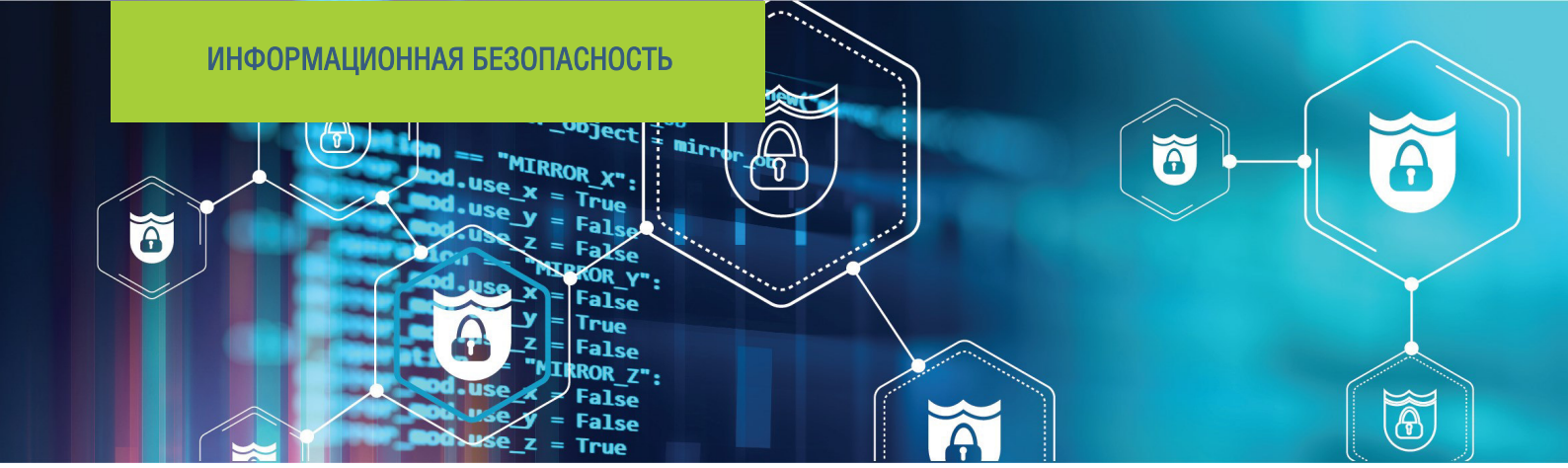


Применение HoneyPot и Deception с однонаправленным шлюзом InfoDiode

В результате кибератак на доверенные сети предприятий и организаций может существенно пострадать критическая инфраструктура. Для предотвращения кибератак требуется своевременно выявлять признаки вторжения и передавать соответствующие оповещения в центр мониторинга безопасности (SOC). В решении этой задачи помогают специализированные продукты — средства обнаружения вторжений (СОВ, Intrusion Detection Systems, IDS). Одним из примеров IDS систем являются системы класса Deception, которые получили также название HoneyPot. Этот класс решений позволяет обеспечивать мониторинг и реагирование на действия злоумышленника в закрытых сетях, не оказывая влияния на промышленные процессы.

SOC зачастую расположен в отдельном сегменте сети, что автоматически требует обеспечения надёжной защиты сетевого периметра доверенного сегмента при передаче оповещений кибербезопасности. «Воздушный зазор» между защищаемым сегментом и корпоративной сетью не позволяет реализовать указанную задачу, в то время как применение только программных средств защиты создает значительные риски для объектов КИИ. В таких сценариях целесообразно использовать решения по однонаправленной передаче данных, которые физически изолируют защищаемый сегмент и, при этом, позволяют организовать доставку оповещений в центр мониторинга безопасности.

Одной из систем класса Deception является решение HoneyCorn, которое представляет собой специализированную систему класса HoneyPot и Deception, позволяющую выявлять злоумышленника как на ранних, так и на поздних стадиях проникновения в сеть, максимально препятствуя развитию атаки. При выявлении атаки HoneyCorn позволяет изучать действия злоумышленника, собирать данные о нем в целях принятия нужных административных решений, или сразу воспользоваться готовыми шаблонами принятия решения по защите от кибератаки.

InfoDiode – это продукт, построенный на принципах однонаправленной передачи данных и позволяющий обеспечить эффективную защиту доверенного сегмента. Технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, обеспечивают возможность передачи данных в одном направлении и нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

Результаты комплексного тестирования подтвердили успешное и эффективное совместное применение **АПК InfoDiode SMART** и СОВ HoneyCorn для обеспечения высочайшего уровня защиты критических сетевых сегментов и передачи оповещений о киберугрозах за границу периметра КИИ. Таким образом обеспечивается своевременное обнаружение киберугроз внутри защищаемого сегмента и передача оповещений во внешний центр мониторинга безопасности через однонаправленный канал, предотвращающий внешнее воздействие на защищаемый сегмент.

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

28.08.2024

Сценарий передачи оповещений из закрытого сегмента в центр мониторинга безопасности

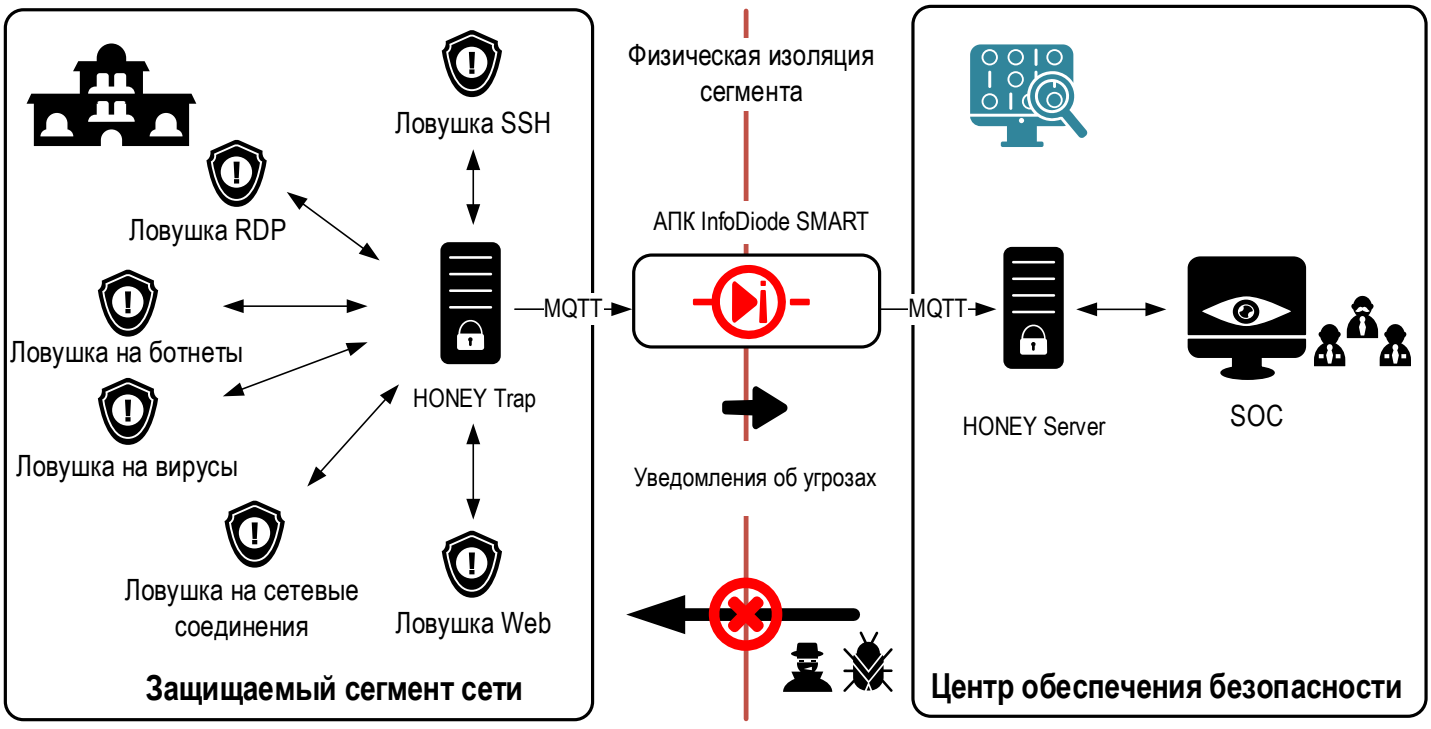
Центры мониторинга безопасности могут размещаться централизованно или даже предоставляться как «облачный сервис» за пределами периметра защищаемого сегмента сети. При этом очевидно, что объекты критической инфраструктуры должны поддерживать высокий уровень изоляции, предотвращающий любые внешние воздействия на объекты этих сетевых сегментов со стороны сегментов с другим уровнем доверия. Представленный сценарий демонстрирует решение этой задачи при помощи совместного использования HoneyCorn и **InfoDiode**.

InfoDiode в совместном решении выступает в качестве системы однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется канал для обеспечения передачи оповещений безопасности на внешний сервер HoneyCorn.

Архитектура совместного использования HoneyCorn и **InfoDiode** предполагает применение аппаратно-программных комплексов **InfoDiode SMART** между ПО HoneyCorn, выступающим в роли ловушки в закрытом сегменте, и ПО HoneyCorn, выполняющим роль сервера в открытом сегменте. При этом обеспечивается своевременная передача оповещений безопасности в SOC, а любое воздействие через этот же канал связи на защищённый сегмент сети полностью исключается.

В результате всестороннего тестирования установлено:

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



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 программным обеспечением класса HoneyPot и Deception

HoneyCorn

правообладателем которого является

ИП Прокопов Максим Дмитриевич

(630089, Новосибирская обл., город Новосибирск г.о., г. Новосибирск, ул. Бориса Богаткова, д. 226/1, кв. 208)

в дальнейшем именуемыми «**HoneyCorn**» и «**ИП Прокопов**» соответственно

и

Комплексом однонаправленной передачи данных «AMT InfoDiode»,

являющийся продукцией 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, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется нужный уровень их функциональности для взаимодействия со смежными информационными системами.

HoneyCorn является специализированной системой класса HoneyPot и Deception, позволяющей выявлять злоумышленника как на ранних, так и на поздних стадиях проникновения в сеть, максимально препятствуя развитию атаки. При выявлении атаки позволяет изучать действия злоумышленника для сбора данных необходимых при принятии административного решения или воспользоваться готовыми шаблонами принятия решения по защите от кибератаки. Данный класс продукта позволяет обеспечивать мониторинг и реагирование на действия злоумышленника в закрытых сетях, не оказывая влияния на промышленные процессы.

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

«АМТ-ГРУП» и **ИП Прокопов** провели всесторонние тесты ПО **HoneyCorn** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

- при установке **InfoDiode** между ПО **HoneyCorn**, выступающим в роли ловушки в закрытом сегменте и ПО **HoneyCorn**, выступающим сервером 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»

16 февраля 2024 года

Технический директор

Подпись _____

(Б. В. Молчанов)

ИП Прокопов Максим Дмитриевич

16 февраля 2024 года

Подпись _____

(М. Д. Прокопов)