Обзор отчёта Gartner «Магический квадрант для информации о безопасности и управления событиями»

Опубликован 10 Октября 2022

Откорректирован 12 октября 2022

Содержание презентации

1 Описание отчета

2 Лидеры магического квадранта

3 Претенденты на лидерство

4 Нишевые игроки

5 Дальновидные производители

Термины и определения отчета

SIEM — это **S**ecurity **I**nformation and **E**vent **M**anagement.

Объединение двух терминов, обозначающих область применения ПО: SIM (**S**ecurity **I**nformation **M**anagement) — управление информацией о безопасности, и **SEM** (**S**ecurity **E**vent **M**anagement) — управление событиями безопасности.

Система предназначена для анализа информации, поступающей от различных других систем, таких как DLP, IDS, антивирусов, сетевого оборудования и т.д. и дальнейшего выявления отклонения от норм по каким-то критериям.

В случае выявления отклонение генерируется инцидент. В основе работы SIEM математика и статистика.

Каких-либо защитных функций система SIEM сама по себе не несет

Термины и определения отчета

UEBA - **U**ser and **E**ntity **B**ehavior **A**nalytics (система аналитики поведения пользователей и сущностей). Продукт UEBA определяет шаблоны в типичном поведении пользователей, а затем детектирует аномальные действия, которые не соответствуют этим шаблонам и могут представлять проблемы с безопасностью. Кроме того, системы UEBA выявляют нетипичные события в различных сущностях (entity), к которым относят рабочие станции, программное обеспечение, сетевой трафик, СХД и прочее и т. п.

Для определения отклонений применяются разнообразные аналитические методы, включая машинное обучение. Источниками данных для UEBA-систем являются файлы логов серверных и сетевых компонентов, систем безопасности, локальные журналы с конечных рабочих ПК.

Обычно решения UEBA выполняют свою работу уже после того, как другие средства киберзащиты не смогли выявить угрозы внутри сети.

Термины и определения отчета

SOAR (**S**ecurity **O**rchestration, **A**utomation and **R**eporting)

Gartner определяет SOAR как инструментарий, позволяющий сводить данные об угрозах безопасности из разных источников для последующего анализа. SOAR автоматизирует этот процесс: от назначения приоритета до работе с шаблонными «ответами» на инциденты.

SOAR-продукты направлены на интеграцию различных источников данных о рисках и формализацию работы с инцидентами.

- Оркестровка (Orchestration) — интеграция технологий и инструментов для принятия решений на основе информации об уровне риска и состоянии системы.
- Автоматизация (Automation) — для замещения задач, которые ранее выполняли «вручную», автоматическими действиями со стороны системы (playbooks).
- Формирование отчетов (Dashboards and Reporting) — визуализация информации по ключевым метрикам и составление отчетов (для трех типов сотрудников — аналитиков, руководителей SOC (Security Operations Center) и директоров по ИБ (Chief Information Security Officer, CISO).

Термины и определения отчета

TIP - **T**hreat **I**ntelligence **P**latform (Платформа анализа угроз)

Программное решение, используемое организациями для обнаружения, блокирования и устранения угроз информационной безопасности.

Платформа объединяет несколько каналов сбора данных об угрозах, сравнивает с предыдущими событиями и генерирует оповещения для группы безопасности.

TIP интегрируются с существующими решениями по управлению информацией и событиями безопасности (SIEM) и присваивают значения оповещениям, расставляя среди них приоритеты в соответствии с уровнем срочности.

Описание отчета

Магический квадрант для информации о безопасности и управления событиями

SIEM собирает данные о событиях, которые создаются решениями для мониторинга, оценки , обнаружения и реагирования, развернутыми в приложениях, сети, конечных точках и облачных средах. Возможности включают обнаружение угроз с помощью корреляции и анализа поведения пользователей и объектов (UEBA), а также интеграцию реагирования, обычно управляемую с помощью оркестровки безопасности, автоматизации и реагирования (SOAR). Отчеты о безопасности и постоянно обновляемый контент об угрозах с помощью функций платформы анализа угроз (TIP) также являются распространенными интеграциями . Хотя SIEM в основном развертывается как облачная служба , она может поддерживать локальное развертывание.

