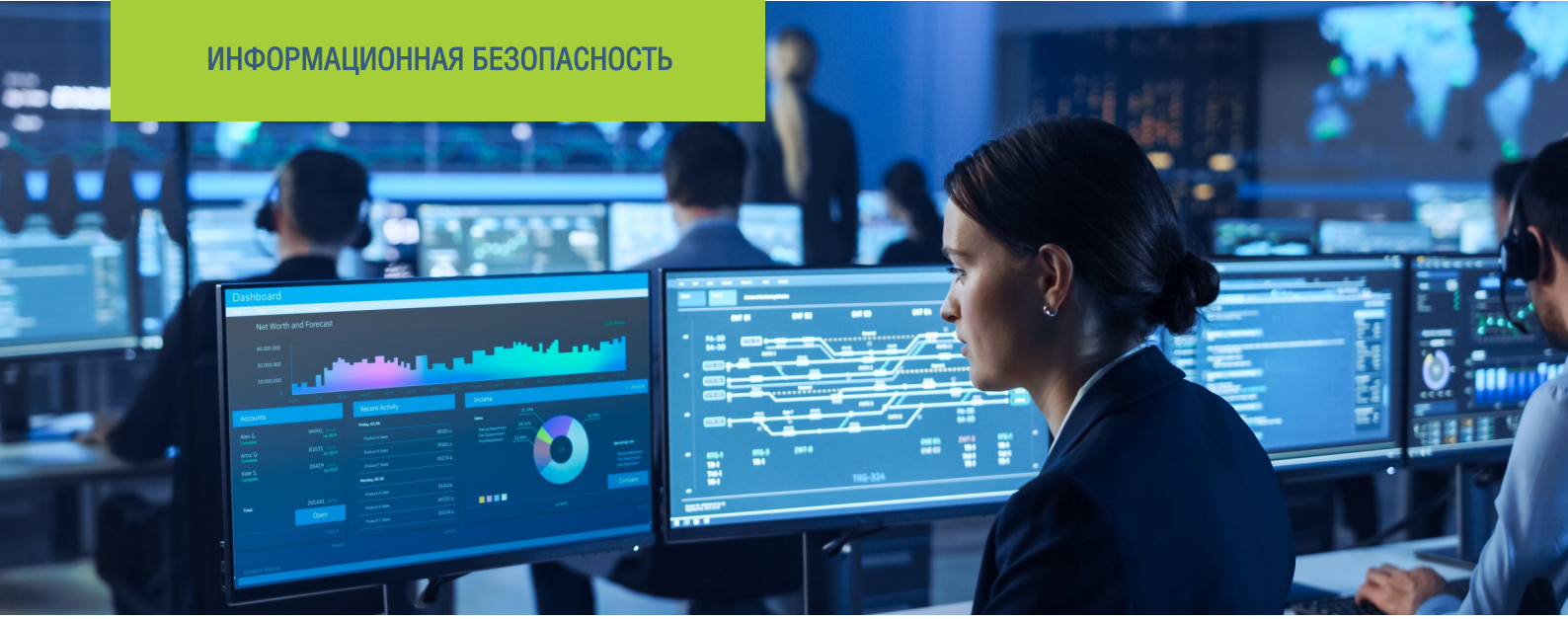


Работа Positive MaxPatrol SIEM и PT ISIM через однонаправленный шлюз InfoDiode

Требования к обеспечению информационной безопасности государственных информационных систем, организаций финансовой отрасли, 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) и центры мониторинга информационной безопасности (SOC).

В качестве решения могут выступать технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, обеспечивающие возможность передачи данных из закрытого контура во внешние сети. Такие технологии гарантируют целостность и доступность данных в защищенном сегменте и 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 и в SOC.

Были проведены всесторонние тесты в сетях передачи данных промышленных объектов с разграничением доступа на базе InfoDiode в следующих сценариях:

- InfoDiode между источником анализируемых событий в закрытом сегменте и компонентом сбора событий MaxPatrol SIEM Agent в открытом сегменте при передаче событий по протоколу UDP;
- InfoDiode между компонентом сбора событий MaxPatrol SIEM Agent в закрытом сегменте и модулями анализа событий MaxPatrol SIEM Server в открытом сегменте;
- InfoDiode между источником анализируемого трафика и сенсором PT ISIM View Sensor.

Результаты комплексного тестирования подтвердили успешное и эффективное совместное использование продуктов в указанных сценариях для обеспечения высочайшего уровня защиты критических сетевых сегментов.

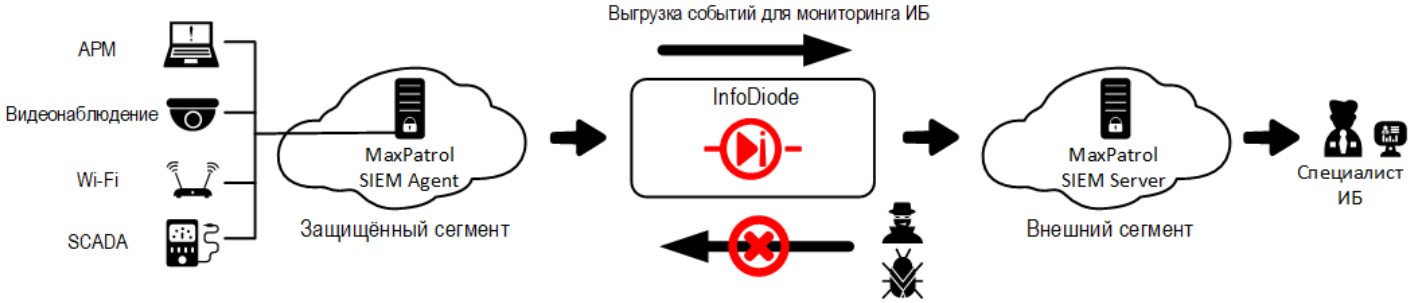
119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий работы MaxPatrol SIEM через однонаправленный канал передачи данных

Для систем АСУ ТП часто применяется не только логическая, но и физическая изоляция сетей как метод защиты от внешних воздействий. При этом возрастают требования к оперативности сбора событий безопасности для целей централизованного мониторинга и выявления инцидентов информационной безопасности. Совместное использование решений InfoDiode и MaxPatrol SIEM позволяет реализовать централизованный сбор событий из технологических сетевых сегментов, гарантируя изоляцию таких сегментов.

MaxPatrol SIEM является решением, обеспечивающим сбор и анализ событий и позволяющим выявлять инциденты информационной безопасности в реальном времени.

InfoDiode является системой однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется канал для обеспечения мониторинга и передачи логов в центры мониторинга систем и сетей.

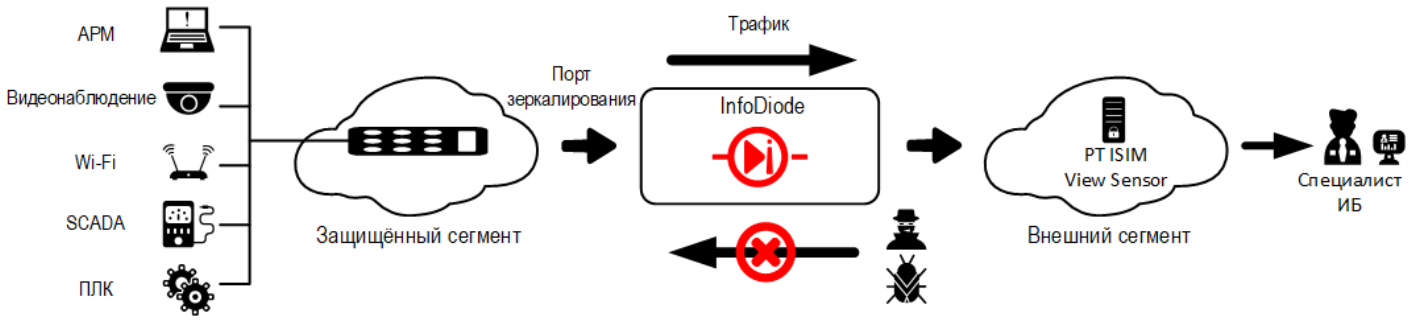


Сценарий работы PT ISIM через однонаправленный канал передачи данных

Поиск следов нарушений информационной безопасности в сетях АСУ ТП с помощью решения PT ISIM помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала и обеспечивает соответствие требованиям 187-ФЗ, приказам ФСТЭК № 31, 239, ГосСОПКА. Продукты InfoDiode позволяют передавать копии трафика с порта зеркалирования сетевого коммутатора в PT ISIM View Sensor для дальнейшего анализа специалистами ИБ АСУ ТП.

PT ISIM является специализированным решением пассивного мониторинга и анализа технологического трафика промышленной сети, предназначенным для выполнения требований к мерам защиты информации в автоматизированных системах управления технологическими процессами (АСУ ТП).

InfoDiode является системой однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется канал для сбора и передачи трафика в целях его дальнейшего анализа специализированными инструментами за пределами доверенного сегмента.



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

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программным обеспечением
MaxPatrol Security Information and Event Management,
правообладателем которого является
АО «Позитив Текнолоджиз»
(Россия, 107241, г. Москва, Щёлковское ш., д. 23А, помещение V комната 30)
в дальнейшем именуемыми «**MaxPatrol SIEM**» и «**Positive Technologies**» соответственно

и

Комплексом
«АМТ InfoDiode» однонаправленной передачи данных
продукция компании
АО «АМТ-ГРУП»
Россия, 115162, г. Москва, ул. Шаболовка, д. 31, корп. Б, под. 3
в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**» соответственно

Комплекс **InfoDiode** является системой однонаправленной передачи данных, обеспечивающий высочайший уровень изоляции критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами.

MaxPatrol SIEM является решением, обеспечивающим сбор и анализ событий и позволяющем выявлять инциденты информационной безопасности в реальном времени.

АМТ-ГРУП и **Positive Technologies** настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

АМТ-ГРУП и **Positive Technologies** провели всесторонние тесты программного обеспечения **MaxPatrol SIEM** при совместном использовании с моделями комплексов **InfoDiode** в сетях передачи данных с разграничением доступа на базе **InfoDiode**, используемого в следующих сценариях:

- между источником анализируемых событий в закрытом сегменте и компонентом сбора событий **MaxPatrol SIEM Agent** в открытом сегменте при передаче событий по протоколу UDP;
- между компонентом сбора событий **MaxPatrol SIEM Agent** в закрытом сегменте и модулями анализа событий **MaxPatrol SIEM Server** в открытом сегменте.

В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно в указанных сценариях. Тесты подтвердили полную совместимость продуктов в заявленном сценарии использования.

АО «Позитив Текнолоджиз»

Дата:

«20» декабря 2021 года

Должность:

Заместитель коммерческого директора

Подпись _____

(И.А. Глебов)

АО «АМТ-ГРУП»

Дата:

«21» декабря 2021 года

Должность:

Технический директор

Подпись _____

(В.В. Леонов)

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программным обеспечением
PT Industrial Security Incident Manager,
правообладателем которого является
АО «Позитив Текнолоджиз»
(Россия, 107241, г. Москва, Щёлковское ш.,
д. 23А, помещение V комната 30)
в дальнейшем именуемыми «**PT ISIM**» и «**Positive Technologies**»
соответственно

и

Аппаратным комплексом
«AMT InfoDiode» однонаправленной передачи данных
продукция компании
АО «АМТ-ГРУП»
Россия, 115162, г. Москва, ул. Шаболовка, д. 31, корп. Б, под. 3
в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**»
соответственно

Аппаратный комплекс **InfoDiode** является системой однонаправленной передачи данных, обеспечивающий высочайший уровень изоляции критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами.

PT ISIM является специализированным решением пассивного мониторинга и анализа технологического трафика промышленной сети, направленным на выполнение требований к мерам защиты информации в автоматизированных системах управления технологическими процессами (АСУТП).

АМТ-ГРУП и **Positive Technologies** настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

АМТ-ГРУП и **Positive Technologies** провели всесторонние тесты программного обеспечения **PT ISIM** при совместном использовании с моделями аппаратных комплексов **InfoDiode** (AK InfoDiode RACK single/double, AK InfoDiode MINI) в сетях передачи данных промышленных объектов с разграничением доступа на базе **InfoDiode**, используемого между источником анализируемого трафика и сенсором **PT ISIM View Sensor**. В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно. Тесты подтвердили полную совместимость продуктов в заявленном сценарии использования.

АО «Позитив Текнолоджиз»

Дата:

«20» декабря 2021 года

Должность:

Заместитель коммерческого директора

Подпись_____

(И.А. Глебов)

АО «АМТ-ГРУП»

Дата:

«20» декабря 2021 года

Должность:

Технический директор

Подпись_____

(В.В. Леонов)