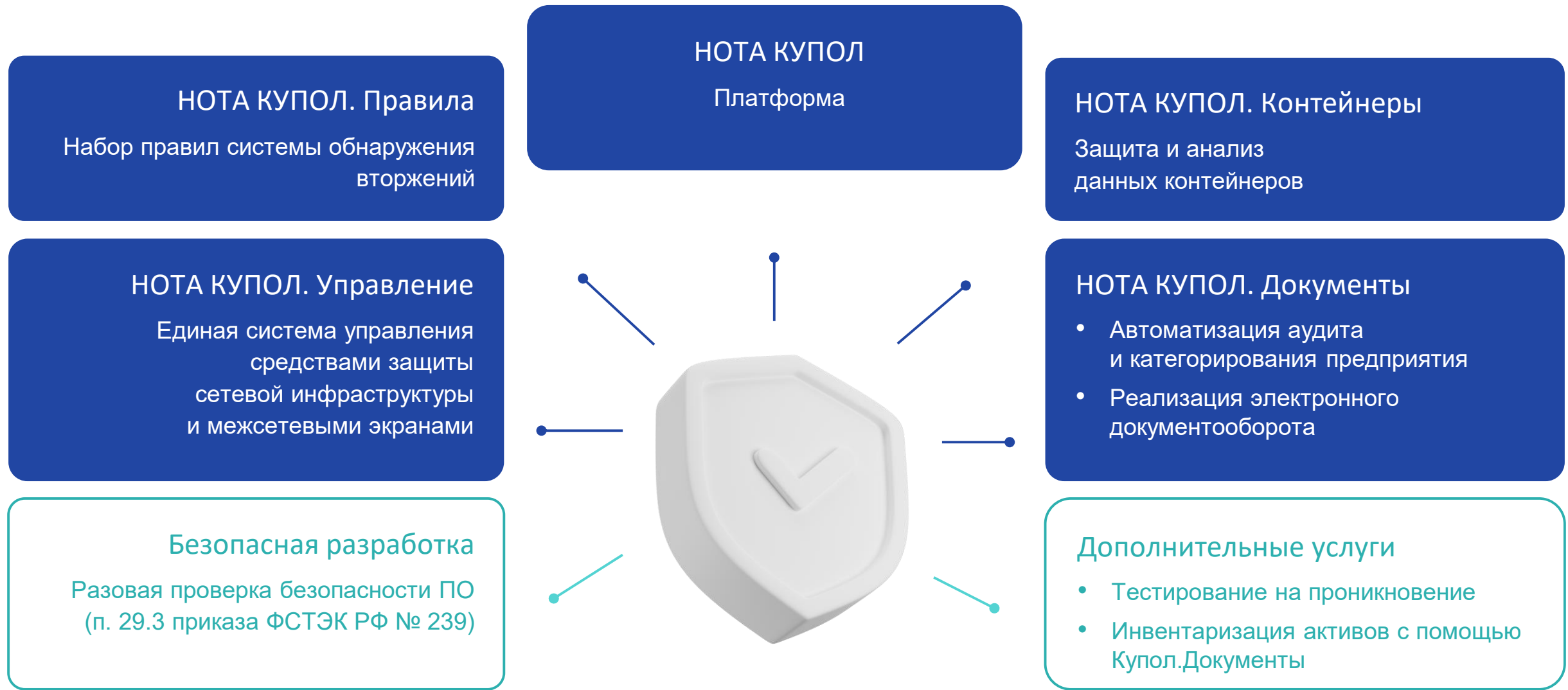


НСТС | КУПОЛ

Новая экосистема
продуктов и услуг
по информационной
безопасности

3 апреля
2024





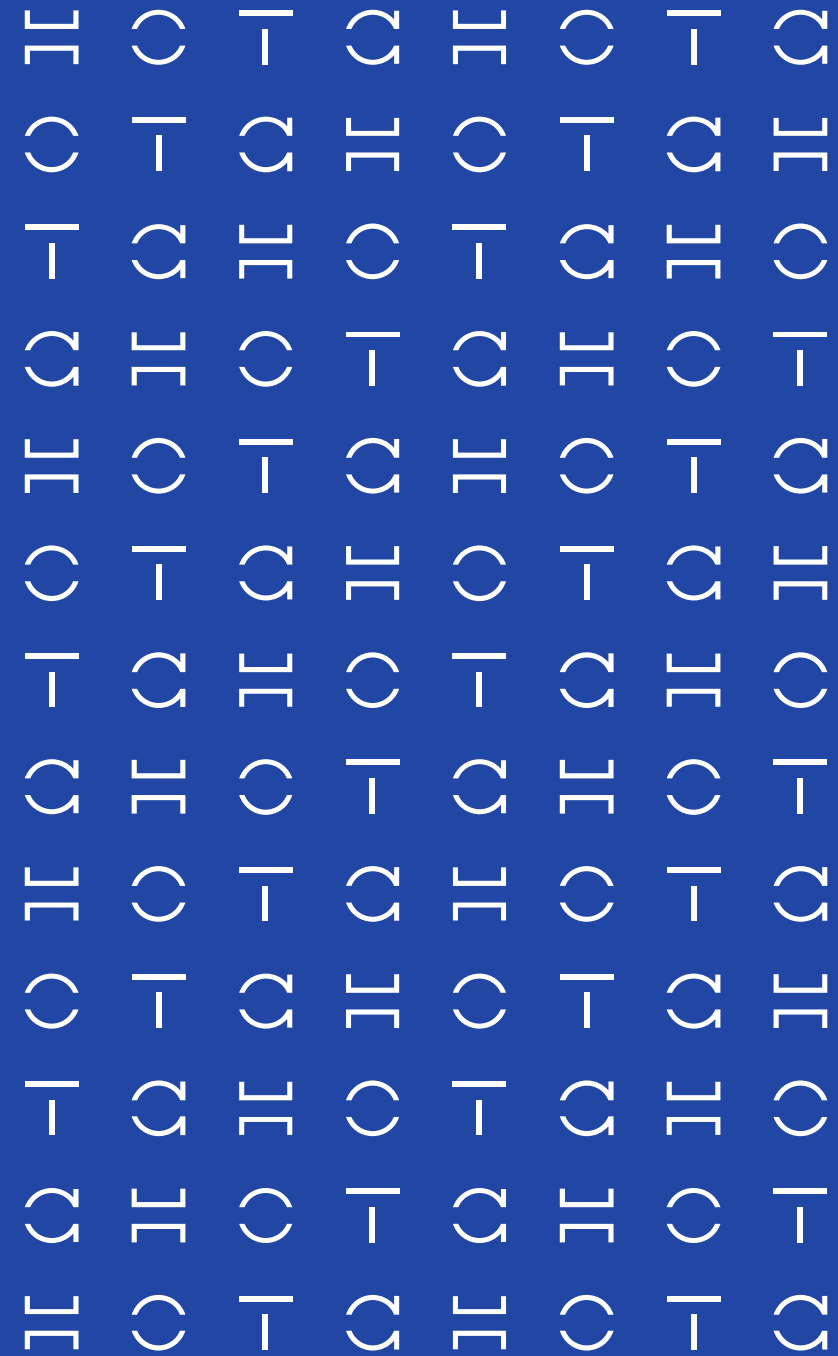
Н С Т С | КУПОЛ

НОТА КУПОЛ. УПРАВЛЕНИЕ

+ | Т1

НОТА КУПОЛ. УПРАВЛЕНИЕ

Единый мультивендорный центр аналитики и управления сетевыми устройствами, имеющий функции создания и применения политик безопасности



ОСНОВНЫЕ ПРОБЛЕМЫ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ



Оптимизация политик

Как эффективно анализировать и оптимизировать политики безопасности?



Уход иностранных вендоров

Какую замену выбрать?



Мониторинг и контроль

Как контролировать состояние подключенных устройств?



Обновление

Как правильно обновить версию продукта и продлить лицензии?



Мультивендорная реализация

Как интегрировать решения разных вендоров в систему управления?



Безопасность

Как обеспечить безопасность обмена данными и управления?



Совместимость

Как установить систему и интегрировать её в существующую инфраструктуру?



Ограничение прав

Как ограничить права доступа и контролировать систему и подключенные устройства?

Единый мультивендорный центр управления межсетевыми экранами и NGFW



Ценность для клиента

- Ускорение и унификация настройки из единого интерфейса NGFW всех вендоров, установленных в инфраструктуре компании (политик безопасности, доступа и др.)
- Видимость всех устройств в сети компании и своевременное нахождение неисправного устройства
- Полная видимость изменений политик на устройствах и возможность быстро найти устройство, политики которого нарушили какие-либо бизнес-процессы компании
- Оптимально настроенные политики безопасности во всей инфраструктуре и отсутствие излишних политик, снижающих пропускную способность сети компании
- Уменьшение количества закупаемых новых устройств за счёт оптимизации политик

Функции



Мониторинг состояния всех установленных МЭ

Отслеживание состояния подключённых МЭ, кластера, загрузки ЦП и памяти, трафика и другой информации



Контроль и управление конфигурациями

Отслеживание всех изменений конфигураций. Раскатка конфигурации на схожие устройства



Уведомления по необходимым событиям

Гибкие настройки уведомлений о состоянии устройства, изменении конфигураций, политик и событий безопасности



Управление политиками безопасности

Создание и изменение политик: МЭ, COB, AppControl, URL-фильтрации. Оценка риска изменения политики. Раскатка политики на несколько устройств



Оптимизация политик на всех устройствах

Обнаружение «теневых», дублирующих и излишних политик в контексте сети предприятия, рекомендации по оптимизации, в том числе в контексте 1 устройства



Аудит и соответствие политик. Отчётность

Создание глобальной политики безопасности сети компании, с учётом требований надзор и госорганов. Аудит всех политик на соответствие, получение отчёта

ИНТЕГРАЦИЯ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ



Единая система для анализ и управления

FORTINET

UserGate

CHECK POINT

CISCO

КОД
безопасности

РЕЛИЗ
Q2 2024

ViPNet

ИНТЕГРАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ РАЗЛИЧНЫХ ВЕНДОРОВ

The screenshot displays a web-based network management interface. At the top, there is a navigation bar with the title 'Подключение и мониторинг доступности МЭ' and a user profile 'Святослав'. Below this, a summary section shows 'Список устройств' with 6 connected, 4 disconnected, and 0 reloading devices. The main area features a table of devices with columns for Name, Status, IP address, Vendor, and Responsible. The 'UG2602' device is selected. A context menu is open over the 'Ответственный' column, showing options like 'Настройки устройства', 'Перезагрузить', 'Клонировать конфигурацию', and 'Удалить'. A sidebar on the left contains navigation links for 'Управление', 'Рабочий стол', 'Список устройств', 'Конфигурации', 'Анализ политик', and 'Администратор'. A blue callout box at the bottom right highlights the 'Клонирование и перенос конфигураций' feature.

Главная > Список устройств

Подключение и мониторинг доступности МЭ

Святослав

Список устройств

Подключены 6 | Отключены 4 | Перезагрузка 0

Управление

Рабочий стол

Список устройств

Конфигурации

Анализ политик

Администратор

Список устройств

Управление ответственными за устройства

+ Добавить

Название	Статус	IP-адрес	Вендор	Ответственный
Fortigate_test	Подключен	fortigate.fortidemo.com	Fortigate	test@test.ru
CheckPoint1	Подключен	172.31.142.120	CheckPoint	Иванов Дмитрий Кузьмин Владимир
Cisco ASA	Подключен	172.31.142.14	Cisco	Иванов Дмитрий Кузьмин Владимир
<input checked="" type="checkbox"/> UG2602	Подключен	10.229.0.74	UserGate	Андрей test@test.ru Святослав
UserGate	Подключен	172.31.142.126	UserGate	

- Настройки устройства
- Перезагрузить
- Клонировать конфигурацию
- Удалить
- Настройка столбцов

ФИЛЬТРЫ

- Без фильтра
- Сохранить фильтр

Клонирование и перенос конфигураций

АНАЛИЗ ПОЛИТИК БЕЗОПАСНОСТИ

☰ | КУПОЛ
Управление

🏠 Рабочий стол
🗃️ Список устройств
⚙️ Конфигурации
🔍 Анализ политик
👤 Администратор

Главная > Анализ политик > Сводка 👤 Святослав

Анализ политик

Сводка Оптимизация Очистка

Выбор устройства: UG2602 10.229.0.74 # Всего правил: 12

Получите наглядное представление обо всех правилах, прописанных в брандмауэре

Запрещающие правила	4	<div style="width: 25%;"></div>
Разрешающие правила	8	<div style="width: 50%;"></div>
Входящие правила брандмауэра	0	<div style="width: 0%;"></div>
Исходящие правила брандмауэра	0	<div style="width: 0%;"></div>
Отключенные правила	8	<div style="width: 66.6%;"></div>
Правила с отключённым логированием	7	<div style="width: 58.3%;"></div>
Разрешенные ANY-ANY правила	7	<div style="width: 58.3%;"></div>
Правила, разрешающие трафик любого сервиса без ограничений	6	<div style="width: 50%;"></div>
Двунаправленные правила	0	<div style="width: 0%;"></div>

Анализ политик безопасности межсетевых экранов

Политики Отключенные правила x

№	Название	Действие	Зона источника	Включено	Адрес источника	Зона назначения
2	Block from botnets	❌ Запретить		<input type="checkbox"/>	Iran, Islamic Republ... Iceland Latvia Holy See (Vatican C... Slovakia Georgia Kazakhstan Estonia Croatia Moldova, Republic of Mexico Saudi Arabia Malta Hungary Bermuda	
3	Allow trusted to untrusted	✅ Разрешить	Trusted	<input type="checkbox"/>		Untrusted
4	Block to botnets	❌ Запретить	Trusted	<input type="checkbox"/>	BAD_SEARCH_BLA... ENTENSYS_KAZ_B...	Untrusted
5	Allow from DMZ to Untrusted	✅ Разрешить	DMZ	<input type="checkbox"/>		Untrusted
6	VPN for Site-to-Site to Trusted and Untrusted	✅ Разрешить	VPN for Site-to-Site	<input type="checkbox"/>		Untrusted Trusted

Категорирование результатов анализа

РЕКОМЕНДАЦИИ ПО ОПТИМИЗАЦИИ

☰ | КУПОЛ
Управление

- Рабочий стол
- Список устройств
- Анализ политик**
- Сканер уязвимостей
- Администратор

Анализ политик > Переупорядочивание 🔔 👤 Смирнов

Анализ политик

Обзор Оптимизация Очистка Сравнение **Переупорядочивание** Временные правила

Выбор устройства: Firewall 1 192.168.1.1 | Период: 08.03.2024 00:00 - 15.03.2024 00:00 | Анализ политик от 27.03.2024 09:26:00 [Обновить](#)

В результате анализа частоты срабатывания правил за определенный период система предлагает вам изменить порядок правил для повышения производительности брандмауэра

Правила

<input type="checkbox"/>	№	Название	Рекомендация смены порядка	Кол-во срабатываний	Эффективность
<input type="checkbox"/>	6	Блокировать доступ network1	↑ 5	412	78%
<input type="checkbox"/>	11	Блокировать доступ network1	↑ 9	21	26%
<input type="checkbox"/>	12	Блокировать доступ network1	↑		

Список устройств > Firewall 1 > Межсетевой экран

Firewall 1 Статус: Подключен IP-адрес: 192.168.1.1

🔔 **Рекомендуется перенести на ↑ 5 позицию**
В результате анализа частоты срабатывания правил система предлагает вам переместить выбранное правило на 5 позицию

- Политики
- Межсетевой экран**
- IPv6 доступ
- Подраздел
- Подраздел
- Правила авторизации
- Подраздел
- Подраздел

Межсетевой экран

<input type="checkbox"/>	№	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Включено
<input type="checkbox"/>	1	Блокировать доступ network1	❌ Запретить	Network6	WTC dms server	Network6	WTC dms server	🔴
<input type="checkbox"/>	2	Блокировать доступ network1	✅ Разрешить	Network6	Network6	Network6	Network6	🟢
<input type="checkbox"/>	3	Блокировать доступ network1	✅ Разрешить	Network6	Network6	Network6	Network6	🟢
<input type="checkbox"/>	4	Блокировать доступ network1	✅ Разрешить	Network6	Network6	Network6	WTC dms server	🟢

СРАВНЕНИЕ КОНФИГУРАЦИЙ (Q2 2024)

☰ | КУПОЛ
Управление

Рабочий стол
Список устройств
Конфигурации
Анализ политик
Сканер уязвимостей

Администратор

Устройства

Конфигурации

Резервные копии Избранное **Сравнение** Отслеживание изменений

Выбрать сохраненные конфигурации
 Загрузить файлы
 Конфигурация и файл

Устройство 1
Firewall 1 192.168.1.1

Конфигурация 1
Текущая конфигурация

Устройство 2
Firewall 1 192.168.1.1

Конфигурация 2
config2 25.10.2021, 12:48

Сравнить

Сравнение правил **+** 2 **✎** 16 **✖** 7 Показывать только отличия [↑ Экспорт](#)

Конфигурация 2				Конфигурация 1	
№	ID	Правило	Сравнение	ID	Правило
1			+ Добавлено	722	Блокировать доступ network1
2			+ Добавлено	161	Блокировать доступ network1
3	46	Блокировать доступ network1		46	Блокировать доступ network1
4	725	Блокировать доступ network1	✎ Изменено	725	Блокировать доступ network1
	126	Блокировать доступ network1	✖ Удалено		
5	51	Блокировать доступ network1		51	Блокировать доступ network1
	414	Блокировать доступ network1	✖ Удалено		
	61	Блокировать доступ network1	✖ Удалено		
6	53	Блокировать доступ network1		53	Блокировать доступ network1
7	423	Блокировать доступ network1		423	Блокировать доступ network1

ПРОВЕРКА УЯЗВИМОСТЕЙ МЭ (Q2 2024)

☰ | КУПОЛ
Управление

Рабочий стол
Список устройств
Анализ политик
Уязвимости
Администратор

Список устройств 🔔 👤 Смирнов

Уязвимости ☰ Купол.Сети | ⚠️ Уязвимости 7 351 🟡 +124 🔍 18 | База уязвимостей от 25 мар 2023г 🔄

Список уязвимостей Все 25 68 125 6 616 Показать только изменения

Название	Уровень ↑	Источник	Дата обновления	Устройства
● Переход в режим CVT	10	CVE	📅 15 мар 2023, 15:43	📄 24
Выход за пределы контура	10	CERT	📅 15 мар 2023, 15:43	📄 156
Прекращение или нарушение функционирования...	10	CERT	📅 15 мар 2023, 15:43	📄 12
Переход в режим CVT	9,5	CERT	📅 15 мар 2023, 15:43	📄 22
● Множественная уязвимость доступа	8	JSA	📅 15 мар 2023, 15:43	📄 70
● Переход в режим CVT	7,7	CVE	📅 15 мар 2023, 15:43	📄 46
Множественная уязвимость доступа	6	BID	📅 15 мар 2023, 15:43	📄 11
🔍 Ошибка протокола авторизации	5,1	INTEL	📅 15 мар 2023, 15:43	📄 515
Выход за пределы контура	4	JSA	📅 15 мар 2023, 15:43	📄 44
Переход в режим CVT	4	JSA	📅 15 мар 2023, 15:43	📄 1 254

Найдено записей: 47 « < 1 из 5 > » 10 ▾

ПРИМЕР РЕШЕНИЯ ПРОБЛЕМ

Предприятие с ~110 межсетевыми экранами 4 различных производителей

Проблема клиент до внедрения продукта



Обслуживание межсетевых экранов

Обслуживание межсетевых экранов осуществлялось 2 специалистами (блок ИТ), тем не менее, ввиду импортозамещения и наличие у каждого производителя своего центра управления- время на контроль и настройку значительно увеличивалось



Отсутствуют решения, которые работают с российскими межсетевыми экранами

Рынок российских решений, которые будут поддерживать российские МЭ очень скудный. А также требуется поддержка специфичных межсетевых экранов.



Сложность в анализе правил МЭ

Наличие на каждом из МЭ по 50-100 тысяч правил, что значительно снижает производительность сетевых средств защиты, На анализ которых у персонала просто нет времени.

Результат внедрения продукта



Единый центр управления

У заказчика появилась возможность не только управлять всеми межсетевыми экранами, но и проводить перенос настройки из одной группы МЭ в другую.



Поддержка любого производителя

Решение из коробки поддерживала 3 производителя заказчика, в течении пилотного проекта был освоен и подключен 4, финальный производитель, который использовался у заказчика. В дорожную карту также были заложены 2 производителя, которые в перспективе заменят оставшихся западных производителя.



Оптимизация политик МЭ

Были выявлены аномалии в настройках политик подключенных МЭ, что позволило снизить количество правил до 30 тысяч правил и увеличить производительность сетевых средств защиты.

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА НОТА КУПОЛ. УПРАВЛЕНИЕ



Централизованное мультивендорное управление правилами МЭ, подключенных устройств



15 категорий анализа правил МЭ устройств различных вендоров и формирование рекомендаций по их оптимизации



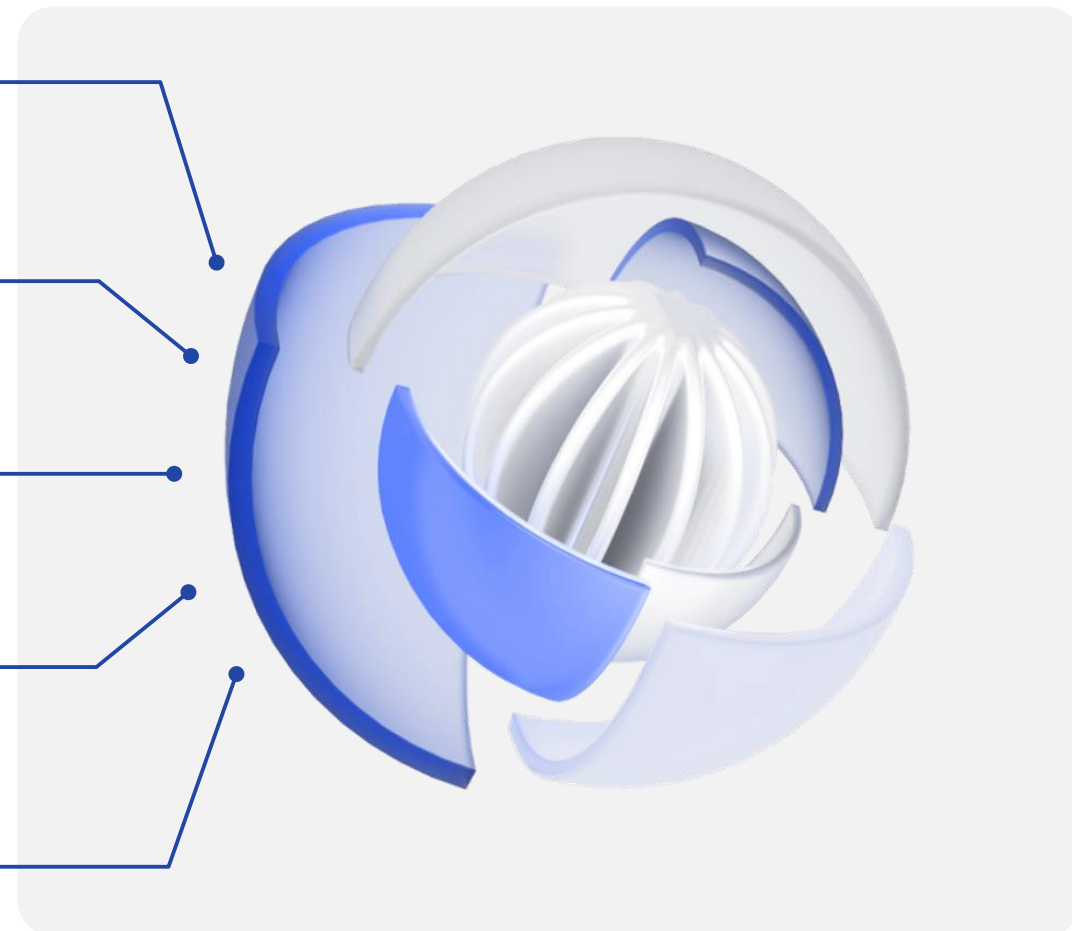
Автоэкапирование конфигураций подключенных устройств и возможность их клонирования на другие устройства вендора



