

# Critical Path Exploration Dashboard for Alert-driven Attack Graphs

Authors: Azqa Nadeem, Sònia Leal Díaz, Sicco Verwer

## Summary:

Intrusion alert management often leads to alert fatigue. Recently, alert-driven attack graphs (AG) were proposed to reduce analyst workload by extracting attacker strategies directly from intrusion alerts. This paper proposes a web-based visual analytics dashboard with querying and prioritization capabilities for alert-driven AGs.