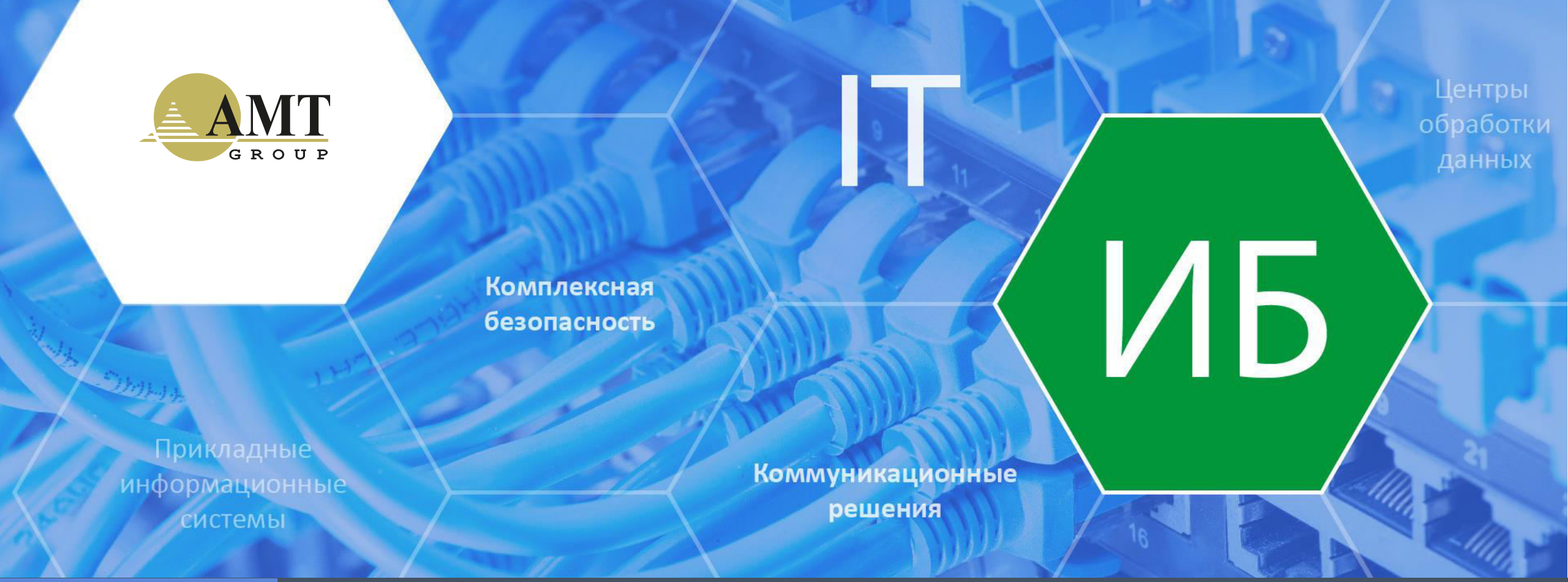


14.02.2019

АМТ-ГРУП

Актуальные подходы к автоматизации процессов ИБ

Кондратьев Илья, зам. директора ДИБ АМТ-ГРУП

Проблемы и предпосылки

- Количество и разнообразие средств защиты растет. Угроз тоже
- «Нехватка рук и других частей тела…»
- Многие процессы опираются на бумажные и ручные процедуры
- Ошибки и очепятки при ручном конфигурировании - усилия и время
- IT ушло далеко вперед по пути автоматизации, «облаков» и SDN
- ФЗ 187 - появление средств защиты там, где их раньше не было и вовлечение в процессы ИТ и ИБ новых, «непрофильных» сотрудников

