Применение Гарда Deception и Гарда NDR с InfoDiode

Защита более доверенных сегментов автономных и удаленных объектов является актуальной задачей для подразделений информационной безопасности. Для решения этой задачи используется целый набор средств: от базовых инструментов антивирусной защиты до построения комплексных систем обнаружения вторжений (СОВ, IDS\IPS). В том числе частью этих средств являются решения Гарда Deception и Гарда NDR.

Гарда Deception – DDP (Distributed Deception Platform) платформа для создания ложного слоя сетевой инфраструктуры, дезинформирующего злоумышленников о реальном присутствии атакуемых объектов.

Гарда NDR – система анализа внутрисетевого трафика и выявления аномалий.

Отдельным моментом, который является крайне важным для защиты автономных и удаленных значимых объектов критической инфраструктуры является необходимость их эффективной и, часто, полной (физической) изоляции, которая служит действенным методом защиты от внешних (реализуемых удаленно) векторов атак. Однако в случае применения в качестве меры изоляции воздушного зазора возникает не только ограничение в выполнении ряда рабочих и технологических процессов, но и ограничение в передаче информации в системы управления событиями информационной безопасности (SIEM), ситуационные центры информационной безопасности (SOC), что, в свою очередь, ухудшает качество контроля за более доверенным сегментом со стороны подразделений ИБ, находящихся, как правило, в менее доверенном сетевом сегменте.

Решением указанной задачи может выступать комплекс однонаправленной передачи данных **InfoDiode** – продукт, основанный на принципах физической изоляции одного сетевого сегмента от другого, обеспечивающий возможность передачи данных из закрытого контура во внешние сети. InfoDiode гарантирует целостность и доступность данных в защищенном сегменте и исключает риски передачи каких-либо данных в обратном направлении, внутрь защищаемого сегмента. Комплексы **InfoDiode** прошли совместное тестирование на совместимость и возможность передачи данных от СЗИ Гарда Deception и Гарда NDR внешним потребителям (SOC, SIEM и др.).

Результаты комплексного тестирования подтвердили успешное и эффективное применение **InfoDiode** совместно с Гарда Deception и Гарда NDR в противодействии внутренним и внешним угрозам в сетях передачи данных с воздушным зазором, реализуемым комплексом **InfoDiode**, с выполнением всех требований кибербезопасности.

AMT GROUP

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

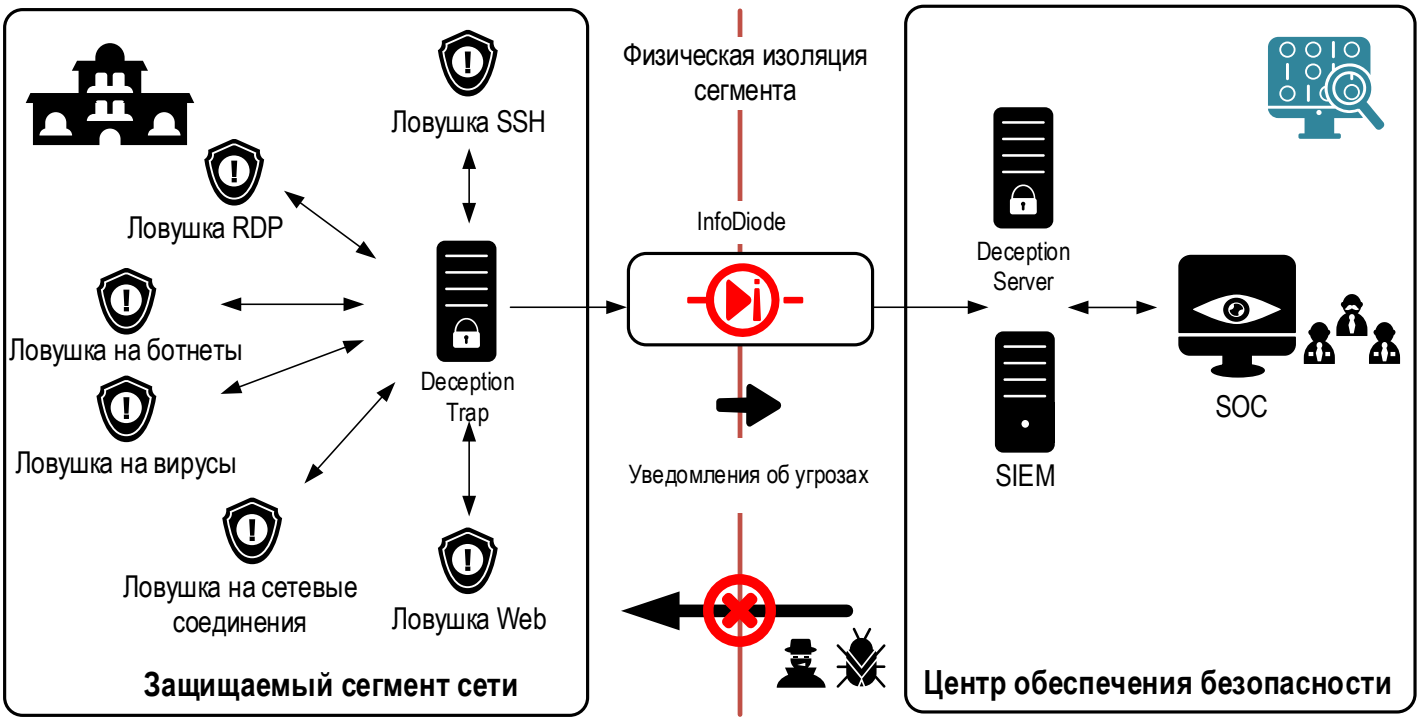
www.amt.ru
www.infodiode.ru

Сценарий работы Гарда Deception через однонаправленный канал передачи данных

На практике использование комплекса однонаправленной передачи данных InfoDiode и платформы «Гарда Deception» предполагает применение комплекса InfoDiode между центром управления системой «Гарда Deception» или системой SIEM, расположенными в открытом сегменте, и подсистемой эмуляции ложного сетевого слоя и обнаружения вредоносной активности (ловушками), расположенными в закрытом сегменте.

Совместное использование решений позволяет изолировать более доверенный сетевой сегмент и, таким образом, повысить его защищенность. Кроме того, интеграция решений позволяет физически передавать данные с ловушек в центры SOC за периметр защищаемого объекта.

Построение такой архитектуры обеспечивает своевременную передачу оповещений безопасности из закрытого сегмента в центры SOC, а также исключает любое воздействие через этот же канал связи на защищённый сегмент сети.



AMT GROUP

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

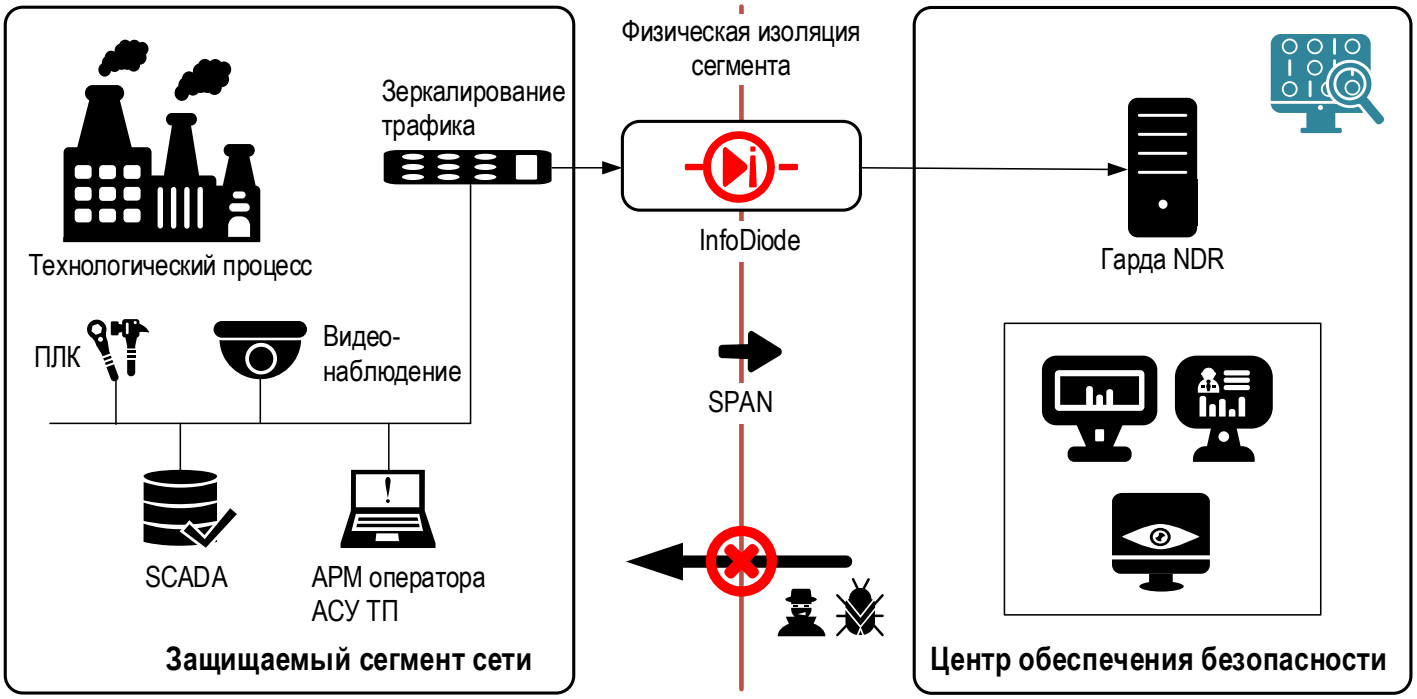
www.amt.ru
www.infodiode.ru

Сценарий работы Гарда NDR через однонаправленный канал передачи данных

Сценарий совместного использования комплекса однонаправленной передачи данных InfoDiode и комплекса Гарда NDR предполагает применение аппаратного комплекса InfoDiode между более доверенной сетью организации и центром безопасности SOC с развёрнутым в нем комплексом Гарда NDR, которые в свою очередь расположены в менее доверенном сетевом сегменте.

В результате такого комплексного подхода реализована передача SPAN трафика из промышленных или корпоративных сетей в центры SOC через диод данных по однонаправленному каналу. Комплекс Гарда NDR анализирует метаданные пакетов сетевого трафика, детектирует аномалии и отклонения от нормального поведения в сети, что позволяет выявить даже скрытые атаки и продвинутые угрозы и реагировать на сетевые инциденты. Комплекс способен работать как с копией сетевого траффика, так и с телеметрией (Netflow).

Совместное применение InfoDiode и Гарда NDR исключает возможность проникновения в доверенный сегмент сети в целях организации атаки, а также обеспечивает контроль за эталонным состоянием сети и управляющих команд в ней на основе анализа получаемого трафика.



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

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между платформой

Гарда Deception,

правообладателем которой является

ООО «Гарда Технологии»

603093, г. Нижний Новгород, ул. Родионова, д.192, корп. 1, пом. 153, оф. 901

в дальнейшем именуемыми «**Гарда Deception**» и «**Гарда Технологии**» соответственно

и

Комплексом однонаправленной передачи данных «AMT InfoDiode»,

являющийся продукцией компании

АО «АМТ-ГРУП»

119121, Россия, Москва, Ружейный переулок, д. 6, стр. 1

в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**» соответственно

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

Гарда Deception - платформа для создания ложного слоя сетевой инфраструктуры, дезинформирующего злоумышленников. Останавливает кибератаки до нанесения ущерба реальным объектам сети, предотвращая тем самым финансовые и репутационные потери компании. Решение Гарда Deception способно обнаружить злоумышленника как на самых ранних стадиях развития атаки, так и на более поздних этапах - когда злоумышленник уже прочно закрепился в сети и действует в ней, с точки зрения логики работы классических средств защиты, «легитимно».

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

АМТ-ГРУП и **Гарда Технологии** провели всесторонние тесты платформы **Гарда Deception** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

- при установке **InfoDiode** между ПО **Гарда Deception**, выступающим в роли ловушки в закрытом сегменте и SIEM системой, размещенной в открытом сегменте.

Результаты тестирования:

- продукты могут использоваться совместно в указанном сценарии, с учетом их индивидуальных системных требований;
- подтверждена полная совместимость продуктов в заявленном сценарии использования.

АО «АМТ-ГРУП»

18 сентября 2024 года

Технический директор

Подпись _____ (Е.В. Молчанов)

ООО «Гарда Технологии»

18 сентября 2024 года

Заместитель генерального директора по продажам

Подпись _____ (Р.Н. Хайретдинов)

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между платформой

Гарда NDR,

правообладателем которой является

ООО «Гарда Технологии»

603093, г. Нижний Новгород, ул. Родионова, д.192, корп. 1, пом. 153, оф. 901

в дальнейшем именуемыми «**Гарда NDR**» и «**Гарда Технологии**» соответственно

и

Комплексом однонаправленной передачи данных

«AMT InfoDiode»,

являющимся продукцией компании

АО «АМТ-ГРУП»

119121, Россия, Москва, Ружейный переулок, д. 6, стр. 1

в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**» соответственно

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

Гарда NDR – решение для защиты от сложных и неизвестных киберугроз на основе анализа сетевого трафика и телеметрии, с возможностью активного реагирования на инциденты.

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

«АМТ-ГРУП» и **Гарда Технологии** провели всесторонние тесты платформы **Гарда NDR** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

- при установке аппаратных продуктов **InfoDiode** (АК InfoDiode RACK single/double, АК InfoDiode MINI) между сетью предприятия (закрытый сегмент) и центром SOC (открытый сегмент), где развёрнут комплекс **Гарда NDR**

Результаты тестирования:

- продукты могут использоваться совместно в указанном сценарии, с учетом их индивидуальных системных требований;
- подтверждена полная совместимость продуктов в заявленном сценарии использования.

АО «АМТ-ГРУП»

7 октября 2024 года

Технический директор

Подпись _____

(Б.В. Молчанов)

ООО «Гарда Технологии»

7 октября 2024 года

Заместитель генерального директора по продажам

Подпись _____

(Р.Н. Хайретдинов)