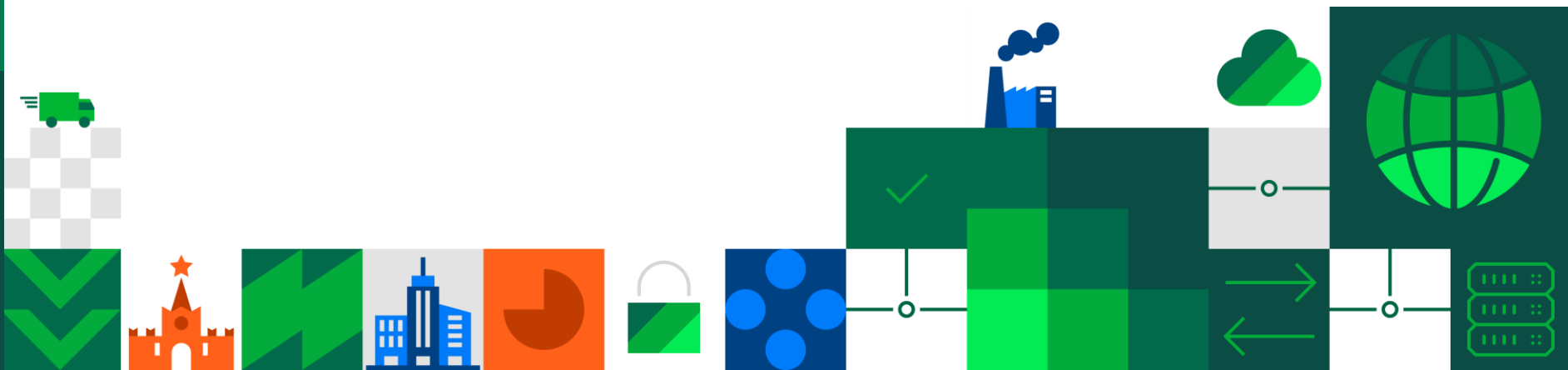


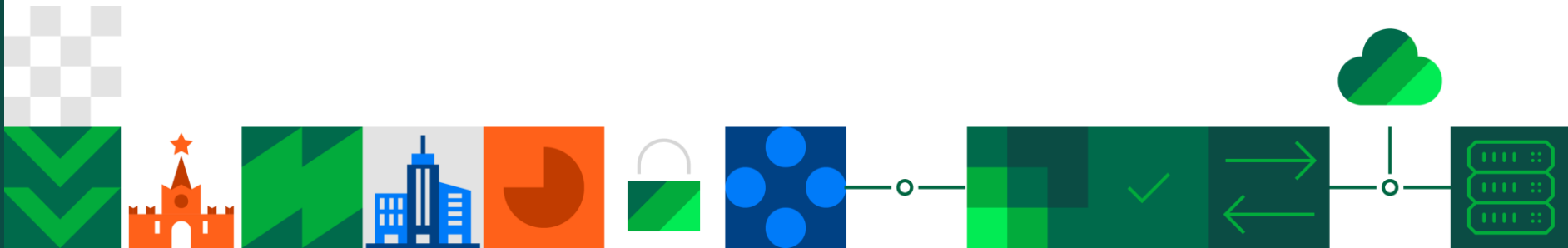


Континент СОВ/СОА





О продукте



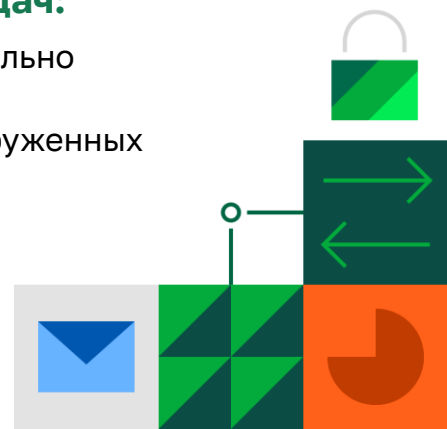


Континент **СОВ/СОА**

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





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

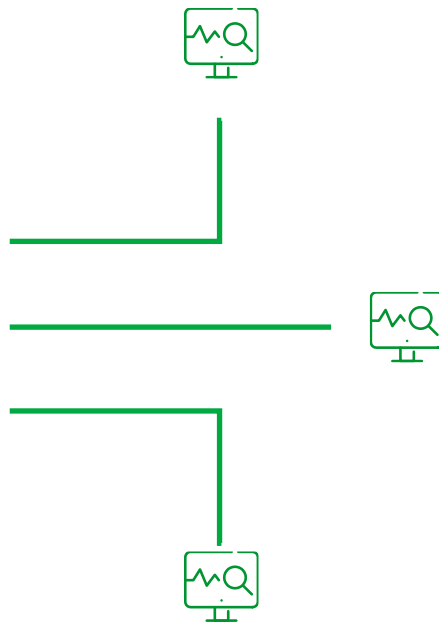
- КИИ до 1 категории включительно
