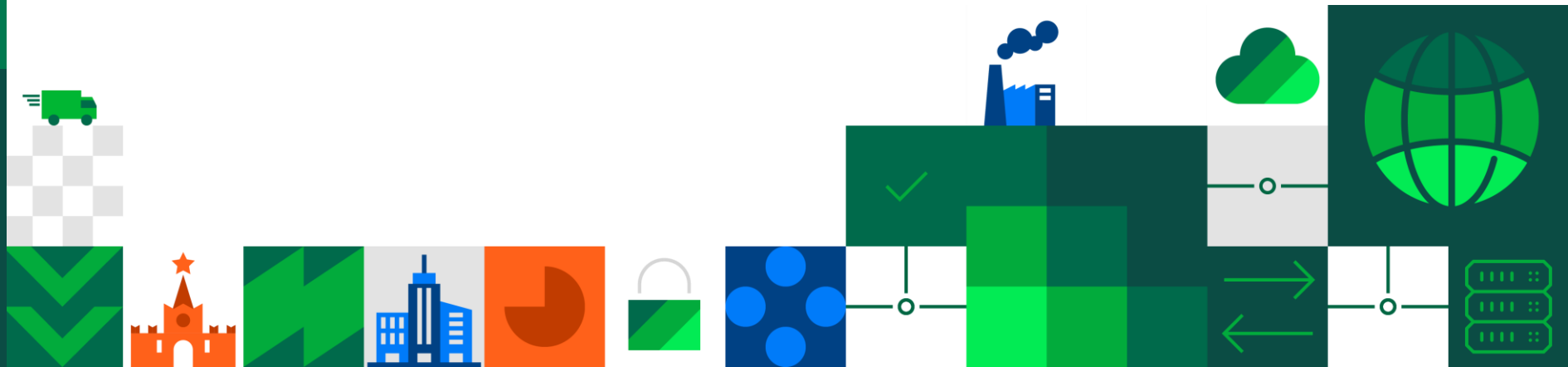
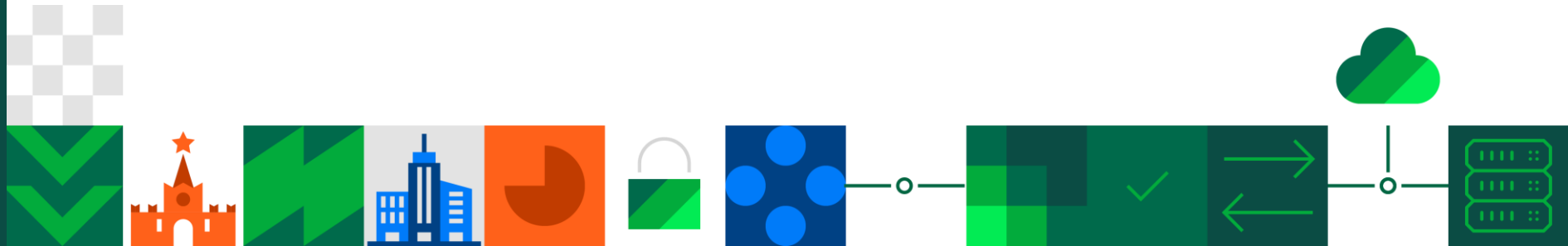
КОД безопасности

Континент СОВ/СОА



КОД безопасности

О продукте



КОД безопасности

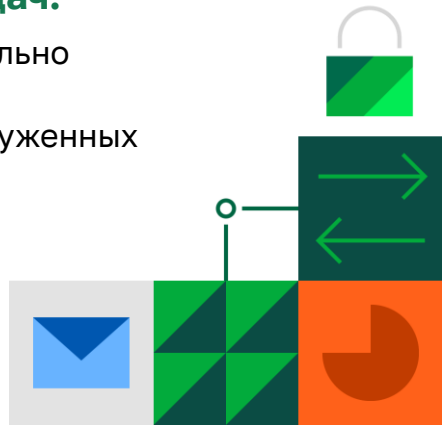
О продукте

Континент СОВ/СОА

Высокопроизводительная система обнаружения и предотвращения вторжений

Предназначен для решения следующих задач:

- Защита от сетевых вторжений в территориально распределённых сетях
- Защита от сетевых вторжений в высоконагруженных сетях
- Выполнение требований регуляторов



КОД безопасности

Сертификация

ФСТЭК России (Континент СОВ)

- 3-й класс защиты СОВ уровня сети
- 3-й уровень доверия

ФСБ России (Континент СОА)

- Средство обнаружения компьютерных атак класса ВП

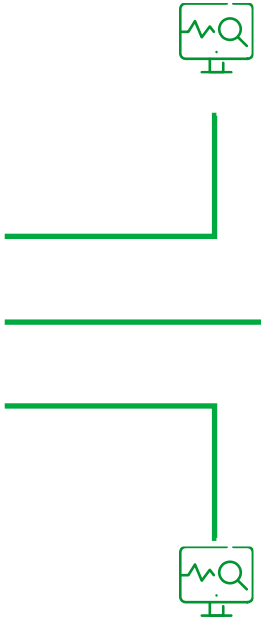
Сертифицирован для защиты

- КИИ до 1 категории включительно
- ГИС до 1 класса защищенности включительно
- ИСПДн до класса УЗ1 включительно
- АС до класса 1В включительно

Архитектура Континент СОВ/СОА

Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга всеми компонентами системы защиты.

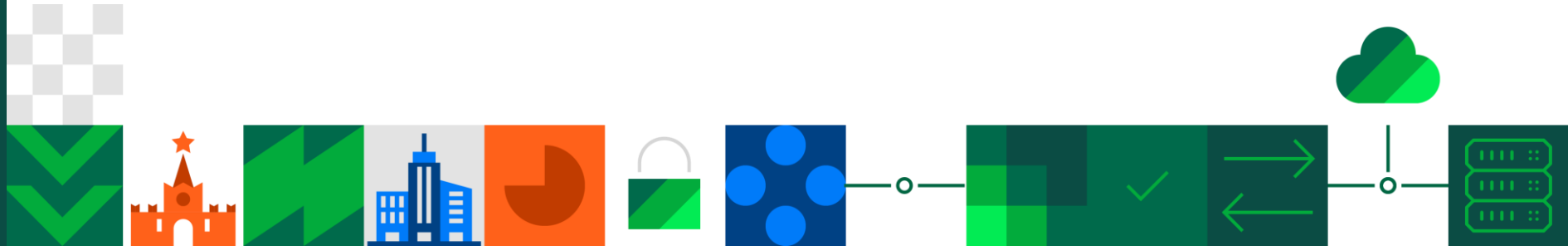


Детектор атак

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения и предотвращения вторжений.

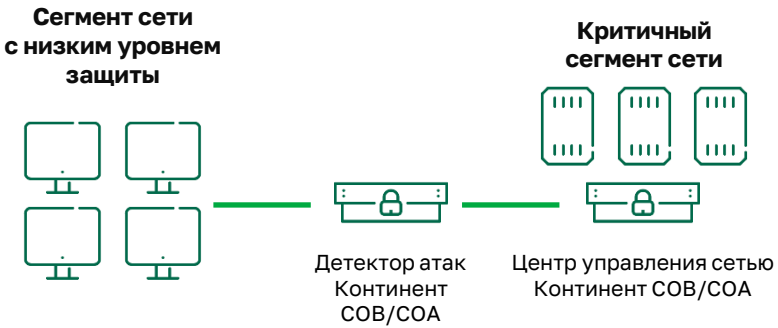
КОД безопасности

Варианты применения



КОД безопасности

Защита критичных сегментов сети



Задачи

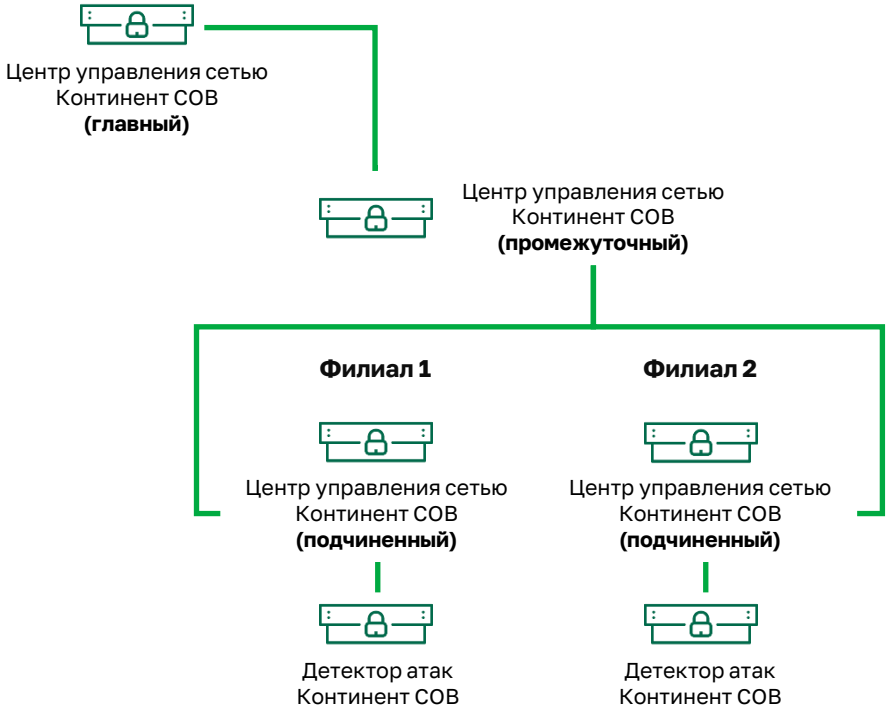
- Автоматическое предотвращение атаки на критичные ресурсы

