IBM QRadar – Offense Indexing e Offense State & Retention

Contexto

O IBM QRadar é uma plataforma de **SIEM (Security Information and Event Management)** que tem como objetivo identificar, correlacionar e priorizar incidentes de segurança em ambientes corporativos. Dentro desse ecossistema, dois conceitos essenciais para o gerenciamento eficiente de alertas são o **Offense Indexing** e o **Offense State & Retention**. Esses mecanismos definem, respectivamente, **como as ofensas são agrupadas** e **como elas são mantidas, armazenadas e removidas do sistema ao longo do tempo**.

Com a quantidade crescente de eventos e fluxos de rede monitorados diariamente, o QRadar precisa de mecanismos sofisticados para evitar redundâncias e otimizar a análise. O Offense Indexing garante que incidentes correlacionados sejam agregados em uma única ofensa, enquanto o gerenciamento de estados (state) e retenção (retention) assegura a manutenção eficiente das ofensas durante o ciclo de vida da investigação.

Offense Indexing

O **Offense Indexing** é o processo que permite ao QRadar **agrupar eventos ou fluxos de diferentes regras** com base em um mesmo parâmetro. Esse agrupamento é essencial para reduzir a fragmentação de alertas e garantir que eventos relacionados sejam tratados de forma unificada. Na prática, o indexador define o **campo-chave** utilizado para agrupar ofensas, como endereço IP, nome de usuário ou atributo personalizado.

Por exemplo, considere um cenário em que uma ofensa é gerada a partir de um único **endereço IP de origem** que se comunica com múltiplos destinos. Isso indica que há um atacante único agindo contra diversas vítimas. Ao indexar as ofensas com base no IP de origem, o QRadar agrupa todos os eventos e fluxos relacionados a esse IP em uma **única ofensa consolidada**. Esse tipo de correlação reduz o ruído e facilita a compreensão do escopo do ataque.

O QRadar utiliza o **parâmetro offense index** configurado nas regras para determinar **quais ofensas devem ser encadeadas**. Isso significa que, sempre que um novo evento for detectado e tiver o mesmo índice de ofensa (por exemplo, o mesmo IP de origem), ele será automaticamente adicionado à ofensa existente, e não criará uma nova. Essa abordagem melhora o desempenho e garante maior coerência nas análises de ameaças contínuas.

Além disso, o QRadar permite configurar o indexamento com base em **campos normalizados** (como IP de origem, IP de destino ou nome de usuário) ou propriedades personalizadas de eventos e fluxos. Essa flexibilidade possibilita criar **regras específicas para diferentes tipos de ameaças**, adaptando o comportamento de

indexação ao contexto operacional da organização.

Desafios do Offense Indexing

O principal desafio no uso do Offense Indexing é escolher corretamente o campo de indexação. Se o parâmetro selecionado for muito genérico, múltiplos ataques não relacionados podem ser agrupados em uma única ofensa, dificultando a análise. Por outro lado, se o índice for muito específico, o sistema poderá gerar **ofensas fragmentadas**, perdendo o contexto geral do ataque. A configuração ideal requer um equilíbrio entre granularidade e abrangência.

Outro ponto crítico é a **interação entre o indexador e o Offense Chaining**. Ambos os mecanismos trabalham juntos para agrupar ofensas relacionadas e construir uma linha temporal de eventos. Uma configuração inadequada de indexação pode interromper a cadeia de ofensas, fragmentando o histórico e prejudicando a visibilidade do incidente completo.

Offense State & Retention

O **Offense State** define o estado atual de uma ofensa no ciclo de vida da investigação. Já o **Offense Retention** determina por quanto tempo as ofensas inativas e encerradas permanecem armazenadas antes de serem removidas do sistema. Esses dois mecanismos trabalham em conjunto para garantir que o QRadar mantenha apenas informações relevantes e otimize o uso de recursos do banco de dados.

O ciclo de vida de uma ofensa no QRadar passa por diversos estados: **Active, Dormant, Recalled, Inactive, Closed e Removed**. Quando uma ofensa é criada, ela inicia no estado **Active**, significando que novos eventos ainda estão sendo adicionados a ela. Caso não receba novos dados após um determinado período, ela entra no estado **Dormant**. Se novos eventos relacionados forem detectados, a ofensa pode ser **Recalled**, retornando ao estado ativo.

Quando o analista encerra uma investigação, a ofensa é marcada como **Closed**, mas permanece disponível por um tempo definido pelo período de retenção. Após esse prazo, ela se torna **Inactive** e, eventualmente, **Removed**, sendo apagada permanentemente do console. Esse ciclo permite um equilíbrio entre **histórico de investigação e eficiência de armazenamento**, garantindo que o sistema permaneça rápido e responsivo mesmo em grandes volumes de dados.

Benefícios Operacionais

O uso combinado de **Offense Indexing e Offense State Management** proporciona uma abordagem inteligente e escalável para o tratamento de incidentes de segurança. O indexador reduz o número de ofensas redundantes, enquanto o controle de estado e retenção assegura que apenas informações úteis sejam mantidas ao longo do tempo. Essa combinação otimiza a experiência dos analistas e melhora a **eficiência operacional do SOC (Security Operations Center)**.

Outro benefício importante é a capacidade de priorização automática. Ao consolidar ofensas relacionadas e gerenciar seu ciclo de vida de forma automatizada, o QRadar permite que os analistas se concentrem nas ameaças mais críticas, reduzindo o tempo médio de detecção e resposta (MTTD/MTTR). Além disso, a retenção controlada de ofensas antigas facilita auditorias e revisões forenses, sem comprometer o desempenho geral da plataforma.

Recursos Avançados e Integrações

O QRadar permite personalizar políticas de retenção e critérios de transição entre estados de ofensa com base em **níveis de gravidade, categorias de ataque ou ativos críticos**. Por exemplo, ofensas relacionadas a sistemas financeiros podem ter um período de retenção maior, enquanto alertas de baixo risco são removidos mais rapidamente. Isso garante uma **gestão de incidentes orientada a risco**, alinhada com as práticas de segurança corporativa.

Além disso, o QRadar pode integrar essas funcionalidades com o **QRadar SOAR** e o **QRadar Advisor with Watson**, permitindo automação de investigações e correlação com inteligência de ameaças global. Assim, o processo de indexação e gerenciamento de ofensas torna-se parte de um ecossistema mais amplo de **detecção, resposta e aprendizado contínuo**.

Conclusão

Os conceitos de **Offense Indexing** e **Offense State & Retention** são fundamentais para o funcionamento eficaz do IBM QRadar como plataforma SIEM. Enquanto o primeiro garante a correlação lógica de eventos e a consolidação de alertas, o segundo assegura o gerenciamento eficiente do ciclo de vida das ofensas. Juntos, eles formam a base de uma arquitetura de monitoramento inteligente, capaz de transformar grandes volumes de dados em insights claros e acionáveis para equipes de segurança.