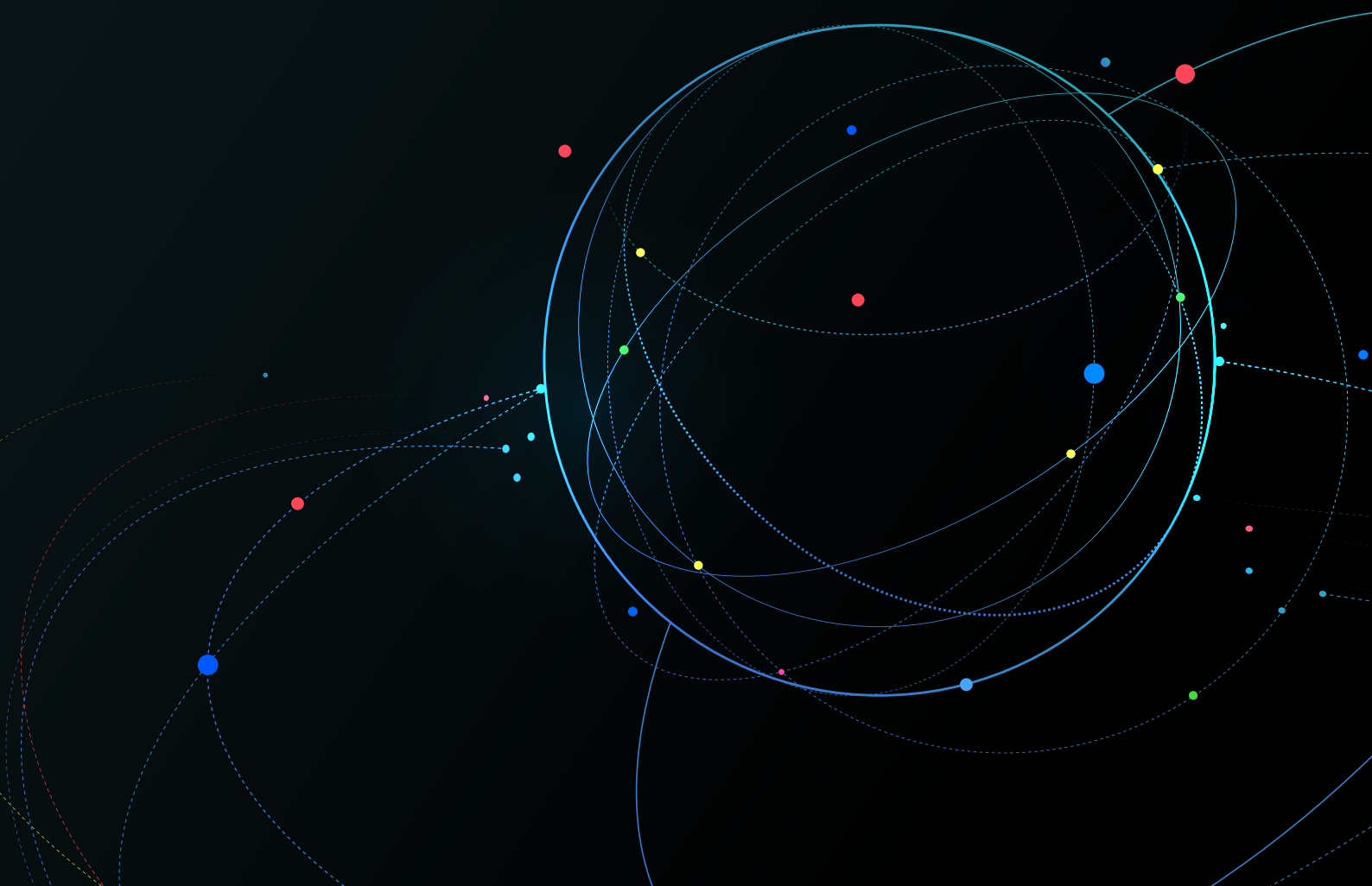
Информзащита
Системный интегратор

Зарубежные тренды ИБ

ноябрь –декабрь 2023г
итоги 2023г



Резюме

2023 год был годом прорыва для ИИ в сфере кибербезопасности.

