Однонаправленные шлюзы для подключения объектов технологической сети к SOC

Вячеслав Половинко, *руководитель направления собственных продуктов АМТ-ГРУП*
Виктория Стерлядева, *инженер группы информационной поддержки АМТ-ГРУП*
Анастасия Лазарева, *инженер группы информационной поддержки АМТ-ГРУП*

Квалифицированные злоумышленники, владеющие различными методами взлома и способные реализовать сложные кибератаки на ИТ-инфраструктуру, в настоящее время являются одной из наиболее опасных угроз для любого бизнеса. Нарушение целостности, потеря доступности сетевой инфраструктуры и/или потеря конфиденциальных данных могут поставить под угрозу достижение целей компании и нанести ей непоправимый репутационный, а также экономический ущерб. Именно поэтому необходимо на ранних этапах выявлять организацию и развитие кибератаки, своевременно реагируя на инциденты ИБ.

Что такое SOC?

Для обнаружения и обработки инцидентов многие организации выделяют в своей инфраструктуре центр мониторинга и управления информационной безопасностью, то есть SOC (Security Operations Center), или, другими словами, ситуационный центр информационной безопасности.

Концепция SOC направлена на обеспечение непрерывного анализа возникающих рисков и угроз, выбора эффективных мер защиты, своевременной реакции на инциденты и успешного взаимодействия подразделений в рамках обеспечения безопасности.

Следует отметить, что для мониторинга всей ИТ-инфраструктуры требуется отслеживать и обеспечивать корреляцию для достаточно большого объема событий. При этом неизбежно возникает и целый ряд технически сложных задач, среди которых можно выделить следующие:

1. Сбор событий из самых разных источников информации – средств защиты, АРМ, бизнес-систем, баз данных, серверов... И все это с учетом возможных ограничений по каналам связи, ресурсам хранения данных и т.п.

2. Поступление событий от источников на разных языках прикладного уровня и доставляемых до системы анализа по разным протоколам; каждый тип такого события должен быть корректно прочитан и обработан для последующего анализа и соответствующей реакции.

3. Необходимость проведения комплексной корреляции событий и выстраивание правильных и значимых с точки зрения ИБ взаимосвязей.

Технической основой SOC является система управления событиями информационной безопасности – SIEM (Security Information and Event Management).

SIEM предназначена для анализа поступающей информации от различных устройств, подключенных к ней, и дальнейшего выявления возникающих инцидентов, в том числе в отдельном (защищаемом) сегменте сети. Она работает с большим потоком разнородной информации от различных источников. Данная система служит инструментом для сбора, фильтрации, унификации, хранения и поиска, корреляции, создания оповещений об инцидентах, визуализации, разбора и расследования инцидентов информационной безопасности.

Рассмотрим пример работы SIEM в части сбора событий от источников в защищаемом сегменте сети (см. рис. 1).

На рисунке показано схематическое взаимодействие источников событий, расположенных в защищаемом сегменте сети, с приемником событий SIEM ситуационного центра. Источники могут быть как активными, то есть умеющими самостоятельно передавать данные в SIEM, и им достаточно указать сетевой адрес приемника событий, так и пассивными, то есть к которым SIEM сама должна обратиться. Примеры активных источников – устройства, передающие данные, например, по протоколам Syslog или Netflow. Пассивные источники – это устройства, которые только принимают сетевые подключения, например, по протоколам FTP, CIFS, HTTP, SCP для выгрузки своих файлов журналов.

Поскольку защищенный сегмент, как правило, отделен от остальных корпоративных и внешних сетей, то он может представлять собой "слепую" или "полуслепую" зону для инженеров SOC. Это прежде всего связано с тем, что на практике могут существовать значительные законодательные, организационные и технические трудности при организации передачи данных в ситуационный центр из защищаемого сегмента и наоборот. Канал связи и каналообразующее оборудование между защищаемым сегментом и SOC представляют собой потенциальную возможность для облегчения компрометации объекта, тем самым снижая уровень защищенности последнего.

