Arquitetura de Implantação do QRadar

Este documento descreve os principais componentes do diagrama de arquitetura do IBM QRadar, explicando a função de cada elemento e o fluxo de dados entre eles.

1) Console (31xx - All-in-One)

- **Função:** Interface gráfica, gerenciamento central, correlação, buscas e coleta de logs em setups menores.
- **Processos:** Coleta, parse, correlação e buscas.
- **Quando usar:** Em ambientes pequenos ou apenas para administração.

2) Event Processor – EP (16xx)

- **Função:** Recebe e processa eventos (logs), faz parsing, normalização e envio para correlação.
- **Detalhes:** Aplica parsers, enriquece eventos e indexa.
- **Escala:** Dimensionado por EPS (events per second).

3) Flow Processor – FP (17xx)

- **Função:** Processa fluxos (NetFlow, IPFIX, sFlow), correlaciona comunicações.
- **Detalhes:** Extrai IPs, portas, protocolos e bytes.
- **Escala:** Dimensionado por FPM (flows per minute).

4) EP + FP Combinado (18xx)

- **Função:** Executa processamento de eventos e fluxos no mesmo appliance.
- **Quando usar:** Ambientes médios que não precisam separar funções.

5) Data Node (14xx)

- **Função:** Armazenamento de índices e eventos para buscas rápidas (Ariel DB).
- **Requisitos:** CPU, disco e RAM adequados para retenção e performance.

6) Event Collector Remoto – EC (15xx)

- **Função:** Coletor remoto para parsing leve e store & forward.
- **Uso:** Sites remotos com links instáveis ou de baixa largura de banda.

7) QFlow Processor – QFP (12xx / 13xx)

- **Função:** Recebe tráfego espelhado (SPAN/TAP) e gera fluxos enriquecidos.
- **Detalhes:** Análise dos primeiros 64 bytes do payload para identificar aplicações.
- **Uso:** Identificação de aplicações e geração de flows sem payload completo.

8) QNI – QRadar Network Insights (19xx / 20xx)

- **Função:** Deep Packet Inspection (DPI) e captura de payload completo.
- **Detalhes:** Extrai mais de 40 campos, hashes, tamanhos de arquivos e conteúdo.
- **Uso:** Investigações forenses, exfiltração de dados, análise de malware.

9) App Node / UBA

- **Função:** Execução de aplicativos adicionais (UBA, módulos analíticos).
- **Observação:** Não é um managed host, roda em RedHat ou CentOS.
- **Uso:** Necessário para User Behavior Analytics e apps adicionais.

Fluxo de Dados

1. Logs chegam ao Console/EP → parsing e normalização.
2. Flows chegam ao FP → correlação de fluxos.
3. Pacotes espelhados chegam ao QFP ou QNI → enriquecimento ou payload completo.
4. Dados indexados são armazenados nos Data Nodes.
5. Event Collectors remotos garantem entrega em links instáveis.
6. App Nodes consomem dados para análises adicionais.

Termos Técnicos

- **EPS:** Events per second – taxa de eventos processados.
- **FPM:** Flows per minute – taxa de fluxos processados.
- **SPAN:** Espelhamento de tráfego em switch (pode descartar em alta carga).
- **TAP:** Cópia passiva de tráfego (ideal para captura completa).
- **First 64 bytes:** Técnica para identificação de aplicações sem payload completo.
- **Store & Forward:** Armazenar localmente e enviar quando possível.

Boas Práticas

- Separar roles para escalabilidade.
- Usar QFP para identificação leve e QNI para análise profunda.
- Preferir TAP a SPAN para captura confiável.
- Dimensionar EPS e FPM conforme sizing guide.
- Usar Event Collectors em locais remotos.
- Isolar App Nodes para não afetar correlação.