



IT

Центры
обработки
данных

Комплексная
безопасность

ИБ

Прикладные
информационные
системы

Коммуникационные
решения

AMT-ГРУП

Управление сетью МСЭ: быстрее, безопаснее,
эффективнее

Кондратьев Илья, зам. директора ДИБ АМТ-ГРУП

Автоматизация процессов ИБ



- 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

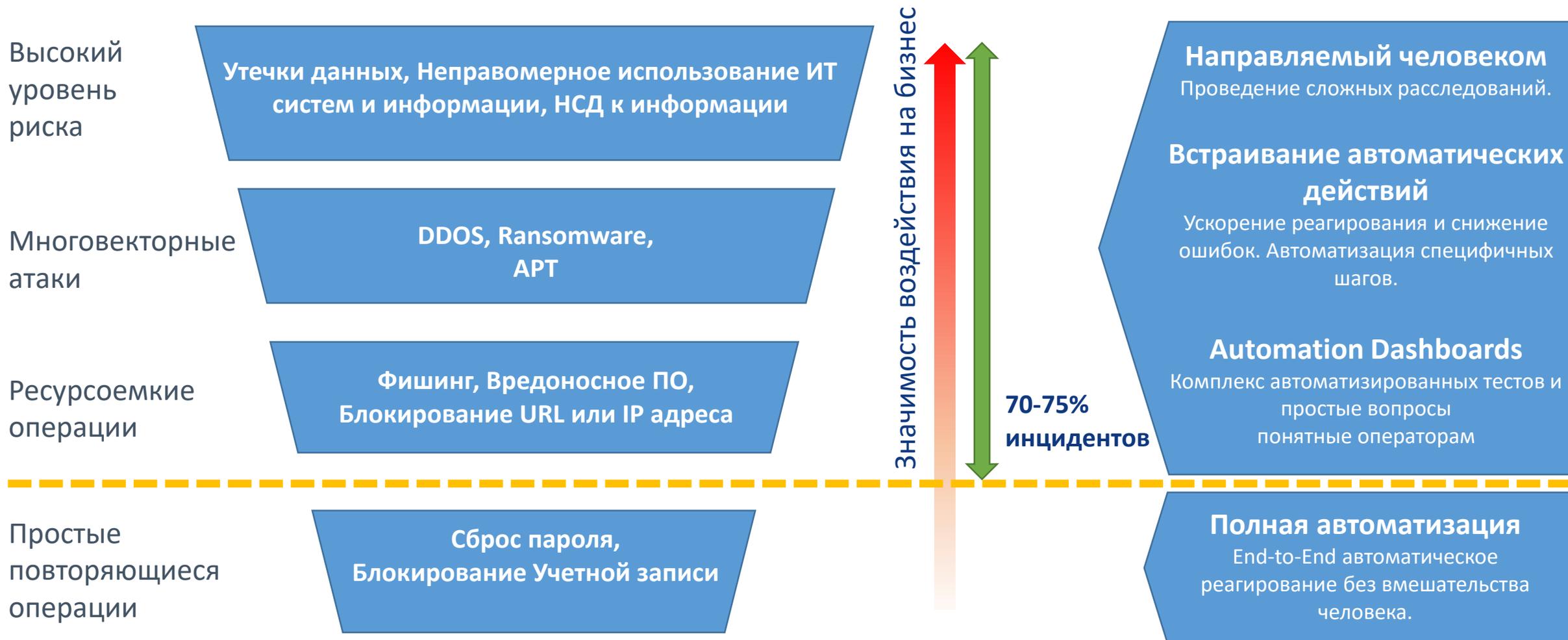
- Чтобы выжить и развиваться организациям нужно повысить скорость в процессах обеспечения ИБ
 - управление правами и доступом
 - управление изменениями
 - инвентаризация и аудит
 - реагирование и расследование
- Дефицит квалифицированных кадров - знание в головах профессионалов (“tribal knowledge”).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

Автоматизация прямо влияет на эффективность

Позволяют справиться со сложными кейсами и быстро адаптироваться

Классы задач/инцидентов ИБ

Уровень применения автоматизации



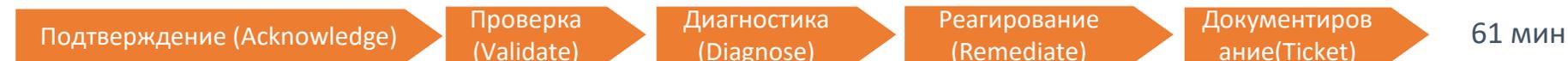
Внедрение поэтапно, эффект сразу

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

Типовое время выполнения операций вручную

Общее MTTR

MTTI = 30 минут



Автомат. подтверждение и проверка



Автомат. подтверждение, проверка и диагностика



Автомат. подтверждение, проверка и диагностика, Реагирование и документирование – направляемое человеком



Полная автоматизация



Цели автоматизации

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

Принципы автоматизации

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

Автоматизируют процессы

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

Что уже автоматизировано

- Сбор и консолидация событий
- Корреляция
- Мониторинг и аналитика

Что для этого нужно?