Дело в том, что в современной терминологии сетей связи практически любое сетевое подключение к защищаемому сегменту или объекту трактуется как двунаправленное и чаще всего таким и является. Промежуточные звенья сети, средства защиты, дополнительное оборудование не оказывают какого-либо влияния на принципиально двунаправленный характер такого взаимодействия, вне зависимости от используемого типа средств защиты – межсетевые экраны, маршрутизаторы, программное обеспечение и т.п.

При этом важным аспектом двунаправленного взаимодействия остается тот факт, что оно несет риски потери управления критическим объектом со стороны авторизованных управляющих служб, диспетчерских подразделений, служб поддержки. Это становится возможным из-за относительно высокой вероятности реализации атаки по двунаправленному каналу. Речь идет о классе управляемых атак, для эффективной организации которых необходимым условием является наличие оперативной обратной связи – обмена вида "запрос-ответ", обеспечиваемого пре-

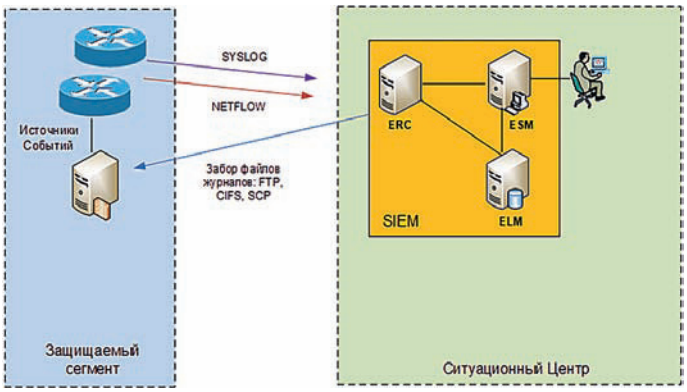

Рис. 1. Пример сбора событий от источников в защищаемом сегменте сети

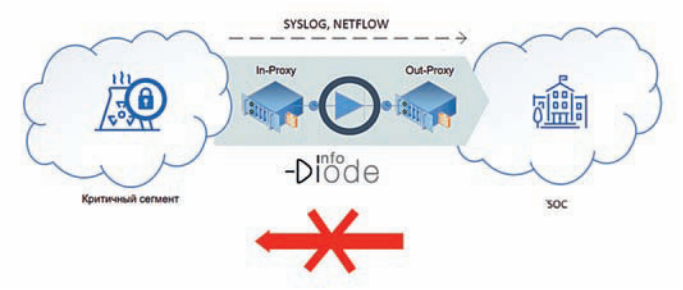

Рис. 2. Односторонняя передача информации во внешнюю систему мониторинга

имущественно в рамках стека протоколов TCP/IP. Помимо стандартных угроз прямого получения злоумышленником доступа к критическому объекту и последующего нанесения ущерба, примерами известных реализуемых угроз, в основе которых лежит двунаправленный характер информационного обмена, являются WannaCry, Petya, EternalRocks и др.

Отдельный значимый риск для защищаемой инфраструктуры – это возможность направления, загрузки чего-либо в критический сегмент, например вредоносного кода, шпионского ПО и т.п., для целей мониторинга, сбора информации, нанесения отложенного ущерба.

Безусловно, атаки могут носить и однонаправленный характер. Так, используя протоколы без обратной связи UDP или ICMP, злоумышленник может попытаться не захватить контроль над объектом, но вывести его из эксплуатации, например, с помощью DoS-атаки. Однако в действительности такие атаки распространены существенно меньше.

Для решения подобных проблем и подключения к SOC источников без повышения рисков воздействия на важный объект и защиты со стороны злоумышленника целесообразно применять технические решения на основе устройств однонаправленной передачи данных, например таких, как аппаратный комплекс InfoDiode (АК InfoDiode) или аппаратно-программный комплект InfoDiode (АПК InfoDiode).