Компоненты

- Центр управления сетью
- Детектор атак

КОД безопасности

Обнаружение вторжений в распределенных сетях (Континент СОВ)



Задачи

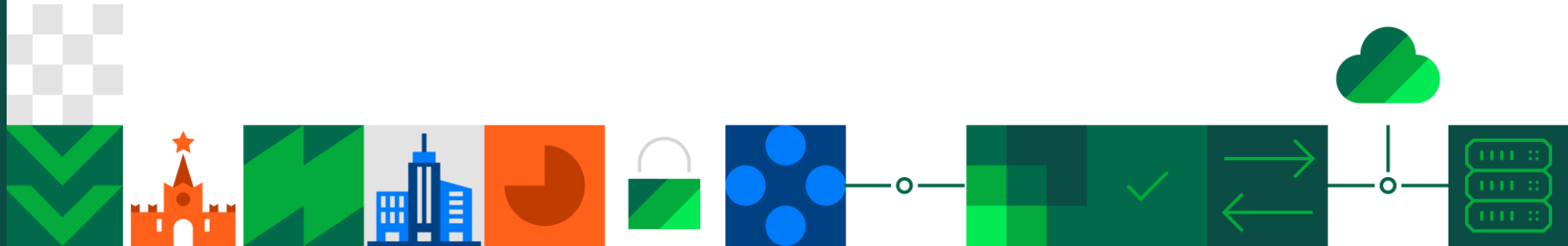
- Обнаружение вторжений
- Выполнение глобальной политики безопасности
  - Сквозная система мониторинга и управления
  - Выделение ограниченных прав администраторам «на местах»

Компоненты

- Центр управления сетью
- Детектор атак

КОД безопасности

Компоненты



КОД безопасности

Управление инфраструктурой Континент COB/COA

Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент COB/COA

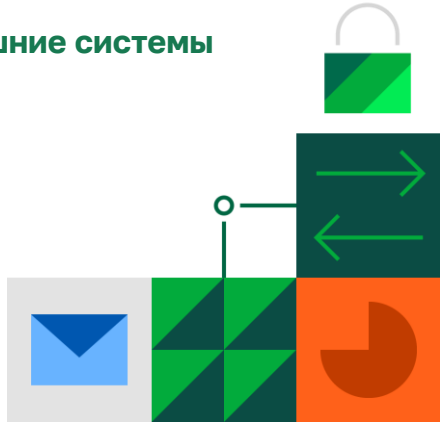
Мониторинг событий в режиме реального времени

Дистанционное обновление компонентов комплекса

Автоматическое обновление базы решающих правил с серверов «Кода Безопасности»

Гибкая система отчетов

Экспорт событий безопасности во внешние системы мониторинга и управления ИБ



КОД безопасности

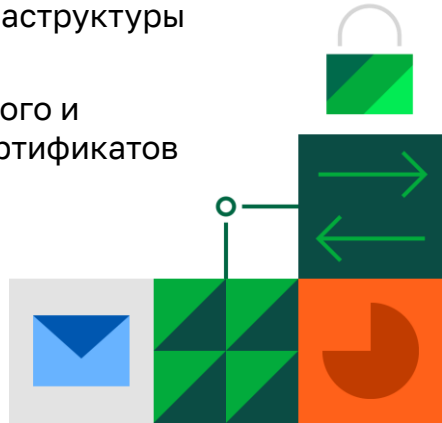
Управление инфраструктурой Континент СОВ

Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент СОВ

Система иерархического управления большой инфраструктурой (Континент СОВ)

- Три уровня иерархии управления
- Делегирование прав в рамках глобальной политики безопасности
- Сквозной мониторинг всей инфраструктуры Континент СОВ
- Взаимная аутентификация главного и подчиненных ЦУС с помощью сертификатов



КОД безопасности

Управление инфраструктурой Континент COB/COA

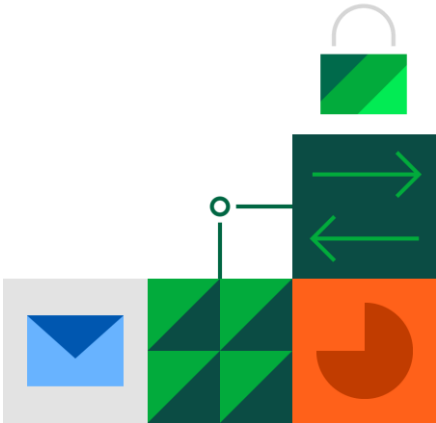
Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент COB/COA

Новые консоли управления и мониторинга

Высокопроизводительная система хранения и обработки событий безопасности

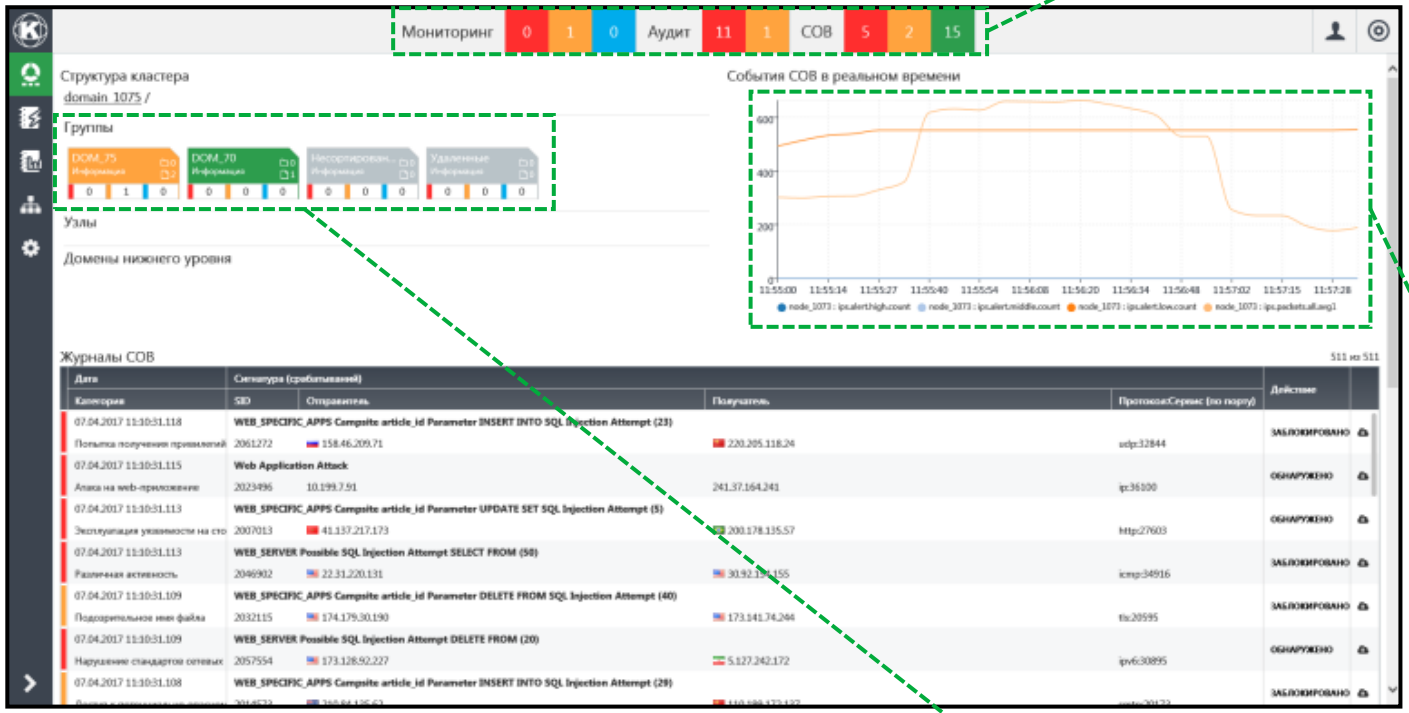
Ролевая модель доступа администраторов



КОД безопасности

Панель мониторинга

Состояние центра управления сетью и детекторов атак



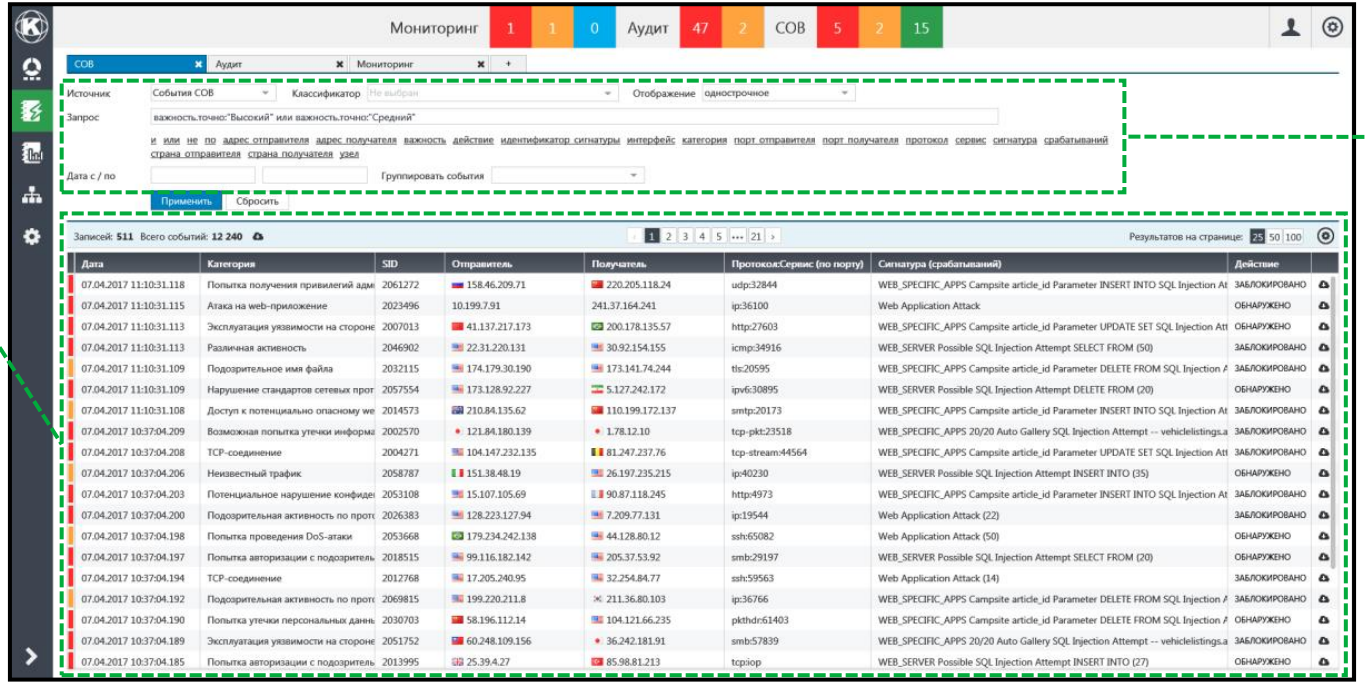
Распределение событий детекторов атак в реальном времени

Сводная информация по состоянию всей инфраструктуры СОВ/СОА

КОД безопасности

Список событий безопасности

Список событий безопасности



Поисковая строка - фильтр по событиям безопасности

КОД безопасности

Подробная информация по событию

Время последнего события **в час. поясе ДА**	07.04.2017 11:10:31.118 07.04.2017 08:10:31.118 (UTC)
Важность	Высокий
Отправитель	158.46.209.71 : 4227
Получатель	220.205.118.24 : 32844
Протокол	udp
Сервис (по порту)	(32844)
Действие	заблокировано
Категория событий	Попытка получения привилегий администратора
Детектор атак	node_1070@domain_1070 (eth1)
Кол-во срабатываний	23
Сигнатура	WEB_SPECIFIC_APPS Campsite article_id Parameter INSERT INTO SQL Injection Attempt
Доп. информация	SID: 2061272

