

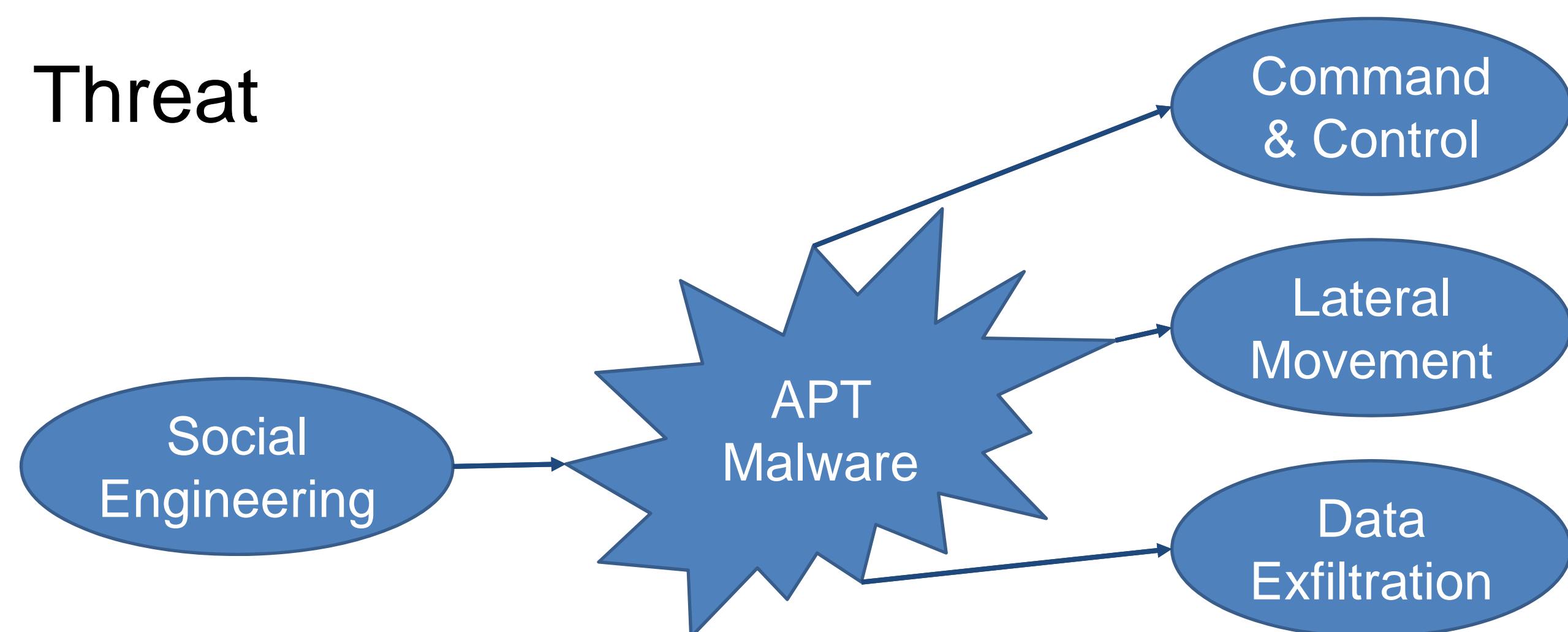
## Log-Centric Analytics for Advanced Persistent Threat Detection

