Method, product, and system for detecting malicious network activity using a graph mixture density neural network

1. United States Patent:11880764
2. Date of Patent: January 23, 2024
3. Inventor(s):
    a. **Kazerounian; Sohrob (Somerville, MA)**
    b. **Hannah; Daniel Carlton (Melrose, MA)**
    c. **Oikarinen; Tuomas P. (Boston, MA)**
4. Assignee: Vectra AI, Inc. (San Jose, CA)
5. Abstract: Disclosed is an approach for detecting malicious network activity (e.g. based on a data hoarding activity identifies using a graph mixture density neural network (GraphMDN)). Generally, the approach includes generating embeddings using a graph convolution process and then processing the embeddings using a mixture density neural network. The approach may include collecting network activity data, generating a graph representing the network activity, or an aggregation thereof that maintains the inherent graphical nature and characteristics of the data, and training a GraphMDN in order to generate pluralities of distributions characterizing one or more aspects of the graph representing the network activity. The approach may also include capturing new network activity data, and evaluating that data using the distributions generated by the trained GraphMDN, and generation corresponding detection results.
6. SUMMARY
    a. The method, product, and system for detecting malicious network activity using a graph mixture density neural network.
    b. In some embodiments, the approach includes the detection of malicious network activity (e.g. based on a data hoarding activity identified using a graph mixture density neural network (GraphMDN)) as will be described herein. Additionally, the approach may include collecting network activity data, generating a graph representing the network activity, or an aggregation thereof that maintains the inherent graphical nature and characteristics of the data, and training a GraphMDN in order to generate pluralities of distributions characterizing one or more aspects of the graph representing the network activity. In some embodiments, the approach includes capturing new network activity data, and evaluating that data using the distributions generated by the trained GraphMDN, and generation corresponding detection results.
    c. Further details of aspects, objects, and advantages of some embodiments are described below in the detailed description, drawings, and claims. Both the foregoing general description and the following detailed description are exemplary and explanatory and are not intended to be limiting as to the scope of the embodiments.