Центр безопасности Ovation™

Описание

Характеристики

- Сканирование на наличие уязвимостей.
- Обнаружение ресурсов.
- Прозрачное применение исправлений безопасности (патчей).
- Позволяет запускать на рабочих станциях только разрешенные приложения.
- Обеспечивает защиту рабочих станций на базе Ovation для Windows® от вирусов.
- Собирает, нормализует и соотносит события для идентификации проблем безопасности.
- Хранит журналы для анализа инцидентов и проверки целостности.
- Проверяет пакеты данных, проходящих через границы системы Ovation.
- Создание резервных образов и восстановление системы Ovation.
- Поддержка операционных платформ Ovation Windows® и Solaris™ (ограниченно).
- Поддержка кибер-безопасности нескольких систем управления Ovation.

Введение

Центр безопасности Ovation™ (OSC) представляет собой набор функций безопасности по управлению кибербезопасностью и повышению надежности распределенной системы управления Ovation без ущерба для контролируемого процесса.

Эти средства защиты специально были выбраны за их способность повышать надежность системы безопасности, снижая затраты на соответствие стандартам Североамериканской корпорации по обеспечению надежности электросистем (NERC) для защиты критической инфраструктуры (CIP).

Возможности решений по автоматизации процедур, которые в настоящее время выполняются вручную, а также способность встраиваться в системы управления в режиме реального времени дают клиентам Ovation значительные преимущества в обеспечении безопасности системы.

Кроме выполнения стандартов NERC CIP функции OSC повышают надежность и готовность к работе всей станции благодаря грамотной реализации управления безопасностью в системе управления. OSC состоит из функций безопасности, которые имеют важнейшее значение для бесперебойной работы оборудования и которые разрабатываются исходя из приоритетов клиента в отношении безопасности.

Комплексные аппаратные/программные решения OSC объединены в корпусе с сетевым интерфейсом для подключения к системе управления Ovation. Управление всеми представленными функциями безопасности осуществляется из-за периметра безопасности, предоставляя отдельную демилитаризованную зону (DMZ), обеспечивающую максимальную целостность, гибкость и безопасность.

OSC выполняет все административные функции, функции контроля и ведения отчетов, а также предоставляет возможности локального и/или удаленного просмотра данной информации через стандартные веб-браузеры.

Компания Emerson организует инфраструктуру технической поддержки, необходимую для функционирования приложения OSC. В нее входят регулярные функциональные проверки ПО и обновление для обеспечения совместимости с различными версиями Ovation. Инфраструктура технической поддержки включает в себя организацию веб-сайта поддержки пользователей для распространения обновлений.

Компоненты центра безопасности Ovation

Оценка уязвимостей (Vulnerability Assessment)

Функция оценки уязвимостей OSC опирается на CIP-010-1 «Управление изменением конфигураций и оценки уязвимостей», раздел R3 «Оценка уязвимостей».

Функция оценки уязвимостей обеспечивает централизованную идентификацию оборудования и оценку уязвимостей систем Ovation. Она представляет собой работающее напрямую с системой сетевое решение для сканирования, которое выполняет всестороннюю проверку всех устройств в сети Ovation, включая серверы, рабочие станции, маршрутизаторы, принтеры и коммутаторы. Задачей сканирования является обнаружение устройств в сети и идентификация их уязвимостей, таких как отсутствующие пакеты обновлений, а также устранение уязвимостей до того, как они могут быть использованы злоумышленниками.

Оценка уязвимостей также может выполнять подробные проверки конфигурации, в ходе которых анализируется количество портов, пользователей, групп, общих ресурсов, агентов и служб. Уведомление о связанных со сканированием событиях и мерах по устранению найденных проблем могут рассылаться по SNMP или электронной почте.

Менеджер оценки уязвимостей работает в виртуальной среде и обменивается зашифрованными данными с браузером клиента.

Преимущества оценки уязвимостей

- Автоматическое обнаружение всех сетевых устройств, операционных систем и инфраструктуры.
- Выполнение специального сканирования конкретной одной или нескольких машин.
- Предоставление информации об обнаруженных уязвимостях, ущербе для организации и о необходимых для их устранения действиях.
- Сканирование по расписанию.

