■ Resumo e Tradução – Introdução ao IBM QRadar

1. Contexto e Desafios

- Evolução da TI trouxe mais endpoints remotos, cloud e SaaS. - Aumento de vetores de ataque. - Ferramentas de segurança isoladas. - Problemas: excesso de alertas, falta de visão unificada, analistas sobrecarregados.

2. Solução da IBM

IBM propõe modernização da detecção e resposta: 1. Eliminar silos. 2. Fluxo unificado de investigação e resposta. 3. Automação de tarefas repetitivas/complexas. Implementado na QRadar Suite com UAX (Unified Analyst Experience).

3. Componentes da QRadar Suite

- ASM (Randori): identifica ativos expostos. - EDR (ReaQta/QRadar EDR): protege endpoints com IA. - Log Insights: ingestão massiva de logs. - SIEM: correlação em tempo real, UBA, MITRE ATT&CK.; - SOAR: orquestração e automação da resposta.

4. Funcionalidades-Chave

- Integração IBM + terceiros. - Automação + IA (investigações automáticas, análise de causa raiz). - Integrações abertas via App Exchange. - X-Force Threat Intelligence.

5. Arquitetura do QRadar SIEM

- Coleta de logs e fluxos de rede. - Normalização, correlação e geração de ofensas. - Console central com abas: Offenses, Log Activity, Network Activity, Assets, Reports.

6. Modelos de Deploy

- On-premises: hardware IBM ou virtual. - Cloud: IBM, AWS, Azure. - Híbrido. - QRoC: versão em nuvem gerenciada pela IBM.

7. Benefícios

- Visibilidade completa. - Detecção avançada (insider e externa). - Compliance com relatórios prontos. - Escalabilidade (multi-tenant, MSSPs). - Resposta mais rápida com automação.

8. Recursos Avançados

- Cognitive Analytics (Watson). - Machine Learning (UBA e Network Threat Analytics). - App Exchange para extensões. - Integração com X-Force Exchange.

■ Conclusão

QRadar é uma plataforma modular e extensível que une SIEM, EDR, SOAR, ASM e Log Insights. Resolve problemas modernos de SOC: excesso de alertas, ferramentas isoladas, lentidão na resposta e falta de visibilidade.