# IBM QRadar – Domínios e Tenants Explicado e Aplicado

## 1. Contexto e Introdução

O **IBM QRadar** é uma plataforma de **SIEM (Security Information and Event Management)** que oferece uma visão centralizada e abrangente sobre eventos de segurança em uma infraestrutura corporativa. Em organizações complexas ou distribuídas, a necessidade de isolar, segmentar e delegar visibilidade torna-se crítica. É nesse contexto que entram os conceitos de **Domínios** e **Tenants**, responsáveis por garantir segregação lógica, governança e eficiência operacional no QRadar.

Esses mecanismos permitem que diferentes unidades de negócio, filiais, departamentos ou até clientes compartilhem uma mesma infraestrutura SIEM, sem comprometer a confidencialidade ou a autonomia de gestão. Dessa forma, o QRadar se torna uma solução eficaz tanto para empresas privadas de grande porte quanto para provedores de serviços gerenciados (MSSPs), que precisam monitorar ambientes de múltiplos clientes simultaneamente.

## 2. Conceito de Domínios no QRadar

Um **Domínio** no QRadar é uma subdivisão lógica que agrupa ativos, eventos e fluxos dentro de um mesmo contexto operacional. Cada domínio define quais dados são visíveis e processados para um grupo específico de usuários, o que garante controle granular sobre a informação. Os domínios funcionam como “janelas de visibilidade” que filtram eventos e ofensas de acordo com regras de associação baseadas em IPs, sub-redes ou propriedades de ativos.

Por exemplo, uma corporação com filiais em diferentes países pode criar um domínio para cada unidade. Analistas de segurança em São Paulo só verão eventos da filial paulista, enquanto o time global de segurança pode visualizar todos os domínios. Essa abordagem aumenta a eficiência e a confidencialidade, ao mesmo tempo em que reduz o ruído de alertas não relacionados ao escopo de atuação de cada equipe.

## 3. Estrutura de Tagging e Hierarquia de Rede

A estrutura de **tagging** do QRadar é o mecanismo que associa dispositivos e eventos a um domínio. Cada ativo configurado no QRadar pode ser vinculado a um ou mais domínios, e os eventos gerados por esses ativos herdam automaticamente essa associação. Esse processo é transparente e garante que, desde o momento da ingestão do log, o domínio correto seja atribuído ao evento, mantendo a integridade da segregação lógica.

Além disso, o QRadar suporta hierarquia de domínios. Um domínio “pai” pode conter diversos domínios “filhos”, permitindo que administradores corporativos mantenham uma visão consolidada, enquanto delegam a operação de domínios regionais ou setoriais. Essa estrutura hierárquica é amplamente utilizada em grandes instituições financeiras, empresas multinacionais e órgãos governamentais com operações

distribuídas.

## 4. Correlação e Avaliação Multi-Domínio

No QRadar, o motor de correlação (Custom Rules Engine – CRE) pode operar dentro de contextos de domínio. Isso significa que as regras podem ser configuradas para agir em domínios específicos ou em todos os domínios simultaneamente. Essa flexibilidade é essencial em ambientes com diferentes requisitos de segurança, pois evita que um evento de baixo impacto em um domínio gere alertas indevidos em outro.

O componente **Magistrate** é responsável por gerenciar as ofensas geradas e garantir que a correlação entre eventos ocorra de forma coerente dentro dos limites de cada domínio. Isso assegura que as investigações de incidentes não se sobreponham e que as métricas de desempenho e severidade sejam mantidas de forma independente.

## 5. Multi-Tenancy e Isolamento Lógico

O **Multi-Tenancy** no QRadar é a capacidade de suportar múltiplas entidades (tenants) dentro de uma única infraestrutura compartilhada. Cada tenant representa uma organização ou cliente isolado, com suas próprias regras de correlação, relatórios, usuários e domínios. Essa funcionalidade é amplamente empregada em MSSPs, que precisam gerenciar simultaneamente vários clientes sem comprometer a confidencialidade dos dados.

No nível técnico, o QRadar implementa camadas de isolamento lógico que separam completamente as informações de cada tenant. Os administradores podem definir quais domínios pertencem a cada tenant e quais usuários têm acesso a eles. Isso garante que nem mesmo metadados ou estatísticas de um cliente sejam visíveis a outro, preservando conformidade com normas como a **LGPD**, **GDPR** e **ISO 27001**.

## 6. Perfis de Usuário e Acesso Delegado

O QRadar utiliza um modelo de controle de acesso baseado em papéis (RBAC – Role-Based Access Control). Cada usuário é associado a um ou mais papéis que definem suas permissões dentro dos domínios e tenants. Isso inclui visibilidade de ofensas, capacidade de criação de regras, acesso a dashboards e relatórios, entre outros recursos.

Essa abordagem possibilita a delegação eficiente de responsabilidades, permitindo que analistas regionais, engenheiros de segurança e administradores globais atuem simultaneamente no mesmo ambiente, mas com níveis distintos de acesso. A integração com sistemas de autenticação centralizada, como **LDAP** e **Active Directory**, facilita a sincronização de perfis e reforça o controle de segurança.

## 7. Benefícios e Conclusão

Os conceitos de **Domínios e Tenants** tornam o QRadar uma solução escalável e adaptável para diferentes realidades organizacionais. Ao permitir a segregação lógica de dados e o controle granular de acesso, o QRadar melhora a eficiência operacional,

reduz a sobrecarga de alertas e mantém a conformidade com requisitos legais e normativos.

Em resumo, o domínio e o tenant são pilares estruturais da governança de segurança no QRadar. Seu uso adequado possibilita que equipes trabalhem de maneira autônoma e coordenada, preservando a confidencialidade e garantindo que o SIEM opere de forma otimizada mesmo em ambientes altamente complexos e distribuídos.