КОД безопасности

Континент СОВ/СОА

Высокопроизводительная система обнаружения и предотвращения вторжений с возможностью контроля сетевых приложений

- Предотвращение атак в режиме реального времени
- Двухуровневая система анализа трафика
- Подключение к ГосСОПКА (Континент СОА)
- Система централизованного управления
- Иерархическое управление (Континент СОВ)
- Контроль сетевых приложений
- Сигнатуры детектора атак, разработанные собственной лабораторией

Возможности

Защита от сетевых атак

- Два режима работы:
  - Обнаружение сетевых атак
  - Предотвращение сетевых атак в режиме реального времени
- Двухуровневая система анализа трафика
  - Сигнатурный анализ (более 25 000 сигнатур в базе решающих правил):
  - Анализ сетевых приложений
- Несколько типов контролируемых приложений:
  - Системы удаленного администрирования
  - Системы туннелирования трафика
  - Торренты
  - Социальные сети
  - Мессенджеры
- Автоматическое обновление базы решающих правил с серверов «Кода Безопасности»
- Сигнатуры детектора атак, разработанные собственной лабораторией

Управление и мониторинг

- Иерархическое управление (только для 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
- Мониторинг событий в режиме реального времени
- Ролевая модель доступа администраторов
- Высокопроизводительная система хранения и обработки событий безопасности
- Дистанционное обновление компонентов комплекса (системного ПО и базы решающих правил)
- Гибкая система отчетов
- Экспорт событий безопасности во внешние системы мониторинга и управления ИБ

Отказоустойчивость

- Гибкая интеграция в сетевую инфраструктуру:
  - Установка в режиме мониторинга
  - Установка «в разрыв»

Сценарии применения

Обнаружение сетевых атак в территориально распределенных сетях

Результат:

- Защита от атак на критичные ресурсы в крупных территориально распределенных сетях
- Распределение полномочий между главным администратором и администраторами на местах
- Сквозной мониторинг всей инфраструктуры обнаружения сетевых вторжений
- Оптимизация затрат на развертывание и эксплуатацию комплексной системы обнаружения вторжений

Обнаружение сетевых атак в высоконагруженных сетях

Результат:

- Обнаружение атак в сетях с производительностью 10 Гбит/с

Соответствие требованиям регуляторов

Результат:

- Защита информационных систем в соответствии требованиям приказов ФСТЭК России № 17, № 21 и № 31
- Подключение к ГосСОПКА (только для Континент СОА)

Модельный ряд

Детектор атак

Характеристики	IPC-50	IPC-500F	IPC-800F	IPC-1000NF2	IPC-3000F
Интерфейсы	4x 1000BASE-T RJ45 1x 1G SFP	8x 1000BASE-T RJ45 2x 1G SFP	8x 1000BASE-T RJ45 4x 1G SFP	8x 1000BASE-T RJ45 8x 1G SFP 4x 10G SFP+	1x 1000BASE-T RJ45 8x 1G SFP 4x 10G SFP+
Континент СОВ					
Производительность в режиме IDS, Мбит/с	до 300	до 700	до 1 000	до 4 000	до 7 200
Производительность в режиме IPS, Мбит/с	до 150	до 350	до 750	до 2 000	до 4 200
Континент СОА					
Производительность в режиме IDS, Мбит/с	до 700	до 800	до 1 000	до 4 000	до 8 000
Производительность в режиме IPS, Мбит/с	до 150	до 350	до 750	до 2 000	до 4 000

Центр управления сетью

Характеристики	IPC-50M	IPC-500M	IPC-1000FM	IPC-3000FM
Интерфейсы	4x 1000BASE-T RJ45 1x 1G SFP	6x 1000BASE-T RJ45	8x 1000BASE-T RJ45 8x 1G SFP	1x 1000BASE-T RJ45 8x 1G SFP 4x 10G SFP+
Континент СОВ				
Производительность ЦУС (количество управляемых Континент СОВ)	до 20	до 40	до 100	до 150
Континент СОА				
Производительность ЦУС (количество управляемых Континент СОА)	до 20	до 40	до 100	до 150

Сертификаты

ФСТЭК России (Континент СОВ)
- 3-й класс защиты СОВ уровня сети
- 3-й уровень доверия

ФСТЭК России (Континент СОА)
- система обнаружения компьютерных атак класса ВП

Техническая поддержка

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Каталог услуг	Пакет поддержки			
	Базовый	Стандартный	Расширенный	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**