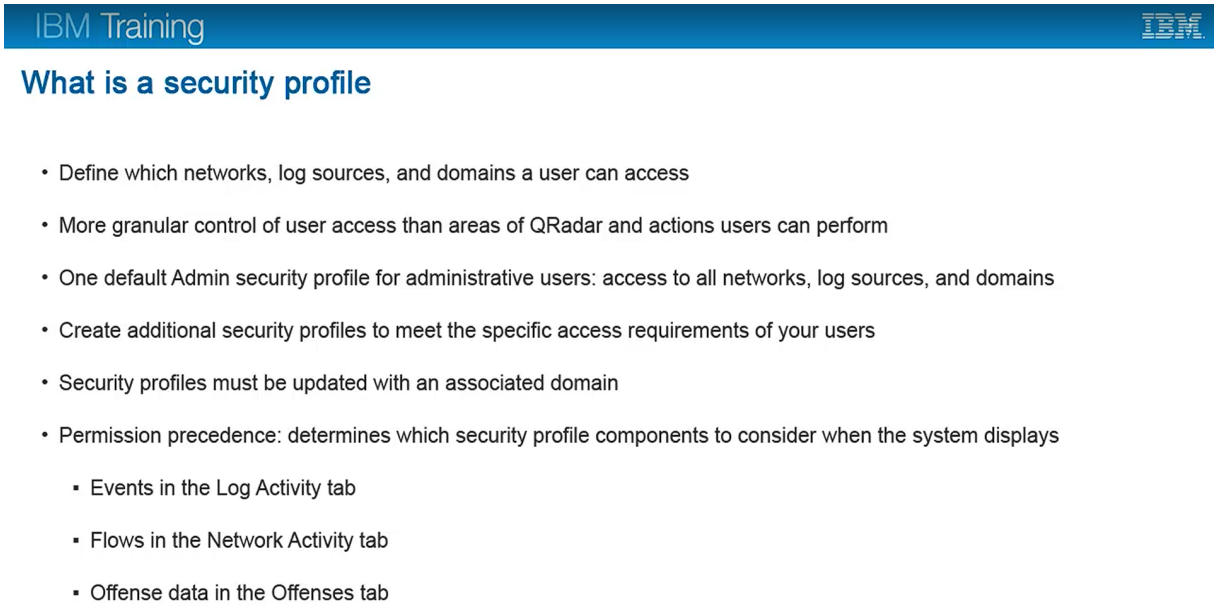
Gerenciamento de Perfis de Segurança no IBM QRadar

Material técnico de revisão — Segurança da Informação

Slide de referência: 'What is a Security Profile' — IBM Training



Contexto

No IBM QRadar, o controle de acesso baseado em perfis de segurança (security profiles) é um elemento essencial para garantir que cada usuário visualize apenas os dados, redes, fontes de log e domínios necessários à sua função. Esses perfis permitem um controle granular, indo além da simples atribuição de papéis administrativos, ao definir limites de visibilidade e ação dentro do ambiente de segurança. Em ambientes corporativos com múltiplos times — como SOC, Red Team, Blue Team e áreas de auditoria — o uso adequado dos perfis de segurança é fundamental para manter a confidencialidade e o princípio do menor privilégio (Least Privilege).

O conceito de perfis de segurança foi introduzido para complementar a separação lógica de domínios e fluxos dentro do QRadar, permitindo que a administração controle o escopo de cada analista sem comprometer a operação global do sistema. Por exemplo, um analista de rede pode ter acesso apenas a eventos e fluxos da infraestrutura de borda, enquanto um auditor corporativo tem permissão apenas para leitura em todos os domínios. Esse tipo de configuração evita vazamento de informações sensíveis e reduz riscos de manipulação indevida de dados.

Desafios

O principal desafio no gerenciamento de perfis de segurança é equilibrar controle granular e usabilidade. Perfis excessivamente restritivos podem impedir que analistas executem tarefas legítimas, enquanto permissões muito amplas ampliam a superfície de risco. Outro ponto crítico é a sincronização entre perfis, domínios e usuários, especialmente em ambientes com múltiplas instâncias de QRadar ou integrações via LDAP/AD.

Outro desafio comum é o controle da precedência de permissões, que determina como o sistema avalia o acesso a eventos, fluxos e ofensas quando há múltiplos perfis aplicados a um mesmo usuário. Sem uma política clara de herança e auditoria, o resultado pode ser acesso acidental a informações confidenciais ou bloqueio de visualização em investigações de incidentes.

Conceitos Fundamentais

Perfis de Segurança (Security Profiles)

Um perfil de segurança define quais redes, fontes de log e domínios um usuário pode acessar. É um nível de controle mais granular do que as funções (roles), permitindo diferenciar não apenas o que o usuário pode fazer, mas também o que ele pode ver. O QRadar vem com um perfil de segurança administrativo padrão (Admin Security Profile), que possui acesso total a todos os componentes do sistema, incluindo redes, fontes e domínios.

