

Monitoring System Stats Browser Event Source Monitoring Settings							
Event Source	Event Source Type	Log Collector	Log Decoder	Time Frame	Order By		
[0-9.]{1,100}	ciscorouter	Any		Last 48 hours	Any	Apply	Cle
<input checked="" type="checkbox"/> Regex				<input checked="" type="radio"/> Received <input type="radio"/> Not Received	<input checked="" type="radio"/> Ascending <input type="radio"/> Descending		
Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Histor
	ciscorouter			967	22 hours, 38 min	2015-03-26 04:45:27 ...	
	ciscorouter			243	1 days, 6 hours, 38 min	2015-03-26 08:45:34 ...	
Page 1 of 3							
Items 1 - 50 of 130							

Monitoring System Stats Browser Event Source Monitoring Settings							
Event Source	Event Source Type	Log Collector	Log Decoder	Time Frame	Order By		
	winevent_nic	Any	Any	Any	Any	Apply	Cle
<input checked="" type="checkbox"/> Regex				<input checked="" type="radio"/> Received <input type="radio"/> Not Received	<input checked="" type="radio"/> Ascending <input type="radio"/> Descending		
Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Histor
	winevent_nic			288339	43 days, 16 hours, 48 ...	2015-02-11 10:38:26 ...	
	winevent_nic			3019413	4 min	2015-03-27 03:22:22 ...	
Page 1 of 5							
Items 1 - 50 of 208							

В рамках проекта проведены следующие работы:

- установка компонентов в серверные стойки, коммутация, инициализация компонентов (в составе системы используются три аппаратных сервера)
- обновление программного обеспечения до последней версии
- создание пользователей, разграничение прав доступа пользователей
- консультирование персонала Заказчика по администрированию и настройке системы
- формирование информационных панелей с учетом требований Заказчика
- разработка инструкций по подключению и контроль подключения источников событий с выявлением ошибок в настройках
- разработка фильтров для событий и сетевых пакетов для экономии объемов жесткого диска
- разработка отчетов, правил, уведомлений под требования заказчика
- подготовка проектной документации

В результате внедрения системы заказчик получил:

- видимость событий со средств защиты информации в «одном окне»
- уведомление о наиболее критичных событиях ИТ-инфраструктуры на электронную почту
- формирование ретроспективных выборок (отчетов) по критичным категориям событий
- отслеживание действий определенных категорий пользователей
- отслеживание действий над определенными объектами в ИТ-инфраструктуре
- сокращение времени реакции на события в ИТ-инфраструктуре
- понимание структуры сетевого трафика и дополнительный канал визуализации действий сотрудников и/или внешних нарушителей