CYBER SECURITY VISUALISATION

GROUP WORK

2017-04-18

0.1 Introduction

Cyber security is a central concern for all organizations. The iterative approach to building and maintaining IT networks has left them with in-built and growing vulnerabilities. Criminals, terrorists, nation states, as well as activists and opportunistic amateurs, pose a real and persistent threat to corporate and government IT systems- a situation exacerbated by their complexity. [1] The fields of information visualization and visual analytics strive to leverage the unique perceptual capabilities of humans in concert with algorithmic support in order to better understand complex data. In recent years, visualization has emerged as a promising technique to better equip analysts to operate effectively in an evolving digital threat landscape. [2]

0.2 Background

Cyber security is a data-led battle, with terabytes of different information collated from around the enterprise into centralized dashboards, sometimes in dedicated network operations centers (NOCs) or security operations centers (SOCs). Existing tools do an excellent job of collating this data, often with automated real time alerts. Too frequently, however they lack the visualization capability required for humans to interpret the data. This means alerts are not effectively investigated and post- attack forensics are inefficiently managed. Integration of network visualization into the enterprise cyber security dashboard is a logical and effective approach to the manual investigation of real-time alerts and post-attack forensics.[3]