- ГИС до 1 класса защищенности включительно
- ИСПДн до класса УЗ1 включительно
- АС до класса 1В включительно





Центр управления сетью

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

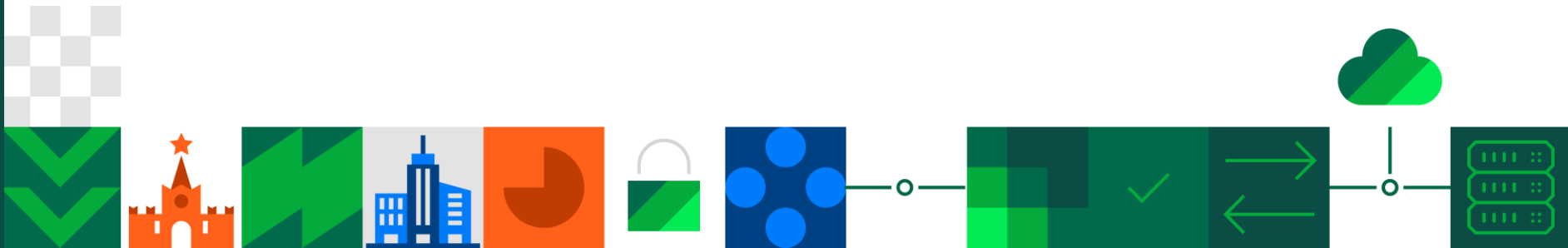


Детектор атак

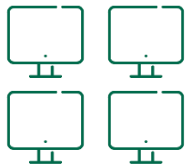
Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения и предотвращения вторжений.



Варианты применения

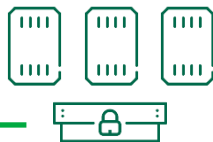


Сегмент сети
с низким уровнем
защиты



Детектор атак
Континент
COB/COA

Критичный
сегмент сети



Центр управления сетью
Континент COB/COA

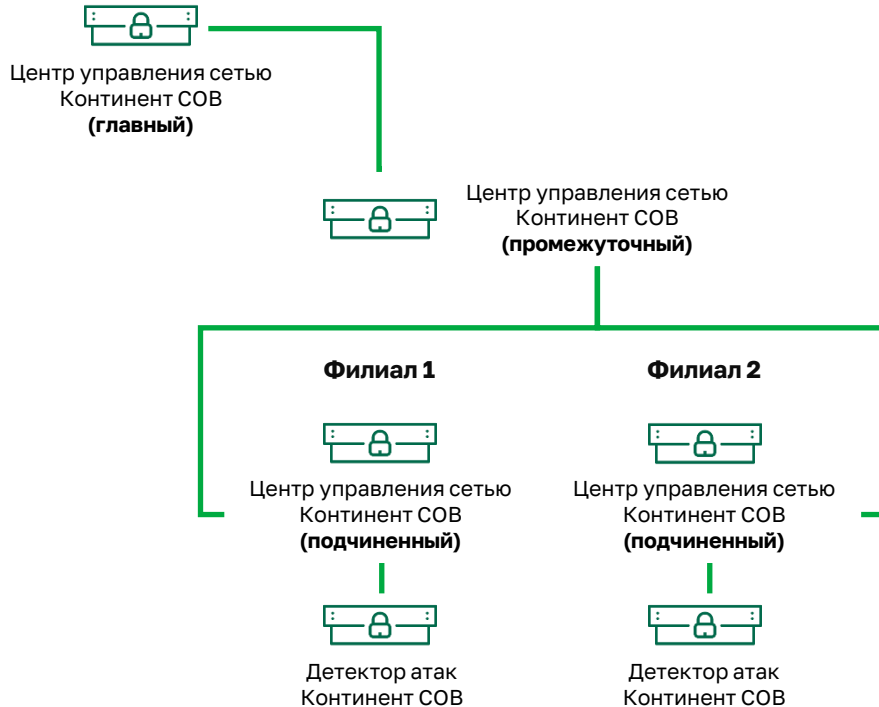
Задачи

- Автоматическое предотвращение атаки на критичные ресурсы

Компоненты

- Центр управления сетью
- Детектор атак





Задачи

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

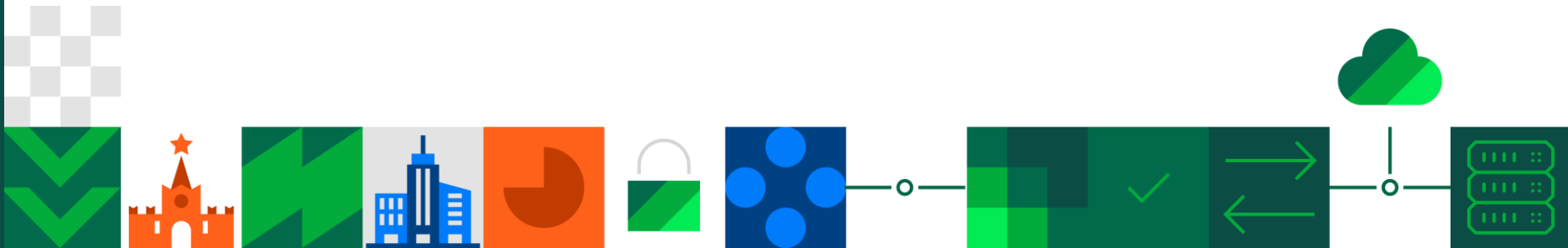
Компоненты

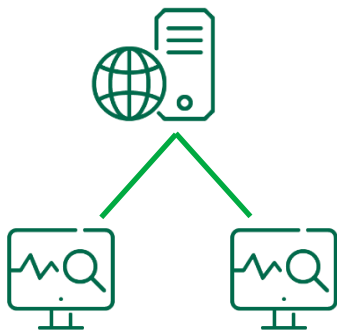
- Центр управления сетью
- Детектор атак





Компоненты





Центр управления сетью

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

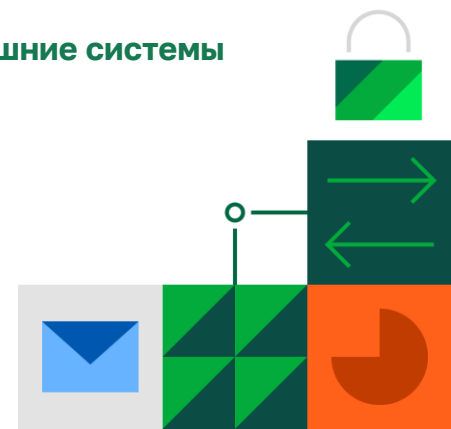
Мониторинг событий в режиме реального времени

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



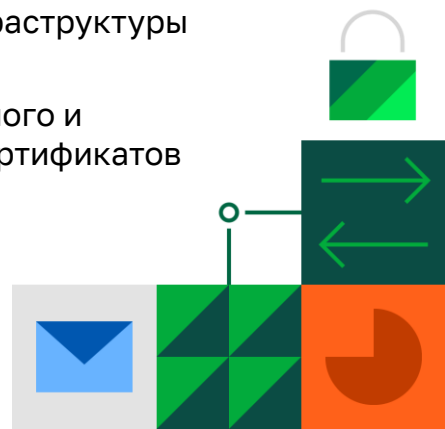


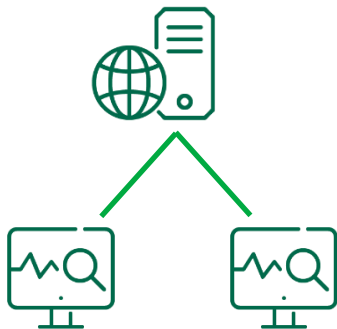
Центр управления сетью

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





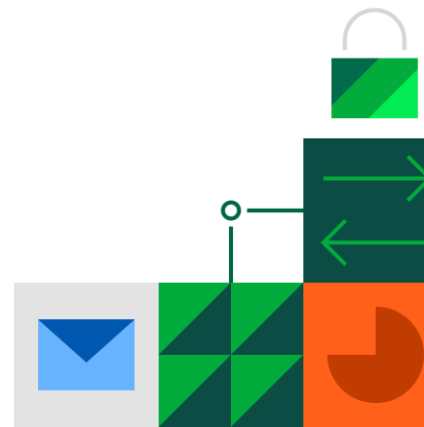
Центр управления сетью

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

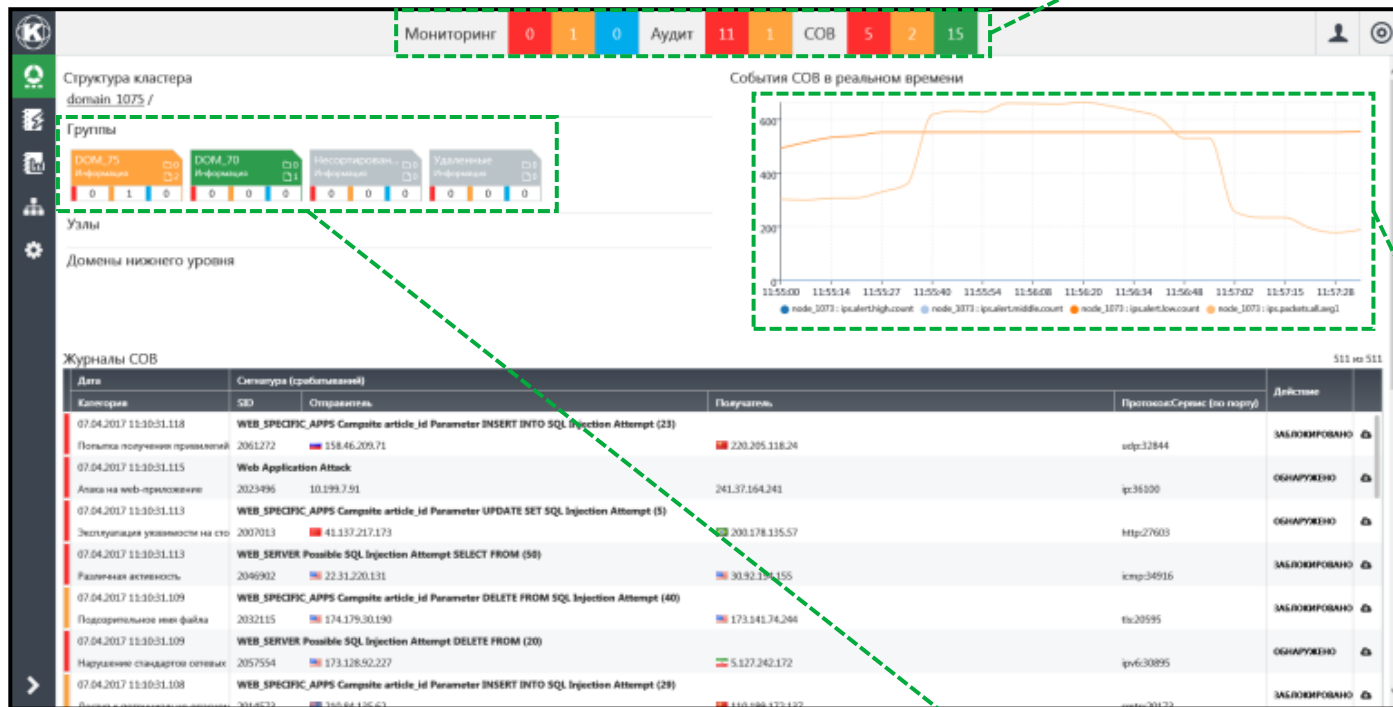
Новые консоли управления и мониторинга

**Высокопроизводительная система хранения
и обработки событий безопасности**

Ролевая модель доступа администраторов



Состояние центра управления сетью и детекторов атак



Распределение событий детекторов атак в реальном времени

Сводная информация по состоянию всей инфраструктуры COB/COA

Список событий безопасности

Мониторинг 1 1 0 Аудит 47 2 COB 5 2 15

Источник: События COB | Классификатор: [Не выбран] | Отображение: однострочное

Запрос:

и/или не по адрес отправителя адрес получателя важность действие идентификатор сигнатура интерфейс категория порт отправителя порт получателя протокол сервис сигнатура срабатываний



