IBM QRadar: Propriedades de Evento, Coalescência e Encaminhamento

Material técnico expandido e traduzido — Segurança da Informação e Administração de SIEM

Contexto

Este material corresponde à segunda parte do curso introdutório sobre o processamento de eventos no IBM QRadar. Ele aborda três pilares essenciais da configuração e operação do SIEM: as Propriedades de Evento Personalizadas (Custom Event Properties – CEPs), a Coalescência de Eventos (Event Coalescing) e o Encaminhamento de Eventos (Event Forwarding). Cada um desses mecanismos aprimora a forma como o QRadar interpreta, organiza e distribui as informações provenientes de diversas fontes de log e dispositivos de segurança.

O objetivo desses recursos é permitir que os administradores adaptem o comportamento do SIEM às características específicas de seu ambiente, garantindo uma coleta e análise eficiente, minimizando ruídos e otimizando a capacidade de correlação e resposta a incidentes. Esses conceitos são a base da inteligência operacional do QRadar.

Desafios

Em ambientes corporativos complexos, os principais desafios estão relacionados à diversidade dos formatos de logs e à necessidade de extrair informações relevantes que não são interpretadas nativamente pelos DSMs (Device Support Modules). Sem uma definição adequada de propriedades personalizadas, muitos campos importantes — como IDs de ameaças, nomes de vírus ou parâmetros de APIs — podem permanecer invisíveis para as regras de correlação.

Outro desafio recorrente é o balanceamento entre performance e detalhamento. A coalescência, por exemplo, reduz o número de registros processados, mas exige que os analistas compreendam como eventos consolidados são apresentados. Por fim, o roteamento e o encaminhamento de eventos requerem cuidado para evitar duplicidade de dados, perda de registros ou configurações de filtragem que prejudiquem a visibilidade do SOC.

Conceitos Fundamentais

Propriedades de Evento Personalizadas (Custom Event Properties - CEPs)

As CEPs permitem que o QRadar extraia informações específicas de um evento que o DSM padrão não interpreta. Essas propriedades podem ser criadas manualmente a partir da aba *Log Activity*, onde o administrador seleciona um evento, inspeciona seu payload e usa a função *Extract Property* para definir o elemento desejado. O QRadar oferece três modos principais de extração: *Extraction-based* (regex, JSON, XML), *Calculation-based* (operações numéricas sobre propriedades existentes) e *AQL-based* (combinação de múltiplas expressões).

Por exemplo, se um evento contém um campo 'ThreatID' não reconhecido, é possível criar uma propriedade personalizada para extraí-lo e usá-lo em regras, relatórios e correlações. A definição pode incluir o tipo de dado (texto, número, endereço IP, data, etc.), descrição e ativação para uso em indexação e pesquisas. No DSM Editor, essas propriedades também podem ser visualizadas, modificadas ou substituídas por expressões regulares (regex) geradas automaticamente a partir do payload.

Coalescência de Eventos (Event Coalescing)

A coalescência é um mecanismo que agrupa múltiplos registros de evento semelhantes em uma única entrada, reduzindo o volume de dados processados e armazenados. Esse recurso é particularmente útil em situações de alta repetição, como ataques de negação de serviço (DoS), onde milhares de eventos idênticos podem ser condensados em poucos registros.

O QRadar compara propriedades como QID, IP de origem e destino, entre outras, para determinar se os eventos podem ser coalescidos. Após receber três eventos idênticos em um intervalo de 10 segundos, o

sistema agrupa os subsequentes no mesmo registro consolidado. Isso mantém o desempenho do SIEM sem perder a visibilidade contextual. As regras e ofensas continuam a ser avaliadas sobre eventos individuais e coalescidos.

Encaminhamento e Roteamento de Eventos (Event Forwarding & Routing Rules)

O QRadar permite encaminhar eventos para outros sistemas ou instâncias de QRadar por meio de regras de encaminhamento e roteamento. Essa funcionalidade é configurada no *Admin Console*, nas opções *Store and Forward* e *Routing Rules*. O recurso é utilizado tanto para redundância de dados quanto para integração com plataformas externas, como sistemas de *ticketing* e *alerting*.

É possível agendar a coleta e o envio de dados com limitação de banda e janelas de transmissão específicas, ideal para ambientes com conectividade intermitente. As regras de roteamento permitem definir filtros, como 'Encaminhar apenas eventos de firewall' ou 'Descartar eventos antes da correlação'. Modos de operação incluem *Drop*, *Bypass Correlation* e *Log Only*, que influenciam diretamente a forma como os dados são armazenados e correlacionados.

Arquitetura do Processamento de Eventos

O pipeline de eventos do QRadar é composto por múltiplas camadas: coleta (Event Collector), processamento (Event Processor), correlação (Magistrate) e armazenamento (Ariel Database). Em cada etapa, as CEPs, a coalescência e o roteamento influenciam o comportamento do sistema. A criação de propriedades personalizadas ocorre no nível de parsing, enquanto a coalescência atua no momento da normalização e armazenamento.

O módulo *Custom Rules Engine* (CRE) é responsável por avaliar as regras sobre eventos coalescidos e brutos, garantindo que nenhuma detecção crítica seja perdida. O componente *Event Forwarder* utiliza protocolos padronizados (Syslog, TCP, UDP, TLS) para enviar eventos em tempo real ou de forma agendada para outros destinos.

Modelos de Uso

• **Ambientes Corporativos:** CEPs são usadas para normalizar logs de aplicações internas, coalescência para otimizar performance e roteamento para integração com sistemas de helpdesk. • **MSSPs (Managed Security Service Providers):** utilizam encaminhamento seletivo e regras de roteamento para isolar clientes em multi-tenancy. • **Infraestruturas Críticas:** coalescência configurada para reduzir impacto de eventos massivos sem perda de contexto.

Benefícios

Esses mecanismos em conjunto proporcionam maior eficiência, escalabilidade e precisão analítica. As CEPs ampliam a capacidade de detecção do QRadar; a coalescência otimiza o desempenho e armazenamento; e o roteamento garante redundância e interoperabilidade com outras plataformas de segurança. A combinação correta desses recursos torna a operação do SOC mais enxuta e resiliente.

Recursos Avançados e Boas Práticas

1. Automatize a criação de CEPs usando APIs REST do QRadar. 2. Documente regex e propriedades personalizadas em repositórios versionados. 3. Utilize coalescência de forma seletiva, priorizando fontes de alta frequência. 4. Defina janelas de encaminhamento em períodos de baixa atividade de rede. 5. Revise periodicamente regras de roteamento para evitar sobrecarga e redundância.

Conclusão

O domínio dos conceitos de Propriedades Personalizadas, Coalescência e Encaminhamento é essencial para extrair o máximo potencial do IBM QRadar. Esses recursos, quando bem aplicados, permitem customização profunda, economia de recursos e melhor integração com o ecossistema de segurança da organização. São pilares indispensáveis para a maturidade operacional de qualquer SOC moderno.