ArcSight для предотвращения атак, ориентированных на пользователей

ArcSight повышает устойчивость к киберугрозам, предоставляя SOC контекстные приоритизированные данные о пользователях вашей компании, которые наиболее подвержены рискам и могут с большей долей вероятности стать целью атаки. Благодаря целостному решению SecOps ваши специалисты смогут эффективно обнаруживать и отслеживать уязвимые учетные записи и выявлять угрозы, ориентированные на пользователей.

Краткий обзор решения ArcSight для предотвращения атак, ориентированных на пользователей:

Чем ArcSight отличается от других решений?

- **Многоуровневая аналитика:**
  ArcSight предоставляет комплексную контекстную аналитическую информацию о пользователях с помощью корреляции событий в режиме реального времени, сбора информации об угрозах, поведенческого анализа, обнаружения аномалий, расширенного выявления угроз и сведений MITRE ATT&CK.
- **Оценка рисков:**
  ArcSight использует математические модели для обнаружения пользователей вашей организации, находящихся в зоне наибольшего риска, и эффективной приоритизации угроз, ускоряя процесс их отслеживания.
- **Постоянная проверка поведенческих моделей:**
  Возможности неконтролируемого машинного обучения позволяют определить уникальные поведенческие модели каждого пользователя и непрерывно обучаются, чтобы выявлять наиболее уязвимых пользователей, находящихся в зоне наибольшего риска.

Трудноуловимые угрозы, ориентированные на пользователя

Атаки, ориентированные на пользователей, рассчитаны на небрежность или связаны с использованием вредоносного ПО и могут нанести серьезный ущерб. Они могут быть сложными для обнаружения в какой-либо организации, поскольку поведенческие модели каждого пользователя уникальны, в значительной степени зависят от ситуации и редко следуют традиционным шаблонам. Поскольку индикаторы этих угроз трудноуловимы, особую важность имеет способность SOC распознавать приоритеты и масштабы атак, ориентированных на пользователей, для их эффективного предотвращения. Тем не менее вашим специалистам, скорее всего, приходится сталкиваться с проблемами отсутствия контекстной аналитической информации, наличия большого объема необработанных данных о событиях и ложных срабатываний, которые отвлекают внимание от наиболее серьезных угроз. Кроме того, отсутствие мониторинга и контроля над привилегированными учетными записями и доступом пользователей означает, что в вашей инфраструктуре появляются более уязвимые точки доступа для злоумышленников. Существование привилегированных учетных записей в компании осложняет выявление и устранение уязвимостей. Как правильно защитить свою компанию от угроз, ориентированных на пользователей? Вам необходим эффективный, продуманный и точный инструмент SecOps с ориентацией на поведенческий аспект.

ArcSight для предотвращения атак, ориентированных на пользователей

Для борьбы с атаками, ориентированными на пользователей компании, ArcSight позволяет SOC идентифицировать пользователей, находящихся в зоне наибольшего риска, с помощью корреляции событий в режиме реального времени и возможностей неконтролируемого машинного обучения. Благодаря расширенному поведенческому анализу, позволяющему составить список из миллиардов приоритизированных событий ваш центр SOC может сосредоточиться на трудноуловимых, ориентированных на пользователей атаках для предотвращения ущерба. Интуитивно понятный и унифицированный интерфейс ArcSight обеспечивает более быстрый отклик и целостное представление о безопасности на единой

> «ArcSight дополнила свой мощный механизм корреляций расширенной аналитикой [ArcSight Intelligence] для обеспечения выявления инсайдерских РИСКОВ и угроз, которые уникальны для каждой компании».
>
> **ОБЗОР GARTNER PEER INSIGHT REVIEW, 2020 Г.**

Контактная информация:
www.microfocus.com

Вам понравился материал?
Поделитесь им.

панели. С помощью ArcSight ваше подразделение безопасности сможет сузить поиск угроз до уровня отдельных сотрудников или групп, повышая устойчивость к киберугрозам и снижая количество атак, ориентированных на пользователей.

Почему именно ArcSight?

ArcSight — это целостное решение SecOps, обеспечивающее надежность SOC. С помощью ArcSight ваша организация сможет адаптировать свою систему безопасности, чтобы обнаружить и установить приоритеты для потенциально уязвимых пользователей, которые наиболее подвержены атакам. Благодаря мониторингу поведения пользователей с помощью многоуровневой аналитики ваши специалисты смогут эффективно и точно снизить риски и потери, связанные с атаками, ориентированными на пользователей.

Возможности и преимущества

Обнаружение неизвестных угроз. Угрозы, ориентированные на пользователей, крайне трудноуловимы и редко следуют традиционным шаблонам. ArcSight сочетает в себе возможности контролируемого и неконтролируемого машинного обучения для целостного анализа потенциально уязвимых пользователей, что позволяет точно и быстро выявлять неизвестные угрозы.

Контекстная информация о пользователях. Для обнаружения угроз, ориентированных на пользователей, подразделение безопасности должно точно отслеживать действия пользователей и определять, какие действия и лица представляют наибольший риск. Расширенные возможности поведенческого анализа ArcSight предоставят вашим специалистам SOC необходимый контекст потенциально рискованного поведения пользователей для ускорения поиска атак.

Централизованный пользовательский интерфейс. При использовании разрозненных инструментов специалистам доступно лишь ограниченное представление состояния безопасности, что препятствует обнаружению трудноуловимых угроз. ArcSight имеет централизованный интерфейс с единой панелью для сотрудников SOC. Это целостное представление позволяет выявлять трудноуловимые угрозы, ориентированные на пользователя, в различных отделах организации.

Оценка рисков. Тщательное наблюдение за действиями отдельных сотрудников организации ведет к чрезмерной нагрузке для аналитиков, так как обычно это приводит к бесконечному потоку оповещений, длинным спискам потенциальных угроз и множеству ложных срабатываний. ArcSight предоставляет специалистам SOC уникальную оценку рисков для каждого пользователя и объекта в вашей организации, позволяя аналитикам выбрать правильный пользовательский контекст и снизить вероятность ложного срабатывания.

Приоритетные потенциальные угрозы. Ваши аналитики, скорее всего, тратят много времени на просмотр сотен оповещений и сообщений о потенциальных угрозах, тем самым увеличивая время реагирования. ArcSight предоставляет вашему SOC приоритетный список потенциальных угроз, основанный на оценке индивидуальных рисков, позволяя аналитикам сосредоточиться на наиболее серьезных и важных угрозах, ориентированных на пользователей.

Security Orchestration and Automated Response (SOAR). Встроенная функция SOAR в рамках ArcSight помогает автоматизировать повторяющиеся задачи и быстрее реагировать на угрозы. С помощью SOAR ваша команда сможет более эффективно распределять время на устранение критических угроз, ориентированных на пользователей, и автоматизировать процесс реагирования для их устранения.

Более 400 моделей. В отличие от многих других решений поведенческого анализа, ArcSight использует более 400 математических моделей для точного определения рискованного поведения, скрытого в вашей организации. Благодаря такой поведенческой аналитике ваши специалисты смогут эффективно и точно определять угрозы, ориентированные на пользователей.

Непрерывное обучение. ArcSight использует непрерывное неконтролируемое машинное обучение для получения актуальной информации xal, чтобы быстрее выявлять актуальные угрозы, ориентированные на пользователей. Благодаря непрерывному обучению моделей ваши аналитики смогут определить приоритет потенциальных угроз и сосредоточиться на выявлении критических угроз для пользователей.

Унифицированный анализ угроз. Ваша организация, скорее всего, сталкивается с огромным объемом данных, который аналитикам необходимо обрабатывать для выявления угроз, и это оборачивается тратой драгоценного времени. ArcSight объединяет различные аналитические функции, чтобы обеспечить SOC более глубоким пониманием текущих угроз и улучшить охват потенциально уязвимых пользователей и учетных записей.

Подробности на сайте:
www.arcsight.com