IBM QRadar: Métodos de Uso de Coleções de Dados de Referência (Reference Data Collections)

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

Contexto

As coleções de dados de referência (Reference Data Collections) são recursos fundamentais no IBM QRadar para armazenar e consultar informações auxiliares utilizadas em correlações, regras e relatórios. Elas podem conter listas de IPs, mapas de valores ou tabelas complexas que são constantemente atualizadas. Para manipular essas coleções, o QRadar oferece diferentes interfaces: a interface gráfica (UI), a linha de comando (CLI), a API RESTful e consultas AQL (Ariel Query Language). Cada uma delas serve a propósitos distintos e pode ser utilizada em diferentes estágios da análise ou automação de eventos.

Além disso, as coleções de referência podem ser integradas diretamente a regras e condições de correlação, o que permite criar respostas automatizadas, listas dinâmicas e mecanismos de detecção baseados em contexto. O uso combinado dessas ferramentas torna o QRadar uma plataforma flexível e poderosa para a operação de segurança corporativa.

Desafios

O principal desafio no uso de dados de referência está na escolha da interface e no controle de consistência dos dados. Alterações manuais pela UI, por exemplo, são práticas em ambientes pequenos, mas se tornam inviáveis em operações de grande escala, onde APIs e scripts são necessários para automação. Outro ponto crítico é a gestão de acesso: como as coleções podem conter dados sensíveis (IPs internos, usuários monitorados), é essencial aplicar boas práticas de governança e segregação de privilégios.

Por fim, há o desafio da sincronização. Em ambientes distribuídos, atualizações simultâneas por API, regras e consultas podem causar conflitos ou atrasos de replicação. É recomendável definir políticas de atualização (TTL, expiração e versionamento) e monitorar a integridade das coleções com scripts automatizados.

Conceitos Fundamentais

Uso pela Interface do QRadar (QRadar UI)

A interface gráfica (UI) do QRadar é o método mais acessível para visualizar, criar e gerenciar coleções de referência. Por meio dela, o administrador pode acessar o menu *Admin → Reference Data Management*, onde é possível adicionar novos conjuntos, mapas ou tabelas, importar dados CSV e visualizar estatísticas como número de entradas, tempo de vida (TTL) e tamanho total.

A UI é ideal para gerenciamento manual e atividades de verificação rápida, como adicionar um IP a uma lista negra (Reference Set) ou inspecionar o conteúdo de uma tabela de referência. Contudo, sua limitação está na escalabilidade: em ambientes com automação contínua, a API REST e a CLI são mais eficientes para atualizações em massa e integração com sistemas externos.

Uso via Linha de Comando (CLI)

A CLI (Command Line Interface) do QRadar é uma ferramenta poderosa para administradores avançados. Ela permite o gerenciamento direto das coleções por meio de scripts e comandos específicos, localizados geralmente em /opt/qradar/bin ou através do utilitário *reference_data_cli.sh*. Com ela, é possível listar coleções, adicionar valores, excluir chaves e importar conjuntos inteiros de dados.

Exemplo prático: o comando `./reference_data_cli.sh list` exibe todas as coleções existentes. Já `./reference_data_cli.sh add --name Blacklisted_IPs --value 10.10.10.5` adiciona um IP à lista ‘Blacklisted_IPs’. Essa abordagem é ideal para automações internas e integrações com cron jobs que executam limpezas ou atualizações periódicas.

Uso via API RESTful

A API RESTful do QRadar é a forma mais moderna e flexível de interagir com as coleções de referência. Ela permite integrações com sistemas externos de threat intelligence, ferramentas SOAR (Security Orchestration, Automation and Response) e scripts Python ou PowerShell. As APIs seguem o padrão REST e utilizam autenticação baseada em tokens, garantindo segurança e rastreabilidade.

Exemplo: uma requisição GET para `/api/reference_data/sets` retorna a lista de conjuntos disponíveis. Um POST para o mesmo endpoint permite inserir novos valores, enquanto um DELETE remove entradas específicas. Essa capacidade de integração é crucial para ambientes de SOC modernos que operam em arquiteturas híbridas e com múltiplos fornecedores de dados.

Uso em Consultas (AQL – Ariel Query Language)

O QRadar permite o uso de coleções de referência em consultas AQL, integrando-as com buscas em eventos e fluxos. Isso possibilita consultas cruzadas, como identificar eventos onde o IP de origem está presente em uma lista de referência. As funções AQL, como `IN REFERENCESET()` e `GET_REFERENCE_MAP_VALUE()`, tornam a análise mais dinâmica e contextualizada.

Exemplo: uma consulta como `SELECT sourceip FROM events WHERE sourceip IN REFERENCESET('Blacklisted_IPs')` permite localizar todos os eventos que envolvem IPs maliciosos conhecidos. Esse tipo de análise é amplamente utilizado em investigações forenses e detecção de anomalias comportamentais.

Uso em Regras (Conditions e Rule Responses)

As coleções de referência podem ser integradas diretamente às regras do QRadar, tanto em condições quanto em respostas. Nas condições, elas são usadas para comparar valores de eventos com listas, mapas ou tabelas; nas respostas, podem ser usadas para atualizar as próprias coleções de referência dinamicamente.

Exemplo prático: uma regra pode acionar um alerta quando um IP de origem pertence ao conjunto ‘Suspicious_Connections’. Ao mesmo tempo, ela pode adicionar o usuário envolvido em um mapa de monitoramento (‘User_Risk_Map’), criando um ciclo de aprendizado contínuo. Essa capacidade transforma o QRadar em um SIEM adaptativo, capaz de evoluir com base nos próprios eventos observados.

Benefícios

O uso integrado das coleções de referência em diferentes interfaces amplia a flexibilidade operacional e a eficiência do SOC. Combinando UI, CLI e API REST, é possível gerenciar desde pequenos ajustes manuais até integrações automatizadas com plataformas de inteligência de ameaças. Além disso, a incorporação em consultas e regras aumenta a precisão das correlações e a capacidade de resposta.

Recursos Avançados e Boas Práticas

1. **Automatize o ciclo de atualização:** use APIs e scripts para inserir e remover dados dinamicamente. 2. **Controle de acesso:** restrinja quem pode modificar coleções via UI, CLI ou API. 3. **Versionamento:** mantenha backups e logs das alterações em coleções críticas. 4. **Auditoria:** utilize registros do QRadar para monitorar modificações em tempo real. 5. **Otimização de desempenho:** evite coleções com mais de 1 milhão de entradas sem filtros adequados.

Conclusão

As coleções de dados de referência são um dos pilares da arquitetura inteligente do QRadar. Seu uso combinado — via UI, CLI, API, AQL e regras — oferece um ecossistema unificado de automação, contexto e detecção. Em um SOC moderno, dominar esses métodos é essencial para otimizar o tempo de

resposta, reduzir falsos positivos e fortalecer a postura de defesa cibernética da organização.