AMT GROUP

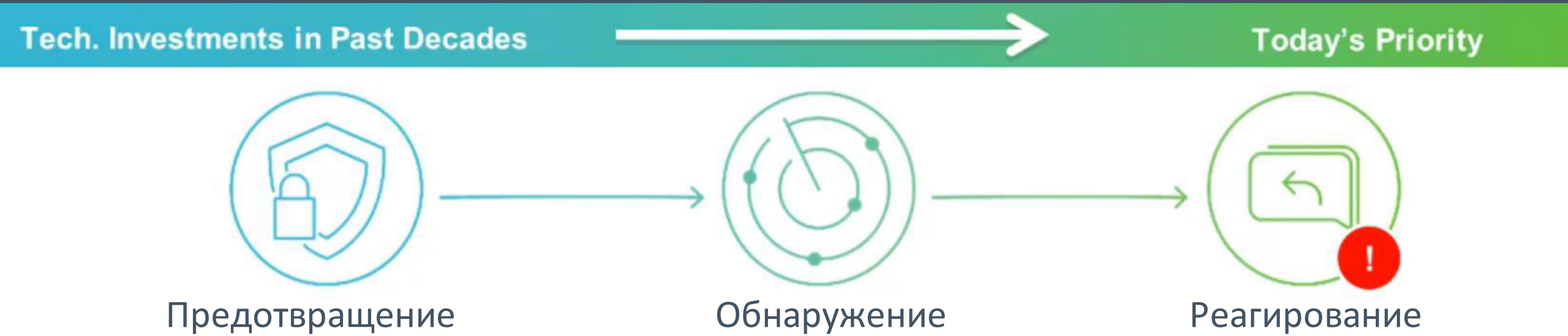
Проблемы и предпосылки

- Чтобы выжить и развиваться организациям нужно повысить скорость в процессах обеспечения ИБ
  - управление правами и доступом
  - управление изменениями
  - инвентаризация и аудит
  - реагирование и расследование
- Дефицит квалифицированных кадров - знание в головах профессионалов(“tribal knowledge”).
- Проблемы сохранения знаний - «единая точка экспертного знания», «смена команды»
- Увеличение количества специалистов может снизить скорость
- Оперативность реагирования играет ключевую роль