Практически каждый поставщик средств безопасности в течение года рекламировал новые продукты и возможности, использующие GenAI. В их число вошли некоторые крупнейшие компании в области кибербезопасности, такие как Microsoft, CrowdStrike и SentinelOne, которые указали на потенциал GenAI, который поможет командам безопасности работать более продуктивно и быстро реагировать на угрозы. Однако не только GenAI сыграл роль в создании основных новых инструментов кибербезопасности, выпущенных в 2023 году. Многие ведущие поставщики объявили в 2023 году о заметных обновлениях продуктов, которые больше связаны с «традиционным» ИИ и **машинным обучением**, чем с GenAI. Например, Palo Alto Networks с популярным решением XSIAM. Что касается тематики, многие из ключевых инструментов кибербезопасности, запущенных в 2023 году, включали в себя **продукты классов SIEM и XDR** от таких поставщиков, как Cisco, Palo Alto Networks и Sophos.

10 самых популярных инструментов и продуктов кибербезопасности 2023 года:

Cisco XDR

Cisco запустила новую платформу расширенного обнаружения и реагирования (XDR), которая была создана «с нуля». Платформа Cisco XDR объединяет обнаружение и реагирование сети (NDR) и обнаружение и реагирование конечных точек (EDR). Cisco XDR представляет собой важный шаг на пути Cisco к реализации своего видения Security Cloud по предоставлению комплексной унифицированной платформы ИБ. Запланированное приобретение Cisco Splunk за 28 миллиардов долларов обеспечит огромный приток данных на платформу Cisco XDR и использование возможностей искусственного интеллекта.

Securonix Unified Defense SIEM

Securonix представила новую платформу SIEM, которая работает с потоками данных из озера данных Snowflake. Платформа может использовать «горячие» данные с возможностью поиска за 365 дней из Snowflake Data Cloud. Это обеспечивает улучшенную видимость потенциальных угроз, а также предлагает одноуровневую модель хранения, которая может поддерживать крупномасштабный поиск, устраняя при этом многие проблемы управления данными, связанные со стандартной моделью многоуровневого хранения.

Zscaler Risk360

Zscaler представила Risk360, инструмент для количественной оценки и визуализации рисков, призванный помочь организациям принимать более эффективные и быстрые решения по снижению рисков безопасности.

SentinelOne Purple AI

Изначально технология GenAI Purple AI предназначена для поиска угроз. Purple AI предлагает аналитикам возможность использовать естественный язык для запросов. Далее функции Purple AI расширились в части рекомендаций аналитикам по запросам и действиям для решения проблем, а также формирования сценариев для автоматизации реагирования. Технология GenAI, лежащая в основе Purple AI, не только выступает в качестве автономного инструмента, но и интегрирована в последнюю версию платформы Singularity от SentinelOne, получившую название Unity.

CrowdStrike Charlotte AI

Инструмент для аналитиков SOC. По заявлениям топ-менеджмента, Charlotte может превратить аналитика 1-й линии в аналитика 3-й линии. Последняя версия платформы безопасности Falcon от CrowdStrike, получившая название Raptor, также использует возможности Charlotte GenAI. В Raptor добавлен Charlotte AI Investigator, который может сопоставлять контекст инцидентов безопасности и предоставлять сводные данные об инцидентах на основе GenAI.

Palo Alto Networks XSIAM 2.0

Palo Alto Networks представила второе поколение своего предложения по обеспечению безопасности на основе искусственного интеллекта Cortex XSIAM с улучшениями в области пользовательского опыта и поддержкой пользовательских моделей машинного обучения (ML).

ThreatLocker Ops

ThreatLocker Ops отслеживает среду на предмет потенциальных уязвимостей или аномалий, которые могут привести к кибератаке. Он использует данные телеметрии, собранные со всех модулей ThreatLocker, для выявления индикаторов компрометации и реагирования на них. В то время как принцип нулевого доверия, используемый ThreatLocker, снижает вероятность успешной кибератаки, ThreatLocker Ops еще больше укрепляет среду, уведомляя и автоматически реагируя на идентификаторы попыток взлома в случае атаки.

Tanium Autonomous Endpoint Management

Tanium представила свою платформу автономного управления конечными точками, цель которой — вывести на новый уровень автоматизации работу как служб безопасности, так и ИТ-команд. Функция Autonomous Insights платформы использует большие языковые модели для повышения производительности, в том числе за счет определения приоритетов рисков с использованием данных о важности различных активов. Autonomous Workflows обеспечивает автоматизацию создания рабочих процессов по управлению конечными точками. Autonomous Remediation формирует автоматические ответные действия, которые не требуют вмешательства человека (хотя у клиентов есть выбор, сколько автономности предоставить системе).

