SOC и SIEM: безопасное взаимодействие через InfoDiode

Современные требования к обеспечению информационной безопасности государственных информационных систем, организаций финансовой отрасли, критически важных объектов, объектов КИИ и АСУ ТП в энергетической, нефтегазовой, транспортной, ЖКХ и других отраслях приводят к выбору принципиально новых технических и организационных мер защиты. В ряде случаев наилучшим вариантом защиты становится полная изоляция информационных систем. Однако абсолютная изоляция не позволяет в полной мере реализовать весь потенциал IT-технологий для решения задач автоматизации процессов, построения систем оперативного реагирования на инциденты и эффективного управления инфраструктурой, в частности, оперативно предоставлять информацию в системы управления событиями информационной безопасности (SIEM) ситуационных центров информационной безопасности (SOC).

В качестве решения могут выступать технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, и при этом обеспечивающие возможность передачи данных из закрытого контура во внешние сети. Такие технологии гарантируют целостность и доступность данных в защищенном сегменте, а также полностью исключают риски передачи каких-либо данных в обратном направлении, внутрь защищаемого сегмента.

Построенная на принципах однонаправленной передачи данных линейка продуктов **InfoDiode** позволяет эффективно решать задачи безопасной передачи данных для SIEM в SOC.

Продукты InfoDiode выпускаются в различных форм-факторах и конфигурациях: аппаратно-программные решения **АПК InfoDiode PRO в базовой и кластерной конфигурации**, **АПК InfoDiode SMART**, аппаратные решения **АК InfoDiode RACK single, АК InfoDiode RACK double** для монтажа в 19” стойку и **АК InfoDiode MINI** в компактной конфигурации в настольном исполнении или для монтажа на DIN-рейку.

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

Что такое SOC

В настоящее время одна из наиболее опасных угроз для любого бизнеса — это квалифицированные злоумышленники, владеющие различными методами взлома и способные реализовать сложные кибератаки на IT-инфраструктуру. Нарушение целостности и/или конфиденциальности данных, потеря доступности сетевой инфраструктуры могут поставить под угрозу достижение целей компании и нанести ей непоправимый репутационный и экономический ущерб.

Именно поэтому даже на ранних этапах организации и развития кибератаки необходимо выявлять и реагировать на инциденты ИБ.

Для выявления и обработки инцидентов многие организации выделяют в своей инфраструктуре **центр мониторинга и управления информационной безопасностью – SOC (security operations center)** или, как говорят, **Ситуационный Центр Информационной Безопасности.**

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

Ежедневные задачи SOC

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

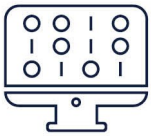
Задачи мониторинга в деятельности SOC являются одними из ключевых.

Следует заметить, 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.

Задачи мониторинга

Сбор событий от 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.



Сбор событий, сформированных 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

Проведение комплексной корреляции событий и выстраивание правильных и значимых с точки зрения ИБ взаимосвязей для своевременного принятия решений по реагированию

119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

Что такое SIEM

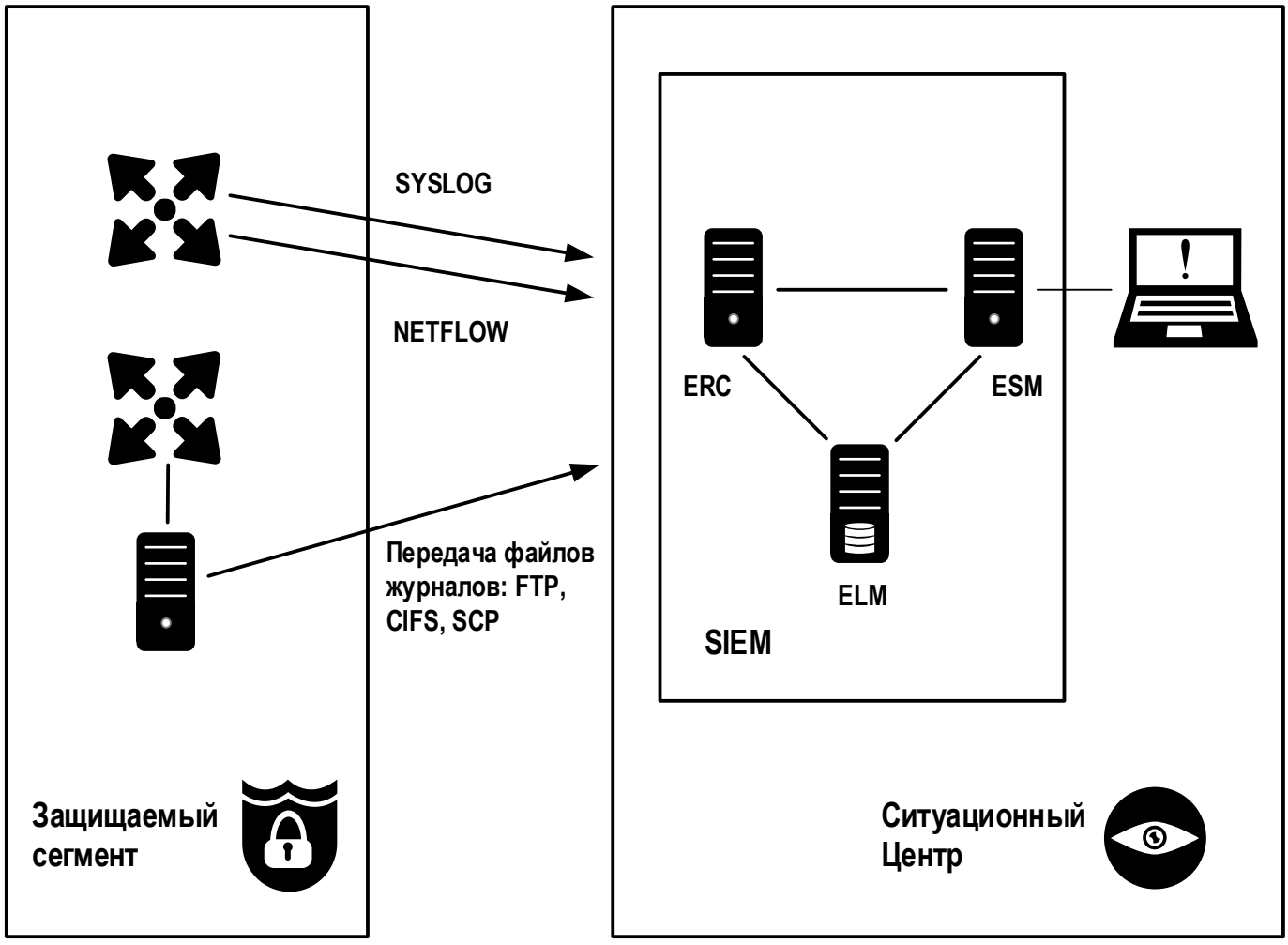
Технической основой SOC является **Система управления событиями информационной безопасности — SIEM (Security Information and Event Management)**.

SIEM предназначена для анализа поступающей информации от различных устройств, подключенных к ней, и дальнейшего выявления возникающих инцидентов, в том числе, часто расположенных в отдельном (защищаемом) сегменте сети.

Система работает с большим потоком разнородной информации от различных источников и служит инструментом для сбора, фильтрации, унификации, хранения и поиска, корреляции, создания оповещений об инцидентах, визуализации, разбора и расследования инцидентов информационной безопасности.

На рисунке ниже схематично показано взаимодействие источников событий, расположенных в защищаемом сегменте сети, с приемником событий SIEM Ситуационного центра. Источники могут быть как активными, то есть такими, которые сами умеют передавать данные в SIEM и им достаточно указать сетевой адрес приемника событий, так и пассивными, то есть такими, к которым SIEM должна обратиться самостоятельно. 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, 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 компрометации объекта, тем самым снижая уровень его защищённости.



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

Проблемы защиты взаимодействия сегментов

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 принципиальный, «двунаправленный», характер такого взаимодействия, вне зависимости от типа средств защиты (межсетевые экраны, маршрутизаторы, программное обеспечение и т.п.).

Важным аспектом двунаправленного взаимодействия остается тот факт, что оно несет риски потери управления критическим объектом авторизованными управляющими службами: диспетчерскими подразделениями, службами 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 преимущественно в рамках стека протокола 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 другие.

Отдельным значимым риском для защищаемой инфраструктуры является возможность «загрузки» чего-либо в критический сегмент: вредоносного кода, шпионского ПО и т.п. для целей мониторинга, сбора информации, нанесения отложенного ущерба.

Безусловно, атаки также могут носить и однонаправленный характер. Так, используя протоколы UDP или ICMP (протоколы без обратной связи), злоумышленник может пытаться не захватить контроль над объектом, а вывести его (объект) из эксплуатации (так называемые DoS атаки). Однако такие атаки на практике распространены существенно меньше.

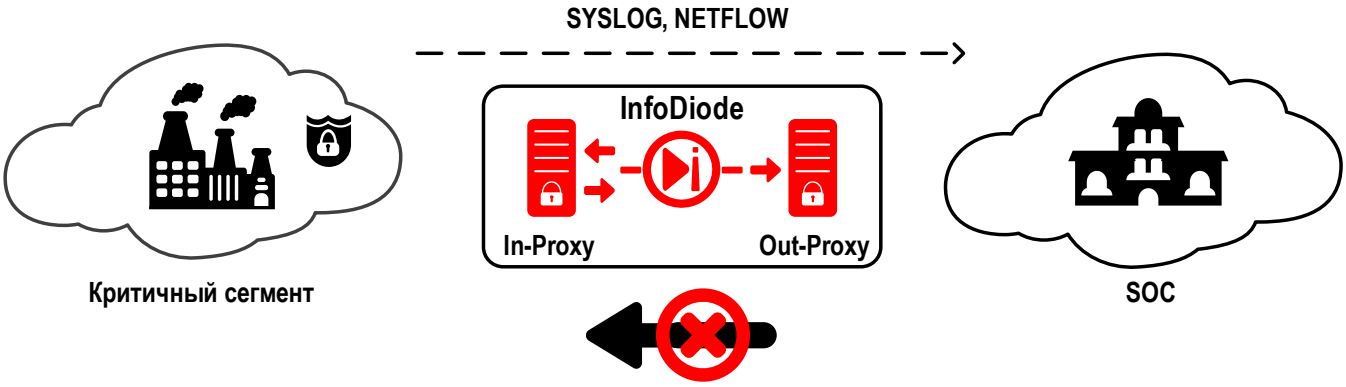
Для решения подобных проблем и подключения к SOC источников без повышения рисков воздействия на важный объект защиты со стороны злоумышленника, целесообразно применять технические решения на основе устройств однонаправленной передачи данных, например, таких как аппаратный комплекс InfoDiode (далее, АК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

Наиболее распространённые сценарии применения АПК InfoDiode PRO как шлюза между сегментом значимого объекта и сегментом SOC рассмотрены далее.

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

Сценарий 1. Передача информации от активных источников защищаемого объекта на коллекторы SOC

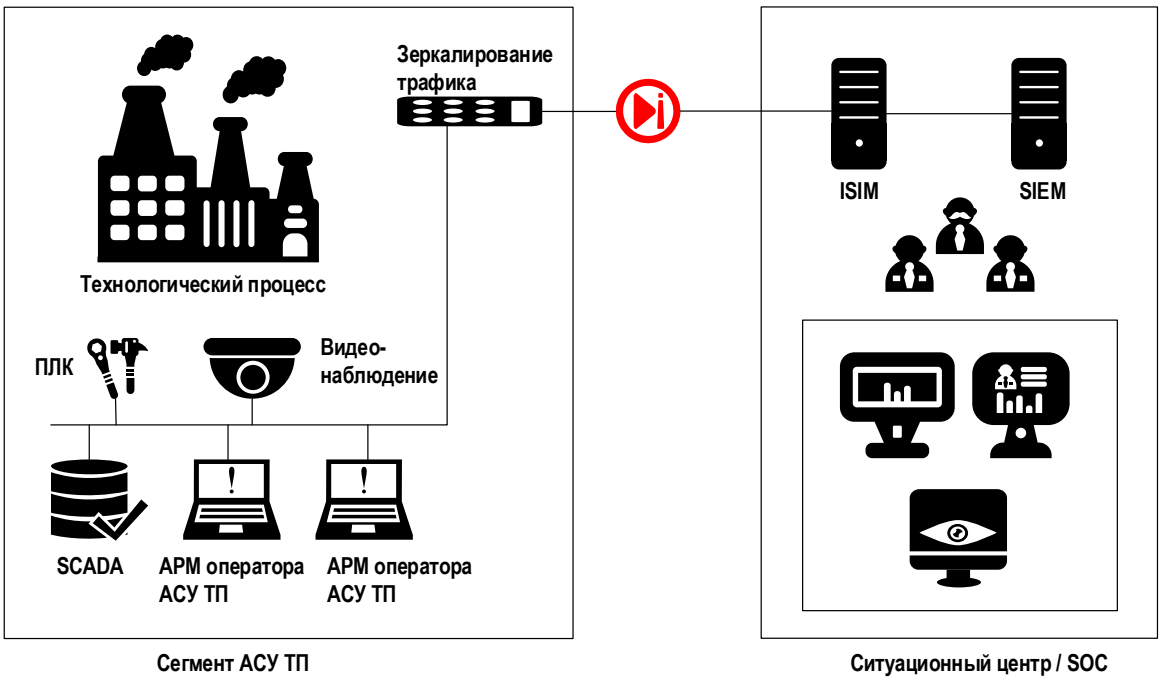
В этом случае передача событий из защищаемого сегмента происходит с использованием syslog и netflow на внешнюю систему мониторинга SOC. Передача UDP-трафика через АПК InfoDiode PRO позволяет обеспечить одностороннюю автоматическую передачу информации до внешней системы мониторинга или файлового сервера.



Сценарий 2. Анализ 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) или Kaspersky Industrial CyberSecurity (KICS).

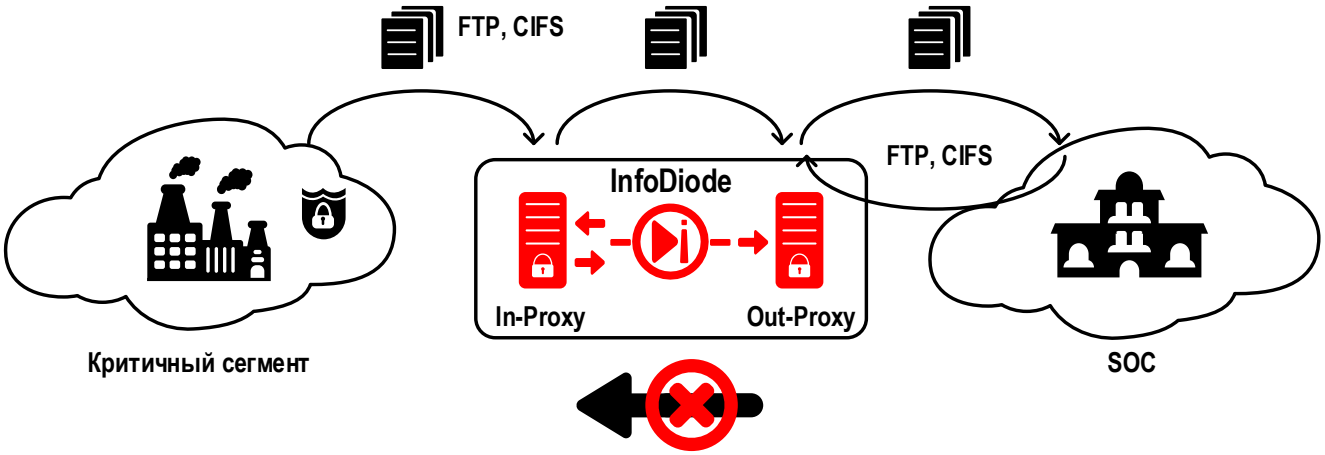
АК InfoDiode устанавливается на границе критического сегмента, подключаясь к порту зеркалирования коммутатора сегмента защищаемого объекта, и к PT ISIM, находящегося во внешнем сегменте. Тем самым обеспечивается безопасная передача копии трафика из защищаемого сегмента во внешний сегмент без риска нарушения периметра со стороны операторов SOC.



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

Сценарий 3. Передача информации от пассивных источников защищаемого объекта с последующим их чтением коллекторами SOC

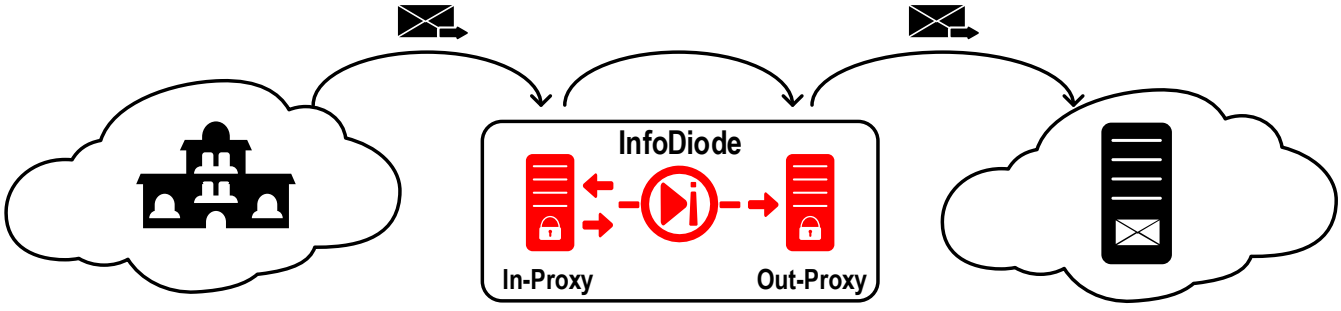
В этом сценарии данные передаются по протоколам FTP/CIFS с сервера In-Proxy через аппаратный комплекс InfoDiode на сервер Out-Proxy.
Файлы, которые необходимо передать из защищаемого сегмента, помещаются на сервер In-Proxy, проходят через АПК InfoDiode PRO и отправляются в конечную папку Out-Proxy сервера, к которой сможет обращаться внешняя система мониторинга (например, SIEM) или сотрудники SOC.



Сценарий 4. Отправка оповещений по e-mail

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

1. SMTP-клиент передает на SMTP-сервер In-Proxy сообщение электронной почты
2. In-Proxy пересылает сообщение на Out-Proxy
3. SMTP-клиент Out-Proxy 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 SIEM система. 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.

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