InfoDiode и интеграция с системами обнаружения вторжений (СОВ, IDS)

ИТ-ландшафт современных компаний и предприятий становится все более требовательным к связности различных компонент, систем и сетевых сегментов.

Такая связность порождает большое количество рисков несанкционированного или деструктивного воздействия на ключевые системы организации и приводит к пересмотру средств и методов защиты критических систем и сегментов. Развитие систем защиты идет в направлении применения различных инструментов защиты, в частности - средств защиты конечных устройств, средств анализа сетевого трафика, средств сегментации или изоляции сетей, решений по защите локальной инфраструктуры, сбора и анализа событий. Несмотря на очевидные достоинства каждого средства защиты, будучи примененным изолированно (автономно), любой из рассмотренных выше инструментов имеет значимые недостатки, которые требуют комплиментарного, компенсирующего применения других средств.

В качестве примера можно привести подходы к сегментации критических сетей, которые варьируются от сегментации с применением «классических» средств межсетевого экранирования до организации воздушного зазора или применения «физически однонаправленных шлюзов» между технологической сетью и корпоративной инфраструктурой. Например, воздушный зазор неприменим на многих современных предприятиях по целому ряду причин: «ручной» перенос данных между сегментами, низкая скорость такого обмена, необходимость дополнительных мер по учету и применению носителей информации. Межсетевые экраны требуют дополнительных затрат на поддержание корректной конфигурации, являются программными решениями (не исключают наличие программных «уязвимостей нулевого дня») и даже при выполнении всех условий по настройке и обновлению не дают гарантию защиты от успешной сетевой атаки извне. Однонаправленные шлюзы являются эффективным средством сегментации сети, но не позволяют сами по себе обеспечить анализ сетевого трафика для своевременного обнаружения и купирования инцидента ИБ. Другим примером является автономное применение систем, задачей которых является своевременное обнаружение нехарактерных действий на конечных устройствах пользователей и серверах или нетипичного сетевого трафика в технологическом сегменте предприятий. Собираемые данные передаются в ситуационный центр информационной безопасности (SOC), в сетевой сегмент, расположенный вне сегмента-источника, что в условиях недостаточной сегментации несет риски организации атаки из внешнего сегмента.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

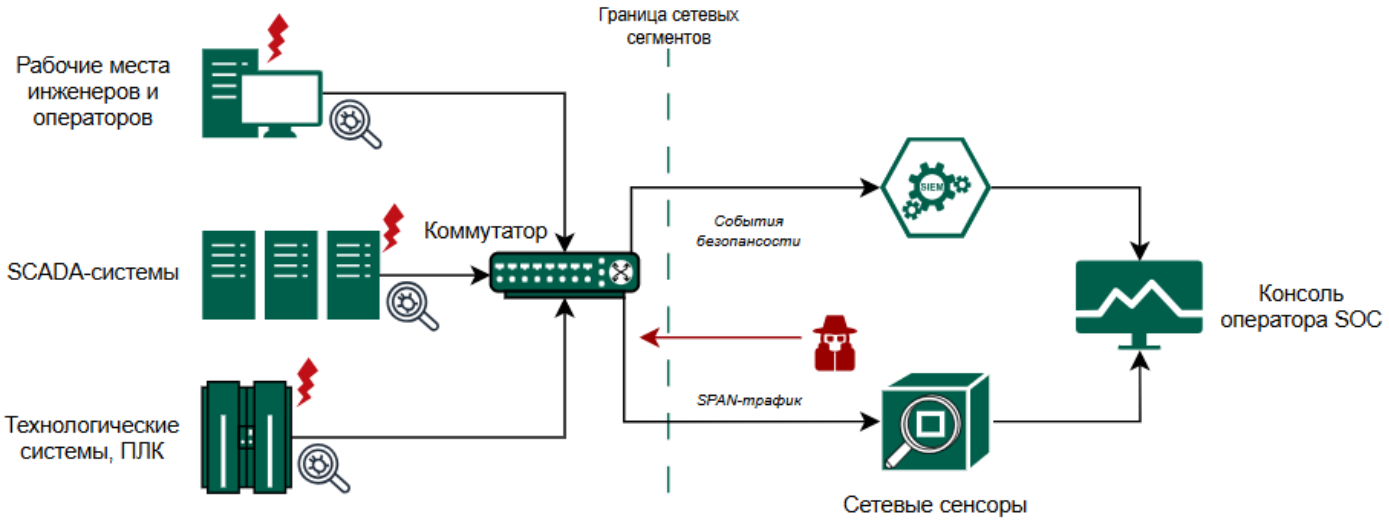
Особенности проектирования СОИБ защищаемого объекта, возникающие риски

При проектировании СОИБ предприятия необходимо учитывать критичность и значимость защищаемого объекта, модель угроз и нарушителя, актуальную именно для данного объекта, а также сильные и слабые стороны используемых средств защиты, которые при эффективном использовании должны дополнять друг друга и компенсировать свои ограничения в применении.