Предоставление доступа в систему пользователям каталога Astra Linux Directory



Возможность назначения пользователей системы ответственными за одно или несколько подключенных устройств



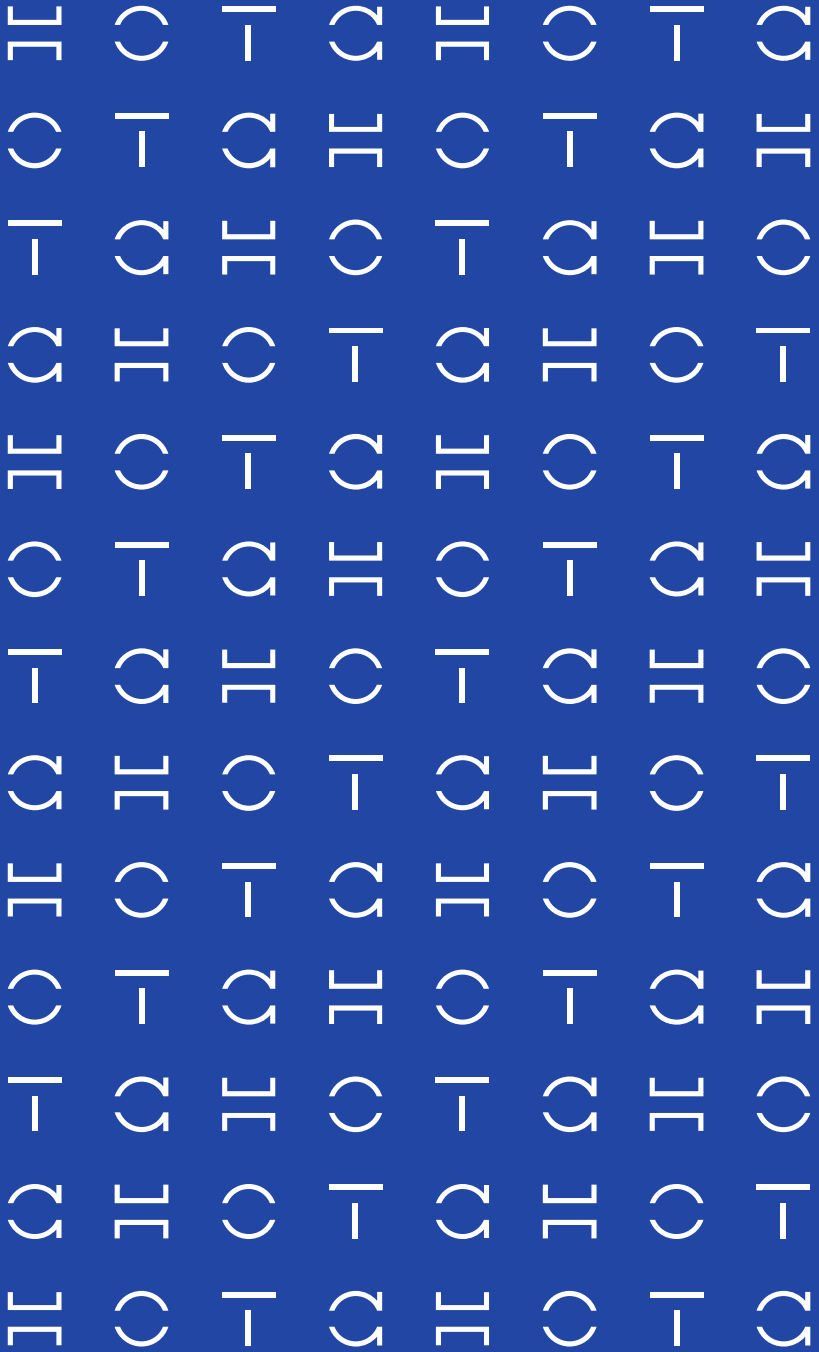
Н С Т С | КУПОЛ

НОТА КУПОЛ. КОНТЕЙНЕРЫ

+ | Т1

НОТА КУПОЛ. КОНТЕЙНЕРЫ

Система защиты контейнерных сред разработки



ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ СИСТЕМЫ КОНТЕЙНЕРИЗАЦИИ



Мониторинг и контроль

Как обеспечить мониторинг и контроль контейнеров и системы оркестрации?



Безопасность

Как обеспечить безопасность системы и анализировать уязвимости?



Контроль целостности

Как обеспечить контроль целостности образов и данных?



Визуализация и отчёты

Как визуализировать использование ресурсов и реализовать составление отчётности?

Программный продукт по обеспечению безопасности контейнерных сред разработки



Ценность для клиента

- Безопасность инфраструктуры с использованием контейнерных платформ
- Оценка рисков на всех этапах работы с контейнерами
- Повышение отказоустойчивости разрабатываемых и используемых приложений
- Оптимизация использования ресурсов и выявление аномалий

Функции



Мониторинг состояния кластеров

- Непрерывное сканирование состояния образов и конфигурационных файлов
- Мониторинг и контроль запуска контейнеров в runtime



Карта компонентов кластера и отчётность

- Построение карты компонентов кластера на основе данных встроенного сканера
- Визуализация ресурсов и трафика кластера



Контроль целостности образов

- Отслеживание изменений конфигураций
- Контроль запуска процессов внутри контейнера в соответствии с политиками безопасности



Управление политиками безопасности контейнеров

- Централизованное управление политиками всех кластеров
- Создание и изменение собственных политик и использование предустановленных политик



Управление уязвимостями

- Проверка образов на наличие уязвимостей по международной базе уязвимостей
- Встроенный механизм согласования принятия решений по каждой уязвимости
- Классификация уязвимостей по влиянию на образы



Защита контейнерных сред разработки и приложений

Защите процесса разработки CI/CD построенного на контейнерной архитектуре с использованием оркестратора



Проверка соответствия требованиям и стандартам

Проверка системы на предмет соответствия политикам безопасности. Единая точка управления политиками кластеров



Организация защищенной сервисной инфраструктуры

Анализ уязвимостей и проверка на соответствие стандартам безопасности приложений и сервисов на базе контейнерной архитектуры



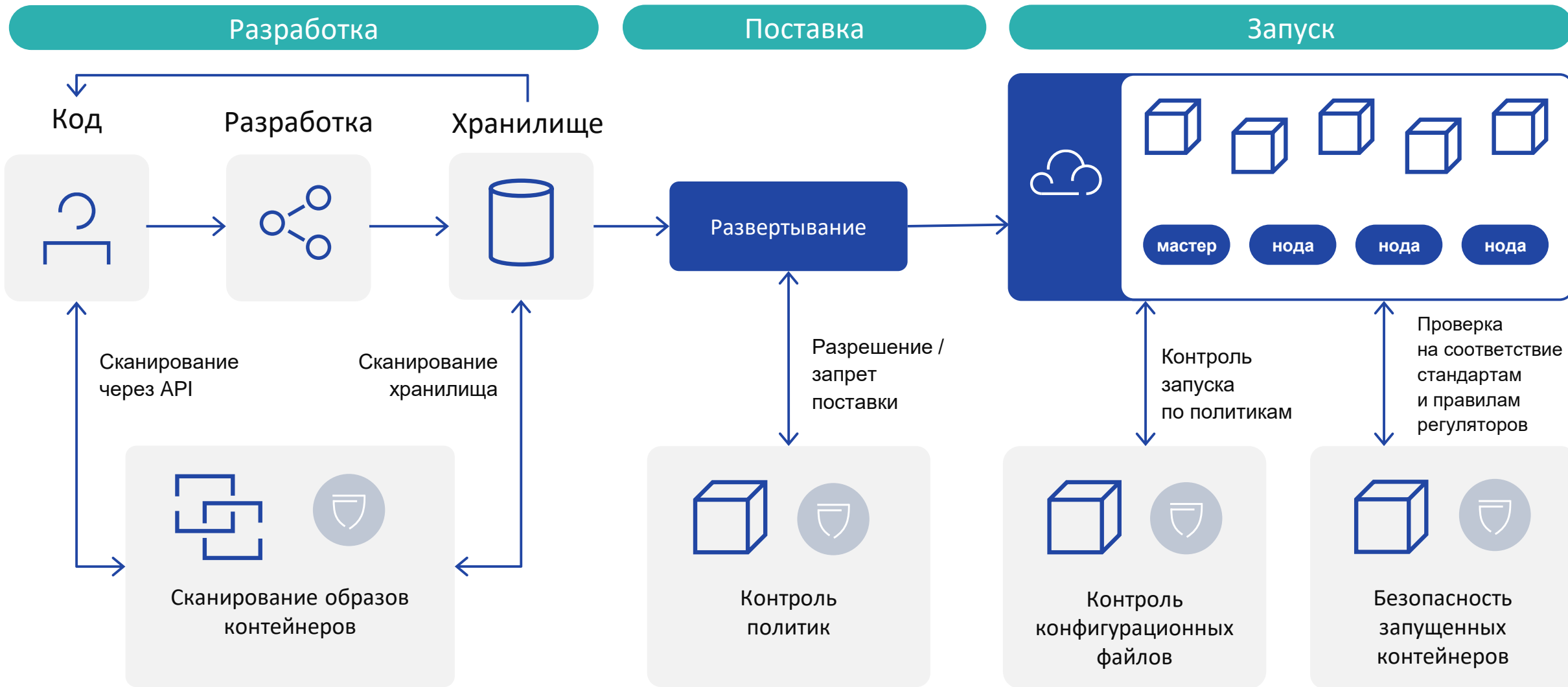
Оптимизация и визуализация работы контейнерной системы

Централизованный анализ работы системы, включая анализ использования ресурсов, наличия уязвимостей и создания отчетов

ЗАЩИТА СИСТЕМЫ КОНТЕЙНЕРИЗАЦИИ



СХЕМА ВНЕДРЕНИЯ



СКАНИРОВАНИЕ ОБРАЗОВ КОНТЕЙНЕРОВ

Уязвимости

Образы

Реестры образов Разовая проверка

Реестр:

Отчёты о сканировании уязвимостей д

- Репозиторий
- k8s/nota.kupol/frontend
- k8s/nota.kupol/frontend
- k8s/nota.kupol/frontend
- ansible/ansible_rsync
- k8s/nota.kupol/frontend
- debian11_minimal/minimal_image_deb
- astra1.7/node_build_image_astra1.7_ar
- astra1.7/base_image_astra1.7_amd64
- k8s/nota.kupol/keycloak
- cicd/build_astra1.7_amd64

Найдено записей: 1365

Детали образа

Образ nexuswatchman.t1-consulting.ru:8123/astra1.7/base_image_astra1.7_amd64:0.0.0-240118141023.gd7381bb0-0

ИД sha256:58ffe0be6923f1af8c9e148c6514f3338f6c0466318464ca8251aa54410c3902

ОС Astra Linux

Последний скан 28 февраля 2024 г. в 10:24:37 [Сканировать](#)

Уязвимости | Пакеты | Секреты | Слои

Уровень опасности	Пакет	Уязвимость
<input checked="" type="radio"/> Критический уровень	libtcl8.6	BDU:2022-01774
<input type="radio"/> Средний уровень	libip4tc0	CVE-2019-11360
<input type="radio"/> Высокий уровень	gnupg-utils	BDU:2023-03850
<input type="radio"/> Высокий уровень	libkrb5support0	BDU:2022-06933
<input type="radio"/> Средний уровень	libssl1.1	BDU:2022-04284
<input type="radio"/> Средний уровень	libssl1.1	CVE-2022-4304
<input type="radio"/> Высокий уровень	libssl1.1	CVE-2022-4450
<input type="radio"/> Высокий уровень	libssl1.1	BDU:2023-00675
<input type="radio"/> Высокий уровень	libssl1.1	BDU:2023-03652
<input type="radio"/> Высокий уровень	libssl1.1	BDU:2023-00665

↑ Экспорт

Package libtcl8.6

Идентификатор BDU:2022-01774

Fix status 0:8.6.9+dfsg-2+ci202302131725+astra1

Описание

Рекомендации по устранению:
- <https://wiki.astralinux.ru/astra-linux-se17-bulletin-20>: CVE: CVE-2021-35331
** DISPUTED ** In Tcl 8.6.11, a format string vulnerabi code execution via a crafted file. NOTE: multiple third of this finding.

Данные БДУ ФСТЭК

Уязвимость компонента pmakehlp.c языка програ недостаточной обработкой форматной строки. Экп позволяет нарушителю, действующему удаленно, конфиденциальным данным, нарушить их целост в обслуживании с помощью специально созданны

Вендор:
Сообщество свободного программного обеспечен

Найдено записей: 749

« < 1 из 75 > » 10 ▾

ДЕТАЛЬНАЯ ИНФОРМАЦИЯ ПО СКАНИРОВАНИЮ ОБРАЗОВ

Главная > Уязвимости > Образы > Разовая проверка

Уязвимости

Образы

Реестры образов **Разовая проверка**

Отчёты о сканировании образов, добавленные

- Реестр
- nexuswatchman.t1-consulting.ru:8123
- 172.31.142.57:8123
- nexuswatchman.t1-consulting.ru:8123
- nexuswatchman.t1-consulting.ru:8123

0.0...

Найдено записей: 4

Детали образа

Образ nexuswatchman.t1-consulting.ru:8123/vasylii/astra:vuln3

ИД sha256:189c383f1a8dc26121c2e35edb5f574e7586379c664e868120552596db759c3c

ОС Astra Linux

Последний скан 28 февраля 2024 г. в 11:21:14 [Сканировать](#)

Уязвимости Пакеты **Секреты** Слои [Экспорт](#)

Тип	Правило	Уровень важности	Где нашли
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Cipher/__pycache__/test_pkcs1
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Cipher/test_pkcs1_15.py
Поиск по содержимому	AWS Session Token	Высокий	usr/lib/python3/dist-packages/Crypto/SelfTest/Hash/test_HMAC.py
Поиск по содержимому	Facebook Secret Key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Hash/test_MD4.py
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Signature/__pycache__/test_pkc
Поиск по содержимому	Contains a private key	Средний	usr/lib/python3/dist-packages/Crypto/SelfTest/Signature/test_pkcs1_15.py
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/__pycache__/ipa.cpython-3
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/ipa.py
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/network/a10/__pycache__
Поиск по содержимому	Username and password in file	Высокий	usr/lib/python3/dist-packages/ansible/module_utils/network/a10/a10.py

