ИССЛЕДОВАНИЕ

Решения Fortinet для обеспечения кибербезопасности в нефтегазовой отрасли

Защита критической инфраструктуры и ресурсов от киберугроз и физических угроз с помощью интеграции

Аннотация

Инфраструктура нефтегазовых компаний не только приносит прибыль отдельным организациям, но и обеспечивает экономическую и геополитическую стабильность во всем мире. На разных этапах нефтедобычи — от буровых площадок и трубопроводов до нефтеперерабатывающих заводов — существует множество рисков, которые обусловлены самыми разными мотивами злоумышленников. Более десяти лет компания Fortinet предоставляет комплексные интегрированные решения в области физической и информационной безопасности для нефтегазовой отрасли и ее удаленной инфраструктуры. Устройства повышенной прочности выполняют свои задачи в самых суровых условиях окружающей среды, многоуровневые системы безопасности обеспечивают защиту удаленных пунктов добычи, переработки и транспортировки сырья. Для главных офисов нефтегазовых компаний разработана комплексная система безопасности Fortinet Security Fabric. Также эта архитектура охватывает розничные точки продажи бензина.

60 % нефтегазовых компаний недавно столкнулись с серьезными нарушениями кибербезопасности.[1]

Нефтяные и газовые компании владеют и управляют основными объектами критически важной инфраструктуры, которые имеют жизненно важное значение не только для деятельности компаний, но и для экономического и военного благосостояния страны. Операции по добыче, переработке и транспортировке сырья являются важнейшими объектами кибератак со стороны злоумышленников с различными мотивами — от личной выгоды до промышленного шпионажа и экономической дезорганизации[2]. По словам одного специалиста, «все составляющие нефтегазового цикла уязвимы, поэтому стандартные статические компоненты защиты не справляются со своими задачами»[3].

На первый взгляд это высказывание может показаться преувеличением, однако опасность вполне реальна. Атака на систему диспетчерского управления и сбора данных (SCADA), с помощью которой осуществляется управление морскими буровыми установками, нефтяными скважинами, трубопроводами или устройствами нефтепереработки, либо на IoT-устройства, которые предоставляют данные мониторинга для таких систем, может иметь разрушительные последствия.[4] Это может нанести существенный ущерб объектам, вызвать длительные перебои с поставками и даже привести к травмам и жертвам среди сотрудников, случайных прохожих и ближайших жителей.

Атаки на инфраструктуры на базе операционных технологий (OT) в последнее время участились[5]. Эта тенденция касается и корпоративных инфраструктур нефтегазовых компаний. Успешные атаки могут поставить под угрозу интеллектуальную собственность, такую как исследования данных разведки, а также создать риски безопасности данных для деловой и кадровой информации. Кроме того, подобные атаки не только затрудняют коммерческую деятельность, но и создают нормативные риски.

Более десяти лет компания Fortinet предоставляет комплексные решения в области безопасности для нефтегазовой отрасли и ее инфраструктур: от наземных и морских буровых площадок до нефтеперерабатывающих заводов, трубопроводов и АЗС. Основной составляющей стратегии является система безопасности Fortinet Security Fabric, которая обеспечивает интеграцию всех компонентов глобальной инфраструктуры нефтегазовых компаний.

Основные проблемы кибербезопасности в нефтегазовой отрасли

Основные проблемы кибербезопасности в нефтегазовой отрасли:

Оптимизация затрат

Для рынков нефтяного сырья свойственны существенные колебания продажной цены нефти, бензина и природного газа. Эта волатильность означает, что буквально за считанные дни прибыльная компания может начать нести операционные убытки. Таким образом, приоритетной задачей нефтегазовых компаний является минимизация издержек. Чтобы выжить в периоды низких цен, им приходится структурировать операции.

