Войны в «песочнице»

Среди многочисленных технологий киберзащиты особое место занимают методы карантина и обмана. Их цель – заставить условный «коронавирус» проявить себя раньше времени.

Один из ключевых инструментов упреждающей защиты от кибератак – «песочницы» (sandboxes), представляющие собой выделенную среду для безопасного исполнения подозрительного кода. Такие решения предлагаются рядом производителей систем информационной безопасности, также есть программные продукты (браузеры, операционные системы) со встроенной функциональностью песочницы. В чем-то близкие решения класса Deception («обман») предназначены для того, чтобы сбить с толку атакующую сторону и заставить ее раскрыться.

«СиБ» разобрался, как работают «песочницы» и приманки и какие из них можно встретить на украинском рынке.

Анатомия «песочницы»

«Песочницы» – это инструмент упреждающей борьбы с киберугрозами. Они закрывают брешь между технологиями, пропускающими только безопасный код (белые списки, репутационный анализ) и отсеивающими опасный (черные списки, сигнатурный и эвристический анализ). Назначение «песочницы» – проанализировать сущность, о которой ничего не известно, и установить ее вредоносность не по атрибутам, а на основании реального поведения (например, операции с дисковым пространством, внешние соединения, попытки изменения конфигурации системы). Прежде чем «зловред» выйдет на просторы корпоративной сети, он отправляется в изолированную среду, где можно безопасно произвести его запуск («детонацию»), при этом все его действия записываются и анализируются. Таким манером можно выявлять целенаправленные атаки типа APT, а также атаки с использованием угроз нулевого дня.

Техническая реализация «песочницы» бывает разной. В простейшем случае она может входить в состав антивирусного продукта либо устанавливаться на рабочую станцию как отдельная программа. Запускаемое приложение имеет доступ ко всем ресурсам, которые его интересуют, однако остается невидимым за пределами «песочницы», и все созданные или измененные им данные не сохраняются. По истечении определенного времени приложение просто удаляется. Эмуляция операционной системы обеспечивает лучшую видимость действий вредоносного кода, однако так как при этом обычно воссоздается лишь часть ОС, киберпреступники могут обнаружить подделку, посылая редко используемые системные обращения, которые «песочница» не поддерживает.

Самый «продвинутый» вариант – эмуляция всего аппаратного обеспечения, включая процессор, память и порты ввода-вывода. Этот метод не привносит никаких артефактов, поэтому такую «песочницу» намного труднее обнаружить. Кроме того, «песочница» позволяет видеть на аппаратном уровне все действия, которые пытается совершать вредоносная программа, и взаимодействовать с этой программой (например, в ответ на запросы возвращать разные результаты для выяснения реакции).

Производители предлагают «песочницы» как функциональность в составе межсетевого экрана или как отдельное

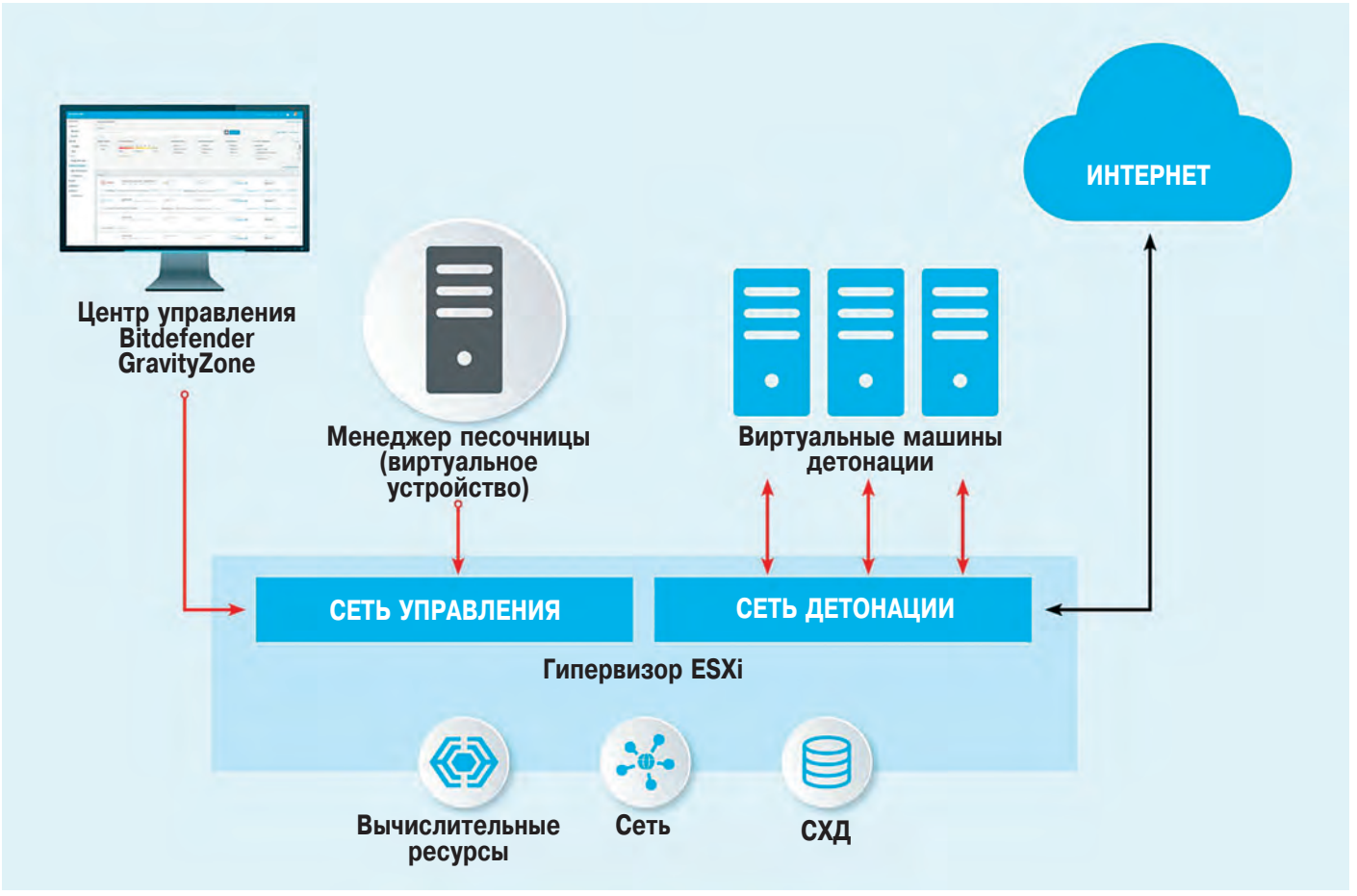

Рис. 1. «Песочница» Bitdefender GravityZone Sandbox Analyzer

решение (аппаратно-программный комплекс или виртуальное устройство). В последнее время все чаще компании используют облачный вариант «песочницы», который не только обладает всеми достоинствами облачных сервисов (низкая стоимость, масштабируемость), но и обеспечивает защиту за пределами периметра сети.

Работу песочницы можно грубо проиллюстрировать на примере решения ***Bitdefender*** GravityZone Sandbox Analyzer (**рис. 1**). Оно реализовано в форме виртуального устройства, которое работает на сервере с центральным процессором x86 и под управлением гипервизора VMware EXSi. С помощью двух сетевых карт организуются изолированные друг от друга сети: одна для управления и одна для детонации вредоносного контента, последняя также подключается к Интернету. Решение использует нейросети, машинное обучение и поведенческий анализ, а также механизм выделения подозрительных файлов, который исключает избыточное сканирование.

Мировой рынок «песочниц» уже довольно значителен и растет очень быстро. Например, по оценкам компании Maximize Market Research, в 2018 году его объем составил $1,7 млрд и к 2025-му достигнет $41,2 млрд при среднегодовом росте 52,61%. Markets&Markets дает такие цифры: $2,9 млрд в 2017 году, $9,4 млрд к 2022-му при среднем росте 26,5%. Это сопоставимо с рынком межсетевых экранов NGFW, который в том же 2017 году оценивался на уровне $2,4 млрд.

Обмануть «песочницу»

Впрочем, сами по себе «песочницы» стопроцентной гарантии безопасности не дают. Казалось бы, как победить защиту, которая вообще не выпускает ни один код в свободное плаванье, пока он не докажет свою безвредность? Однако способы обхода «песочниц» существуют достаточно давно, и здесь идет та же война снаряда и брони, что и на других фронтах кибервойны. Стратегии обхода можно разделить на две большие группы: использование слабых мест автоматической защиты для ее обмана и попытки обнаружения «песочницы».

Для первой цели чаще всего используется метод отложенного исполнения. Простейший случай – «логическая бомба», когда «детонация» кода напрямую привязана к заданной дате и времени. Но чаще «зловред» задерживает исполнение на определенный период (5–15 минут). Это может достигаться путем бессмысленных вычислений либо просто с помощью системной функции Sleep() с указанием времени задержки в качестве аргумента. «Песочницы» давно научились обнаруживать эту попытку обхода и реагируют на нее разными способами (например, подстановкой нужного аргумента, заменой функции задержки чем-то другим или просто за счет пропуска «сна» и возвращения к исполнению кода). Со своей стороны, злоумышленники придумывают способы «обхода анти-обхода», которые обнаруживают факт ускоренного исполнения или используют второй программный слой (встроенный ассемблерный

код, который создает собственную задержку); защитники борются с этим, выявляя дополнительные программы и запросы, реагируя на них и т.д.

Кроме волокиты, злоумышленники могут применять другие средства, предназначенные для того, чтобы сбить «песочницу» с толку: например, использовать файлы малоизвестных форматов или текстовые документы большого размера, которые она не может обработать. Технология под названием Fast Flux (что вообще-то означает «поток быстрых частиц») предполагает быструю смену IP-адресов и DNS-имен для обхода «черных списков». Некоторые бот-сети используют шифрование, которое «песочница» не в состоянии прочесть.

Попытки обнаружения «песочницы», в свою очередь, основываются на оценке двух факторов: окружения и пользовательской активности. Первая стратегия отталкивается от того факта, что искусственная среда, как правило, несколько отличается от реальной. Например, как уже упоминалось, для этого используются системные запросы, которые «песочница» не поддерживает. Также «зловред» может искать признаки наличия на компьютере виртуальных машин.

Нередко проверка осуществляется на аппаратном уровне (размер оперативной памяти, тип и доступная емкость жесткого диска, количество ядер процессора). Поскольку «песочницы» рассчитаны на обработку нескольких образцов кода параллельно, на каждый процесс выделяется минимальное количество ресурсов, тем самым виртуальное пространство сильно отличается от реальной машины. Обнаружив эти различия, программа может с высокой достоверностью установить, что находится в искусственной среде, после чего она либо прекратит работу, либо остановит ту часть, которая является вредоносной.

Например, по данным ***McAfee***, оценивать физическую память любят программы-вымогатели и криптомайнеры, а один «зловред» даже замерял температуру центрального процессора. Современные «песочницы» пытаются скрывать свою настоящую конфигурацию. В свою очередь, злоумышленники ищут обходные способы «прощупывания» инфраструктуры.

Альтернативно «зловред» ждет срабатывания определенного триггера, характерного только для реальной пользовательской среды (перезагрузка компьютера, взаимодействие с клавиатурой или мышью и т.д.). Большинство «песочниц» имеют механизмы имитации пользовательского поведения (перемещение курсора, открытие окон, нажатие клавиш), однако реалистичная имитация – дело нелегкое. Например, программа может дожидаться, чтобы: а) пользователь произвел какое-нибудь действие; б) следующее действие произошло меньше чем через заданный промежуток времени; б) это повторилось определенное число раз. Другие «трояны», наоборот, проверяют, чтобы операции с мышью не происходили подозрительно часто. Компания ***Lastline*** еще несколько лет назад писала о «зловреде», который использовал уже упоминавшуюся функцию «сна» не для задержки, а для отслеживания движений мыши в течение заданного периода. Если «песочница» наивно пыталась ускорить «сон» путем подстановки аргумента времени, программа не фиксировала никаких событий и таким образом обнаруживала, что ее запустили в безопасной среде.

Еще один популярный триггер – скроллинг текста. Известен случай, когда «зловред» запускался после перемотки на вторую страницу RTF-документа; при имитации скроллинга в «песочнице» текст никогда не загружался в активное окно, и потому вирус оставался незамеченным.

Для противодействия техникам обхода эксперты предлагают меры общего характера: динамическое изменение настроек времени для обмана того вредоносного ПО, которое пытается «пересидеть» карантин; проведение статического анализа в дополнение к динамическому (то есть не только проверка ПО в действии, но и исследование самого кода); поведенческий анализ для выявления методов обхода. Можно использовать группу «песочниц» для исследования в несколько итераций, а анализ с помощью машинного обучения позволяет превентивно выявлять методы обхода.

В «железе» и в облаке

Из сказанного следует, что при оценке «песочницы» важна не только производительность, но и умение обнаруживать попытки злоумышленников избежать поимки. На этом качестве делают упор сами производители. Вот несколько примеров того, что собой представляют такие «песочницы».

«Песочница» ***Check Point*** носит название SandBlast Zero-Day Protection. Технология Threat Emulation, которая в ней используется, обеспечивает мониторинг на уровне инструкций центрального процессора, отлавливая попытки обойти защиту операционной системы. По заявлению производителя, это позволяет остановить атаку еще до использования техники обхода обнаружения. Дальнейшее расследование (проверка файлов и URL-ссылок) проводится на уровне операционной системы, для чего используются несколько версий Microsoft Windows. Средства анализа включают, в том числе, поведенческие алгоритмы на основе машинного обучения. Работает «песочница» и с шифрованным трафиком, извлекая файлы из SSL– и TSL-туннелей. После анализа каждого файла генерируется отчет, а данные о новых угрозах отправляются в облачную базу Check Point ThreatCloud, где они доступны для других устройств защиты.

ThreatExtraction — еще одна используемая технология, дает возможность предоставить пользователям безопасную версию потенциально вредоносного контента, вырезая активные элементы и встроенные объекты, тогда как доступ к оригинальному документу блокируется на время анализа.

«Песочницы» Check Point доступны в аппаратном исполнении (4 модели производительностью от 450 до 5000 уникальных файлов в час), как функциональность в составе шлюзов защиты от угроз (Next Generation Threat Prevention) или через облачный сервис SandBlast Cloud. Для пользовательских устройств есть браузерное расширение, агент SandBlast Agent и мобильное приложение.

У ***Fortinet*** семейство «песочниц» FortiGate включает четыре модели производительностью от 600 до 5600 файлов в час (**рис. 2**). Они могут работать самостоятельно, принимая файлы с почтовых серверов, портов коммутаторов или напрямую от аналитиков, также возможна интеграция с другими решениями Fortinet (межсетевые экраны, системы защиты почты, веб-приложений и т. д.) и с продуктами других компаний. Несколько устройств FortiSandbox, установленные на разных локациях компании, могут обмениваться информацией в реальном времени. Кроме физических устройств, есть варианты развертывания на виртуальных машинах, в публичном облаке (AWS, Microsoft Azure) или пользования по модели SaaS.

Рис. 2. Пример аппаратной реализации «песочницы»: FortiSandbox FSA-3000E

В решениях используется двухэтапная оценка алгоритмами искусственного интеллекта. Первый ИИ исследует подозрительные файлы с помощью статического анализа, на втором этапе жизненный цикл атаки прослеживается в изолированной среде с помощью поведенческого анализа, причем ИИ обучается новым приемам злоумышленников и соответственно корректирует индикаторы поведения. «Песочница» передает данные о выявленных угрозах в международную базу знаний Mitre ATT&CK, также есть возможность записать видео всех действий вредоносного ПО или взаимодействия с ним в ручном режиме.

Palo Alto Networks предлагает несколько моделей использования своих «песочниц» WildFire. Во-первых, они доступны в виде облачного сервиса (есть глобальный центр США и региональные в Нидерландах, Японии и Сингапуре). Все облака обмениваются друг с другом сигнатурами выявленного вредоносного ПО. Возможно развертывание «песочницы» на территории заказчика в виде «частного облака», для чего используется аппаратное решение WF-500. Каждое устройство способно обрабатывать до 7 тыс. файлов в день, а кластер размером до 20 «песочниц» – свыше 120 тыс. файлов. Аппаратная «песочница» может обрабатывать все файлы локально либо передавать их в облако для параллельной проверки, сигнатуры затем рассылаются на все шлюзы Palo Alto с лицензиями Threat Prevention и WildFire. Как вариант, можно настроить WF-500 таким образом, чтобы «песочница» отдавала в облако WildFire не сами файлы, а только готовые сигнатуры. Возможна и гибридная схема, когда особо конфиденциальные материалы не покидают территорию компании, а остальные направляются в облако на анализ.

WildFire использует четыре подхода для проверки вредоносного кода: динамический анализ в виртуальной среде, статический анализ, исследование с помощью алгоритмов машинного обучения, что в дальнейшем позволяет распознавать новый вредоносный код, и анализ «на голом железе» («детонация» кода происходит на реальном аппаратном обеспечении, так что методы обхода виртуальных машин, которые в ходу у злоумышленников, становятся бесполезными). Кроме того, WildFire использует гипервизор собственной разработки, который, по утверждению производителя, устойчив к технологиям обхода виртуальных машин. «Песочница» отслеживает такие «продвинутые» методы, как детектирование отладчика и VM, вставка кода в доверенные процессы, отключение средств защиты на компьютере. Palo Alto предлагает использовать «песочницу» в сочетании с сервисом контекстуального анализа угроз AutoFocus, который обеспечивает корреляцию выявленных индикаторов компрометации с данными, полученными командой аналитиков производителя.

Решение ***McAfee*** Advanced Threat Defense совмещает несколько подходов защиты: сигнатурная и репутационная проверки, динамический анализ в «песочнице», глубокий статический анализ кода с целью выявления его фактических намерений и способов уклонения и в завершение – проверка на наличие вредоносных признаков с помощью средств машинного обучения. Отправка образца одновременно в несколько виртуальных сред повышает скорость проведения расследования, поскольку позволяет определить, какие условия необходимы для исполнения кода в анализируемом файле.

Threat Defense интегрируется с другими системами защиты, которые могут принимать решения сразу, как только файл классифицируется как вредоносный. Через программный соединительный модуль Advanced Threat Defense Email Connector решение получает от почтового шлюза подлежащие анализу вложения из сообщений электронной почты. Обмен через локальную базу данных об угрозах Threat Intelligence Exchange дает возможность другим решениям сразу принимать меры на основе полученного заключения: например, конечные точки могут заблокировать установку вредоносных программ. А выявленные признаки взлома позволяют искать артефакты атак в сохраненных данных за период до шести месяцев и обнаруживать системы, которые обменивались данными с источниками вредоносного ПО.

Обман во благо

Однако «песочницы», как и другие средства защиты, имеют одну цель: не пустить врага внутрь. Что делать, если вредоносный код уже проник в сеть и распространяется по ИТ-инфраструктуре компании? Можно попытаться поймать его на горячем, и для этого, среди прочего, используются технологии обмана (Deception). По принципу действия они сходны с «песочницами» в том смысле, что вынуждают злоумышленников проявить себя в контролируемой среде. Однако происходит это не в изолированном виртуальном пространстве, а на приманках, расставляемых в стратегических местах и неотличимых от настоящих ресурсов компании. Помимо того, что атака вязнет в ложных целях, этот подход дает еще одно преимущество: любое взаимодействие с ловушкой является реальной атакой и позволяет с высокой достоверностью засечь злоумышленника, избежав ложных срабатываний. После того, как «зловред» обнаружен, можно наблюдать за его последующим поведением в ловушке или отправить для дальнейшего анализа, например, в ту же «песочницу».

Ловушки и приманки восходят корнями к технологии Honeypot («горшок меда»), которые использовались в начале нулевых. В простейшем сценарии задачей этих артефактов является всего лишь оповещение об атаке, и им не нужно обладать высокой достоверностью. Более сложные системы умеют качественно имитировать настоящие серверы, базы данных, пользовательские устройства и вообще все, что вирус может встретить в сети компании. Эти артефакты могут обеспечивать более сложные реакции на действия атакующих, а низкий уровень ложных срабатываний позволяет автоматизировать реагирование. Еще более радикальный сценарий предусматривает генерацию «хлебных крошек» – особо привлекательных и слабо защищенных целей, которые атакующая сторона не сможет проигнорировать, тем самым уже обороняющиеся пытаются диктовать, где произойдет атака.

По мнению Gartner, технологии обмана изменят парадигму киберзащиты: поиск атак становится проблемой не «больших данных», как в решениях типа SIEM и UEBA, а «правильных данных». Кроме того, если сейчас обороняющаяся сторона должна отражать 100% атак, а нападающей достаточно одного попадания, при новом подходе уже атакующие должны всегда выбирать правильные цели, иначе они будут разоблачены, тогда как защите достаточно одного срабатывания ловушки. Gartner также полагает, что к 2022 году 25% всех решений для поиска угроз будут включать функции обмана.

Решения класса Deception предлагает тоже целый ряд компаний. Одна из них – ***TrapX Security*** со своей платформой DeceptionGrid. Платформа использует простые приманки (Deception Tokens), представляющие собой имитацию рабочих станций с измененной конфигурацией. Если атакующая сторона пытается проникнуть вглубь сети, для противодействия используются ловушки средней сложности, которые имитируют различные устройства (серверы, рабочие станции, банкоматы, POS-терминалы, камеры видеонаблюдения и т.д.). Эти артефакты позволяют определить место и тип атаки, а затем вручную или автоматически изолировать атакующее устройство. После блокирования кибератаки ловушка меняет свой тип и расположение. Еще более сложные алгоритмы имитируют операционную систему (FullOS), также есть возможность

Рис. 3. Принцип работы решения Attivo ADSecure

клонирования реальных серверов. FullOS-ловушки реагируют на действия злоумышленников и записывают их для дальнейшего расследования.

Платформа ThreatDefend компании ***Attivo Networks*** включает несколько модулей. Из них ключевым является BOTsink – сетевая защита с помощью ловушек. BOTsink создает достоверные артефакты, имитирующие серверы на Windows и Linux, рабочие станции, специализированные устройства наподобие IoT и POS-терминалов, а также приложения, базы данных и документы. Аппаратно BOTsink реализован в виде устройства объемом 1RU.

Отдельный модуль ADSecure защищает службу каталогов Windows Active Directory, подменяя результаты запросов. Кстати, этот пример вообще наглядно демонстрирует действие технологии Deception (**рис. 3**). Решение ThreatStrike – это безагентная технология защиты рабочих станций, которая использует приманки (поддельные учетные записи, файлообменники и приложения) для перенаправления атакующих в ловушки. Другие важные компоненты платформы – ThreatPath (визуализация возможных путей продвижения злоумышленника), ThreatOps (автоматизация реакции на инциденты), ThreatDirect (защита облаков и удаленных офисов).

Платформа обмана ***Illusive Networks*** также включает несколько модулей. Attack Detection System размещает на конечных станциях легковесные артефакты, имитирующие реальные данные, учетные записи и соединения, при этом генерация ловушек происходит автоматически на основе реальных данных компании. Attack Surface Manager непрерывно отслеживает пути, которыми могут воспользоваться атакующие после проникновения в сеть, и может автоматически устранять нарушения. Attack Intelligence System обеспечивает сбор данных для расследования инцидентов. Похожие разработки есть и у других компаний – например, ***Fidelis Security***, ***Smokescreen*** и т.п.

Конечно, как и любая технология, Deception имеет свои слабые места. Чем больше артефактов, тем дороже будет стоить защита, но неприкрытые ресурсы будут являть собой «слепые пятна». Примитивные ловушки могут отпугнуть обычных хакеров, но преступники, стоящие за целенаправленными атаками, будут предупреждены. Как и везде, остается опасность со стороны инсайдеров. Тем не менее, пишет Gartner, для предприятий СМБ средства обмана представляют собой такое простое и элегантное решение, что даже с трудом верится.

Однако никакая, даже самая инновационная и «продвинутая» технология, сама по себе не может быть панацеей. Лучше всего иметь комплексную защиту, объединяющую различные подходы: фильтрацию, карантин, обман, сигнатурный и поведенческий анализ, машинное обучение.

Василий ТКАЧЕНКО, **СиБ**

СИСТЕМЫ БЕЗОПАСНОСТИ

В Киеве представлены новые решения Palo Alto Networks

Компания Palo Alto Networks совместно с группой «БАКОТЕК» 4 марта провела в Киеве конференцию A More Secure Everywhere, посвященную упрощению и повышению уровня ИТ-безопасности на пути к цифровой трансформации бизнеса. В ходе мероприятия специалисты обеих организаций, а также компаний-партнеров рассказали о развитии продуктов Palo Alto и опыте их использования.

В рамках новой стратегии Palo Alto разделила свои продукты на три категории. Межсетевые экраны следующего поколения (NGFW) теперь известны под брендом Strata. Как и раньше, архитектура этих устройств построена по принципу Single Pass (параллельная проверка разными методами) и разделения плоскостей управления и обработки. В новой версии операционной системы Pan-OS 9.X появился ряд дополнительных функций — в частности, интегрированная защита DNS, которая борется с атаками типа DGA (алгоритмы генерации доменов) и DNS-туннелирования, используя машинное обучение и данные из множества источников. Механизм URL-фильтрации присваивает каждой ссылке репутационную категорию, а внутренняя логика проверяет сайт на принадлежность к фишингу. Инструмент Policy Optimizer позволяет настраивать политику использования приложений. A Secure SD-WAN проверяет характеристики каналов доступа, распределяет приложения по этим каналам в зависимости от критичности и обеспечивает динамическое переключение между провайдерами.

Пакет решений для защиты облаков получил название Prisma. Он включает в себя решение Prisma Access для защиты доступа удаленных и мобильных сотрудников, филиалов, Prisma SaaS (контроль использования общедоступных облачных приложений) и Prisma Cloud (сюда вошли разработки приобретенных Palo Alto компаний RedLock и Twistlock, обеспечивающие защиту инфраструктуры в облаке).

Наконец, бренд Cortex объединяет решения для управления кибербезопасностью, включающие платформу, которую производитель позиционирует как XDR — «расширенную систему обнаружения и устранения угроз». Cortex XDR собирает данные не только с рабочих станций, но также из сети, облаков и сторонних организаций. Кроме защиты конечных точек, решение обеспечивает анализ сетевого трафика и действий пользователей, предотвращение атак и расследование инцидентов. Во второй версии продукта добавлена возможность получения данных от межсетевых экранов других производителей, улучшена защита конечных точек (в частности, появилась функция управления USB-устройствами), а также включена новая система анализа вредоносного ПО на основе машинного обучения.

Второе решение для SOC, под названием Cortex XSOAR, призвано разгрузить сотрудников от однотипной ручной работы. Решение обеспечивает взаимодействие со всеми системами безопасности из одной точки, автоматическое выполнение сценариев и реагирование на инциденты. Буква «X» в названии означает, что в дополнение к функциям SOAR решение содержит платформу управления каналами данных об аналитике угроз (Threat Intelligence).