Найдено записей: 26

« < 1 из 3 > » 10

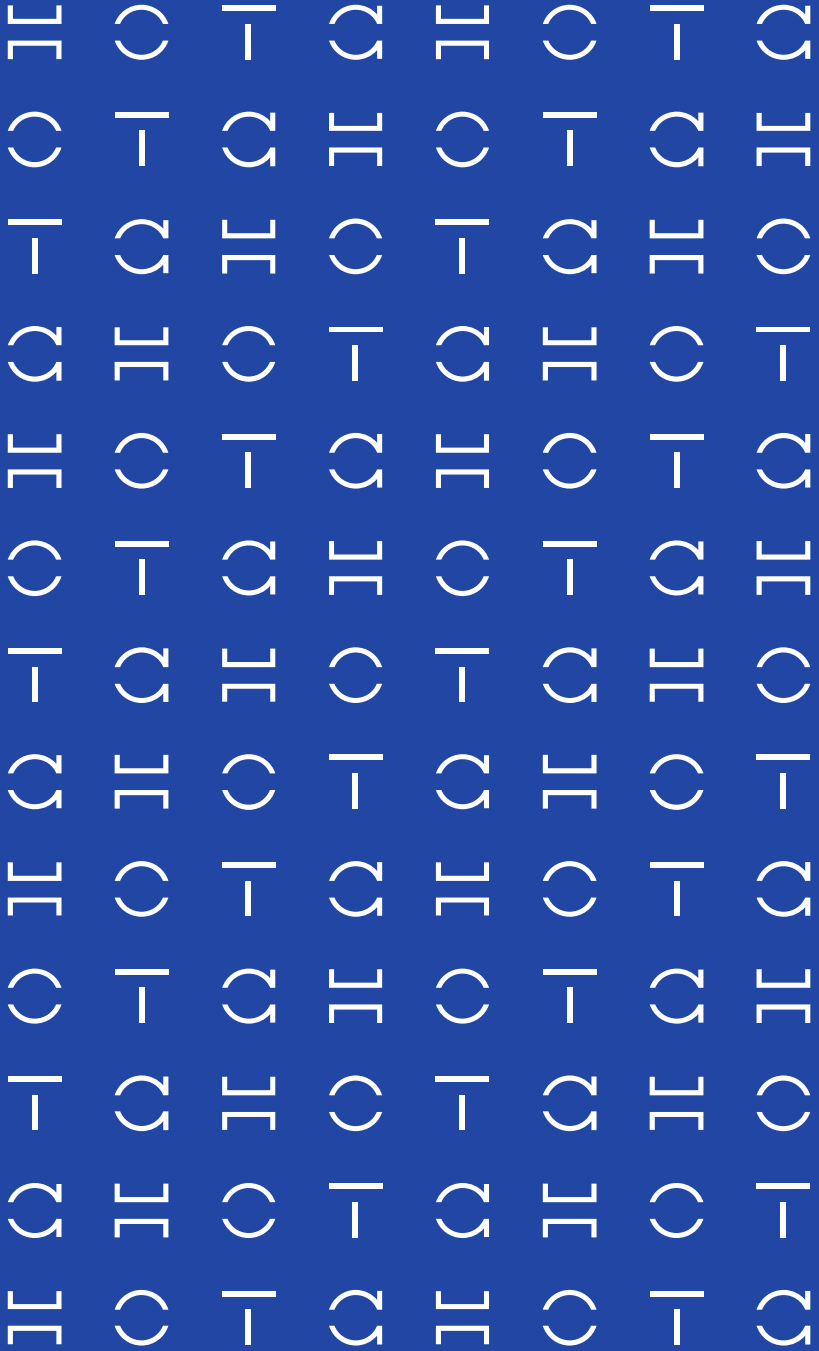
Н С Т С | КУПОЛ

НОТА КУПОЛ. ДОКУМЕНТЫ

+ | Т1

НОТА КУПОЛ. ДОКУМЕНТЫ

Система автоматизации процесса
аудита и категорирования
КИИ (ФЗ-187) и учёта ИТ-активов



ОСНОВНЫЕ ПРОБЛЕМЫ КАТЕГОРИРОВАНИЯ И АУДИТА

Категорирование объектов КИИ в соответствии требованиям 187-ФЗ



Единое рабочее пространство для учёта сведений о субъекте КИИ и относящихся к нему объектов



Автоматизация процесса категорирования объектов КИИ



Формирование актов категорирования для ФСТЭК России



Контроль мероприятий по соответствию требованиям регуляторов

Субъекты КИИ

- Ракетно-космическая промышленность
- Банковская сфера и иные сферы фин. рынка
- Топливо-энергетический комплекс
- Военно-промышленный комплекс
- Атомная промышленность
- Горнодобывающая промышленность
- Metallургическая и химическая промышленность
- ЮЛ и ИП, взаимодействующие с системами КИИ
- Здравоохранение

Объекты КИИ

- Информационные системы
- Телекоммуникационные системы
- Автоматизированные системы управления технологическими процессами

КАК РЕШАЕТ ПРОБЛЕМЫ ИЗ КОРОБКИ

Ручное категорирование



Сотрудник службы информационной безопасности

Ведение юридической информации субъекта КИИ

- Добавление сведений о субъекте КИИ
- Создание комиссии
- Занесение общей информации об объектах
- Определение критических бизнес-процессов

Инвентаризация информационной инфраструктуры и определение ОКИИ

- Формируется список систем
- Описание единицы оборудования
- Определение связи между системами и критичности данных

Формирование информации об угрозах и мерах обеспечения ИБ

- Формирование актуальных угроз и их экспертная оценка
- Формирование модели угроз
- Определение списка мер по обеспечению ИБ и их покрытие текущими СЗИ

Определение состава объектов КИИ

- Включение систем в состав объекта КИИ
- Проставление показателей значимости
- Определение категории значимости каждого объекта
- Определение уровня защищенности ОКИИ

Подготовка пакета документов

- Формирование акта категорирования
- Перечня объектов
- Приказа о комиссии

- Ведение справочной информации,
- Контроль исполнения мероприятий в рамках процесса категорирования

- Отслеживание изменения законодательства
- Ручная актуализация информации, формирования отчетных документов в рамках перекатегорирования

Категорирование с использование Купол. Документы



Сотрудник службы информационной безопасности

Ведение юридической информации субъекта КИИ

- Добавление сведений о субъекте КИИ
- Создание комиссии
- Занесение общей информации об объектах
- Определение критических бизнес-процессов



Автоматическое заполнение требуемых параметров

Инвентаризация информационной инфраструктуры и определение ОКИИ

- Формируется список систем
- Сканирование сетевых активов (оборудование, ПО, порты, пользователи, интерфейсы, сервисы и тд)
- Определение связи между системами и критичности данных
- Актуализация данных за счет повторного сканирования

Формирование информации об угрозах и мерах обеспечения ИБ

- Формирование актуальных угроз и их экспертная оценка
- Формирование модели угроз
- Определение списка мер по обеспечению ИБ и их покрытие текущими СЗИ

Определение состава объектов КИИ

- Включение систем в состав объекта КИИ
- Проставление показателей значимости
- Определение категории значимости каждого объекта
- Определение уровня защищенности ОКИИ

Подготовка пакета документов

- Формирование акта категорирования
- Перечня объектов
- Приказа о комиссии

Отправка сформированного и подписанного пакета документов во ФСТЭК России

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ ПРОДУКТА



Возможность **самостоятельного** проведения аудита и категорирования с минимальным количеством формальностей и сохранением конфиденциальности



Полный список активов компании или предприятия (с возможностью простого масштабирования и расширения)



Учет и оперативное обновление объектов КИИ и их состава (в возможность простого масштабирования и расширения)



Акт категорирования объектов критической информационной инфраструктуры предприятия



Полный пакет документов для информирования регуляторов



Значительное сокращение **временных затрат** и **человеческих ресурсов** для проведения первичного или повторного категорирования

УЧЕТ СВЕДЕНИЙ ОБ ОБЪЕКТАХ КИИ

■ ИАТ

☰ | КУПОЛ
Документы

НОВЫЕ ТЕХНОЛОГИИ ↗

🏠 Рабочий стол

🗪 **Объекты**

🗪 Системы

👤 Сотрудники

👤 Администратор

📄 Документы

📖 Справочники

14:39

Версия 0.0.0-2308021... >>

Объекты > Система резервного копирования и восстановления > Оборудование admin

Система резервного копирования и восстановления ⋮

🌟 Статус: Новый |
 📄 Акт категорирования: Не утвержден |
 ⚠ Категория: 1 |
 ➕ Создан: 27.06.2023, 00:47 admin |
 ✎ Изменен: 31.07.2023, 13:27 admin

Общие сведения |
 Системы |
 Программы |
 Оборудование |
 Меры |
 Показатели

Общие сведения |
 Системы |
 Программы |
 Оборудование |
 Показатели |
 Меры |
 Контрагенты |
 Угрозы

Формирование списка активов для объектов КИИ

<input type="checkbox"/>	Наименование	Тип	Изготовитель	Источник	Описание
<input type="checkbox"/>	172.31.142.236	Сетевое устройство	ООО «КИНЕТИК»	Ручное	Роутер Keenetic Giga
<input type="checkbox"/>	172.31.142.235	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD
<input type="checkbox"/>	172.31.142.234	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD
<input type="checkbox"/>	172.31.142.233	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD
<input type="checkbox"/>	172.31.142.236	Сетевое устройство	ООО «КИНЕТИК»	Ручное	Роутер Keenetic Giga
<input type="checkbox"/>	172.31.142.235	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD
<input type="checkbox"/>	172.31.142.234	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD
<input type="checkbox"/>	172.31.142.233	APM	Hewlett Packard Inc	Ручное	Intel core i5, 8 Gb Ram, 512 SSD

Найдено записей: 8 ⏪ < 1 из 1 > ⏩ 10 ▾

СОЗДАНИЕ МОДЕЛИ УГРОЗ

☰ | КУПОЛ
Документы

Субъект
АО "Система" >

🏠 Рабочий стол

☰ Объекты

☰ Системы

👤 Сотрудники

👤 Администратор

📄 Документы

📖 Справочники

12:14

Версия 0.0.0-2308281... >>

Объекты > Производство > Угрозы admin

Производство

✓ Статус: Эксплуатация |
 📄 Акт категорирования: Не утвержден |
 ▲ Категория: 3 |
 + Создан: 29.08.2023, 18:26 admin |
 ✎ Изменен: 29.08.2023, 18:45 admin

Общие сведения Системы Программы Оборудование Показатели Меры Контрагенты Угрозы

Угрозы 🔍 ...

Формирование модели угроз

Наименование	УБИ	К	Ц	Д	Аппаратное устройство	
<input type="checkbox"/> Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	УБИ. 210	Ц	Д		Аппаратное устройство	+3
<input type="checkbox"/> Угроза несанкционированного доступа к защищаемой памяти ядра процессора	УБИ. 209	К	Ц	Д	Аппаратное устройство	
<input type="checkbox"/> Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	УБИ. 208	Д			Мобильное устройство	+1
<input type="checkbox"/> Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	УБИ. 207	К	Ц	Д	Аппаратное устройство	+1
<input type="checkbox"/> Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	УБИ. 206	К	Д		Аппаратное устройство	
<input type="checkbox"/> Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	УБИ. 205	Д			Аппаратное устройство	+1
<input type="checkbox"/> Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	УБИ. 204	Ц			Аппаратное устройство	
<input type="checkbox"/> Угроза несанкционированной установки приложений на мобильные устройства	УБИ. 202	К			Аппаратное устройство	+1
<input type="checkbox"/> Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	УБИ. 200	К			Аппаратное устройство	+1
<input type="checkbox"/> Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	УБИ. 199	К	Д		Аппаратное устройство	+1

АВТОМАТИЗАЦИЯ ПРОЦЕССА КАТЕГОРИРОВАНИЯ ОБЪЕКТА КИИ

Объекты > Система резервного копирования и восстановления > Показатели

Система резервного копирования и восстановления

Статус: Новый | Акт категорирования: Не утвержден | Категория: 1 | Создан: 27.06.2023, 00:47 admin

Общие сведения | Системы | Программы | Оборудование | **Показатели** | Меры | Контрагенты | Угрозы

Показатели

Отсутствуют категории
Есть группы в которых еще не выставлены значения

Социальная значимость 1

Политическая значимость ⚠

Экономическая значимость ⚠

Экологическая значимость ⚠

Государственная значимость ⚠

Социальная значимость

1	Причинение ущерба жизни и здоровью людей (человек)	1
3	возможно	3
2	людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	2
3-а	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг	2
3-б	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, оцениваемые по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	⚠
4	Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек)	⚠
5-а	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	⚠

Показатель применим

Кол-во человек *
1000
3 категория: более или равно 1, но менее или равно 50; 2 категория: более 50, но менее или равно 500; 1 категория: более 500;

Обоснование

Ответственное лицо
Шпала Семён Геннадиевич

Автоматический расчет категории значимости на основании оценок для применимых показателей значимости

14:04
Версия 0.0.0-2308021...

АВТОМАТИЗАЦИЯ ПРОЦЕССА КАТЕГОРИРОВАНИЯ ОБЪЕКТА КИИ

☰ | КУПОЛ
Документы

Субъект
Новые технологии >

🏠 Рабочий стол

📊 **Объекты**

📁 Системы

👤 Сотрудники

👤 Администратор

📄 Документы

📖 Справочники

14:19

Версия 0.0.0-2308021... >>

Объекты > Система резервного копирования и восстановления > Меры admin

Система резервного копирования и восстановления ⋮

🌟 Статус: Новый |
 📄 Акт категорирования: Не утвержден |
 ⚠️ Категория: 1 |
 ⊕ Создан: 27.06.2023, 00:47 admin |
 ✎ Изменен: 31.07.2023, 13:27 admin

Общие сведения |
 Системы |
 Программы |
 Оборудование |
 Показатели |
 Меры

Автоматическое формирование списка мер обеспечения информационной безопасности

Меры защиты

Название	Статус	Тип	№	Группа
<input type="checkbox"/> Регламентация правил и процедур идентификации и аутентификации	Не обеспечено	Организационная	ИАФ.0	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Идентификация и аутентификация пользователей и инициируемых ими процессов	Обеспечено	Техническая	ИАФ.1	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Идентификация и аутентификация устройств	Не обеспечено	Техническая	ИАФ.2	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Управление идентификаторами	Не обеспечено	Техническая	ИАФ.3	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Управление средствами аутентификации	Не обеспечено	Техническая	ИАФ.4	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Идентификация и аутентификация внешних пользователей	Не обеспечено	Техническая	ИАФ.5	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Защита аутентификационной информации при передаче	Не обеспечено	Техническая	ИАФ.7	Идентификация и аутентификация (ИАФ)
<input type="checkbox"/> Регламентация правил и процедур управления доступом	Не обеспечено	Организационная	УПД.0	Управление доступом (УПД)
<input type="checkbox"/> Управление учетными записями пользователей	Не обеспечено	Техническая	УПД.1	Управление доступом (УПД)
<input type="checkbox"/> Реализация модели управления доступом	Не обеспечено	Техническая	УПД.2	Управление доступом (УПД)

Найдено записей: 116 << < 1 из 12 > >> 10 ▾

ПРИМЕР РЕШЕНИЯ ПРОБЛЕМ

Крупный промышленный холдинг

Проблема клиент до внедрения продукта



Сокращенное время на категорирование

По полученным предписаниям от регулятора необходимо было провести процедуру категорирования в короткий срок. Подрядные организации проводили процедуру в течении 3-4 месяцев, что не устраивало заказчика.



Непрозрачное ценообразование

Стоимость запланированных в начале года расходов на процедуру категорирования выросла на 30-40%, что не входило в рамки бюджета.



Утечка конфиденциальных данных

Компания ранее страдала при утечке конфиденциально информации и идеальным вариантом был либо найм сотрудников для категорирования, либо поиск продукта.

Результат внедрения продукта



Ускоренное категорирование

При внедрении продукта подготовка полного пакета документов по 84 ОКТИ заняло 4 рабочих дня (при учёте отраслевой специфики). Ошибок в ходе проверки со стороны регулятора не выявлено.



Ценообразование

Ввиду того, что заказчик приобретал программное обеспечение мы смогли предоставить трехлетнюю спецификацию с ежегодной оплатой, тем самым зафиксировать стоимость в договоре и дать возможность не только корректного прогноза по бюджету, но и сэкономить.



Ведение информации на протяжении всего цикла жизни объектов КИИ

Вся информация хранилась у заказчика без передачи третьим лицам, что уменьшало риски утечки данных.



Категорирование в соответствии требованиям 187-ФЗ

Позволяет субъектам КИИ с минимальными трудозатратами провести категорирование объектов КИИ в соответствии требованиям федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ.



Автоматизации процесса категорирования объектов КИИ

Благодаря автоматическому расчёту категории значимости объекта КИИ, автоматическому учёту примененных и необходимых мер защиты в отношении объекта КИИ, автоматическому формированию актов категорирования.



Обеспечение полного контроля и прозрачности процесса категорирования

За счёт агрегации в едином пространстве сведений:
о субъекте КИИ, об ОКИИ,
о лице эксплуатирующем ОКИИ, о взаимодействии ОКИИ и сетей электросвязи, о программных и программно-аппаратных средствах используемых на ОКИИ.



Ускорение процесса подготовки документов по форме ФСТЭК России

Позволяет субъектам КИИ подготовить необходимые документы по результатам проведения категорирования для отправки во ФСТЭК России.

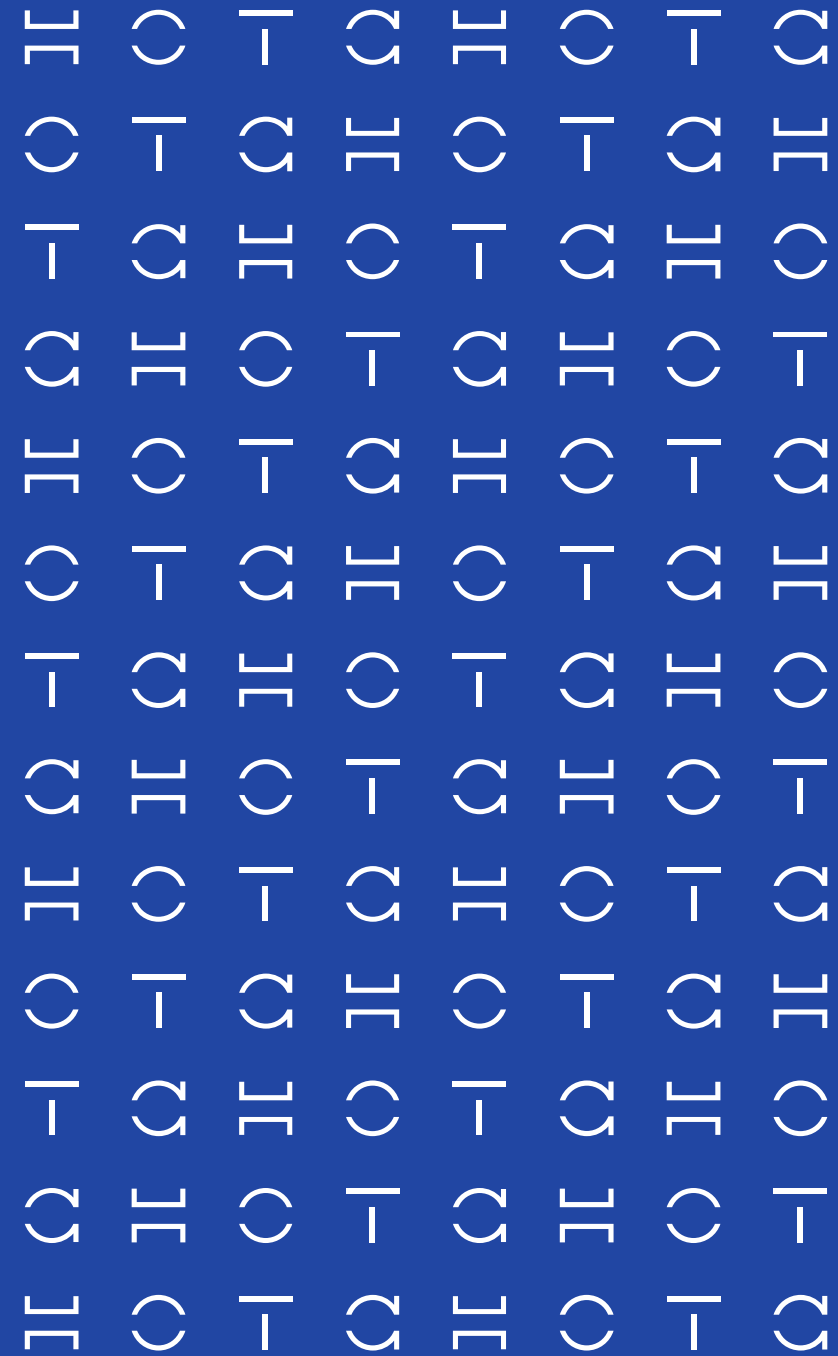
Н С Т С | КУПОЛ

НОТА КУПОЛ.
ПРАВИЛА

+ | Т1

НОТА КУПОЛ. ПРАВИЛА

Единая платформа для унификации
и обновления правил системы обнаружения
вторжений (СОВ)



ОСНОВНЫЕ ПРОБЛЕМЫ С НАСТРОЙКОЙ ПРАВИЛ



Правила не работают

Часто вендоры используют готовые базы правил, правила из открытых источников и самописные базы правил, не уделяя должного внимания тестированию



Разные наборы правил для межсетевых экранов

В сетевой инфраструктуре используются различные наборы правил



Отсутствие централизованного обновления

Отсутствует единая точка загрузки правил и автоматизация их получения



Неудобная система лицензирования

Лицензия создает искусственные ограничения и блокирует обновления при истечении срока действия

Универсальные наборы правил для систем обнаружения вторжений и межсетевых экранов нового поколения

Решаемые проблемы

- Покупные правила не работают
- Разные наборы правил для разных межсетевых экранов
- Отсутствие централизованного обновления

Особенности создания продукта

- Выделенная команда профессионалов, занимающаяся разработкой, отладкой и тестированием совместимости правил со сторонними устройствами
- Постоянное обновление и актуализация правил
- Наборы правил, с учётом отраслевой специфики
- Создание специализированных групп правил по запросу

Преимущества



Гарантия работы правил

Правила проходят тестирование и контроль совместимости



Унификация базы правил

Единая база правил, которая подходит для межсетевых экранов различных вендоров



Единая платформа обновления

Вы получаете доступ к единой платформе, с которой можно скачивать постоянно обновляющуюся базу правил



Простая и понятная система лицензирования

Подписка на обновления на год, нет искусственных ограничений в работе устройств, можно в любой момент продлить подписку и загрузить обновленный список правил



Гарантия работы правил

Правила проходят тестирование и контроль совместимости



Унификация базы правил

Единая база правил, которая подходит для межсетевых экранов различных вендоров



Единая платформа обновления

Заказчик получает доступ к единой платформе, с которой может скачивать постоянно обновляющуюся базу правил



Простая и понятная система лицензирования

Подписка на обновления на год, не создается искусственных ограничений по работе устройств, можно в любой момент продлить подписку и загрузить обновленный список правил

Н С Т С | КУПОЛ

ЗАКЛЮЧЕНИЕ

+ | Т1

**Помогаем сделать первые шаги по
выстраиванию
информационной
безопасности
в Вашей компании**



При развитии продуктов
мы ориентируемся на



Мы открыты для получения
обратной связи!



Современные технологии



Зарубежные и российские тренды



Требования регуляторов



Отраслевые требования



Требования отдельных заказчиков

П С Т С | +111

Спасибо
за внимание