В связи с этим вопрос замены более старого и дорогостоящего оборудования из-за уязвимостей в системе безопасности иногда даже не рассматривается. В этой ситуации специалисты разрабатывают такие обходные решения безопасности, которые не помешали бы рабочему процессу. В инфраструктуре многих компаний имеется множество элементов с уязвимостями подобного рода, которые ограничивают ресурсы кибербезопасности.

Дефицит специалистов по кибербезопасности усугубляется: согласно прогнозам, он превысит 4 миллиона сотрудников при том, что количество уже работающих специалистов составляет 2,8 миллиона[6]. Это означает, что попытки решить проблему путем найма дополнительных специалистов обойдутся очень дорого, к тому же на рынке труда может не оказаться профессионалов с конкретными навыками даже при условии высокой заработной платы. Более того, увеличение числа сотрудников не решает основной проблемы, которая заключается в том, что процессы обеспечения безопасности, выполняемые в ручном режиме, не эффективны против угроз, распространяющихся с высокой скоростью.

Отслеживание ИТ- и ОТ-систем

Распространение промышленных устройств IoT (IIoT) создало новые риски для систем диспетчерского управления и сбора данных (SCADA), служащих для управления буровыми установками, трубопроводами и нефтеперерабатывающими заводами. В прошлом системы SCADA, физически изолированные от Интернета, были практически не подвержены кибератакам, однако появление подключенных к сети датчиков и контроллеров изменило ситуацию.

В результате этого расширилась поверхность атак. Проблема усугубляется тем фактом, что многие IIoT-устройства не имеют средств управления, поэтому их нельзя обновить с помощью исправлений системы безопасности. Чтобы закрыть эти бреши в безопасности, организации часто внедряют множество изолированных специализированных средств защиты[7]. Системы, состоящие из неинтегрированных решений, создают сложности[8] и негативно влияют на отслеживание, замедляя процессы обнаружения угроз, предотвращения атак и реагирования на них. Это увеличивает риск того, что быстро распространяющаяся угроза проникнет в систему раньше, чем ее обнаружат с помощью процессов, выполняемых вручную.

Операционная эффективность

Эта архитектурная фрагментация также увеличивает неэффективность работы специалистов по кибербезопасности. Без комплексной интеграции всех элементов безопасности автоматизация процессов безопасности невозможна. При этом контроль многих процессов обеспечения безопасности должен осуществляться в ручном режиме, что вынуждает высокооплачиваемых сотрудников тратить время. Системы безопасности усложняются, из-за этого руководители сталкиваются с необходимостью нанимать специалистов в разных сферах. К примеру, перед проведением аудита некоторые организации отвлекают сотрудников от выполнения других задач для составления отчетов вручную.

Изолированность компонентов архитектуры также создает избыточность в управлении приложениями и даже в лицензировании программного и аппаратного обеспечения, снижая эффективность специалистов по юридическим вопросам, закупкам и финансам, которые управляют этими лицензиями. Также в организациях могут столкнуться с ростом технологических издержек из-за работы с несколькими поставщиками, предоставляющими разные продукты с частично одинаковым функционалом.

Уровень удовлетворенности клиентов

Розничные продавцы топлива взаимодействуют со своей клиентской базой с помощью различных электронных средств, включая инфраструктуру торговых терминалов (POS) с возможность самообслуживания, мобильные приложения и карты лояльности. Все транзакции POS должны соответствовать стандарту безопасности данных индустрии платежных карт (PCI DSS). В целях обеспечения соответствия требованиям внедряются функции составления отчетов. Качество обслуживания клиентов также зависит от производительности датчиков IoT, отслеживающих уровень в резервуарах, температуру холодильников и другие показатели. Для обеспечения соответствия требованиям и поддержания ценности бренда необходимо позаботиться о защите инфраструктуры от киберугроз. Учитывая, что розничные сети, как правило, используют логотипы крупных производителей, ценность бренда в первую очередь отражается на организациях, занимающихся добычей, переработкой и транспортировкой сырья.

