LogRhythm

INTELLIGENT IT DISTRIBUTION

Data Sheet

LogRhythm SIEM

Получите непревзойденную видимость, защиту и обнаружение угроз на всех участках поверхности, во всех системах и на всех объектах

Для организаций, которые нуждаются в self-hosted решениях из-за регуляторных требований или ИТ-преимущества, LogRhythm SIEM является самой полной платформой в отрасли, предоставляющей новейшие функциональные возможности и аналитику безопасности. LogRhythm SIEM предлагает встроенные модули, дашборды и правила, которые помогут вам быстро выполнить миссию вашего операционного центра безопасности (SOC): мониторинг угроз, поиск угроз, расследование угроз и реагирование на инциденты при низкой совокупной стоимости владения.

LogRhythm SIEM упрощает расследование инцидентов и реагирование на них благодаря визуальному анализу. Аналитики видят полную историю нарушений безопасности пользователя или хоста, что помогает вашей команде быстро расследовать и реагировать на угрозы. LogRhythm SIEM предоставляет подробную информацию, необходимую для расследования и остановки атак до того, как будет нанесен серьезный ущерб.

LogRhythm поддерживает различные механизмы сбора данных. LogRhythm имеет механизм синтаксического анализа JSON, встроенный в LogRhythm's System Monitor (SysMon), механизм сбора SIEM. Новый механизм, совместимый с LogRhythm версии 7.13, значительно быстрее обрабатывает облачные источники журналов и может собирать тысячи сообщений в секунду. И теперь LogRhythm предлагает неограниченное количество System Monitors, что делает масштабирование простым и без дополнительных затрат.

Преимущества

- **Предотвращение:** Уменьшение риска воздействия киберугроз;
- **Обнаружение:** Устранение слепых зон в вашей среде;
- **Реагирование:** Останавливайте атаки и уменьшайте урон и ущерб;
- **Выберите свой вариант:** Гибкие возможности развертывания.

Нестандартная ценность

LogRhythm SIEM упрощает работу и сокращает среднее время обнаружения (MTTD) и среднее время реагирования (MTTR), позволяя проводить операции безопасности на протяжении всего жизненного цикла угрозы.

- **Сбор данных:** Собирайте, нормализуйте и интерпретируйте данные из более 950 сторонних продуктов и облачных источников.
- **Обнаружение**: Выбирайте из более 1100 готовых наборов правил корреляции и используйте удобный графический интерфейс, чтобы создавать и настраивать правила для вашей среды.
- **Оценка**: Используйте готовую аналитику угроз, каналы Threat Intelligence Service и определение приоритетов на основе рисков, чтобы направить свои усилия.
- **Расследования**: Оптимизируйте и стандартизируйте рабочий процесс ваших аналитиков с помощью кейс-менеджмента, плейбуков и метрик.
- **Нейтрализация**: Выбирайте между полностью автоматизированными действиями согласно сценарию или полуавтоматизированными, основанными на одобрении действиями реагирования, которые позволяют пользователям просматривать их перед применением.
- **Восстановление**: Оптимизируйте процесс комплаенса с помощью нашей Consolidated Compliance Framework, которая обеспечивает отчетность в соответствии с десятками нормативных актов.

Какие проблемы мы решаем

Управление логами

Осуществляйте быстрый поиск в огромном массиве данных вашей организации, чтобы легко находить нужные ответы, выявлять инциденты, связанные с ИТ и безопасностью, а также быстро устранять неисправности.

Аналитика безопасности

Не тратьте время на бессмысленные оповещения. Благодаря усовершенствованной машинной аналитике ваша команда будет точно выявлять злонамеренную активность с помощью контента юзкейсов по безопасности и комплаенсу, а также приоритетных уведомлений на основе рисков, которые мгновенно выявляют критические угрозы.

UEBA

Защититесь от инсайдерских угроз с помощью встроенной детерминированной аналитики поведения пользователей или компаний (UEBA) LogRhythm. Чтобы выявить аномалии с помощью машинного обучения, используйте LogRhythm UEBA, наше усовершенствованное аналитическое решение UEBA.

SOAR

Работайте умнее, а не больше. Объединяйте усилия, оптимизируйте и повышайте уровень безопасности вашей команды с помощью функции оркестровки, автоматизации и реагирования на угрозы (SOAR), которая встроена в LogRhythm SIEM и интегрируется с более чем 80 партнерскими решениями.

Мониторинг конечных точек

Реализуйте сценарии безопасности и соответствия требованиям, дополнив традиционное логирование данными об активности хостов, полученными в результате сбора данных и мониторинга конечных точек.

Как мы помогаем

LogRhythm собрал наиболее квалифицированное и надежное сообщество специалистов и партнеров в мире, чтобы помочь вашей команде построить устойчивую защиту на передовой кибертехнологий.

LogRhythm Labs

Никто не понимает злоумышленников лучше нас. Наша команда LogRhythm Labs проактивно анализирует новые угрозы со всех уголков Интернета и создает правила, дашборды, отчеты и модули комплаенса, чтобы дать вашей организации преимущество.

Зрелость безопасности

Имея двадцатилетний опыт в сфере кибербезопасности, LogRhythm объединяет самые современные технологии, чтобы помочь вам улучшить состояние вашей безопасности. За
с помощью нашей модели Security Operations Maturity Model (SOMM) мы помогаем определить базовые показатели, а затем вместе создаем план для достижения ваших целей в сфере безопасности.

Выбор профессионалов в сфере безопасности

Большинство инструментов кибербезопасности сложны, неуклюжи и неудобны в использовании. LogRhythm SIEM прост в настройке и использовании, позволяя вашим аналитикам видеть весь ландшафт угроз и хронологию событий. Мы помогаем загруженным и малочисленным командам безопасности достигать операционных целей и экономить время.

Службы для поддержки вашей команды

Работая с LogRhythm, вы привлекаете команду экспертов, которые помогут вам в достижении ваших целей в сфере безопасности. Мы предлагаем специализированные услуги, которые помогут вам достичь статуса эксперта и повысить уровень зрелости безопасности вашей организации.

SOC на базе LogRhythm содержит наше SIEM-решение и контент с примерами использования безопасности от LogRhythm Labs, и все это поддерживается реальным опытом нашей команды по работе с клиентами.

E-mail: **sales.ua@iitd.io**

Узнайте больше на **www.iitd.io**

Параметры развертывания

Наши гибкие варианты развертывания гарантируют, что вы получите наилучший вариант для вашей организации - независимо от того, осуществляете ли вы развертывание в центре обработки данных или в облаке.

Программные продукты могут быть предварительно развернуты в центре обработки данных на сервере LogRhythm или на вашем сервере или виртуальной машине с соответствующими характеристиками. Кроме того, наш опыт SIEM также доступен благодаря простоте и гибкости нашего предложения SaaS. Сборщики данных могут быть развернуты как на собственном хосте, так и в облаке.

Какой вариант развертывания подходит именно вам?

Возможности	Self-Hosted SIEM	LogRhythm Cloud SIEM
Управление инфраструктурой	✗	✓
Управление обновлениями ПО	✗	✓
Управление обновлениями базы знаний	✗	✓
База знаний	✓	✓
*Аналитика поведения пользователей и организаций (UEBA)	✓	✓
*Сетевое обнаружение и реагирование (NDR)	✓	Частичнo[1]
Управление объектами, сетью и хостами	✓	✓
Создание правил AI Engine	✓	✓
Доступ к REST API (внутренний)	✓	✓
Интеграция с Active Directory	✓	✗[2]
Единый вход (SSO)	✓	✓
Полная сборка логов	✓	✓
Архивирование данных	✓	✓
Отчетность	✓	✓
кейсменеджмент	✓	✓
Высокая доступность	✓	N/A
Аварийное восстановление	✓	N/A
веб-консоль	✓	✓
Кастомные дашборды	✓	✓
Создание правил механизма обработки сообщений (MPE)	✓	✓
SmartResponse	✓	✓ - от агента
Плейбуки	✓	✓
Службы распределения журналов (LDS)	✓	✗

[1] Интеграция LogRhythm Cloud с автономными сетевыми мониторами для получения PCAP в веб консоли не поддерживается.

[2] Windows Host Wizard и списки на основе групп AD в LogRhythm Cloud требуют доступных обходных путей. Управление пользователями через синхронизацию AD перешло на единый вход в LogRhythm Cloud.

* LogRhythm UEBA и LogRhythm NDR являются дополнительными компонентами к SIEM.

Заказывайте демо уже сегодня!

www.logrhythm.com

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 28019 7185