Консоль АИБ,
оператора



Playbooks, Scripts,
KB



Платформа
автоматизации



- 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 реализующая автоматизируемые функции

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

Автоматизация управления МСЭ



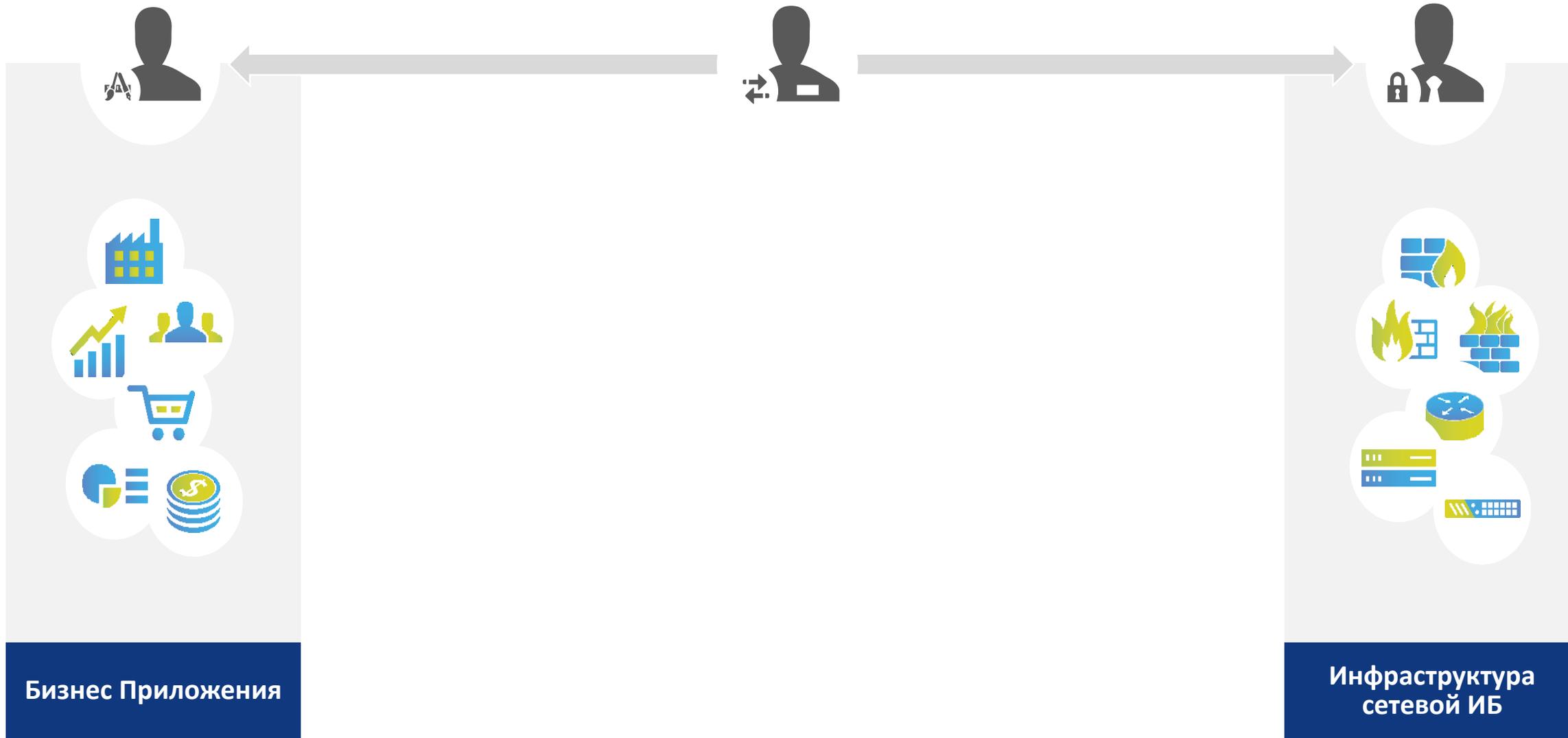
- Маршрутизаторов и МСЭ просто много. Часто от разных производителей
- При объединении сетей требуется анализ и изучение «новой» сети
- Миграция МСЭ других производителей на МСЭ корпоративного стандарта
- «Владельцы» приложений и администраторы говорят на разных языках
- «Безопасное» удаление правил часто непосильная задача
- Ошибки и оцепятки при ручном конфигурировании - усилия и время
- Заявки на открытие доступа выполняются долго (до нескольких недель)
- Compliance – PCI DSS, GDPR и др.
- Многие процессы ИБ опираются на бумажные и ручные процедуры