Особенностью современных XDR-систем является возможность проведения анализа как локально (на агентах или сетевых сенсорах), так и в централизованном ядре – единой точке анализа всех собираемых данных и принятия решения об информировании специалистов ИБ о возможных несанкционированных действиях. Современные XDR решения представляют собой многокомпонентную систему, включающую:

1. Агентов-сборщиков данных, которые внедряются на рабочих местах инженеров и операторов, технологических системах, SCADA-системах, ПЛК и других информационных системах и отслеживают множество различных событий систем, и, в случае выявления потенциальных индикаторов компрометации, передают сведения о них в центр анализа и принятия решений. Такие агенты являются аналогом EDR-решения в составе XDR.
2. Сетевые сенсоры, размещенные на различных узлах сети, которые позволяют выявлять несанкционированные сетевые пакеты в сети предприятия или передавать полную копию сетевого трафика в единый центр для анализа. Данные компоненты аналогичны функционалу NDR.
3. Центр анализа и принятия решений агрегирует всевозможные данные от агентов и сетевых сенсоров, и, в случае выявления вредоносной активности, оповещает сотрудников подразделений безопасности и выполняет заданный порядок действий по нейтрализации атаки. Как упоминалось выше, чаще всего такой центр размещается в сетевом сегменте ситуационного центра информационной безопасности.

Аналитическая часть таких систем находится в ситуационном центре информационной безопасности (SOC), в сетевом сегменте, отличном от технологического и связанного с корпоративным. Такая связность открывает еще один канал в самое «сердце» предприятия, который могут использовать злоумышленники. То есть – несмотря на высокую эффективность IDS системы, без корректной сегментации сети не будет исключена возможность атаки на защищаемый сегмент в рамках существующего двунаправленного канала.



AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

Применение InfoDiode совместно с XDR-системами, компенсация рисков

Таким образом, универсальные современные решения также имеют свои слабые места. Основной проблемой использования XDR-решений в инфраструктуре критически значимых промышленных объектов, как уже было отмечено выше, является необходимость организации дополнительного канала связи между технологическим сегментом сети и SOC. Исходя из принципов модели «нулевого доверия», канал связи даже с таким «безопасным» сегментом, как ситуационный центр информационной безопасности, должен считаться угрозой. Такой канал требует внимания при проработке МУиН для промышленных систем, а также применения мер, нейтрализующих угрозу проникновения злоумышленника в технологический сегмент через сеть SOC.

Для компенсации указанных выше недостатков необходимо обеспечить максимальную изоляцию технологического сегмента от всех других корпоративных сегментов, и при этом не потерять возможность передачи данных из технологического сегмента вовне. Такая задача может быть решена с помощью «классических» средств межсетевого экранирования. Однако решения, основанные на программных функциях защиты, могут иметь уязвимости (в том числе «уязвимости нулевого дня»), позволят в определенной степени эксплуатировать уязвимости даже разрешенных протоколов и будут зависимы от корректности конфигурации таких средств. В случае атаки высококвалифицированных злоумышленников программные решения не смогут обеспечить гарантированную защиту ключевых критически значимых систем предприятия.

Рассмотрим, каким образом можно построить эффективную и комплексную систему обнаружения вторжений на критически значимом объекте. То есть на объекте, который обладает следующими характеристиками: максимально автономен и изолирован, сохранена передача данных внешним потребителям как ИБ так и другим подразделениям, канал связи гарантированно не может быть использован в качестве точки проникновения в технологический сегмент, применяются иные решения для повышения общего уровня безопасности и защиты.

Эффективным решением данной задачи является совместное применение СЗИ класса «однонаправленный шлюз» (InfoDiode) и XDR решений. InfoDiode представляет собой аппаратно-программное устройство, функция безопасности которого базируется на физических принципах. Однонаправленная передача данных в решениях InfoDiode основана на применении «оптического диода», который физически изолирует более доверенный сегмент от менее доверенных, сохраняя возможность передачи информации из более доверенного сегмента в менее доверенный.

Таким образом, InfoDiode передает все получаемые данные из технологического сегмента на анализаторы в сегмент SOC по физически одностороннему каналу. Далее данные направляются в центр анализа и принятия решений, также размещенный в сегменте SOC.

Использование InfoDiode при построении систем обнаружения вторжений или расширенного обнаружения и реагирования позволяет надежно получать из изолированной технологической сети события безопасности и копию сетевого трафика для их дальнейшей обработки и анализа, и при этом устраняет дополнительный канал доступа к промышленным системам через инфраструктуру ситуационного центра информационной безопасности. Применение таких решений является примером комплексного и эффективного использования нескольких эффективных СЗИ в целях защиты значимых технологических объектов.

AMT GROUP

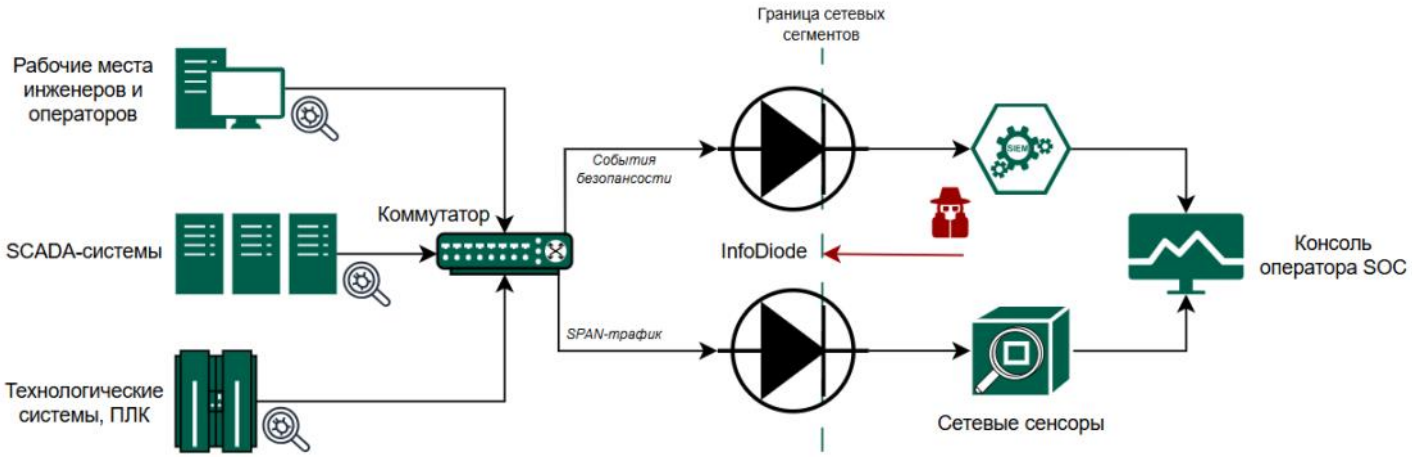
119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

Схема и примеры применения InfoDiode совместно с XDR-системами

Схема совместного применения XDR-систем и однонаправленных шлюзов InfoDiode может выглядеть следующим образом. Агенты XDR-системы, размещенные на рабочих местах и промышленных системах, передают данные событий безопасности на единый IP адрес InfoDiode в технологическом сегменте сети, и далее InfoDiode направляет полученный трафик в целевые системы-получатели. Аналогично на IP адрес InfoDiode передаются данные сетевых сенсоров с различных сетевых устройств. В свою очередь копия сетевого трафика передается в InfoDiode за счет физического подключения InfoDiode к SPAN-порту коммутатора.

В зависимости от типов передаваемых данных используются различные конфигурации размещения InfoDiode на границе сетевых сегментов. В случае передачи только SPAN-трафика достаточно использовать аппаратный «диод» (АК InfoDiode), который обеспечит передачу копии трафика в однонаправленном режиме в сегмент SOC. При передаче событий безопасности с использованием протоколов обмена, основанных на стеке TCP/IP, дополнительно используется аппаратно-программное решение, позволяющее преобразовывать такой трафик для его передачи в однонаправленный канал.



Практическими примерами подобных комплексных решений являются сценарии применения InfoDiode с такими решениями как Kaspersky Industrial CyberSecurity (KICS for Networks и KICS for Nodes), PT Industrial Security Incident Manager (PT ISIM), а также решениями данного класса других вендоров. Совместное использование обеспечивает стабильную работу указанных XDR-систем, обеспечивая высокий уровень защищенности даже в случае компрометации инфраструктуры ситуационного центра информационной безопасности и/или корпоративной сети в целом.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru