Александр ПОЗНЯКЕВИЧ:
«Есть ли место XDR в промышленной сети»

Цифровизация отечественных предприятий набирает обороты, причем не только в офисном сегменте, но и в промышленной сети, где происходит операционная деятельность предприятия. Именно потому эти технологии называют операционными – OT, чтобы отличить их от классической офисной автоматизации. Однако безопасность операционных технологий часто страдает, поскольку нередко считается, что хакеры до них добраться не могут. Однако опыт показывает, что это не так. По теме обнаружения присутствия внешних злоумышленников в промышленных сегментах сети мы задали несколько вопросов руководителю направления по защите промышленных инфраструктур «Лаборатории Касперского» Александру Познякевичу.

– Что такое XDR и для чего он нужен компаниям?

– Хотя рынок решений класса XDR (от англ. Extended Detection and Response – расширенные обнаружение и реагирование) находится в процессе становления, перспективы его применения уже горячая тема в информационной безопасности. Четкого списка технологий, которые должны входить в XDR, на данный момент нет. Но речь идет об объединении данных, телеметрии и ключевых защитных решений в единую платформу для выявления киберинцидентов и реагирования на них. Это синхронизированные друг с другом средства защиты, системы мониторинга, обнаружения и реагирования на инциденты в промышленной сети, защищенные веб-шлюзы, EDR-решения и SIEM-системы, которые и являются объединяющим звеном, фактически мозгом комплексной системы ИБ. Такая платформа позволяет улучшить процесс анализа и принятия решений, сократить среднее время обнаружения инцидента и реагирования на него, сделать более эффективной работу отделов информационной безопасности. Многие разработчики средств защиты развивают свои продуктовые портфели в этой парадигме.

– Какое применение находит XDR в операционных технологиях (OT) и, в частности, в промышленных сетях?

– Одна из ключевых проблем в области безопасности OT-сред заключается в том, что промышленные организации, которые пытаются защитить свои операционные технологии, полагаются при поиске индикаторов атаки исключительно на данные сетевого трафика. Однако многие сложные киберугрозы, особенно те, которые нацелены на конечные устройства, нельзя обнаружить с помощью только этих данных. И даже если в сетевом трафике будет выявлена подозрительная активность, необходимые меры реагирования, такие как реконфигурация системы, приняты не будут, поскольку это лишь источник данных. В XDR же входят технологии, которые в том числе предполагают активное реагирование на угрозу.

Ключевое преимущество XDR в вопросах безопасности OT-сред заключается в том, что такая платформа сочетает данные, получаемые как с уровня конечных узлов (посредством EDR-агентов), так и из других источников – мониторинг сети, идентификационные данные, информация о фактах предоставления доступа к ресурсам. Все это дает последовательную картину того, что происходит в промышленной сети, на конечных узлах и в приложениях и, как следствие, дает возможность устранить угрозу до того, как она превратится в инцидент информационной безопасности.

– XDR – это только обнаружение угроз?

– Нет. XDR – это еще и аналитика. В дополнение к расширенному доступу к информации об угрозах из источников внутри OT-инфраструктуры XDR позволяет обращаться к регулярно обновляемым потокам данных об угрозах и аналитическим отчетам из внешних источников.

Ключевой источник данных по передовым угрозам – это база данных MITRE ATT&CK.

Это глобально доступный источник тактик, техник и процедур злоумышленников, основанный на наблюдениях из реального мира. База включает также специфические тактики и техники, используемые для атак на автоматизированные системы управления (АСУ). Описывается вся последовательность действий атакующих: начиная с того, как они получают начальный доступ, действуют в системе, закрепляются в ней, повышают свои привилегии, и заканчивая тем, какие способы они используют, чтобы избежать обнаружения, как перемещаются по сети, собирают информацию и контролируют устройства.

В целом XDR также дает возможность включать в средства контроля безопасности самые актуальные промышленные потоки данных об угрозах (Threat Intelligence) – актуальные для конкретных отраслей, регионов или даже отдельных предприятий.

– Как лучше всего внедрять XDR-подход в OT-среды?

– Чтобы реализовать преимущества XDR, нужно следовать определенным правилам. Должны быть предоставлены три главные функции: централизованный сбор данных об угрозах, анализ передовых угроз и интегрированное реагирование на них. В целом XDR-платформа для промышленного сегмента должна создаваться с учетом специфики OT-сред для каждой из этих функций.

Централизованный сбор данных должен предлагать следующие функции: извлечение данных из промышленных сетевых протоколов на уровне сети и узла; безопасный сбор событий и телеметрии с узла; получение данных с устаревших операционных систем (Windows/ Linux). Причем инструменты сбора данных не должны перегружать сеть и ресурсы узла, а сам процесс сбора данных должен быть легким в настройке и поддержке (в идеале не должна требоваться перезагрузка устройства). Следует отметить, что атрибуты промышленных активов и изменения в процессах и данных телеметрии – это важные источники данных для корреляции событий, поиска аномалий и корреляции с киберфизическими инцидентами.

Анализ продвинутых угроз должен строиться следующим образом: XDR-разработчики должны вносить обнаруженные угрозы в базу MITRE ATT&CK. Причем потоки данных об угрозах должны включать не только индикаторы компрометации (IoC), но и техники, тактики и процедуры из базы MITRE, включая сигналы о подозрительном поведении промышленных протоколов, подозрительную активность на промышленных устройствах (программно-логических контроллерах и удаленных терминалах).

Функция автоматизированного реагирования на угрозы должна использовать нативную интеграцию или интеграцию по API с решениями по ИБ и основываться на фреймворке RE&CT Framework.

– Каково место XDR (в частности промышленного) в комплексной системе защиты современного цифровизированного предприятия?

– Ландшафт киберугроз постоянно меняется, и промышленная кибербезопасность сегодня гораздо шире, чем просто защита периметра. По предварительным данным Kaspersky ICSCERT, кибератакам в 2022 г. подверглось более 43% компьютеров АСУ, а основным источником киберугроз для промышленных предприятий остается Интернет. Несмотря на то что технологические сети стараются полностью изолировать от интернет-ресурсов и приложений, доступ к ним – неотъемлемая часть ИТ- и зачастую OT-сегмента. Опасность сегодня может прийти из любого узла сети. Это необходимо учитывать при разработке подхода к защите в промышленности, поэтому следующая ступень – всеобъемлющая защита всего предприятия от офисов до производственных площадок.

> В основе нашей промышленной экосистемы лежит XDR-платформа Kaspersky Industrial CyberSecurity

Современные экосистемные решения, разработанные специально для технологического сегмента, например Kaspersky OT CyberSecurity, органично и без потери производительности интегрируются с продуктами для корпоративного сегмента и позволяют полностью защитить всю инфраструктуру предприятий и минимизировать убытки, связанные с киберинцидентами. Это существенно экономит ресурсы команды ИБ и дает ей полную картину безопасности предприятия и эффективные инструменты аналитики и противодействия угрозам.

В основе нашей промышленной экосистемы лежит XDR-платформа Kaspersky Industrial Cyber Security, объединяющая два нативно интегрированных решения: для мониторинга сети – пассивный мониторинг сети с возможностью активного опроса и для защиты конечных промышленных узлов и рабочих станций – со встроенной функцией EDR. ■

Подробнее о Kaspersky OT CyberSecurity