Интегрированное решение для активной киберзащиты систем SCADA

Павел Гирак, Юрий Макуха / ООО «СОЛИТОН» (Киев)

Задачи киберзащиты промышленных систем управления (ICS) и систем SCADA находятся на стыке информационных технологий (IT) и производственных технологий (OT). Системы киберзащиты ICS/SCADA основаны на системах сетевого мониторинга с глубоким анализом промышленных протоколов передачи данных, и, как правило, являются пассивными и прозрачными для данных промышленной сети передачи данных. Если в процессе работы возникают аномалии, они детектируются сенсорами системы, регистрируются командным центром и могут быть визуализированы через клиентское приложение.

Операторы системы SCADA выполняют контроль и управление технологическим процессом, в их функции обычно не входят вопросы кибербезопасности и кибезащиты, однако им критически важно иметь информацию о попытках несанкционированного доступа к серверу SCADA, контроллерам, или аномалиях в работе системы управления, сети передачи данных на уровне журналов событий и тревог системы SCADA, поскольку эти аномалии могут влиять на надежность и устойчивость технологического процесса.

Кроме того, для повышения функциональности и надежности киберзащиты системы SCADA, важно автоматически выполнить действия по блокированию нежелательного IP адреса, с которого выполняются подозрительные действия, и предоставить оператору системы SCADA информацию о возможной атаке и действиях, необходимых для ее нейтрализации.

Такие возможности предоставляет интегрированное решение на основе системы SilentDefense, межсетевого экрана Firewall и программных модулей [1] и [2] (рис.1).

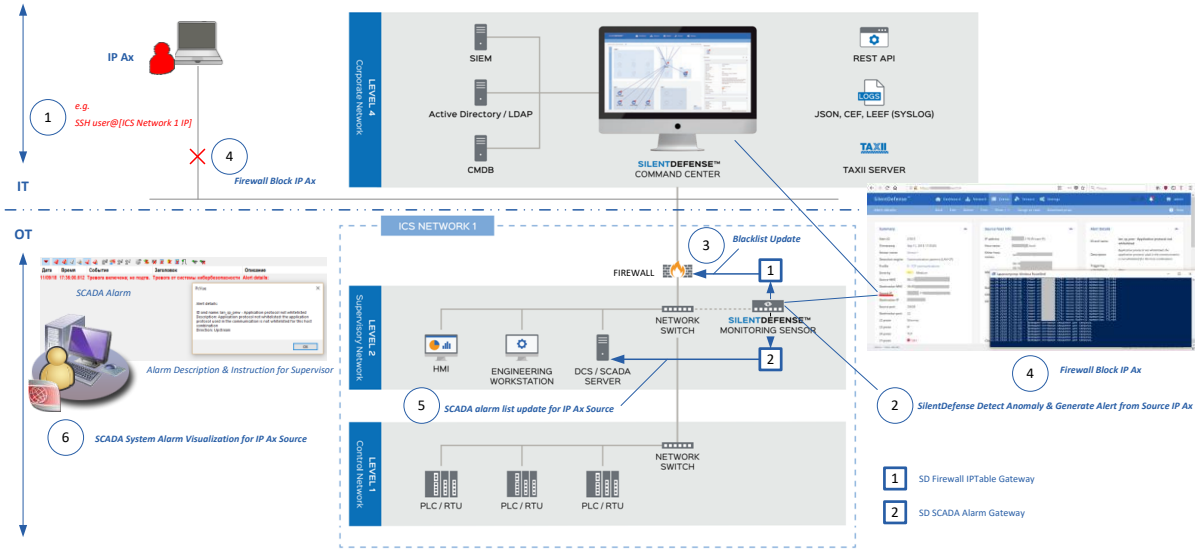

Рис.1. Пример архитектуры платформы SilentDefense для защиты системы SCADA

Если система SilentDefense определяет угрозу со стороны IP устройства, она генерует тревогу, на основе которой программный модуль [1] SD Firewall IPTable Gateway автоматически добавляет адрес такого IP устройства в список заблокированных адресов Firewall (blacklist).

При этом программный модуль [2] SD SCADA Alarm Gateway автоматически обеспечивает запись тревожного сообщения в журнал тревог системы SCADA и его визуализацию. Оператор получает тревожное сообщение, поступившее от системы киберзащиты, его краткое описание и инструкцию о необходимых действиях на дисплее рабочей станции системы SCADA. После просмотра и подтверждения данного сообщения оператор может выполнить необходимые процедуры для обеспечения безопасности системы управления.

Тестирование решения выполнено на стенде с платформой SilentDefense, Firewall и системой SCADA PcVue (рис.1).

Если адрес [IP Ax, в примере x.x.x.179] удаленного удаленного компьютера отсутствует в списке правил SilentDefense (White List), при попытке обращения с [IP Ax] к IP устройству в сети управления [ICS NETWORK 1] по протоколу SSH (рис.1 (1)), сенсор SilentDefense определяет аномалию от источника [IP Ax] и генерирует тревогу (рис.1 (2)). Эта тревога отображается в списке тревог командного центра SilentDefense.

