IBM QRadar: Fundamentos da Hierarquia de Rede (Network Hierarchy)

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

Contexto

A 'Network Hierarchy' do IBM QRadar é um componente essencial da configuração do SIEM, localizado no console de administração (Admin Console). Ela define as faixas de endereços CIDR que compõem a rede da organização, permitindo ao QRadar distinguir entre tráfego local (interno) e remoto (externo). Essa diferenciação é fundamental para a correta análise de eventos e fluxos, possibilitando correlações mais precisas e a detecção eficiente de ameaças direcionadas ao ambiente corporativo.

Por meio da hierarquia de rede, administradores podem agrupar faixas de IP em objetos lógicos, refletindo a estrutura física ou lógica da rede real. Essa modelagem serve como base para várias funcionalidades internas do QRadar, incluindo regras de correlação, relatórios, análises de vulnerabilidade, classificação de ativos e ofensas. Além disso, diversos blocos de construção (building blocks) e regras padrão dependem dessas definições.

Desafios

Um dos desafios mais críticos no uso da Network Hierarchy é manter a consistência entre a topologia real da rede e a configuração declarada no QRadar. Quando novas sub-redes são adicionadas sem atualização do modelo, o SIEM pode classificar erroneamente eventos como externos, prejudicando a análise e a priorização de ofensas. Outro problema recorrente é a sobreposição de faixas CIDR, especialmente em ambientes com múltiplos domínios, o que exige cuidado para evitar redundâncias e conflitos.

Além disso, administradores precisam compreender o impacto de modificar ou remover objetos da hierarquia padrão. Como muitos blocos e regras utilizam essas referências internamente, qualquer alteração indevida pode afetar a lógica de correlação e a geração de ofensas. Por isso, recomenda-se sempre revisar as regras e building blocks associados antes de realizar mudanças estruturais na hierarquia de rede.

Conceitos Fundamentais

CIDR e Objetos de Rede

Cada objeto de rede dentro da hierarquia é composto por uma ou mais faixas CIDR (Classless Inter-Domain Routing), que definem blocos de endereços IP. Um CIDR pode pertencer apenas a um objeto de rede por domínio, garantindo que não haja ambiguidade na classificação de tráfego. No entanto, conjuntos diferentes de CIDRs podem coexistir em objetos distintos dentro do mesmo domínio, desde que não se sobreponham.

O QRadar sempre faz correspondência (matching) com a faixa mais específica disponível. Por exemplo, um endereço individual (como 192.168.1.5/32) tem precedência sobre uma faixa ampla (192.168.0.0/16). Essa precisão é essencial para o correto mapeamento de ativos e a identificação do contexto de origem e destino dos eventos.

Grupos de Rede e Organização Hierárquica

Os grupos de rede permitem organizar objetos de forma lógica e hierárquica. É possível criar grupos e subgrupos seguindo uma convenção de nomes com pontos, por exemplo: 'Corp.Infraestrutura.Servidores'. Essa estrutura em camadas facilita a administração e o uso em regras de correlação, pois cada grupo pode representar um nível de granularidade diferente da rede corporativa.

Um grupo padrão, denominado 'net-10-172-192', inclui as faixas privadas mais comuns (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Esse grupo serve para detectar tráfego interno não autorizado, como dispositivos que utilizam endereços privados não mapeados no inventário ou varreduras (scans) em faixas inexistentes.

Arquitetura e Funcionamento

A Network Hierarchy é aplicada em todo o pipeline de eventos e fluxos do QRadar. Quando um evento chega, ele é analisado e classificado com base no IP de origem e destino. O sistema determina se cada extremo pertence à rede local ou remota com base nas definições da hierarquia. Essa classificação influencia diversos módulos internos, como o 'Asset Profiler', o 'Custom Rules Engine' e o 'Magistrate' (responsável pela correlação de ofensas).

Essa arquitetura permite que o QRadar realize uma correlação contextualizada, diferenciando, por exemplo, um ataque externo a um servidor público de uma atividade lateral interna (lateral movement) entre hosts corporativos. Essa capacidade aumenta a precisão das ofensas e reduz falsos positivos em investigações de segurança.

Modelos de Uso

• **Modelo Corporativo Centralizado:** todas as redes da organização são geridas em um único domínio. Ideal para empresas pequenas e médias. • **Modelo Multi-Domínio:** cada unidade de negócio possui sua própria hierarquia, usada em conjunto com perfis de segurança e domínios de correlação. • **Modelo MSSP:** provedores de serviços gerenciados mantêm hierarquias independentes por cliente (tenant), assegurando isolamento completo dos dados.

A escolha do modelo deve considerar o tamanho da infraestrutura, o número de analistas SOC e a necessidade de segregação de dados. Em ambientes híbridos, é comum combinar hierarquias locais e remotas, garantindo visibilidade total sem sobreposição de CIDRs.

Benefícios

O uso adequado da hierarquia de rede traz diversos benefícios: melhora a precisão de correlação, otimiza a classificação de eventos, reduz falsos positivos e aprimora o inventário de ativos. Também facilita a criação de regras mais específicas, como 'Detectar comunicação entre redes críticas e externas', sem precisar listar faixas individualmente.

Além disso, a hierarquia fornece uma visão consolidada da topologia lógica da empresa, apoiando auditorias e planos de resposta a incidentes. Ela ajuda a identificar tráfego inesperado entre sub-redes e serve como base para análises forenses em investigações de comprometimento (Breach Analysis).

Recursos Avançados e Boas Práticas

1. **Versionamento:** mantenha cópias exportadas da hierarquia para controle de mudanças. 2. **Validação:** use buscas AQL para confirmar se ativos e eventos estão sendo atribuídos corretamente. 3. **Integração:** combine a hierarquia de rede com o módulo de 'Asset Profiler' e varreduras de vulnerabilidade. 4. **Segurança:** evite sobreposição de CIDRs entre domínios; isso pode gerar inconsistências nas ofensas. 5. **Monitoramento:** configure alertas para tráfego em faixas privadas não registradas (indicando shadow IT).

Conclusão

A hierarquia de rede é um dos pilares do IBM QRadar SIEM. Ela permite mapear, segmentar e contextualizar o tráfego de rede, oferecendo à equipe de segurança uma visão precisa do que é interno e externo. Uma hierarquia bem projetada aumenta a eficiência das regras, melhora a precisão das ofensas e fortalece a postura defensiva da organização.

Com manutenção regular, documentação e integração com outras funções do SIEM, a Network Hierarchy transforma-se em um recurso estratégico de gestão e detecção, essencial para operações SOC maduras e ambientes corporativos complexos.