Управление ИТ/ИБ

Ответственные за
бизнес приложения

ИТ менеджер
Администраторы сети

Ответственные за ИБ



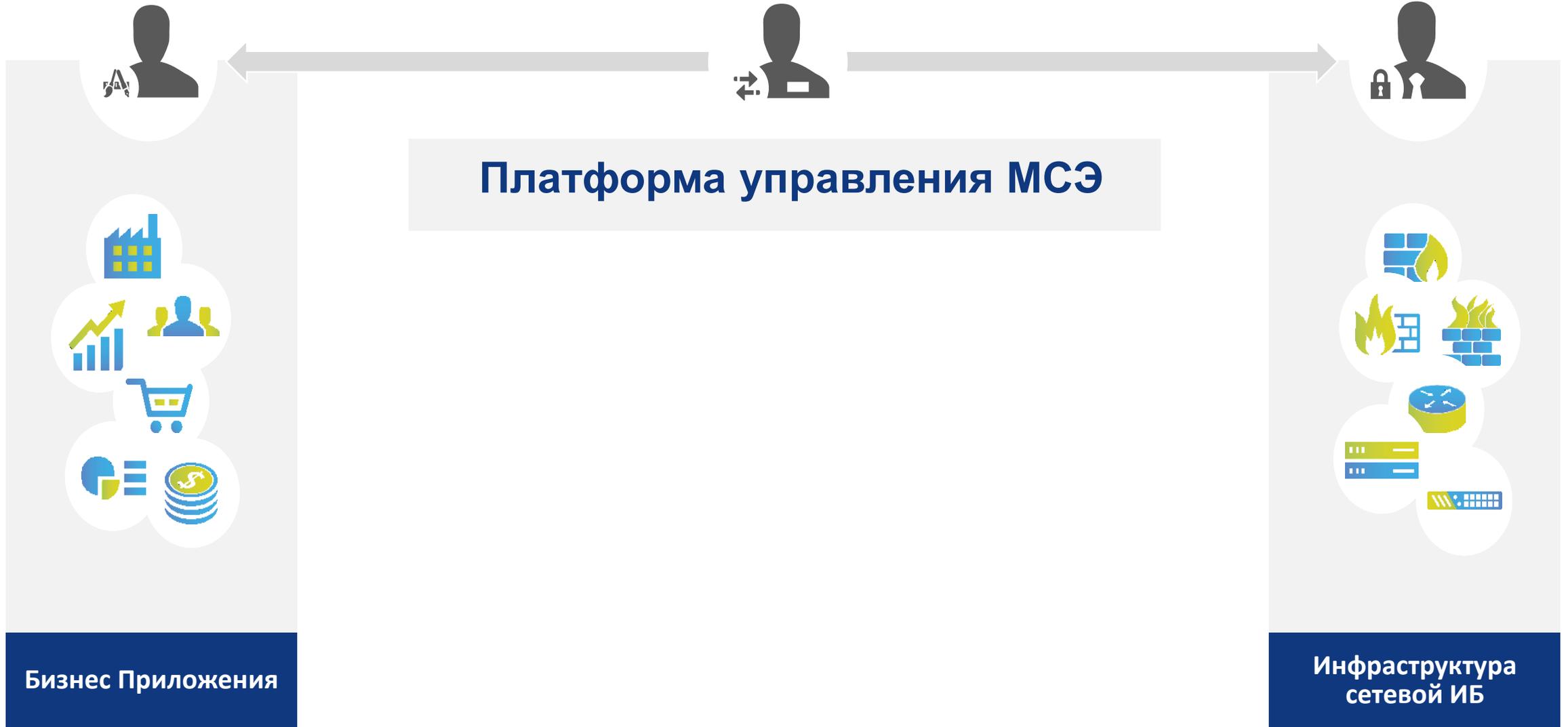
Бизнес Приложения

Инфраструктура
сетевой ИБ

ИТ менеджер
Администраторы сети

Ответственные за
бизнес приложения

Ответственные за ИБ



Бизнес Приложения

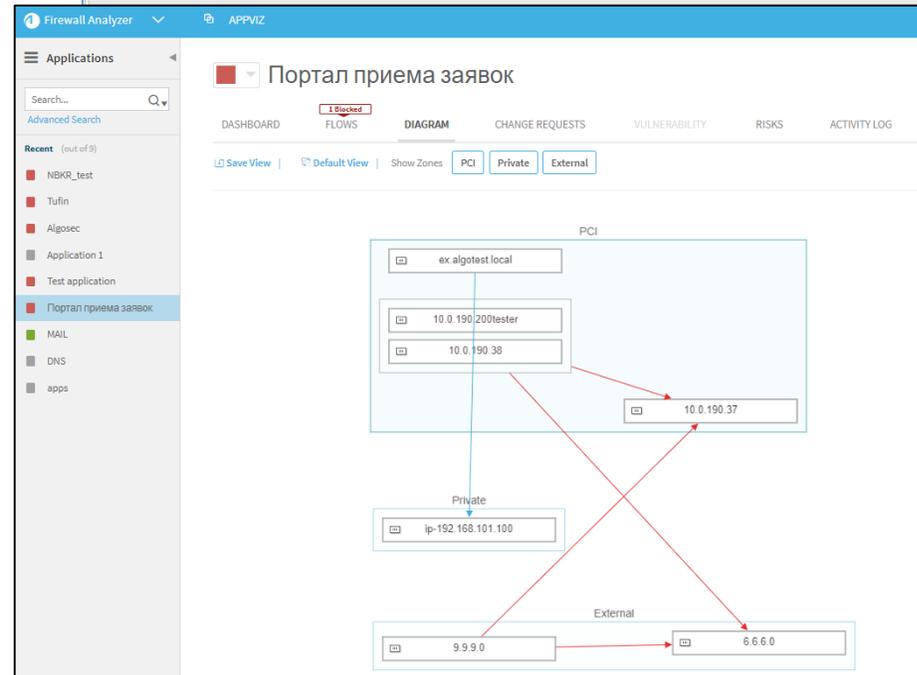
Инфраструктура
сетевой ИБ



Управление взаимосвязью приложений и услуг с правилами фильтрации трафика в МСЭ и роутерах

- Центральная, обновляемая база данных требований бизнес приложений и услуг к сетевым услугам и соединениям, с возможностью углубиться on-line в данные до уровня правила в МСЭ
- Автоматический перевод заявок на подключение услуг и бизнес приложений в технические детали для изменений в МСЭ
- Автоматический расчет влияния изменений топологии и конфигурации СПД на приложение/услугу (к примеру миграция сервера).
- Безопасное удаление правил в МСЭ, в которых нет больше потребности (к примеру в результате вывода приложения из эксплуатации).
- Интеллектуальное соотношение (mapping) правил и политик МСЭ с бизнес услугами и приложениями.
- Полный аудит соединений бизнес-услуг и приложений (connectivity audit trail)

The screenshot displays the Tufin SecureApp interface. The top navigation bar includes 'tufin OrchestrationSuite', 'SecureChange', 'SecureApp', 'Applications', 'Server Lookup', and 'Cloud Console'. The main content area is titled 'APPLICATIONS → Active Directory' and shows a 'Connectivity' view. It features a table with columns for 'Source', 'Service/Application Identity', 'Destination', and 'Comment'. Two connectivity entries are visible: 'Access 01 (Access to Sales)' and 'Access from Toronto (Application 210 - File Transfer)'. The 'Access 01' entry shows a source of 'h_172.16.40.50 (Access...)' with 'Toronto Users*' and a destination of 'sales_192.168.2.50 (Ac...)' and 'sales_192.168.2.60 (Ac...)' via 'https' and 'ssh' protocols. The 'Access from Toronto' entry shows a source of 'Toronto Users*' and a destination of 'f_172.16.30.98 (Applic...)' and 'f_172.16.30.99 (Applic...)' via 'ftp' protocol. A 'Resources' sidebar on the right lists various servers and services, including 'db01_10.200.1.235', 'Finance_*', and 'Finance_192.168.50.100' through '104'. A 'Create Ticket' button is visible in the top right.



