بسمه تعالی

معرفی و بررسی سامانه LogRhythm

فهرست مطالب

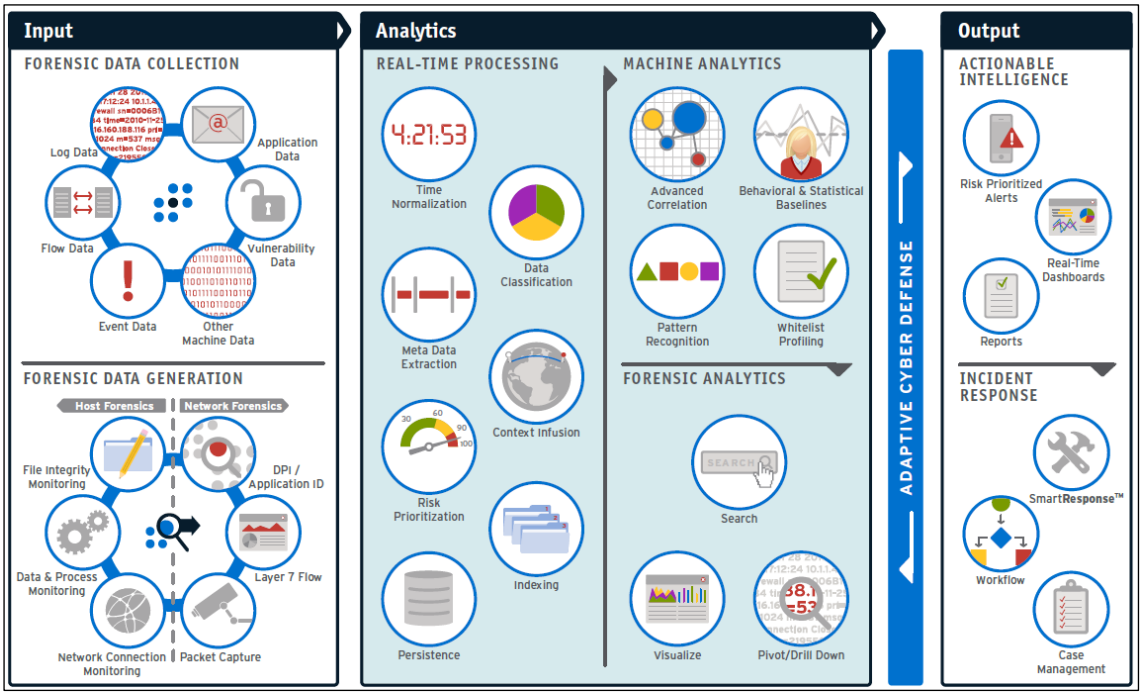
فهرست اشکال

۱ مقدمه

امروزه محافظت در برابر رشد بسیار بالای تهدیدات نیاز به دیدگاه عمیق و گسترده‌ای در سراسر محیط فن آوری اطلاعات دارد. میدان دید عمیق‌تر می‌تواند از طریق پایش و مدیریت متمرکز و یکپارچه‌ی تمامی سرویس ها، برنامه‌های کاربردی و اجزاء شبکه حاصل گردد. در این مستند به بررسی یکی از سیستم‌های مطرح و جدید در این حوزه به نام LogRhythm می‌پردازیم. LogRhythm به تازگی یکی از سیستم‌های پیشرو در حوزه مدیریت رویداد شده است که اغلب می‌توان بر مبنای گزارش‌های گوناگون و مطالب منتشر شده و مورد ادعای شرکت سازنده، به بیان ویژگی‌ها و قابلیت‌های آن پرداخت.

۱-۱ معرفی محصول LogRhythm

ابزار LogRhythm محصول SIEM شرکت LogRhythm می‌باشد که فرآیند مدیریت رویداد و فایل‌های ثبت رویداد، پایش صحت فایل و تحلیل‌های ماشین را با جرم‌یابی شبکه و میزبان ترکیب نموده و چارچوب هوشمندی تهدید یکپارچه‌ای را بوجود آورده است. این محصول به‌منظور جمع‌آوری داده رویداد از نرم‌افزار سازمان شامل کنترل‌های امنیتی شبکه، سیستم‌های عامل و برنامه‌های کاربردی استفاده می‌کند. ابزار SIEM، داده را جهت شناسایی علائم احتمالی فعالیت بدخواهانه تحلیل می‌نماید. بنابراین افراد یا فرآیندهای خودکار می‌توانند از پیشرفت حملات جلوگیری نموده یا به کاهش اثرات سوء و ترمیم موفق سازمان از حملات کمک کنند. چارچوب SIEM در LogRhythm نیز گزارش‌های جزیی و رویدادهای امنیتی را که می‌توانند در جهت مستندسازی تطابق با مقررات امنیتی، قوانین و دیگر نیازمندی‌ها به‌کار روند، تولید می‌نماید. در شکل ۱-۱ بستر کلی هوشمندی تهدید در LogRhythm نشان داده شده است.



شکل ۱-۱: بستر هوشمندی تهدید در LogRhythm

ویژگی‌های کلیدی LogRhythm عبارتند از:

- جمع‌آوری داده چندسکویی[۱] از کلیه منابع ثبت وقایع ازجمله برنامه‌ها و پایگاه داده‌ها
- بایگانی خودکار و بازیابی فایل‌های ثبت وقایع، ساده‌سازی و جست‌وجوی فراگیر
- دسته‌بندی، نرمال‌سازی، یکپارچه‌سازی، و همبسته‌سازی خودکار داده‌های ثبت وقایع
- داده‌کاوی پیشرفته برای تحلیل علت وقوع رویداد
- فیلتر کردن و جست‌وجو، از جمله جرم‌یابی شبکه و میزبان
- پایش بی‌درنگ و هشدارهای مبتنی بر نقش و انعطاف‌پذیر مناسب
- اولویت‌بندی مبتنی بر ریسک
- تولید هشدارهای مبتنی بر نقش
- گزارش‌های انطباق قانونی برای SOX، PCI-DSS، FISMA، GLBA، GPG13 و غیره

[۱] Cross-platform

- تولید گزارش‌های خودکار
- سفارشی کردن گزارش‌های
- جست‌وجوی هوشمند به‌صورت بی‌درنگ
- همبستگی با یک کلیک از هر جست‌وجو
- پیمانه‌ای بودن و قابلیت‌های پایش بی‌درنگ
- آگاهی وضعیتی: فراهم آوردن اطلاعات بی‌درنگ از وضعیت فعلی و تهدید به BES، اطمینان از تشخیص و بازرسی حوادث
- دفاع از شبکه: افزایش متقابل اقدامات امنیتی دیگر، ارائه یک رویکرد دفاع در عمق و تسهیل پاسخ به تهدیدات به سیستم‌های نیروگاهی بزرگ

۲-۱ قابلیت‌های پیشرفته

علاوه بر ارائه ویژگی‌های کلیدی و سنتی SIEM، بستر LogRhythm دامنه‌ای از قابلیت‌های امنیتی پیشرفته را فراهم می‌کند. با توجه به این‌که در ابتدا سازمان قصد دارد تا دقت تشخیص تهدید را در محصول SIEM بهبود دهد، این چارچوب با استفاده از موقعیت جغرافیایی و هوشمندی تهدید از اشتراک‌های مجزا بهره می‌گیرد و سازمان‌ها می‌توانند از یک یا چند قابلیت آن برحسب نیاز خود استفاده نمایند. چارچوب فوق به‌طور گسترده‌ای دارای قابلیت‌های جرم‌یابی و رویدادنگاری نقطه پایانی از جمله پایش و تحلیل رویدادهای میزبان بوده و در برگیرنده پایش رجیستری و فایل، اجرای فرآیند، ترافیک شبکه و وقایع تولید شده توسط کاربر[۱] و همچنین جرم‌یابی شبکه می‌باشد.

LogRhythm در سطح سازمان، مدیریت رویداد، پایش صحت فایل و تحلیل ماشین را با جرم‌یابی شبکه و میزبان ترکیب می‌کند و دیدگاه عمیقی را نسبت به تهدیدات و ریسک‌ها برای سازمان فراهم می‌نماید. بر طبق ادعای شرکت سازنده، LogRhythm امکان پیشگیری از نفوذها پیش از وقوع آن‌ها را می‌دهد و به‌صورتی دقیق دامنه وسیعی از نشانه‌های نفوذ را تشخیص می‌دهد و قادر به پاسخگویی سریع و کاهش نفوذها به سازمان

[۱] User-generated events

می‌باشد. دیدگاه عمیق و درک حاصل شده توسط چارچوب LogRhythm نسبت به سازمان در امن‌سازی شبکه و انطباق با الزامات قوانین و مقررات قدرت می‌دهد.

۱-۲-۱ هوشمندی تهدید

LogRhythm قابلیت‌های جدیدی را با تشخیص، دفاع و پاسخگویی در برابر تهدیدات سایبری و مرتبط با ریسک‌ها ارائه می‌دهد که عبارتند از:

- جرم‌یابی میزبان مستقل و پایش صحت فایل‌ها
- تحلیل پیشرفته ماشین
  - همبستگی پیشرفته و تشخیص الگو
  - تشخیص ناهنجاری رفتار چند بعدی شبکه/میزبان/کاربر
- جست‌وجوی سریع و هوشمند
- تحلیل نمونه داده بزرگ با تحلیل‌های تصویری، جست‌وجوگر[۱]
- جریان کاری توانمند در پاسخگویی خودکار با Smart Response
- مدیریت مورد یکپارچه

تحلیل کلیه داده‌های ماشین و فایل ثبت رویداد و ترکیب آن با دیدگاه عمیق جرم‌یابی در هر دو سطح شبکه و میزبان، میدان دید صحیحی را ارائه می‌دهد. این دیدگاه توسط ماشین AI، یعنی تکنولوژی تحلیل ماشین (هوش مصنوعی)، تحلیل مستمر و خودکاری را از کلیه فعالیت‌های مشاهده شده با محیط فراهم می‌کند. موتور AI به سازمان امکان شناسایی تهدیدها و ریسک‌های کشف نشده پیشین را می‌دهد. معماری یکپارچه، زمان تشخیص تهدیدها را تضمین می‌کند، و مشتریان می‌توانند به سرعت به یک دیدگاه کلی از فعالیت‌ها، توانمندسازی هوشمندی امنیتی استثنایی و پاسخ‌گویی سریع دست یابند. LogRhythm قابلیت‌های مورد نیاز هوشمندی فعال و پاسخ‌گویی سریع را ارائه می‌دهد تا بتوان اغلب تهدیدات سایبری پیچیده امروزی را بررسی نمود.

[۱] Pivot & drill down

۱-۲-۲ ارزش زمان نسبت به هزینه[۱]

مشتریان با وجود معماری یکپارچه LogRhythm و تمرکز بر سهولت استفاده، امکان بهره‌گیری از قابلیت‌های بسیار بالای LogRhythm را دارند و با این وجود می‌توانند هزینه‌های حاصل از نگه‌داری تجهیزات یا TCO[۲] را کنترل نمایند. آزمایشگاه LogRhythm قابلیت‌های حاضر و آماده[۳] ضروری را ارائه می‌دهد که متناسب با پیاده‌سازی مشتریان بوده و آن‌ها را به اهداف تجاری برساند. امکان به‌روزرسانی با آخرین تهدیدات و تحقیقات تطابق به‌صورت خودکار فراهم گردیده و به‌صورت مستمر انجام می‌شود. دانش و به‌کارگیری LogRhythm مشتریان را برای مقابله با تهدیدات، با حفظ سازگاری با نیازمندی‌های دارایی و تطابق، قدرتمند می‌نماید. پایگاه داده آن عبارتند از:

- تجزیه رویداد و قوانین نرمال‌سازی برای بیش از ۶۰۰ سیستم عامل واحد، برنامه‌های کاربردی، پایگاه داده‌ها، تجهیزات و غیره.
  - مجموعه خودکار تطابق با حوزه گسترده‌ای از مقررات (PCI، SOX، HIPAA، FISMA، GLBA، ISO27001، DODI 8500.1، NERCCIP و غیره)
- پیمانه‌های هوشمندی امنیتی
  - پایش کاربر مجاز
  - دفاع برنامه کاربردی وب
  - تشخیص ناهنجاری رفتار شبکه/ میزبان/کاربر

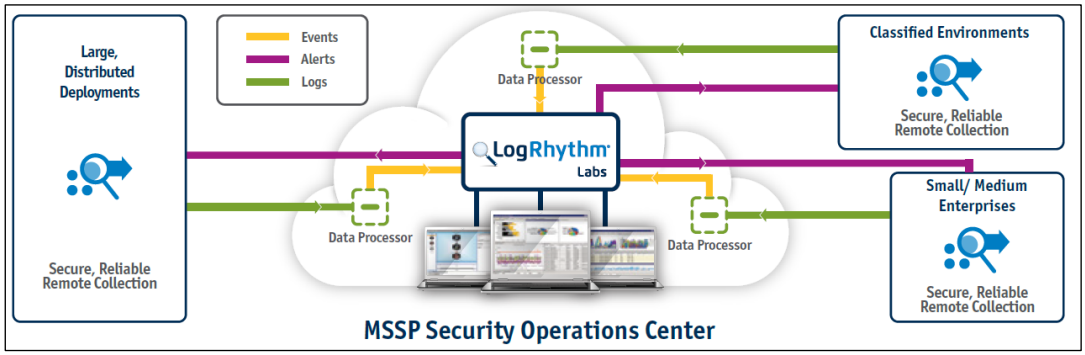
در شکل ۱-۲ نمایی منطقی از آزمایشگاه LogRhythm نشان داده شده است.

---

[۱] Rapid Time-to-Value

[۲] Total Cost of Ownership

[۳] Out of the box



شکل ۱-۲: آزمایشگاه LogRhythm

۲ نتایج بررسی گارتنر

شرکت LogRhythm راه‌حل SIEM خود را برای سازمان‌های بزرگ و متوسط ارائه می‌دهد. این SIEM می‌تواند در یک سری تجهیزات آماده، نرم‌افزار یا قالب‌های فوری مجازی مستقر شده و یک معماری متمرکز مقیاس‌پذیر و لایه‌ای برای پایش شبکه و میزبان فراهم کند. LogRhythm شامل مؤلفه‌های متعددی است که می‌تواند از طریق تجهیزات منفرد یا مجزا به مانند مؤلفه‌های گسسته اجرا گردد که متشکل از جمع‌آورکننده داده[۱]، موتور هوش مصنوعی[۲]، پردازش‌گرهای داده[۳]، شاخص‌گذارهای داده[۴]، مدیر چارچوب[۵] و سرویس‌های گرافیکی می‌باشد. عامل‌های پایش سیستم دردسترس برای ویندوز، چارچوب‌های لینوکس و یونیکس بوده و در دو نوع Pro و Lite قابلیت FIM[۶] را فراهم می‌آورند، اما می‌تواند به‌عنوان ارسال‌کننده رویداد به جمع‌آورکننده داده نیز عمل کنند. شکل ۲-۱ نمایی از مربع جادویی گارتنر را نشان می‌دهد که در سال ۲۰۱۷ منتشر شده است.

---

[۱] Data Collector
[۲] AI Engine
[۳] Data Processors
[۴] Data Indexers
[۵] Platform Manager
[۶] File Integrity Monitoring

شکل ۲-۱: مربع جادویی گارتنر در سال ۲۰۱۷

پایش سیستم و شبکه می‌تواند برای راه‌اندازی و فراهم آوردن قابلیت‌های جرم‌یابی شبکه مانند فرآیند سیستم، صحت فایل و پایش NetFlow، ضبط کامل بسته و DPI تنظیم شوند. این ابزار قابلیت‌های پایش شبکه را با ویژگی‌های UEBA و یک جریان کاری پاسخ‌گویی به حوادث یکپارچه و قابلیت‌های پاسخگویی خودکار ترکیب می‌نماید. پایش‌گر شبکه میدان دیدی از ترافیک برنامه کاربردی و شبکه و همچنین ضبط انتخابی بسته برای اهداف جرم‌یابی فراهم می‌کند.

در سال ۲۰۱۵، دو قابلیت پردازش فایل ثبت رویداد و شاخص‌گذاری SIEM به دو جزء مجزا با افزودن یک محل ذخیره‌سازی براساس Elasticsearch، به‌منظور فراهم آوردن قابلیت‌های جست‌وجوی غیرساخت‌یافته از این ابزار منفک شد. تکثیر کامل داده خوشه‌ای نیز به آن افزوده گردید. دیگر تغییرات شامل بهبود الگوریتم

رتبه‌بندی اولویت بندی مبتنی بر ریسک[۱] (RBP)، تجزیه‌کننده‌های بیشتر برای برنامه‌های کاربردی و پروتکل‌ها جهت پایش شبکه، پشتیبانی برای سرویس‌های ابر مانند AWS، Box و Okta، و یکپارچه‌سازی با راه‌حل‌های کارگزار امنیتی دسترسی به ابر[۲] (CASB) شامل Microsoft's Cloud App Security[۳] و Zscaler می‌شود.

سیستم SIEM می‌تواند به شیوه‌های گوناگونی از جمله نرم‌افزار، یا تجهیزات مجازی و فیزیکی و یا به‌عنوان یک راه‌حل منفرد یا برای مؤلفه‌های گسسته مختلف جهت پشتیبانی از رویکردهای معماری گوناگون پیاده سازی شود.

چارچوب LogRhythm می‌تواند در داخل سازمان در IaaS و مدل‌های اجرای ترکیبی مستقر گردد، همچنین امکان پیاده‌سازی به‌صورت MSSP را نیز فراهم می‌کند. بر طبق گزارش گارتنر در سال 2017، LogRhythm پیشرفت‌های کارآمدی در جهت انواع کارکردها و ویژگی‌ها داشته است که شامل مدیریت حالت[٤]، جریان کاری و پاسخ‌گویی به حوادث امنیتی با ویژگی SmartResponse، تحلیل‌های بهبودیافته پایش، بهبودهای ارائه شده به پایش سیستم[٥] و پایش شبکه[٦] (شامل توسعه نسبت به پایش محیط OT)، بهبودهای قابلیت استفاده برای پایش بی‌درنگ و به‌روزرسانی‌های محتوای ارائه شده با هوش مصنوعی (AI) می‌باشد.

نقاط قوت LogRhythm از دید گارتنر عبارتند از:

- مدیریت فایل ثبت رویداد، گزارش‌گیری، مدیریت رویداد، پایش کاربر مجاز و قابلیت‌های پایش صحت فایل
- استقرار سریع با حداقل پیکربندی‌ها
- برنامه بررسی سلامت فصلی پس از استقرار، خدمات پس از فروش بسیاری را ارائه می‌دهد.

در انتهای تحلیل گارتنر هشدارهایی درباره بکارگیری این سیستم بیان شده است:

- تنها برای داده‌ها و رویدادهای امنیتی مناسب است.

---

[۱] Risk-based prioritization
[۲] Cloud access security broker
[۳] Formerly Adallom
[٤] Case Management
[٥] System Monitor
[٦] Network Monitor

- هیچ پشتیبانی برای یکپارچه‌سازی بهترین کنترل‌های مناسب دسترسی مبتنی بر نقش[1] برای شرکت‌های کوچک و متوسط با امنیت پایه و لوازم قانونی و نیازهای گزارش‌گیری وجود ندارد.
- ممکن است برای استقرارهای محیط‌های خیلی بزرگ، مقیاس‌پذیری مناسبی نداشته باشد.

۳ تحلیل ویژگی‌ها از دیدگاه SANS

موسسه SANS در سال ۲۰۱۷ چارچوب مدیریت چرخه حیات تهدید را در نسخه ۷,۲ از سیستم LogRhythm مورد بررسی قرار داده است. برطبق این گزارش، لایه شاخص‌گذاری Elasticsearch خوشه بندی شده در سیستم، حجم بالایی از رویدادهای امنیتی را که طی وقایع شبیه‌سازی شده نیاز به ترمیم و بررسی دارند، پشتیبانی نموده است. توانایی سیستم LogRhythm در اصل شامل پردازش داده، تحلیل ماشین، جست‌وجوی سریع وجست‌وجو می‌شود که همگی نیاز به سرعت و دقت دارند. به‌عنوان مثال یک نمای آبشاری از رویدادهای ثبت شده و تلفیقی از رویدادهای پیشین از برابر نگاه شما در سیستم SIEM عبور می کند. موردی در این حین نظر شما را جلب می‌کند و تصمیم می‌گیرید اطلاعات بیشتری را درباره آن به‌دست آورید. برای مثال با راست کلیک بر روی آن مشاهده می‌کنید که منابع رویداد تلفیق شده این رویداد کدام هستند. دیگر ویژگی‌های قوی سیستم شامل اتوماسیون امنیت LogRhythm از طریق مدیریت موارد SmartResponse می‌شود.

آخرین چارچوب مدیریت چرخه تهدید شامل بسیاری ویژگی‌های جدید و پیشرفته است که اصولاً همگی بر پایه کاهش زمان پاسخ‌گویی و تشخیص برای تحقیقات و عملیات امنیتی هستند. موتور گردآوری و پرس وجوی داده هم اکنون از Elasticsearch به دلیل قابلیت بالا در لایه پرس‌وجو و شاخص‌گذاری مقیاس‌پذیر استفاده می‌کند. زبان جست‌وجوی بومی و انجام جست‌وجوی متنی از بیشتر مکان‌ها در رابط نیز در دسترس هستند. گزارش فوق بر مقیاس‌پذیری و کارآیی و همچنین سیاست‌های مبتنی بر میزبان و قابلیت‌های پیکربندی تمرکز نموده است که از موارد جدید در این چارچوب هستند. به طور کلی، انتشارات SANS در گزارش فوق بر موارد زیر تاکید دارد:

- سهولت در استفاده

[1] RBAC

- مقیاس‌پذیری و کارآیی از طریق نمونه داده‌های توزیع‌شده و بزرگ
- سیاست‌های مبتنی بر میزبان و قابلیت‌های پیکربندی
- جست‌وجوی سریع، تحلیل و همبستگی حوادث
- ابزارهای مدیریت موارد که می‌توانند به تیم‌های امنیت در انجام عملیات موثر کمک کنند.

٤ معماری سیستم

چارچوب SIEM در LogRhythm در قالب‌های متعددی از جمله بسته همه‌جانبه[1] یا مؤلفه‌های توزیع‌یافته وجود دارد و با تجهیزات مبتنی بر سخت‌افزار، نرم‌افزار مبتنی بر سرویس‌دهنده و تجهیزات مجازی (پشتیبانی شده توسط VMWare ESX، Microsoft Hyper-V و XenServer) در دسترس می‌باشد. سه قالب سخت‌افزار، مجازی و نرم‌افزار سرویس‌دهنده می‌توانند با یکدیگر ترکیب شده و بر حسب نیاز در پیاده‌سازی چارچوب هوشمندی امنیتی منفرد LogRhythm یکپارچه شوند تا حداکثر انعطاف‌پذیری در تحویل اطلاعات با کلیه گزینه‌های همه‌جانبه ایجاد گردد و در نتیجه، حداکثر کارکرد و تجهیزات اختصاص‌یافته برای مقیاس‌پذیری گسترده در محیط‌های بزرگ حاصل شود. معماری توزیع‌یافته و افزایشی در آن امکان مقیاس‌پذیری افقی و عمودی را فراهم آورده است.

٤-١ مؤلفه‌های LogRhythm

مؤلفه‌های اصلی LogRhythm عبارتند از:

٤-١-١ ساختار XM

XM مؤلفه‌های PM، DP، DX و AI را در یک سری تجهیزات همه‌جانبه ترکیب می‌کند. بیشتر استقرارها با یک ابزار XM شروع می‌گردد و در طول زمان به مؤلفه‌های بیشتری جهت افزایش تحمل‌پذیری خطا، ظرفیت و کارآیی توسعه می‌یابند.

[1] All-in-one

۲-۱-٤ سازمان LogRhythm

مدیر چارچوب (PM): مدیر چارچوب، مدیریت و سرپرستی متمرکز هشدارها، اخطارها، مدیریت وضعیت و حوادث امنیتی و APIها، تنظیم خودکار گردش کار و غیره را بر عهده دارد. همچنین داشبوردهای بی‌درنگ، اقدامات SmartResponse و گزارش‌دهی را فراهم می‌کند. در هر راه‌اندازی LogRhythm یک مدیریت چارچوب مجزا وجود دارد.

پردازش‌گر داده (DP): پردازش‌گر داده جمع‌آوری و مدیریت رویداد را انجام می‌دهد. ابزار DP داده جرم‌یابی و ماشین را از جمع‌آورکننده داده، عامل‌های پایش سیستم و پایش‌گرهای شبکه دریافت نموده و سپس پردازش توزیع شده را انجام می‌دهد. DPها از Machine Data Intelligence Fabric برای تبدیل داده به شکل ساختاریافته و متنی استفاده می‌کنند. پردازش‌گرها داده را بایگانی نموده و هر دو رونوشت ساختار یافته و اصلی را به اجزای چارچوبی که عملیات شاخص‌گذاری، تحلیل امنیتی مبتنی بر ماشین و هشداردهی را انجام می‌دهد، توزیع می‌نماید. در واقع پردازش‌گر داده، ابر داده را استخراج نموده و غنی‌سازی آن را انجام می‌دهد و تحلیل‌های مبتنی بر جست‌وجو و ماشین را امکان‌پذیر می‌نماید. پردازش‌گرها به طور افقی و عمودی مقیاس‌پذیر هستند.

شاخص‌گذار داده (DX): شاخص‌گذار داده در پشت صحنه از Elasticsearch جهت ذخیره‌سازی تکثیرهای داده‌های ماشینی و متنی غیرساخت‌یافته، ابرداده ساخت‌یافته به‌منظور فعال نمودن تحلیل‌های مبتنی بر جست‌وجو استفاده می‌کند. تعدد ابزارهای DX از خوشه‌بندی را برای مقیاس‌پذیری بیشتر، کارآیی و دردسترس‌پذیری پشتیبانی می‌کند. شاخص‌گذاری بسیار مقیاس‌پذیر و توزیع شده از ماشین و داده جرم‌یابی را انجام می‌دهد. شاخص‌گذارها، داده خام اصلی و همچنین داده ساختاریافته را ذخیره می‌کنند تا بتواند تحلیل مبتنی بر جست‌وجو و ساختار یافته و غیر ساخت‌یافته را انجام دهد.

موتور AI (AI): موتور هوش مصنوعی یا AIE تحلیل بی‌درنگ و مبتنی بر جریان[۱] از داده‌های جرم‌یابی و متنی انجام می‌دهد و هشدارهای اولویت‌بندی شده براساس ریسک با بهره‌گیری از تکنیک‌های الگوریتمی تولید می‌کند. تجهیزات AIE بسیار مقیاس‌پذیر بوده و تحلیل‌های رفتاری از جمله پروفایل رفتار خودکار،

[۱] Stream-based

آماری و لیست سفید ارائه می‌دهند. موتور AI به‌صورت افقی جهت انجام تحلیل توزیع‌شده در ظرفیت‌های کاری با حجم بالا مقیاس‌پذیر است. با یک رویکرد فراگیر و انعطاف‌پذیر، دیدگاه بی‌درنگی را نسبت به ریسک‌ها، تهدیدات، و مسائل عملیات بحرانی که با روش عملی غیر قابل تشخیص هستند، ارائه می‌دهد. موتور AI این موارد را همبسته می‌کند. گره‌های موتور AI به‌صورت افقی و عمودی با یک مدل مقیاس‌پذیر واحد به‌منظور حفظ تحلیل متمرکز مقیاس‌پذیر هستند.

٤-١-٣ تجهیزات همه‌جانبه

عامل پایش‌گر سیستم[1]: عامل پایش‌گر سیستم نقاط پایانی را برای بررسی صحت فایل، فعالیت کاربر، ارتباطات شبکه و برنامه‌های کاربردی و فرآیندها پایش می‌نماید. این عامل‌ها می‌توانند در سیستم عامل‌های لینوکس، AIX، HP-UX، Solaris و ویندوز نیز پشتیبانی شوند.

پایش‌گر شبکه[2] **(NM)**: پایش‌گر شبکه تحلیل و بازرسی عمیق محتوای ترافیک شبکه را برای شناسایی برنامه کاربردی، استخراج متا داده‌ی قابل جست‌وجو، و ضبط کامل بسته، انجام می‌دهد. پایش‌گر شبکه می‌تواند SmartFlow لایه ۷ را به SIEM و راه‌حل‌های شخص ثالث برای تحقیقات بیشتر ارسال نماید.

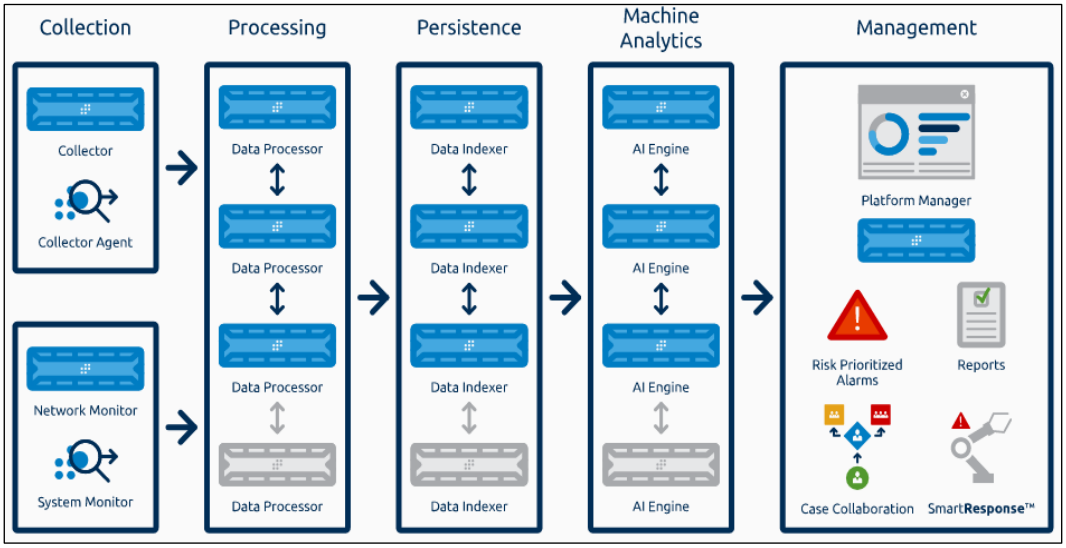
قابلیت‌های آن عبارتند از:

- شناسایی صحیح برنامه کاربردی
- طبقه‌بندی نشست SmartFlow
- تحلیل عمیق بسته
- ضبط کامل بسته
- SmartCapture
- جست‌وجوی غیرساخت‌یافته و سریع
- ساخت مجدد فایل
- داشبوردها و هشدارها
- یکپارچه‌سازی API

[1] System Monitor Agent

[2] Network Monitor

جمع‌آورکننده داده (DC): جمع‌آورکننده داده، داده رویداد، جریان و ماشین را به‌صورت محلی یا از سیستم‌های راه دور جمع‌آوری نموده و آن را برای انتقال امن به بستر چارچوب هوشمندی امنیتی LogRhythm متمرکز، آماده می‌نماید. جمع‌آورکننده‌ها داده را رمز نموده و فشرده کرده، سپس آن را از موقعیت‌های راه دور به DPها منتقل می‌کنند، که این کار یا به‌صورت بی‌درنگ یا به‌صورت دوره‌ای انجام می‌شود. مدل‌های گوناگونی برای این مؤلفه‌ها وجود دارد و برنامه‌های کاربردی وب و آرایه‌های ذخیره‌سازی نیز نسبت به توسعه بیشتر پیاده‌سازی در دسترس هستند. در شکل ٤-١ یک طراحی از چارچوب سیستم هوشمندی تهدید نقطه به نقطه نشان داده شده است.

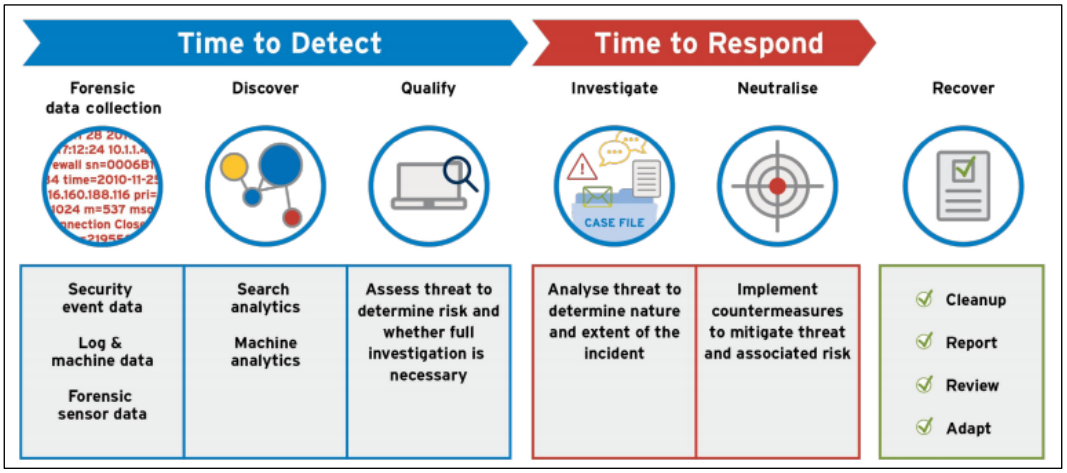


شکل ٤-١: چارچوب سیستم هوشمندی تهدید نقطه به نقطه

٤-٢ چارچوب مدیریت چرخه تهدید[1]

چارچوب مدیریت چرخه تهدید به‌منظور کاهش زمان تشخیص و پاسخ‌گویی، طراحی شده است. مراحل گوناگون این چارچوب شامل جمع‌آوری داده جرم‌یابی، کشف، کنترل، تحقیق، خنثی‌سازی و بازیابی می‌گردد که در شکل ٤-٢ نشان داده شده است.

[1] Threat Lifecycle Management Framework



شکل ٤-٢: چارچوب مدیریت چرخه تهدید

۵ تحلیل قابلیت‌ها

در حقیقت، همان‌گونه که گارتنر تصریح نموده است، یکی از نقاط قوت LogRhythm ترکیب قابلیت‌های SIEM با UEBA، مدیریت حادثه، پایش نقطه پایانی و موارد کاربردی پایش پیشرفته تهدید می‌باشد که در ادامه برخی قابلیت‌های LogRhythm مورد تحلیل قرار می‌گیرند.

۵-۱ جمع‌آوری

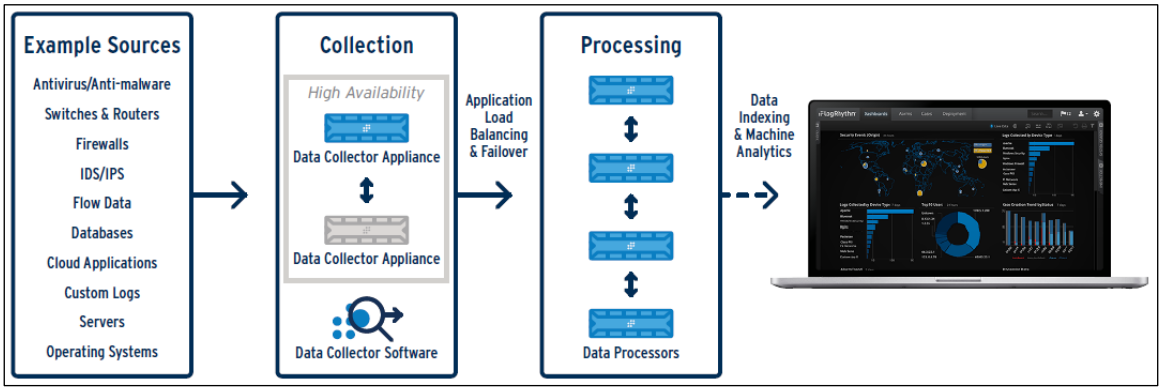
فن‌آوری جمع‌آوری LogRhythm، گردآوری رویدادها، وقایع امنیتی و دیگر داده‌های ماشین را تسهیل می‌کند. جمع‌آورکننده‌های داده می‌توانند به‌صورت محلی یا راه دور عمل کنند و به‌صورت متمرکز پایش و مدیریت شده تا راه‌اندازی و پیاده‌سازی به‌سادگی صورت گیرد. مقیاس‌پذیری در راه‌اندازی با تعادل بار برنامه کاربردی میان پردازش‌گرهای داده بهبود می‌یابد. داده از جمع‌آورکننده‌های داده با ارتباطات TLS احراز هویت و رمزگذاری شده منتقل می‌شود که می‌تواند به‌منظور حداقل نمودن استفاده از پهنای باند فشرده گردد. جمع‌آورکننده‌های داده می‌توانند برای مسیرهای ارتباطی و تک‌سویه شبکه که از محیط‌های طبقه‌بندی شده و اهداف مطابقت با قوانین و مقررات پشتیبانی می‌کنند، پیکربندی شوند. جمع‌آورکننده‌ها صحت داده را طی قطع شبکه با چرخش ترافیک فرار UDP و پیگیری وضعیت برای داده غیر فرار به‌صورت هوشمند تضمین می‌کنند.

۵-۱-۱ ابزار جمع‌آورکننده داده

جمع‌آوری با کارآیی بالا و راه دور از کلیه داده‌های ماشین از جمله پیام‌های رویداد، داده‌های برنامه کاربردی، وقایع امنیتی و جریان شبکه را فراهم می‌کند. یک ابزار جمع‌آورکننده منفرد می‌تواند تا ۱۰۰۰۰ پیام در ثانیه را از هزاران دستگاه جمع‌آوری نموده و انتقال دهد.

۵-۱-۲ نرم‌افزار جمع‌آورکننده داده

در جمع‌آوری محلی مبتنی بر عامل، پایش‌گر سیستم و نرم‌افزاری وجود دارد که مشابه یک پایش‌گر نقطه پایانی نیز عمل می‌کند. پایش‌گر سیستم می‌تواند بر روی سرویس‌دهنده‌ها و ماشین‌های مجازی قابل اجرا در ویندوز، لینوکس یا یونیکس نصب شود. این پایش‌گر، فایل‌های ثبت رویداد و داده ماشین را از محیط‌های راه دور و زیرساخت ابری جمع‌آوری و یکپارچه می‌کند. یک عامل منفرد به‌عنوان یک جمع‌آورکننده می‌تواند هزاران پیام را در ثانیه از ده‌ها دستگاه جمع‌آوری نماید.



شکل ۵-۱: ساختار جمع‌آوری داده

۵-۱-۳ جمع‌آوری عمومی

جمع‌آورکننده‌های داده با تجهیزات و قالب‌های بی‌شماری شامل منابع سفارشی فایل ثبت وقایع سازگار هستند که متدهای زیر را پشتیبانی می‌کنند:

- UDP/TCP و syslog امن (syslog-ng)
- SNMP
- داده جریان (از جمله IPFIX، NetFlow، J-Flow، SmartFlow)
- مبدل فایل ثبت رویداد پایگاه داده عمومی LogRhythm برای سیستم و فایل‌های ثبت رویداد سفارشی به جداول پایگاه داده (از جمله Oracle، SQL Server، MySQL) تحت پروتکل‌های ODBC و JDBC

- فایل‌های ثبت رویداد وقایع ویندوز (شامل فایل‌های ثبت رویداد سفارشی)
- فایل‌های مسطح (تک خطی و چندخطی، فشرده و غیرفشرده)
- APIهای اختصاصی فروشنده (منابعی از جمله):
  - AS/400 و iSeries
  - Checkpoint OPSEC/LEA
  - Cisco SDEE
  - Sourcefire eStreamer
- پویش‌گر آسیب‌پذیری (منابعی از جمله):
  - Qualys
  - Rapid7
  - Tenable Security Center
- راه‌حل‌های Cloud/SaaS (منابعی از جمله):
  - Amazon AWS
  - Box
  - Cradlepoint
  - Office 365
  - Salesforce

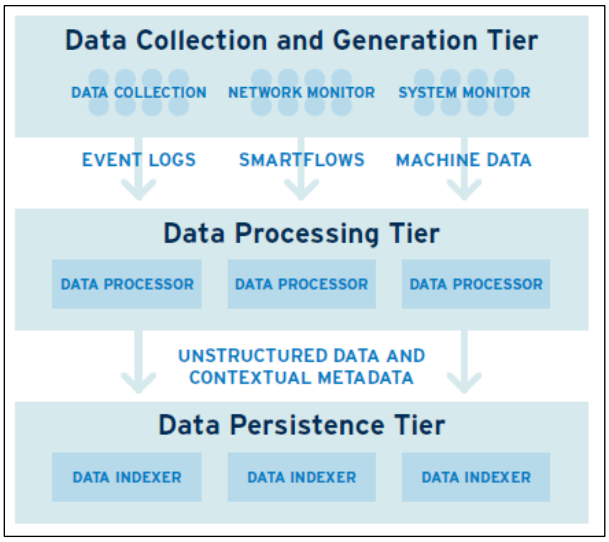
۵-۲ پایش صحت فایل

در سازمانی که نیاز به حفاظت از داده‌های بحرانی خود دارد، بایستی راهی برای پایش مستمر کلیه فایل‌ها وجود داشته باشد تا بتواند فایل‌های مرتبط با بدافزار، تغییرات فایل، دسترسی نادرست به فایل‌های پیکربندی یا سرقت داده حساس را بررسی نماید. هرگاه موارد گفته شده پیش آید بایستی صحت فایل‌های نقض شده مورد بررسی قرار گیرد. انواع فایل‌ها شامل فایل‌های اجرایی، فایل‌های پیکربندی، فایل‌های محتوا، فایل‌های ممیزی و رویداد، فایل‌های وب، سیستم‌های point-of-sale می‌باشند. هنگامی‌که هرگونه جزئیات در رابطه با آن‌چه که کاربر مشاهده نموده، تغییر یابد یا حذف گردد بایستی به‌صورت بی‌درنگ مورد بررسی قرار گیرند.

۵-۳ شاخص‌گذاری و پردازش داده

معماری LogRhythm چالش‌های مدیریت داده بزرگ را با برطرف نمودن نیازمندی‌های کارکرد، مقیاس‌پذیری و مسئولیت‌پذیری بزرگترین و پیچیده‌ترین محیط‌های عملیات امنیت و IT بر طرف می‌نماید. این معماری براساس لایه‌های پردازش و شاخص‌گذاری داده ساخته‌شده است که می‌تواند چندین پتابایت از داده ماشین را در سرعت بالا در محدوده وسیعی از منابع داده پردازش نماید. این لایه‌ها تحلیل‌های امنیتی خودکار ماشین و جست‌وجو با کارکرد بالا را بر روی حجم بسیاری از داده‌های جمع‌آوری شده از سراسر محیط پشتیبانی

می‌کنند. این معماری لایه‌ای، هزینه‌های عملیاتی و سرمایه را با فعال نمودن مقیاس مستقل لایه‌های پردازش و شاخص‌گذاری نیز کاهش می‌دهد. در شکل ۵-۲ نمایی از این معماری نشان داده شده است.



شکل ۵-۲: شاخص‌گذاری و پردازش داده

۵-۳-۱ لایه پردازش داده

پردازش‌گرهای داده، داده ماشین غیرساخت یافته را از لایه جمع‌آوری دریافت نموده و آن را به قالب متنی که از تحلیل در چندین پتابایت سازگار از داده ماشین ناهمگن پشتیبانی می‌کند، تبدیل می‌نماید. پردازش‌گرهای داده، داده متفرقه را از محصولات و تولیدات متفاوت بسیار طبقه‌بندی و نرمال‌سازی می‌کنند که یک Fabric هوشمند داده ماشین سازگار برای هر دو نوع تحلیل مبتنی بر ماشین و جست‌وجو را ایجاد می‌کنند. MDI Fabric یک مجموعه بزرگ از فیلدهای ابرداده را شامل می‌شود و دربرگیرنده عواملی مانند بحران رویداد، میزبان متأثر از حمله و میزبان منبع می‌باشد. داده جمع‌آوری شده به‌صورت امن به پردازش‌گر داده ارسال می گردد، در مکانی که آن به‌صورت ابرداده متنی نرمال و تجزیه شده است، به هر دو ماشین AI برای تحلیل امنیتی خودکار ماشین و شاخص‌گذار داده جهت فعال نمودن جست‌وجوی متنی و غیرساخت‌یافته، ارسال می‌گردد. یک رونوشت از هر پیام خام نیز برای بایگانی ارسال می‌شود. در صورت لزوم، پیام‌های بایگانی شده می‌توانند فراخوانی شده و مجدداً پردازش شوند، سپس به لایه شاخص‌گذاری شده برای تحلیل بیشتر جرم‌یابی افزوده گردند.

۵-۳-۲ Machine Data Intelligence Fabric [۱]

MDI Fabric فراهم‌کننده هوشمندی امنیتی و تحلیل در چارچوب با درک سازگار از فایل ثبت رویداد و داده ماشین پردازش شده از کلیه برنامه‌های کاربردی و تجهیزات می‌باشد. این مورد تحلیل‌های امنیتی پایین دست، جست‌وجوهای جرم‌یابی، داشبوردها، گزارش‌ها و پیمانه‌های خودکارسازی تطابق را ایجاد می‌نماید. MDI Fabric مجهز به یک کتابخانه از قوانین پردازش است که داده ماشین را از منبع، تجزیه نموده، نرمال می‌کند و سپس ابرداده‌ای به‌صورت اختصاصی جهت فعال نمودن تحلیل‌های امنیتی تولید می‌کند. LogRhythm این ابر داده را با اطلاعات متنی حیاتی از جمله طبقه‌بندی رویداد، اولویت‌بندی مبتنی بر ریسک و موقعیت جغرافیایی غنی می‌سازد. TrueTime نشان زمان را با حذف اختلاف‌ها از مناطق زمانی، ساعت‌های داخلی و زمان جمع‌آوری و پذیرش نرمال می‌کند که امکان دنباله مبتنی بر الگوریتم‌های تحلیل امنیتی را فراهم می‌کند.

۵-۳-۳ انتقال امن، آماده ممیزی

جمع‌آوری امن و تحویل داده خام در لایه جمع‌آوری تضمین می‌شود که یک زنجیره تأمین دیجیتالی را ایجاد می‌کند. هر فایل بایگانی جهت تأمین تأیید اعتبار برای اهداف قانونی و ممیزی، به‌صورت دیجیتالی، امضا شده است. فایل‌های بایگانی براساس زمان سازمان‌دهی می‌شوند و خود، توصیفی را ارائه می‌دهند که آن را برای انتقال فایل‌ها به محل ذخیره‌سازی ثانویه آسان می‌سازد.

۵-۴ تحلیل‌های تهدید پایه

مجموعه تحلیل‌های هسته برای تهدید به سازمان‌ها جهت غلبه بر انواع تهدیدات سایبری کمک می‌کند و امکان تحلیل‌های حیاتی رفتاری کاربر، نقطه پایانی و فعالیت‌های شبکه برای حفاظت سریع از بردارهای حمله رایج را فراهم می‌کند. این سیستم به‌منظور کار با انواع داده‌های رویداد که در بیشتر محیط‌ها موجود هستند طراحی شده است که عبارتند از:

- Directory/LDAP
- آنتی ویروس و ضد بدافزار
- دیواره آتش

---

[۱] MDI Fabric

- میزبان
- IDS/IPS
- VPN
- داده جریان شبکه

تحلیل‌های هسته توسط موتور AI فراهم گردیده و جمع‌آوری بسیاری از قوانین طراحی شده خودکار تحلیل‌های ماشین را برای عمل با پیکربندی یا تنظیم[۱] حداقل به‌کار گرفته است و از تکنیک‌های مختلفی شامل همبسته‌سازی پیشرفته، تشخیص الگو، لیست سیاه و سفید و تحلیل آماری استفاده می‌کند. این مجموعه همراه با یک راهنما ارائه شده است که شامل توصیه‌نامه برای دستورالعمل‌های نصب و تنظیم است.

۵-٤-۱ تحلیل تهدید نقطه پایانی

پیمانه تحلیل تهدید پیشرفته، فایل‌های ثبت وقایع موجود در میزبان و داده جمع‌آوری شده از پایش‌گرهای سیستم LogRhythm را با استفاده از جمع‌آوری قوانین تحلیل‌های رفتاری پیشرفته برای موتور AI تحلیل می‌کند که تهدیدات نقاط پایانی سازمان را تشخیص، اولویت‌بندی و خنثی می‌کنند. علاوه بر تشخیص بدافزار و رفتار بدخواه مرتبط با حملات روز صفرم، قادر به یافتن حساب‌های کاربری غیرمجاز و تغییرات نسبت به امتیازات ارائه شده از استفاده نادرست حساب‌های کاربری و مصالحه نقطه پایانی[۲] می‌باشد. این پیمانه با راهنمایی درباره نحوه پیاده‌سازی با دستورالعمل‌های نصب و تنظیم ارائه می‌شود.

۵-۵ برنامه کاربردی UEBA

تحلیل‌های رفتار هویت و کاربر[۳] (UEBA) هر دو گونه از تهدیدات شناخته شده و شناخته نشده مبتنی بر کاربر را تشخیص داده و خنثی می‌کنند. آن داده‌های متنوع مصرف شده توسط LogRhythm جهت افشای تهدیدات داخلی، حساب‌های آسیب‌دیده و سوءاستفاده مجاز را در زمان واقعی تحلیل می‌نماید.

UEBA در چارچوب LogRhythm تعبیه شده است و کاربر را از صرف هزینه تکثیر داده و اداره سیستم‌های دوگانه بی‌نیاز می‌کند. این راه‌حل امکان مدیریت چرخه تهدید نقطه به نقطه را با قابلیت‌های زیر فراهم می‌کند:

---

[۱] Tuning

[۲] Endpoint compromise

[۳] User and Entity Behavior Analytics

- موتور AI با یادگیری ماشین، پروفایل رفتاری، تحلیل گروه همکار و دیگر تکنولوژی‌ها را استفاده می‌کند.
- جست‌وجوی متنی و غیرساخت‌یافته، امکان بررسی سریع جرم‌یابی را فراهم می‌کند.
- استنتاج شناسایی از احراز هویت، دسترسی، DHCP و دیگر داده‌ها به‌منظور شناسایی خودکار کاربر استفاده می‌کند.
- خودکارسازی و سازمان‌دهی پاسخ‌های امنیتی را (تاحدودی) خودکار می‌کند.
- افزونه‌های SmartResponse وظایف دستی را خودکار می‌کنند و امکان اجرای متمرکز اقدامات مقدماتی پیشگیرانه را فراهم می‌کنند.

۵-۶ گزارش‌ها

LogRhythm می‌تواند در حدود ۸۰۰ گزارش از پیش تعریف شده با هزاران قالب اضافی که امکان ارائه گزارش‌های سفارشی را ایجاد می‌کنند، برای موارد کاربردی[۱] امنیت، عملیات و تطابق، تولید نماید. گزارش‌ها می‌توانند برای تحویل یا تولید برحسب تقاضا برنامه‌ریزی شوند. آن‌ها به‌راحتی می‌توانند به داشبوردهای شخصی بی‌درنگ، اخطارهای ایمیل و هشدارها یا ابزارهای صادر شده با قالب‌هایی مانند فایل‌های Excell دسترسی داشته باشند. LogRhythm می‌تواند به‌منظور ارسال هشدارها و گزارش‌های مستقیم به افراد، گروه‌ها، مسیرهای مشترک و یا هر ترکیب دیگری استفاده شود.

[۱] Use Case

شکل ۵-۳: ارسال هشدار در LogRhythm

به‌طور کلی، انواع گزارش‌های تولید می‌تواند به‌صورت گزارش‌های از پیش‌تعریف‌شده، تطابق، و سفارشی‌شده باشد.

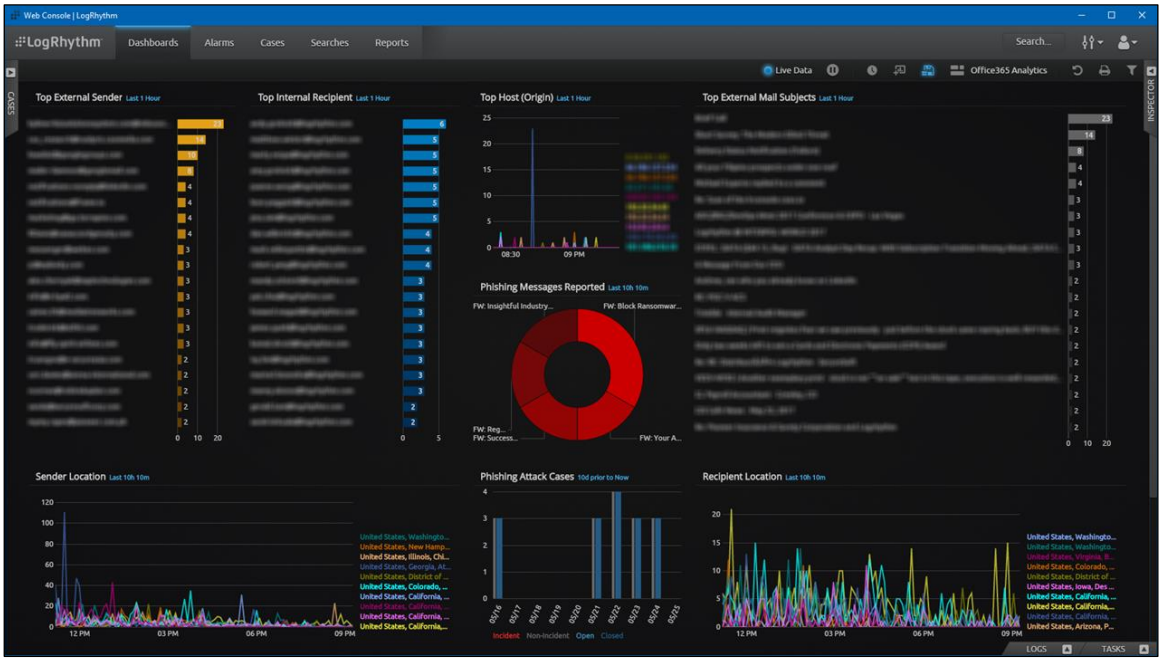
۵-۷ داشبورد

نمونه‌های از داشبوردها در آدرس زیر ارائه شده است که در ادامه به‌صورت اجمالی به معرفی هر یک پرداخته می‌شود.

https://github.com/LogRhythm-Labs/PIE/tree/master/SIEM-Dashboards

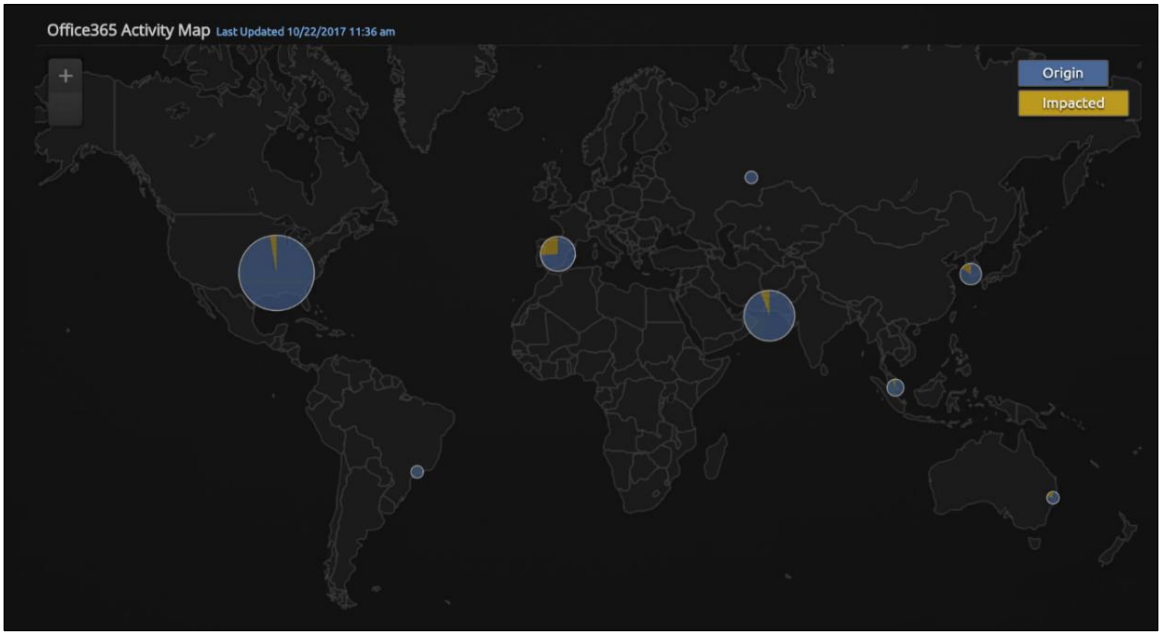
این داشبوردها با سیستم LogRhythm یکپارچه شده و امکان آسان جست‌وجو، همبسته‌سازی و خودکارسازی را فراهم می‌کند.

- **داشبورد تحلیل**: این داشبورد مهمترین داشبورد تحلیلی است که ترافیک پست الکترونیکی داخلی و خارجی، گزارش حملات فیشینگ و معیارهای وضعیت را مشخص می‌نماید.



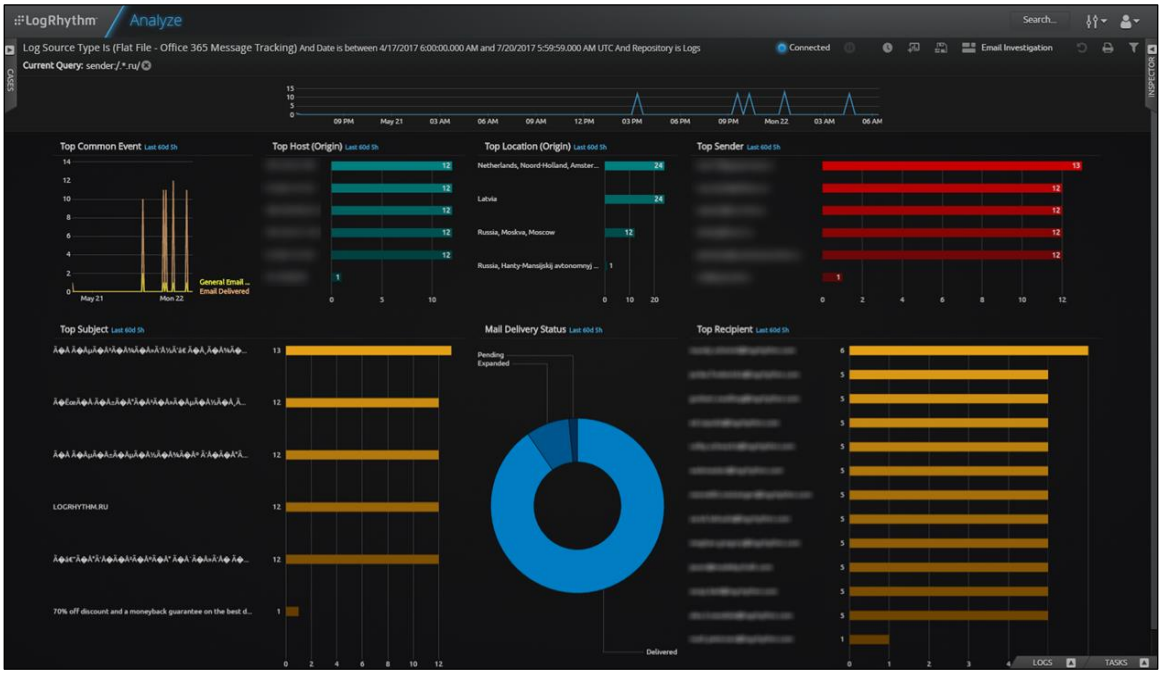
شکل ۵-٤: داشبورد تحلیل

- **داشبورد نقشه تهدید:** همانند داشبورد تحلیل است اما بر محور نقشه تهدید بوده و موقعیت اصلی ترافیک را نشان می‌دهد.



شکل ۵-۵: داشبورد نقشه تهدید

- **داشبورد تحقیق:** داشبورد تحقیق، نتایج را با امکان تحلیل آسان، جست‌وجو و همبسته‌سازی در SIEM پیاده‌سازی می‌نماید.



شکل ۵-۶: داشبورد تحقیق

دو داشبورد نیز به‌صورت نمونه توسط شرکت SecureSense[۱] و دیواره آتش Palo Alto Networks Ignite[۲] ارائه شده است (شکل‌های ۵-۷ و ۵-۸).

[۱] http://securesense.ca/secure-sense-named-2016-logrhythm-partner-year/

[۲] https://logrhythm.com/blog/palo-alto-networks-ignite-2016/

شکل ۵-۷: داشبورد نمونه شرکت SecureSense

شکل ۵-۸: داشبورد نمونه دیواره آتش Palo Alto Networks Ignite