Буклет с описанием решений

Информационная безопасность

ArcSight для сокращения Длительности инцидентов

ArcSight позволяет повысить киберустойчивость организации, сокращая длительность инцидента ИБ: машинное обучение, автоматизация и реализация многоуровневой аналитики ИБ на единой платформе дают возможность быстрее и эффективнее выявлять угрозы и реагировать на них.

Обзор решения ArcSight для сокращения длительности инцидентов:

Чем ArcSight отличается от других решений?

- **Несколько инструментов аналитики безопасности:**

  Комплексная платформа ArcSight обеспечивает корреляцию событий в реальном времени, сбор информации об угрозах, поведенческий анализ и быстрое расширенное выявление как известных, так и неизвестных угроз.

- **Многоуровневая аналитика:**

  ArcSight объединяет контекстную информацию из каждого уровня аналитики в единый пользовательский интерфейс для лучшего понимания общего риска наступления событий информационной безопасности и повышения точности оповещений.

- **Автоматизация:**

  Обеспечивайте эффективное взаимодействие специалистов и оборудования. Машинный анализ и автоматизация выявляют потенциальные угрозы и начинают реагировать на них, сокращая время уязвимости за счет ускорения реагирования.

Уязвимость и риск

Одной из важнейших задач подразделений информационной безопасности является ограничение бизнес-рисков за счет снижения уязвимости компании к взломам и другим угрозам безопасности. Для многих подразделений безопасности это может представлять трудности. Центры SOC борются с большим количеством киберугроз, как с уже известными, которые следуют установленным и формализуемым последовательностям действий, так и с новыми угрозами, которые постоянно видоизменяются. По всему миру внутренние угрозы, APT и другие сложные для обнаружения угрозы постоянно ставят под сомнение возможности SOC в части детектирования. Чем дольше угроза остается необнаруженной, тем более сильный ущерб она может нанести критически важным информационным активам компании.

Использование разрозненных инструментов аналитики безопасности позволит сделать все возможное для выявления угроз, но приведет в конечном итоге к чрезмерной нагрузке для аналитиков из-за бесконечного потока оповещений, множества ложных срабатываний и несогласованности интерфейсов. Это замедляет расследование и реагирование, что дает злоумышленникам еще больше времени для нанесения вреда компании. В конечном итоге специалистам SecOps остается в срочном порядке снижать уязвимость за счет более быстрого и точного обнаружения угроз и реагирования на них.

Снижение времени уязвимости благодаря ArcSight

Комплексная платформа информационной безопасности ArcSight помогает контролировать вероятность реализации киберугроз, позволяя подразделениям информационной безопасности быстро и точно обнаруживать угрозы и реагировать на них. Платформа ArcSight использует многоуровневую аналитику, позволяющую собирать и нормализовать данные информационной безопасности вашей организации по мере их появления, а затем анализировать с помощью нескольких инструментов. Широко известный механизм корреляции событий ArcSight позволяет в реальном времени выявлять угрозы, соответствующие установленным шаблонам атак (известные угрозы). Возможности поведенческой аналитики, основанной на процессах неконтролируемого машинного обучения, позволяют аналитикам выявлять аномальное поведение, потенциальные инсайдерские угрозы и целевые кибератаки. Заблаговременно обнаруживайте трудноуловимые угрозы Инновационное решение для аналитики больших данных,

оптимизированное для работы с событиями информационной безопасности и включающее мощные средства визуализации и обнаружения аномалий, позволяет заблаговременно обнаруживать неизвестные угрозы. Совместное использование этих инструментов обеспечивает комплексное обнаружение как известных, так и неизвестных угроз. Еще большую эффективность обеспечивает сочетание этих инструментов с мощными TI платформами MISP и Anomali.

Но зачем останавливаться на этом? Далее ArcSight централизует информацию каждого из своих аналитических компонентов в интерфейсе многоуровневой аналитики, предоставляя подразделениям информационной безопасности единую панель для визуализации, выявления и анализа контекста наиболее серьезных угроз компании. Более широкий контекст повышает точность оповещений и тем самым значительно снижает нагрузку на специалистов. Встроенная функция SOAR дополнительно сокращает длительность инцидента ИБ, обеспечивая быстрое автоматизированное реагирование на угрозы.

Уменьшите длительность инцидента ИБ с помощью быстрого и точного обнаружения угроз и реагирования на них благодаря единой платформе SecOps. Расширьте возможности вашего центра SOC с помощью информативной визуализации событий безопасности ArcSight, комплексного обнаружения угроз, многоуровневой аналитики и автоматического реагирования.

Почему именно ArcSight?

ArcSight — это комплексное решение SecOps, обеспечивающее надежность SOC и помогающее интеллектуально адаптировать ресурсы для снижения общей уязвимости. С помощью передовых технологий ArcSight вы сможете сократить время обнаружения и реагирования даже в условиях огромного числа инцидентов, наличия узких мест и чрезмерного количества оповещений. Единая платформа ArcSight позволяет направлять ресурсы на наиболее важные задачи за счет более быстрого и точного обнаружения как известных, так и неизвестных угроз с помощью многоуровневой аналитики и ускоренного реагирования благодаря встроенным возможностям SOAR.

Возможности и преимущества

Обнаружение угроз в реальном времени. Ведущий механизм корреляции ArcSight загружает и коррелирует события в реальном времени, что позволяет практически мгновенно обнаруживать и эскалировать известные угрозы.

Поведенческая аналитика. Обнаружение неизвестных угроз и борьба с ними представляет довольно большую сложность. ArcSight определяет уникальные базовые параметры для всех пользователей и объектов компании, чтобы выявлять аномальное и подозрительное поведение. Благодаря точному мониторингу действий и дополнительному контексту угроз можно сократить время обнаружения трудноуловимых угроз и целевых кибератак.

