

INFOWATCH ARMA INDUSTRIAL FIREWALL 3.10

What's new

Новые возможности

Промышленные протоколы

Использовать шаблон	ADS
Действие	Предупредить (Alert)
Сообщение	
IP-адрес отправителя	any
Порт источника	any
Выберите направление	Прямое
IP-адрес получателя	any
Порт назначения	48898
Фильтровать на основе протокола	Указать дополнительные параметры
Тип Транспорта	TCP
Тип условия AMS Target Net Id	Значение
Значение AMS Target Net Id	
Значение AMS Target port	<input type="checkbox"/> Укажите значение Dec
Тип условия AMS Source Net Id	Значение
Значение AMS Source Net Id	
Значение AMS Source port	<input type="checkbox"/> Укажите значение Dec

Тип запроса	CALL
Тип идентификатора узла вызываемого объекта	GUID тип
Значение идентификатора узла вызываемого объекта	Отсутствует
Тип идентификатора узла вызываемого метода	GUID тип

Сообщение	test 1
IP-адрес отправителя	any
Порт источника	any
Выберите направление	Прямое
IP-адрес получателя	any
Порт назначения	502
Фильтровать на основе протокола	Указать дополнительные параметры
Совпадение по	Данные
Идентификатор устройства	<input type="checkbox"/> 5 Dec

- Добавлен шаблон создания правил для промышленного протокола ADS Beckhoff, позволяющий указать команды, необходимые для детектирования. Фильтрация по протоколу ADS Beckhoff позволяет контролировать (разрешить / запретить) команды, поступающие по этому протоколу на промышленное оборудование Beckhoff или настроить получение уведомлений (Alert)
- В шаблон для протокола OPC UA добавлены новые параметры настройки детектирования. Для запроса типа CALL разрешается установить идентификатор узла вызываемого объекта GUID или Numeric
- В шаблон для протокола Modbus добавлена возможность фильтрации правил по Unit ID. Это позволит заблокировать команду на одном конкретном устройстве в случае, если за одним IP-адресом несколько устройств

Иные улучшения

Режим midstream	<input type="checkbox"/>
-----------------	--------------------------

Обнаружение на уровне приложения в середине TCP потока, т.е. без предварительного обнаружения рукопожатий (3WHS)

- Добавлена настройка, позволяющая проверять пакеты TCP-сессии без обнаружения «рукопожатий»

Включить
 Заголовок: rdp inverse
 Группа:
 Использовать шаблон: RDP
 Действие: Предупредить (Alert)
 Сообщение: rdp inverse
 IP-адрес отправителя: any
 Порт источника: any
 Выберите направление: Прямое
 IP-адрес получателя: any
 Порт назначения: 3389
 Фильтровать на основе протокола: Указать дополнительные параметры
Инвертировать правило: Да
 Значение RDP Cookie: user

- Возможность инвертировать правило фильтрации по протоколу RDP

Инструменты
 Создание отчетов
 Мексетевой экран
 Обнаружение вторжений
 Система
 Интерфейсы
 Сеть
 Маршрутизация
 Службы
 VPN
 IPsec
 OpenVPN
 Серверы
 Клиенты
 Переопределение значений для конкретного клиента
 Экспорт настроек клиента
 Статус соединения
Конфигурация

VPN: OpenVPN: Конфигурация

```

server1.conf
dev ovpn1
verb 1
dev-type tun
tun-ipv6
dev-node /dev/tun1
writepid /var/run/openvpn_server1.pid
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-256-CBC
auth RSA-SHA256
up /usr/local/etc/inc/plugins.inc.d/openvpn/ovpn-linkup
down /usr/local/etc/inc/plugins.inc.d/openvpn/ovpn-linkdown
log-append /var/log/openvpn/openvpn-server-1.log
multihome
ifconfig 10.0.10.1 10.0.10.2
lport 1194
management /var/etc/openvpn/server1.sock unix
push "route 192.168.41.0 255.255.255.0"
secret /var/etc/openvpn/server1.secret

server2.conf
dev ovpn2
verb 1
dev-type tun
tun-ipv6
dev-node /dev/tun2
writepid /var/run/openvpn_server2.pid
script-security 3
daemon
keepalive 10 60
  
```

- Возможность просмотра через веб-интерфейс конфигурационного файла настроенного OpenVPN сервера или клиента

- Поддержка модуля IPMITool, позволяющая подключаться, управлять, конфигурировать и вести мониторинг аппаратной части файрвола