Управление исправлениями (Patch Management)

Функция управления исправлениями в OSC соответствует CIP-007-5 «Управление безопасностью систем», раздел R2 «Управление исправлениями безопасности».

Функция управления исправлениями обеспечивает централизованный механизм распространения исправлений для рабочих станций Ovation на базе Microsoft® Windows® и Sun™ Solaris™.

Данная функция генерирует всесторонний централизованный обзор статуса установки исправлений в системе Ovation, что достигается с помощью сканирования клиентским приложением каждой отслеживаемой конечной точки. Графическая информационная панель, содержащая более 20 стандартных отчетов, отражает текущий статус исправлений, историю применения исправлений, тренды, имеющиеся ресурсы и множество другой информации, представленной на уровне отдельной машины или на общем уровне. Данная информация встраивается в функции управления инцидентами и событиями безопасности для обеспечения соответствия требованиям по отчетности.

Функция управления исправлениями способна применять обновления безопасности для подчиненных операционных систем и выбранных встроенных приложений сторонних разработчиков. Применение исправлений происходит автоматически в соответствии с настраиваемой пользователем политикой распространения. Загрузка исправлений инициируется OSC и выполняется через модуль поддержки центра безопасности Ovation SureService™ компании Emerson.

Можно запланировать автоматический запуск установки исправлений, но обычно для вступления изменений в силу требуется перезагрузка рабочей станции.

Менеджер функции управления пакетами обновлений работает в виртуальной среде и использует клиент, устанавливаемый на каждую управляемую рабочую станцию и позволяющий выполнять удаленную установку обновлений ПО.

Преимущества управления исправлениями

- Позволяет обрабатывать все исправления, выполнять автоматическое сканирование и доступ к сканеру.
- Позволяет выполнять по графику обработку нескольких компьютеров/исправлений.
- Возможность обновления операционных систем нескольких типов.
- Возможность автоматической или ручной перезагрузки каждой рабочей станции после применения обновлений.

Предотвращение запуска вредоносного ПО (Malware Prevention)

Функция предотвращения запуска вредоносного ПО в составе OSC опирается на требования CIP-007 «Управление безопасностью систем», раздел R4 «Предотвращение запуска вредоносных программ».

Данная функция обеспечивает централизованное конфигурирование и управление защитным клиентским приложением, которое устанавливается на каждой хост-станции Ovation. Если имя исполняемого файла отсутствует в списке доверенных программ, программное обеспечение ограничивает запуск этого исполняемого файла, помещая его в «карантин».

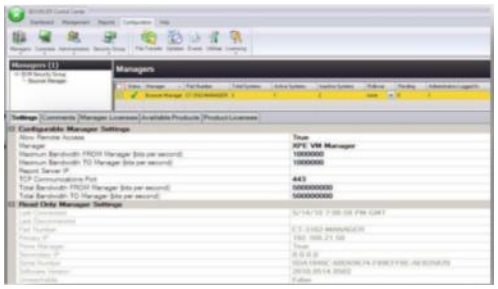
ПО для предотвращения исполнения вредоносного кода вносит в журнал все заблокированные приложения и предлагает опцию стирания, с помощью которой администратор может удалить приложение с клиентского ПК.

Функция предотвращения запуска вредоносного ПО предлагает уникальный подход для защиты рабочих станций Ovation от вирусов, червей и троянских программ. Вместо регулярных обновления черного списка и предположений, что все вторжения были остановлены, данное ПО использует список доверенных программ на уровне ядра в каждой оконечной рабочей станции, что упрощает работу и эффективно блокирует выполнение любых несанкционированных исполняемых файлов. Если исполняемый файл отсутствует в списке, он не будет запущен. ПО защищает от проникновений с четырех фронтов:

1. Напрямую защищает от вредоносного ПО и других угроз путем предотвращения их выполнения.
2. Ограничивает привилегии пользователей.
3. Не дает конечным пользователям изменять одобренную и проверенную конфигурацию системы.
4. Перехватывает любое подозрительное поведение (например, лазейки в памяти, такие как DLL-инъекции) и исследует другие механизмы, которые используются злоумышленниками.

Менеджер функции предотвращения запуска вредоносного ПО работает в виртуальной среде и использует клиентское приложение, которое интегрируется в ядро каждой защищаемой рабочей станции. Это позволяет защищать рабочую станцию от вторжений в память (даже если они выполняются с помощью одобренных приложений) и выполнять проверки целостности, включая контрольную-сумму, расположение файла и его размер.

События срабатывания защиты от вредоносного ПО вносятся в отчет и передаются функции управления инцидентами и событиями центра безопасности Ovation в качестве событий безопасности. Для управления работой и соответствия требованиям правил доступны стандартные отчеты по предотвращению запуска вредоносного ПО.



Преимущества предотвращения запуска вредоносного ПО

- Отсутствие вредоносного ПО, условно вредоносного ПО или неавторизованных исполняемых файлов, снижающих безопасность, производительность или готовность оборудования.
- Защита от несанкционированного вмешательства предотвращает несанкционированный доступ и атаки, защищая пользователей от вредоносного ПО, которое попытается отключить защиту.
- Упрощает выполнение требований норм и правил.
- Обеспечивает превентивную защиту от целенаправленных атак.

Антивирусная защита

Функция антивирусной защиты OSC опирается на требования CIP-007-5 «Управление безопасностью систем», раздел R3 «Предотвращение запуска вредоносного кода».

Данная функция обеспечивает защиту от вирусов в режиме реального времени на основе известных сигнатур вредоносного ПО. Сигнатуры тестируются еженедельно и публикуются компанией Emerson. Целями защиты являются рабочие станции на базе Windows, которые более уязвимы для вирусных атак.

Защита более эффективна, когда устройства в составе рабочих станций, такие как дисковые накопители, порты USB или приводы CD/DVD, находятся под жестким контролем или имеют ограниченный доступ. При заблокированном доступе содержащие вирус файлы не могут быть перенесены на рабочую станцию со съемных носителей. Такая мера еще более повышает защиту от потенциальной кражи информации при несанкционированной передаче файлов.

Менеджер функции антивирусной защиты работает в виртуальной среде и использует клиент, устанавливаемый на каждую управляемую рабочую станцию и позволяющий выполнять удаленную установку обновлений ПО.

Преимущества антивируса

- Проверенная технология.
- Простота развертывания.
- Доступная цена.
- Защита устройства от основных угроз.

Управление инцидентами и событиями безопасности (Security Incident & Event Management)

Функция управления инцидентами и событиями безопасности в составе OSC обеспечивает централизованные механизмы сбора и сопоставления данных, что ускоряет анализ и регистрацию состояния обеспечения безопасности системы Ovation.

Функция собирает и стандартизует все события и журналы, переданные различными имеющимися в системе брандмауэрами, системами обнаружения вторжения, ПО для защиты от вредоносных программ, сканерами уязвимостей, сетевыми устройствами, рабочими станциями и активными директориями. Данные действия опираются на CIP-007 «Управление безопасностью систем», раздел R6 «Мониторинг статуса системы безопасности».

Кроме того, данная функция упрощает работу с большими объемами разнородных данных с целью обнаружения проблем безопасности. Функция управления событиями анализирует подробные данные и предоставляет необходимый контекст. Отдельные отчеты могут создаваться специально для соответствия NERC CIP.

Преимущества управления инцидентами и событиями безопасности

- Интеллектуальная защита, уверенность и соответствие требованиям нормативов.
- Всесторонний сбор событий безопасности и мониторинг для сред безопасности нескольких клиентов.
- Сопоставление событий в режиме реального времени для обнаружения известных и неизвестных угроз.
- Всесторонняя интерактивная отчетность для быстрого и интуитивного анализа угроз безопасности.
- Простая настройка, информационная панель, настройка отчетов и предупреждений.

Управление журналами[1]

Являясь частью функции управления инцидентами и событиями безопасности, управление журналами обеспечивает возможность сохранения оригинальных файлов журналов в течение длительного периода времени. Хранение множества исходных журналов требует наличия сетевого хранилища данных. Данная функция необходима согласно CIP-008 «Оповещение об инцидентах и планирование реакций» в случае, если был определен реальный инцидент в сфере кибербезопасности и необходимо сохранить доказательства.