AMT GROUP

Мировые тенденции – Автоматизация в ИБ

Смена парадигмы - от Предотвращения к Обнаружению и Реагированию*



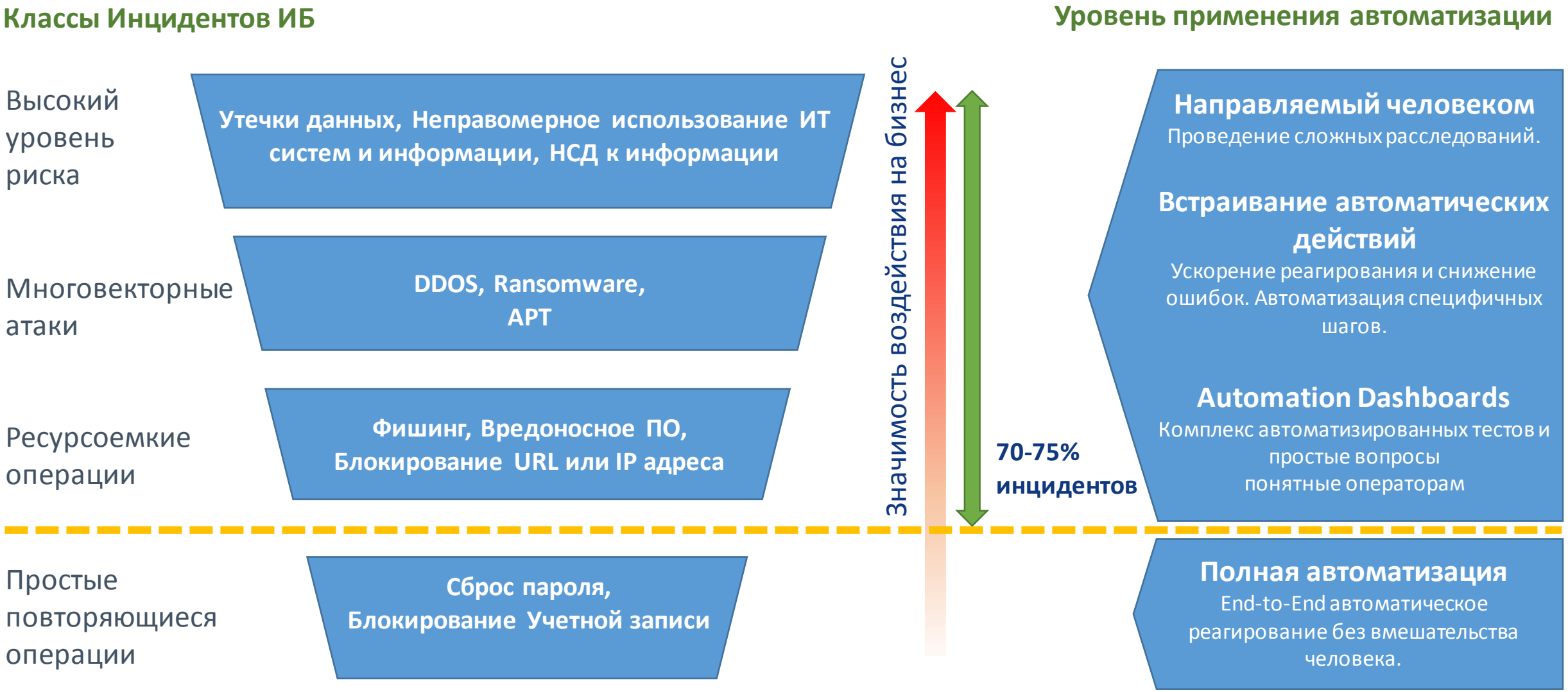
*Согласно исследованиям SANS Institute

- "By year-end 2020, 15% of organizations with a security team larger than five people will leverage SOAR tools for orchestration and automation reasons, up from less than 1% today."
  – Gartner, Innovation Insight for Security orchestration, Automation, and Response, Nov. 2017
- "Due to staff shortages in security operations, there is a growing need to automate, streamline workflows and orchestrate security tasks." – Gartner, Innovation Insight for Security orchestration, Automation, and Response, Nov. 2017

Gartner

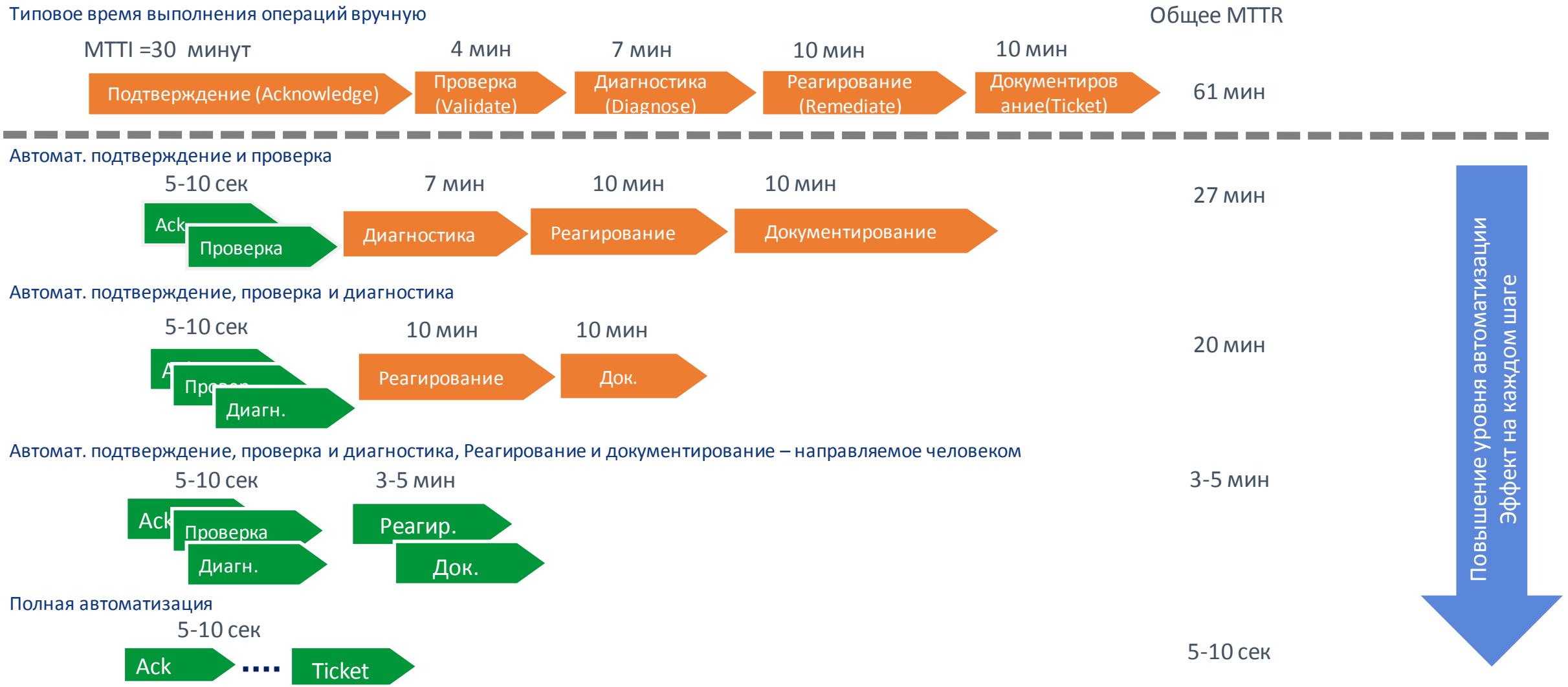
Автоматизация прямо влияет на эффективность

