ArcSight Recon

Micro Focus ArcSight Recon — это комплексный инструмент управления журналами аудита (log management) и решение для threat hunting, которое упрощает соблюдение нормативных требований и ускоряет процесс обнаружения угроз.

Основные возможности продукта

Обеспечение безопасности играет очень важную роль. Все больше бизнес-операций осуществляется в Интернете, все больше конфиденциальных данных хранится в цифровом виде и все больше работы выполняется удаленно. Нормативные требования становятся все более строгими, а злоумышленники используют все более сложные методы атак.

По мере того как организации стремятся собирать и хранить данные информационной безопасности из бесконечного числа источников, мониторинг этих данных и управление ими также усложняются. Многие решения на рынке разрабатывались без учета требований безопасности и непреднамеренно оказались неэффективными при реализации в контексте SIEM, соответствия нормативным требованиям, ведения журналов аудита и обнаружения угроз. Централизованный сбор журналов аудита и обнаружение угроз являются важными задачами современного SOC, и организациям необходимо решение, которое обеспечит не только соответствие современным стандартам, но и будет ориентировано на будущее.

ArcSight Recon — это комплексное решение для управления событиями и аналитики информационной безопасности, которое упрощает соблюдение нормативных требований и ускоряет процесс обнаружения угроз. Оно сочетает в себе соответствие стандартам, а также требования к хранению и отчетности для управления журналами с возможностями поиска и анализа больших данных. Решение Recon создавалось для аналитиков информационной безопасности и не требует знаний DBA для его использования. Оно помогает обнаруживать и устранять угрозы,

обрабатывая миллиарды событий и предоставляя их для быстрого поиска, визуализации и формирования отчетов. Recon обеспечивает инженерам SOC более полное представление о состоянии корпоративной безопасности и играет важную роль в предоставлении значимой многоуровневой аналитики ArcSight.

Основные преимущества

Централизация управления журналами

ArcSight Recon сохраняет терабайты событий аудита от различных источников. Он позволяет хранить данные, а также выполнять их аналитику для централизованного получения информации о состоянии корпоративной безопасности. Панель Event Details в Recon позволяет исследовать отдельные события и группы событий для быстрого получения данных. Представление событий в исходном виде (RAW) позволяет аналитикам просматривать ненормализованные журналы событий. Решение было разработано с целью упрощения аналитики, повышения удобства использования и с учетом требований безопасности. Для его развертывания не требуется администратор баз данных.

Основные функции

- Панель данных о событии
- Просмотр исходных событий
- Обнаружение аномалий
- Удобная панель поиска
- Готовые наборы отчетов
- Унифицированная платформа ArcSight
- Single Sign-On (SSO)

Основные преимущества

- Централизация управления журналами
- Ускорение поиска и устранения угроз
- Создание отчетов о соответствии нормативным требованиям
- Возможности горизонтального масштабирования
- Интеграция в существующую среду информационной безопасности

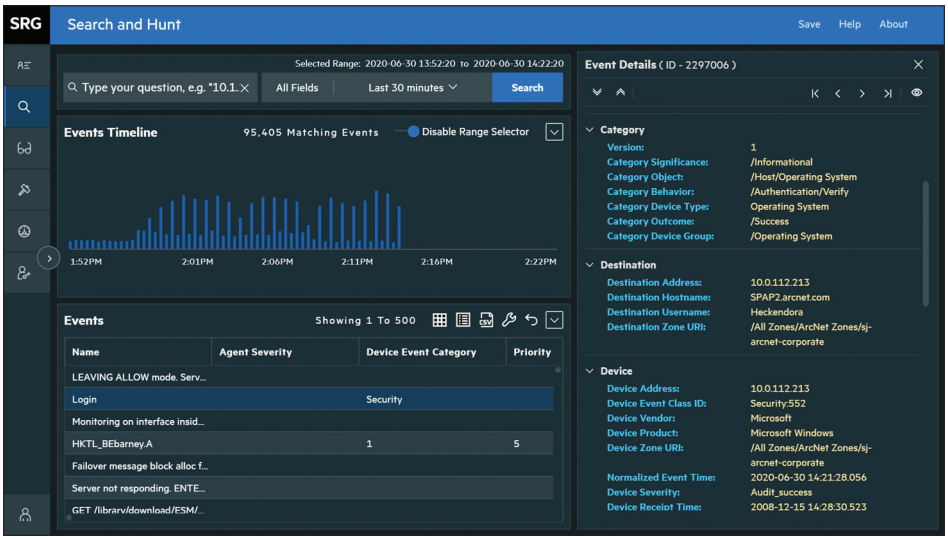

Рис. 1. Панель Event Details

Ускорение поиска и устранения угроз

Динамические подсказки в Recon позволяют обрабатывать огромное количество данных журналов, не прилагая больших усилий, а мощная технология аналитики безопасности обеспечивает быстрое получение результатов. Столбчатая база данных ArcSight Recon отвечает на запросы быстрее, чем традиционные базы данных, что позволяет оперативно и эффективно исследовать миллионы событий. Централизованное хранение доверенных (целостных) и нормализованных данных ускоряет процесс расследования и повышает качество результатов. Выявление аномалий позволяет быстро определять отклонения от базовых метрик поведения хоста. Удобный интерфейс поиска Recon отображает события в табличном виде, а также гистограмму по времени. Он оптимизирует поиск угроз в на больших потоках событий, обеспечивая аналитику безопасности в необходимом масштабе. Решение позволяет приоритизировать обнаруженные аномалии, что повышает его эффективность.

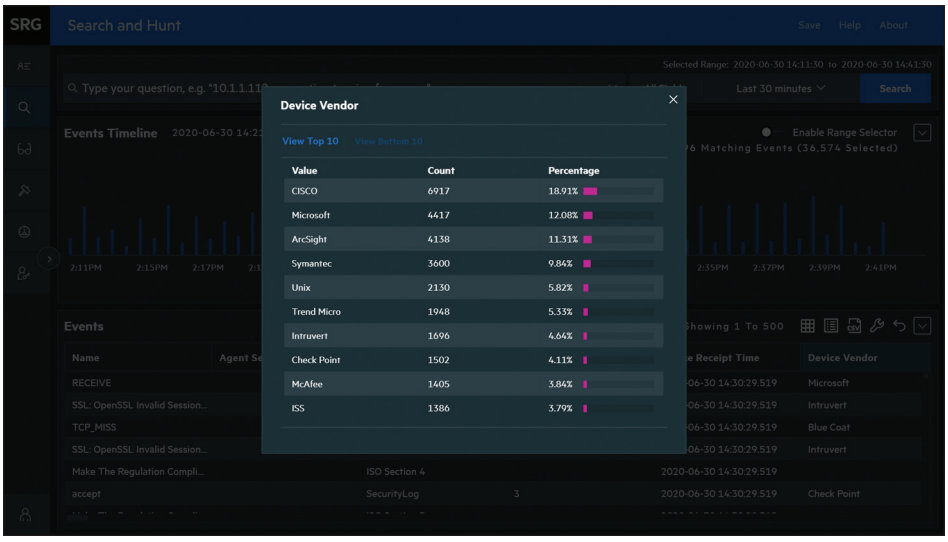

Рис. 2. Гистограмма значений устройств поставщика

Создание отчетов о соответствии нормативным требованиям

Ускорьте создание отчетов о соответствии нормативным требованиям благодаря пакетам отчетов Recon. Используйте мастера создания отчетов или выберите подходящий шаблон для создания отчета с перекрестными ссылками, таблиц или отчетов на основе диаграмм. Доступен предварительный вариант в соответствии со стандартом FIPS 140-2. В последующих выпусках ожидается расширение ассортимента шаблонов. Контент MITRE ATT&CK в Recon помогает оптимизировать меры вашей организации по обеспечению безопасности и соответствию лучшим практикам.

Масштабирование систем хранения данных

Повышайте эффективность хранения данных с помощью агрегирования событий и сжатия журналов в Recon. ArcSight Recon обеспечивает экономичное хранение данных журнала событий безопасности благодаря впечатляющему коэффициенту сжатия. ArcSight SmartConnectors позволяет агрегировать и фильтровать события для уменьшения использования ресурсов хранения журналов. Независимо от количества развертываемых узлов, ArcSight Recon масштабируется в соответствии с вашими потребностями.