Машинное обучение. Ваш SOC, скорее всего, получает множество оповещений и ложных срабатываний, что приводит к трате ценного времени аналитиков и увеличению времени реагирования. ArcSight сочетает в себе контролируемое машинное обучение от ArcSight Recon и неконтролируемое машинное обучение от ArcSight Intelligence для оптимизации выявления потенциальных угроз в SOC, позволяя специалистам сосредоточиться на наиболее серьезных угрозах.

Поиск угроз на основе больших данных. ArcSight включает в себя аналитику больших данных, оптимизированную для анализа событий информационной безопасности и упрощенную для повседневного использования. Мощные средства визуализации позволяют аналитикам ИБ изучать и заблаговременно выявлять угрозы в большом объеме данных без необходимости привлечения администратора базы данных.

Интеграция с аналитическими данными об угрозах. Интеграция с каналами аналитических данных об угрозах, такими как MISP и Anomali, помогает поддерживать платформу ArcSight в актуальном состоянии, чтобы выявлять новейшие виды атак в постоянно меняющейся среде (включая атаки нулевого дня).

Централизованный пользовательский интерфейс. Различные компоненты ArcSight имеют общий централизованный интерфейс, который позволяет SOC использовать единую панель без необходимости обновления данных вручную, что экономит время аналитиков.

Контекстная информация об угрозах. Благодаря объединению информации от нескольких аналитических инструментов в единый пользовательский интерфейс многоуровневая аналитика ArcSight может проанализировать результаты и предоставить более широкий спектр контекстуальной информации о каждом оповещении об угрозе и уязвимом пользователе. Это увеличивает точность вашего SOC в определении истинных угроз и ложных срабатываний, позволяя специалистам быстро устранять самые приоритетные и опасные угрозы.

Security Orchestration and Automated Response (SOAR). Встроенные в ArcSight возможности SOAR помогают аналитикам автоматизировать выполнение рутинных задач и быстро реагировать на угрозы. С помощью SOAR вы сможете снизить рабочую нагрузку на специалистов, сэкономив им время и позволив сосредоточиться на более важных действиях по снижению уязвимости.

Единая платформа. Разрозненность решений информационной безопасности приводит к неэффективности и усложняет работу SOC, поскольку аналитикам требуется управлять несколькими хранилищами данных и переключаться между различными инструментами и интерфейсами. ArcSight упрощает процесс обеспечения информационной безопасности, объединяя комплексное решение на единой панели с универсальной платформой данных, общей системой хранения, многоуровневой аналитикой и общим интуитивно понятным интерфейсом.

Приоритетные потенциальные угрозы. Ваши аналитики тратят много времени на просмотр сотен оповещений и сообщений о потенциальных угрозах, тем самым увеличивая время реагирования. ArcSight предоставляет SOC список приоритетных потенциальных угроз, основанный на индивидуальных оценках риска и контекстной информации, чтобы ускорить работу SOC и позволить аналитикам сосредоточиться на самых опасных угрозах.

«Благодаря Micro Focus ArcSight мы не просто обнаруживаем реальные атаки за короткий промежуток времени, но и автоматизируем организацию реагирования на них в режиме, близком к реальному времени. Гибкость ArcSight помогает нам интеллектуально адаптироваться к будущему».

ДМИТРИЙ РЫЖКОВ
Старший аналитик по информационной безопасности
НЭК «Укрэнерго»

Контактная информация:
www.microfocus.com

Вам понравился материал?
Поделитесь им.

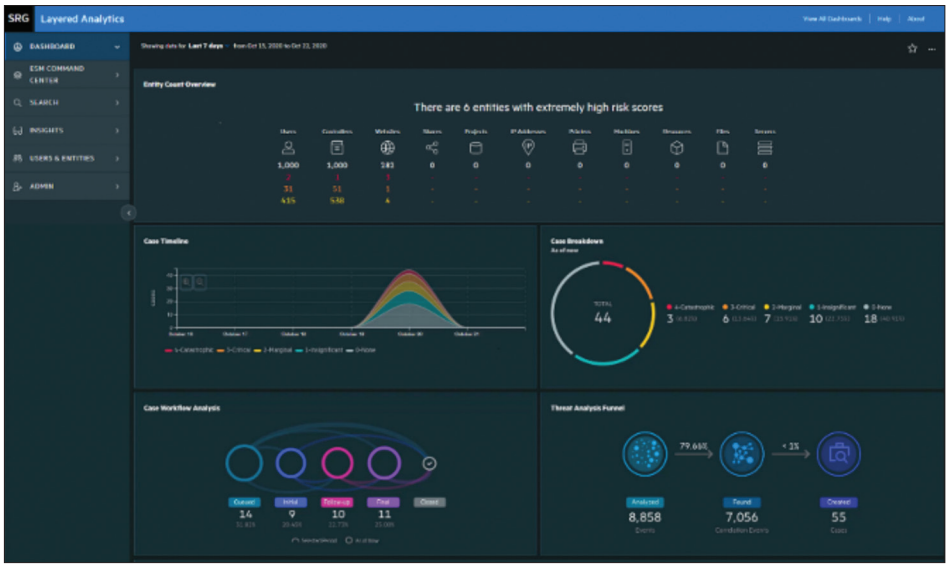

Рис. 1. ArcSight централизует информацию каждого из своих аналитических компонентов через интерфейс многоуровневой аналитики, предоставляя подразделениям информационной безопасности единую панель для визуализации, выявления и анализа контекста наиболее серьезных угроз компании.

Подробности на сайте:
www.microfocus.com/arcsight