КОД безопасности

КОНТИНЕНТ СОВ

Система предотвращения вторжений с иерархическим управлением и контролем сетевых приложений

ПРЕИМУЩЕСТВА

- ПРЕДОТВРАЩЕНИЕ АТАК В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ
- ДВУХУРОВНЕВАЯ СИСТЕМА АНАЛИЗА ТРАФИКА
- ПРОИЗВОДИТЕЛЬНОСТЬ ДО 10 ГБИТ/С
- РАЗВИТАЯ СИСТЕМА ЦЕНТРАЛИЗОВАННОГО ИЕРАРХИЧЕСКОГО УПРАВЛЕНИЯ
- КОНТРОЛЬ СЕТЕВЫХ ПРИЛОЖЕНИЙ
- СОБСТВЕННАЯ ЛАБОРАТОРИЯ ПО РАЗРАБОТКЕ СИГНАТУР

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»
- Собственная лаборатория, разрабатывающая сигнатуры

ОТКАЗОУСТОЙЧИВОСТЬ

- Отказоустойчивый кластер
- Производительность в кластере до 10 Гбит/с
- Гибкая интеграция в сетевую инфраструктуру:
  - Установка в режиме мониторинга
  - Установка «в разрыв»

УПРАВЛЕНИЕ И МОНИТОРИНГ

- Иерархическое управление:
  - 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

СЦЕНАРИИ ПРИМЕНЕНИЯ

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННЫХ СЕТЯХ

Результат:

- Защита от атак на критичные ресурсы в крупных территориально распределенных сетях
- Обнаружение несанкционированного использования сетевых приложений
- 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
- Обнаружение несанкционированного использования сетевых приложений

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Результат:

- Защита информационных систем в соответствии требованиям приказов ФСТЭК России № 17, № 21 и № 31

МОДЕЛЬНЫЙ РЯД

МОДЕЛЬ	IPC-50	IPC-500F	IPC-800F	IPC-1000NF2	IPC-3000F
					
Производительность в режиме IDS, Мбит/с	до 300	до 700	до 1 000	до 4 000	до 7200
Производительность в режиме IPS, мбит/с	до 150	до 350	до 750	до 2 000	до 4 200
Интерфейсы	4x Ethernet 10/100/1 000 1x Gigabit Ethernet Fiber SFP	8x Ethernet 10/100/1 000 2x Gigabit Ethernet Fiber SFP	8x Ethernet 10/100/1000 4x Gigabit Ethernet Fiber SFP	8x Ethernet 10/100/1000 8x Gigabit Ethernet Fiber SFP 4x 10G Ethernet Fiber SFP+	1x Ethernet 10/100/1000 8x Gigabit Ethernet Fiber SFP 4x 10G Ethernet Fiber SFP+

МОДЕЛЬ	IPC-50M	IPC-500M	IPC-1000FM	IPC-3000FM
				
Производительность ЦУС (количество подконтрольных устройств)	до 20	до 40	до 100	до 150

СЕРТИФИКАТЫ

ФСТЭК России

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

Континент СОВ может использоваться для защиты:

- АС до класса 1В включительно (защита гостайны с грифом «секретно»)
- ИСПДн до УЗ1 включительно
- ГИС до 1 класса включительно
- АСУ ТП до 1 класса включительно

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.
Существует несколько пакетов технической поддержки:


Базовый


Стандартный


Расширенный


VIP

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