IBM QRadar – Log Source Concepts, Protocols e Device Support Modules (DSMs)

Contexto

O **IBM QRadar** é uma solução de **SIEM (Security Information and Event Management)** que coleta e analisa dados de segurança de várias fontes, fornecendo visibilidade abrangente das atividades da infraestrutura. Entre os pilares fundamentais do QRadar estão a ingestão de dados (Data Ingestion), as fontes de log (Log Sources), os protocolos de comunicação e os módulos de suporte a dispositivos (Device Support Modules – DSMs). Esses elementos garantem que o QRadar interprete corretamente as informações vindas de diferentes sistemas, permitindo a detecção eficiente de ameaças e o cumprimento de políticas de conformidade.

Data Ingestion – Coleta de Dados

O processo de **Data Ingestion** é responsável pela entrada de dados no QRadar. Ele abrange a coleta de logs, eventos e fluxos de rede (flows) oriundos de dispositivos, servidores, sistemas operacionais, aplicações e serviços em nuvem. Essas informações podem ser recebidas em tempo real ou de forma agendada, dependendo do tipo de integração.

Durante a ingestão, o QRadar atua com **Event Collectors**, que recebem os dados, aplicam filtros de licença (EPS) e encaminham os registros para os **Event Processors**, onde ocorre a normalização, correlação e armazenamento. Essa arquitetura modular permite escalar a coleta de eventos de acordo com o crescimento do ambiente monitorado, mantendo a integridade e a performance do sistema.

Log Sources – Fontes de Logs

As **Log Sources** são as origens dos dados processados pelo QRadar. Elas representam dispositivos e sistemas como firewalls, roteadores, servidores web, controladores de domínio, endpoints, switches, bancos de dados e aplicações em nuvem. Cada log source envia registros de eventos que descrevem atividades relevantes, como tentativas de login, modificações de sistema, conexões de rede ou bloqueios de tráfego.

O QRadar identifica automaticamente muitos tipos de fontes por meio de assinaturas conhecidas. Caso o dispositivo não seja reconhecido, o analista pode associá-lo manualmente a um DSM ou criar um modelo personalizado. Essa flexibilidade garante que praticamente qualquer dispositivo capaz de gerar logs possa ser integrado ao SIEM, aumentando a cobertura de segurança.

Protocolos de Comunicação

Para realizar a ingestão, o QRadar utiliza uma variedade de **protocolos de comunicação**, como **Syslog (UDP, TCP, TLS)**, **SNMP**, **HTTP/HTTPS**,

JDBC, **SFTP**, **LEEF**, **CEF** e **API Polling**. Cada protocolo define um método específico de envio, transporte e autenticação de logs. A escolha correta depende das características do dispositivo, do volume de dados e dos requisitos de segurança da organização.

Por exemplo, dispositivos de rede como firewalls e switches geralmente utilizam o **Syslog**, enquanto bancos de dados fazem uso de conexões **JDBC** para exportar informações de auditoria. Ambientes em nuvem, como AWS, Azure e Google Cloud, se integram via APIs RESTful autenticadas. O uso de protocolos seguros (como TLS e HTTPS) é fundamental para evitar interceptações e garantir a confidencialidade dos dados em trânsito.

Device Support Modules (DSMs)

Os **Device Support Modules (DSMs)** são componentes do QRadar responsáveis por **interpretar e normalizar** os logs recebidos. Cada DSM contém regras específicas que permitem ao sistema traduzir diferentes formatos de log em um modelo padronizado, facilitando a correlação entre fabricantes e tecnologias distintas. Isso é essencial para o funcionamento do motor de correlação de eventos do QRadar.

Por exemplo, um log de bloqueio de tráfego de um firewall Fortinet pode ter campos diferentes de um log equivalente em um Cisco ASA. O DSM converte esses dados em campos uniformes, como “source IP”, “destination IP”, “action” e “severity”. Dessa forma, o QRadar pode correlacionar ambos os eventos e determinar se fazem parte do mesmo ataque ou incidente de segurança.

Além dos DSMs oficiais disponibilizados pela IBM, o QRadar oferece o **DSM Editor**, ferramenta que permite criar e ajustar módulos personalizados. Isso é útil para integrar soluções proprietárias ou sistemas legados que não possuem modelos prontos, garantindo que o ambiente mantenha visibilidade total de suas operações.

Event Pipeline – Fluxo de Processamento

Após a ingestão, os logs seguem um fluxo interno conhecido como **Event Pipeline**, composto por várias etapas de processamento. O pipeline inclui a **verificação de licença**, **parsing via DSM**, **coalescência de eventos**, **correlação de regras (CRE)** e **armazenamento na base Ariel**. Cada fase desempenha um papel crucial na filtragem, organização e análise dos dados recebidos.

Durante o parsing, o DSM interpreta o log e aplica o mapeamento de campos. Em seguida, o mecanismo de correlação (Custom Rules Engine) verifica se o evento corresponde a uma regra predefinida de segurança. Caso atenda aos critérios, o evento pode gerar uma **ofensa**, representando uma possível ameaça ou violação de política.

Benefícios e Conclusão

Compreender o funcionamento dos **Log Sources**, **Protocolos** e **DSMs** é essencial para a operação eficiente do QRadar. Esses elementos garantem que os

dados coletados sejam traduzidos em informações acionáveis, permitindo a detecção de incidentes em tempo real e a construção de um panorama de segurança unificado.

A arquitetura modular e escalável do QRadar, aliada à sua capacidade de integração com centenas de tecnologias, faz dele uma solução robusta para **centros de operações de segurança (SOC)**. Ao dominar esses conceitos, o profissional de segurança consegue ajustar a coleta de dados, melhorar a correlação de eventos e otimizar a resposta a incidentes, elevando o nível de maturidade cibernética da organização.