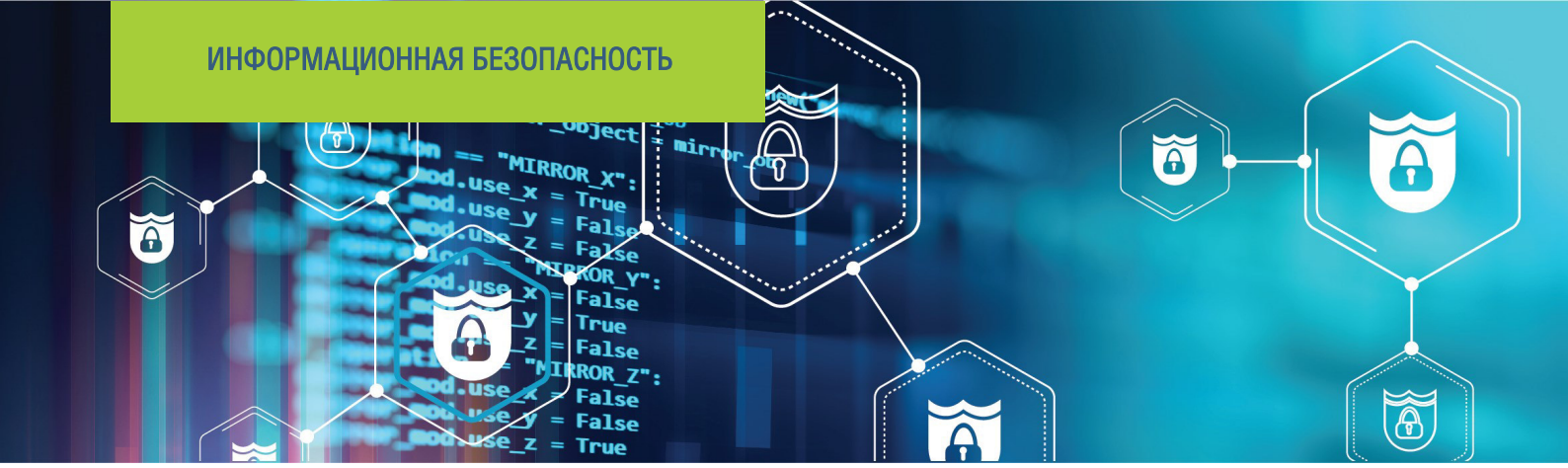


Применение САЗ RedCheck с однонаправленным шлюзом InfoDiode

Безопасность критической и значимой информационной инфраструктуры складывается из целого ряда факторов и, в том числе, зависит от применяемых инструментов, которые обеспечивают своевременный мониторинг состояния защищенности. Одним из наиболее действенных методов, способных опережать активно пополняющийся инструментарий злоумышленника, является использование систем анализа защищенности (САЗ). Примером таких систем является программное обеспечение RedCheck.

САЗ RedCheck – система анализа защищенности и соответствия стандартам, решающая задачи в повседневном цикле управления безопасностью ИТ-инфраструктуры предприятия. Принцип работы САЗ RedCheck подразумевает передачу отчётов ИБ, полученных в результате сканирования (вручную или по расписанию) сетевой инфраструктуры организации, в центр мониторинга безопасности (SOC), который, как правило, расположен в отдельном сегменте сети. Такое сопряжение сетевых сегментов потенциально допускает проникновение стороннего злоумышленника за сетевой периметр защищаемого объекта. В частности оно возможно ввиду особенностей двустороннего обмена информацией между сегментами. Двунаправленный канал связи несёт в себе риск компрометации злоумышленником как сети источника, так и самого средства защиты информации с возможностью дальнейшего развития удалённой атаки на защищаемый сегмент. В целях гарантированной изоляции контролируемого объекта с сохранением возможности передачи отчётов САЗ о состоянии защищенности этого объекта в центры SOC применяются средства однонаправленной передачи данных **InfoDiode**.

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 эффективное совместное применение комплексов **InfoDiode** и САЗ RedCheck в сценариях передачи данных от САЗ RedCheck в центры SOC и иным получателям. Таким образом обеспечивается изоляция более защищенного сетевого сегмента и сохраняется контроль за этим сегментом со стороны центра SOC и профильных служб.

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

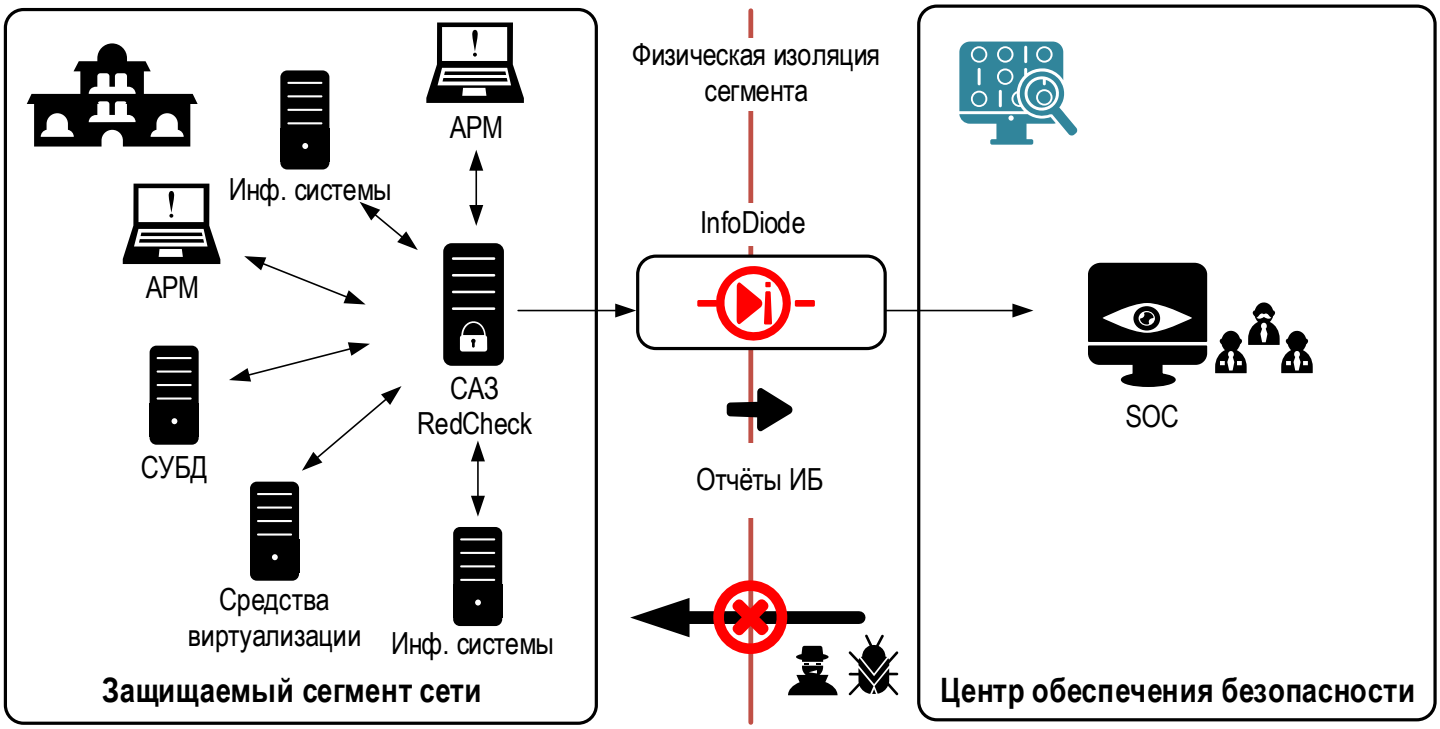
06.11.2024

Сценарий защищённой передачи отчётов ИБ в центр обеспечения безопасности

На практике использование комплекса однонаправленной передачи данных InfoDiode и СА3 RedCheck предполагает применение комплекса InfoDiode между закрытым сегментом, с развёрнутой в нём системой анализа защищенности RedCheck, и центом SOC, расположенном в открытом сегменте.

Совместное использование решений позволяет физически изолировать более доверенный сетевой сегмент и, таким образом, повысить его защищенность. При этом сохраняется возможность передачи информации от СА3 Redcheck из изолированного сегмента в центры SOC, то есть, за периметр защищаемого объекта.

Построение такой архитектуры обеспечивает своевременный анализ защищенности более доверенного сетевого сегмента специалистами SOC, оперативное реагирование на возникающие угрозы и своевременную переоценку рисков, возникающих в изолированном сегменте в связи с появлением новых угроз и уязвимостей.



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 системой анализа защищенности

RedCheck

правообладателем которой является

АО "АЛТЭКС-СОФТ"

(141090, Московская обл., г. Королев, мкр. Болшево, ул. Маяковского, д. 10А, пом.VII (3 этаж))

в дальнейшем именуемыми «**САЗ RedCheck**» и «**АЛТЭКС-СОФТ**» 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.

САЗ RedCheck – система анализа защищенности и соответствия стандартам, решающая задачи в повседневном цикле управления безопасностью IT-инфраструктуры предприятия. Система предназначена для получения данных о параметрах ИТ-инфраструктуры, влияющих на защищенность объектов информатизации, а также для поддержки принятия решений по устранению выявленных уязвимостей и созданию эффективных конфигураций безопасности контролируемых систем.

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

«АМТ-ГРУП» и **АЛТЭКС-СОФТ** провели всесторонние тесты платформы **САЗ RedCheck** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

- Отчёты ИБ, полученные в результате работы **САЗ RedCheck** по сканированию сетевой инфраструктуры организации в закрытом сегменте, передаются через **InfoDiode** на сервер SOC или иным получателям, расположенным 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»

21 октября 2024 года

Технический директор

Подпись _____

(Б.В. Молчанов)

АО "АЛТЭКС-СОФТ"

21 октября 2024 года

Генеральный директор

Подпись _____

(В.Н. Сердюк)