Sophos XDR Updates

Sophos раскрыла набор новых возможностей обеспечения безопасности конечных точек, которые укрепят ее платформу расширенного обнаружения и реагирования (XDR), включая возможность, которую компания назвала «адаптивной активной защитой от злоумышленников». Эта функция переводит инструмент безопасности конечных точек Sophos в «режим взлома», когда выясняется, что клиент подвергается атаке. Затем инструмент может, например, запретить запуск исполняемого файла или запретить подключение к определенной конечной точке. В конечном итоге эта возможность дает возможность прервать уже существующие атаки и выиграть больше времени для реагирования. Кроме того, Sophos развернула поддержку на своей платформе XDR ключевых продуктов от 21 вендора, включая таких конкурентов, как CrowdStrike, Fortinet и Palo Alto Networks. В результате платформа Sophos XDR теперь имеет более 75 интеграций сторонних технологий. Sophos также объявила, что ее платформа XDR теперь поддерживает сетевое обнаружение и реагирование (NDR). Обновление делает NDR доступным как отдельное предложение для клиентов, тогда как ранее оно было доступно только для клиентов в рамках MDR.

Microsoft Security Copilot

Security Copilot адаптирует технологию генеративного искусственного интеллекта к кибербезопасности, объединяя GPT-4 с собственной моделью искусственного интеллекта Microsoft, ориентированной на безопасность. Кроме того, Microsoft анонсировала единую платформу операций безопасности, которая сочетает в себе Security Copilot с предложениями Sentinel и Defender XDR.

Значимые сделки по слияниям и поглощениям в области кибербезопасности в 2023 году:

Thales досрочно завершила приобретение Imperva,

это приобретение добавит в портфель Thales возможности обеспечения безопасности приложений, безопасности данных, а также управления идентификацией и доступом.

Palo Alto Networks приобретает:

- израильский стартап Talon Cyber Security,
  который предоставляет безопасный браузер и инструменты безопасности для управления доступом к клиентским серверам со сторонних и персональных устройств.

- Dig Security,
  поставщика услуг управления состоянием безопасности данных (DPSM)

Proofpoint завершила приобретение Tessian,

компании, специализирующейся на безопасности облачной электронной почты.

WatchGuard Technologies приобрела компанию CyGlass Technology Services,

занимающуюся обнаружением и реагированием на облачные и сетевые угрозы.

Cisco покупает:

- Splunk (SIEM)
- Oort,
  разработчика технологии обнаружения и реагирования на угрозы идентификации (ITDR)
- Armorblox,
  платформу безопасности электронной почты
- Lightspin Technologies,
  предлагает комплексное управление состоянием облачной безопасности (CSPM)
- Isovalent,
  специализируется на разработке сетевых решений open source для обеспечения безопасности, в том числе в облачных средах.

Check Point купила компанию Perimeter 81,

которая разрабатывает сетевые решения для кибербезопасности для гибридных сотрудников на своей облачной платформе (SSE)

IBM приобрела Polar Security,

поставщика услуг управления состоянием безопасности данных (DPSM)

Hewlett Packard Enterprise (HPE) купила поставщика услуг облачной безопасности Axis Security,

чтобы предоставить унифицированное предложение услуг безопасного доступа (SASE)

Rubrik объявил о подписании соглашения о приобретении израильского стартапа Laminar,

предлагающую платформу управления состоянием безопасности данных (DSPM).

Tenable завершила сделку по приобретению Ermetic.

В сферу компетенции Ermetic входит управление правами на облачную инфраструктуру (CIEM).

Стартапы в ИБ

Даже несмотря на более высокий приоритет консолидации инструментов безопасности — основной темы для партнеров и клиентов в 2023 году — потребность в инновациях в ключевых сегментах кибербезопасности остается крайне востребованной. Хотя венчурное финансирование остается ограниченным в связи со сложными экономическими условиями, оно по-прежнему доступно для стартапов в области кибербезопасности, особенно для тех, чьи основатели ранее добились успеха в предыдущих компаниях.

Среди основных направлений развития стартапов в области ИБ в 2023 году —

операции по обеспечению безопасности (SecOps), безопасность данных и — особенно — безопасность цепочки поставок программного обеспечения. Безопасность цепочки поставок программного обеспечения стала главной проблемой в последние годы после атаки на SolarWinds и ее клиентов, а в этом году угроза усилилась из-за инцидентов, включая взлом цепочки поставок программного обеспечения у производителя коммуникационных приложений 3CX. Другие стартапы сосредоточены на таких областях, как предотвращение программ-вымогателей, технология безопасного веб-шлюза и аутентификация без пароля.

10 популярных стартапов в области кибербезопасности 2023 года

(основаны с 2020г, без стартапов в области обеспечения облачной безопасности, которые рассмотрены отдельно):

Chainguard

предлагает инструменты, которые призваны значительно повысить безопасность цепочки поставок программного обеспечения и программного обеспечения с открытым исходным кодом, в том числе за счет предоставления собственных защищенных образов контейнеров, которые по умолчанию помогают командам разработчиков избегать многих уязвимостей. В ноябре Chainguard объявила о раунде финансирования серии B на сумму 61 миллион долларов, возглавляемом Spark Capital, и сообщила, что ее образы контейнеров используются рядом компаний из списка Fortune 500.

Descope

предлагает инструмент, который помогает разработчикам более легко интегрировать аутентификацию без пароля в приложения, уделяя особое внимание упрощению подключения к ключам доступа от таких поставщиков, как Apple, Microsoft и Google. В феврале Descope привлекла $53 млн начального финансирования под руководством Lightspeed Venture Partners и GGV Capital.

Dope.security

предлагает новое поколение безопасных веб-шлюзов, которые призваны упростить развертывание — благодаря запатентованной архитектуре «fly-direct», которая позволяет избежать необходимости перенаправлять веб-трафик через промежуточные центры обработки данных. В марте стартап получил $16 млн в рамках финансирования серии A от GV (Google Ventures).

Endor Labs

стремится обеспечить повышенную безопасность цепочки поставок программного обеспечения с помощью платформы, ориентированной на обеспечение безопасного использования программного обеспечения с открытым исходным кодом, включая выбор зависимостей, управление и устранение проблем безопасности кода. В августе, стартап объявил о раунде финансирования серии A на сумму 70 миллионов долларов от инвесторов, включая Lightspeed Venture Partners и Dell Technologies Capital.

Gutsy

предлагает инструмент для управления безопасностью, который использует методы интеллектуального анализа процессов для автоматического анализа данных, что в конечном итоге позволяет снизить риски безопасности и улучшить аудит, а также снизить риски, связанные с ключевыми проектами, такими как миграция в облако и внедрение управляемых услуг. Стартап получил начальный раунд финансирования в размере 51 миллиона долларов, возглавляемый YL Ventures и Mayfield.

Halcyon

предлагает ряд возможностей, направленных на противодействие программам-вымогателям, включая предотвращение программ-вымогателей перед их выполнением с использованием искусственного интеллекта и машинного обучения, а также методы, позволяющие заставить атаку раскрыть себя или прервать ее. В апреле Halcyon привлек $50 млн в рамках финансирования серии A под руководством Syn Ventures.

NetRise

фокусируется на повышении прозрачности расширенного Интернета вещей (XIoT), охватывая проблемы встроенного ПО и программного обеспечения, связанные с IoT, IT, OT и другими подключенными системами. Недавние обновления включали добавление возможностей, упрощающих работу с файлами SBOM (спецификация программного обеспечения). В ноябре NetRise запустила новые возможности для повышения безопасности цепочки поставок программного обеспечения, позволяя выявлять скомпрометированные программные активы с помощью семантического поиска на основе искусственного интеллекта.

Next DLP

предлагает платформу для выявления внутренних рисков, а также обнаружения утечки данных и их потери с помощью программного агента, который оказывает минимальное влияние на производительность процессора и производительность сотрудников. В сентябре Next DLP объявила о расширении своей платформы Reveal, включив в нее инструменты генеративного искусственного интеллекта, включая Hugging Face, Bard, Claude и некоторые другие, в дополнение к ChatGPT.

Radiant Security

предлагает инструмент автоматизации SOC на базе искусственного интеллекта, направленный на повышение производительности и обнаружение угроз, в том числе за счет динамического анализа всех предупреждений безопасности, а также расследования и анализа первопричин инцидентов. Стартап объявил о привлечении $15 млн в раунде серии A под руководством Next47 в ноябре.

Torq

предлагает метод автоматизации операций безопасности без кода, а недавние обновления включают запуск инструмента на базе GenAI, который предназначен для автономной обработки подавляющего большинства Tier-1 тикетов.

Облачная безопасность

Для зарубежных ИТ-специалистов и специалистов по безопасности обеспечение надежной защиты использования в их организациях общедоступных облачных сред, таких как Amazon Web Services, Microsoft Azure и Google Cloud, остается главным приоритетом и одной из самых серьезных проблем. То же самое касается защиты использования облачных приложений: многие компании становятся все более зависимыми от приложений SaaS, таких как Salesforce, Microsoft 365 и Workday. Многочисленные стартапы в области облачной безопасности пытаются удовлетворить растущий спрос. Основные направления деятельности стартапов в сфере облачной безопасности в 2023 году включают предложение новых способов защиты личных данных и данных в облачных средах, а также улучшенные методы защиты использования SaaS-приложений на рабочем месте.

10 самых популярных стартапов в области облачной безопасности 2023 года

(основаны с 2020г.; без учета стартапов, которые уже достигли значительных масштабов, таких как Wiz, Orca Security):

Augmentt

предлагает мультитенантную платформу безопасности, позволяющую MSP защищать использование приложений Microsoft SaaS своими клиентами. По словам компании, платформа Augmentt призвана обеспечить улучшенную видимость облачных приложений Microsoft, а также упростить аудит сред и улучшить обнаружение угроз.

Cado Security

предлагает то, что она называет первой платформой для криминалистики и реагирования на инциденты в облаке. По словам стартапа, платформа цифровой криминалистики является облачной, что делает ее уникальной для облачных сред и ориентирована на автоматизацию расследования и реагирования.

DoControl

предлагает безагентную платформу для обеспечения безопасности SaaS, обеспечивающую защиту приложений и данных SaaS. В ноябре DoControl представила новую интеграцию, направленную на улучшение защиты данных в Microsoft 365. Интеграция обеспечивает более быструю адаптацию, повышенную целостность данных и поддержку облачной защиты от потери данных (DLP) для Microsoft Teams.

Dazz

предлагает платформу облачной безопасности, ориентированную на улучшенную приоритизацию и устранение уязвимостей в облаке, которая контрастирует с инструментами, которые в основном предназначены для генерации оповещений. Платформа Dazz служит централизованным местом для устранения проблем на облачных платформах, в инфраструктуре, приложениях и коде. В ноябре Dazz представила свою новую унифицированную платформу исправлений, которая объединяет данные из многочисленных инструментов обнаружения, сопоставляет связанные проблемы и отслеживает проблемы до их источников, что в конечном итоге предоставляет «контекстный план исправления для заметного снижения риска».

Gomboc

предлагает то, что он называет «самовосстанавливающейся облачной безопасностью», с возможностью непрерывного развертывания исправлений безопасности для облачной инфраструктуры, которые могут быть одобрены командами DevOps посредством запроса на включение. Неправильные настройки облака являются ключевой причиной нарушений, которые приводят к потере данных на предприятии, особенно с учетом продолжающегося перехода к облачным и мультиоблачным средам. Но исследование и мониторинг всех возможных конечных точек и соединений с облачными сервисами — слишком большая работа, чтобы люди могли справиться с ней в одиночку. Gomboc.ai стремится решить эту проблему с помощью детерминированного искусственного интеллекта. Генеративный ИИ, включающий такие известные модели, как ChatGPT от OpenAI и Bard от Google, анализирует большие коллекции данных, чтобы изучить структуры достаточно хорошо, чтобы собрать из них правдоподобный новый контент, то есть генерировать выходные данные. Детерминированный ИИ, с другой стороны, определяет характеристики данных так, чтобы конкретная проблема имела одно конкретное, правильное решение, которое не меняется, то есть значения данных определяют выходные данные.

Grip Security

предлагает платформу для снижения рисков безопасности личных данных, связанных с использованием SaaS, посредством возможностей обнаружения, определения приоритетов и координации исправлений.

Island

предлагает веб-браузер на базе Chromium, предназначенный для обеспечения безопасного использования приложений SaaS предприятиями. По словам компании, браузер Island призван обеспечить гораздо более высокий уровень видимости и контроля над использованием данных внутри SaaS-приложений.

Legit Security

предлагает платформу управления состоянием безопасности приложений, целью которой является обеспечение улучшенной прозрачности и безопасности на протяжении всего процесса разработки программного обеспечения. По словам компании, платформа стартапа «код в облако» предлагает «унифицированную» плоскость управления безопасностью приложений, а также возможности автоматического обнаружения и анализа в жизненном цикле разработки программного обеспечения.

Sentra

предлагает платформу управления состоянием безопасности данных, целью которой является улучшение видимости конфиденциальных облачных данных, а также более высокая автоматизация оценки рисков и анализа доступа, связанного с данными.

Veza

предлагает инструмент, призванный помочь организациям улучшить свою безопасность в отношении разрешений и привилегий доступа, уделяя особое внимание обеспечению визуального представления для более легкого обнаружения аномальных и рискованных разрешений. Инструмент также позволяет отслеживать активность разрешений, автоматизировать проверку доступа и устранять нарушения привилегий.

Использование ИИ преступниками

Sophos опубликовала два отчета об использовании ИИ в киберпреступности.

Первый отчет — *“The Dark Side of AI: Large-Scale Scam Campaigns Made Possible by Generative AI”* — демонстрирует, как в будущем мошенники смогут использовать такие технологии, как ChatGPT, для проведения крупномасштабного мошенничества с минимальными техническими навыками. Однако второй отчет, озаглавленный *"Cybercriminals can’t agree on GPTs"*, показал, что, несмотря на серьезную озабоченность многих экспертов по информационной безопасности и правоохранительных органов различных стран по поводу использования киберпреступниками генеративного ИИ, многие опытные хакеры скептически относятся к современным чат-ботам и нейросетям. Злоумышленники убеждены, что добиться значимых результатов с помощью ИИ-инструментов сейчас крайне сложно.

Безопасность облачных сред

Слияния и поглощения

Компания Wiz, занимающаяся облачной безопасностью, приобрела Raftt, облачную платформу для разработчиков. Это приобретение, первое для израильской компании Wiz, расширит ее возможности разработки безопасных облаков.

Cisco в декабре объявила, что планирует купить Isovalent, чтобы упростить решение сложных облачных проблем безопасности и сетей, а также укрепить платформу Cisco Security Cloud. Isovalent является участником проекта eBPF (extended Berkeley Packet Filter), нацеленного на использование возможностей ядра Linux для мониторинга активности, обнаружения проблем с производительностью и выявления рисков безопасности различных рабочих нагрузок. Кроме того, Isovalent принимает участие в двух других проектах open source: Cilium и Tetragon. Первый помогает управлять потоками сетевого трафика между контейнерами, а второй дополняет Cilium, предоставляя дополнительные возможности кибербезопасности. Isovalent недавно представил решение Cilium Mesh, которое позволяет подключать кластеры Kubernetes к существующей инфраструктуре в гибридных облаках.

В январе компания SonicWall заявила, что приобрела Banyan Security, поставщика периферийных услуг безопасности (SSE). Сделка принесет в портфель SonicWall технологию ZTNA (доступ к сети с нулевым доверием), что в конечном итоге поможет компании расширить свое предложение в SASE. Это второе приобретение SonicWall за два месяца после заключенной в середине ноября сделки по приобретению Solutions Granted, MSP, который призван улучшить позиции SonicWall на рынке управляемого обнаружения и реагирования (MDR).

SentinelOne планирует приобрести компанию PingSafe, специализирующуюся на защите приложений, чтобы стать лидером рынка облачной безопасности. CNAPP от PingSafe будет интегрирован в платформу Singularity от SentinelOne, чтобы создать единую платформу безопасности с расширенными операциями безопасности на базе искусственного интеллекта для защиты предприятий на конечных точках, учетных записях и в облаках. CNAPP от PingSafe обеспечивает мониторинг мультиоблачных рабочих нагрузок в режиме реального времени, простую настройку, а также низкий уровень ложных срабатываний.

Безопасность приложений

Слияния и поглощения

Оборонная и аэрокосмическая компания Thales объявила в декабре, что завершила сделку по приобретению Imperva. Это приобретение выводит Thales в ряды крупнейших мировых поставщиков систем безопасности, а в 2024 году ожидается выручка от кибербезопасности в размере 2,6 млрд.долл. Imperva - давний игрок в таких категориях безопасности приложений, как межсетевой экран веб-приложений и защита от DDoS. В последние годы вендор вышел в новые сегменты рынка, такие как безопасность API, а также уделяет все больше внимания другим смежным категориям, таким как безопасность данных. Thales сообщила, что ее портфель кибербезопасности теперь сосредоточен на безопасности приложений, безопасности данных, а также управлении идентификацией и доступом.

Услуги информационной безопасности

Слияния и поглощения

Компания SentinelOne приобрела консалтинговую фирму Krebs Stamos Group (KSG) для запуска PinnacleOne, группы стратегического анализа рисков и консультирования, которую возглавят бывший директор CISA Кристофер Кребс и бывший директор по информационной безопасности Facebook Алекс Стамос.

SonicWall приобрела ведущего поставщика услуг управляемой безопасности Solutions Granted, чтобы расширить свой портфель управляемых обнаружений и реагирования (MDR) и бизнес по управляемым услугам, ориентированный на МСП.

Безопасность и конфиденциальность данных

Слияния и поглощения

Proofpoint завершила приобретение Tessian, компании по безопасности облачной электронной почты. Tessian предлагает платформу безопасности, работающую на основе искусственного интеллекта, для защиты от случайной утечки данных и угроз, связанных с электронной почтой. Их решения Guardian, Enforcer и Defender используют машинное обучение для обеспечения комплексной защиты от потери данных. Proofpoint планирует представить новое решение на базе возможностей Tessian на рынке уже в начале 2024 года. Новая технология будет обеспечивать эффективную защиту от широкого спектра угроз, включая социальную инженерию и фишинг, а также предотвращать утечку данных в различных каналах связи, от электронной почты до облака, используя пользовательскую активность, искусственный интеллект и классификацию данных. В Proofpoint подчеркивают, что более 90% успешных кибератак и потери данных вызваны ошибками сотрудников, вплоть до 65% случаев утечки данных по неправильно направленным электронным письмам.

Новые продукты, услуги, обновления

Среди перспективных стартапов 2024г - Concentric AI. Платформа класса DSPM использует глубокое обучение для автоматического обнаружения и классификации конфиденциальных данных, определения рисков и устранения проблем. С декабря 2023г продукт стартапа Semantic Intelligence™ DSPM предлагает обнаружение, идентификацию, мониторинг рисков и защиту от исправления аудио- и видеофайлов. Подчеркивается, что благодаря этому обновлению организации теперь могут впервые защищать конфиденциальные данные, передаваемые на собраниях, с помощью Zoom, Microsoft Teams, WebEx и других популярных инструментов для совместной работы. До объявления в отрасли не существовало обнаружения конфиденциальных данных в аудио- и видеофайлах. Ранее в октябре компания Concentric AI сделала доступным продукт Semantic Intelligence™ DSPM на CrowdStrike Marketplace и добавила функцию определения происхождения данных.

Управление идентификацией и доступом

Слияния и поглощения

Компания Okta заключила в декабре сделку о приобретении израильского стартапа в области кибербезопасности Spera Security. По оценкам Calcalist, стоимость сделки составляет от 100 до 130 миллионов долларов, в зависимости от результатов работы и вознаграждения сотрудников. Spera Security предоставляет программное обеспечение для обнаружения, предотвращения и реагирования на угрозы цифровой идентификации, а также возможности управления состоянием безопасности.

Защита инфраструктуры

Слияния и поглощения

Компания Singapore Technologies Engineering Ltd (ST Engineering) объявила о том, что ее киберподразделение ST Engineering Info-Security заключило соглашение о приобретении 100% выпущенных акций D'Crypt, косвенной дочерней компании StarHub Ltd. Основанная в 2000 году компания D'Crypt специализируется на разработке криптографических технологий и предлагает решения в области зашифрованных коммуникаций, одночиповых криптотокенов, безопасных вычислений и высокопроизводительных

Новые продукты, услуги, обновления

Palo Alto Networks в ноябре представила второе поколение XSIAM (расширенная аналитика безопасности и управление автоматизацией). Первоначально выпущенный в октябре 2022 года, XSIAM позиционируется компанией как современная замена устаревшим системам SIEM. Ключевые обновления включают новый командный центр XSIAM, который обеспечивает единое представление обо всех действиях в SOC — от приема данных и анализа до создания правил и обнаружения предупреждений. С помощью новой информационной панели покрытия MITRE ATT&CK в XSIAM 2.0 Palo Alto Networks обеспечивает наглядность того, насколько хорошо клиент защищен каждым из различных элементов структуры MITRE ATT&CK. XSIAM 2.0 также представляет новую возможность «привнести в платформу свое собственное машинное обучение» (Bring Your Own ML). Это позволяет командам безопасности интегрировать свои собственные модели машинного обучения поверх XSIAM и выполнять сценарии использования машинного обучения для обеспечения безопасности, уникальные для их среды. Первоначальными целевыми клиентами XSIAM являются крупные организации со зрелыми командами SOC и обработки данных, однако, по заявлению менеджеров, в перспективе продукт имеет потенциал для удовлетворения потребностей более широкого круга клиентов. Сюда входят компании среднего бизнеса, где поставщики услуг могут использовать XSIAM для разработки индивидуальных решений для клиентов.

В ноябре Microsoft анонсировал частную предварительную версию Unified Security Operations Platform - единой платформы управления безопасностью, объединяющей Sentinel, Defender XDR и Microsoft Security Copilot. Ожидается, что платформа выйдет в публичную предварительную версию в 2024 году. Эта платформа имеет унифицированный опыт сортировки инцидентов с учетом угроз в цифровом пространстве. Пользователи имеют единый набор правил автоматизации и сборников сценариев на базе GenAI, а также возможность запрашивать все данные SIEM и XDR в одном месте, чтобы обнаруживать угрозы и предпринимать действия по устранению. Так, пользователи могут попросить Copilot на естественном языке проанализировать вредоносные сценарии или создать запросы Kusto Query Language (KQL) для поиска данных в Microsoft Sentinel и Defender XDR. Пользователи также могут мгновенно создать отчет об инциденте, в котором подводятся итоги расследования и предпринятых действий по исправлению ситуации.

В ноябре Sophos объявила об обновлениях своего портфеля продуктов, в том числе программного обеспечения межсетевого экрана и платформы расширенного обнаружения и реагирования (XDR).

В рамках обновлений компания развернула поддержку на своей платформе XDR ключевых продуктов от 21 крупного поставщика технологий, включая таких конкурентов, как CrowdStrike, Fortinet и Palo Alto Networks.

Sophos объявила о добавлении в свое программное обеспечение сетевого брандмауэра возможностей Active Threat Response, которые могут автоматически блокировать вредоносное поведение и предотвращать проникновение злоумышленников в сеть. Новая версия Sophos Firewall также включает в себя шлюз доступа к сети с нулевым доверием (ZTNA).

Sophos также объявила, что обновление делает NDR доступным как отдельное предложение для клиентов (ранее NDR был доступен только для клиентов с MDR).

Управление рисками

Слияния и поглощения

Mimecast в январе 2024г объявила о приобретении стартапа Elevate Security, который разработал технологию для выявления пользователей, которые демонстрируют рискованное поведение в сфере безопасности внутри организации. Технология Elevate Security будет интегрирована с обучающей платформой Mimecast по вопросам безопасности. Компания Elevate Security со штаб-квартирой в Сан-Франциско привлекла $18,25 млн инвестиций с момента ее основания в 2017 году. Среди спонсоров были CrowdStrike Falcon Fund, Foundry Group, Salesforce Ventures и Shasta Ventures.

Прочее ИТ

Слияния и поглощения

Компания Broadcom завершила в ноябре сделку по приобретению VMware общей суммой на 69 миллиардов долларов. Broadcom сразу же принялась за изменение портфеля продукта и параметров лицензирования. Компания анонсировала обновленную платформу VMware vSphere Foundation, которая включает в себя vSphere с интеллектуальным управлением работой. Продукты VMware Cloud Foundation и VMware vSphere Foundation будут дополнены различными функциями, включая хранилища, кибербезопасность, аварийное восстановление и другие. Также планируются расширения на основе ИИ, хотя они еще в стадии разработки. Компания также намерена отказаться от решений для конечных пользователей, таких как VDI (например, VMware Horizon).

Hewlett Packard Enterprise (HPE) ведет переговоры о покупке производителя телекоммуникационного оборудования Juniper Networks за $13 млрд, сообщают Reuters и The Wall Street Journal. Juniper Networks предлагает решения в области маршрутизации, Wi-Fi, сетевой безопасности, а также соответствующее оборудование. Кроме того, Juniper занимается разработками в области искусственного интеллекта (ИИ) — ей принадлежит платформа Mist, которая использует технологии ИИ и машинного обучения. Если сделка состоится, она поможет поставщику «облачных» услуг Hewlett Packard Enterprise усилить позиции в сфере разработок ИИ.

Информзащита
Системный интегратор

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru

IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru