IBM QRadar – Domínios e Locatários (Tenants)

Contexto

O IBM QRadar é uma das plataformas de SIEM (Security Information and Event Management) mais avançadas e difundidas no mercado corporativo. Seu objetivo central é correlacionar, armazenar e analisar eventos de segurança provenientes de diferentes fontes dentro de uma infraestrutura de TI. Em ambientes corporativos modernos, onde coexistem múltiplas redes, departamentos e clientes, a necessidade de segmentação lógica e de isolamento de dados é primordial. É nesse contexto que emergem os conceitos de **Domínios (Domains)** e **Locatários (Tenants)**, elementos estruturais que permitem ao QRadar manter organização, segurança e governança em larga escala.

Em um cenário empresarial complexo, o SIEM deve ser capaz de distinguir entre fluxos de dados provenientes de diferentes unidades de negócio ou de clientes independentes. O QRadar resolve esse desafio utilizando domínios e locatários como mecanismos de separação e controle. Essa abordagem garante que eventos de segurança, ativos, fluxos de rede, regras e ofensas sejam tratados dentro de seus respectivos contextos administrativos, evitando sobreposição de informações e preservando a integridade da análise de segurança.

Fundamentos Teóricos

Os fundamentos por trás da implementação de domínios e locatários no QRadar estão ancorados nos princípios clássicos da segurança da informação: **confidencialidade, integridade e disponibilidade (CIA Triad)**, bem como na necessidade de segregação lógica e de controle de acesso granular. Do ponto de vista teórico, um domínio representa uma unidade de compartimentalização de dados. Ele cria uma barreira lógica que impede que informações provenientes de uma área organizacional se misturem com as de outra. Esse modelo reflete o conceito de “zonas de confiança” em arquitetura de segurança, onde cada zona possui regras próprias de monitoramento, autenticação e auditoria.

A criação de domínios permite ao QRadar estruturar internamente a correlação de eventos de modo independente. Isso significa que as ofensas geradas em um domínio não interferem na contagem de regras ou nos indicadores de outro. Esse comportamento reforça a integridade dos resultados de correlação e evita falsos positivos entre ambientes distintos. Em essência, o domínio atua como um **espaço de segurança isolado**, mas integrado, dentro da infraestrutura global do QRadar.

Os locatários (tenants), por sua vez, estendem essa segregação para um nível administrativo superior. Enquanto os domínios lidam com a separação de dados e eventos, os locatários tratam da separação de políticas, licenças e responsabilidades operacionais. Cada tenant pode representar um cliente, uma divisão corporativa ou uma unidade administrativa. A hierarquia de locatários permite o uso do QRadar em

contextos **multiusuário e multiempresa**, sem comprometer a confidencialidade dos dados entre entidades distintas.

Arquitetura e Funcionamento dos Domínios

Dentro da arquitetura do QRadar, o processo de atribuição de domínios ocorre por meio do chamado **Domain Tagging**, um mecanismo automatizado que insere metadados em cada evento ou fluxo assim que ele percorre o pipeline de processamento. Esse pipeline envolve etapas como parsing, coalescência, enriquecimento e correlação. O domínio é determinado com base em uma **ordem de precedência**, que segue critérios definidos: propriedades de evento personalizadas (Custom Event Properties), fontes de log, grupos de log sources e coletores de eventos. Assim, o sistema assegura que cada evento seja devidamente associado ao domínio correto antes de entrar na camada de correlação e armazenamento.

Essa associação é crucial, pois determina como as regras de correlação são aplicadas. Por exemplo, em uma arquitetura com múltiplas redes sobrepostas, dois dispositivos diferentes podem compartilhar o mesmo endereço IP. Sem o domínio, o QRadar não seria capaz de distinguir a origem real desses eventos. Com a aplicação de tags de domínio, o sistema sabe que o endereço 192.168.100.100 pode representar um servidor Linux em um domínio e um servidor Windows em outro, permitindo análises independentes e precisas.

Regras de Correlação em Ambientes Multi-Domínio

O mecanismo de correlação do QRadar é altamente sensível à estrutura de domínios. Cada regra, seja genérica ou específica, é avaliada dentro do contexto do domínio a que pertence o evento. Existem quatro categorias principais: regras não cientes de domínio, de domínio único, de múltiplos domínios e de dados compartilhados. Essa diferenciação permite à equipe de segurança definir o escopo de atuação das correlações de forma granular.

Nas **regras não cientes de domínio**, os contadores são mantidos separadamente para cada domínio, mas a lógica é idêntica. Já nas **regras de domínio único**, somente os eventos pertencentes a um domínio específico podem ativar a condição de alerta. As **regras de múltiplos domínios** permitem correlação entre diferentes domínios, mantendo a separação lógica dos contadores e ofensas. Por fim, as **regras de dados compartilhados** combinam dados de todos os domínios, gerando uma ofensa unificada marcada como “All Domains”. Esse modelo reflete a maturidade da arquitetura de correlação do QRadar.

Gestão de Locatários (Tenants) e Administração Delegada

Os locatários no QRadar são responsáveis por estabelecer o controle administrativo de ambientes multiempresa. Um tenant possui sua própria hierarquia de rede, limites de licença, buckets de retenção de dados e parâmetros de limitação de taxa (Eventos por Segundo – EPS, e Fluxos por Minuto – FPM). Essa granularidade permite que administradores configurem políticas específicas sem interferir em outros locatários do

sistema. Em implementações de MSSP (Managed Security Service Provider), isso garante que cada cliente opere de forma isolada e segura, mesmo utilizando a mesma infraestrutura física do SIEM.

A administração delegada é outro pilar do modelo multi-tenant. Administradores locais (delegated admins) podem criar e gerenciar regras, relatórios e dashboards dentro de seus próprios domínios, mas não têm permissão para alterar configurações que afetem o desempenho global. Essa limitação é intencional, uma vez que propriedades personalizadas mal otimizadas podem impactar todo o pipeline de eventos. Assim, o QRadar equilibra flexibilidade operacional com segurança de desempenho, garantindo estabilidade mesmo em ambientes de alta densidade de dados.

Relação com Políticas de Segurança e Compliance

A estrutura de domínios e locatários no QRadar está alinhada com práticas de conformidade e governança exigidas por normas internacionais como a **ISO/IEC 27001**, **NIST 800-53** e a **LGPD (Lei Geral de Proteção de Dados)**. A segmentação lógica proporcionada pelos domínios assegura que o princípio do menor privilégio (Least Privilege) e o controle de acesso baseado em funções (RBAC) sejam aplicados de forma rigorosa. Além disso, a existência de locatários independentes facilita auditorias e a rastreabilidade de incidentes, permitindo identificar responsabilidades administrativas e técnicas.

Conclusão

Os conceitos de **Domínios e Locatários no IBM QRadar** representam a base da escalabilidade e da segurança em implementações de grande porte. Por meio deles, é possível atingir níveis elevados de isolamento, controle e governança sem comprometer o desempenho do sistema. A separação lógica de dados não apenas reforça a segurança operacional, mas também permite que o QRadar seja utilizado como uma plataforma unificada para múltiplas organizações, consolidando seu papel como uma das soluções mais completas do mercado de SIEM.