Bing chat: 6/7

1. Behaviorial
2. rule/ baseline based
3. the casuality
4. timestamp/severity
5. xql/ use query builder
6. root cause
7. palo alto network fw traffic logs