Позволяют справиться со сложными кейсами и быстро адаптироваться

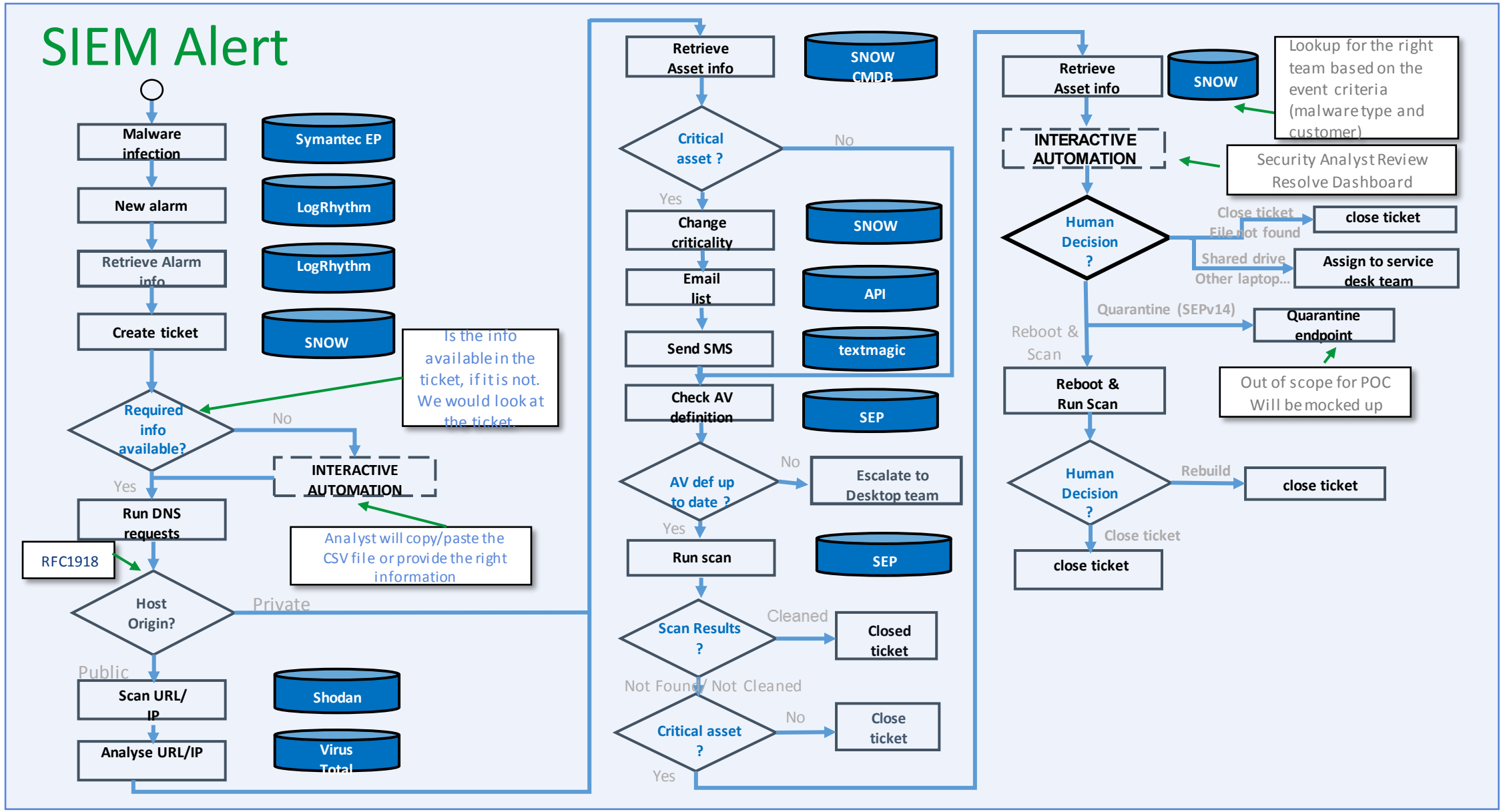


Внедрение поэтапно, эффект сразу

Поэтапное внедрение: автоматизировать где возможно, ускорять операции там где пока нельзя автоматизировать



