаку и восстановления после нее[2]

[1] Source: TechValidate

[2] Source: Based on internal simulation



Спасибо!