[1] Управление журналами и обнаружение вторжений в сеть доступны в версиях Ovation Security Center 2.1 и 3.0.

Целостность файлов журналов обеспечивается с помощью MD5- алгоритма . Изменение одного бита в этих данных приведет к получению полностью отличной контрольной суммы. Исходные подписанные сообщения защищены шифрованием.

Преимущества управления журналами

- Соответствие требованиям по хранению журналов.
- Адаптация систем хранения под каждый источник журналов.
- Удобный и эффективный анализ и поиск по журналам.
- Хранение журналов в управляемом NAS.

Обнаружение вторжений в сеть[1]

Входящая в состав OSC функция обнаружения вторжений в сеть является ответом на растущую озабоченность возможностью кибератак из сети предприятия, а не с зараженной управляющей рабочей станции или конечных устройств.

Система обнаружения вторжений в сеть подключается к линии или к диапазону портов отслеживания трафика на точках доступа по периметру системы Ovation.

Трафик данных через эти точки доступа будет всестороннее изучен в отношении заголовков протокола и информационного наполнения. Таким образом можно обнаружить потенциальные сетевые атаки, включая червей, DOS-атаки и другие формы вредоносного ПО.

Механизм обнаружения может быть реализован на основе сигнатур или на основе обнаружения отклонений, чтобы эффективно обнаруживать как известные, так и неизвестные угрозы. В настоящее время данная функция предназначена для защиты периметра Ovation или пространства между системами Ovation в составе многосетевой архитектуры Ovation.

Менеджер обнаружения вторжений в сеть работает в виртуальной среде, взаимодействуя с внешними аппаратными устройствами для мониторинга сетевого трафика. Событие вторжения может в качестве опции быть направлено в модуль управления инцидентами и событиями безопасности OSC для дальнейшего сопоставления или анализа.

Преимущества обнаружения вторжений в сеть

- Обнаружение кибератак из прилегающих сетей.
- Протоколы комплексной проверки и проверка информационного наполнения.
- Встраивание информации по обнаружению в управление инцидентами и событиями безопасности.

Сетевое хранилище данных[2]

Сетевое хранилище данных предоставляет простое в использовании и высокопроизводительное решение для хранения данных с целью коллективного доступа и защиты критической информации. Хранилище устанавливается в шкаф Ovation Security Center и служит для решения следующих задач функциональных модулей центра безопасности Ovation и системы управления Ovation:

- Внешнее запоминающее устройство для архивных журналов функции управления журналами.
- Многофункциональное запоминающее устройств для резервных образов устройств центра безопасности Ovation.
- Резервные образы Ovation из новой функции резервного копирования и восстановления системы.
- Удаленное копирование на другое устройство хранения для поддержки архивирования за пределами объекта.

[1] Управление журналами и обнаружение вторжений в сеть доступны в версиях Ovation Security Center 2.1 и 3.0.

[2] Сетевое хранилище данных доступно в версиях Ovation Security Center 2.1 и 3.0.

Резервное копирование и восстановление системы[3]

Задачей функции резервного копирования и восстановления системы заключается в облегчении полного восстановления, если в системе Ovation наблюдается частичная или полная потеря программных средств.

На основе технологии создания образов функция резервного копирования и восстановления может выполнять резервирование диска или файла, которое будет включать операционную систему управляющей системы, прикладное ПО, конфигурацию и данные. Может быть создан план полного, дифференциального, пошагового резервирования или план, сочетающий любые или все описанные ранее типы. План может запускаться по графику, по событию или же вручную. Резервные файлы могут быть отправлены во множество точек, хотя предпочтительным выбором является сетевое хранилище данных. Восстановление ПО можно выполнить для всей системы Ovation, отдельной рабочей станции или даже каталога и файлов.

Преимущества резервного копирования и восстановления системы

- Максимальное использование имеющейся инфраструктуры OSC для поддержки нескольких систем Ovation.
- Быстрое восстановление из образов дисков в случае аварии.
- Четкий план полного восстановления Ovation, в случае когда необходима синхронизация котнроллера и базы данных реального времени.

[3] Резервное копирование и восстановление системы доступно для версий Ovation Security Center 3.0.

Конфигурирование центра безопасности Ovation

OSC предназначена для безопасного добавления в систему Ovation без прерывания защищаемого процесса. Для выполнения этой задачи OSC включает в себя сетевое оборудование, необходимое для формирования собственной DMZ, и поэтому не требует модификации каких-либо существующих DMZ или полевого коммуникационного оборудования локальной сети.

Одним из требований является наличие возможности подключения по TCP/IP. Нет необходимости в специальной настройке или в изменении существующей системы Ovation. На рис. 1 показан обзор коммуникационных возможностей стандартного OSC. Все устройства соединяются между собой через частную DMZ, которая с помощью маршрутизатора изолирована от Ovation и сети предприятия заказчика. Каждый из каналов связи описан следующим образом:

Обмен центра безопасности информацией с Ovation

Сетевой пакет стандартного OSC спроектирован таким образом, чтобы обеспечивать необходимую универсальность в подключении к наиболее распространенным конфигурациям Ovation:

- Может быть напрямую подключен к одной до восьми независимым (не объединенным между собой) сетям Ovation DCS. Точка подключения на каждой сети Ovation представляет собой порт на одном из коммутаторов Ovation в каждой локальной сети ПТК.
- Может напрямую подключаться к одиночной многосетевой системе Ovation (до 16 подключенных подсетей Ovation). Точка подключения на многосетевой системе представляет собой порт на одном из внутренних коммутаторов Ovation.
- Если многосетевая система Ovation не использует архитектуру Emerson с компактной магистралью, OSC может подключаться к порту на любой из объединенных локальных сетей ПТК. Многосетевые конфигурации необходимо изучить и удостовериться, что можно внедрить все устройства.

Обмен данными внутри устройств

Стандартный сетевой пакет OSC обеспечивает выделенную DMZ, что позволяет организовать обмен данными между функциями. Эта особенность позволяет функции управления инцидентами и событиями безопасности получать и собирать информацию по безопасности от других функций безопасности.

Поставляемый компанией Emerson маршрутизатор со встроенным брандмауэром используется для защиты DMZ и управления всем трафиком между OSC и системой управления Ovation. Кроме того, данный маршрутизатор контролирует весь трафик к/от локальной сети предприятия.

Примечание. *Маршрутизатор настроен на регистрацию событий безопасности для функций управления инцидентами и событиями безопасности.*

