LogRhythm

INTELLIGENT IT DISTRIBUTION

Data Sheet

LogRhythm SIEM

Отримайте неперевершену видимість, захист і виявлення загроз на всіх ділянках поверхні, в усіх системах і на всіх об'єктах

Для організацій, які потребують self-hosted рішень через регуляторні вимоги або IT-переваги, LogRhythm SIEM є найповнішою платформою в галузі, що надає найновіші функціональні можливості та аналітику безпеки. LogRhythm SIEM пропонує вбудовані модулі, інформаційні панелі та правила, які допоможуть вам швидко виконати місію вашого операційного центру безпеки (SOC): моніторинг загроз, пошук загроз, розслідування загроз та реагування на інциденти при низькій сукупній вартості володіння.

LogRhythm SIEM спрощує розслідування інцидентів та реагування на них завдяки візуальному аналізу. Аналітики бачать повну історію порушень безпеки користувача або хоста, що допомагає вашій команді швидко розслідувати та реагувати на загрози. LogRhythm SIEM надає детальну інформацію, необхідну для розслідування та зупинки атак до того, як буде завдано серйозної шкоди.

LogRhythm підтримує різні механізми збору даних. LogRhythm має механізм синтаксичного аналізу JSON, вбудований в LogRhythm's System Monitor (SysMon), механізм збору SIEM. Новий механізм, сумісний з LogRhythm версії 7.13, значно швидше обробляє хмарні джерела журналів і може збирати тисячі повідомлень в секунду. І тепер LogRhythm пропонує необмежену кількість System Monitors, що робить масштабування простим і без додаткових витрат.

Переваги

- **Запобігання:** Зменшення ризику впливу кіберзагроз;
- **Виявлення:** Усунення сліпих зон у вашому середовищі;
- **Реагування:** Зупиняйте атаки та зменшуйте шкоду і збитки;
- **Оберіть свій варіант:** Гнучкі можливості розгортання.

Out-of-the-box Value

LogRhythm SIEM спрощує роботу і скорочує середній час виявлення (MTTD) і середній час реагування (MTTR), дозволяючи проводити операції безпеки протягом усього життєвого циклу загрози.

- **Збір даних:** Збирайте, нормалізуйте та інтерпретуйте дані з понад 950 сторонніх продуктів і хмарних джерел.
- **Виявлення**: Вибирайте з понад 1100 готових наборів правил кореляції і використовуйте зручний графічний інтерфейс, щоб створювати і налаштовувати правила для вашого середовища.
- **Оцінка**: Використовуйте готову аналітику загроз, канали Threat Intelligence Service та визначення пріоритетів на основі ризиків, щоб скерувати свої зусилля.
- **Розслідування**: Оптимізуйте та стандартизуйте робочий процес ваших аналітиків за допомогою кейс-менеджменту, плейбуків та метрик.
- **Нейтралізація**: Вибирайте між повністю автоматизованими діями згідно зі сценарієм або напівавтоматизованими, заснованими на схваленні діями реагування, які дозволяють користувачам переглядати їх перед застосуванням.
- **Відновлення**: Відновлюйтеся: Оптимізуйте процес комплаєнсу за допомогою нашої Consolidated Compliance Framework, яка забезпечує звітність відповідно до десятків нормативних актів.

Які проблеми ми вирішуємо

Log Management

Здійснюйте швидкий пошук у величезному масиві даних вашої організації, щоб легко знаходити потрібні відповіді, виявляти інциденти, пов'язані з IT та безпекою, а також швидко усувати несправності.

Аналітика безпеки

Не витрачайте час на безглузді сповіщення. Завдяки вдосконаленій машинній аналітиці ваша команда буде точно виявляти зловмисну активність за допомогою контенту юзкейсів з безпеки та комплаєнсу, а також пріоритетних сповіщень на основі ризиків, які миттєво виявляють критичні загрози.

UEBA

Захистіться від інсайдерських загроз за допомогою вбудованої детермінованої аналітики поведінки користувачів або компаній (UEBA) LogRhythm. Щоб виявити аномалії за допомогою машинного навчання, використовуйте LogRhythm UEBA, наше вдосконалене аналітичне рішення UEBA.

SOAR

Працюйте розумніше, а не більше. Об'єднуйте зусилля, оптимізуйте та підвищуйте рівень безпеки вашої команди за допомогою функції оркестрування, автоматизації та реагування на загрози (SOAR), яка вбудована в LogRhythm SIEM та інтегрується з більш ніж 80 партнерськими рішеннями.

