Analytical Methodologies - Network Analysis

Table of Contents

Analytic Methodologies – Network Analysis

27

027 Another analytical methodology is called network analysis, or social network analysis, and it is an exploration technique.

Social Network Analysis

- Investigating social structures through the use of network or graphs
- Networked structures
  - Usually called nodes ((individual actors, people, or things within the network)
- Connections between nodes: Edges or Links
- Focus on relationships between actors in addition to the attributes of actors
- Extensively used in mapping out social networks (Twitter, Facebook)
- Examples: Palantir, Analyst Notebook, MISP and Maltego

http://www.fmsasg.com/socialnetworkanalysis/

28

**028 Social network analysis is good for understanding links, relationships between nodes, key nodes, which could be people in a terrorist group, key IPs or MAC addresses. It's investigating social structures that are used between networks or graphs. So network structures are usually called nodes, and nodes typically tend to be individual actors, people or things within the network. Those are called nodes.

The connections between the nodes are typically referred to as edges or links, and what network analysis does is it makes not just the nodes important but the relationships or edges between the actors or nodes as equally as important in your analysis. Social network analysis is extensively used in mapping out

networks on Twitter, Facebook, Tencent, Weibo, to see how people computers, domains and hashes. Some software programs that do this include Maltego, Palantir, i2 Analyst's Notebook, MISP. Not endorsing any, but those are some that you might be familiar with or might want to look into.

Notices

Notices

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0262