# IBM QRadar: Estrutura e Planejamento da Hierarquia de Rede (Network Hierarchy Structure)

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

## Contexto

A Hierarquia de Rede (Network Hierarchy) no IBM QRadar é uma ferramenta estratégica de classificação e organização dos endereços IP, sub-redes e grupos de rede que compõem o ambiente monitorado. Ela não precisa refletir a topologia física da rede, mas sim ser estruturada de acordo com a forma como a equipe de segurança visualiza e analisa os eventos. O objetivo é permitir uma segmentação lógica e funcional dos ativos, facilitando a criação de regras de correlação, relatórios e buscas precisas.

Durante o planejamento, o administrador deve considerar como os grupos de rede serão usados nas análises e testes do sistema. A estrutura ideal depende da maturidade da organização e do tipo de visibilidade que se deseja obter — seja por funções de sistema, unidades de negócio ou localizações geográficas.

## Desafios

O maior desafio ao estruturar a hierarquia de rede está em equilibrar detalhamento e manutenção. Quanto mais granular for a definição dos objetos e grupos, mais fácil será criar regras e relatórios específicos; contudo, a atualização contínua da hierarquia torna-se mais complexa. Em ambientes dinâmicos, onde ativos e servidores são frequentemente adicionados ou reconfigurados, manter a consistência da hierarquia é um trabalho crítico para garantir a integridade dos dados e a eficácia das correlações.

Outro desafio é a padronização de nomes e descrições. Grupos e objetos mal nomeados dificultam a análise e podem gerar confusões durante a escrita de regras. Além disso, administradores precisam decidir se os objetos serão definidos por faixas CIDR amplas ou por IPs específicos — a segunda opção oferece maior precisão, mas aumenta o esforço de manutenção. Por exemplo, um grupo 'Mail Servers' que lista IPs específicos exige atualização toda vez que um servidor de e-mail é adicionado ou removido.

## Conceitos Fundamentais

### *Hierarquia Lógica vs. Física*

A estrutura de hierarquia de rede não precisa replicar a topologia física da infraestrutura. Em vez disso, deve representar uma visão lógica orientada à análise de segurança. Isso significa agrupar redes de forma que facilite a investigação de incidentes e o monitoramento de comportamentos. Por exemplo, um grupo 'Infraestrutura Crítica' pode reunir servidores de DNS, autenticação e controle de acesso, mesmo que fisicamente estejam em diferentes data centers.

Esse modelo lógico torna as buscas e relatórios mais intuitivos. Em vez de consultar dezenas de sub-redes dispersas, o analista pode concentrar-se em grupos que representam contextos operacionais — como 'Financeiro-Europa' ou 'Produção-Brasil'.

### *Critérios para Agrupamento*

O agrupamento de redes pode seguir diferentes critérios, sendo os mais comuns: funções de sistema (servidores, firewalls, endpoints), unidades de negócio (RH, TI, Vendas) e localização geográfica (América do Norte, EMEA, APAC). Essa abordagem facilita a aplicação de políticas de segurança específicas e a criação de regras de correlação contextualizadas. Por exemplo, um analista pode comparar o tráfego de servidores Active Directory do departamento financeiro em Cincinnati com os de Belfast, esperando comportamentos semelhantes.

Diferenças de comportamento entre esses grupos podem indicar anomalias — como tentativas de acesso fora do horário comercial, picos de autenticação ou comunicações entre objetos que normalmente não interagem. Esses padrões são facilmente identificáveis quando a hierarquia de rede está bem estruturada.

### *Diretrizes de Definição*

O QRadar recomenda seguir boas práticas ao definir a hierarquia de rede: incluir todas as faixas CIDR privadas e públicas da organização; nomear grupos e objetos de forma descritiva e consistente; criar grupos abrangentes que englobem subgrupos; e definir políticas precisas quando necessário. A precisão na estrutura da hierarquia melhora diretamente a eficiência das regras e relatórios do SIEM.

Entretanto, o nível de detalhamento deve estar alinhado à capacidade operacional da equipe. Um modelo excessivamente detalhado, sem processo de atualização automatizado, pode levar a inconsistências e perda de visibilidade sobre os ativos mais recentes.

## Arquitetura da Hierarquia de Rede

A hierarquia de rede no QRadar é acessada pelo console administrativo (Admin Console) e armazenada no banco de configuração. Cada objeto contém um ou mais blocos de endereços CIDR. Os grupos podem ser hierarquizados, permitindo subgrupos dentro de estruturas principais — por exemplo: 'Corporação.Finanças.Europa'. Essa hierarquia lógica é usada internamente pelo mecanismo de correlação e pelas buscas AQL (Ariel Query Language).

O modelo hierárquico também serve como base para recursos como perfis de segurança (Security Profiles), domínios e comportamentos esperados de rede. Cada evento e fluxo coletado pelo QRadar é avaliado em função de seu contexto hierárquico, permitindo que regras sejam escritas para detectar desvios dentro de grupos específicos.

## Modelos de Uso

• **Modelo por Função:** agrupa ativos conforme sua função técnica (servidores, firewalls, endpoints). Ideal para SOCs focados em detecção técnica. • **Modelo por Unidade de Negócio:** organiza a hierarquia segundo a estrutura corporativa (TI, RH, Finanças), permitindo visibilidade por área. • **Modelo Geográfico:** útil em empresas multinacionais, facilita comparações entre regiões e detecção de desvios comportamentais regionais. • **Modelo Híbrido:** combina os anteriores, com grupos geográficos contendo subgrupos funcionais.

## Benefícios

Uma hierarquia de rede bem projetada melhora a visibilidade, reduz ruídos analíticos e aumenta a precisão das correlações. Ela permite comparar comportamentos entre regiões ou departamentos, identificar comunicações anômalas e aplicar políticas de segurança de forma seletiva. Além disso, torna as investigações forenses mais rápidas, pois as buscas AQL e os relatórios são otimizados por grupos lógicos.

Do ponto de vista operacional, uma hierarquia bem estruturada também facilita a integração com domínios e tenants no QRadar, refletindo a organização real da empresa e suas fronteiras de responsabilidade. Isso é especialmente importante para MSSPs e grandes ambientes corporativos com múltiplos times de segurança.

## Recursos Avançados e Boas Práticas

1. Automatize atualizações da hierarquia via APIs REST do QRadar. 2. Padronize nomenclaturas e descrições para garantir clareza nas buscas e relatórios. 3. Combine faixas CIDR com IPs individuais para granularidade seletiva. 4. Utilize scripts de verificação para identificar sobreposições ou CIDRs órfãos. 5. Documente a estrutura hierárquica e mantenha versões exportadas periodicamente para auditoria e restauração rápida.

## Conclusão

A hierarquia de rede é um dos pilares da administração do QRadar, pois conecta o contexto de rede com a inteligência de correlação de eventos. Ela traduz a topologia lógica da organização em um modelo analítico, facilitando detecção, resposta e governança. Uma estrutura bem planejada proporciona uma visão holística e reduz o tempo de análise em operações de segurança. Investir na criação e manutenção da hierarquia de rede é essencial para alcançar eficiência e maturidade no SOC.