Решения АК InfoDiode и АПК InfoDiode

Наиболее распространенными сценариями применения АПК InfoDiode как шлюза между сегментом значимого объекта и сегментом SOC могут быть:

- сценарий передачи информации от пассивных источников защищаемого объекта с последующим их чтением коллекторами SOC;
- сценарий передачи информации от активных источников защищаемого объекта на коллекторы SOC;
- сценарий анализа сетевого трафика от компонентов защищаемого объекта (например, на базе продуктов PT ISIM);
- отправка оповещений по e-mail.

Сценарий передачи информации от пассивных источников защищаемого объекта с последующим их чтением коллекторами SOC

В этом сценарии данные передаются по протоколам FTP/CIFS с сервера In-Proxy через аппаратный комплекс InfoDiode на сервер Out-Proxy.

Файлы, которые необходимо передать из защищаемого сегмента, помещаются на сервер In-Proxy, проходят через АПК InfoDiode и отправляются в конечную папку Out-Proxy сервера, к которой сможет обращаться внешняя система мониторинга (например, SIEM) или сотрудники SOC.

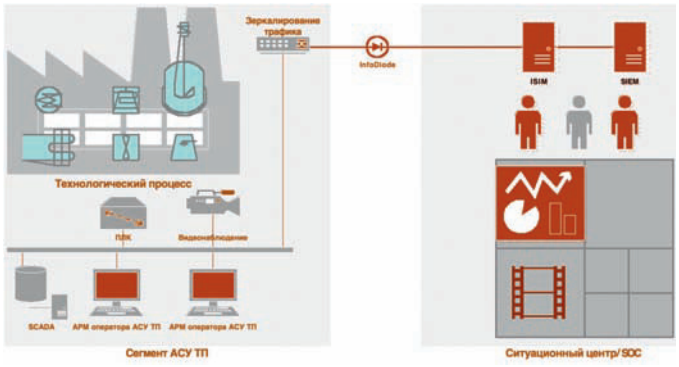

Рис. 3. АК InfoDiode устанавливается на границе критического сегмента, подключаясь к порту зеркалирования коммутатора сегмента защищаемого объекта и к PT ISIM, находящемуся во внешнем сегменте

Сценарий передачи информации от активных источников защищаемого объекта на коллекторы SOC

В этом случае передача событий из защищаемого сегмента происходит с использованием Syslog и Netflow на внешнюю систему мониторинга SOC. Передача UDP-трафика через АПК InfoDiode позволяет обеспечить одностороннюю автоматическую передачу информации во внешнюю систему мониторинга или на файловый сервер (см. рис. 2).

Сценарий анализа сетевого трафика от устройств защищаемого сегмента

Данный сценарий обеспечивает реализацию защиты закрытого сегмента в случае организации сбора и последующего анализа копии технологического трафика внешней системой мониторинга (например, IDS) через однонаправленный шлюз. Одним из примеров реализации данного сценария является совместное решение АК InfoDiode и Positive Technologies Industrial Security Incident Manager (PT ISIM)[1] (см. рис. 3).

Отправка оповещений по e-mail

Данный сценарий позволяет передачу уведомлений через АПК InfoDiode от системы мониторинга, находящейся в закрытом сегменте, с помощью почтового трафика:

1. SMTP-клиент передает на SMTP-сервер InProxy сообщение электронной почты.
2. InProxy пересылает сообщение на OutProxy.
3. SMTP-клиент OutProxy пересылает сообщение на внешний SMTP-сервер.

Каждый из представленных сценариев позволяет построить комплексную систему защиты, базирующуюся на исключении воздействия на защищаемый объект со стороны менее доверенного сегмента, в том числе такого, в котором находится SOC и функционирующая в нем система SIEM. В каждом из сценариев однонаправленные шлюзы InfoDiode позволяют обеспечить безопасную интеграцию технологической и корпоративной сетей, а также непрерывный мониторинг функционирования технологической сети из других сегментов, в том числе возможность реагирования со стороны служб SOC на инциденты ИБ. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru