Pharos Static Analysis Tools

**ObjDigger**
- Analyzes OO (Object-Oriented) program and finds:
  - Classes with members
  - Methods for each class
  - Virtual function tables
  - Member accesses
  - Virtual function calls

**ApiAnalyzer**
- Signature Match
- FileIO Activity
  - CreateFile@ 0x404284
  - ReadFile@ 0x404360
  - WriteFile@ 0x404492

**PDGGrep**
- 5-Gram Chains
  - ABCDG
  - BCDGH
  - CDGHI
  - AEFDG
  - EFDGH
  - FDGHI

### Description:
- **BaseClass**
  - Member1
  - Member2
  - Member3
  - Method1()
  - Method2()

- **DerivedClassA**
  - Member1
  - Member2
  - Method1()
  - Method2()
  - Method3()

- **DerivedClassB**
  - Member1
  - Method1()
  - Method2()
  - Method3()

- **Signature Match**
  - CreateFile
  - ReadFile
  - WriteFile

- **ApiAnalyzer**
  - Function Calls
    - Func1
    - Func2
    - Func3

- **PDGGrep**
  - 5-Gram Chains
    - ABCDG
    - BCDGH
    - CDGHI
    - AEFDG
    - EFDGH
    - FDGHI

**ROSE use-def makes chains**:
- Index is built from chains
- Query is built the same way
- Insensitive to register changes
- Match or ignore constants
- More semantic than BigGrep

Contact: Cory Cohen  cfc@sei.cmu.edu

Distribution Statement A: Approved for Public Release; Distribution is Unlimited