Дата с/по: | Группировать события:

Записей: 511 | Всего событий: 12 240 | Результаты на странице: 25 | 50 | 100

Дата	Категория	SID	Отправитель	Получатель	Протокол:Сервис (но порту)	Сигнатура (срабатываний)	Действие
07.04.2017 11:10:31.118	Попытка получения привилегий адм	2061272	158.46.209.71	220.205.118.24	udp:32844	WEB_SPECIFC_APPS Campsite article_id Parameter INSERT INTO SQL Injection At	ЗАБЛОКИРОВАНО
07.04.2017 11:10:31.115	Атака на web-приложение	2023496	10.199.7.91	241.37.164.241	ip:36100	Web Application Attack	ОБНАРУЖЕНО
07.04.2017 11:10:31.113	Эксплуатация уязвимости на стороне	2007013	41.137.217.173	200.178.135.57	http:27603	WEB_SPECIFC_APPS Campsite article_id Parameter UPDATE SET SQL Injection At	ОБНАРУЖЕНО
07.04.2017 11:10:31.113	Различная активность	2046902	22.312.220.131	30.92.154.155	icmp:34916	WEB_SERVER Possible SQL Injection Attempt SELECT FROM (50)	ЗАБЛОКИРОВАНО
07.04.2017 11:10:31.109	Подозрительное имя файла	2032115	174.179.30.190	173.141.74.244	tls:20595	WEB_SPECIFC_APPS Campsite article_id Parameter DELETE FROM SQL Injection A	ЗАБЛОКИРОВАНО
07.04.2017 11:10:31.109	Нарушение стандартов сетевых прот	2057554	173.128.92.227	5.127.242.172	ip:630895	WEB_SERVER Possible SQL Injection Attempt DELETE FROM (20)	ОБНАРУЖЕНО
07.04.2017 11:10:31.108	Доступ к потенциально опасному we	2014573	210.84.135.62	110.199.172.137	smb:20173	WEB_SPECIFC_APPS Campsite article_id Parameter INSERT INTO SQL Injection At	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.209	Возможная попытка утечки информ	2002570	121.84.180.139	1.78.12.10	tcp-pkt:23518	WEB_SPECIFC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclistings.a	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.208	TCP-соединение	2004271	104.147.232.135	81.247.237.76	tcp-stream:4564	WEB_SPECIFC_APPS Campsite article_id Parameter UPDATE SET SQL Injection At	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.206	Неизвестный трафик	2058787	151.38.48.19	26.197.235.215	ip:40230	WEB_SERVER Possible SQL Injection Attempt INSERT INTO (35)	ОБНАРУЖЕНО
07.04.2017 10:37:04.203	Потенциальное нарушение конфиде	2053108	15.107.105.69	90.87.118.245	http:4973	WEB_SPECIFC_APPS Campsite article_id Parameter INSERT INTO SQL Injection At	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.200	Подозрительная активность по прот	2026383	128.223.127.94	7.209.77.131	ip:19544	Web Application Attack (22)	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.198	Попытка проведения DoS-атаки	2053668	179.234.242.138	44.128.80.12	ssh:5082	Web Application Attack (50)	ОБНАРУЖЕНО
07.04.2017 10:37:04.197	Попытка авторизации с подозрите	2018515	99.116.182.142	205.37.53.92	smb:29197	WEB_SERVER Possible SQL Injection Attempt SELECT FROM (20)	ОБНАРУЖЕНО
07.04.2017 10:37:04.194	TCP-соединение	2012768	17.205.240.95	32.254.84.77	ssh:59563	Web Application Attack (14)	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.192	Подозрительная активность по прот	2069815	199.220.211.8	211.36.80.103	ip:36766	WEB_SPECIFC_APPS Campsite article_id Parameter DELETE FROM SQL Injection A	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.190	Попытка утечки персональные данн	2030703	58.196.112.14	104.121.66.235	pkthdr:61403	WEB_SPECIFC_APPS Campsite article_id Parameter DELETE FROM SQL Injection A	ОБНАРУЖЕНО
07.04.2017 10:37:04.189	Эксплуатация уязвимости на стороне	2051752	60.248.109.156	36.242.181.91	smb:57839	WEB_SPECIFC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclistings.a	ЗАБЛОКИРОВАНО
07.04.2017 10:37:04.185	Попытка авторизации с подозрите	2013995	25.39.4.27	85.98.81.213	tcp:oop	WEB_SERVER Possible SQL Injection Attempt INSERT INTO (27)	ОБНАРУЖЕНО

Поисковая строка -
 фильтр по событиям
 безопасности



Время последнего события	07.04.2017 11:10:31.118
в час. поясе ДА	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

Вы хотите открыть или сохранить **packet-20160418-095001.pcap** из **cdc.kodb.ru**?

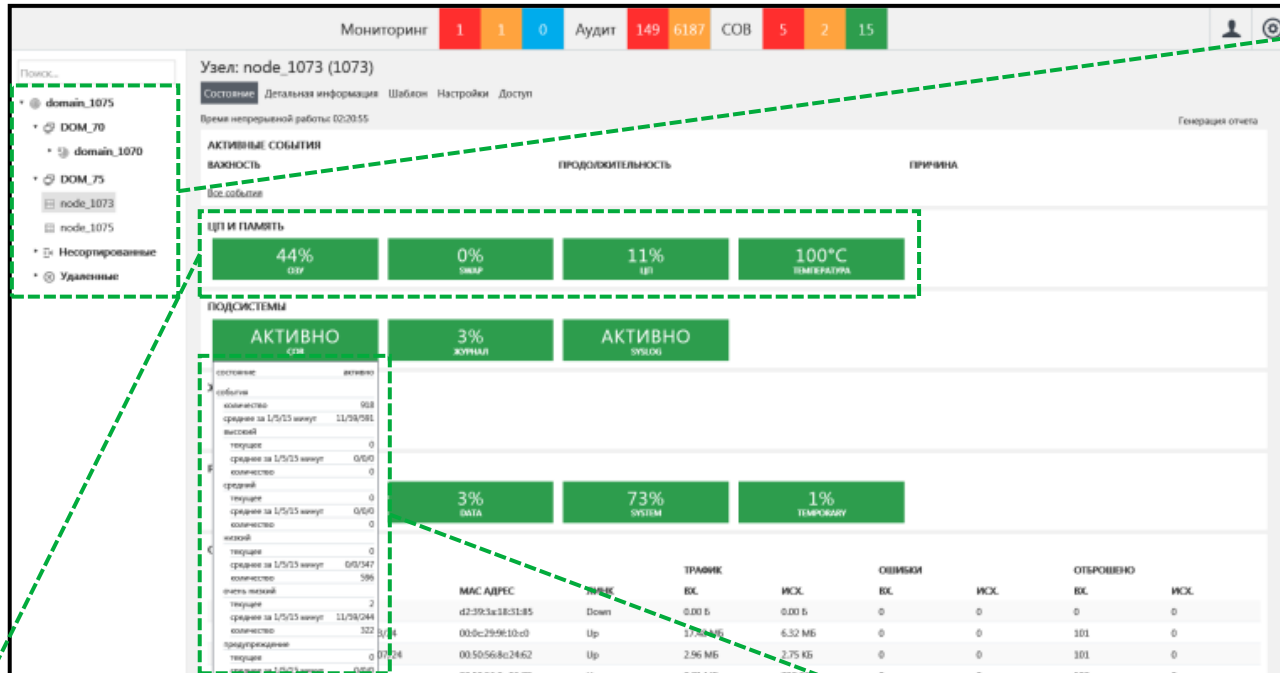
Открыть

Сохранить

Отмена



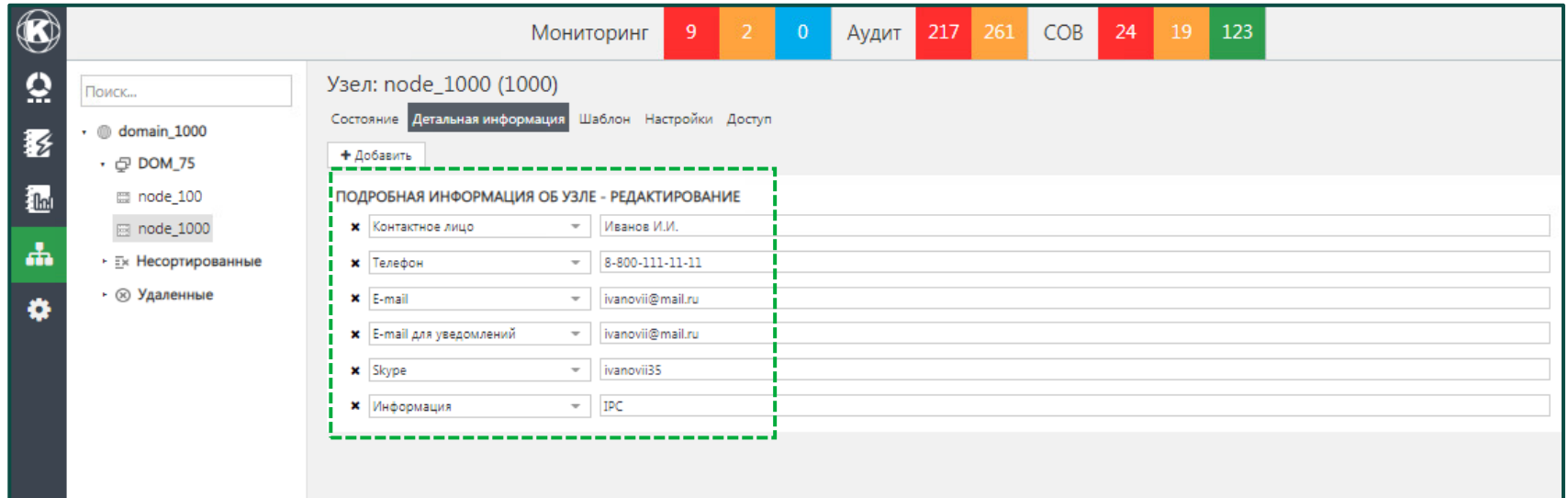




Иерархия системы управления

Уровень загрузки ресурсов Детектора атак

События подсистемы



Мониторинг 9 2 0 Аудит 217 261 СОВ 24 19 123

Поиск...

- domain_1000
 - DOM_75
 - node_100
 - node_1000
 - Несортированные
 - Удаленные

Узел: node_1000 (1000)

Состояние: **Детальная информация** Шаблон Настройки Доступ

+ Добавить

ПОДРОБНАЯ ИНФОРМАЦИЯ ОБ УЗЛЕ - РЕДАКТИРОВАНИЕ

✕ Контактное лицо	Иванов И.И.
✕ Телефон	8-800-111-11-11
✕ E-mail	ivanovii@mail.ru
✕ E-mail для уведомлений	ivanovii@mail.ru
✕ Skype	ivanovii35
✕ Информация	IPC



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)





Детектор атак

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

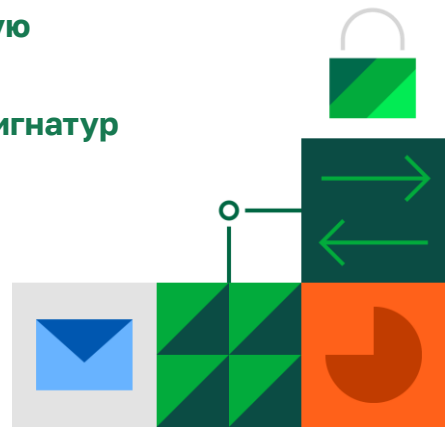
Более 25000 сигнатур в базе решающих правил