Отчетность о соответствии требованиям

Энергетические компании должны соответствовать целому ряду норм и стандартов, охватывающих разные направления: от экологических требований, предъявляемых к бурению и переработке, до правил кибербезопасности. К сожалению, неинтегрированная архитектура безопасности делает процесс составления отчетов трудоемким и времязатратным. Неспособность продемонстрировать соответствие нормам может нанести ущерб репутации бренда и привести к существенным штрафам и санкциям.

Примеры использования

Ниже описаны самые распространенные примеры использования решений кибербезопасности в нефтегазовой отрасли.

Защита инфраструктуры добывающих организаций

Организации, занимающиеся производством энергии, должны обеспечивать защиту находящейся на удаленных территориях комплексной инфраструктуры, как на суше, так и на море. Эти объекты — главные цели хакеров, задачей которых является нарушение работы, экологический терроризм или даже травмы и гибель сотрудников и проживающих неподалеку граждан.

Чтобы обезопасить эти объекты, необходимо должным образом выполнить интеграцию всех компонентов безопасности, от промышленных систем управления до элементов физической безопасности, обеспечив централизованное отслеживание и управление. Инфраструктура электронных устройств и систем наблюдения небольшой буровой площадки должна быть защищена не хуже корпоративного центра обработки данных. При этом степень ее отслеживаемости должна быть одинаковой для всех сотрудников отдела безопасности.

Комплексное решение **Fortinet Security Fabric** обеспечивает интегрированную информационную и физическую безопасность для нефтегазовой отрасли. Межсетевые экраны следующего поколения (NGFW) серии **FortiGate Rugged** и беспроводные точки доступа серии**FortiAP Outdoor** обеспечивают надежную защиту и способны работать в суровых, экстремальных условиях бурения и геологоразведки на суше и на воде. Эти межсетевые экраны получают данные о промышленных системах управления (ICS) и системах SCADA из подразделения **FortiGuard Labs**. Продукты **FortiCamera** и **FortiRecorder** предназначены для защиты от физического вторжения, в то время как решения **Fortinet Secure SD-WAN** и **Fortinet SD-Branch** отвечают за безопасность сети удаленного объекта. Средства **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** и **FortiNAC**, обычно предоставляемые из корпоративной инфраструктуры главного офиса, обеспечивают безопасность этих уязвимых и удаленно расположенных объектов.

Защита инфраструктуры компаний, осуществляющих хранение и транспортировку сырья

Транспортировка нефти в промышленных масштабах расширяет поверхность физической атаки организации на сотни или тысячи километров. Трубопроводы подвержены как случайным утечкам, так и физическому саботажу, а системы диспетчерского управления и сбора данных (SCADA) и устройства IIoT, которые их отслеживают и контролируют, зачастую уязвимы[9]. Последствия успешной атаки могут быть катастрофическими, способны нанести огромный ущерб окружающей среде и привести к человеческим жертвам.

При разработке собственной электронной инфраструктуры операторам, отвечающим за хранение и транспортировку сырья, желательно использовать ссылочную архитектуру предприятия (PERA) в качестве стандарта[10]. При помощи стандарта PERA можно определить оптимальные точки расположения компонентов безопасности в архитектуре, однако он не дает ответа на вопрос о принципах разработки архитектуры кибербезопасности.

Решение **Fortinet Security Fabric** обеспечивает необходимый уровень защиты благодаря интегрированной системе информационной и физической безопасности и безопасному использованию сети. Межсетевые экраны следующего поколения (NGFW) серии **FortiGate Rugged** и беспроводные точки доступа серии **FortiAP Outdoor** обеспечивают надежную защиту на местах пролегания трубопроводов. Решения **FortiCamera** и **FortiRecorder** призваны защищать от физического вторжения, в то время как продукты **Fortinet Secure SD-WAN** и **Fortinet SD-Branch** гарантируют безопасную связь с насосными станциями и другими удаленными объектами. Широкий спектр инструментов, предоставляемых из корпоративной инфраструктуры главного офиса, обеспечивает многоуровневую защиту: к их числу относятся **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** и **FortiNAC**.

«Поскольку OT-системы часто используют устаревшие технологии, а операции безопасности часто менее проработаны, у атакующих больше шансов на успех»[11].

«Страны, располагающие определенными информационными ресурсами, нередко проводят рекогносцировочные операции против важнейших инфраструктур в целях подготовки к возможным разрушительным атакам злоумышленников»[12].

Защита инфраструктуры компаний, обеспечивающих переработку сырья

На нефтеперерабатывающих заводах из сырья производится ряд горючих материалов, что создает новые риски физического характера. Как и организации, занимающиеся добычей и транспортировкой сырья, перерабатывающие предприятия являются жертвами физических атак и кибератак. Атаки любого типа представляют значительную физическую опасность как для сотрудников, так и для граждан, не работающих на предприятии. Успешные атаки могут также повлиять на состояние национальной экономики, вызвав дефицит предложения. Угрозы могут быть как внешними, так и внутренними или исходить от третьих лиц. Несмотря на то, что некоторые внутренние атаки могут осуществляться преднамеренно, другие могут быть случайными.

Чтобы обеспечить защиту в таких нестабильных условиях, специалисты по безопасности должны иметь возможность отслеживать всю сеть с помощью одного окна и использовать инфраструктуру наблюдения. Интегрированное комплексное решение **Fortinet Security Fabric** обеспечивает информационную и физическую безопасность на объектах подобного рода. Межсетевые экраны следующего поколения (NGFW) серии **FortiGate Rugged** и беспроводные точки доступа серии **FortiAP Outdoor** обеспечивают надежную защиту в самых суровых средах. **FortiCamera** и **FortiRecorder** служат для интеграции устройств физической безопасности в систему Security Fabric. Многоуровневую защиту объекта обеспечивает широкий спектр средств, в числе которых **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** и **FortiNAC**.

Защита корпоративной инфраструктуры

Корпоративные инфраструктуры нефтегазовых компаний содержат множество важных для бизнеса данных: от геологических данных и данных разведки до финансовых данных и личной информации сотрудников и клиентов. В большинстве компаний есть удаленные сотрудники и сотрудники с разъездным характером работы, сторонние партнеры с доступом к корпоративным ресурсам и службам, расположенным в нескольких облаках. Помимо защиты этих ресурсов от внешних атак крайне важно обеспечить защиту от нарушений безопасности с лучшими побуждениями и злонамеренных инсайдеров, раскрывающих конфиденциальные данные.

Такие факторы, как разрозненность архитектуры безопасности и большое количество мобильных пользователей, снижают как безопасность, так и эффективность работы. Однако система отслеживания и управления с помощью одного окна улучшает оба этих аспекта. Комплексная интеграция инфраструктуры безопасности открывает возможности для автоматизации процессов обнаружения угроз, реагирования и отчетности, освобождая время для дорогостоящих специалистов по безопасности и позволяя им сосредоточиться на стратегически важных задачах.

Это становится возможным благодаря интегрированной архитектуре безопасности решения **Fortinet Security Fabric**. Продукты компании Fortinet обеспечивают комплексную, интегрированную и автоматизированную защиту, охватывая всю поверхность атаки — от центра обработки данных до облаков и периферии сети. Решения **динамической облачной безопасности Fortinet** объединяют общедоступные и частные облака, обеспечивая согласованное управление политиками. Решения **FortiManager**, **FortiAnalyzer** и **FortiSIEM** предоставляют возможность комплексного управления и аналитики. Решения **FortiInsight** и **FortiDeceptor** направлены на защиту от внутренних угроз. Средства **FortiWeb**,

FortiMail, **FortiClient** и **FortiEDR** включают функции защиты устройств и приложений, а также выявления и реагирования на атаки. Безопасный доступ мобильных пользователей к корпоративной сети можно обеспечить при помощи решений **FortiAuthenticator** и **FortiToken**. Межсетевые экраны **FortiGate** NGFW поддерживают сегментацию на основе намерений, что повышает защищенность удаленных пользователей за счет предоставления только авторизованного доступа к данным и системам.

Только 17 % специалистов по безопасности в нефтегазовой отрасли уверены в своей способности своевременно выявить изощренную кибератаку[13].

Защита розничных предприятий, торгующих нефтегазовой продукцией

Розничные предприятия, торгующие нефтегазовой продукцией, обычно продают и другие товары. Они сталкиваются с теми же проблемами, что и другие продавцы физических магазинов. Кроме того, в работе они используют множество IP-камер и устройств IoT, позволяющих отслеживать уровень в резервуарах и температуру холодильников. При нахождении на участке топливных баков необходимо соблюдать дополнительные требования нормативно-правового соответствия и безопасности, с которыми не сталкиваются другие розничные продавцы, а инфраструктура наружных торговых терминалов (POS) самообслуживания представляет собой еще один риск. В результате интеграция систем информационной и физической безопасности имеет решающее значение, равно как и соответствие стандартам индустрии платежных карт (PCI) и обеспечение комфортных условий для покупателей.

При таком сложном наборе потребностей бизнеса и безопасности комплексная интеграция архитектуры безопасности является особенно важным аспектом для розничных продавцов бензина. Наличие такой инфраструктуры устраняет необходимость выполнения процессов в ручном режиме и использования обходных путей, которые замедляют реагирование на угрозы и отвлекают сотрудников от их главной задачи — обслуживания клиентов.

Сетевые решения и решения в области обеспечения безопасности Fortinet помогают соединять разрозненные объекты в цепочку, обеспечивая надежную сетевую безопасность и автоматическое ведение отчетов о соответствии требованиям. Межсетевые экраны следующего поколения **FortiGate NGFW** предоставляют надежную защиту всей поверхности атак и обладают большим набором встроенных функций, для использования которых не требуется приобретать дополнительное оборудование. Решение **Fortinet Secure SD-WAN** обеспечивает безопасность сети во всех магазинах без необходимости использования дорогостоящего канала многопротокольной коммутации по меткам (MPLS). Средства **Fortinet SD-Branch**, в число которых входят **FortiAP**, **FortiSwitch** и **FortiNAC**, обеспечивают работу компонентов безопасности Fortinet в инфраструктурах всех магазинов.

Кроме того, эта инфраструктура позволяет предоставлять другим подразделениям доступ к общим службам безопасности главного офиса, включая средства управления удостоверениями и доступом **FortiAuthenticator**, продвинутой защиты конечных точек **FortiClient** и **FortiEDR**, анализа поведения пользователей и организаций **FortiInsight**, а также маскировочную технологию **FortiDeceptor**. Помимо этого, инструменты управления и аналитики **FortiManager**, **FortiAnalyzer** и **FortiSIEM** предоставляют возможность отслеживания с помощью одного окна и автоматического создания отчетов для соответствия таким стандартам, как PCI Software Security Framework (SSF)[14]. Эта инфраструктура выявляет и устраняет неизвестные угрозы при помощи интегрированных технологий искусственного интеллекта (ИИ) и машинного обучения (ML).

Конкурентные преимущества решений Fortinet

Конкурентные преимущества решений по обеспечению кибербезопасности Fortinet в нефтегазовой отрасли:

Интегрированная архитектура

Решение **Fortinet Security Fabric** предоставляет *комплексную интегрированную архитектуру кибербезопасности от одного поставщика* для ИТ- и ОТ-систем на каждом этапе производственного процесса: от защиты до обнаружения и реагирования. Такой подход обеспечивает более удобное отслеживание и управление.

Сеть, информационная и физическая безопасность

Решения компании Fortinet дают возможность объединения функций сетей, а также систем кибербезопасности и наблюдения с помощью *одного окна* независимо от местонахождения — в главном офисе, на удаленной площадке для бурения или на местной заправочной станции.

Устройства защиты повышенной прочности

Компания Fortinet предлагает широкий выбор *устройств повышенной прочности*, отвечающих всем экологическим требованиям, чтобы обеспечить защиту от кибератак на всех этапах производства и доставки.

Высокая производительность

Межсетевые экраны следующего поколения **FortiGate NGFW** способны работать в сложных удаленных средах и *обеспечивают высочайшую производительность даже при активированной проверке зашифрованного трафика на уровне защищенных сокетов (SSL) и протокола (TLS).*

Компания Fortinet признана лидером по результатам исследования Gartner Magic Quadrant, посвященного межсетевым экранам[15], и получила от NSS Labs максимальную оценку в сравнительной таблице характеристик межсетевых экранов NGFW[16].

Надежная система анализа угроз на основе искусственного интеллекта

В дополнение к выявлению ориентированных на ИТ угроз, **FortiGuard Labs** предоставляет надежную систему анализа угроз на основе искусственного интеллекта для защиты OT-систем, разработанную в результате 15-летней работы на местах. Для обнаружения угроз «нулевого дня» Fortinet в течение восьми лет с беспрецедентной точностью анализирует файлы, *используя системы искусственного интеллекта (ИИ) и машинного обучения (ML)*.

Большая партнерская сеть

Программа **интеграции решений партнеров** с системой безопасности Fortinet включает в себя *крупнейшую в отрасли сеть партнеров с определенным опытом работы с OT* и промышленными системами.

Комплексная безопасность при минимальном количестве устройств

Fortinet предоставляет широкий спектр сетевых функций и функций безопасности в одном комплексном решении, в то время как для использования аналогичных решений, предлагаемых конкурентами, часто требуются приобретать несколько устройств и, соответственно, несколько лицензий.

«Эффективная защита систем SCADA требует осведомленности о потенциальных проблемах и заблаговременного планирования. Работа над повышением эффективности системы безопасности перестала быть излишеством — теперь это настоятельная необходимость»[17].

Заключение

Нефтегазовые компании контролируют ряд инфраструктур мировой значимости. Успешные атаки могут привести к экономической дезорганизации, экологическим бедствиям и даже гибели людей. Компания Fortinet предлагает широкую линейку интегрированных и автоматизированных средств информационной и физической безопасности, внедрение которых снижает риск и способствует защите масштабных инфраструктур.

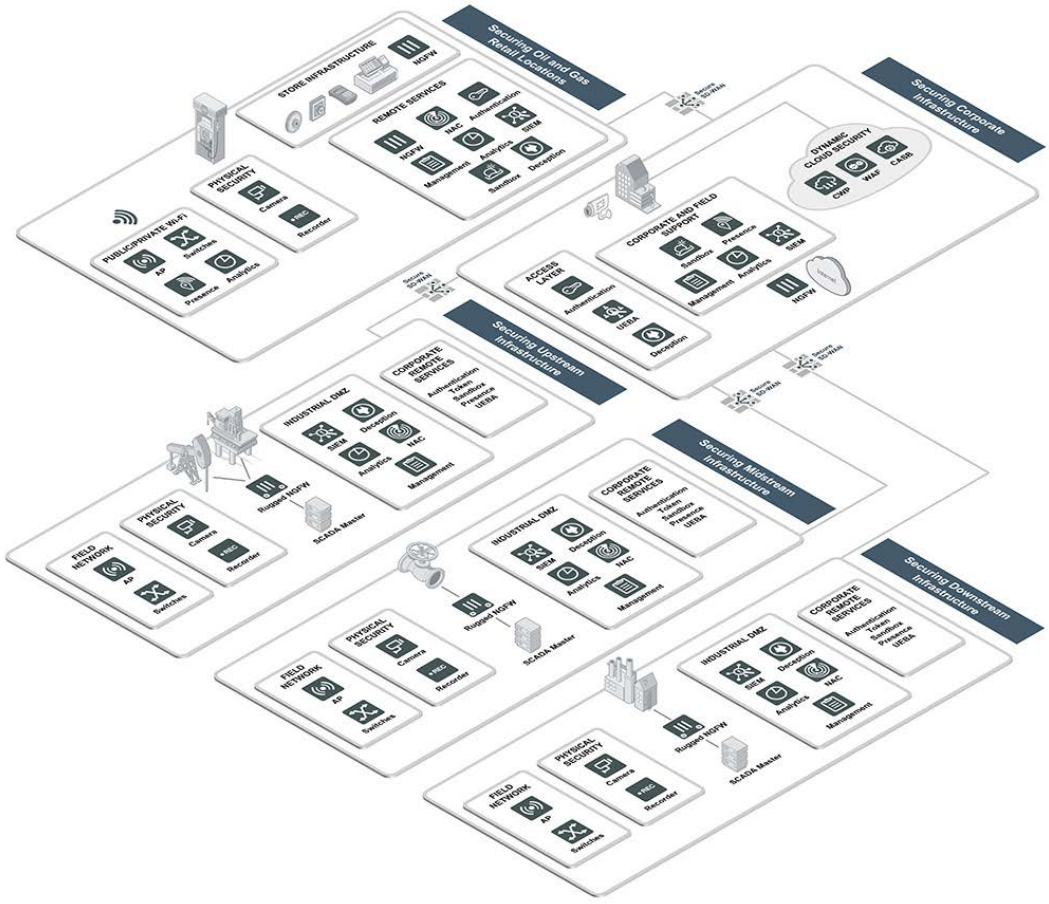

Рис. 1: решения по обеспечению кибербезопасности Fortinet в нефтегазовой отрасли охватывают все этапы производственного процесса — от разведки до розничной продажи.

[1] Джефф Уильямс (Jeff Williams) и другие, Six cybersecurity issues for oil and gas companies, EY, 12 апреля 2019 г.

[2] Independent Study Pinpoints Significant SCADA/ICS Security Risks, Fortinet, 28 июня 2019 г.

[3] Александр Горковенко (Aleksander Gorkowienko), Ensuring Oil and Gas Critical Infrastructure Security, Oil & Gas IQ, 26 июня 2019 г.

[4] Там же.

[5] Адлан Чайкин (Adlan Chaykin), New systems, new cyber threats, Petroleum Economist, 12 ноября 2019 г.

[6] Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019, (ISC)², 2019 г.

[7] Джон Мэддисон (John Maddison), The Problem with Too Many Security Options, Fortinet, 9 мая 2019 г.

[8] См. Strategies That Reduce Complexity and Simplify Security Operations, Fortinet, 3 июля 2019 г.

[9] Уильям Т. Шоу (William T. Shaw), SCADA System Vulnerabilities to Cyber Attack, Electric Energy Online, по состоянию на 21 января 2020 г.

[10] Гэри Минтчелл (Gary Mintchell), Purdue Enterprise Reference Architecture Meets IIoT, The Manufacturing Connection, 16 марта 2016 г.

[11] Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, Fortinet, 16 мая 2019 г.

[12] Адлан Чайкин (Adlan Chaykin), New systems, new cyber threats, Petroleum Economist, 12 ноября 2019 г.

[13] Джефф Уильямс (Jeff Williams) и другие, Six cybersecurity issues for oil and gas companies, EY, 12 апреля 2019 г.

[14] См. Complying with PCI SSF Without Sacrificing Customer Experience: What to Look for in a Security Solution, Fortinet, 24 августа 2019 г.

[15] Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls, Fortinet, по состоянию на 15 января 2020 г.

[16] Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests, Fortinet, январь 2019 г.

[17] Александр Горковенко (Aleksander Gorkowienko), Ensuring Oil and Gas Critical Infrastructure Security, Oil & Gas IQ, 26 июня 2019 г.

FORTINET®

www.fortinet.com/ru

28 апреля, 2020 10:07 AM

532367-0-1-RU