5 основных причин для выбора Micro Focus ArcSight

В этом документе приводится 5 основных причин, по которым вашей организации следует выбрать решение Micro Focus ArcSight для построения SOC. ArcSight предоставляет организациям все необходимое для мониторинга событий информационной безопасности, выявления потенциальных угроз и минимизации их воздействия в реальном времени — от корреляции в реальном времени до использования открытых данных об угрозах.

1. **Лучший механизм корреляции.** ArcSight Enterprise Security Manager (ESM) обеспечивает обнаружение угроз и реагирование на них в реальном времени, позволяя выявлять и нейтрализовать их по мере возникновения. В отличие от других решений SIEM, ArcSight может практически мгновенно обрабатывать огромные объемы входящих событий, поскольку это решение создано для обработки данных крупных организаций. ArcSight ESM анализирует данные из различных источников и обеспечивает высочайший уровень корпоративной безопасности. Это решение предлагает широкие возможности кастомизации, позволяя создавать собственные наборы правил для конкретной компании, в соответствии с которыми будет реализовано своевременное реагирование. ArcSight ESM предоставляет возможности по активному противодействию любого уровня сложности, которые могут отрабатывать автоматизированно или по требованию. Кроме того, ArcSight ESM интегрируется с ведущими решениями SOAR и Service Management, такими как ServiceNow, Cortex SOAR, Siemplify, Resilient и ATAR Labs.

2. **Информация об угрозах (Threat Intelligence).** Micro Focus ArcSight обеспечивает безопасность вашей компании с помощью самых современных средств TI. ArcSight ESM поддерживает автоматическую интеграцию с MITRE ATT&CK и MISP CIRCL, а также интеграцию с продуктами таких компаний-партнеров, как Anomali, Ixia и LookingGlass, которые способны предоставить вашей компании самые современные средства обеспечения безопасности. Решения Micro Focus упрощают задачи по оценке общего уровня защищенности организации за счет интеграции методологии MITRE ATT&CK в отчеты и графические панели. Узнайте, как решения ArcSight и Interset от Micro Focus совместно обеспечивают защиту вашей компании, на сайте **mitre.microfocus.com**.

3. **Интеграция UEBA.** Внедрение системы поведенческого анализа действий пользователей и объектов (UEBA) Interset является важным этапом расширения возможностей ArcSight по выявлению угроз. С ее помощью ваша организация сможет получить ценную практическую информацию об аномалиях поведения пользователей в течение первых 30 дней. В отличие от других предложений UEBA, представленных на современном рынке, аналитические возможности Interset реализованы на базе неконтролируемого машинного обучения и продвинутых математических моделей, которые позволяют выявить аномалии еще до того, как будет нанесен ущерб. Этот расширяемый подход в сочетании с интуитивно понятным интерфейсом позволяет вашей организации более точно и эффективно обнаруживать и исследовать угрозы, а также реагировать на них. На основании поступающих событий система выстраивает профиль нормального поведения пользователей вашей компании и мгновенно реагирует на любые аномалии. Interset не требует от пользователя создания сложных правил выявления аномалий, все алгоритмы уже включены в продукт. UEBA позволяет приоритизировать поток поступающих инцидентов за счет данных об аномальности поведения каждого пользователя или актива.

А Вы используете актуальную версию ArcSight? Ниже перечислены некоторые возможности, доступные пользователям последних релизов.

ArcSight ESM

- **Глобальный идентификатор события**
- **Стандартный корреляционный контент**
- **Более тесная интеграция с ServiceNow**
- **Интеграция с MISP CIRCL**
- **Панель управления MITRE ATT&CK**

ArcSight Logger

- **Возможности использования алгоритмов ML**
- **Отчеты по MITRE ATT&CK**
- **Использование Гео-данных**

SODP

- **Поддержка новых источников событий**
- **Развертывание в контейнерах**
- **Расширенная поддержка «облачной» инфраструктуры**

«Благодаря порталу ArcSight Marketplace и методологии Activate мы можем воспользоваться преимуществами наборов стандартного контента (корреляционных правил, отчетов и графических панелей), разработанных специалистами SOC Micro Focus и сообществом ArcSight. Это существенно повысило эффективность работы нашего SOC, а также позволило сократить время выявления угроз.

МАДЖИД БЕХЗАДИ

Исполнительный директор, отдел управления информационной безопасностью группы и проектирования ИТ-инфраструктуры
Kuwait Finance House

Контактная информация:
www.microfocus.com

Вам понравился материал? Поделитесь им.

4. **Открытая, эффективная и масштабируемая платформа данных.** Micro Focus ArcSight использует Security Open Data Platform (SODP) для сбора, упорядочения, обогащения и распространения событий безопасности. Приведение всех собираемых данных к единому формату Common Event Format (CEF) позволяет аналитикам легко и быстро применять их в своей работе. Большое количество поддерживаемых источников событий и наличие партнерских интеграций позволяют легко взаимодействовать с существующей в организации инфраструктурой информационной безопасности. Открытая инфраструктура ArcSight позволяет использовать уже имеющиеся ресурсы, одновременно наслаждаясь всеми преимуществами нормализованных и централизованных данных.

5. **Широкая поддержка сообщества.** Micro Focus ArcSight активно используется тысячами участников сообщества ArcSight. Если у вас возникает какой-либо вопрос, скорее всего вы сможете найти на него ответ в сообществе. Если же ответа пока нет, то наша служба поддержки готова оказать вам необходимую помощь. Кроме того, на портале ArcSight Marketplace доступны сотни приложений и пакетов контента, созданных участниками сообщества и одобренных ArcSight. Вы даже можете создать и монетизировать свои собственные пакеты ArcSight на портале ArcSight Marketplace.

Подробности на сайте:
www.microfocus.com/en-us/products/security-operations/overview

169-RU0056-001 | M | 08/20 | © Компания Micro Focus или один из ее филиалов, 2020 год. Micro Focus и логотип Micro Focus, кроме прочих, являются товарными знаками или зарегистрированными товарными знаками компании Micro Focus или ее филиалов или дочерних компаний в Великобритании, США и других странах. Все прочие товарные знаки являются собственностью соответствующих правообладателей.