IBM QRadar: Domínios e Locatários (Tenants)

Resumo técnico expandido com tradução e análise — Segurança da Informação

Contexto

O documento 'QRadar Domains and Tenants - OpenMic' da IBM (2018) detalha o funcionamento e as melhores práticas para o uso de Domínios e Locatários (Tenants) dentro do IBM QRadar SIEM. Esses recursos são essenciais para a segregação lógica de dados e o suporte a arquiteturas multiempresa (multi-tenancy). Por meio deles, administradores podem controlar quais eventos, fluxos, ativos e vulnerabilidades pertencem a cada segmento, cliente ou unidade organizacional.

Os domínios segmentam a correlação de eventos e a criação de ofensas, enquanto os tenants permitem atribuir limites de processamento (EPS e FPM) e retenção específica para cada cliente. Essa arquitetura é amplamente usada por MSSPs (Managed Security Service Providers) e corporações de grande porte, garantindo isolamento e segurança de dados.

Desafios

O principal desafio no uso de domínios e tenants está na configuração correta da precedência de critérios e da lógica de classificação dos eventos. A ordem de avaliação — propriedades personalizadas, fontes de log, grupos e coletores — precisa ser precisa, pois qualquer falha pode gerar ofensas incorretas ou perda de visibilidade. Além disso, em ambientes multi-tenant, o controle de taxa (EPS/FPM) é essencial: exceder o limite pode causar descarte de eventos e degradação do desempenho do SIEM.

Outro ponto desafiador é a governança: definir quem administra cada domínio, quem pode criar propriedades personalizadas e como delegar funções sem comprometer a estabilidade do pipeline. A administração delegada (delegated administration) precisa ser planejada para evitar que scripts ou propriedades mal otimizadas afetem todo o ambiente.

Conceitos Fundamentais

Domínios (Domains)

Os domínios são marcadores lógicos aplicados aos eventos durante o pipeline de ingestão do QRadar. Eles criam entidades de correlação independentes, garantindo que ofensas e regras de detecção sejam processadas separadamente por contexto. Essa segmentação é ideal para lidar com IPs sobrepostos (por exemplo, fusões de empresas) ou ambientes com múltiplas redes internas isoladas.

A atribuição de domínios ocorre no pipeline por meio de fontes como propriedades personalizadas, coletores, ou grupos de logs. O primeiro critério que corresponde determina o domínio. Caso nenhum se aplique, o evento é enviado para o ‘Default Domain’. Essa abordagem garante consistência e previsibilidade na classificação dos dados.

Locatários (Tenants)

Os tenants são subconjuntos de domínios usados para dividir o ambiente em instâncias lógicas para diferentes clientes ou departamentos. Cada tenant pode ter limites de EPS, buckets de retenção e permissões de administração próprias. A arquitetura multi-tenant do QRadar foi projetada para provedores de serviço e empresas multinacionais que exigem isolamento completo de dados.

Cada tenant pode ter até 10 buckets de retenção, e a sobrecarga de processamento é controlada por throttling. Quando o limite é atingido, o QRadar descarta eventos excedentes e gera logs informativos, preservando a integridade do sistema. A criação de tenants não exige um deploy completo, o que facilita a expansão do ambiente.

Arquitetura

O pipeline de eventos do QRadar é composto por módulos (ecs-ec, ecs-ep, magistrate) que realizam parsing, normalização, enriquecimento e correlação. O ‘Domain Tagging’ ocorre nessa fase e define a

segmentação lógica de cada dado. Os domínios impactam diretamente regras, ofensas, ativos, vulnerabilidades e buscas. Cada domínio mantém seus próprios contadores e índices, o que evita correlação cruzada indevida.

No contexto de regras, o QRadar suporta quatro tipos principais: Domain-Unaware, Single-Domain, Multi-Domain e Shared-Data. Regras domain-aware garantem isolamento, enquanto as Shared-Data permitem correlação global. Essa flexibilidade possibilita operar ambientes híbridos, combinando domínios isolados com análises agregadas de segurança corporativa.

Modelos de Uso

• **Modelo Interno:** separação por departamentos (Financeiro, Engenharia, Produção) usando domínios específicos. • **Modelo MSSP:** cada cliente recebe um tenant dedicado, com domínios, regras e retenções próprias. • **Modelo Híbrido:** usado por corporações com divisões regionais, permitindo análise consolidada e isolamento simultâneo.

Em todos os modelos, a segurança e a conformidade são fortalecidas pela capacidade de aplicar políticas distintas de acesso, retenção e correlação, conforme o contexto do usuário e o domínio ao qual ele pertence.

Benefícios

A principal vantagem da arquitetura de domínios e tenants é o isolamento lógico e operacional dos dados, garantindo privacidade e desempenho em ambientes compartilhados. Outros benefícios incluem: escalabilidade dinâmica, gestão de capacidade simplificada, conformidade com LGPD e PCI-DSS e maior precisão nas investigações de incidentes.

A segmentação também reduz a superfície de erro humano: analistas só visualizam eventos relevantes ao seu escopo, diminuindo riscos de manipulação indevida de dados sensíveis e otimizando a triagem de ofensas.

Recursos Avançados e Boas Práticas

1. **Uso de Custom Event Properties (CEP):** para classificar eventos por domínio automaticamente. 2. **Integração LDAP/AD:** mapeia grupos de usuários para domínios e perfis de segurança. 3. **Auditoria com AQL:** usando DOMAINNAME(domainid) ou ‘NULL as Domain’ para identificar eventos sem domínio. 4. **APIs REST:** automatizam criação e atualização de tenants e domínios. 5. **Documentação e Governança:** definir políticas claras para precedência e administração delegada.

Conclusão

O IBM QRadar utiliza os conceitos de Domínios e Locatários para oferecer uma arquitetura escalável, segura e aderente às melhores práticas de segmentação de dados. A correta implementação desses recursos garante visibilidade precisa, isolamento de clientes e departamentos e conformidade regulatória. Com administração delegada e automação, o QRadar torna-se uma plataforma poderosa para operações de segurança em larga escala, mantendo o princípio de mínimo privilégio e controle granular sobre todo o ecossistema de eventos e fluxos.