Perfis adicionais podem ser criados para atender a necessidades específicas — por exemplo, um perfil 'SOC Tier 1' pode acessar apenas logs de autenticação e firewalls, enquanto um perfil 'Threat Intel' pode visualizar eventos de IDS e fluxos NetFlow. Essa segmentação permite construir uma estrutura de governança mais alinhada à política de segurança corporativa.

Domínios e Associação de Perfis

Cada perfil de segurança deve ser associado a um domínio (domain) no QRadar. Os domínios são agrupamentos lógicos de ativos, fontes de log e redes. Essa relação é essencial para limitar o escopo de visualização do usuário. Por exemplo, um domínio 'Financeiro' pode incluir apenas servidores ERP e bases de dados de contabilidade, e o perfil 'Auditor Financeiro' será associado exclusivamente a ele.

Quando novos domínios são criados, os perfis existentes precisam ser atualizados para refletir as mudanças. Negligenciar essa etapa pode causar inconsistências de acesso, onde usuários legítimos não veem informações relevantes ou, inversamente, passam a ter visibilidade sobre ativos indevidos.

Precedência de Permissões (Permission Precedence)

O QRadar utiliza um modelo de precedência de permissões para determinar qual perfil é considerado em situações onde múltiplos perfis se sobrepõem. A precedência influencia a exibição de eventos na aba 'Log Activity', fluxos na aba 'Network Activity' e dados de ofensas na aba 'Offenses'. Em termos práticos, o sistema avalia as permissões mais permissivas ou mais restritivas conforme a política definida pelo administrador.

Exemplo: se um usuário pertence a dois perfis — um que concede acesso apenas a logs de firewall e outro que inclui toda a rede interna — a precedência configurada determinará qual escopo de dados o usuário verá. Esse mecanismo deve ser planejado com cuidado para evitar sobreposição indevida.

Arquitetura e Integração

A arquitetura de controle de acesso do QRadar é composta por três camadas principais: roles (funções), security profiles (perfis) e domains (domínios). As funções determinam o que o usuário pode fazer (ações administrativas, criação de regras, visualização de relatórios), enquanto os perfis e domínios determinam o que ele pode ver. Esses elementos se combinam para formar a matriz completa de permissões.

Em ambientes integrados ao Active Directory, é possível mapear grupos AD diretamente para perfis de segurança, automatizando a aplicação de políticas de acesso. Essa integração facilita o onboarding e offboarding de usuários, além de garantir conformidade com políticas corporativas de IAM (Identity and Access Management).

Modelos de Uso

• **Modelo centralizado:** todos os usuários pertencem ao mesmo domínio, e perfis de segurança são usados apenas para limitar o tipo de dado (logs, fluxos, ofensas). Adequado para pequenas equipes SOC. • **Modelo segmentado:** cada unidade de negócio ou região tem seu próprio domínio e perfil. Comum em corporações multinacionais ou com múltiplos SOCs regionais. • **Modelo híbrido:** mistura os dois anteriores; perfis limitam dados sensíveis, mas funções administrativas são compartilhadas entre equipes globais.

Benefícios

A adoção correta de perfis de segurança traz benefícios como: aumento da confidencialidade, melhor governança, redução de riscos de acesso indevido e cumprimento de requisitos de auditoria. Além disso, simplifica o gerenciamento de usuários, pois as alterações podem ser aplicadas a perfis em vez de contas individuais.

Em ambientes regulamentados (como PCI-DSS, HIPAA, LGPD), os perfis de segurança ajudam a demonstrar controle efetivo de acesso e segregação de funções (SoD – Segregation of Duties), elementos críticos para conformidade.

Recursos Avançados

Entre os recursos mais avançados estão a combinação de perfis com **custom domains**, uso de **API REST** para automação de criação/atualização e integração com sistemas externos de IAM. É possível, por exemplo, automatizar a criação de perfis temporários para equipes de resposta a incidentes, com validade controlada e auditoria completa.

Outra prática recomendada é o uso de dashboards específicos para cada perfil, garantindo que os usuários visualizem somente indicadores relevantes à sua função. Isso melhora a performance e reduz ruído operacional.

Conclusão

O gerenciamento de perfis de segurança no QRadar é um pilar essencial para a proteção de dados e a eficiência operacional em centros de operações de segurança (SOC). Com uma configuração bem planejada, é possível garantir que cada usuário tenha acesso somente às informações e ações que realmente precisa desempenhar, mantendo a integridade do ambiente e aderência às melhores práticas de segurança e conformidade.