Интеграция в среду информационной безопасности

Разрозненные и неструктурированные системы хранения увеличивают время расследования и ограничивают возможности обнаружения паттернов сложных атак. Получите полное представление о событиях безопасности за счет интеграции и консолидации существующих решений по обеспечению безопасности. ArcSight Recon использует архитектуру Security Open Data Platform (SODP), которая позволяет собирать, нормализовать, агрегировать и обогащать данные из более чем 480 типов источников. В выпуске ArcSight 2020.2 сбор и хранение данных были объединены в унифицированную платформу хранения. Recon позволяет подразделениям информационной безопасности обеспечивать хранение данных в структурированном «озере данных» для проведения расследований. Собирайте и сохраняйте данные один раз, чтобы использовать их сколько угодно. Благодаря этому объединению можно легко

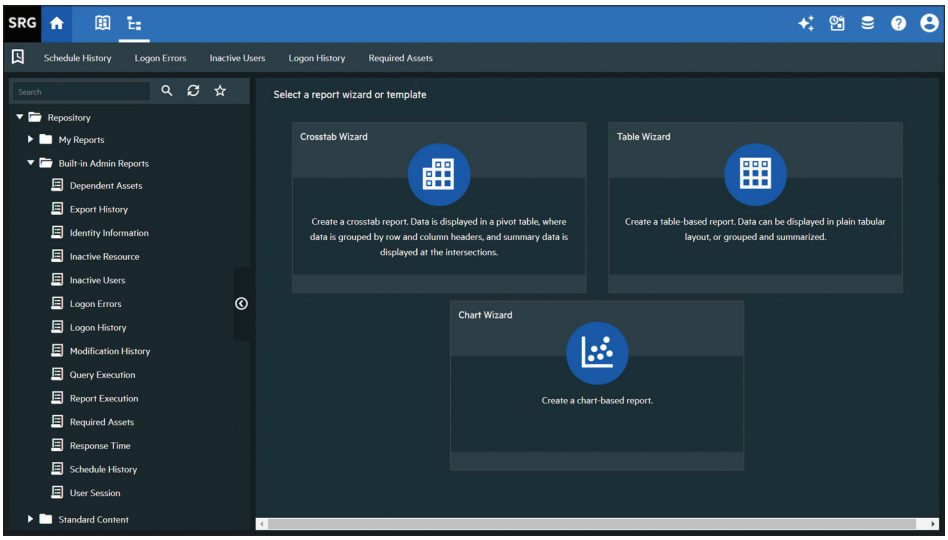

Рис. 3. Создание отчетов

переключаться между ArcSight ESM, ArcSight Interset и ArcSight Recon, нажав всего одну кнопку. Вход в ArcSight с единым идентификатором (с возможностью настройки) экономит время при переключении между продуктами из портфеля ArcSight. Для организаций, использующих несколько решений, Recon также поддерживает интеграцию с ведущими инструментами обеспечения безопасности для обнаружения, и сокращения времени реакции.

Почему именно ArcSight?

Мощная платформа SIEM следующего поколения ArcSight обеспечивает необходимую масштабируемость. Это комплексное решение, разработанное специалистами по безопасности для специалистов по безопасности. Оно использует комплексный подход к интеллектуальным системам безопасности, уникальным образом объединяя сбор больших данных, мониторинг сети, пользователей и конечных устройств, а также обнаружение угроз с помощью передовых технологий аналитики безопасности, включая решения для threat hunting и UEBA. Данное решение предоставляет возможности обнаружения и реагирования на угрозы в реальном времени, автоматизацию и гарантию соответствия нормативным требованиям, а также аналитику ИТ-операций в рамках целостного многоуровневого подхода к аналитике для обеспечения корпоративной безопасности. Несмотря на то, что многие поставщики предлагают надежные решения SIEM, специалистов ArcSight отличает наличие необходимого опыта и знаний, а также лидирующих позиций в отрасли. Решение нового поколения, проверенные методики и 20-летний опыт работы с самыми крупными и сложными SOC в мире делают компанию Micro Focus вашим надежным партнером, который сможет повысить уровень безопасности и эффективности вашей работы.

Подробности на сайте:
www.microfocus.com/en-us/products/arcsight-recon/overview

Контактная информация:
www.microfocus.com

Вам понравился материал? Поделитесь им.