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



Правило БРП - 4104240

Общие сведения | Параметры | Сигнатура

Описание: Web Wiz Forums SQL Injection Attempt -- page.asp NewsID ASCII

Класс: Атака на web-приложение

Ревизия: 5

Ссылки

Тип	Значение
cve	CVE-2007-1548
url	www.securityfocus.com/bid/23051

Степень опасности: Высокая

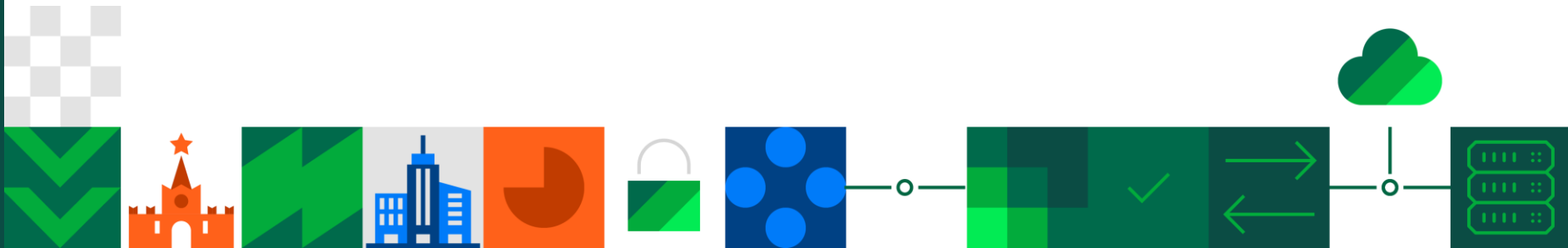
Вендор: Security Code

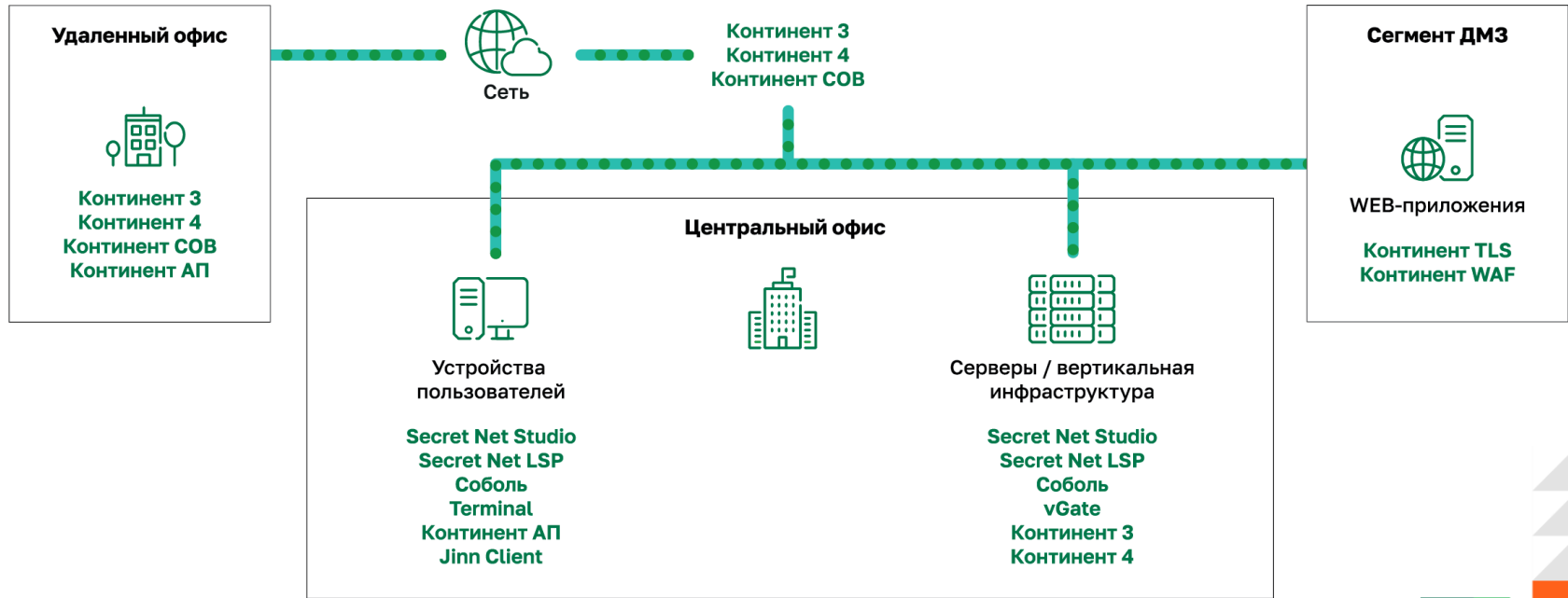
Идентификатор: 4104240

OK Отмена Применить



О компании





«Крупнейшие производители высокотехнологичного оборудования»



«Эксперт РА»



«Коммерсант»

«Крупнейшие разработчики ПО»



«Эксперт РА»



«Коммерсант»

«Крупнейшие ИТ-компании России»



«Коммерсант»



«TAdviser»

- ✓ 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**



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

Финансовые организации:



ПАО «Сбербанк»



Центральный банк Российской Федерации



ГК «Внешэкономбанк»



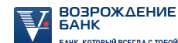
АО «Газпромбанк»



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»



РОСНЕФТ

ПАО «НК «Роснефть»

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»



КОД безопасности

info@securitycode.ru
www.securitycode.ru

