

INFOWATCH ARMA INDUSTRIAL FIREWALL 3.12

What's new

В версии 3.12 появилась поддержка протоколов Fanuc Focas, ENIP / CIP, DNP3 и LLDP, интеграция с антивирусом Dr. Web. Появилась возможность принудительного разрыва сессии TCP / ICMP в технологиях АСУ ТП с непрерывной передачей данных. Настройка межсетевого экрана стала более гибкой.

Новые возможности

Промышленные протоколы Fanuc Focas, ENIP / CIP и DNP3

Заголовок	Fanuc FOCAS test rule	ENIP/CIP test rule	DNP3 test rule
Группа			
Использовать шаблон	Fanuc FOCAS	ENIP/CIP	DNP3
Действие	Предупредить (Alert)	Предупредить (Alert)	Предупредить (Alert)
Сообщение	Fanuc FOCAS test rule	ENIP/CIP test rule	DNP3 test rule

Появились шаблоны создания правил для промышленных протоколов Fanuc Focas, ENIP / CIP и DNP3. Фильтрация по перечисленным протоколам позволяет разрешать и запрещать команды, поступающие на промышленное оборудование, настраивать уведомления (Alert).

Антивирус Dr. Web Gateway Security Suite

Работает с прокси-сервером через плагин C-ICAP и проверяет файлы на наличие вредоносного кода. Появились возможности гибко настраивать уровень детектирования, категоризировать веб-ресурсы и регулярно обновлять базы сигнатур.

Поддержка протокола LLDP

Включите сервис LLDP	<input checked="" type="checkbox"/>	Это запускает сервис LLDP.
Включить CDP	<input type="checkbox"/>	Установленный флажок активирует протокол Cisco Discovery.
Включить FDP	<input type="checkbox"/>	Установленный флажок активирует протокол Foundry Discovery.
Включить EDP	<input type="checkbox"/>	Установленный флажок активирует протокол Extreme Discovery.

Теперь InfoWatch ARMA Industrial Firewall обменивается информацией с устройствами сети о своём существовании и статусе по протоколу LLDP.

Он собирает аналогичную информацию от соседних устройств сети. Информация накапливается в устройствах и может запрашиваться через протокол SNMP, что делает сеть более стабильной и упрощает процесс построения топологии сети.

Разрыв сессии TCP / ICMP при срабатывании правила

Возможность принудительного разрыва сессии при срабатывании запрещающего правила межсетевого экрана.

Журналирование	<input type="checkbox"/> Журналировать пакеты, соответствующие правилу
Разрывать сессию	<input checked="" type="checkbox"/> Разрывать сессию, когда правило сработало
Категория	<input type="text"/>
Описание	<input type="text"/>

Это актуально для технологий АСУ ТП с непрерывной передачей данных, в которых сессия никогда не разрывается.

Другие улучшения

Последние		Настройки GeoIP	
Последнее обновление	2024-02-13T07:35:38	Время последнего обновления. Это время, когда списки были созданы.	
Совокупное количество диапазонов	504553	Совокупное число записей в указанном наборе	
URL	<input type="text"/>	Откуда брать диапазоны geoIP адресов.	

- Появилась возможность сброса Alias в GeoIP

- Теперь восстановление IPsec-тоннеля после длительной недоступности второго участка соединения происходит автоматически

Транспортный протокол	UDP(4)
Формат	SYSLOG
Приложения	Обнаружение вторжений (snort), Обнаружение
Уровни	<input type="text"/>
Категории	<ul style="list-style-type: none"> Кширующий DNS-сервер (unbound) Маршрутизация (bgpd) Маршрутизация (miniptrrd) Маршрутизация (ospf) Маршрутизация (ospfd) Маршрутизация (routed) Маршрутизация (routed) Маршрутизация (routed) Маршрутизация (zebra)
Имя хоста	
Порт	
Описание	

- Стало доступно описание экспортируемых приложений и категорий

- Появилась возможность экспорта журнала в разделе «Анализ трафика» в форматах .pcap и .csv и журнала предупреждений системы обнаружения вторжений в .pdf и .csv