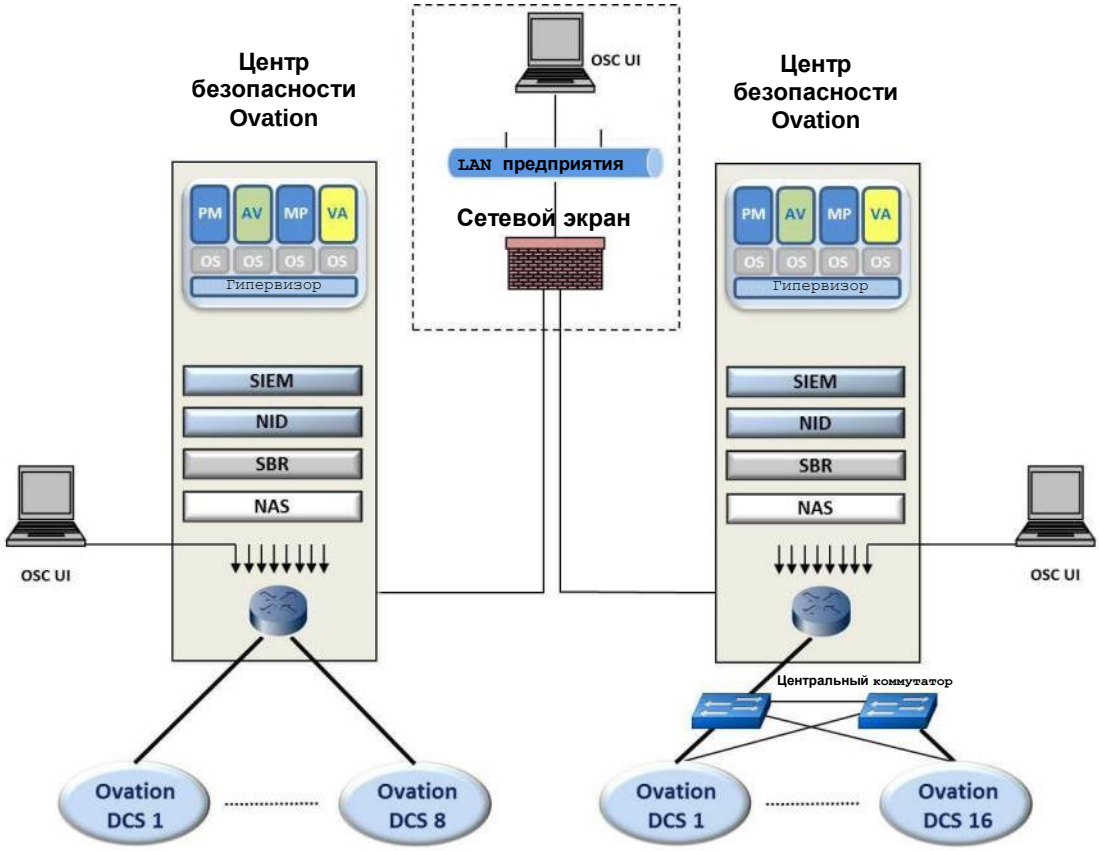


Рис. 1. Соединение от одной до восьми независимых сетей ПТК Ovation и подключения к одиночной многосетевой системе Ovation (до 16 подсетей Ovation)

Обмен данными между центром безопасности Ovation и локальной сетью предприятия

Стандартный сетевой пакет OSC обеспечивает одну точку доступа для безопасной передачи данных из корпоративной локальной сети в OSC. Данное соединение используется для создания отчетов, анализа событий, обновления исправлений, определения уязвимостей и обслуживания.

Для обеспечения безопасности данное соединение реализуется через VPN-туннель от пользовательской рабочей станции к маршрутизатору OSC. Туннель конфигурируется таким образом, чтобы авторизовать пользователя либо на корпоративном, либо на доменном контроллере Ovation. Кроме того, такой же подход с VPN-туннелем используется, если клиент требует/разрешает для OSC поддержку SureService.

При необходимости может использоваться дополнительный брандмауэр, устанавливаемый последовательно с предоставленным компанией Emerson маршрутизатором.

Пользовательский интерфейс центра безопасности Ovation (OSC UI)

Пользователи могут отслеживать и управлять функциями OSC с помощью пользовательского интерфейса OSC (OSC UI). OSC UI представляет собой стандартный ПК для ОС Windows с удаленным рабочим столом и браузером. ПК не имеет какого-либо функционала Ovation. Компания Emerson рекомендует, чтобы в случае локального управления эта рабочая станция была соединена с маршрутизатором DMZ. При необходимости OSC UI можно подключить к локальной сети предприятия для удаленного управления или дальнейшего анализа данных.

Поддержка центра безопасности Ovation

Поддержка программного обеспечения Ovation

OSC версии 2.0 и 2.1 поддерживает версии Ovation с 2.4 по 3.3.1 для Microsoft Windows и версии Ovation с 1.7.2 по 1.9.2 для Sun Solaris. OSC версии 3.0 и 3.1 поддерживает Ovation 3.0 и выше для Microsoft Windows, за исключением функции резервного копирования и восстановления системы. Функция резервного копирования и восстановления системы поддерживает Ovation версии 3.5 и выше.

Поддержание центра безопасности Ovation в актуальном состоянии

Модуль поддержки SureService центра безопасности Ovation предназначен для поддержания на высшем уровне эффективности работы как ПО, так и аппаратного обеспечения центра безопасности Ovation. Модуль поддержки состоит из следующих элементов:

Обновления ПО и исправления безопасности

Компания Emerson утверждает важные исправления, предлагаемые сторонними поставщиками, которые применяются к системам Ovation, включая:

- Операционную систему Microsoft® Windows® 7.
- Операционные системы Microsoft® Windows® Server 2008 и Server 2003.
- Операционную систему Sun Solaris™ 10.
- Microsoft® Internet Explorer.
- Adobe® Reader®.

Важно поддерживать актуальность OSC с помощью обновлений ПО и исправлений безопасности. Пакеты, состоящие из проверенных исправлений, определений уязвимостей и любых обновлений для ПК, ежемесячно распространяются через выделенный веб-сайт поддержки.

Для загрузки размещенных файлов используется ПК заказчика с установленным интернет-браузером. Эти файлы затем передаются в OSC через OSC UI с помощью съемных носителей (например, карт памяти). Кроме того, один раз в год выпускается накопительный DVD со всеми исправлениями.

Ремонт компонентов

Ремонт любого из компонентов OSC будет выполнен в течение срока действия контракта SureService, который включает модуль поддержки центра безопасности SureService Ovation.

Ежегодное обновление лицензии

Также предусмотрен сбор за ежегодное обновление каждого из трех лицензированных компонентов.

Модуль поддержки необходимо приобретать ежегодно. Однако контракт на первый год использования модуля поддержки центра безопасности SureService Ovation входит в стоимость покупки OSC.

Примечание. *Модуль поддержки центра безопасности SureService Ovation также требует наличия модуля экспертной поддержки по телефону SureService.*

Заключение

OSC обеспечивает улучшенное управление безопасностью, что позволяет заказчикам системы управления Ovation соответствовать стандартам NERC CIP. Он предлагает центральный пульт управления, оснащенный средствами управления событиями безопасности, получения и применения исправлений, предотвращения запуска вредоносного ПО, хранения журналов и ведения отчетности, предотвращения вторжений, восстановления данных и обнаружения уязвимостей.

Не принадлежащие Ovation приложения

Многие функции OSC можно с легкостью расширить на другие системы управления на том же объекте. Применение этих функций может потребовать совместной работы поставщика системы управления и владельца объекта.

Каждое устройство, которое необходимо охватить, должно быть доступно для OSC по сети. Может потребоваться модифицировать маршрутизаторы и брандмауэры в составе инфраструктуры сети предприятия для поддержки требований OSC к подключению.

Оценка уязвимостей (Vulnerability Assessment)

Неинтрузивное сканирование уязвимостей может выполняться на всех устройствах, которые доступны OSC по сети. Сканер может определить операционную систему устройства и другие атрибуты после получения прав администратора.

Управление исправлениями (Patch Management)

- На каждую поддерживаемую рабочую станцию устанавливается агент. После установки агента производитель рабочей станции или владелец оборудования могут убедиться в корректности функционирования рабочей станции.
- Каждый производитель рабочих станций обычно ежемесячно выпускает проверенные исправления операционной системы. Список одобренных исправлений можно сравнить с одобренным списком компании Emerson.
- Любые ненужные исправления можно удалить из списка установки.
- Любые дополнительные необходимые исправления владелец может получить и установить на рабочую станцию, поставленную производителем комплексного оборудования, отдельно.

Предотвращение запуска вредоносного ПО (Malware Prevention)

- Для каждой защищаемой рабочей станции должен быть создан агент.
- Каждый агент может быть разработан вместе с производителями рабочей станции и устройства предотвращения запуска вредоносного ПО и может поддерживаться владельцем оборудования.

Управление инцидентами и событиями безопасности (Security Incident & Event Management)

- Управление инцидентами и событиями безопасности может получать информацию от других устройств.
- Стандартный анализатор, поставляемый вместе с модулем управления инцидентами и событиями безопасности, позволяет получать, стандартизировать и соотносить события от множества устройств.
- Разработка специального анализатора может потребоваться в том случае, если устройство генерирует журналы в нестандартном формате.

Обнаружение вторжений в сеть (Network Intrusion Detection)

- Обнаружение вторжений в сеть может использоваться вместе с другими сетевыми устройствами, предоставленными клиентом.
- Для подтверждения совместимости доступен список поддерживаемых устройств.

Резервное копирование и восстановление системы (System Backup & Recovery)

- Должен быть создан план резервного копирования для правильного определения данных, схем, прав доступа и мест хранения.
- Локальные базы данных должны обслуживаться, прибегая в некоторых случаях к помощи производителя оборудования.