IBM QRadar – Domínios e Locatários (Tenants)

Contexto

O IBM QRadar é uma solução SIEM (Security Information and Event Management) projetada para centralizar, analisar e correlacionar eventos de segurança em ambientes corporativos complexos. Dentro dessa arquitetura, os conceitos de **Domínios (Domains)** e **Locatários (Tenants)** desempenham um papel essencial para permitir **segmentação lógica, isolamento de dados e administração multiusuário**. Isso é particularmente útil em ambientes que atendem múltiplas unidades organizacionais, filiais, clientes ou serviços gerenciados (MSSPs).

Conceito de Domínios

Os **Domínios** no QRadar funcionam como partições lógicas que segregam dados, ativos, regras e relatórios dentro de um mesmo ambiente. Um domínio é identificado por tags (Domain Tags) adicionadas aos eventos e fluxos assim que estes passam pelo pipeline de eventos. Essa tagagem é uma forma de **metadado** que permite que o sistema saiba a qual parte lógica do ambiente aquele dado pertence.

Os domínios são úteis para lidar com **endereços IP sobrepostos**, **fusões corporativas**, ou quando há a necessidade de **segmentar áreas internas da empresa** (por exemplo, produção, finanças, engenharia). Cada domínio pode manter suas próprias ofensas, correlações e pesquisas, garantindo que os eventos de uma área não afetem outras. Isso proporciona **isolamento operacional** e **melhora a precisão na resposta a incidentes**.

Áreas de Uso dos Domínios

Os domínios são amplamente utilizados em múltiplos componentes do QRadar, como eventos, fluxos, ativos, hierarquia de rede, regras, ofensas, pesquisas, perfis de segurança e dados de vulnerabilidade. Além disso, afetam mecanismos avançados como o gerenciamento de índices e backup/recovery, garantindo que todos os processos respeitem os limites de domínio estabelecidos.

Processo de Tagging e Critérios de Avaliação

O **Domain Tagging** ocorre durante o processamento de eventos e fluxos. O QRadar utiliza uma ordem de precedência para determinar o domínio ao qual cada evento pertence, considerando critérios como propriedades personalizadas (Custom Event Properties), fontes de log, grupos de fontes e coletores de eventos. O primeiro critério que corresponder define o domínio do evento. Caso nenhuma correspondência seja encontrada, o evento é atribuído ao domínio padrão (Default Domain).

Regras de Domínio e Correlação

O mecanismo de correlação do QRadar (Custom Rules Engine) permite criar diferentes tipos de regras com base em domínios. Existem quatro categorias principais: **regras

não cientes de domínio**, **regras de domínio único**, **regras de múltiplos domínios** e **regras de dados compartilhados**. Cada tipo define como os contadores de regras e as ofensas são criadas e segregadas.

Por exemplo, uma **regra de domínio único** será aplicada apenas aos eventos marcados com o domínio específico, enquanto uma **regra de dados compartilhados** considera todos os domínios e cria uma ofensa global. Essa flexibilidade é essencial para MSSPs e ambientes corporativos complexos, permitindo **correlação granular** ou **agregada** conforme a necessidade.

Conceito de Locatários (Tenants)

Os **Tenants** são subconjuntos de um domínio e representam entidades ou clientes individuais dentro de uma implantação multiusuário. O QRadar utiliza locatários para aplicar **limites de licença, políticas de retenção de dados e segregação administrativa**. Cada tenant pode ter múltiplos domínios associados, e suas configurações podem incluir limitações de eventos por segundo (EPS) e fluxos por minuto (FPM).

Essa abordagem é crucial para **Managed Security Service Providers (MSSPs)** que administram diversos clientes a partir de uma única instalação do QRadar. Cada locatário visualiza apenas seus próprios dados e relatórios, mantendo a privacidade e a conformidade. A separação de armazenamento é feita através de **buckets de retenção**, armazenados em diretórios específicos sob `/store/ariel/events/payloads/aux/`.

Administração Delegada e Perfis de Segurança

O QRadar implementa um modelo de **administração delegada**, onde administradores de locatários (tenant admins) têm permissões limitadas para gerenciar seus próprios domínios, usuários e regras. No entanto, certas ações – como a criação de propriedades personalizadas complexas – permanecem restritas ao administrador global, para evitar impacto na performance geral do pipeline de eventos.

Os **perfis de segurança (Security Profiles)** definem quais domínios e locatários um usuário pode acessar. Um perfil pode ter acesso a todos os domínios ("All Domains") ou a um subconjunto específico. Isso assegura que apenas usuários autorizados possam visualizar dados sensíveis e operar dentro de seus limites definidos.

Benefícios e Desafios da Segmentação com Domínios e Tenants

A arquitetura de domínios e tenants proporciona **isolamento de dados**, **segurança operacional**, e **eficiência no gerenciamento de múltiplos clientes ou departamentos**. Permite conformidade com normas de proteção de dados, reduz riscos de exposição cruzada e facilita o monitoramento segmentado. Entretanto, exige **planejamento cuidadoso de hierarquias, rate limits e políticas de retenção**, além de garantir que as regras de correlação respeitem a estrutura de domínios e locatários configurada.

Conclusão

O uso combinado de **Domínios e Tenants no QRadar** representa uma das formas mais eficazes de gerenciar grandes infraestruturas de segurança em ambientes complexos. Essa arquitetura suporta múltiplos clientes, unidades de negócio e contextos operacionais sem comprometer a integridade ou o desempenho do sistema. A aplicação adequada dessas práticas garante **controle granular, escalabilidade e conformidade**, pilares fundamentais de qualquer operação de segurança moderna baseada em SIEM.