Shiqing Ma, Xiangyu Zhang, Dongyan Xu

Department of Computer Science and CERIAS, Purdue University

**LogIC : Log-based Investigation of Causality**  
fine-grain system logging & causal analysis

- Threat



- Causal Analysis

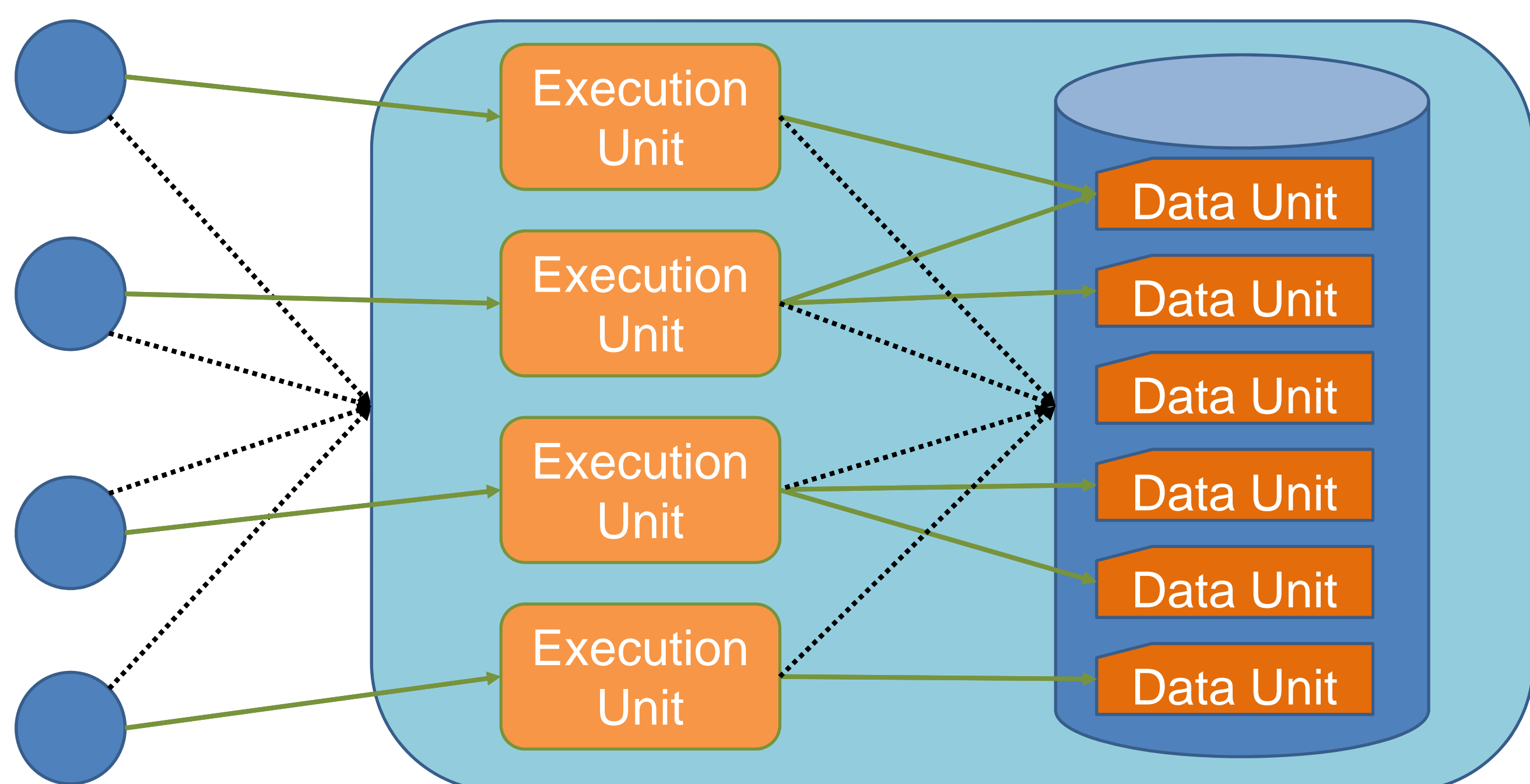
- Backward: trace "entry point"
- Forward: reveals ramifications

- Challenge

- Dependency explosion

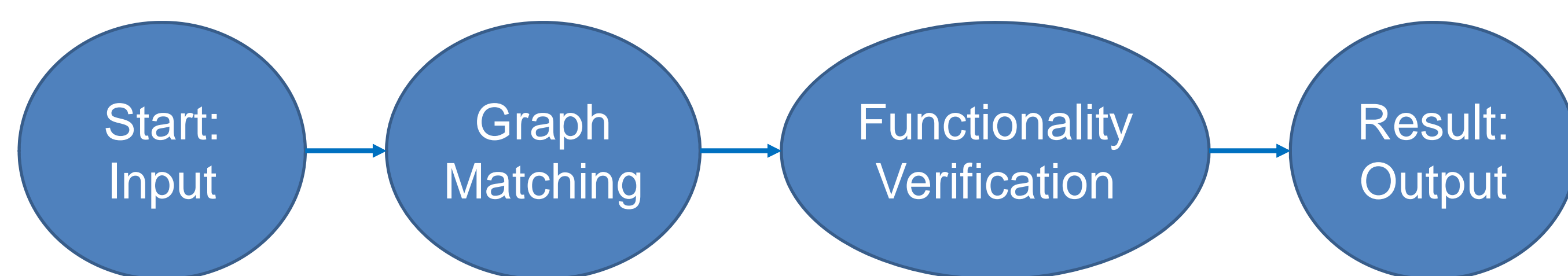
- Solution

- Execution Partitioning: *execution units*
- Data Partitioning: *data units*



**LogAn : Log Analytics**  
"Big Data" analyzer & correlator

- Framework



- Big Data Problem

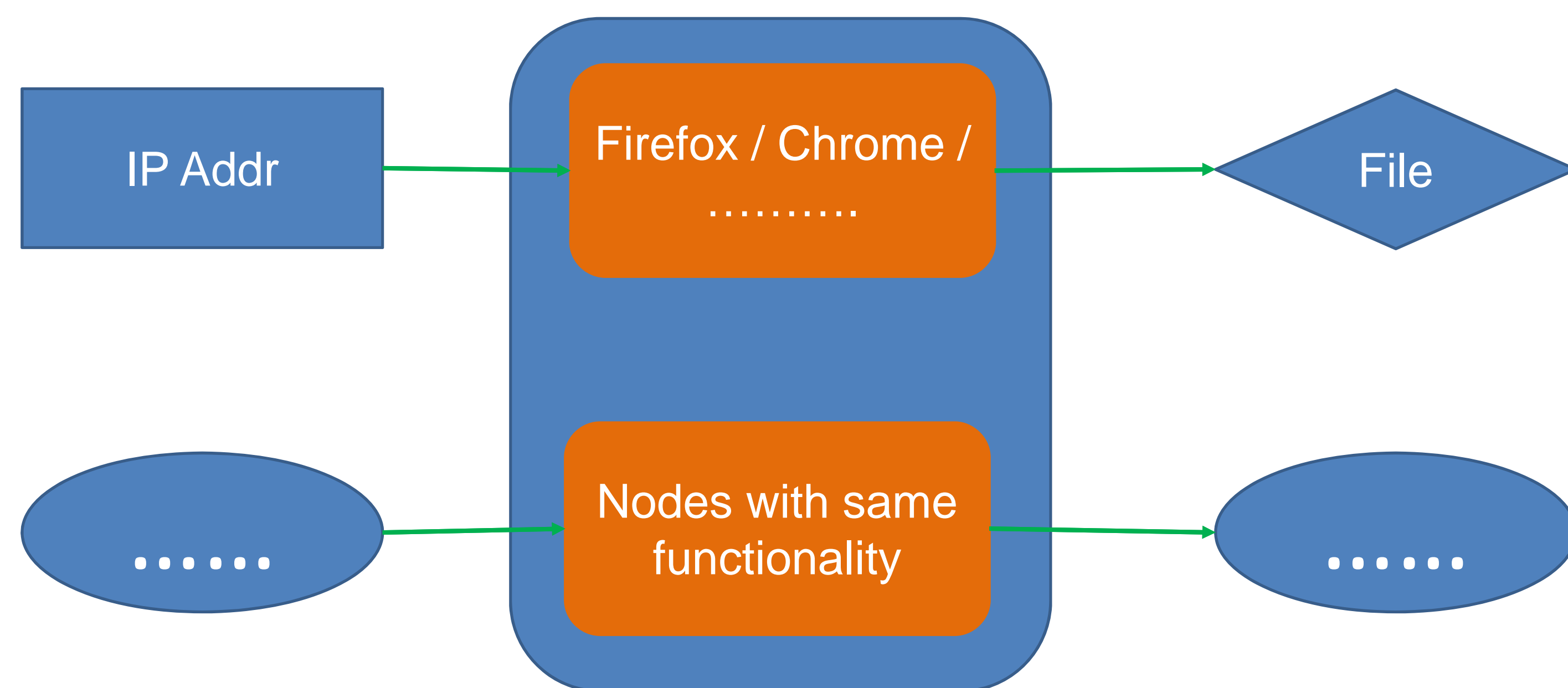
- Hadoop & Map-Reduce

- Causal Graph

- Graph Matching
- System-wide, Inter-process Interactions

- Non-uniform Behavior

- Functionality verification
- Ignore generic information, e.g. IP Address
- Focus on the functionality/behavior(reflected by system calls) instead of names



### Overview

- With LogIC, we have the ability to identify the exact source and behaviors of detected malwares. This will give us an attack sample, which could be used to detect similar attacks on other machines.
- With attack samples and logs generated by different hosts, LogAn is able to detect the same attack or similar attacks while ignoring some details like IP address.

