FORTINET

Как разрабатывать средства безопасности для сетевых сред OT

Профилактика, выявление и правильное реагирование на продвинутые угрозы

Содержание

Аннотация

Сложные кибератаки представляют угрозу для промышленных систем управления (ICS) и систем диспетчерского управления и сбора данных (SCADA). По мере объединения сетей эксплуатационных технологий (OT) с сетями информационных технологий (IT) расширение площади атаки позволяет злоумышленникам создавать продвинутые угрозы, направленные на эти критически важные системы. Системы ICS и SCADA в OT-сетях предъявляют уникальные эксплуатационные требования, вследствие чего их защита может оказываться сложнее по сравнению с IT-секторами тех же сетей. Поэтому для OT-сетей требуются специальные подходы к обеспечению безопасности и решения.

Автоматизированные приемы обеспечения безопасности и обманные технологии могут помочь выявлять продвинутые угрозы в OT-сетях. Центральным элементом такой стратегии является анализ угроз с учетом специфики OT-сферы, позволяющий оперативно выявлять угрозы, направленные на множество объектов OT или на отрасль в целом, и реагировать на них.

64% лиц, принимающих решения в области OT, считают, что сложные кибератаки являются одной из приоритетных проблем.[1]

Введение

Системы эксплуатационных технологий (OT) сталкиваются с новыми киберугрозами. В прошлом OT-сети были физически изолированы от IT-систем «воздушным зазором». Однако для более эффективного внедрения цифровых инноваций многие организации отказываются от такого воздушного зазора или сводят его к минимуму. В результате OT- и IT-сети теперь чаще соединены друг с другом, и киберпреступники используют IT-сети как базу для доступа к OT-сетям.

OT-системы часто имеют большой возраст — в некоторых случаях их компоненты служат уже по 20 и более лет. Неудивительно, что такие устройства нередко имеют множество уязвимостей, которые легко использовать и которые были обнаружены за прошедшие годы. Это старые угрозы. Сейчас злоумышленники создают новые угрозы, так как даркнет позволяет реализовывать новые сложные атаки — многовекторные и направленные конкретно на операторов OT-систем.

Уникальные требования к доступности OT-инфраструктуры означают, что решения для обеспечения безопасности необходимо тщательно разрабатывать таким образом, чтобы они минимально влияли на операции системы. К тому же OT-сети должны соответствовать специальным регламентам для OT-систем — например тем, которые разрабатывают Национальный институт стандартов и технологий (NIST) и Североамериканская корпорация по вопросам надежности электроснабжения (NERC), или Директиве Европейской комиссии по безопасности сетей и информационных систем (Директива NIS).

Автоматизированное выявление угроз и реагирование, специальная аналитика угроз в OT-сфере, обманные технологии и сегментация сетей — четыре ключевых элемента надежного подхода к защите OT-систем от продвинутых угроз.

Почти в трех четвертях организаций, использующих OT-системы, IT- и OT-сети соединены между собой.[2]

Автоматизированное выявление угроз и реагирование на них повышают доступность систем

Злоумышленники, создающие продвинутые угрозы, располагают ресурсами и квалификацией для разработки атак, недоступных для обнаружения традиционными средствами. Организациям необходимы глубокий уровень отслеживания сетей и высокая осведомленность о текущей ситуации, чтобы отличать реальные угрозы от ложных срабатываний, проводить атрибуцию, распознавать признаки атаки и идентифицировать злоумышленников.

Достижение необходимого уровня отслеживания и осведомленности о текущей ситуации для оперативного реагирования на инциденты требует автоматизации. Автоматизированный сбор, агрегирование и анализ данных о безопасности помогают выявлять реальные угрозы (вместо выдачи огромного количества ложных срабатываний) и дают необходимый контекст для точного реагирования на угрозы и устранения последствий.

Автоматизация позволяет также быстрее реагировать на выявленную угрозу. Создав кодифицированные сценарии реакции на распространенные угрозы, организация может автоматизировать элементы процесса выявления угроз и устранения последствий. Это помогает обеспечить соблюдение строгих требований к доступности OT-систем, так как при выявлении аналитиком активной угрозы некоторые или все шаги по устранению последствий могут быть предприняты мгновенно, сведя к минимуму влияние угрозы на операции организации.

Повышенная осведомленность о текущей ситуации и автоматизированное реагирование на инциденты помогают обеспечить безопасность и доступность OT-систем. Целенаправленные ответные действия, идентифицирующие и устраняющие угрозы на уровне процессов, минимизируют нарушение доступности системы в связи с реагированием на инцидент.

78% организаций имеют только фрагментарную централизованную видимость своей OT-среды.[3]

Автоматизация повышает доступность систем благодаря быстрой и целенаправленной реакции на киберугрозы.

Специализированный анализ угроз в OT-сфере позволяет выявить уникальные угрозы

OT-системы представляют собой важные мишени. Злоумышленники готовы вкладывать необходимое время и ресурсы, чтобы выявить и использовать уязвимости в таких системах. Обычно они проводят пробные атаки на конкретные OT-системы. Скрывать свои действия им помогает тот факт, что в таких системах применяются собственные протоколы сетей, часто непонятные решениям по обеспечению кибербезопасности, которые были разработаны для IT-сетей.

Управление киберугрозами в OT-сетях требует хорошего знания их специфики и многолетнего опыта обеспечения безопасности OT-сред. Для защиты OT-сетей необходим доступ к специализированной аналитике угроз в OT-сфере. Поскольку в OT-организациях используется оборудование, созданное ограниченным рядом поставщиков, для эффективной защиты необходимо понимать уязвимости, присутствующие в таких продуктах. Это позволяет поставщикам OT-решений предотвращать взлом своих систем и развертывать виртуальные исправления для эффективной защиты уязвимых систем в течение длительных промежутков между техническим обслуживанием.

Организациям также необходима возможность делиться результатами анализа угроз как с внутренними, так и с внешними заинтересованными лицами, и использовать стороннюю аналитику угроз. Это позволяет выявлять широкие специализированные кампании, направленные на конкретные OT-системы, и реагировать на них, используя технологии искусственного интеллекта (AI) и машинного обучения (ML).

85% OT-угроз направлены на машины, работающие под управлением протоколов OPC Classic, BACnet и Modbus.[4]

Для решений по обеспечению кибербезопасности OT-систем требуется знание специфики угроз и протоколов в OT-сфере.

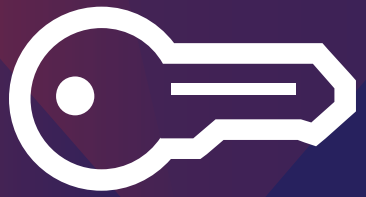
Обманные технологии позволяют выявлять продвинутые угрозы

Авторы продвинутых угроз часто разрабатывают «низкие и медленные» атаки, которые ускользают от традиционных средств защиты сетей. При этом злоумышленник может присутствовать в сети организации, не обнаруживая себя.

Выявить такие труднообнаружимые атаки помогают обманные технологии. Ловушки можно настроить так, чтобы они напоминали реальные OT-системы и привлекали злоумышленника или его вредоносный код к совершению попытки взлома.

Если это происходит, это указывает на присутствие угрозы в теневой сети, так как для разрешенных операций эти системы не используются. Кроме того, изучение подробных данных о действиях злоумышленника в системе может помочь собрать ценные сведения о его инструментах, методах и возможностях. Такая аналитика угроз улучшает выявление и устранение последствий таких угроз в других системах в OT-сети и может помочь организации выявлять атаки «нулевого дня», которые традиционные системы на основе сигнатур обнаружить не способны.

Также для защиты OT-систем эффективно развертывание «песочниц», позволяющих эмулировать конкретные OT-системы. Автоматизированные инструменты и технологии машинного обучения позволяют выявлять неизвестные угрозы путем обнаружения аномального или подозрительного поведения при запуске в такой эмулированной среде.



«Ключ к созданию хорошей ловушки — реалистичность. Она не должна быть защищена настолько хорошо, чтобы ее было невозможно взломать, но не должна также быть настолько доступной, что злоумышленник просто не поверит в нее. Если он распознает ловушку, то сможет ее избежать. Поэтому она ничем не должна отличаться от остальной сети».[5]

Сегментация сетей для изоляции и ограничения распространения угроз

К доступности OT-сред предъявляются чрезвычайно высокие требования, что не способствует эффективной киберзащите. Из-за коротких промежутков для технического обслуживания и высоких требований к доступности многие устройства работают под управлением операционных систем и программного обеспечения, срок поддержки которых уже истек. Часто на старом оборудовании отсутствуют ресурсы для запуска традиционных антивирусных систем. Наконец, в случае инцидента может отсутствовать возможность отключения пострадавших систем для устранения последствий.

Все эти факторы приводят к тому, что обеспечением безопасности OT-систем часто необходимо заниматься на уровне сети, а не конечных устройств. Используя сегментацию сетей и виртуальные исправления, можно снизить риск, создаваемый уязвимыми устройствами без установленных исправлений. Вместо установки обновлений на устройство, что может отрицательно повлиять на доступность системы, виртуальные исправления позволяют блокировать трафик, пытающийся использовать известную уязвимость, прежде чем она достигнет уязвимого устройства.

Сегментация сетей также помогает снизить последствия нарушения безопасности, ограничивая горизонтальное распространение вредоносного содержимого в сети. Сегментация предусматривает проверку всего обмена данными между устройствами на вредоносное или аномальное содержимое и принудительное внедрение строгой проверки подлинности пользователей и контроля доступа во всей сети.

В OT-организациях верхнего уровня вероятность использования сегментации сетей на 51% выше, чем в организациях нижнего уровня.[6]

Сегментация сетей необходима для предотвращения горизонтального распространения продвинутых угроз в OT-сетях.

Заключение

OT-сети все чаще становятся мишенью для продвинутых киберугроз. Злоумышленники хорошо разбираются в OT-системах и создают специальное вредоносное ПО, чтобы использовать уязвимости распространенных в OT-средах систем.

Руководители, отвечающие за эксплуатацию сетей, должны понимать, что площадь атаки на них расширяется, и рассматривать возможность автоматизации функций безопасности, внедрения обманных технологий для анализа специальных угроз в OT-сфере и сегментации сетей для борьбы с продвинутыми угрозами.

При этом им следует задать себе, в частности, следующие вопросы:

- Имеются ли у нас автоматизированные рабочие процессы для реагирования на инциденты и управления событиями, которые позволят устранить последствия успешного вторжения до того, как угроза распространится и нанесет ущерб?
- Наша инфраструктура безопасности интегрирована и позволяет передавать данные об угрозах в режиме реального времени на все элементы систем безопасности?
- У нас имеются такие средства противодействия продвинутым угрозам, как ловушки и «песочницы»?
- Мы приняли меры для сокращения площади атаки и блокирования доступа вредоносного ПО к сетевым ресурсам после вторжения?

[1] Исследование «Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?», Siemens and Ponemon Institute, 2019 г.

[2] Исследование «Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks», Fortinet, 28 июня, 2019 г.

[3] Отчет «2020 State of Operational Technology and Cybersecurity Report», Fortinet, 30 июня 2020 г.

[4] Отчет «Fortinet 2019 Operational Technology Security Trends Report», Fortinet, 8 мая 2019 г.

[5] Кевин Таунсенд (Kevin Townsend), «How Deception Technology Can Defend Networks and Disrupt Attackers», SecurityWeek, 5 июня 2019 г.

[6] Отчет «2020 State of Operational Technology and Cybersecurity Report», Fortinet, 30 июня 2020 г.

www.fortinet.com/ru

726519–0–0–RU

ноября 22, 2020 7:46 PM

eb-how-to-design-security-for-ot-network-environments_RU