بسمه تعالی

معرفی، آموزش نصب، و پیکربندی سیستم مدیریت اطلاعات و وقایع امنیتی IBM Q1 Radar

(بخش اول)

فهرست مطالب

فهرست اشکال

فهرست جداول

۱ مقدمه

گزارش‌ها و آمارهای منتشرشده در حوزه‌ی امنیت اطلاعات، نشان می‌دهد که نشت اطلاعات حساس، وقوع انواع حملات و تهدیدات و پیچیدگی آنها در حال افزایش بوده و در بیشتر موارد زمان نفوذ به سیستم کمتر از یک دقیقه است، در حالی‌که زمان کشف آن‌ها گاهی تا سال‌ها طول می‌کشد. توجه به این روند، اهمیت پایش را به خوبی نشان می‌دهد. از سوی دیگر، استفاده از تکنولوژی‌های مختلف امنیتی به منظور غلبه بر حملات و تهدیدات مختلف امنیتی و متعلق به تولیدکننده‌های متفاوت، موجب تولید حجم انبوهی از رخدادها با قالب‌های متفاوت می‌شود. استفاده از SIEM و SOC با سابقه‌ای بیش از ۱۵ سال، به عنوان تکنولوژی‌های مؤثر در زمینه تشخیص، پایش پیوسته، مدیریت فایل‌های ثبت وقایع و غیره بسیار کارآمد خواهد بود.

اتخاذ یک راه‌حل SIEM صرفاً یک اقدام اجباری برای پیروی از سیاست‌های انطباق نمی‌باشد بلکه یک گام حیاتی به منظور شناسایی انحرافات امنیتی است و به سرعت به فعالیت‌های مشکوک واکنش نشان می‌دهد. بهره‌گیری از SIEM برای کمک به کسب و کارها در رقابت امنیتی به محافظت از اطلاعات حساس مشتریان در خدمات بهداشتی، بانکداری و مالی، مخابرات، بخش عمومی و سایر صنایع کمک می‌نماید.

از سوی دیگر، امنیت مؤثر نیاز به میدان دید فراگیر نسبت به کلیه فعالیت‌ها در سراسر شبکه دارد اما حجم فراوان اطلاعات می‌تواند منجر به از دست رفتن وقایع حیاتی گردد. به منظور بهبود قابلیت‌های تشخیص، برداشتن گامی فراتر از یک SIEM سنتی و بهره‌گیری از رویکردی هوشمند برای تحلیل‌های امنیتی ضروری است. یکی از تولیدات پراستفاده و مهم در این زمینه، محصول شرکت IBM به عنوان SIEM در چرخه SOC به نام بسترهوشمندی امنیتی IBM QRadar می‌باشد که قابلیت دید بلادرنگی را از سراسر شبکه فراهم می‌نماید و مدتی است که با استقبال روبرو شده است. بستر فوق به سازمان‌ها به منظور راه‌اندازی تشخیص تهدید، پاسخگویی سریع‌تر به حوادث و انجام راحت تحلیل‌های امنیتی کمک می‌نماید. این راه‌حل، داده را از سراسر شبکه جمع‌آوری نموده و وقایع مرتبط را به صورت یک واقعه منفرد و پرمفهوم به منظور حذف هشدارهای غیرضروری و نشان‌دادن سریع‌تر تهدیدات حیاتی همبسته می‌نماید. اکوسیستم تعویض برنامه کاربردی امنیتی

IBM[1] مشتریان را قادر می‌سازد تا به راحتی ارزش بستر خود را در کلیه یکپارچه‌سازی‌ها با راه‌حل‌های مکمل و قابلیت‌های افزونه مانند امنیت شناختی با Watson و تحلیل‌های رفتار کاربر گسترش دهند.

۲ معرفی محصول امنیتی IBM QRadar SIEM

IBM QRadar ناهنجاری‌ها را تشخیص داده، تهدیدات پیشرفته را کشف نموده و رخدادهای نادرست‌های مثبت را حذف می‌نماید. این محصول داده جریان شبکه و رخدادهای وقایع[2] امنیتی را از هزاران تجهیز، نقاط پایانی و نرم‌افزارهای توزیع‌شده در سراسر شبکه تقویت می‌کند. سپس از یک موتور Sense Analytics پیشرفته به منظور نرمال‌سازی و همبسته‌سازی داده‌های آن و شناسایی سازوکارهای دفاعی لازم برای انجام تحقیقات استفاده می‌کند. به عنوان یک گزینه، می‌تواند با هوشمندی تهدید IBM X-Force لیستی از آدرس‌های IP شامل میزبان‌های بدافزار، منابع جعلی و دیگر تهدیدات را ارائه دهد. QRadar SIEM با نسخه‌های داخل سازمان و محیط‌های ابری دردسترس مشتریان قرار می‌گیرد.

۲-۱ ویژگی‌های کلیدی

ویژگی‌های کلیدی QRadar IBM عبارتند از:

- بهبود تشخیص تهدید و تقلب، ادراک[3] و پیگیری حوادث و تهدیدات امنیتی داخلی و پیشرفته‌ی قابل توجه با پشتیبانی داده و محتوا برای تحقیق آسان‌تر، همچنین ایجاد دسترسی دقیق داده و گزارش فعالیت‌های کاربر
- انجام نرمال‌سازی و همبسته‌سازی فوری وقایع
- فراهم‌نمودن میدان دید نزدیک به بی‌درنگ، ضبط رخداد وقایع و داده جریان شبکه در زمان نزدیک به بی‌درنگ و انجام تحلیل‌های پیشرفته جهت آشکار نمودن جرایم امنیتی
- کاهش و اولویت‌بندی هشدارها، تمرکز بر تحقیقات تحلیل امنیتی بر روی یک لیست کوچک و قابل مدیریتی از حوادث با احتمال بالا

---

[1] IBM Security App Exchange

[2] Event log

[3] Sense

- استقرار QRadar SIEM بر روی محیط‌های ابری یا داخل سازمان
- افزودن سریع و ارزان ذخیره‌سازی و پردازش بیشتر
- مدیریت آسان تطابق با سیاست‌های سازمانی داخلی و مقررات خارجی با سفارش گزارش‌ها و قالب‌های قابل سفارش
- فراهم‌سازی اعمال سیاست‌های حفظ حریم خصوصی داده
- فراهم‌سازی مهارت در هوشمندی تهدید از طریق IBM X-Force
- قابلیت همکاری و مدیریت در جلوگیری از تهدید
- یکپارچه‌سازی با صدها محصول IBM و غیر IBM

۲-۱-۱ ادراک و تشخیص تهدیدات تقلب، داخلی و پیشرفته

یک بستر بسیار مقیاس‌پذیر و منفرد به‌منظور کاهش هزاران واقعه امنیتی نسبت به یک لیست مدیریتی از جرایم مشکوک را مستقر می‌نماید. فایل‌های ثبت وقایع و رویدادها را از چند منبع شامل دارایی‌های شبکه، تجهیزات امنیتی، سیستم‌عامل‌ها، برنامه‌های کاربردی، پایگاه‌داده‌ها و شناسایی و محصولات مدیریت دسترسی جمع‌آوری می‌نماید. داده جریان شبکه شامل داده لایه برنامه کاربردی از سوئیچ‌ها و مسیریاب‌ها را بیرون می‌کشد.

۲-۱-۲ انجام نرمال‌سازی و همبسته‌سازی فوری وقایع

تشخیص تهدیدات و گزارش تطابق را با کاهش بیلیون‌ها رویداد و جریان به جرایم عملی و اولویت‌بندی آنها بر طبق تأثیر بر کسب و کار بهبود می‌دهد. حد آستانه فعالیت و تشخیص ناهنجاری را به‌منظور شناسایی تغییرات در رفتار مربوط به برنامه‌های کاربردی، میزبان‌ها، کاربران و مناطق شبکه تعریف می‌کند. از هوشمندی تهدید IBM X-Force (به صورت اختیاری) به منظور شناسایی فعالیت مربوط به آدرس‌های IP مشکوک استفاده می‌کند از جمله آن‌ها که مشکوک به میزبانی بدافزار هستند.

۲-۱-۳ ادراک، پیگیری و پیوند حوادث و تهدیدات قابل توجه

تحقیقات را با انجام تحلیل رویداد و جریان یا با استفاده از جریان نزدیک به بی‌درنگ یا داده‌های تاریخی بهبود داده و آسان می‌نماید. جمع‌آوری‌کننده QFlow و VFlow را برای بینش عمیق و میدان دید نسبت به برنامه‌های کاربردی، پایگاه‌داده‌ها، محصولات همکاری و رسانه‌های اجتماعی از طریق بازرسی عمیق بسته ترافیک لایه ۷ شبکه می‌افزاید.

۲-۱-٤ استقرار QRadar SIEM بر روی محیط‌های ابری و داخل سازمان

وقایع و جریان را از برنامه کاربردی در حال اجرا بر روی هر دو نوع ابر و داخل سازمان جمع‌آوری می‌کند، یا اینکه IBM را مستقر نموده، زیرساخت QRadar را در حین انجام وظایف مدیریت تهدیدات امنیتی نگهداری و مدیریت می‌نماید.

۲-۱-۵ افزودن ارزان و سریع ذخیره‌سازی و پردازش بیشتر

این ویژگی به قابلیت‌های ذخیره‌سازی افزونه گره داده[۱] QRadar را می‌افزاید تا ظرفیت ذخیره‌سازی محلی سازمان را افزایش، کارآیی جستجو را هنگام بازیابی داده از تحقیقات نفوذ و حملات، بهبود، و گلوگاه‌ها را بدون افزایش هزینه اضافی و سربار حذف می‌نماید.

۲-۱-٦ اعمال اجرای سیاست‌های حفظ حریم خصوصی

سیاست‌های حفظ حریم خصوصی، در برگیرنده موتور گزارش‌دهی بصری است که نیازی به مهارت‌های نوشتن گزارش و پایگاه‌داده پیشرفته ندارد. شفافیت، پاسخگویی و اندازه‌گیری جهت رسیدگی به مقررات قانونی و گزارش تطابق را فراهم می‌نماید.

قدرت همکاری و مدیریت پیشگیری از تهدید را افزایش داده و امکان دسترسی به برنامه کاربردی امنیتی IBM را به‌وجود می‌آورد.

۲-۲ مزایا

- استقرار و پیکربندی بسیار آسان
- دیدگاه یکپارچه محیط تهدید با استفاده از داده NetFlow، داده IDS/IPS و فایل ثبت رویداد از محیط
- قابلیت‌های تشخیص ناهنجاری و رفتار برای هر دو داده فایل ثبت وقایع و NetFlow
- مناسب برای شرکت‌های بزرگ، متوسط و کوچک
- معماری دسترس‌پذیر و مقیاس‌پذیری بالا

[۱] Data Node

۲-۳ نقاط ضعف

- قابلیت‌های محدود سفارشی کردن
- پشتیبانی چندگانه محدود[۱]
- قابلیت اجرای محدود[۲]
- توسعه و تحلیل موارد کاربردی پیشرفته[۳]

۳ نتایج بررسی گارتنر

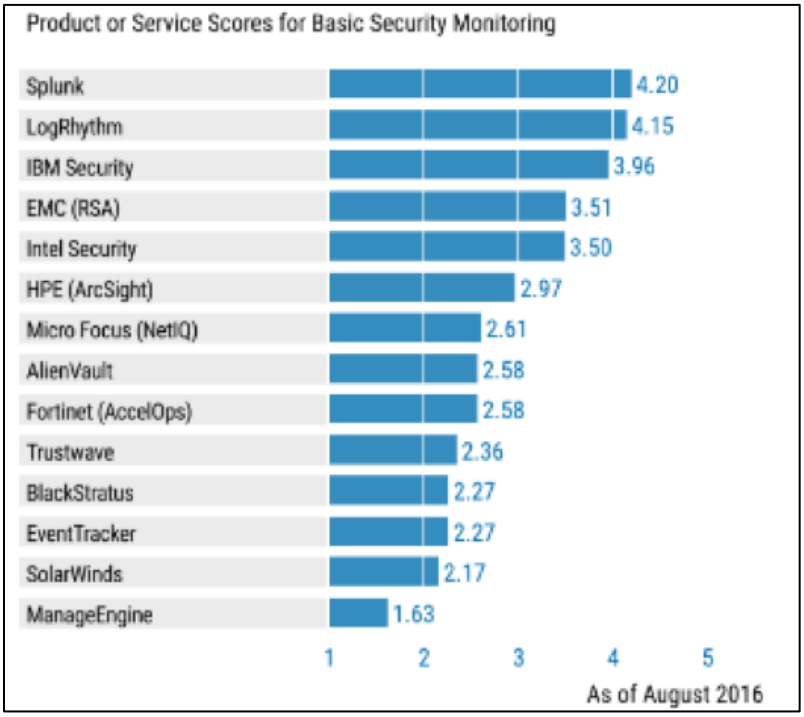
بررسی‌های گارتنر در سال ۲۰۱٦ میلادی نشان می‌دهد که IBM QRadar SIEM مقام سوم در پایش امنیتی، مقام سوم در تشخیص پیشرفته تهدید و مقام دوم در جرم‌یابی و پاسخگویی به حوادث امنیتی را دارد و بر طبق آن QRadar یک بستر پایش امنیتی با چندین ویژگی مدیریت فایل‌های ثبت وقایع، NetFlow، SIEM و بسیاری از ویژگی‌های دیگر از جمله پایش برنامه کاربردی، ضبط کامل بسته، پویش آسیب‌پذیری و تحلیل ریسک را فراهم می‌آورد. در شکل ۲-۱ مربع جادویی گارتنر و سپس ۲-۲ رتبه‌بندی براساس قابلیت پایش امنیتی، شکل ۲-۳ تشخیص پیشرفته تهدید و شکل ۲- ٤ جرم‌یابی و پاسخگویی به حوادث امنیتی نشان داده شده است.

[۱] Limited Multi-tenancy support

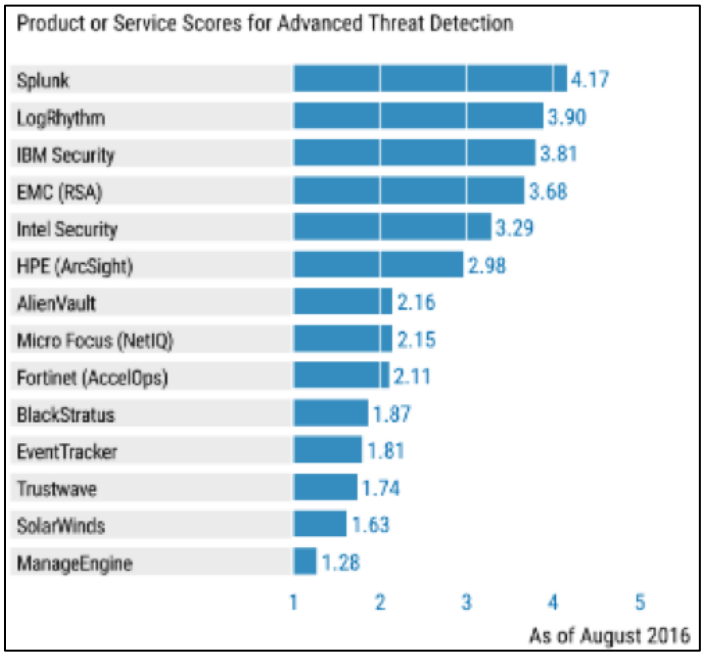
[۲] Limited capability to perform

[۳] Advanced Use Case development & analytics

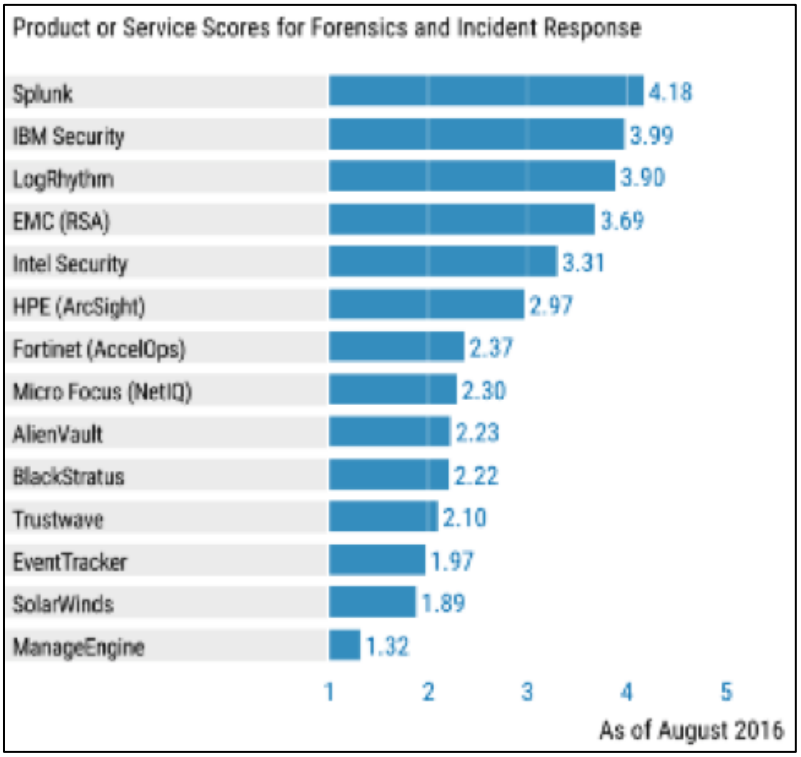
شکل ۳۳-۱: مربع جادویی گارتنر در سال ۲۰۱۶ میلادی



شکل ۳۳-۲: رتبه‌بندی محصولات براساس پایش امنیتی



شکل ۳۳-۳: رتبه‌بندی محصولات براساس تشخیص پیشرفته تهدید



شکل ۳۳-٤:رتبه‌بندی محصولات جرم‌یابی و پاسخگویی به حوادث امنیتی

سازمان‌های بزرگ یا متوسط با نیازمندی‌های عمومی، و همچنین سازمان‌هایی که به دنبال یک بستر منفرد پاسخگویی و پایش وقایع امنیتی برای SOC خود هستند می‌توانند به QRadar به عنوان یک گزینه مناسب

توجه کنند. همچنین اگر شرکتی با اندازه متوسط به دنبال یک راه‌حل با پیاده‌سازی انعطاف‌پذیر، گزینه‌های میزبانی و پایش باشد، می‌تواند از QRadar بهره ببرد. در گزارش گارتنر نقاط قوت و ضعف آن نیز توصیف شده است که در ادامه بیان می‌شوند.

۳-۱-۱-۱ نقاط قوت

- QRadar یک دیدگاه یکپارچه از داده رویداد و فایل ثبت وقایع با جریان شبکه و بسته‌ها، داده ارزیابی و آسیب‌پذیری و هوشمندی تهدید فراهم می‌نماید.
- تحلیل رفتار ترافیک شبکه می‌تواند میان رویدادهای فایل ثبت وقایع و NetFlow همبستگی ایجاد کند.
- معماری پیمانه‌ای QRadar وقایع امنیتی و پایش فایل‌های ثبت وقایع را در محیط IaaS شامل پایش بومی برای AWS CloudTrail و SoftLayer پشتیبانی می‌کند.
- فناوری QRadar و رویکرد وابسته به معماری آن را جهت استقرار و حفاظت، چه به عنوان یک ابزار همه‌جانبه[۱] یا محیط چندبخشی و چند لایه، نسبتاً آسان می‌سازد.
- IBM Security App Exchange یک چارچوب جهت یکپارچه‌نمودن قابلیت‌ها از فناوری‌های شخص ثالث به داشبوردهای SIEM و جریان کاری تجسس و پاسخگویی فراهم می‌کند.

فروشنده‌های بسیاری برنامه‌های کاربردی از جمله Palo Alto یا Blue Coat را برای بهبود عملکرد QRadar طراحی می‌کنند که دسترسی به این برنامه‌ها رایگان بوده و امکان افزودن قوانین و ویژگی‌های رویداد سفارشی را فراهم می‌کنند.

۳-۱-۱-۲ هشدارها

- پایش نقطه پایانی برای تشخیص و پاسخگویی به تهدید، یا صحت فایل پایه نیاز به استفاده از فناوری های شخص ثالث دارد. (این می‌تواند به دلیل آن باشد که IBM QRadar از تعداد بسیاری از ابزارها و افزونه‌های شخص ثالث استفاده می‌کند که نیازمند به مدیریت وصله در محصول می‌باشد)

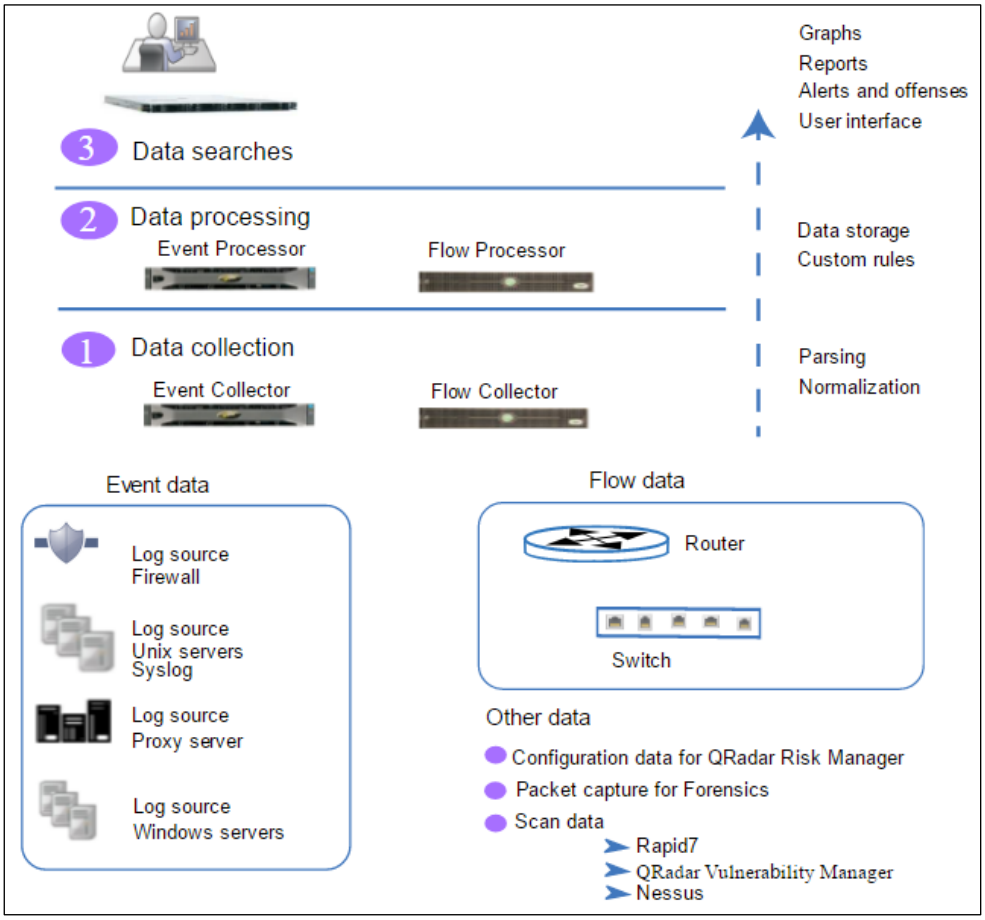
[۱] All-in-One

- مشتریان گارتنر گزارش دادند که موفق به یکپارچه‌سازی افزونه مدیریت آسیب‌پذیری IBM برای QRadar شدند.
- روند تعامل فروش با IBM پیچیده بوده و نیاز به پیگیری دارد.

٤ معماری سیستم

به منظور برنامه‌ریزی و ایجاد در استقرار IBM Security QRadar، نیاز به دانش درباره معماری QRadar جهت ارزیابی چگونگی عملکرد مؤلفه‌های QRadar در شبکه و سپس برنامه‌ریزی نحوه استقرار آن می‌باشد.

IBM Security QRadar داده‌های شبکه را به صورت بی‌درنگ جمع‌آوری، پردازش، گردآوری و ذخیره می‌نماید. QRadar داده را جهت مدیریت امنیت شبکه با فراهم‌نمودن اطلاعات بی‌درنگ و پایش، هشدارها و جرایم پاسخ به تهدیدات شبکه استفاده می‌کند. IBM Security QRadar SIEM دارای یک معماری پیمانه‌ای است که یک میدان دید بی‌درنگ از زیرساخت IT فراهم می‌نماید تا بتوان آن را برای تشخیص و اولویت‌بندی تهدید به‌کار برد. می‌توان مقیاس QRadar را به‌منظور تأمین نیازمندی‌های جمع‌آوری جریان و فایل ثبت وقایع و همچنین تحلیل گسترش داد. می‌توان پیمانه‌های واحد را به بستر QRadar، از جمله QRadar Risk Manager، QRadar Vulnerability Manager و QRadar Incident Forensics افزود. عملیات قابل انجام در بستر هوشمندی تهدید امنیتی QRadar متشکل از سه لایه می‌باشد و در هر ساختار استقرار QRadar، صرف نظر از اندازه و پیچیدگی آن قابل اجرا می‌باشد. نمودار شکل ۳-۱ لایه‌های معماری QRadar را نشان می‌دهد.



شکل ٤٤-١: لایه‌های معماری QRadar

چارچوب هوشمندی تهدید امنیتی QRadar توسط IBM ارائه شده است که در آن تجهیزات IBM QRadar به دسته‌های مختلفی تقسیم می‌شود:

- جمع‌آوری‌کننده‌های QFlow[1] و VFlow
- پردازشگرهای جریان[2]
- جمع‌آوری‌کننده‌های رویداد[3]
- پردازشگرهای رویداد[4]

---

[1] QFlow collectors

[2] Flow processors

[3] Event collectors

[4] Event processors

- پردازشگرهای ترکیب‌شده جریان و رویداد[۱]
- تجهیزات همه‌جانبه[۲]
- کنسول[۳]
- مدیر فایل ثبت رویداد QRadar[٤]
- مدیر آسیب‌پذیری QRadar[٥]
- مدیر ریسک QRadar[٦]
- گره داده
- جرم‌یابی حوادث QRadar[۷]
- ضبط بسته QRadar[۸]
- SIEM
- مدیر ریسک[۹]

معماری تجهیزات QRadar به دو صورت توزیع‌شده و همه‌جانبه و یا به صورت مجازی و فیزیکی و همچنین زیرساخت ابری[۱۰] می‌باشد که در شکل ۳-۲ و ۳-۳ نمونه‌ای معماری‌های توزیع‌شده و همه جانبه را مشاهده می‌کنید.

---

۱ Combined Event and Flow processors

۲ All-In-One appliances

۳ Console

٤ QRadar Log manager

٥ QRadar Vulnerability manager

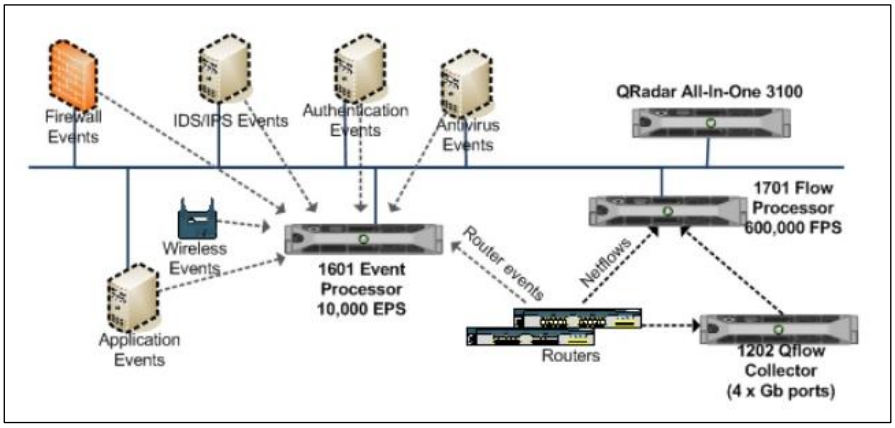
٦ QRadar Risk manager

۷ QRadar Incident Forensics

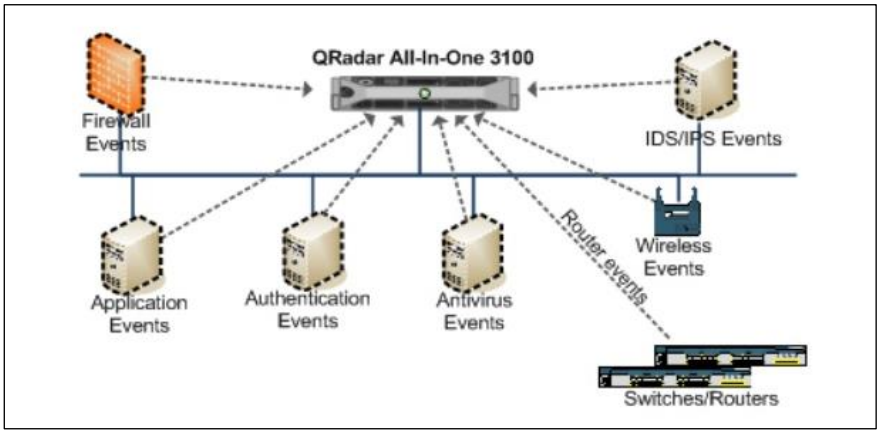
۸ QRadar Packet Capture

۹ Risk Manager

۱۰ IaaS



شکل ٤٤-٢: ساختار توزیع‌شده QRadar SIEM



شکل ٤٤-٣: ساختار همه‌جانبه QRadar SIEM

چارچوب QRadar جمع‌آوری و پردازش رویداد امنیتی و داده فایل ثبت وقایع، NetFlow، پایش ترافیک شبکه با استفاده از ضبط عمیق بسته، تحلیل رفتار برای همه منابع داده پشتیبانی شده تشخیص را امکان‌پذیر می‌سازد. این چارچوب دارای قابلیت‌های زیر است:

QRadar SIEM قابلیت تشخیص ناهنجاری مبتنی بر شبکه[1] (NBAD) با به‌کارگیری NetFlow، JFlow، sFlow و QFlow در ۷ لایه شبکه را دارد. قابلیت‌های کلیدی آن عبارتند از:

- توانایی پردازش داده امنیتی از منابع فراوان از قبیل:
  - دیواره آتش

[1] Network-based Behavior Anomaly Detection

- دایرکتورهای کاربران
- پروکسی‌ها
- برنامه‌های کاربردی
- مسیریاب‌ها

- جمع‌آوری، نرمال‌سازی[۱]، همبسته‌سازی[۲]، و ذخیره‌سازی امن وقایع خام، جریان شبکه، آسیب‌پذیری‌ها، دارایی‌ها
- ضبط بدنه لایه کاربردی شبکه تا تعداد قابل تنظیمی از بایت‌های ترافیک غیر رمزشده
- قابلیت‌های فراگیر جستجو
- پایش تغییرات میزبان و رفتار شبکه که وجود حمله یا نقض در سیاست را نشان می‌دهد
- هشداردهی توسط ایمیل، SNMP و غیره
- دارای قالب‌های جامع گزارش‌دهی
- معماری مقیاس‌پذیر به منظور پشتیبانی از محیط‌های گسترده
- رابط کاربری منفرد

QRadar SIEM دارای داشبوردهای پیش‌فرض می‌باشد که عبارتند از:

- بررسی برنامه کاربردی
- بررسی تطابق
- بررسی شبکه
- پایش سیستم
- پایش امنیت و تهدید
- زیرساخت ابری مجازی
- مدیریت آسیب‌پذیری

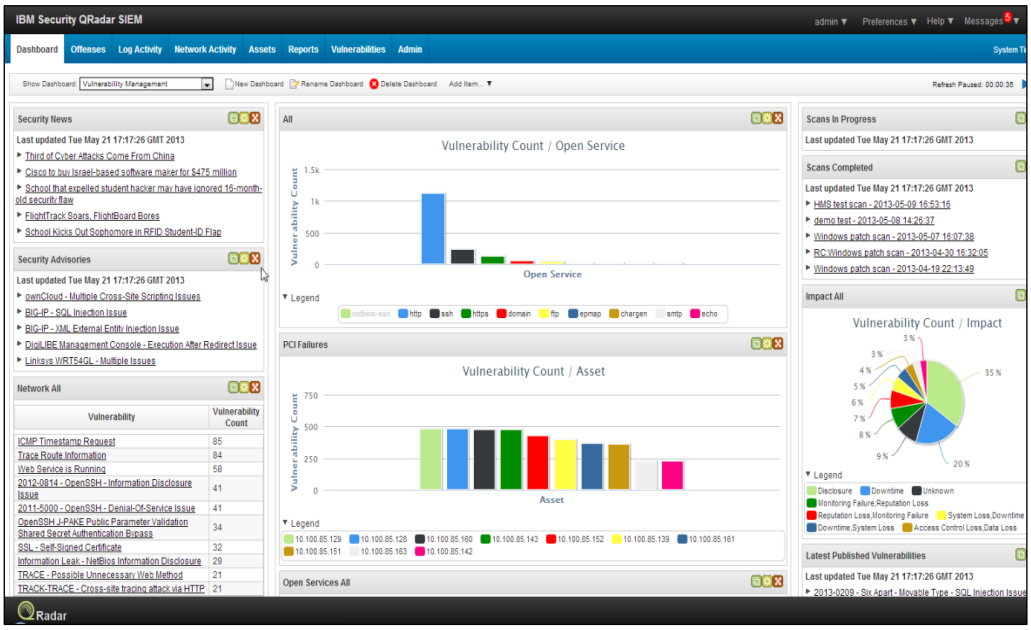
[۱] Normalization

[۲] Correlation

و دیگر داشبوردهای چندگانه که برای سازماندهی بهتر داده به‌کار می‌روند. به عنوان مثال یک کاربر می‌تواند داشبوردهای زیر را جهت نمایش فایل‌های ثبت رویداد و فعالیت‌های شبکه از سیستم‌ها داشته باشد:

- پایگاه‌داده‌ها
- برنامه‌های کاربردی حیاتی

در شکل ۳-٤ یک داشبورد نمونه در کنسول QRadar نشان داده شده است.



شکل ٤٤-٤: کنسول Qradar SIEM

برطبق گزارش گارتنر در سال ۲۰۱٦ میلادی این محصول ویژگی‌های جدیدی شامل IBM X-Force Exchange برای به اشتراک‌گذاری هوشمندی تهدید را دارا است، IBM Security App Exchange توسط چارچوب برنامه کاربردی QRadar پشتیبانی می‌شود.

پیشرفت‌ها در قابلیت‌های تولیدشده محصول، مدیریت سیستم (پایش سلامت و مدیریت وصله) و کارآیی جستجو ایجاد شدند. IBM در آوریل سال ۲۰۱٦ میلادی از سیستم‌های انعطاف‌پذیر[1] به منظورگسترش قابلیت‌های پاسخگویی به حوادث در چارچوب QRadar بهره برده است.

[1] Resilient Systems

٤-١ منابع داده قابل پشتیبانی

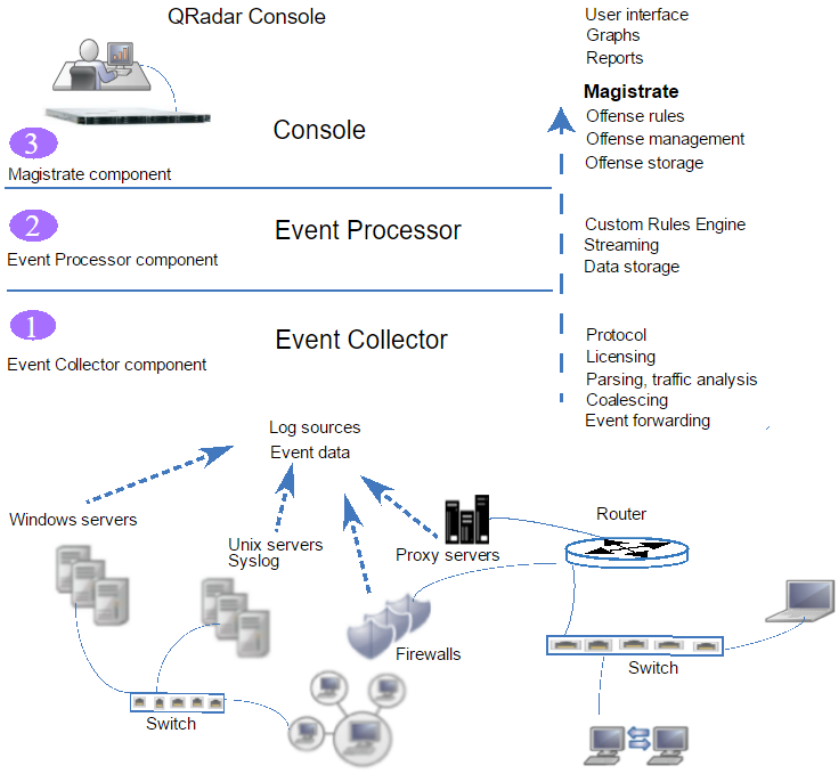
منابع داده قابل پشتیبانی می‌تواند به سه دسته کلی تقسیم شود: وقایع، جریان و اطلاعات ارزیابی آسیب‌پذیری. در ادامه توضیحی درباره هریک از منابع ارائه می‌شود.

٤-١-١ جریان و رویداد در QRadar

توابع هسته IBM QRadar SIEM، مدیریت امنیت شبکه به همراه پایش جریان و رویداد می‌باشد. تفاوت قابل توجه جریان و رویداد آن است که رویداد به طور نمونه یک فایل ثبت رویداد فعالیت خاصی از جمله ورود کاربر، یا یک اتصال VPN می‌باشد که در یک زمان مشخص اتفاق افتاده و رویداد در همان زمان ثبت می‌شود. یک جریان، رکوردی از فعالیت شبکه است که می‌تواند وابسته به فعالیتی که در حین جلسه اتفاق می‌افتد برای ثانیه‌ها، دقایق، ساعت‌ها، یا روزها طول بکشد. برای مثال، یک درخواست وب شاید چندین فایل از جمله تصاویر، آگهی‌ها و ویدئو را بارگذاری کند که ۵ تا ۱۰ ثانیه به طول بیانجامد و یا اینکه کاربری فیلم Netflix را در یک نشست شبکه ببیند که ساعتی به طول انجامد. جریان رکوردی از فعالیت‌های شبکه بین دو میزبان می‌باشد.

٤-٢ خط لوله رویداد

پیش از آنکه شما بتوانید داده رویداد در کنسول QRadar مشاهده و استفاده نمایید وقایع از منابع رویداد توسط پردازشگر رویداد پردازش می‌شوند. ابزار همه‌جانبهQRadar علاوه بر به انجام رساندن نقش کنسول QRadar، به عنوان جمع‌آوری‌کننده و پردازشگر رویداد نیز عمل می‌کند. QRadar با استفاده از تجهیزات اختصاصی جمع‌آوری‌کننده یا با استفاده از تجهیزات همه‌جانبه در جایی که سرویس جمع‌آوری و پردازش رویداد بر روی تجهیز همه‌جانبه اجرا می‌شود، می‌تواند رویدادها را جمع‌آوری نماید.



شکل ٤٤-٥: خط لوله رویداد

٤-٢-١ جمع‌آوری داده رویداد

وقایع توسط منابع تولید فایل ثبت رویداد از جمله دیواره آتش، مسیریاب‌ها، سرویس‌دهنده‌ها و سیستم‌های تشخیص نفوذ (IDS) یا سیستم‌های پیشگیری از نفوذ (IPS) تولید می‌شوند. در جمع‌آوری رویداد، مؤلفه جمع‌آوری‌کننده رویداد کارکردهای زیر را انجام می‌دهد:

٤-٢-١-١ پروتکل‌های قابل پشتیبان

اغلب منابع تولیدکننده رویداد، اطلاعات را با استفاده از پروتکل Syslog به QRadar SIEM ارسال می‌کنند. QRadar SIEM پروتکل‌های زیر را پشتیبانی می‌نماید:

- JDBC
- JDBC – SiteProtector
- Sophos Enterprise Console – JDBC
- Juniper Networks NSM
- OPSEC/LEA
- SDEE
- SNMPv1
- SNMPv2
- SNMPv3
- Sourcefire Defense Center Estreamer

- Log File
- Microsoft Security Event Log
- Microsoft Security Event Log Custom
- Microsoft Exchange
- Microsoft DHCP
- Microsoft IIS
- EMC VMWare
- SMB Tail
- Oracle Database Listener
- Cisco Network Security Event Logging
- PCAP Syslog Combination Protocol
- Forwarded Protocol
- TLS Syslog Protocol
- syslog-tcp
- Juniper Security Binary Log Collector Protocol
- UDP Multiline Syslog Protocol
- IBM Tivoli Endpoint Manager SOAP Protocol

پذیرش وقایع از منابع تولیدکننده رویداد با استفاده از پروتکل‌هایی نظیر syslog، syslog-tcp و SNMP و دیگر پروتکل‌های مشابه صورت می‌گیرد. QRadar همچنین می‌تواند اتصال‌های خارج از محدوده را به منظور بازیابی وقایع توسط پروتکل‌هایی نظیر SCP، SFTP، FTP، JDBC، Check Point OPSEC و SMB/CIFS تنظیم نماید.

برحسب منابع تولید رویداد، ممکن است که نیازمند به یک پیکربندی دستی برای تغذیه مناسب رویداد توسط QRadar SIEM باشید. QRadar SIEM تعداد وقایع ورودی به سیستم را به منظور مدیریت صف‌های ورودی و صدور مجوز EPS پایش می‌نماید.

تجزیه[1]: وقایع خام را از تجهیزات منبع می‌گیرد و فیلدها را با قالب مورد استفاده QRadar تجزیه می‌کند.

تحلیل ترافیک و کشف خودکار منبع فایل ثبت رویداد: داده رویداد تجزیه شده و نرمال شده را به DSMهای ممکن اعمال می‌کند که اکتشاف خودکار را پشتیبانی می‌نمایند.

آمیخته کردن[2]: وقایع ابتدا تجزیه می‌شوند و سپس براساس ویژگی‌های رایج میان وقایع با هم آمیخته می‌شوند.

[1] Parsing

[2] Coalescing

٤-٢-١-٢ ارسال رویداد

قوانین مسیریابی برای سیستم به منظور ارسال داده به اهداف خارج سیستم، سیستم‌های خارجی Syslog، سیستم‌های JSON و دیگر SIEMها اعمال می‌شوند. زمانی‌که در جمع‌آوری‌کننده رویداد، وقایع از منابع فایل‌های ثبت وقایع از جمله دیواره آتش دریافت می‌شوند، وقایع در صف‌های ورودی برای پردازش قرار می‌گیرند. صف را به طور متفاوت براساس پروتکل یا شیوه‌ای که به‌کار می‌رود، اندازه می‌گیرد و از این صف‌ها، وقایع تجزیه شده و نرمال می‌شوند. فرآیند نرمال‌سازی دربرگیرنده تبدیل داده خام به یک قالب است که دارای فیلدهایی از جمله آدرس IP می‌باشد که توسط QRadar قابل استفاده است. QRadar منابع رویداد را با آدرس IP یا نام میزبان موجود در سرآیند تشخیص می‌دهد. QRadar وقایع را در منابع رویداد تجزیه نموده و به صورت رکوردهایی آمیخته می‌کند.

کلیه وقایع جدید یا از منابع ناشناخته‌ای که پیش از این تشخیص داده نشده‌اند به موتور تحلیل ترافیک یا تشخیص خودکار مجدداً ارسال می‌شوند. زمانی‌که منابع جدید تولیدکننده رویداد کشف می‌شوند، یک پیام درخواست پیکربندی به منظور افزودن منبع رویداد به کنسول QRadar ارسال می‌گردد. اگر تشخیص خودکار غیرفعال باشد، یا اینکه از حد مجاز منبع رویداد تجاوز شده باشد، منابع رویداد جدید، دیگرافزوده نخواهند شد.

٤-٢-١-٣ پردازش رویداد

مؤلفه پردازشگر رویداد عملکردهای زیر را انجام می‌دهد:

- موتور قوانین سفارشی[1] (CRE)

موتور CRE مسئولیت پردازش وقایعی را بر عهده دارد که با QRadar دریافت شده‌اند، و در حالی‌که آنها را با قوانین تعریف شده مقایسه می‌کند، سیستم‌های مربوط به حوادث را پیگیری نموده و هشدارها را برای کاربران تولید می‌کند. وقتی وقایع با قوانین سازگار باشند، یک هشدار از پردازشگر رویداد به مدیر بخش[2] ارسال می‌کند که یک رویداد خاص یک قانون را راه‌اندازی نموده است. مؤلفه مدیر بخش بر روی کنسول

[1] Custom Rules Engine

[2] Magistrate

offense QRadarها را ایجاد و مدیریت می‌کند. فایده اصلی QRadar SIEM برای تحلیل‌گران امنیتی تشخیص فعالیت‌های بدخواه و دسته‌بندی آنها در offenseها می‌باشد. یک offense حمله بدخواه یا نقض سیاست را نشان می‌دهد. QRadar SIEM یک offense را زمانی ایجاد می‌کند که وقایع، جریان، و یا هردو، مطابق با معیار تست مشخص‌شده در قوانین قابل تغییری باشند که اطلاعات زیر را تحلیل می‌کنند:

- وقایع و جریان ورودی
- اطلاعات دارایی
- آسیب‌پذیری‌های شناخته‌شده

بنابراین زمانی‌که قوانین راه‌اندازی می‌شوند، پاسخ‌ها یا اعمالی از جمله هشدارها، syslog، SNMP، پیام‌های ایمیل، وقایع جدید و offenseها تولید می‌شوند.

- جاری‌سازی داده[1]

زمانی که یک کاربر وقایع را از سربرگ Log Activity با جاری‌سازی داده بلادرنگ می‌بیند، داده رویداد به کنسول QRadar به صورت بلادرنگ ارسال می‌شود. داده‌های جریان‌یافته از طریق پایگاه‌داده‌ها آماده نمی‌شوند.

- ذخیره‌سازی رویداد (Ariel)

یک پایگاه‌داده سری زمانی، برای وقایعی که داده را لحظه به لحظه ذخیره می‌کنند، مورد نیاز می‌باشد. داده در جایی ذخیره می‌شود که رویداد پردازش شود. جمع‌آوری‌کننده رویداد داده رویداد نرمال شده را به پردازشگر رویداد در جایی که وقایع توسط CRE مورد پردازش قرار می‌گیرند، ارسال می‌کند. اگر وقایع با قوانین سفارشی CRE که از قبل در کنسول QRadar تعریف شده‌اند، سازگار باشد پردازشگر رویداد، عملیاتی را که برای پاسخ قانون تعریف شده، به جریان می‌اندازد.

٤-١-٢-٤ مدیر بخش بر روی کنسول QRadar

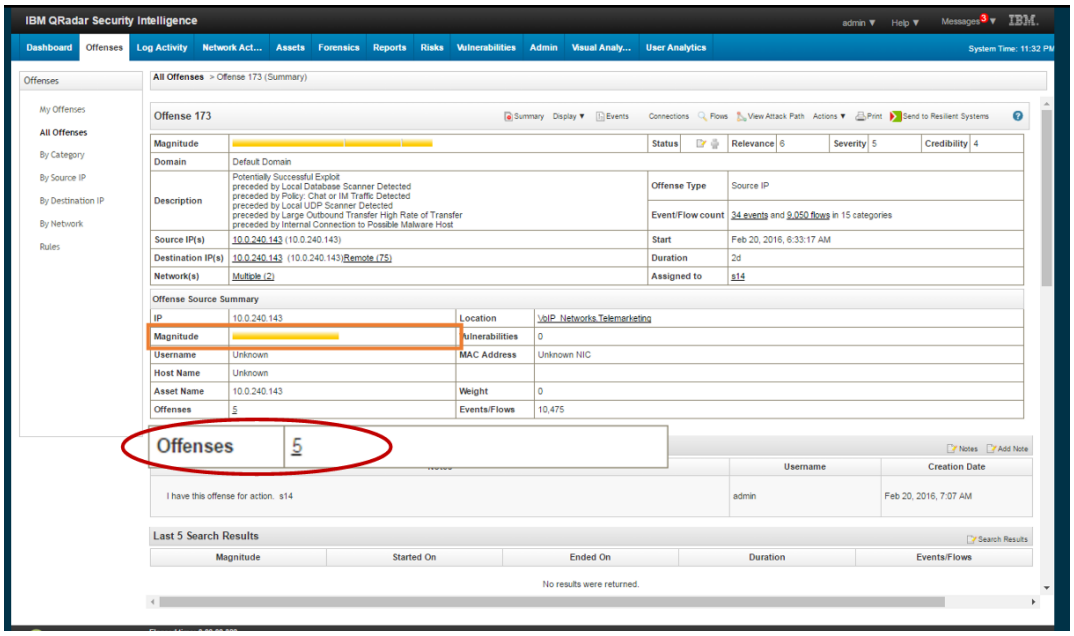
مؤلفه مدیر بخش عملکردهای زیر را انجام می‌دهد:

[1] Streaming

قوانین Offense[1]: پایش‌ها و اعمال بر روی تهاجم‌ها مانند تولید هشدارهای ایمیل انجام می‌شوند.

مدیریت Offense: Offenseهای فعال را به‌روزرسانی می‌کند، وضعیت Offense را تغییر می‌دهد و دسترسی کاربر را نسبت به اطلاعات تهاجم از طریق سربرگ Offenses فراهم می‌کند.

ذخیره‌سازی Offense: داده Offense را در پایگاه Postgres ذخیره می‌کند. هسته پردازش مدیربخش[2] (MPC) مسئولیت همبسته‌سازی حملات با هشدارهای رویداد از مؤلفه‌های پردازشگر متعدد را بر عهده دارد. فقط کنسول QRadar یا تجهیزات همه‌جانبه دارای مؤلفه مدیربخش هستند.



شکل ٤٤-٦: نمایش اطلاعات سربرگ Offense

٤-٢-٢ جمع‌آوری داده جریان

جریان در QRadar اطلاعات فعالیت‌های شبکه را با نرمال‌سازی آدرس‌های IP، درگاه‌ها، تعداد بسته‌ها و بایت‌ها و دیگر داده‌ها به صورت رکوردهای جریان ارائه می‌دهد که حاوی رکوردهای نشست‌های شبکه میان

[1] Offense rules

[2] Magistrate Processing Core

دو میزبان می‌باشند. مؤلفه‌ای که در QRadar اطلاعات جریان را جمع‌آوری و ایجاد می‌کند QFlow نامیده می‌شود.

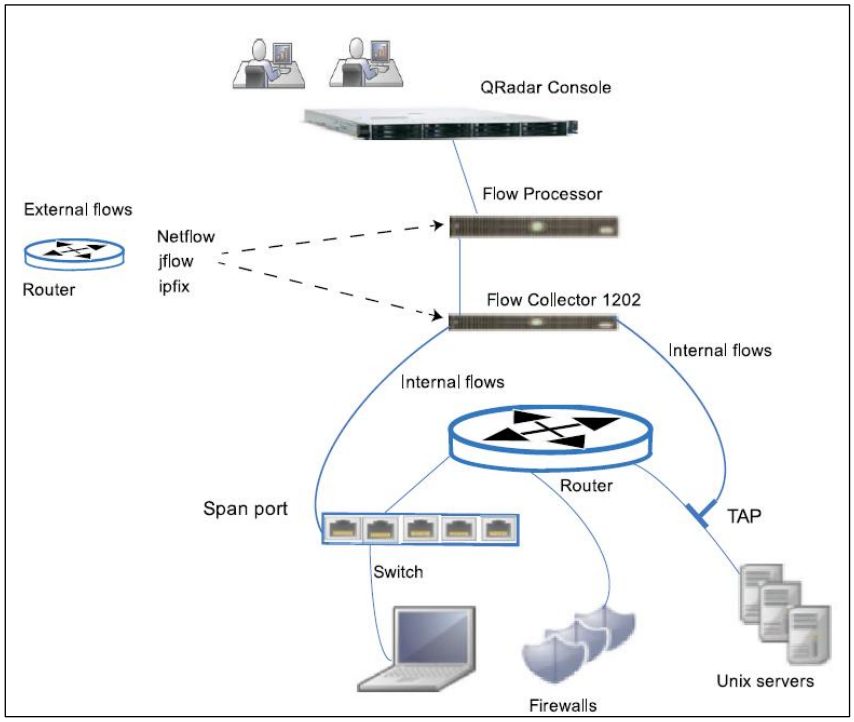
جمع‌آوری جریان QRadar ضبط کامل بسته نیست. برای نشست‌های شبکه‌ای که وقفه‌های زمانی (دقایق) متعددی را طی می‌کنند، خط لوله جریان، رکوردی از پایان هر دقیقه را با داده مرسوم برای مقیاس‌ها از جمله بایت‌ها، و بسته‌ها گزارش می‌دهد. ممکن است که چندین رکورد در هر دقیقه در QRadar با «زمان اولین بسته[۱]» مشاهده شود اما مقادیر «زمان آخرین بسته[۲]» در هر زمانی افزایش یابد. یک جریان زمانی آغاز می‌شود که جمع‌آوری‌کننده، جریان اولین بسته را تشخیص دهد که دارای یک آدرس IP منبع، آدرس IP مقصد، درگاه منبع، درگاه مقصد و دیگر گزینه‌های واحد است. هر بسته جدید نیز ارزیابی می‌شود. تعداد بایت‌ها و بسته‌ها به شمارنده‌های آماری در رکورد جریان اضافه می‌شود. در انتهای هر وقفه، یک رکورد وضعیت از جریان به پردازشگر جریان ارسال می‌شود و شمارنده‌های آماری برای جریان بازنشانی می‌شوند. یک جریان زمانی پایان می‌یابد که هیچ فعالیتی برای جریان در زمان تنظیم شده تشخیص داده نشود. QFlow می‌تواند جریان را از منابع خارجی یا داخلی مورد پردازش قرار دهد که در ادامه بیان می‌شوند:

- منابع خارجی منابع جریان از جمله NetFlow، JFlow، sFlow و QFlow هستند که می‌توانند به یک جمع‌آوری‌کننده جریان اختصاصی یا یک پردازشگر جریان از جمله ابزار پردازشگر ۱۷۰۵ جریان QRadar ارسال گردد. منابع خارجی نیاز به پردازش CPU بالا ندارند زیرا هر بسته به منظور ساخت جریان پردازش نمی‌شود. در این پیکربندی، ممکن است یک پردازشگر و جمع‌آوری‌کننده اختصاصی جریان وجود داشته باشد که هر دو داده جریان را دریافت و ایجاد می‌کنند. در محیط‌های کوچک‌تر با کمتر از ۵۰ Mbps، یک ابزار همه‌جانبه ممکن است کلیه پردازش‌های داده را مدیریت نماید.
- جمع‌آوری‌کننده جریان، جریان‌های داخلی را با اتصال به یک درگاه SPAN یا یک TAP شبکه جمع‌آوری می‌نماید. جمع‌آوری‌کننده شماره ۱۳۱۰ QFlow می‌تواند بسته‌های کامل را از کارت ضبط خود به ابزار ضبط بسته ارسال نماید اما خود، بسته کامل را ضبط نمی‌کند. شکل ۳-۳ گزینه‌ها برای جمع‌آوری جریان در شبکه را نشان می‌دهد.

---

[۱] First Packet Time

[۲] Last Packet Time



شکل ٤٤-٧: گزینه‌ها برای جمع‌آوری جریان

٤-٣ خط لوله جریان

جمع‌آوری‌کننده جریان داده‌ها را از بسته‌های خام جمع‌آوری شده از درگاه‌های پایش از جمله SPAN، TAP و Session Manitoring، یا از منابع خارجی جریان مانند NetFlow، JFlow، sFlow و QFlow تولید می‌کند. سپس این داده به قالب جریان QRadar تبدیل شده و خط لوله را برای پردازش به سمت پردازش می‌برد. پردازشگر جریان عملکردهای زیر را انجام می‌دهد:

٤-٣-١ فشرده‌سازی انتخابی جریان[1]

انباشتگی جریان فرآیندی است که جریان‌های تکراری را حذف می‌کند، سپس جمع‌آوری‌کننده‌های متعدد جریان، داده را به صورت انتخابی فشرده نموده و برای تجهیزات پردازشگر جریان آماده می‌نمایند.

[1] Flow deduplication

٤-٣-١-١ ترکیب مجدد نامتقارن

مسئولیت ترکیب دو طرف هر جریان را، زمانی‌که داده به صورت نامتقارن آماده شده، بر عهده دارد. این فرآیند می‌تواند جریان‌ها را از هر طرف تشخیص داده و آنها را در یک رکورد ترکیب نماید. اما، گاهی اوقات تنها یک طرف جریان وجود دارد. در بحث کنترل و مدیریت مجوز تعداد جریان‌های ورودی به سیستم را به منظور مدیریت صف‌های ورودی و مجوزدهی پایش می‌نماید.

٤-٣-١-٢ ارسال

قوانین مسیریابی برای سیستم از جمله، ارسال داده جریان به اهداف بیرونی، سیستم‌های Syslog خارجی، سیستم‌های JSON و SIEMهای دیگر، را اعمال می‌نماید. داده جریان از میان موتور قوانین شخصی (CRE) عبور می‌کند و در برابر قوانینی که تنظیم می‌شوند، همبسته می‌شود و تهاجم‌ها[1] می‌توانند براساس این همبستگی مشخص شوند. تهاجم ها را می‌توان در سربرگ Offenses مشاهده نمود.

٤-٤ جمع‌آوری و پردازش داده آسیب‌پذیری

٤-٤-١ پروفایل‌های دارایی

QRadar SIEM پروفایل‌های دارایی را برای سیستم در شبکه نگهداری می‌کند. این پروفایل‌ها شامل جزئیات میزبان از جمله آدرس IP، نام دارایی، سرویس‌هایی که درگاه باز را تشخیص می‌دهند و همچنین آسیب‌پذیری‌ها می‌باشند.

Id	IP Address	Asset Name	Aggregate CVSS Score	Vulnerabilities	Services
1030	10.111.219.138	10.111.219.138	0.0	0	0
1013	10.117.220.204	10.117.220.204	0.0	0	0
1014	10.117.220.205	10.117.220.205	0.0	0	0
1012	10.117.254.16	10.117.254.16	0.0	0	0
1011	10.117.254.36	10.117.254.36	0.0	0	0
1010	10.117.254.66	10.117.254.66	0.0	0	0
1009	10.15.20.140	10.15.20.140	0.0	0	0
1015	10.2.100.66	10.2.100.66	0.0	0	0
1018	10.20.0.80	10.20.0.80	0.0	0	0
1007	128.245.120.152	128.245.120.152	0.0	0	0
1019	172.16.254.2	chkpt1	0.0	0	0

شکل ٤٤-٨: یک نمونه پروفایل دارایی

[1] Offense

علاوه بر اطلاعات دارایی، پروفایل‌های دارایی ورود کاربر به دارایی را در صورتی که این اطلاعات توسط Qradar SIEM فراهم شود، پیگیری می‌کنند. QRadar SIEM به طور خودکار پروفایل‌های دارایی را برای سیستمی که در مکان‌های زیر یافت شوند، به‌روزرسانی و ایجاد می‌کند:

- فایل‌های ثبت رویداد DHCP، DNS، VPN، پروکسی، NAT دیواره آتش و AP بی‌سیم
- جریان دوطرفه گردآوری شده به طور غیرفعال
- داده آسیب‌پذیری آماده شده توسط اسکنرهای فعال

اگر اطلاعات دردسترس نباشند، QRadar SIEM پروفایل دارایی را به طور خودکار ایجاد نمی‌کند. اما کاربر می‌تواند پروفایل را در رابط کاربری یا به وسیله ورود داده ایجاد نماید. تنها داده آسیب‌پذیری و جریان‌ها اطلاعات را درباره درگاه‌ها و سرویس‌ها نسبت به پروفایل‌های دارایی اضافه و به‌روز می‌کنند.

اطلاعات پروفایل دارایی برای اهداف همبستگی بکار می‌روند. برای مثال، اگر یک مهاجم تلاش کند تا یک سرویس خاص را نقض کند که در حال اجرا روی یک دارایی خاص می‌باشد، QRadar SIEM می‌تواند با همبسته‌سازی حمله با پروفایل دارایی مشخص کند که دارایی نسبت به این حمله آسیب‌پذیر می‌باشد.

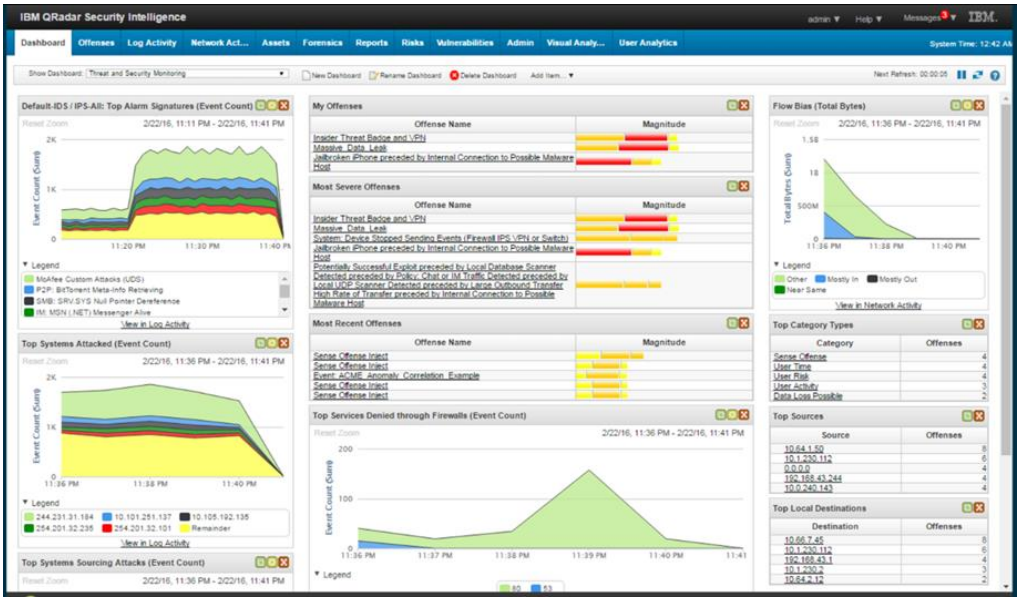
۵ تحلیل قابلیت‌های IBM QRadar SIEM

۵-۱ اطلاعات ارزیابی آسیب‌پذیری[۱] (VA)

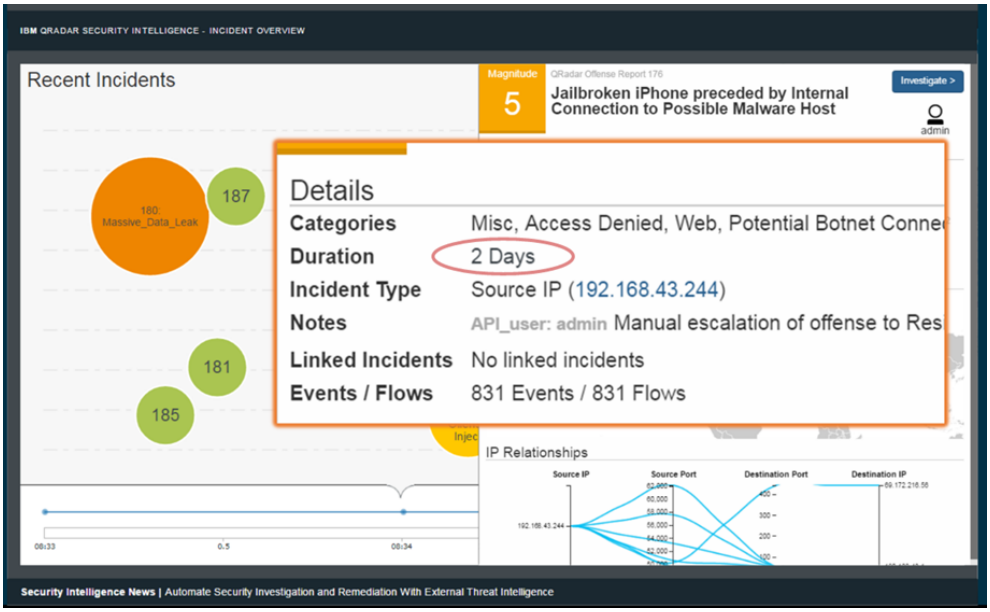
QRadar می‌تواند اطلاعات VA را علاوه بر اسکنرهای آسیب‌پذیری توکار از اسکنرهای شخص ثالث متنوعی نیز وارد کند. اطلاعات VA به مدیر ریسک QRadar[۲] امکان شناسایی میزبان‌های فعال، درگاه‌های باز و آسیب‌پذیری‌های بالقوه را می‌دهد. مدیر ریسک اطلاعات VA را به منظور رتبه‌بندی شدت نفوذها بر روی شبکه به‌کار می‌برد. وابسته به نوع اسکنر VA، مدیر ریسک می‌تواند نتایج اسکن را از سرویس‌دهنده اسکنر دریافت نماید یا به صورت از راه دور شروع به اسکن کند.

[۱] Vulnerability assessment

[۲] QRadar Risk Manager



شکل ۵۵-۱: تحلیل آسیب‌پذیری در QRadar SIEM



شکل ۵۵-۲ : نمایش اطلاعات حاصل از اسکن آسیب‌پذیری

۵-۲ قابلیت‌های ذخیره‌سازی و پردازش داده

همان‌گونه که قبلاً بیان شد، QRadar دارای یک سیستم پیمانه‌ای می‌باشد. بسته به نیازهای مقیاس‌پذیری، شرایط لازم و پردازش، تجهیزات مختلفی را می‌توان افزود تا با نیازهای کارآیی منطبق گردد. IBM تجهیزات

متعددی را برای انتخاب از میان دسته‌بندی‌ها، پردازش و قابلیت‌های ذخیره‌سازی مختلف پیشنهاد می‌دهد. وابسته به تجهیزات مورد نیاز، قابلیت‌های ذخیره‌سازی و پردازش متفاوت می‌باشند.

علاوه بر قابلیت‌های همبستگی، انعطاف‌پذیری در تعریف قوانین امنیتی برای هر راه‌حل SIEM ضروری است. قوانین در QRadar SIEM به رویدادها، جریان‌ها یا offenseها به منظور جستجو یا تشخیص ناهنجاری اعمال می‌شوند. اگر تمام شرایط یک تست مهیا باشد، قانون پاسخ را تولید می‌کند. مجموعه‌ای از قوانین پیش‌فرض با کنسول QRadar حمل می‌شوند. این قوانین می‌تواند به منظور ایجاد قوانین جدید با استفاده از یک نحو[1] ساده ترکیب شوند. قوانین اضافی می‌توانند از طریق تعویض برنامه کاربردی امنیتی IBM دانلود شوند. چهار مفهوم زیر برای فهم چگونگی کار با QRadar اهمیت دارد:

CRE: موتور قوانین سفارشی که به منظور تعریف، مدیریت و نمایش قوانین و بلوک‌های ساخت قانون استفاده می‌شود. CRE اطلاعات را درباره چگونگی گروه‌بندی قوانین، انواع تست‌هایی که قوانین انجام می‌دهند و پاسخ‌هایی که هر قانون تولید می‌کند، ارائه می‌دهد. CRE سیستم‌های درگیر در حوادث را پیگیری می‌کند، وقایع را در تهاجم‌ها شرکت می‌دهد و هشدارهایی را تولید می‌کند.

بلوک‌های ساخت: این بلوک‌ها به منظور تعریف ساخت منطقی و پیچیده استفاده می‌شوند. برخلاف قوانین، بلوک‌های ایجاد می‌تواند عملیات را تحریک نماید.

قوانین: یک قانون مجموعه‌ای از تست‌ها یا بلوک‌های ایجاد است که یک کنش را در هنگامی که شرایطی خاصی پیش می‌آید، راه‌اندازی می‌کند. هر قانون می‌تواند به منظور ضبط و پاسخ به یک رویداد خاص، دنباله‌ای از وقایع، دنباله جریان یا تهاجم پیکربندی شود. کنشی که می‌تواند راه‌اندازی شود می‌تواند شامل ارسال ایمیل یا تولید پیام syslog باشد.

تهاجم‌ها: همان‌گونه که داده رویداد و جریان از طریق CRE عبور می‌کند، در برابر قوانینی که پیکربندی شده offenseی که براساس این همبستگی می‌تواند مشخص گردد، همبسته می‌شوند.

انواع قانون در QRadar عبارتند از:

[1] Syntax

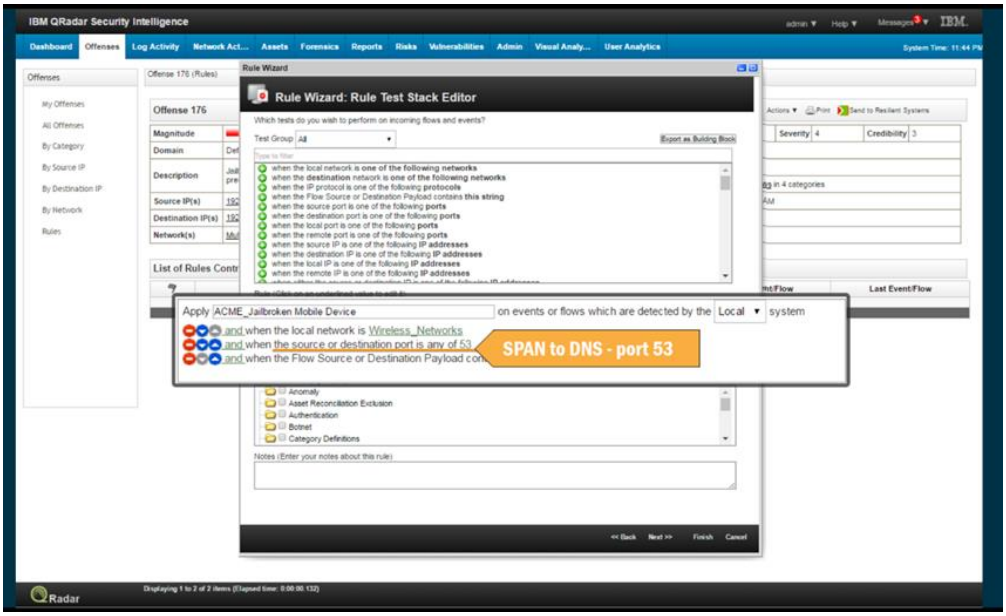
قوانین رویداد: داده منابع فایل‌های ثبت رویداد ورودی که در زمان واقعی توسط پردازشگر رویداد پردازش می‌شود، پیوسته مورد آزمون قرار می‌گیرد. قوانین رویداد می‌تواند به منظور تشخیص یک رویداد منفرد یا دنباله‌ای از وقایع استفاده شود. برای مثال، به منظور پایش شبکه برای تلاش‌های ورود ناموفق، دستیابی میزبان‌های متعدد یا شناسایی رویدادهایی که با یک سوءاستفاده دنبال می‌شوند.

قوانین جریان: داده منبع فایل ثبت رویداد ورودی که در زمان واقعی توسط پردازشگر جریان پردازش می‌گردد، پیوسته مورد آزمون قرار می‌گیرد.

قوانین مشترک: داده جریان و رویداد پیوسته مورد آزمون قرار می‌گیرد.

قوانین Offense: پارامترهای یک تهاجم به منظور راه‌اندازی پاسخ‌های بیشتر مورد آزمون قرار می‌گیرد. برای مثال، وقتی که رویدادهای جدید افزوده می‌شوند یا زمانی‌که سیستم را برای ارزیابی مجدد برنامه‌ریزی نموده است، برای قوانین Offense ایمیل نمودن یک هشدار، به عنوان پاسخ مشترک قلمداد می‌شود.

قوانین دامنه خاص: اگر یک قانون دارای یک دامنه تست باشد، می‌توان قوانین را به منظور این‌که تنها به وقایع اتفاق افتاده داخل یک دامنه خاص اعمال شوند، محدود کرد. وقتی یک رویداد یک برچسب دامنه متفاوت با دامنه تنظیم شده دارد قانون، پاسخی را راه‌اندازی نمی‌کند.



شکل ۵۵-۳: لیست قوانین و نمایش اطلاعات یک قانون

۵-۳ تحلیل رفتار در سطح برنامه کاربردی

تحلیل‌های رفتار کاربر در IBM QRadar محدود است. در حقیقت، ویژگی‌های مورد استفاده در QRadar براساس رفتار کاربر هستند. اولاً استفاده از قوانین تشخیص ناهنجاری مطرح می‌شود، و ثانیاً توان برنامه کاربردی تحلیل رفتار کاربر (UBA) در QRadar معیار بررسی در نظر گرفته می‌شود.

۵-۳-۱ قوانین تشخیص ناهنجاری

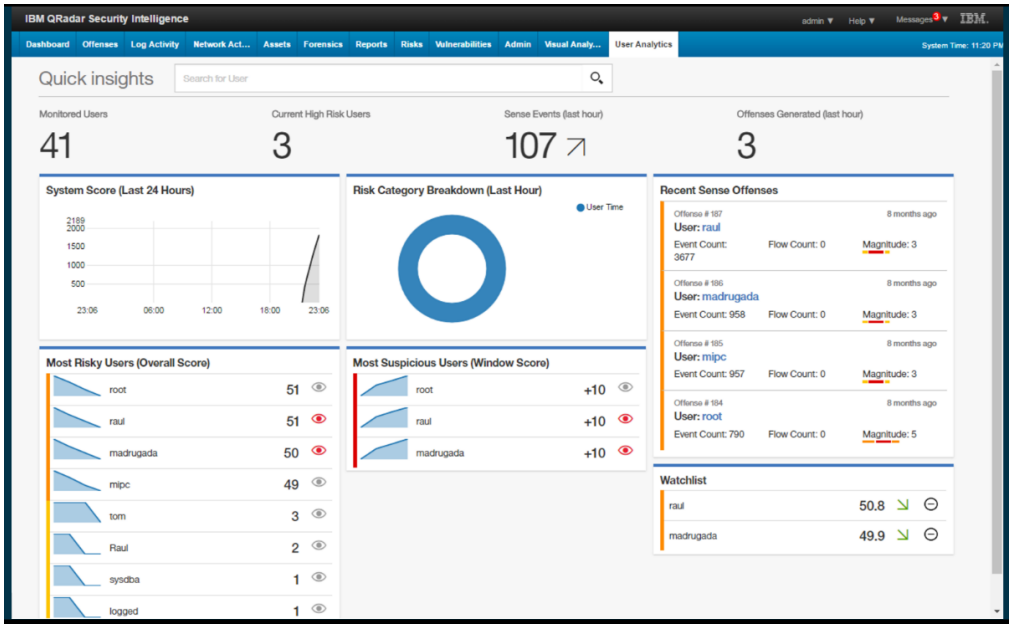
قوانین تشخیص ناهنجاری را می‌توان به قوانین آستانه و رفتاری تقسیم گردد. قوانین ناهنجاری به منظور آزمون رویداد لحظه‌ای[۱] و تغییرات ترافیک جریان به‌کار می‌روند. یک آزمون ناهنجاری، ترافیک جریان و رویداد را برای فعالیت غیرعادی، از جمله وجود ترافیک ناشناخته و جدید، آزمایش می‌کند.

- قوانین آستانه به منظور آزمون فعالیت وقایع و جریان در یک گستره مشخص به‌کار می‌رود. دانش کارشناس جهت تنظیم و میزان نمودن آستانه‌ها استفاده می‌شود. برای مثال قانون آستانه می‌تواند به منظور تشخیص تغییرات استفاده از پهنای باند در برنامه‌های کاربردی یا سرویس‌های شکست خورده مورد استفاده قرار گیرد.
- قوانین رفتاری در QRadar به منظور آزمون وقایع یا جریان‌ها برای تغییرات حجم است که در الگوهای منظم به منظور تشخیص داده‌های خارج از محدوده (ناهنجاری) اتفاق می‌افتد. یک قانون رفتاری نرخ و حجم یک ویژگی، فراتر از یک نشست از پیش‌تعریف شده را فرا می‌گیرد. نشست، خط زمانی مقایسه حدآستانه را برای مقیاس مورد ارزیابی تعریف می‌کند. طولانی‌تر از زمانی یک قانون رفتاری اجرا می‌شود، دقیق‌تر از آن است که در طول زمان باشد. با این حال، استفاده بیشتر از مدل‌های تشخیص ناهنجاری با قوانین رفتاری و تشخیص ناهنجاری فراهم‌شده توسط QRadar امکان‌پذیر نمی‌باشد.

[۱] Shot-term

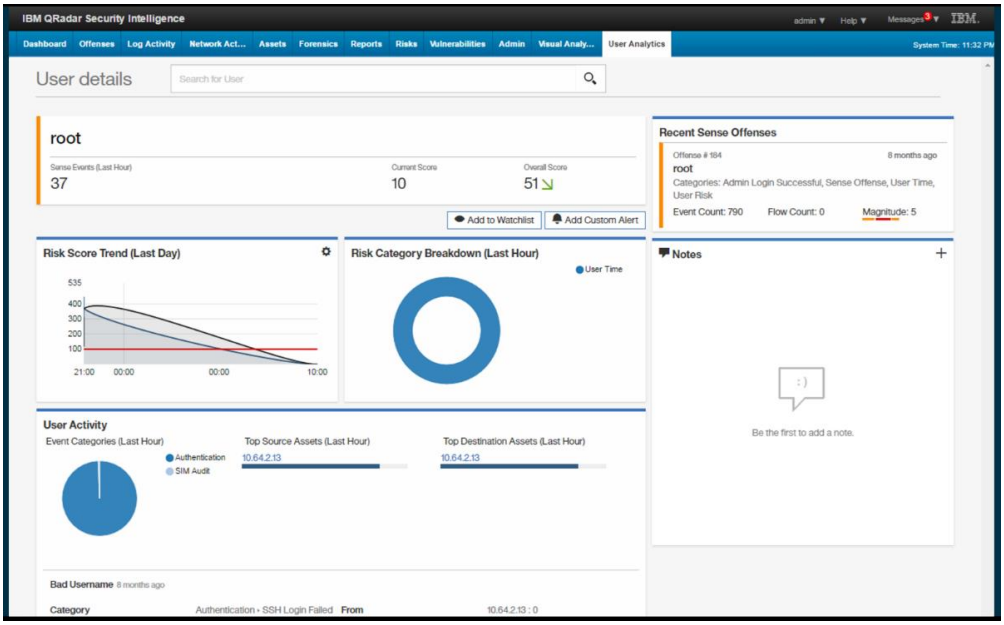
٤-٥ برنامه کاربردی UBA

تحلیل‌های رفتاری کاربر[1] IBM QRadar (UBA) پیمانه‌ای است که به منظور ارائه دیدهای اولیه نسبت به تهدیدات داخلی طراحی شده‌است. این افزونه الگوهای استفاده کاربران داخل یک سازمان را تحلیل می‌کند تا نقض اعتبارنامه‌های آنان را بررسی نماید. الگوریتم‌های یادگیری ماشین به منظور تشخیص رفتارهای غیرعادی کاربر با ایجاد یک حد آستانه رفتار نرمال کاربر و تشخیص انحراف‌های قابل توجه به‌کار می‌روند. برنامه کاربردی UBA با یک داشبورد کاربر محور برای پایش رفتارهای کاربر با حوادث تخصیص داده شده QRadar، رویدادها و جریان‌ها حمل می‌شود. برنامه کاربردی UBA تنها بر روی تهدیدات داخلی تمرکز دارد.



شکل ٥٥-٤: نمایش اطلاعات حاصل از تحلیل برنامه کاربردی UBA

[1] User Behavior Analytics



شکل ۵۵-۵: نمایش اطلاعات حاصل از کاربر root

۵-۵ ظرفیت تحلیل ریسک

مدیریت وقایع و رویدادهای امنیتی IBM QRadar دارای یک افزونه تحلیل ریسک به منظور اولویت‌بندی آسیب‌پذیری‌های برنامه کاربردی جهت کاهش ریسک (مدیر ریسک QRadar) می‌باشد. این افزونه همچنین با یک موتور سیاست برای بررسی‌خودکار تطابق و داشبود ریسک همراه است. مدیر ریسک توپولوژی و پیکربندی شبکه را پایش نموده و داده آسیب‌پذیری را با وقایع و جریان‌ها به منظور تشخیص ریسک‌های امنیت همبسته می‌کند.

۵-۶ APIهای منتشر شده[۱]

کنسول QRadar یک RESTful API را به منظور ارتباطات داخلی با QRadar ارائه می‌دهد. ارسال درخواست‌های HTTPS به نقاط پایانی URL با هر زبان برنامه‌نویسی که دارای پیاده‌سازی HTTP باشد، قابل انجام خواهد بود. جدول ٤-١ خلاصه‌ای از رابط‌های REST API را ارائه می‌دهد:

[۱] Exposed APIs

جدول ۵۵-۱: خلاصه‌ای از لیست REST APIهای QRadar

REST API	توضیحات
/api/ariel	پایگاه‌داده‌های پرس‌وجو، جستجوها، شناسه پرس‌وجو و نتایج جستجو
/api/auth	خروج و باطل کردن نشست رایج
/api/help	برگشت لیستی از قابلیت‌های API
/api/siem	برگشت لیستی از کلیه offenseها
/api/reference_data	بررسی و مدیریت جمع‌آوری‌های داده مرجع
/api/qvm	بازیابی دارایی‌ها، آسیب‌پذیری‌ها، شبکه‌ها، سرویس‌های باز، شبکه‌ها و فیلترها
/api/scanner	بررسی، ایجاد، یا شروع اسکن راه دور که مرتبط با یک پروفایل اسکن می‌باشد
/api/asset_model	لیستی از کلیه دارایی‌ها در مدل را ارائه می‌دهد.

۵-۷ قابلیت انعطاف‌پذیری[۱]

انعطاف‌پذیری داده برای QRadar تنها برای قرارگیری «دسترس‌پذیری سطح بالا[۲]» (HA) مورد توجه قرار می‌گیرد. در رویداد خرابی شبکه یا سخت‌افزار، HA تضمین می‌نماید که QRadar به جمع‌آوری، ذخیره‌سازی و پردازش داده ادامه می‌دهد.

یک استقرار HA QRadar از تکثیر کلیه تجهیزات QRadar مورد استفاده جهت داشتن یک مؤلفه اولیه و ثانویه برای هر گره تشکیل شده است. همزمان‌سازی دیسک یا ذخیره‌سازی خارجی مشترک می‌تواند به‌منظور تضمین گره‌های اولیه و ثانویه‌ای که داده یکسانی دارند، به‌کار رود. در مورد خرابی‌ها، گره‌های ثانویه مسئولیت گره‌های اولیه شکست خورده را می‌پذیرند. سناریوهایی که ممکن است منجر به خرابی شوند عبارتند از:

- شکست شبکه که با آزمون اتصال به شبکه شناسایی می‌شود.
- مدیریت خرابی رابط بر روی میزبان اولیه HA
- شکست کامل دیسک‌های RAID بر روی میزبان اولیه HA

[۱] Resilience

[۲] High Availability

- خرابی تأمین نیروی[1] برق سیستم
- نقض عملکرد سیستم‌عامل که سلامت سیستم را به تأخیر می‌اندازد یا متوقف می‌نماید.

QRadar HA هیچ حفاظتی در برابر خطاهای نرم‌افزاری ایجاد نمی‌کند. Failover زمانی اتفاق می‌افتد که میزبان HA اولیه تجربه شکست را داشته باشد، اتصالات به شبکه را از دست دهد یا یک Failover دستی انجام شود. در طی Failover، میزبان HA ثانویه مسئولیت‌های میزبان HA اولیه را می‌پذیرند. Failover ها در شرایطی اتفاق می‌افتند که یکی از سناریوهای زیر عامل آن باشند:

- شکست‌های اولیه شبکه
- شکست دیسک اولیه
- شکست دیسک یا شبکه میزبان HA ثانویه
- Failoverهای دستی

۵-۸ قابلیت‌های تصویرسازی و مدیریت وقایع امنیتی

ایجاد و مدیریت داشبوردها در QRadar ساده است. دیدگاه پیش‌فرض در کنسول Qradar هنگام ورود سربرگ Dashboard می‌باشد. این امر یک محیط فضای کاری را فراهم می‌کند که داشبوردهای متعددی را پشتیبانی می‌نماید که به منظور نمایش دیدگاه‌های امنیت شبکه، فعالیت یا داده جمع‌آوری شده استفاده می‌شوند. داشبوردها امکان سازمان‌دهی تصویرسازی اقلام را نسبت به دیدگاه‌های عملکردی می‌دهد که به منظور تمرکز بر روی مناطق خاصی از شبکه تهیه می‌شوند. داشبوردها در QRadar قابل سفارشی بوده و کاربران می‌توانند از داشبوردهای پیش‌فرض استفاده نمایند یا داشبوردهای شخصی را برای تحقیق فایل ثبت رویداد یا فعالیت شبکه ایجاد کنند. گزارشات و داشبوردها از نمودارها به عنوان بلوک ساختار در حال استفاده هستند. کاربر هنگام ساخت یک داشبورد یا گزارش می‌تواند نوع نمودار را مشخص کند. در جدول زیر لیستی از انواع نمودارها به همراه توضیحات مربوط به آن‌ها ارائه شده است.

[1] Power supply failure

جدول ۵۵-۲: لیست نمودارهای QRadar SIEM

Chart Type	Description
None	Used as a white space in dashboards and reports
Asset Vulnerabilities	Used to view vulnerability data for each defined
Connections	Used to view network connection information and trends
Device Rules	Used to view firewall rules and the event count of firewall rules
Device Unused Objects	Used to display object references of unused resources in a network. Ex. IP address, hostnames, etc.
Events/Logs	Used to view event information
Log Sources	Used to export or report on log sources.
Flows	Used to view flow information.
Top Destination IPs	Used to display the top destination IPs in a network location selected.
Top Offenses	Used to display the top offenses that occur at present time for a network location selected.
Offenses Over Time	Used to display offenses in a timeline.
Top Source IPs	Used to display and sort the top offense sources (IP addresses)
Vulnerabilities	Used to display vulnerabilities

۵-۹ قابلیت‌های واکنشی

۵-۹-۱ گزارش‌ها

QRadar قالب‌های گزارش پیش‌فرض را ارائه می‌دهد که می‌تواند سفارشی، بازتولید و به کاربران QRadar توزیع گردد. قالب‌های گزارش به صورت انواع گزارش از جمله گزارش‌های تطابق، تجهیزات، اجرایی و شبکه دسته‌بندی می‌شوند. بسته‌های گزارش‌دهی تطابق برای PCI، SOX، FISMA، GLBA، HIPAA با گزارش‌هایی براساس چارچوب‌های کنترلی از جمله NIST، ISO و CoBIT موجود هستند.

رابط گزارش‌دهی در کنسول QRadar امکان عملکردهای زیر را به‌وجود می‌آورند:

- ایجاد، توزیع، و مدیریت گزارش‌ها برای داده QRadar
- ایجاد گزارش‌های سفارشی شده برای کاربردهای اجرایی و عملیاتی
- ترکیب اطلاعات امنیتی و شبکه در یک گزارش منفرد

- استفاده یا ویرایش قالب‌های گزارش از قبل نصب شده
- تولید گزارش‌ها با لوگوهای سفارشی شده. تولید آن برای توزیع گزارش‌ها به مخاطبان مختلف
- تنظیم برنامه برای تولید هر دونوع گزارش پیش‌فرض و سفارشی
- انتشار گزارش‌ها به قالب‌های متنوع

یک گزارش می‌تواند متشکل از عناصر مختلف داده باشد و داده امنیتی و شبکه را در انواع متنوعی از قبیل جداول، نمودارهای خطی، نمودارهای دایره‌ای و نمودارهای میله‌ای ارائه دهد.

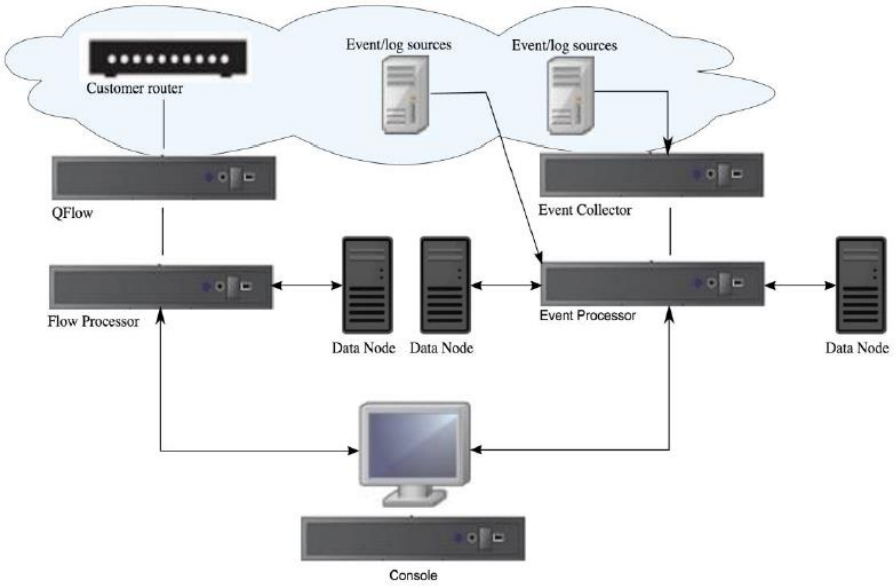
۵-۹-۲ هشداردهی در Qradar

همان‌طور که قبلاً توضیح داده شد، قوانین QRadar هشدارها را با یک عمل قابل پیکربندی به منظور انتساب به قوانین ایجاد شده، تولید می‌کنند. کنش‌های پیش‌فرض و سفارشی نیز می‌توانند ایجاد شوند. برای نمونه امکان پیکربندی یک سرویس‌دهنده ایمیل به منظور توزیع هشدارها، گزارش‌ها، اخطارها و پیام‌های رویداد وجود دارد.

۵-۱۰ پشتیبانی و توسعه

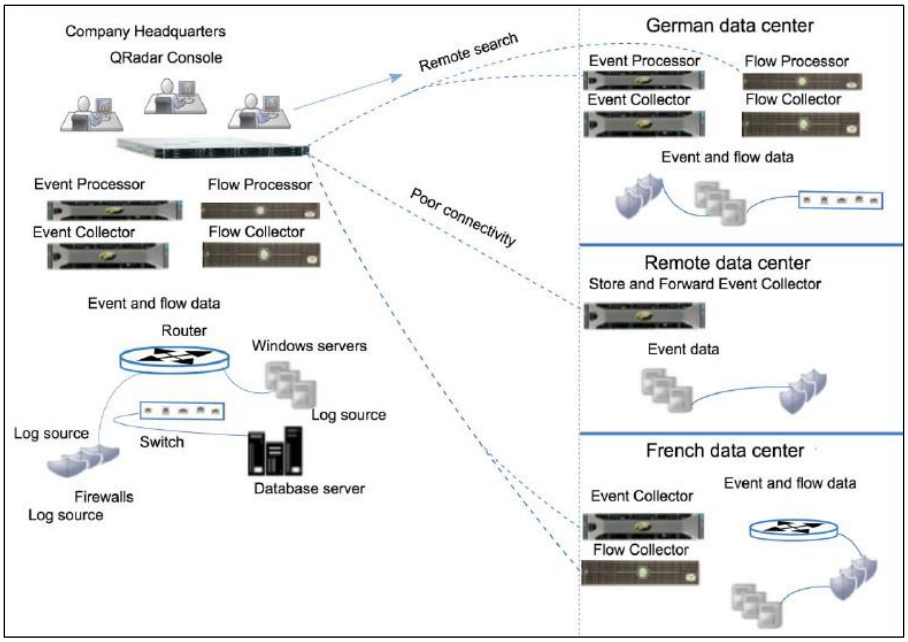
معماری IBM Security QRadar از استقرارهایی با اندازه‌ها و توپولوژی‌های مختلف پشتیبانی می‌کند، از استقرار یک میزبان منفرد در جایی که همه مؤلفه‌های نرم‌افزار بر روی یک سیستم منفرد اجرا می‌شوند گرفته تا میزبان‌های متعدد که در تجهیزاتی از جمله جمع‌آوری‌کننده‌های رویداد، جمع‌آوری‌کننده‌های جریان، گره‌های داده، پردازشگرهای رویداد، پردازشگرهای جریان، نقش‌های متفاوتی دارند. شکل ٤-١ مؤلفه‌های QRadar را نشان می‌دهد که می‌توانند به منظور جمع‌آوری، پردازش و ذخیره داده رویداد و جریان استفاده شوند.

یک دستگاه همه جانبه شامل قابلیت‌های جمع‌آوری داده، پردازش، ذخیره‌سازی، پایش، جستجو، گزارش‌دهی و مدیریت offense می‌باشد. روند کار هریک از اجزا در بخش‌های بعدی بیان خواهد شد.



شکل ۵۵-٦: مؤلفه‌های جریان و رویداد IBM QRadar

کنسول QRadar با یک کمک‌کننده استقرار به نام «Deployment Editor» به منظور افزودن و پیکربندی مؤلفه‌های استقرار ارائه شده است. توپولوژی و ترکیب یک استقرار QRadar تحت تأثیر قابلیت و ظرفیت این استقرار برای جمع‌آوری، پردازش و ذخیره کلیه داده‌هایی قرار می‌گیرد که مورد تحلیل قرار خواهند گرفت. یک استقرار می‌تواند از لحاظ جغرافیایی توزیع گردد اما ممکن است با اتصال متناوب یا ضعیف به مراکز داده از راه دور تحت تأثیر قرار گیرد. شکل ٤-۲ یک استقرار توزیع شده جغرافیایی از QRadar را نشان می‌دهد.



شکل ۵۵-۷: استقرار توزیع‌شده جغرافیایی IBM QRadar

اغلب منابع پشتیبانی برای مشتریان QRadar فراهم می‌شوند و وابسته به درخواست یا مشکل، مشتریان می‌توانند از کانال‌های پشتیبانی زیر استفاده نمایند:

- فروم مشتری QRadar (جهت پشتیبانی از پاسخگویی به سوالات مشتری)
- مرکز دانش QRadar (برای پشتیبانی از مستندات محصول)
- پایگاه دانش پشتیبانی (پشتیبانی QRadar – کلیه یادداشت‌های فنی)
- پرتال پشتیبانی QRadar (پرتال پشتیبانی رسمی)
- مرکز اصلاح IBM برای QRadar (دانلود نرم‌افزار QRadar)
- لیست نسخه‌های نرم‌افزار اصلی (لیست کلیه نسخه‌های نرم‌افزار و یادداشت‌های انتشار)
- درخواست IBM Security QRadar Request برای بهبود (درخواست ویژگی و بهبودها)
- نرم‌افزارها و لوازم IBM Security QRadar (چرخه پشتیبانی)
- اطلاعیه‌های IBM (ایمیل‌های اطلاعاتی/RSS feeds)
- ویدئوهای پشتیبانی QRadar (مرور لیست پخش برای محتوای QRadar)
- توئیتر پشتیبانی امنیتی IBM (حساب توئیتر QRadar)

۵-۱۱ صدور مجوز[۱]

چون IBM QRadar SIEM یک محصول پیمانه‌ای با گزینه‌های متعدد در هر مؤلفه می‌باشد، صدور مجوز و قیمت‌گذاری به صورت عمومی دردسترس نبوده و معمولاً بستگی به توافق میان IBM و مشتریان آن دارد. با این حال، مقیاس شارژ عموماً براساس استفاده از جمله EPS منابع رویداد FPS شبکه می‌باشد. سازمان‌هایی که علاقمند به درک بهتر گزینه‌ها هستند می‌توانند با برقراری ارتباط با نمایندگی تجاری QRadar SIEM اطلاعات آخرین قیمت‌گذاری را برای کلیه مجوزهای موجود دریافت کنند.

[۱] Licensing

٦ مؤلفه‌های سیستم

٦-١ جمع‌آوری داده

جمع‌آوری داده اولین لایه است که در آن داده رویداد یا جریان از شبکه جمع‌آوری می‌شود. می‌توان از تجهیزات همه‌جانبه به‌منظور جمع‌آوری داده به طور مستقیم از شبکه استفاده کرد، و یا از جمع‌آوری‌کننده‌هایی مانند جمع‌آوری‌کننده رویداد یا QFLow به منظور جمع‌آوری رویداد یا جریان استفاده نمود. داده پیش از آن که به لایه پردازش برسد تجزیه شده و نرمال می‌شود. زمانی‌که داده خام تجزیه می‌گردد، جهت ارائه به صورت قالب مفید و ساخت‌یافته نرمال می‌شود.

عملکرد هسته بر روی جمع‌آوری داده رویداد و جریان تمرکز می‌نماید. داده رویداد، وقایعی را که در نقطه‌ای از محیط کاربر، از جمله ورودهای کاربر، ایمیل، اتصال‌های VPN، انکارهای فایروال، اتصال‌های پروکسی و هر رویداد دیگری که ترجیح داده می‌شود، رخ می‌دهند را در ابزار فایل ثبت رویداد ثبت می‌کند. داده جریان اطلاعات فعالیت شبکه یا اطلاعات نشست میان دو میزبان در شبکه می‌باشد که QRadar به صورت رکوردهای جریان ترجمه می‌نماید. داده‌های خام را به صورت آدرس IP، درگاه‌ها، تعداد بسته‌ها یا بایت‌ها و دیگر اطلاعات به رکوردهای جریان نرمال می‌شوند، که به طور مؤثری یک نشست را میان دو میزبان نشان می‌دهند. به علاوه جمع‌آوری اطلاعات جریان با یک جمع‌آوری‌کننده جریان، ضبط کامل بسته با مؤلفه جرم‌یابی حوادث QRadar[1] موجود است.

٦-٢ پردازش داده

پس از جمع‌آوری داده، لایه دوم یا لایه پردازش داده می‌باشد که در آن داده رویداد و جریان میان موتور قوانین شخصی[2] (CRE) اجرا می‌شوند، که offenseها و هشدارها تولید می‌شوند و سپس داده در محل ذخیره‌سازی نوشته می‌شود. داده‌های رویداد و جریان می‌توانند توسط لوازم همه‌جانبه بدون نیاز به افزودن پردازشگرهای جریان یا رویداد پردازش شوند. اگر ظرفیت پردازش تجهیزات همه‌جانبه بالاتر از حد مجاز باشد، نیاز به

[1] QRadar Incident Forensics component

[2] Custom Rules Engine

افزودن پردازشگرهای رویداد، جریان یا هر ابزار پردازش می‌باشد تا نیازمندی‌های اضافی را مدیریت نمایند. همچنین ممکن است که نیاز به ظرفیت ذخیره‌سازی بیشتری باشد که با افزودن گره‌های داده بیشتر برطرف می‌شود. دیگر ویژگی‌ها از جمله مدیر ریسک QRadar[1] (QRM)، مدیر آسیب‌پذیری QRadar[2](QVM) یا جرم‌یابی حوادث QRadar، انواع داده را جمع‌آوری می‌نمایند و کارکردهای بیشتری را فراهم می‌آورند. مدیریت ریسک QRadar پیکربندی زیرساخت شبکه را جمع‌آوری نموده و یک نقشه از توپولوژی شبکه ارائه می‌دهد. می‌توان از داده به منظور مدیریت ریسک با شبیه‌سازی سناریوهای متنوع شبکه با اصلاح پیکربندی و پیاده‌سازی قوانین در شبکه استفاده نمود. از مدیر آسیب‌پذیری QRadar می‌توان به منظور پایش شبکه و پردازش داده آسیب‌پذیری استفاده کرد، و یا برای مدیریت چیزهایی که از دیگر پویشگرهای امنیتی از جمله Nessus و Rapid7 جمع‌آوری گردیده‌اند، استفاده نمود، که داده‌های فوق برای شناسایی ریسک‌های امنیتی در شبکه مورد استفاده قرار می‌گیرد. از جرم‌یابی حوادث QRadar به منظور انجام تحقیقات جرم‌یابی و انتشار نشست‌های کامل شبکه نیز استفاده می‌شود.

۳-٦ جستجوی داده

در سومین یا بالاترین لایه، داده‌های جمع‌آوری و پردازش شده برای جستجو، تحلیل، گزارش و هشدار یا تحقیقات در خصوص حملات، در دسترس کاربران قرار می‌گیرند. کاربران می‌توانند جستجو کنند و وظایف مدیر امنیتی را برای شبکه از طریق واسط کاربر بر روی کنسول QRadar مدیریت نمایند. در یک سیستم همه‌جانبه، کلیه داده‌ها بر روی تجهیزات همه‌جانبه جمع‌آوری، پردازش و ذخیره می‌شوند. در محیط توزیع شده، کنسول QRadar عملیات ذخیره‌سازی و پردارش رویداد و جریان انجام نمی‌شود، در عوض کنسول در اصل به عنوان واسط کاربر به‌کار می‌رود که کاربران بتوانند از آن برای جستجوها، گزارش‌ها، هشدارها و تحقیقات استفاده نمایند.

[1] QRadar Risk Manager

[2] QRadar Vulnerability Manager

٦-٤ ماژول‌ها و اجزا سیستم

QRadar شامل مؤلفه‌های QRadar Console، QRadar Event Collector، QRadar Event Processor، QRadar QFlow Collector، QRadar Flow Processor و QRadar Data Node می‌باشد که در ادامه هریک به اختصار معرفی می‌شوند.

٦-٤-١ QRadar Console

کنسول QRadar واسط کاربری QRadar، دیدگاه بی‌درنگ جریان و رویداد، گزارش‌ها، حملات، اطلاعات دارایی و کارکردهای مدیریتی را فراهم می‌آورد. در استقرارهای توزیع‌شده QRadar از کنسول جهت مدیریت میزبان‌هایی استفاده می‌شود که شامل دیگر اجزا می‌باشند.

٦-٤-٢ QRadar Event Collector

جمع‌آوری‌کننده رویداد، وقایع را از منابع تولیدکننده رویداد محلی یا راه دور جمع‌آوری نموده و وقایع خام منابع تولید رویداد را به صورت قالب مشخص برای کاربر توسط QRadar نرمال می‌کند. جمع‌آوری‌کننده به منظور صرفه‌جویی در مصرف سیستم، وقایع یکسان را یکپارچه‌سازی یا دسته‌بندی می‌نماید و داده‌ها را به پردازشگر رویداد ارسال می‌کند. در مکان‌های راه دور با لینک‌های کند WAN از جمع‌آوری‌کننده رویداد ١٥٠١ استفاده می‌شود. در عوض، تجهیزات، وقایع را پیش از آنکه به تجهیزات پردازشگر رویداد برای ذخیره‌سازی ارسال شوند، جمع‌آوری و تجزیه می‌کنند. جمع‌آوری‌کننده رویداد می‌تواند از محدودکننده‌های پهنای باند استفاده کند و جهت ارسال وقایع به پردازشگر رویداد برنامه‌ریزی می‌کند تا به محدودیت‌های WAN مانند اتصال متناوب غلبه کند. جمع‌آوری‌کننده رویداد به یک لیسانس EPS تخصیص داده می‌شود که با پردازشگر رویدادی که به آن متصل شده، هماهنگ می‌شود.

٦-٤-٣ پردازشگر رویداد QRadar

پردازشگر رویداد، وقایعی را که از یک یا چند مؤلفه جمع‌آوری‌کننده رویداد جمع‌آوری شده، با استفاده از موتور قوانین سفارشی شده (CRE) پردازش می‌نماید. اگر وقایع با قوانین سفارشی CRE که پیش از این تعریف شده است، هماهنگ باشد، پردازشگر رویداد عملی را که برای پاسخ قانون تعریف نموده است، اجرا می‌کند. هر پردازشگر رویداد دارای ذخیره‌سازی محلی می‌باشد و داده رویداد بر روی پردازشگر یا بر روی یک گره داده ذخیره می‌شود. میزان پردازش برای وقایع توسط لیسانس EPS تعیین می‌گردد. اگر میزان EPS از حد تجاوز نماید، وقایع بافر شده و در صف‌های منابع جمع‌آوری‌کننده رویداد تا زمانی که نرخ EPS کاهش

یابد، نگهداری می‌شود. با این حال، اگر تجاوز از میزان مجاز EPS ادامه یابد و صف پر شود، سیستم رویدادها را دور می‌اندازد و QRadar یک هشدار درباره تجاوز از میزان مجاز EPS ارسال می‌کند. زمانی‌که یک پردازشگر رویداد به یک ابزار همه‌جانبه افزوده می‌شود، تابع پردازش رویداد از همه‌جانبه به پردازشگر رویداد منتقل می‌شود.

٦-٤-٤ جمع‌آوری‌کننده QRadar QFlow

جمع‌آوری‌کننده جریان، جریان را با اتصال به یک درگاه SPAN، یا TAP شبکه جمع‌آوری می‌کند. جمع‌آوری‌کننده QFlow[1] نیز از جمع‌آوری منابع مبتنی بر جریان خارجی مانند NetFlow پشتیبانی می‌کند. جمع‌آوری‌کننده‌های QFlow طوری طراحی نشده‌اند تا به عنوان سیستم‌های ضبط کامل بسته قلمداد شوند. برای ضبط کامل بسته و اطلاعات بیشتر، تنظیمات جرم‌یابی حوادث QRadar[2] را مرور خواهیم کرد. تجهیزات جمع‌آوری‌کننده QFlow ۱۳۱۰ می‌تواند بسته‌ها را به تجهیزات ضبط بسته QRadar ارسال نماید که امکان جمع‌آوری جریان و بسته را از یک منبع بسته منفرد می‌دهد. می‌توان یک جمع‌آوری‌کننده QFlow بر روی سخت‌افزار خود نصب نمود یا از یکی از تجهیزات جمع‌آوری‌کننده QFlow استفاده کرد.

٦-٤-٥ پردازشگر جریان QRadar

پردازشگر جریان، جریان را از یک یا چند ابزار جمع‌آوری‌کننده QFlow پردازش می‌نماید. تجهیزات پردازشگر جریان نیز می‌توانند جریان خارجی شبکه مانند NetFlow، J-Flow و sFlow را به طور مستقیم از مسیریاب‌های شبکه جمع‌آوری کنند. می‌توان از تجهیزات پردازشگر جریان به منظور مقیاس‌بندی استقرار QRadar جهت مدیریت بهتر نرخ جریان در دقیقه[3] (FPM) استفاده نمود. پردازشگرهای جریان شامل پردازشگرهای درونی و ذخیره‌سازی برای داده جریان هستند. زمانی‌که پردازشگر جریان به یک ابزار همه‌جانبه افزوده می‌شود، تابع پردازش از ابزار همه‌جانبه به پردازشگر جریان منتقل می‌گردد.

---

[1] IBM Security QRadar QFlow Collector

[2] QRadar Incident Forensics option

[3] Flows per minute

٦-٤-٦ گره داده QRadar

گره‌های داده استقرار QRadar موجود و جدید را قادر می‌سازند تا به ظرفیت ذخیره‌سازی و پردازش برحسب تقاضا و مورد نیاز بیفزایند. گره‌های داده به افزایش سرعت جستجو در استقرار، با فراهم نمودن منابع سخت‌افزاری بیشتر به منظور اجرای پرس‌وجوهای جستجو، کمک می‌کنند.

٧ نسخه‌های مختلف

مستندات موجود برای محصول IBM Security QRadar ماژول‌ها و عملکردهایی نظیر تهاجم‌ها، جریان، دارایی‌ها، و همبستگی تاریخی را تشریح می‌کنند که ممکن است در همه محصولات QRadar موجود نباشند. وابسته به محصولی که سازمان استفاده می‌کند برخی ویژگی‌های مستند شده ممکن است که در استقرار سازمان موجود نباشد. مرور قابلیت‌ها برای هر محصول کاربران را برای انتخاب مناسب‌تر برحسب نیازهای سازمان راهنمایی می‌کند. در جدول ٦-١ مقایسه‌ای از قابلیت‌های هریک از محصولات ارائه شده است.

جدول ٧٧-١: مقایسه قابلیت‌های QRadar

Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Full administrative capabilities	Yes	No	Yes
Supports hosted deployments	No	Yes	No
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
QRadar Vulnerability Manager integration	Yes	Yes	Yes
Network activity monitoring	Yes	No	No
Asset profiling	Yes	Yes	No [1]
Offenses management	Yes	Yes	No
Network flow capture and analysis	Yes	Yes	No
Historical correlation	Yes	Yes	No
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No

[1] QRadar Log Manager only tracks asset data if QRadar Vulnerability Manager is installed.

۷-۱-۱ مدیر فایل ثبت رویداد IBM QRadar[۱]

مدیریت فایل‌های ثبت وقایع و رویداد IBM QRadar یک راه‌حل پایه، کارایی بالا و مقیاس‌پذیر برای جمع‌آوری، تحلیل، ذخیره‌سازی و گزارش‌دهی حجم زیادی از فایل‌های ثبت رویداد امنیتی و شبکه می‌باشد.

۷-۱-۲ IBM Security QRadar SIEM

QRadar SIEM پیشنهادی پیشرفته است که شامل مقیاس وسیعی از قابلیت‌های هوشمندی امنیتی برای استقرارهای داخل سازمان می‌باشد. این راه‌حل، داده منابع رویداد و جریان شبکه را از هزاران دارایی شبکه، تجهیزات، و نقاط پایانی، یکپارچه[۲] می‌کند. این دارایی‌ها در شبکه توزیع‌شده‌اند و فعالیت‌های همبستگی و نرمال‌سازی فوری روی داده‌های خام را به منظور تشخیص تهدیدات واقعی از نادرست‌های مثبت انجام می‌دهند.

۷-۱-۳ IBM QRadar بر روی ابر[۳]

QRadar بر روی بستر ابری برای سطوح حرفه‌ای امنیت امکان مدیریت زیرساخت را فراهم می‌کند در حالی که تحلیلگران امنیتی وظایف تشخیص تهدید و مدیریت را انجام می‌دهند. می‌توان شبکه و بستر ارتباطی را محافظت نمود.

---

[۱] IBM QRadar Log Manager

[۲] Consolidates

[۳] IBM QRadar on Cloud