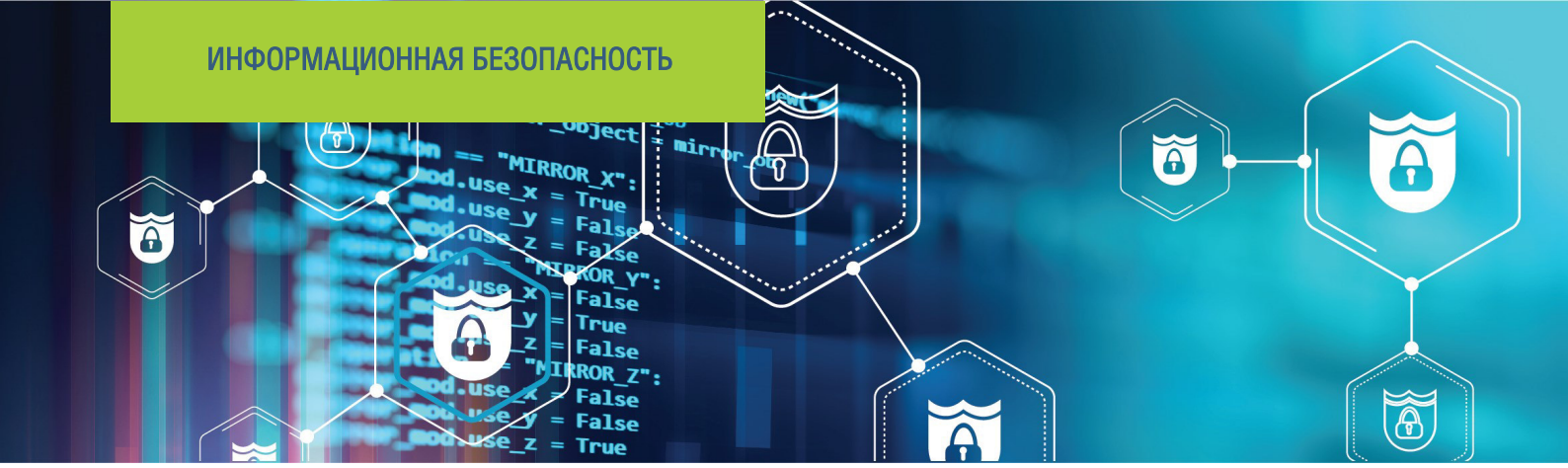


Применение Kaspersky MLAD с однонаправленным шлюзом InfoDiode

Современные промышленные предприятия становятся все более «цифровыми», активно инвестируют в интеллектуальные технологии, новые системы автоматизации, создание цифровых двойников и реализуют концепцию «четвертой промышленной революции». Данные из технологического сегмента являются основой для принятия экономических и управленческих решений, а «большие данные» служат основой для долгосрочного прогнозирования, поиска отклонений и проблем в технологических процессах.

Чтобы получать данные регулярно и безопасно, предприятиям приходится пересматривать подходы к защите промышленных и технологических сегментов. «Воздушный зазор» исключает саму возможность передачи данных для внешних потребителей, но дает гарантию защиты. Отказ от «воздушного зазора» и ориентир на программные средства защиты создает значительные риски проникновения злоумышленника внутрь критической инфраструктуры и нарушения процессов ее функционирования. Помимо этого само оборудование и протоколы обмена в технологических и промышленных сетях требуют применения отдельного класса решений по обеспечению кибербезопасности, которые существенно отличаются от традиционных «офисных» средств защиты.

InfoDiode и Kaspersky MLAD разработаны специально для промышленных предприятий и объектов критической инфраструктуры.

Kaspersky Machine Learning for Anomaly Detection (MLAD) – является специализированным программным решением, которое анализирует существующий поток телеметрии технологического процесса с целью обнаружить отклонения в технологическом процессе или в работе оборудования на самом раннем этапе вне зависимости от их природы.

InfoDiode - это продукт, построенный на принципах однонаправленной передачи данных и позволяющий обеспечивать эффективную защиту доверенного сегмента. Технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, обеспечивают возможность передачи данных из закрытого контура во внешние сети, тем самым нивелируя риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

Результаты комплексного тестирования подтвердили успешное и эффективное совместное использование продуктов. Совместное применение позволяет обеспечить сбор данных о состоянии технологических процессов и промышленного оборудования в закрытом сегменте и гарантировать, что применяемые инструменты сбора и инфраструктура недоверенного сегмента никак не воздействует на защищаемый с помощью InfoDiode объект. В рамках совместного решения MLAD может получать оперативные данные непосредственно с промышленной инфраструктуры в целях формирования моделей прогнозирования.

AMT GROUP

115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

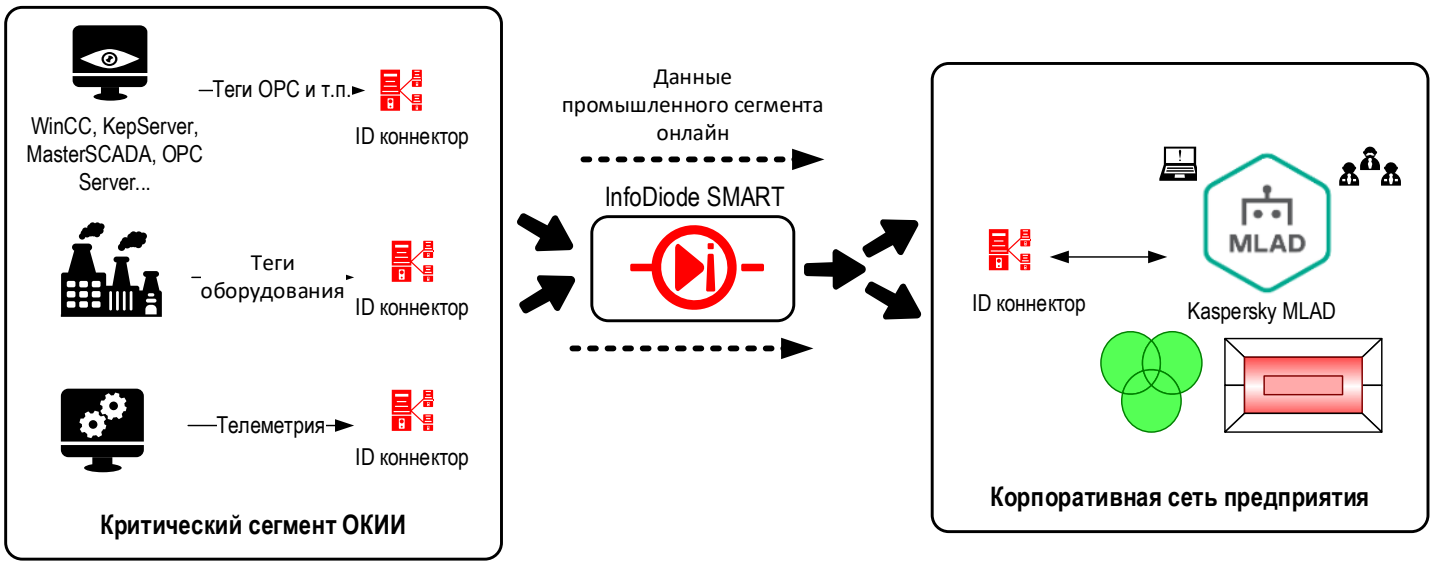
23.10.2024

Сценарий передачи данных SCADA из закрытого сегмента в Kaspersky MLAD

Kaspersky MLAD не воздействует на объект, не вмешивается в контур управления и в передачу данных, однако, для его функционирования требуется обеспечить канал передачи данных, являющийся источником потенциальных уязвимостей для промышленного сегмента сети. Эту проблему можно решить путём установки **InfoDiode** на границе периметра промышленного сегмента. Данный сценарий демонстрирует совместное использования MLAD и **InfoDiode** при организации удалённого мониторинга промышленных объектов.

InfoDiode в совместном решении выступает в качестве системы однонаправленной передачи данных, обеспечивающей передачу данных SCADA систем, OPC серверов, источников промышленного трафика в целях организации функционирования ситуационных центров, центров мониторинга, диспетчерских, аналитических центров, находящихся за границей периметра КИИ, в условиях его гарантированной изоляции. В частности, обеспечивает канал для обеспечения передачи анализируемого трафика на серверы MLAD.

Архитектура совместного использования MLAD и **InfoDiode** предполагает применение комплекса **InfoDiode** между источником анализируемого трафика в промышленном сегменте и MLAD в корпоративном сегменте сети предприятия. Таким образом, промышленный трафик из защищённого сегмента поступает в Kaspersky MLAD для проведения анализа и оповещения об обнаруженных аномалиях, а любое воздействие через этот же канал связи на защищённый сегмент сети полностью исключается.



AMT GROUP

115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программными продуктами

Kaspersky Machine Learning for Anomaly Detection

продукция компании

АО «Лаборатория Касперского»

Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2

в дальнейшем именуемыми «**Kaspersky MLAD**»

и «**Лаборатория Касперского**» соответственно

и

Комплексом

InfoDiode однонаправленной передачи данных

продукция компании

АО «АМТ-ГРУП»

Россия, 119121, Москва, Ружейный переулок, 6с1

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

AMT GROUP -Diode kaspersky

Комплекс **InfoDiode** является решением для однонаправленной передачи промышленных протоколов. Обеспечивает передачу данных SCADA систем, OPC серверов, источников промышленного трафика в целях организации функционирования ситуационных центров, центров мониторинга, диспетчерских, аналитических центров, находящихся за границей периметра КИИ, в условиях его гарантированной изоляции.

Kaspersky MLAD – программное решение, которое использует методы машинного обучения (искусственного интеллекта) для анализа данных телеметрии промышленных установок с целью раннего выявления отклонений в технологическом процессе или в работе оборудования. Решение позволяет обнаруживать скрытые проблемы оборудования, ошибки персонала или специализированные атаки до того, как предприятию будет нанесен ущерб.

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

Лаборатория Касперского и **АМТ-ГРУП** провели всесторонние тесты программного обеспечения **Kaspersky MLAD** при совместном использовании с комплексом **InfoDiode** в сетях передачи данных промышленных объектов в следующем сценарии:

- комплекс **InfoDiode** обеспечивает в реальном времени однонаправленную передачу данных телеметрии по протоколу OPC UA от объекта мониторинга (SCADA, OPC-сервер, оборудование), расположенного в промышленном (закрытом) сегменте, на сервер **Kaspersky MLAD**, расположенный в недоверенном (открытом) сегменте корпоративной сети передачи данных.

В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно в заявленном сценарии.

АО «АМТ-ГРУП»

02 сентября 2024 года

Технический директор

Подпись_____

(Б.В. Молчанов)

АО «Лаборатория Касперского»

02 сентября 2024 года

Управляющий директор в России и странах СНГ

Подпись_____

(А.В. Кулашова)