Моніторинг кінцевих точок

Реалізуйте сценарії безпеки та відповідності вимогам, доповнивши традиційне логуванння даними про активність хостів, отриманими в результаті збору даних і моніторингу кінцевих точок.

Як ми допомагаємо

LogRhythm зібрав найбільш кваліфіковану і надійну спільноту фахівців і партнерів у світі, щоб допомогти вашій команді побудувати стійкий захист на передовій кібертехнологій.

LogRhythm Labs

Ніхто не розуміє зловмисників краще за нас. Наша команда LogRhythm Labs проактивно аналізує нові загрози з усіх куточків Інтернету та створює правила, дашборди, звіти та модулі комплаєнсу, щоб дати вашій організації перевагу.

Зрілість безпеки

Маючи двадцятирічний досвід у сфері кібербезпеки, LogRhythm об'єднує найсучасніші технології, щоб допомогти вам покращити стан вашої безпеки. За допомогою нашої моделі Security Operations Maturity Model (SOMM) ми допомагаємо визначити базові показники, а потім разом створюємо план для досягнення ваших цілей у сфері безпеки.

Вибір професіоналів у сфері безпеки

Більшість інструментів кібербезпеки складні, незграбні та незручні у використанні. LogRhythm SIEM простий у налаштуванні та використанні, дозволяючи вашим аналітикам бачити весь ландшафт загроз і хронологію подій. Ми допомагаємо завантаженим і малочисельним командам безпеки досягати операційних цілей і економити час.

Служби для підтримки вашої команди

Працюючи з LogRhythm, ви залучаєте команду експертів, які допоможуть вам у досягненні ваших цілей у сфері безпеки. Ми пропонуємо спеціалізовані послуги, які допоможуть вам досягти статусу експерта та підвищити рівень зрілості безпеки вашої організації.

SOC на базі LogRhythm містить наше SIEM-рішення та контент з прикладами використання безпеки від LogRhythm Labs, і все це підтримується реальним досвідом нашої команди по роботі з клієнтами.

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

Дізнайтеся більше на **www.iitd.io**

Параметри розгортання

Наші гнучкі варіанти розгортання гарантують, що ви отримаєте найкращий варіант для вашої організації - незалежно від того, чи здійснюєте ви розгортання в центрі обробки даних або в хмарі.

Програмні продукти можуть бути попередньо розгорнуті в центрі обробки даних на сервері LogRhythm або на вашому сервері чи віртуальній машині з відповідними характеристиками. Крім того, наш досвід SIEM також доступний завдяки простоті та гнучкості нашої пропозиції SaaS. Збирачі даних можуть бути розгорнуті як на власному хості, так і в хмарі.

Який варіант розгортання підходить саме вам?

Можливості	Self-Hosted SIEM	LogRhythm Cloud SIEM
Керування інфраструктурою	✗	✓
Керування оновленнями ПЗ	✗	✓
Керування оновленнями бази знань	✗	✓
База знань	✓	✓
*Аналітика поведінки користувачів та організацій (UEBA)	✓	✓
*Мережеве виявлення та реагування (NDR)	✓	Частковo[1]
Керування об'єктами, мережею та хостами	✓	✓
Створення правил AI Engine	✓	✓
Доступ до REST API (внутрішній)	✓	✓
Інтеграція з Active Directory	✓	✗[2]
Єдиний вхід (SSO)	✓	✓
Повне збирання логів	✓	✓
Архівування даних	✓	✓
Звітність	✓	✓
Кейсменеджмент	✓	✓
Висока доступність	✓	N/A
Аварійне відновлення	✓	N/A
Веб консоль	✓	✓
Кастомні дашборди	✓	✓
Створення правил механізму обробки повідомлень (MPE)	✓	✓
SmartResponse	✓	✓ - від агента
Плейбуки	✓	✓
Log Distribution Services (LDS)	✓	✗

[1] Інтеграція LogRhythm Cloud з автономними мережевими моніторами для отримання PCAP у веб консолі не підтримується.

[2] Windows Host Wizard і списки на основі груп AD у LogRhythm Cloud потребують доступних обхідних шляхів. Керування користувачами через синхронізацію AD перейшло на єдиний вхід у LogRhythm Cloud.

* LogRhythm UEBA і LogRhythm NDR є додатковими компонентами до SIEM.

Замовляйте демо вже сьогодні!

www.logrhythm.com

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185