Управление ИТ/ИБ – Algosec AppViz | Tufin SecureApp

Firewall Analyzer APPVIZ

Портал приема заявок

1 Blocked FLOWS

Export to CSV

Application Flows

Name	Source	Destination	Service
1	10.0.190.200tester 10.0.190.38 9.9.9.0	10.0.190.37 6.6.6.0	Any
Telnet	ex.algotest.local	ip-192.168.101.100	http telnet

- Анализ рисков до модификации правил
- Интеграция с тикетинговой системой
- Учет и автоматизация зависимостей
- Миграция серверов упрощается

Traffic Simulation Results

Blocked Apr 05, 2021 | 17:55:37

Requested Traffic

SOURCE	USER	DESTINATION	APPLICATION
192.168.111.100	Any	10.0.187.49	Any

Devices in Path (4)

VIEW BY: Status

MAP

DETAILS

BLOCKING (1)

- VR-192_168_112_5-default

ALLOWING (3)

- ASAS520_admin
- VR-192_168_110_2-ALG_R2
- ASAS510_admin

Network topology diagram showing devices: 10_0_187_129_root, 10_0_187_19_ALG_R1, 192.168.103.0/24, VR-192_168_110_2-ALG_R2, 192.168.111.0/24, 10.0.187.0/24, 192.168.102.0/24, ASAS10_admin, 192.168.113.0/24, SAS520_admin, 192.168.112.0/24, VR-192_168_112_5-default.

- Автоматическая проверка достижимости
- Учет уязвимостей на серверах
- Описание трафика приложения/сервиса отдельно от сетевой топологии

Connection Analysis | Access to Sales: Access 01

Devices

- RTR4
- RTR1
- San Fran (Palo Alto FW) (San Francisco DG)
- SMCPM (CP SMC)
- ASAv
- Pe_1
- Pe_2

ASAv

- Revision: 140
- Action: automatic
- Administrator:
- Date: Mon, 6 Apr 2020
- Date on Device: Mon, 6 Apr 2020
- Installed on:
- GUI Client: -
- Audit Log: -
- Policy Package: Standard
- Global Policy:
- Ticket ID:

Notes:

- This query uses Topology Intelligence to show all of the possible paths of traffic that are relevant to the selected policies.
- All queries use the latest Topology information, even for historical queries.
- The result contains one or more 'Partially Shadowed' rules.

Interface Datacenter, direction out

Datacenter_access_out

#	Shadowing	Action	Source Host/Network	Destination Host/Network	ACL	Service	Log Level Interval	Description
29		✓	172.16.40.50	NetworkGroup_24	Datacenter_access_out	ServiceGroup_17		
51	Partially Shadowed	✗	any	any	Datacenter_access_out	ip		

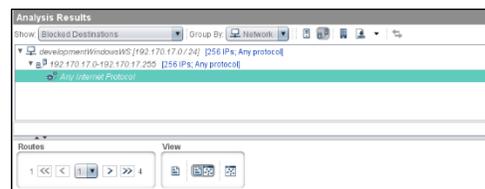
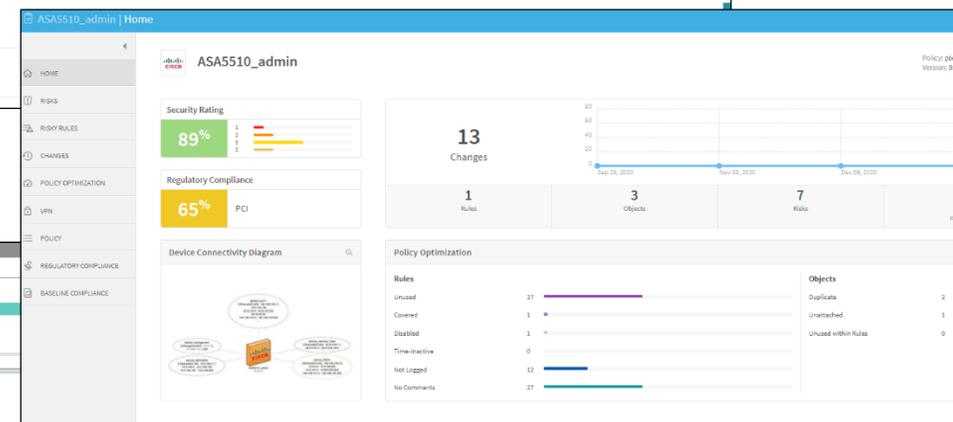
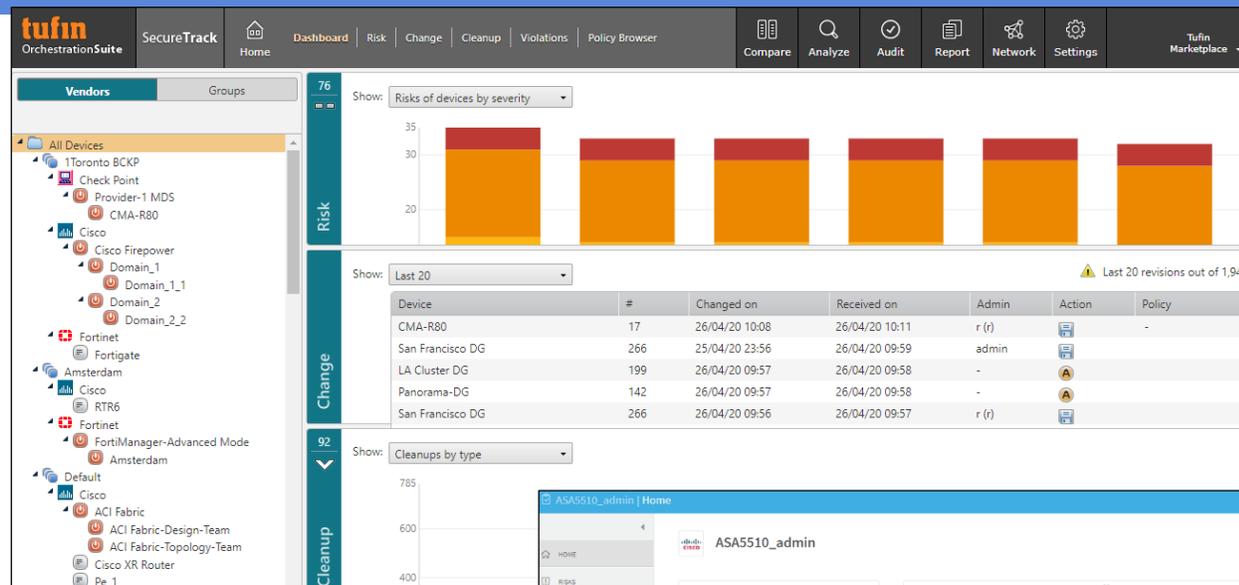




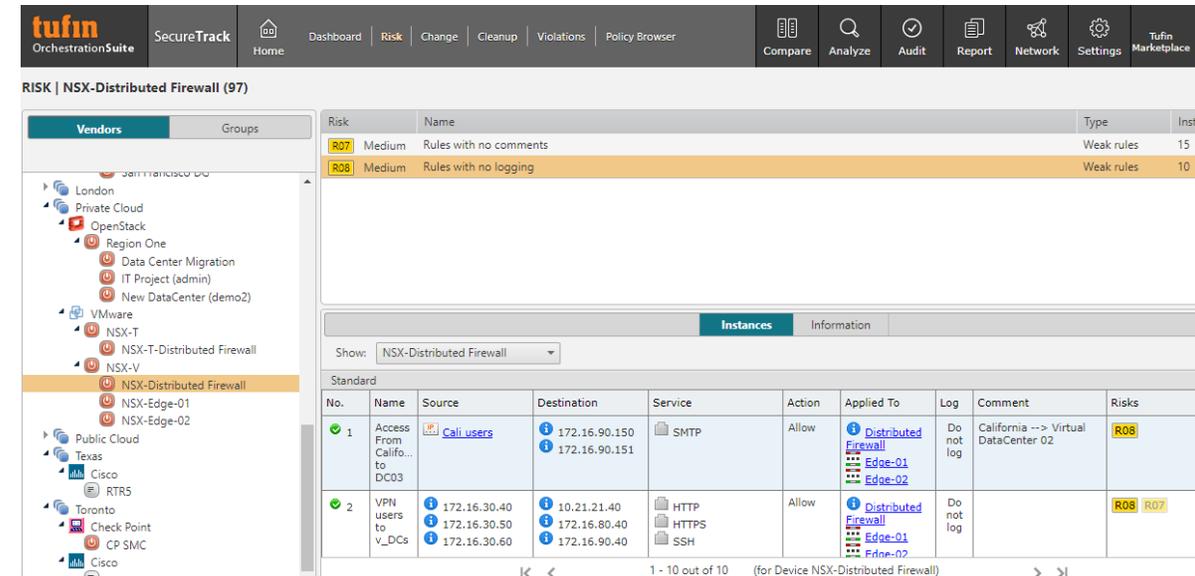
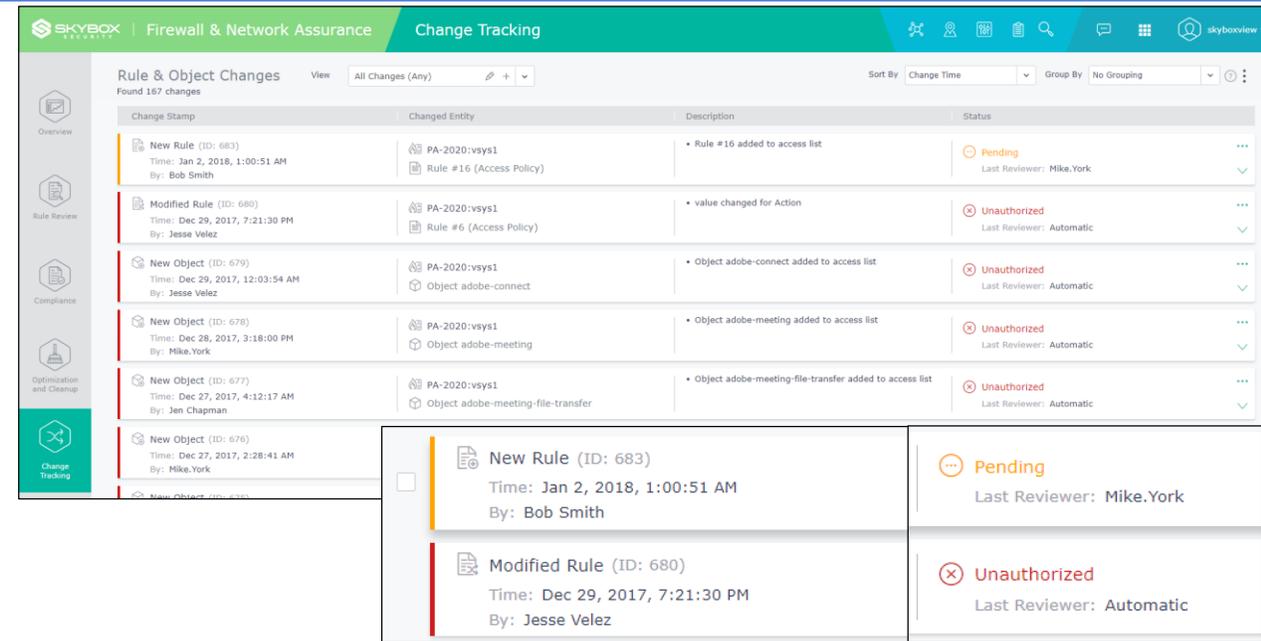
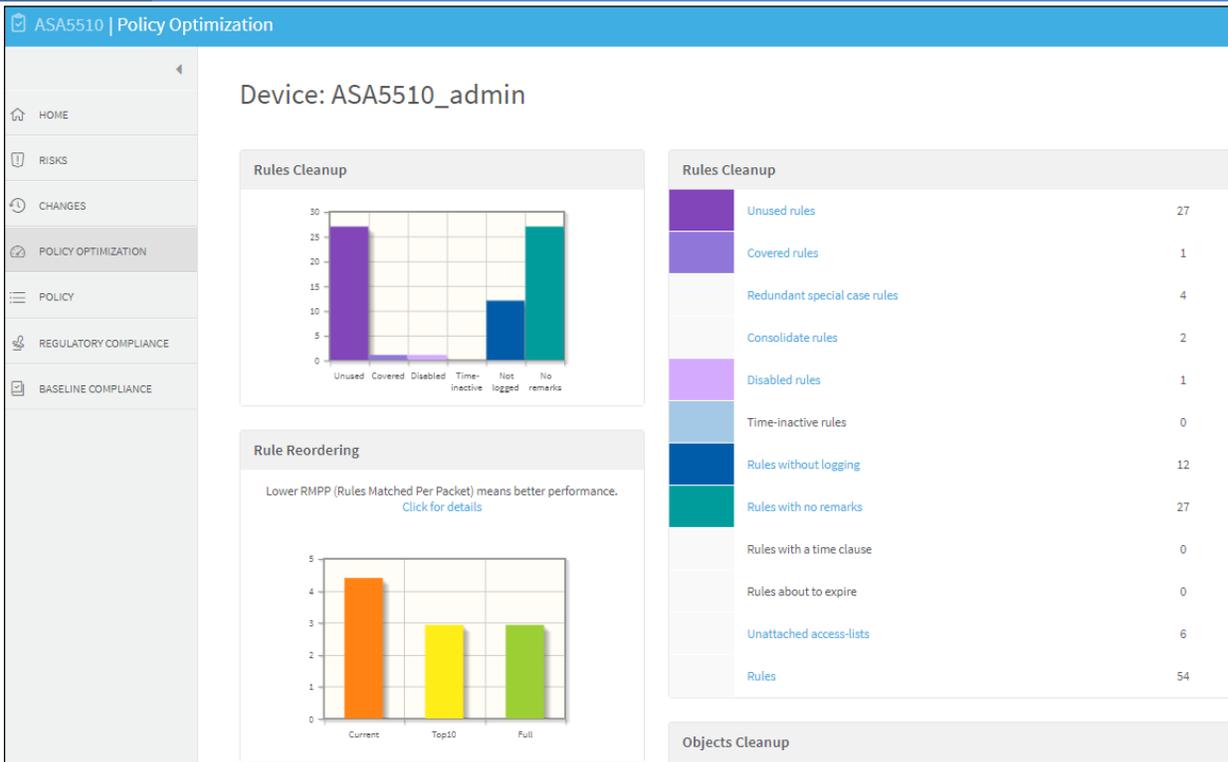


Интеллектуальный анализ политики и правил ИБ

- Определение и анализ топологии сети и зон ИБ (сегментация)
- Контроль изменений политик и правил МСЭ
- Анализ достижимости (Simulation)
- Анализ рисков
- Проверка соответствия требованиям стандартов
- Автоматический сбор и анализ конфигураций («зоопарк» приветствуется)



Управление ИБ – анализ рисков, аудит, оптимизация



- Выявление несанкционированных изменений
- «Чистка» и оптимизация политик и правил МСЭ
- Анализ рисков с учетом уязвимостей на серверах
- Compliance
- Контроль базовой конфигурации МСЭ и устройств ИБ
- Документирование правил – единая база

ИТ менеджер

Ответственные за
бизнес приложения

Администраторы сети

Ответственные за ИБ



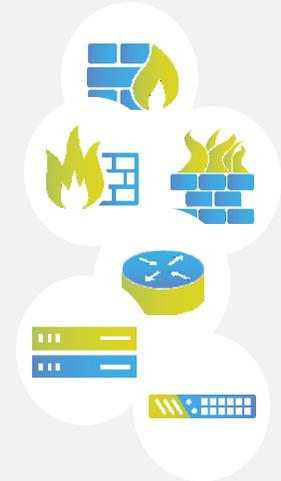
Платформа управления МСЭ



AppViz | SecureApp



Assurance | Analyzer | Secure Track



Бизнес Приложения

Инфраструктура
сетевой ИБ

ИТ менеджер

Ответственные за бизнес приложения

Администраторы сети

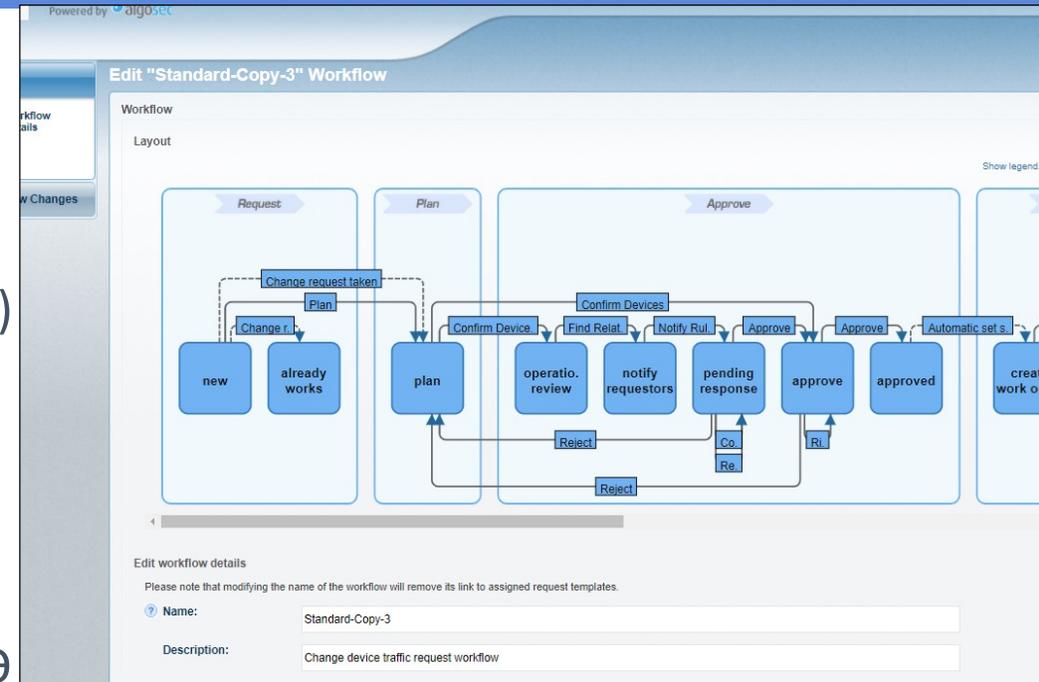
Ответственные за ИБ





Интеллектуальная автоматизация управления изменениями в МСЭ и устройствах ИБ

- Кастомизируемые автоматические процессы работ (workflows)
- Интеллектуальная симуляция и анализ влияния исполнения заявки на работу сети и элементов ИБ
- Проактивная проверка влияния изменений на риски и соответствие стандартам
- Автоматическая установка изменений политик и правил в МСЭ
- Полный аудит изменений в устройствах ИБ
- Контроль качества выполнения заявок/заказов (SLA)
- Интеграция с существующими системами (BMC, HP, CA)



Implement Changes

ID	Chang...	Firewall	Object...	Change Details	Implementation Det...	Object / Rule Comment
524	New ...	dev FW	Service...	Service Object: 8080/TCP		5/11/18 - Created by skybox...
523	New ...	dev FW	Service...	Service Object: 23/TCP		5/11/18 - Created by skybox...
522	New ...	dev FW	Host_...	Address Object: 192.170.19.21		5/11/18 - Created by skybox...
521	New ...	dev FW	Host_...	Address Object: 200.200.200.200		5/11/18 - Created by skybox...
517	Add R...	dev FW	-	Source: Host_200.200.200.200 Destination: Host_192.170.19.21 Services: Service_23_TCP, Service_8080...	Policy: Standard Rule Position: Last Rule Track: Log	5/11/18 - Created by skybox...

Workflow properties: Workflow SLA, Workflow status: Active

Steps: 1. Enter your request, 2. Business approval, 3. Identify targets and risks, 4. Risk review and approval (escalation), 5. Technical Design & Implementation, 6. Technical Design - Commitment, 7. Auto Verification

Step status: Active

- 40 - 50% существующих правил на МСЭ можно удалить (в среднем)
- 20 % заявок не требуют внесения изменений
- Продление жизни существующим МСЭ – до 20%.
- До 80% снижения в трудоемкости подготовки и проведения аудита МСЭ
- Настройки ИБ производятся в 2-4 быстрее
- Проверка наличия доступа в большой сети занимает секунды
- Схема L3 топологии сети поддерживается автоматически - всегда актуальна
- Правила фильтрации соответствуют запрошенным доступам
- Повышение устойчивости к кибератакам благодаря более правильным настройкам МСЭ

Реальный кейс

Российский холдинг: >200 МСЭ и >1000 сетевых L3-устройств

Сотни криптографических шлюзов

Правила МСЭ часто добавляются и практически не удаляются

Документация правил слабая, единая карта сети отсутствует

Заявки на изменения в правила МСЭ выполняются до 2 недель

Процесс управления изменениями в явном виде не документирован

Тысячи приложений и ИТ-сервисов

Аудит правил МСЭ занимает месяцы и поэтому теряет смысл



Реальный кейс. Продолжение

Процесс управления изменениями на МСЭ документирован и адаптирован с учетом средств автоматизации

>40% правил МСЭ могут быть перекрываются и могут быть удалены

Около 20 % заявок на сетевой доступ не требуют выполнения

Время внесения изменений сокращается на 50%. Проверка изменений автоматизирована

SOC получил инструмент для оценки достижимости ИТ-активов с зараженных хостов

Владельцы ИТ-систем получили инструмент для моделирования изменений и упрощения миграции между площадками

Отечественные криптошлюзы подключены к системе для полноты сетевой карты. Выявлен ряд ошибок маршрутизации

Аудит правил МСЭ проводится автоматически



СПАСИБО ЗА ВНИМАНИЕ!