О компании Gartner

Gartner, Inc. — американская компания, специализирующаяся на исследованиях рынка информационных технологий. Штаб-квартира расположена в городе Стэмфорд, штат Коннектикут. Основана в1979 году Гидеоном Гартнером.
Компания работает в трех основных сегментах: исследования, конференции и консалтинг.

- Исследования предоставляют независимые, объективные советы руководителям предприятия через услуги подписки, которые включают доступ по запросу к опубликованным исследованиям, а также прямой доступ к сети, состоящей из примерно 2300 экспертов-исследователей, расположенных по всему миру. Компания обеспечивает надежной, объективной информацией и советами по критически важным приоритетам руководителей во всех функциональных областях предприятия с помощью отчетов, брифингов, запатентованных инструментов, сервисов одноранговых сетей и программ членства, которые позволяют управлять организацией;
- Конференции предоставляют бизнес-профессионалам возможность учиться, знакомиться с сессиями, проводимыми экспертами Gartner по исследованиям и передовыми технологическими решениями, посещать семинары по обмену опытом, индивидуальные встречи с аналитиками и консультантами и многое другое. Конференции также предоставляют участникам возможность пообщаться с руководителями ведущих мировых технологических компаний;
- Консалтинг объединяет в себе возможности ведущих исследований Gartner с индивидуальным анализом и поддержкой на местах, чтобы помочь директорам по информационным технологиям и другим руководителям высшего звена, продвигающим стратегические инициативы, связанные с технологиями, оптимизировать эффективность бизнеса;
- Компания консультирует более чем 15 000 предприятий в США, Канаде, Европе, на Ближнем Востоке и в Африке. География распределения выглядит следующим образом: США и Канада– 64%; Европа, Ближний Восток и Африка -23%; другие -12%.
- Основными конкурентами являются компании Evalueserve, International Data Group, Forrester Research и Nielsen.

Критерии включения в отчёт поставщиков

- Продукт, предоставляющий конечным пользователям возможности SIM и SEM с помощью облачного программного обеспечения и/или SaaS.;
- По крайней мере две из перечисленных ниже функции, функциональных возможностей и дополнительных решений принадлежали поставщику (полностью приобретенные или органически созданные) и включались в продукт SIEM или продавались как отдельные надстройки с 1 февраля. 2022:
  - ✓ Организация безопасности, автоматизация и реагирование (SOAR)
  - ✓ Платформа анализа угроз (TIP)
  - ✓ Аналитика поведения пользователей и объектов (UEBA)
  - ✓ Долгосрочное хранение данных и отчетность (более 365 дней)
- Выручка от лицензий и обслуживания облачных/SaaS (исключая управляемые услуги) превышает 50 миллионов долларов США за 12 месяцев до 1 февраля 2022 г. или иметь 100 отдельных производственных клиентов с прямыми контрактами на облачные или SaaS-платформы на конец того же периода;
- За 12 месяцев до 1 февраля 2022 года; получить 15% дохода от SIEM-облака/SaaS от покупателей, штаб-квартира которых находится за пределами географического региона расположения штаб-квартиры поставщика, или иметь не менее 20 производственных клиентов, каждый из которых имеет штаб-квартиру за пределами географического региона расположения штаб-квартиры поставщика;
- По состоянию на 1 февраля 2022 года операции по продажам и продвижению продуктов SIEM проводились поставщиком как минимум в двух географических регионах;

Определение/описание рынка

Рынок SIEM вырос с 3,41 млрд долларов в 2020 году до 4,10 млрд долларов в 2021 году. Основными драйверами покупки SIEM являются обнаружение угроз, реагирование, управление рисками и соответствие требованиям.