Пример кейса



Автоматизация – это подход, а не продукт

Цели автоматизации

- Скорость изменений и реакции
- Повышение эффективности персонала
- Адекватный ответ современным угрозам

Автоматизируют процессы

- Управление изменениями
- Инвентаризация и аудит
- Диагностика, отчетность и реагирование

Принципы автоматизации

- От простого к сложному
- Измеримость
- Вовлечение ИТ и ИБ специалистов

Что уже автоматизировано

- Сбор и консолидация событий
- Корреляция
- Мониторинг и аналитика

AMT GROUP

Что для этого нужно?

Консоль АИБ, оператора SOC

Playbooks, Scripts, KB

- Процессы – выявить, описать, выстроить/упорядочить.
- Сценарии и «Ролевые игры», База знаний, Case management
- Современные СЗИ и API – хорошо, с Legacy тоже можно работать.
- Ядро - Платформа оркестрации и автоматизации (SOAR, Security Orchestration Automation Response)

Кто это будет делать?

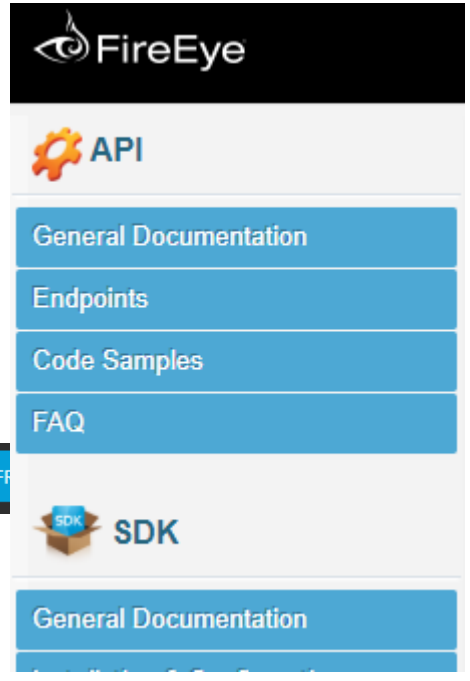
Подход к внедрению – своими силами или позвать на помощь интегратора?

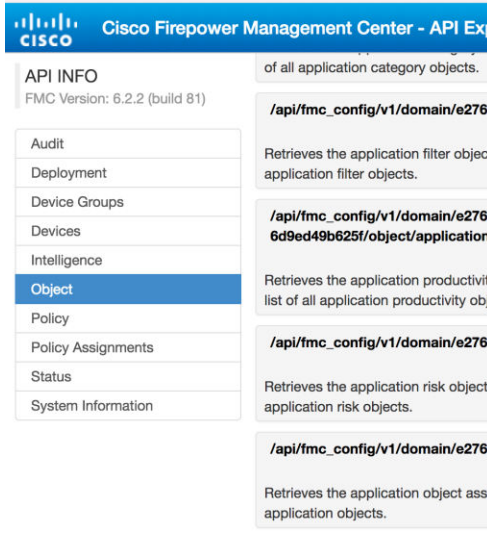
- Выявление, документирование и оптимизация процессов
- Моделирование систем в требуемой среде, разработка НМД
- Облегчение продвижения подхода внутри организации – независимое мнение
- Качественная интеграция разнообразных СЗИ требует экспертных знаний
- Опыт, типовые шаблоны, библиотеки кода – кардинально влияют на сроки
- Инфраструктура для отладки кода и «песочница»
- Поддержка, модификация и адаптация к изменяющимся процессам и процедурам

AMT GROUP

Средства защиты «созрели» - API повсюду

- Времена закрытых СЗИ уходят в прошлое.
- Возможности интеграции через CLI ограничены
- Многие сетевые устройства поддерживают Netconf
- REST API - современные NGFW, NGIPS, SIEM, Anti-APT и т.д
- Возможности
  - Inventory, CRUD, Monitoring, Reporting
- Библиотеки - SDK от производителя,GitHub
- Cisco создала DevNet

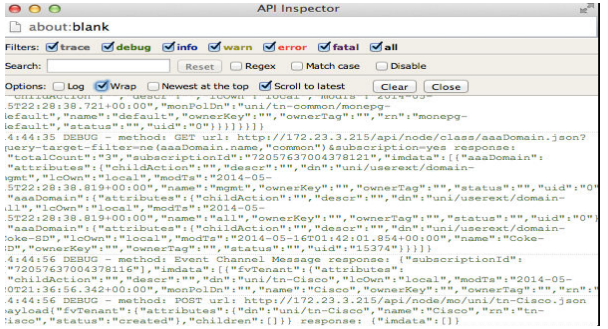




«Бесплатно» можно?

Исторически сложившаяся практика - написанные администратором скрипты

- Python, sh, *.bat…
  - Ручной парсинг (до появления REST API и netconf)
  - Ручная модификация
  - Поддержка и документирование – best effort



Системы управления конфигурациями – модули, библиотеки

- Puppet и Chef (agent)
- Ansible и Ansible Tower (agentless)

А причем здесь Cisco?

- (OpenDayLight & OpenFlow, APIC, pxGrid, VIRL, SandBox, Onbox Scripting)
  - В основном «заточены» под SDN
  - Пакеты для APIC
  - SDK, Python, Github…

AMT GROUP

Нишевые решения

- Автоматизация заранее ограниченного набора задач и процессов ИБ. Но качественно.

- Управление правами доступа – IDM
  - Аванпост, SailPoint, One Identity… (систематизация управления УЗ и правами)

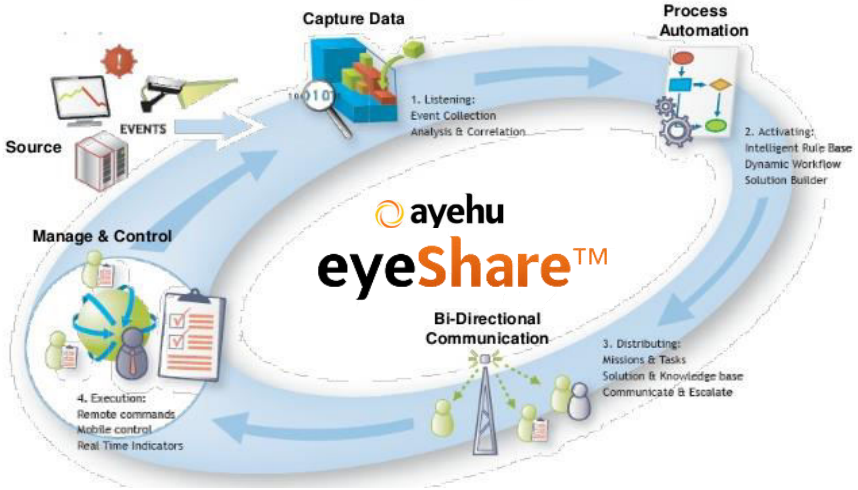
- Управление правилами МСЭ – Firewall Management
  - Algosec, SkyBox, Tufin (+ускорение обработки заявок на изменение)

- Инвентаризация и Управление обновлениями и уязвимостями ПО –
  - MaxPatrol, Ivanti… (идентификация, каталог уязвимостей, контроль)

