IBM QRadar: Protocolos de Fontes de Log (Log Source Protocols)

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

Contexto

O IBM QRadar utiliza protocolos de coleta de logs para receber e processar dados de eventos provenientes de dispositivos, aplicações e sistemas distribuídos em uma rede corporativa. Esses protocolos são a espinha dorsal da capacidade do SIEM de consolidar, normalizar e correlacionar informações de segurança. Cada protocolo possui características específicas — métodos de coleta, requisitos de configuração, suporte a autenticação e particularidades de desempenho.

No momento da apresentação (versão 7.2.6), o QRadar suportava cerca de 52 protocolos de origem de logs e mais de 300 tipos de fontes, incluindo suporte automático (auto-detection) para 174 delas. Esses protocolos são categorizados em três grupos principais: Listening Protocols, Polling Protocols e Specialty Protocols. A correta seleção e configuração desses métodos impactam diretamente a performance do ambiente e a confiabilidade dos dados recebidos.

Desafios

Administradores enfrentam desafios significativos ao lidar com a diversidade de formatos, volumes e protocolos de log. Entre os mais comuns estão: falhas na autodetecção de fontes (especialmente em ambientes com Syslog intermediário), sobrecarga de processamento devido à duplicação de eventos e dificuldades de autenticação em conexões seguras (como TLS).

Além disso, erros na determinação de IPs de origem ou destino podem comprometer correlações e investigações. Quando logs passam por servidores intermediários, o QRadar tende a registrar o IP do relay em vez do dispositivo original. Boas práticas, como preservação de cabeçalhos Syslog ou reconfiguração de encaminhadores para inserir o IP real no header, são essenciais para manter a integridade dos dados.

Conceitos Fundamentais

O que é um Evento

Em termos de QRadar, um evento é uma mensagem registrada por um dispositivo indicando uma ação específica. Exemplos incluem um login SSH bem-sucedido, uma negação de firewall ou uma conexão VPN estabelecida. Esses eventos representam atividades pontuais e são o combustível do mecanismo de correlação e detecção do SIEM.

O que é um Protocolo de Log Source

Um protocolo de log source define como os eventos são coletados. Pode envolver escuta passiva de mensagens (como Syslog), polling ativo de bancos de dados (JDBC) ou acesso a APIs de serviços em nuvem. O protocolo gerencia conexões, filas de entrada e o envio dos dados para o pipeline de eventos (ECS).

O que é um DSM (Device Support Module)

O DSM é o módulo responsável por interpretar (parsear) os logs e classificá-los em categorias reconhecidas pelo QRadar. Cada produto (como Palo Alto, Fortinet, Windows Server) possui um DSM correspondente. O DSM traduz o formato bruto em campos estruturados, como IP de origem, usuário, ação e severidade.

Traffic Analysis (Auto-Discovery)

O recurso de Traffic Analysis permite que o QRadar detecte automaticamente novas fontes de logs com base nos fluxos recebidos. Ele funciona com protocolos Syslog (TCP/UDP) e SNMP. Se os eventos não forem reconhecidos ou vierem em baixa frequência (<5 EPS), o dispositivo é classificado como 'SIM Generic-2' até que seja configurado manualmente.

Arquitetura e Categorias de Protocolos

Os protocolos de coleta são divididos em três grandes categorias: Listening, Polling e Specialty.

Listening Protocols

Esses protocolos aguardam conexões e dados passivamente. Exemplos incluem Syslog, TLS Syslog, TCP/UDP Multiline Syslog e Syslog Redirect. O Syslog, por exemplo, utiliza as portas 514/TCP e 514/UDP e segue os padrões RFC3164 e RFC5424. O TLS Syslog adiciona criptografia, utilizando certificados DER PKCS8 e operando na porta 6514. A configuração incorreta de certificados é uma das falhas mais comuns neste método.

Polling Protocols

Os protocolos de polling realizam consultas periódicas a uma fonte de dados. Exemplos incluem JDBC, Log File e SMB Tail. O JDBC coleta logs diretamente de bancos de dados (Oracle, DB2, Postgres, etc.) e requer um campo incremental (ID, timestamp) para evitar duplicidade. Já o Log File copia arquivos via FTP, SFTP ou AWS, armazenando-os temporariamente em /store/tmp para posterior parsing. O SMB Tail, base de vários protocolos Windows, monitora arquivos em compartilhamentos de rede SMB.

Specialty Protocols

Protocolos especializados permitem integração com serviços em nuvem e APIs REST. Exemplos incluem Amazon AWS CloudTrail, Microsoft Office 365, Salesforce, Okta e IBM Tivoli Endpoint Manager. Esses protocolos exigem chaves de autenticação e, muitas vezes, certificados digitais para estabelecer conexões seguras. No caso do AWS CloudTrail, o certificado deve ser armazenado em /opt/qradar/conf/trusted_certificates/.

Modelos de Uso

• **Ambiente Corporativo Interno:** predominância de Syslog e SMB Tail para logs de sistemas locais. • **Ambiente Multi-cloud:** uso de REST APIs (AWS, Office 365, Salesforce) e Log File via SFTP. • **MSSPs (Managed Security Service Providers):** combinação de TLS Syslog com auto-discovery para integrar clientes múltiplos. • **Infraestruturas Críticas:** JDBC e Log File configurados com verificação SSL e controle rigoroso de credenciais.

Benefícios

A diversidade de protocolos de coleta no QRadar proporciona flexibilidade, escalabilidade e interoperabilidade com quase qualquer sistema de logs. O uso adequado garante ingestão segura e eficiente, enquanto a autodetecção simplifica a integração de novos dispositivos. Além disso, a combinação de métodos passivos e ativos de coleta permite monitoramento contínuo em ambientes híbridos.

A capacidade de parsing via DSMs e Traffic Analysis reduz erros de classificação, garantindo que as regras de correlação operem sobre dados normalizados e precisos — fator essencial para reduzir falsos positivos e melhorar o tempo de resposta do SOC.

Recursos Avançados e Boas Práticas

1. **Evite sobreposição de IPs** — preserve cabeçalhos originais para identificar a verdadeira origem. 2. **Controle o desempenho** — monitore a taxa EPS (Events per Second) e ajuste coalescência quando necessário. 3. **Segurança de transporte** — utilize TLS sempre que possível para Syslog e REST APIs. 4. **Automatize coletas** — use scripts com APIs REST para criação em massa de log sources. 5. **Audite conexões** — configure usuários dedicados e rastreie extrações via logs de auditoria do

QRadar.

Conclusão

Os protocolos de coleta de logs são o primeiro elo na cadeia de detecção do QRadar. Seu domínio garante integridade, confiabilidade e segurança no ciclo de ingestão de dados. Cada protocolo, do simples Syslog ao sofisticado AWS REST, possui um papel específico na arquitetura SIEM, e compreender suas nuances é essencial para analistas e engenheiros de segurança. Ao aplicar boas práticas e ajustar parâmetros conforme o ambiente, é possível alcançar máxima eficiência operacional e resiliência contra falhas na coleta de dados.