Выгрузка копии трафика для анализа

КОД безопасности

Настраиваемые виджеты статистики

КОД безопасности

Мониторинг иерархической структуры

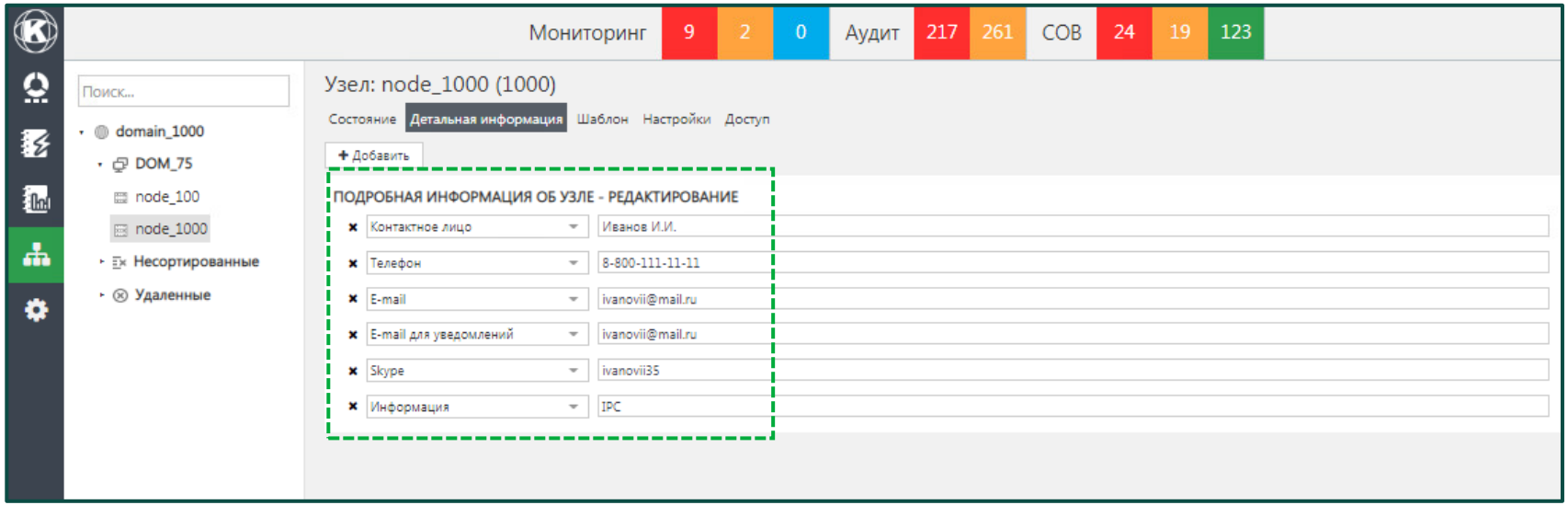
Иерархия системы управления

Уровень загрузки ресурсов Детектора атак

События подсистемы

КОД безопасности

Информация об узле Континент СОВ/СОА



КОД безопасности

Обнаружение атак

Детектор атак

Аппаратно-программный комплекс, сетевой сенсор, предназначенный для анализа сетевого трафика, обнаружения и предотвращения вторжений

Двухуровневая система анализа трафика

- Сигнатурный анализ
- Эвристический анализ

Установка политики безопасности без перерыва в работе сервисов

Дистанционное обновление системного ПО и сигнатур (базы решающих правил)

КОД безопасности

Обнаружение атак
Сигнатурный анализ трафика

Детектор атак

Аппаратно-программный комплекс, сетевой сенсор, предназначенный для анализа сетевого трафика, обнаружения и предотвращения вторжений

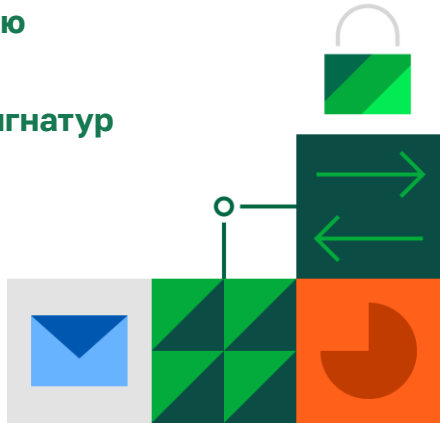
Более 25000 сигнатур в базе решающих правил

Автоматическое обновление базы решающих правил с серверов «Кода Безопасности»

Сигнатуры детектора атак, разработанные собственной лабораторией

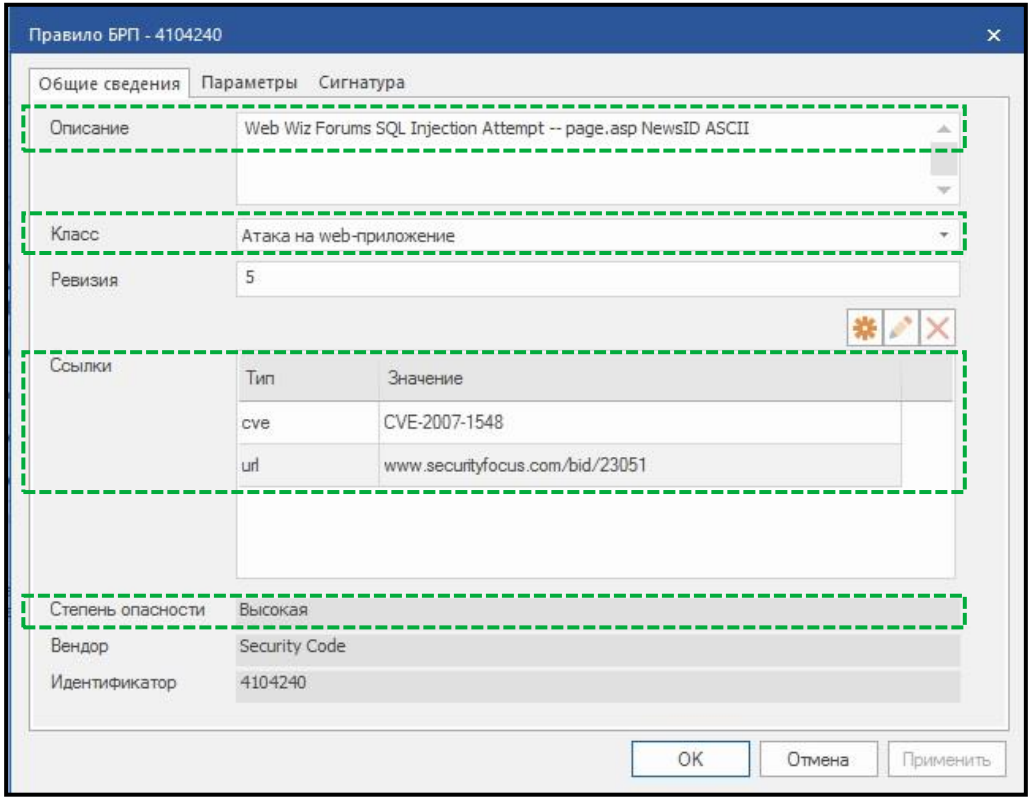
Низкое влияние сигнатур на пропускную способность устройства

Возможность создания собственных сигнатур



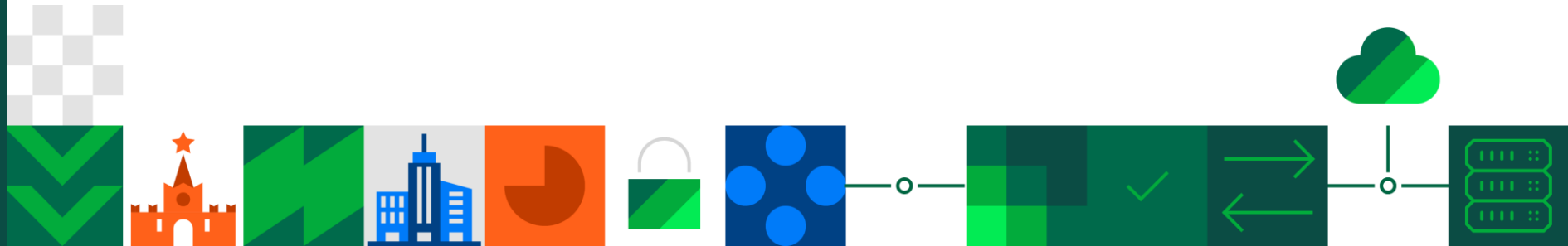
КОД безопасности

Подробное описание правила БРП



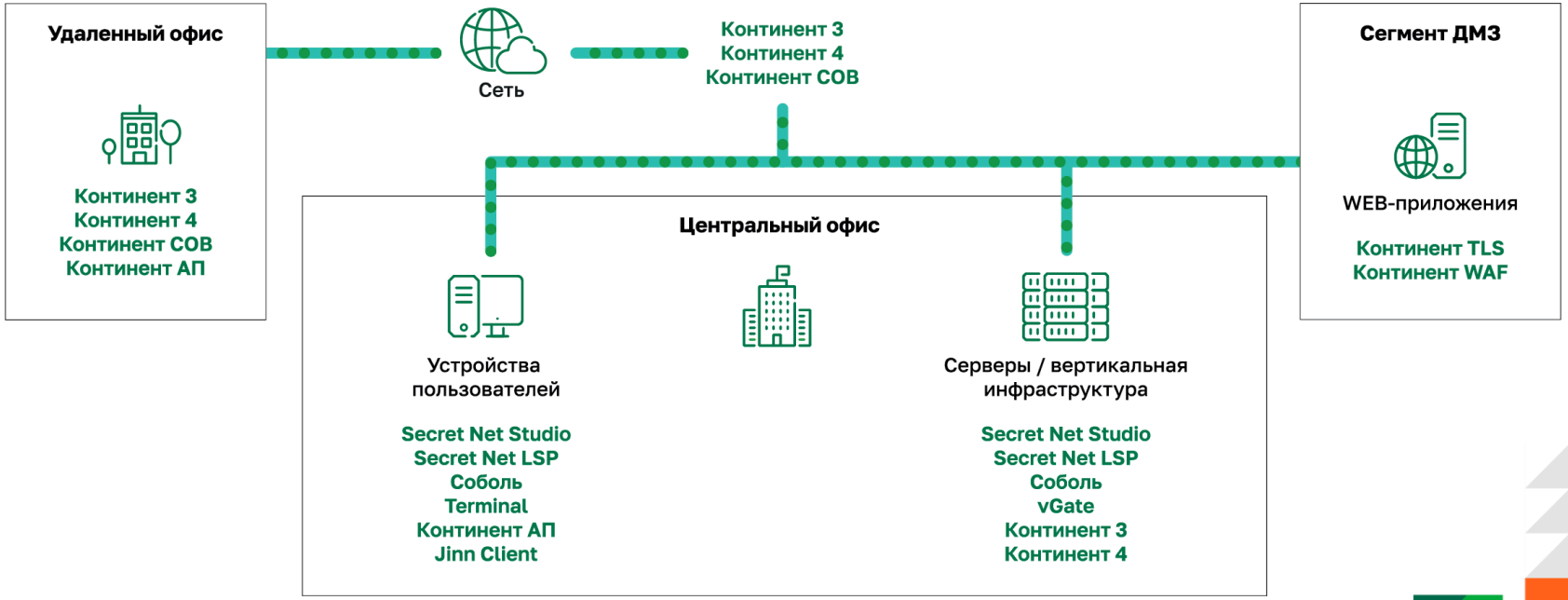
КОД безопасности

О компании



КОД безопасности

Комплексный подход к защите инфраструктуры



КОД безопасности

Факты о компании

«Крупнейшие производители высокотехнологичного оборудования»

«Крупнейшие разработчики ПО»

«Крупнейшие ИТ-компании России»

- Более **20 лет** на страже безопасности крупнейших предприятий России
- **9 лицензий** ФСТЭК, ФСБ и Минобороны России
- **3 центра разработки:** Москва, Санкт-Петербург, Пенза
- Более **400 квалифицированных специалистов R&D**, имеющих уникальные компетенции
- Более **50 разработанных СЗИ и СКЗИ**
- Более **60 сертификатов** соответствия
- Обеспечена безопасность **1 200 000 компьютеров** в **32 000 организаций**
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров**

КОД безопасности

Нам доверяют

Государственные организации:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный Фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

Силовые структуры:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

Телекоммуникационные компании:

- ПАО «Ростелеком»
- ФГУП «Почта России»
- ГК «АКАДО Телеком»
- АО «Воентелеком»

Финансовые организации:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- АО «Страховая группа МСК»
- ПАО «ВТБ24»
- ПАО «Банк «Возрождение»

Промышленные предприятия:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»
- ГКНПЦ им. М.В. Хруничева

Предприятия ТЭК:

- Государственная корпорация по атомной энергии «Росатом»
- ПАО «Газпром»
- ПАО «АК «Транснефть»
- ПАО «НК «Роснефть»

КОД безопасности

info@securitycode.ru
www.securitycode.ru