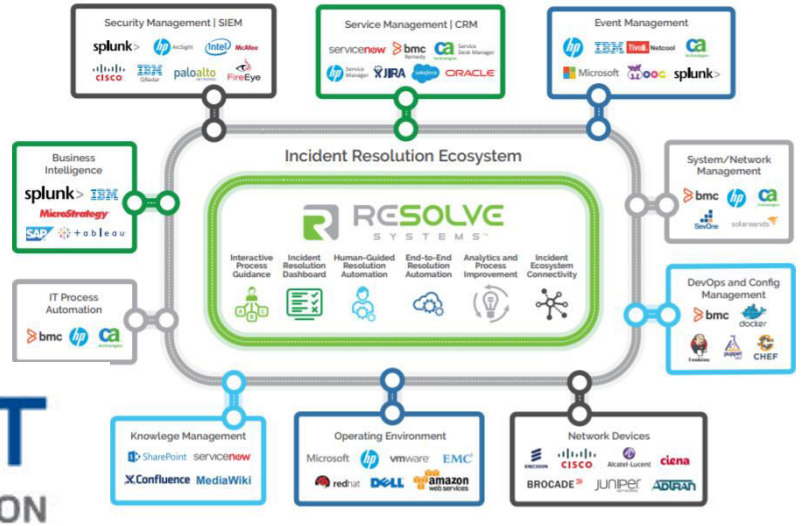
- Управление рисками и организационными процедурами – SGRC системы (автоматизация бумажных процессов, интегральный анализ)

Автоматизация рабочих операций – платформы оркестрации и реагирования

- Изначально задуманы как средства автоматизации широкого применения
- Больше чем Incident/Case Management
- Интеграция с SD, SIEM, BI, KM, Conf/Change Management
- Автоматизация произвольных задач и workflow
- Минимизация написания кода – легко модифицировать
- Быстрая и автоматическая диагностика
- Интерактивное управление процессом реагирования
- Реагирование в режиме «шпаргалка» оператору
- Автоматическое реагирование



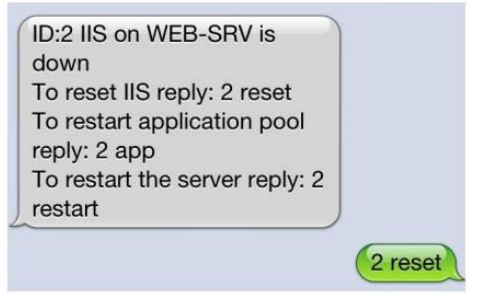
R·Vision
At the root of your security

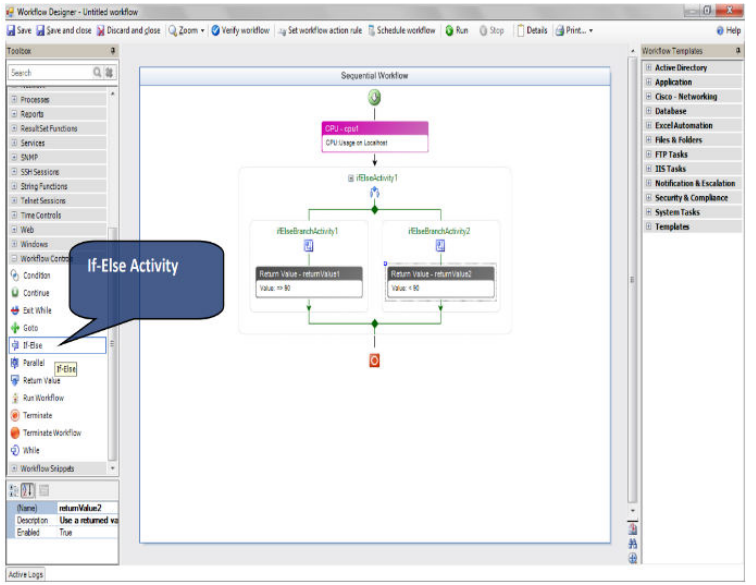


CYBERBIT
PROTECTING A NEW DIMENSION

Универсальные решения. Возможности

- Автоматическое формирование инцидентов на основе данных от SIEM
- Автоматический сбор вспомогательной информации с СЗИ и ИТ-систем
- Выборка сведений из базы знаний
- Оповещение оператора/администратора и автоматическое выполнение действий в зависимости от их решения (IVR, sms, email)
- Блокирование УЗ, портов, подключений, создание сигнатур
- Автоматический сбор данных для расследования
- Предоставление конструктора для сценариев
- Интеграция через API, CLI





Что в итоге?

- Разгрузка дорогостоящих специалистов SOC от рутинных задач
- Снижение «шума» в алертах и концентрация на том, что реально важно
- Возможность справиться с возрастающим объемом задач без расширения штата
- Снижение зависимости от «уникальных» специалистов
- Слаженность работы процессов в ИТ и ИБ
- Реакция на инциденты происходит точнее и быстрее

AMT GROUP

СПАСИБО ЗА ВНИМАНИЕ!