Рынок SIEM развивается быстрыми темпами и продолжает оставаться чрезвычайно конкурентным. Реальность того, чем SIEM была всего пять лет назад, начинает отделяться от того, чем SIEM является и что предлагает сегодня.

В настоящее время SIEM широко поддерживает возможности управления рисками за счет использования точек данных, таких как состояние конфигурации облачных активов, профилирование рисков для пользователей и объектов, инвентаризация активов и рейтинг критичности, с целью обеспечения состояния рисков в реальном времени

Наиболее известная архитектура развертывания перешла от клиентской и управляемой к облачной (SaaS и размещенной), чтобы воспользоваться преимуществами простого развертывания, масштабируемости и гибкости

Рынок SIEM движется к многофункциональному решению для обеспечения безопасности, предлагающему клиентам множество вариантов для удовлетворения их потребностей в безопасности, таких как:

- Обнаружение угроз с использованием аналитики (в реальном времени, пакетной, на основе пользователей, сущностей) алгоритмах Data science
- Реагирование, включая SOAR и управление инцидентами
- Управление воздействием, включая сбор сведений об активах, пользователе, истории инцидентов, конфигурации облачных активов и согласования системы обнаружения угроз
- Следование определенным практикам, включая отчеты, мониторинг, аудит и защиту системы записей

Понятие магического квадранта Gartner

маркетинг и продажи

Ability to Execute →

CHALLENGERS Претенденты на лидерство (**Challengers**) имеют качественные продукты, которые удовлетворяют основным требованиям рынка и имеют высокий уровень продаж и долю рынка, которая позволяет им превосходить нишевых игроков. Претенденты обеспечивают себе прибыль путем конкуренции на уровне базовых функций, но не на уровне более совершенных возможностей. Продукты данных вендоров хороши для решения узкоспециализированных задач.	**LEADERS** Лидеры (**Leaders**) демонстрируют стабильный прогресс и усилия по всем показателям, по которым проводится оценка. Их действия поднимают уровень конкуренции на рынке, они могут изменить курс развития всей индустрии.
Нишевые игроки (**Niche Players**) предлагают жизнеспособные решения, которые отвечают основным требованиям покупателей. Чаще всего эти вендоры упускают возможности оказать влияние на рынок, но это не означает, что они покорно следуют за лидерами отрасли. Нишевые игроки могут быть ориентированы на небольшие сегменты рынка и часто демонстрируют на них более высокую эффективность, чем лидеры. **NICHE PLAYERS**	Дальновидные производители (**Visionaries)** инвестируют средства в лидирующие технологии, которые лягут в основу следующего поколения продукта и позволят покупателям получать более быстрый доступ к улучшенному управлению и безопасности. Вендоры из этой группы могут оказывать влияние на развитие отрасли, но не могут воздействовать на лидеров и претендентов на лидерство. **VISIONARIES**

Completeness of Vision →

технологическая продвинутость и стратегия

Квадрант для систем управления информацией о безопасности и событиями

As of June 2022 © Gartner, Inc

Gartner

Лидеры:	❑ Microsoft ❑ IBM ❑ Splunk ❑ Sequronix ❑ Exabeam
Претенденты	❑ LogRhytm ❑ Rapid 7 ❑ Fortinet ❑ Devo
Нишевые игроки	❑ ManageEngine ❑ Logpoint ❑ Huawei
Дальновидные производители	❑ Sumo Logic ❑ Gurucul ❑ Elastic ❑ Micro Focus

Лидеры магического квадранта

- Microsoft
- IBM
- Splunk
- Sequronix
- Exabeam

Microsoft является лидером в этом магическом квадранте. Его продукт SIEM, **Microsoft Sentinel**, поставляется только как SaaS через центры обработки данных Microsoft Azure. У Microsoft есть большая и разнообразная клиентская база, которая обслуживает как крупных, так и мелких клиентов и предлагает продукт SIEM в различных условиях на международном уровне.

Лицензирование основано на объеме принимаемых данных, зарезервированной емкости или с оплатой по мере использования. Однако отмечается что трудно понять реальную стоимость: хотя в ценообразовании используется простая модель приема данных. Клиенты сообщают, что цены непредсказуемы и сложны для понимания в сочетании с другими лицензиями Microsoft

IBM является лидером в этом магическом квадранте. Его продукт **IBM QRadar** можно развернуть с помощью локального программного обеспечения, в общедоступном/частном облаке или гибридном, или доставить в облачном формате как QRadar on Cloud (QROC). Клиентская база IBM SIEM охватывает Северную Америку, Европу, Азиатско-Тихоокеанский регион, Ближний Восток и Латинскую Америку.

Помимо QRadar, IBM предлагает другие продукты для обеспечения безопасности, такие как QRadar Network Insights, QRadar Vulnerability Manager, QRadar XDR Connect, QRadar SOAR (формально Resilient) и Cloud Pak for Security (CP4S). Лицензирование для QRadar SIEM основано на количестве событий в секунду (EPS) и/или потоках в минуту (FPM). Неограниченное серверное лицензирование — это альтернативный вариант только для экземпляров, развернутых в облаке

Положительные стороны, отмеченные в отчете

- Сильная аналитика и настройка: QRadar имеет большое количество готового контента и аналитических возможностей. Клиенты также дали положительные отзывы о способности QRadar создавать и настраивать приложения и информационные панели.
- Крупный бизнес и присутствие в области безопасности: IBM обладает необходимым глобальным присутствием (через прямые и партнерские каналы) для предоставления своих продуктов, поддержки и услуг в каждом крупном географическом регионе. Кроме того, у него достаточно сотрудников, которые понимают региональные правила и говорят на нескольких языках, чтобы поддерживать индивидуальные проекты и конфигурации.
- Множество предложений продуктов для обеспечения безопасности: IBM предлагает широкий спектр дополнительных и тесно интегрированных дополнительных технологий, а также услуги, дополняющие и поддерживающие QRadar. К ним относятся сетевая безопасность, управление уязвимостями, анализ угроз, защита данных, услуги UEBA, SOAR и MSS/MDR.

Высказанные предостережения для покупателя

- Правила корреляции и аналитика аналогичны: QROC не делает различий между правилами корреляции и аналитикой; следовательно, существует разная степень сложности, от простой до продвинутой, в отношении готового контента, что затрудняет сравнение.
- Cloud Pak замедляет инновации SIEM: инновации QRadar SIEM продвигаются медленно, поскольку IBM переключает ресурсы на платформу Cloud Pak for Security и возможности безопасности нового поколения.
- Внедрение требует улучшения: на основе отзывов клиенты сообщают, что начальное развертывание может быть сложным процессом. Ему также может не хватать гибкости с точки зрения подключения новых источников данных..

Splunk является лидером в этом магическом квадранте. Его SIEM называется **Enterprise Security** (Splunk ES) и является дополнением к решению Splunk Enterprise. Большинство покупателей Splunk ES находятся в Северной Америке.

Основные покупатели Splunk ES - крупные корпоративные организации. Направление Splunk ES состоит в том, чтобы предложить больше обогащения событий и артефактов через свой пользовательский интерфейс и способствовать доставке большего количества контента.

Лицензирование доступно как объем в день или облачные рабочие нагрузки (называемые «Splunk Virtual Compute»).

Securonix является лидером в этом магическом квадранте. Его SIEM-решение называется **Next-Gen SIEM** и включает в себя SIEM Next-Gen, Security Data Lake, UEBA, SOAR, NDR, анализ угроз, анализ поведения злоумышленников.

Большинство клиентов Securonix находятся в Северной Америке, затем следуют Европа, Азия/Тихоокеанский регион, Ближний Восток и Африка, а также Латинская Америка.

Клиентами в основном являются крупные предприятия, и некоторые клиенты среднего размера.

Лицензирование основано на тождествах и ЭПС. Большинство покупателей выбирают временные лицензии, но доступны бессрочные лицензии

Exabeam является лидером в этом магическом квадранте. Решение **Exabeam SaaS SIEM**, известное как Exabeam Fusion SIEM, доступно в качестве основного продукта или в комплекте с корпоративными версиями. Эти продукты также доступны для гибридного облака.

Корпоративная версия включает Advanced Analytics, Threat Hunter, Entity Analytics и Case Manager. Дополнительное облачное хранилище данных (Cloud Archive) и средство реагирования на инциденты (SOAR) доступны в качестве надстроек.

Большинство клиентов Exabeam находятся в Северной Америке, а вторая по величине — в Европе. Большинство клиентов — крупные предприятия. Лицензирование основано на сроках и зависит от объемов получаемых данных.

Претенденты на лидерство

- LogRhytm
- Rapid7
- Fortinet
- Devo

LogRhythm — претендент в этом магическом квадранте. Его SIEM-решение представляет собой платформу **LogRhythm SIEM**, которая включает в себя несколько дополнительных компонентов для обеспечения аналитики конечных точек, сети и поведения пользователей.

Подавляющее большинство ее клиентов SIEM находятся в Северной Америке и Европе, остальные — в Азиатско-Тихоокеанском регионе, на Ближнем Востоке, в Африке и Латинской Америке.

Клиентская база ориентирована на предприятия среднего размера и небольшие организации, хотя крупные предприятия также приобрели LogRhythm SIEM. Доступен облачный вариант, но большинство клиентов развернули SIEM локально. Лицензирование доступно на бессрочной основе (по среднему количеству сообщений в секунду в день) или по подписке (по количеству сотрудников).

Rapid7 — претендент в этом магическом квадранте. Его SIEM-решение **InsightIDR** работает на облачной платформе Insight.

Другие доступные продукты включают InsightVM (управление уязвимостями), InsightAppSec, InsightConnect (SOAR), InsightCloudSec (управление уровнем безопасности в облаке) и Threat Command (анализ угроз).

Клиенты InsightIDR SIEM больше всего сконцентрированы в США, за которыми следуют Европа и Азиатско-Тихоокеанский регион.

Лицензирование основано на срочной лицензии с простой моделью ценообразования, основанной на количестве отслеживаемых активов

Fortinet — претендент в этом магическом квадранте. Его SIEM-решение — **FortiSIEM**. Он имеет глобальное присутствие и клиентов во всех основных регионах мира, но особенно в Северной Америке и Европе. Этот продукт включает расширенные агенты (для UEBA на базе Windows). FortiSIEM интегрируется с FortiSOAR, FortiAnalyzer и другими элементами набора продуктов безопасности Fortinet.

Цены основаны на устройствах для SOAR, EPS и количестве агентов для SIEM. FortiSIEM доступен в виде виртуального или физического устройства.

Лицензирование основано на устройствах, связанных с 10 событиями в секунду на устройство. Доступны бессрочные лицензии и лицензии по подписке.

Devo — претендент в этом магическом квадранте. Его продукт SIEM, приложение **Security Operations**, поставляется как предложение SaaS. Клиентская база Devo SIEM в основном находится в Северной Америке, за которой следуют Европа и Ближний Восток, и состоит из малых, средних и крупных организаций.

В начале 2022 года Devo получила статус «В процессе» для стандарта Федеральной программы управления рисками и авторизацией (FedRAMP) и рассчитывает получить полную авторизацию позже в этом году.

Лицензирование, включая его дополнительные возможности (TIP через MISP, горячее хранилище, Entity Analytics и Devo Flow), основано на объеме принимаемых данных

Положительные стороны, отмеченные в отчете

- Поддержка поставщиков услуг и сложных организаций: Fortinet FortiSIEM предлагает встроенную поддержку многопользовательского режима для сложных организаций и поставщиков услуг, а также множество характерных для них функций. Он также предлагает модель на основе потребления для поставщиков управляемых услуг безопасности (MSSP) с неограниченным EPS.
- Fortinet FortiSIEM обладает мощными возможностями обнаружения активов и встроенной базой данных управления конфигурацией (CMDB). Это обеспечивает централизованную видимость активов, обнаруженных с помощью активного сканирования и пассивной проверки журналов.
- Fortinet предлагает разнообразную экосистему продуктов для обеспечения безопасности и сетевых продуктов, интегрированных через Fortinet Security Fabric. Потенциальные и существующие клиенты Fortinet, которые ищут единого поставщика для предоставления им решений для мониторинга, обнаружения и реагирования на угрозы, должны рассмотреть Fortinet.

Высказанные предостережения для покупателя

- Fortinet полагается на партнеров, которые предлагают услуги хостинга для FortiSIEM в качестве средства предоставления покупателям услуг, подобных SaaS. Организации конечных пользователей могут развернуть решение в своем собственном общедоступном или частном облаке или в виде модели гибридного облака.
- Охват облачной безопасности FortiSIEM не так силен, как у других конкурентов. В нем отсутствует поддержка нескольких общедоступных облачных инфраструктур и сервисов платформы (CIPS), а единственными поддерживаемыми брокерами безопасности доступа к облаку (CASB) являются собственный продукт FortiCASB от Fortinet и Oracle CASB.
- UEBA доступен в двух вариантах: премиум-предложение и более ограниченная версия, встроенная в FortiSIEM. Оба требуют развертывания агента и не имеют функций, доступных у конкурентов. Однако в дорожной карте Fortinet указано, что эти пробелы будут устранены.

Нишевые игроки

- ManageEngin
- Logpoint
- Huawei

ManageEngine — нишевый игрок в этом магическом квадранте. Его решение **Log360 SIEM** основано на облаке и развернуто в собственном центре обработки данных Zoho Corporation.

Основными покупателями Log360 являются клиенты среднего и крупного бизнеса в основном в Северной Америке, Европе, на Ближнем Востоке и в азиатско-тихоокеанском регионе.

Помимо инструмента SIEM, Log360 включает в себя другие продукты безопасности, такие как Firewall Analyzer, EventlLog Analyzer, ADAudit Plus, Vulnerability Manager Plus, Cloud Security Plus, DataSecurity Plus и FileAnalysis. Лицензирование SaaS основано на объеме данных, хранящихся в облаке за определенный период. Лицензирование локальной версии зависит от количества источников журналов. Сюда входят такие устройства, как рабочие станции, серверы Windows и другие сетевые устройства. К возможностям продукта включают аналитику поведения пользователей и объектов (UEBA),

Logpoint — нишевый игрок в этом магическом квадранте. Его решение SIEM изначально сочетается с функциональностью SOAR и в основном используется клиентами в формате SaaS или облачном формате. Самая большая концентрация покупателей — это малые и средние клиенты из Европы. У Logpoint есть замечательное предложение для мониторинга и реагирования на угрозы для платформ SAP. Лицензирование основано на количестве контролируемых «узлов». Компонент SOAR измеряется количеством пользователей с однопользовательской лицензией, включенной в продукт SIEM. Возможности UEBA лицензируются отдельно.

Huawei является нишевым игроком в этом магическом квадранте. Его SIEM-решение **называется HiSec Insight** и включает в себя Huawei Cloud Security Brain.

Существует множество дополнительных модулей и сопутствующих технологий для конкретных требований к функциям или архитектуре.

Его клиенты SIEM в основном сосредоточены в Китае; хотя меньшее количество клиентов находится на Ближнем Востоке, в Африке и Латинской Америке. Клиентская база почти поровну разделена между крупными и средними предприятиями. Цены на локальные развертывания основаны на скорости передачи данных (EPS) и объеме (гигабайт в день) с дополнительными расходами на хранение журналов и дополнительные модули. Развертывание SaaS основано на количестве приобретенных Elastic CloudServers

Дальновидные производители

- SumoLogic
- Gurucul
- Elastic
- MicroFocus

Sumo Logic — провидец в этом магическом квадранте. Его продукт SIEM, **Cloud SIEM**, поставляется только как решение SaaS. Клиентская база Sumo Logic состоит из малого, среднего и крупного бизнеса, большинство из которых находится в Северной Америке.

За последний год компания увеличила свое присутствие в Европе и Азии/Тихоокеанском регионе. В 2021 году Sumo Logic приобрела DFLabs, которая обеспечивает дополнительные процессы обработки инцидентов, автоматизированные действия по сценариям и обогащение за счет внешних источников информации с эффективностью, аналогичной автономному предложению SOAR.

Лицензирование осуществляется на основе подписки (с ценообразованием, основанным на приеме данных) или на основе кредитов (с кредитами, используемыми для обеспечения использования определенных ресурсов, например, для периодического поиска или непрерывной аналитики), с вариантами многоуровневого и пакетного анализа.

Gurucul — Провидец в этом Магическом квадранте. Его SIEM называется **Analytics-Driven SIEM** и представляет собой модульное решение, широко ориентированное на SIEM, UEBA, аналитику идентичности, аналитику мошенничества, SOAR и анализ сетевого трафика.

Gurucul предлагает пакетные возможности TDIR через свою платформу Security Analytics и Operations Platform. Компания представлена на рынке преимущественно в Северной Америке, а ее клиентский профиль преимущественно основан на крупных корпоративных организациях. У Gurucul есть надежная дорожная карта, включающая интеграцию с социальными сетями, интеграцию с оценкой состояния безопасности и улучшенную интеграцию со службами анализа угроз и защиты от цифровых рисков. Лицензирование основано на отслеживаемых активах и доступно по подписке или бессрочно.

Elastic — провидец в этом магическом квадранте. Его решение **Elastic Security** в основном ориентировано на аналитику безопасности и функции корпоративного поиска в сочетании с агентом безопасности Elastic Endpoint, который включен в решение SIEM.

Большинство клиентов Elastic Security находятся в Северной Америке и Европе, и в равной степени это малые, средние и корпоративные клиенты. Прирост новых клиентов в настоящее время выше среди небольших организаций. В 2021 году Elastic завершила приобретение Cmd и создала систему безопасности, чтобы предложить функциональные возможности платформы защиты облачных рабочих нагрузок в Elastic Agent, входящем в состав Elastic Security. Лицензирование основано на облачных ресурсах, таких как вычислительные ресурсы и хранилище, для поддержки клиентской среды..

Micro Focus — провидец в этом магическом квадранте. Его продукт **ArcSight** в основном ориентирован на функциональность SIEM, UEBA, SOAR и TIP. Деятельность ArcSight географически диверсифицирована (за исключением Латинской Америки).), а его клиентский профиль преимущественно среднего размера.

Локальные развертывания намного перевешивают облачные развертывания, в основном благодаря недавней доступности облачного варианта. Micro Focus вложила значительные средства в свой портфель продуктов для обеспечения безопасности CyberRes, который включает в себя защиту данных, управление доступом к идентификационным данным (IAM), безопасность приложений и безопасность операций. Первым крупным продуктом из портфеля операций безопасности CyberRes является Galaxy, облачное решение для анализа угроз, которое интегрируется в рабочий процесс ArcSight.

Лицензирование основано на EPS для SIEM и на объект для UEBA.

Благодарю за внимание

Ронжин В.В.
Специально для компании HIHOL
Ташкент 2022, 9 декабря 2022г.