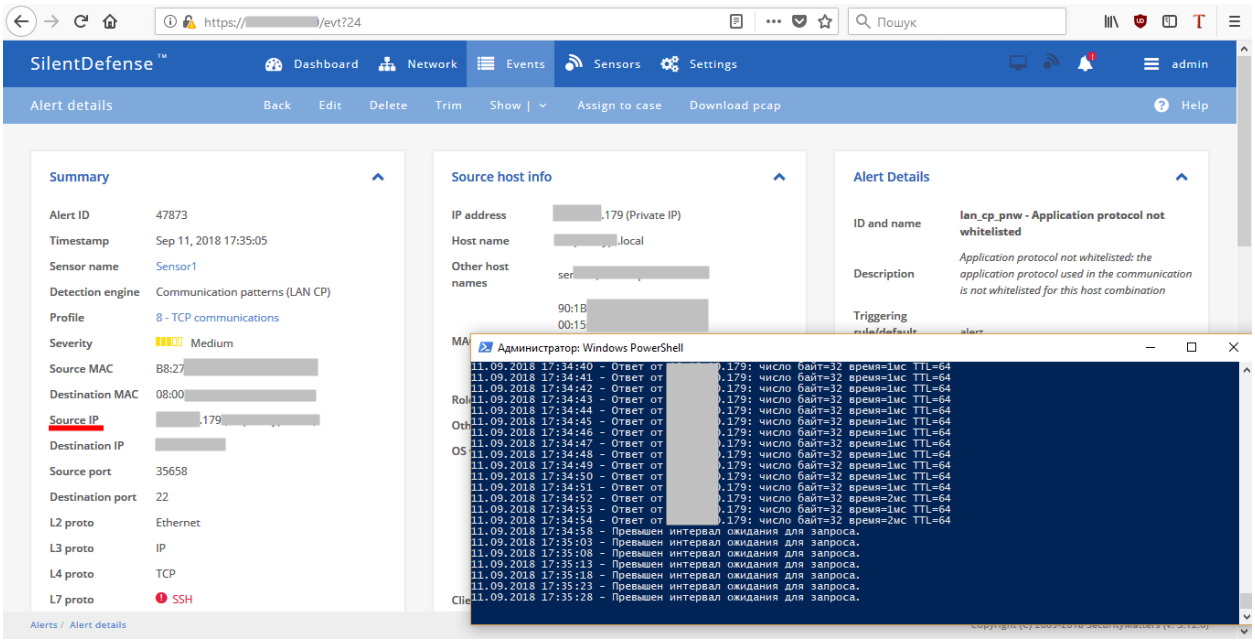

Рис.2 Окно тревоги SilentDefense и окно с ping IP Ax до и после блокировки его Firewall

Программный модуль [1] автоматически добавляет [IP Ax] в BlackList межсетевого экрана Firewall (рис.1 (3)), после чего доступ к сети [ICS NETWORK 1] для устройства [IP Ax] будет заблокирован (рис.1 (4)).

Программный модуль [2], получает список событий от сенсора SilentDefense и вносит запись о тревоге системы SilentDefense в журнал системы SCADA (рис.1 (5)).

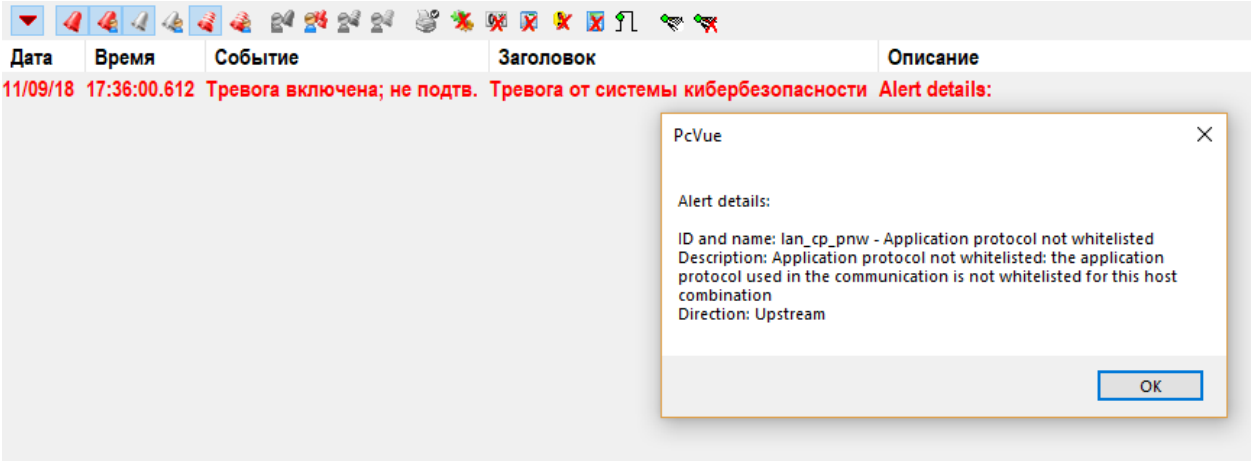

Рис.3 Окно журнала тревог системы SCADA PcVue с сообщением от платформы SilentDefense

Оператор системы SCADA получает сообщение о тревоге (рис.3) на дисплее операторского терминала (рис.1 (6)). Он может просмотреть детальную информацию о тревоге и предпринять необходимые действия по реагированию на нее. Действия оператора регистрируются в базе данных системы SCADA. При программировании системы SCADA можно также настроить в деталях сообщения инструкции по действиям оператора в случае получения тревоги от системы кибербезопасности. После этого можно провести анализ тревоги и предпринять необходимые действия по ее устранению.

Таким образом, автоматическое блокирование IP адреса источника тревоги, регистрация события в журнале тревог системы SCADA, уведомление оператора системы SCADA о тревоге и предоставление ему инструкций о необходимых действиях, позволяет повысить надежность и устойчивость работы системы управления.

Источники:

1. https://www.secmatters.com/hubfs/Security_Matters-March2017/PDF/Solution-Brief-SecurityMatters-and-Phoenix-Contact.pdf