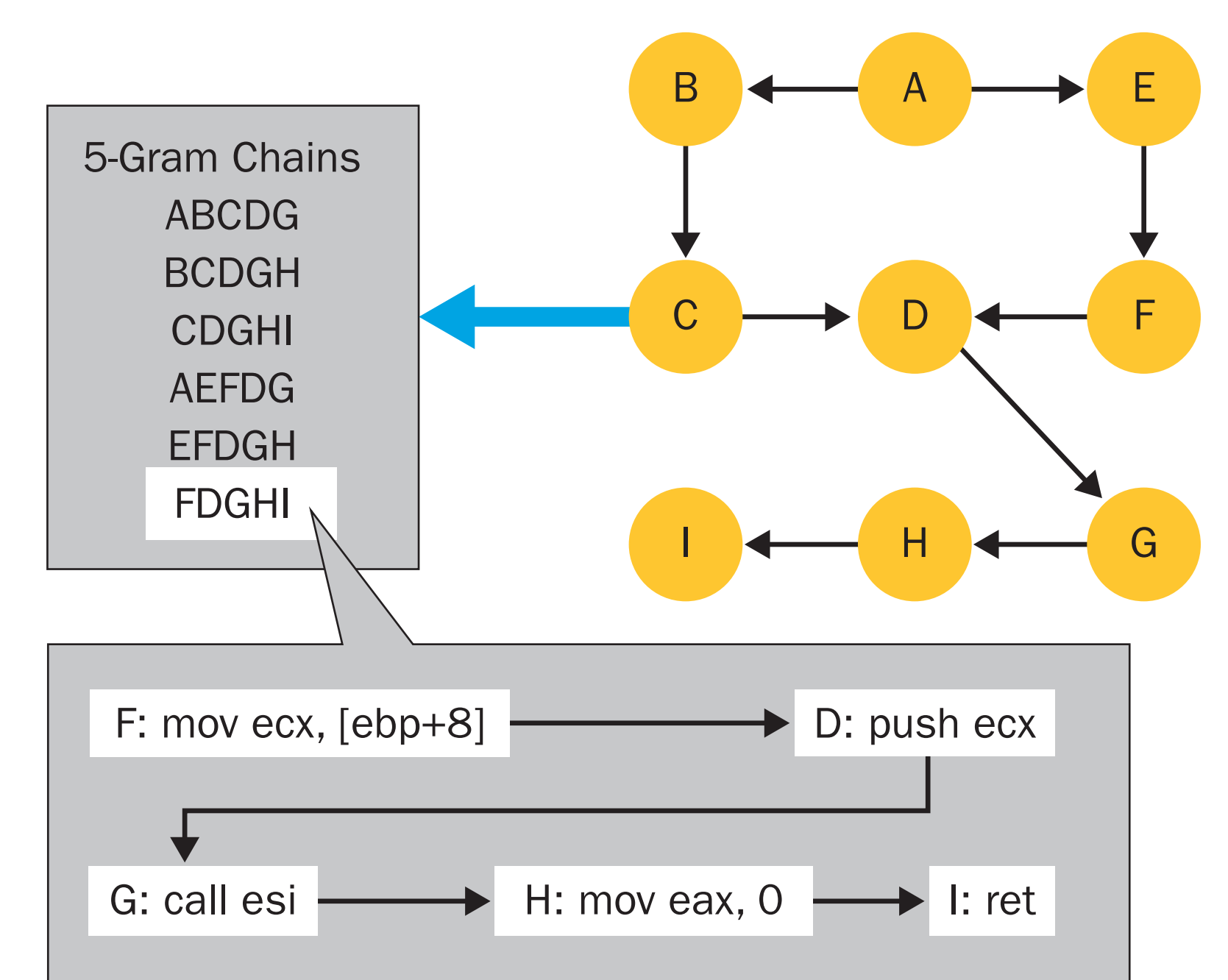
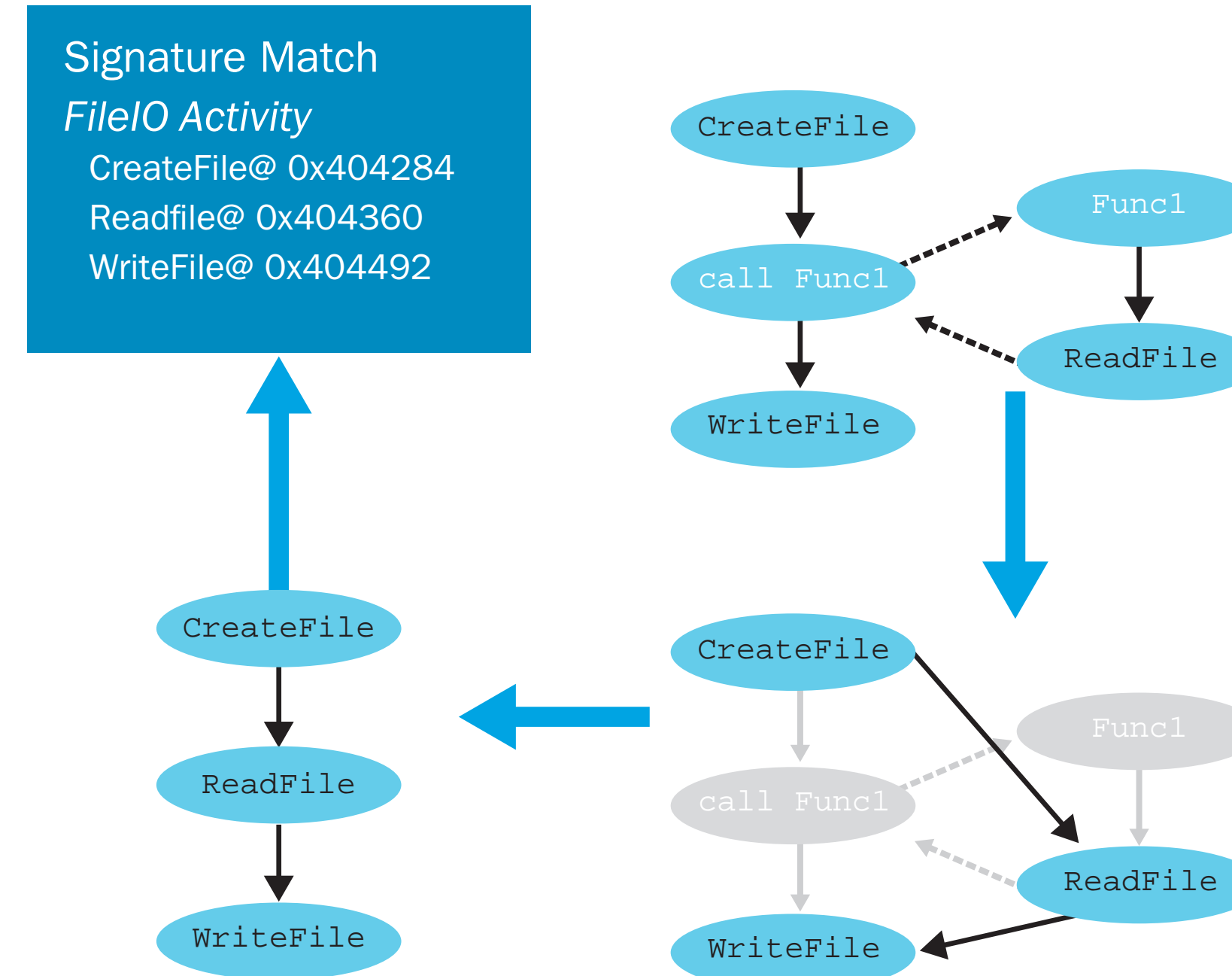
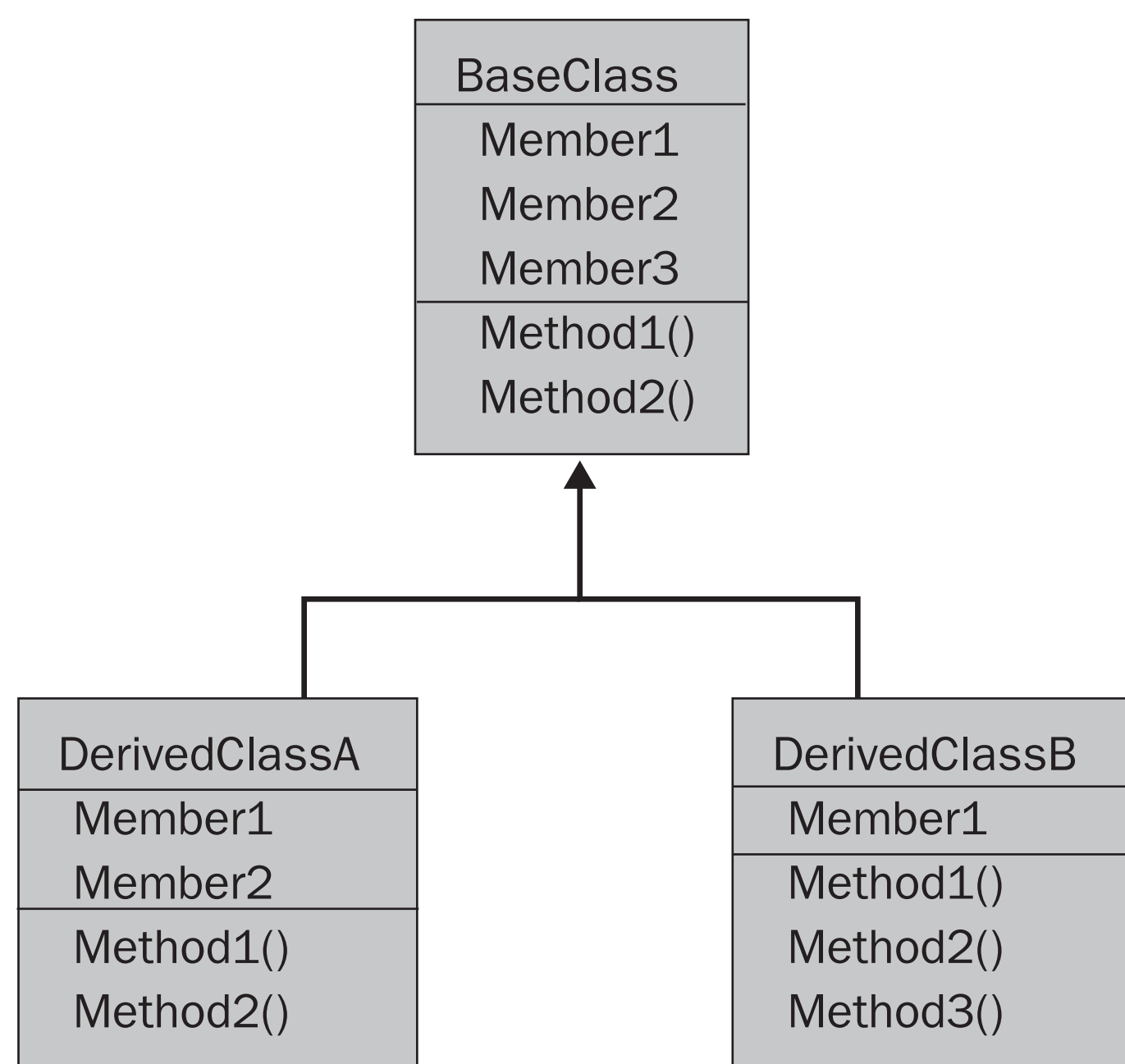
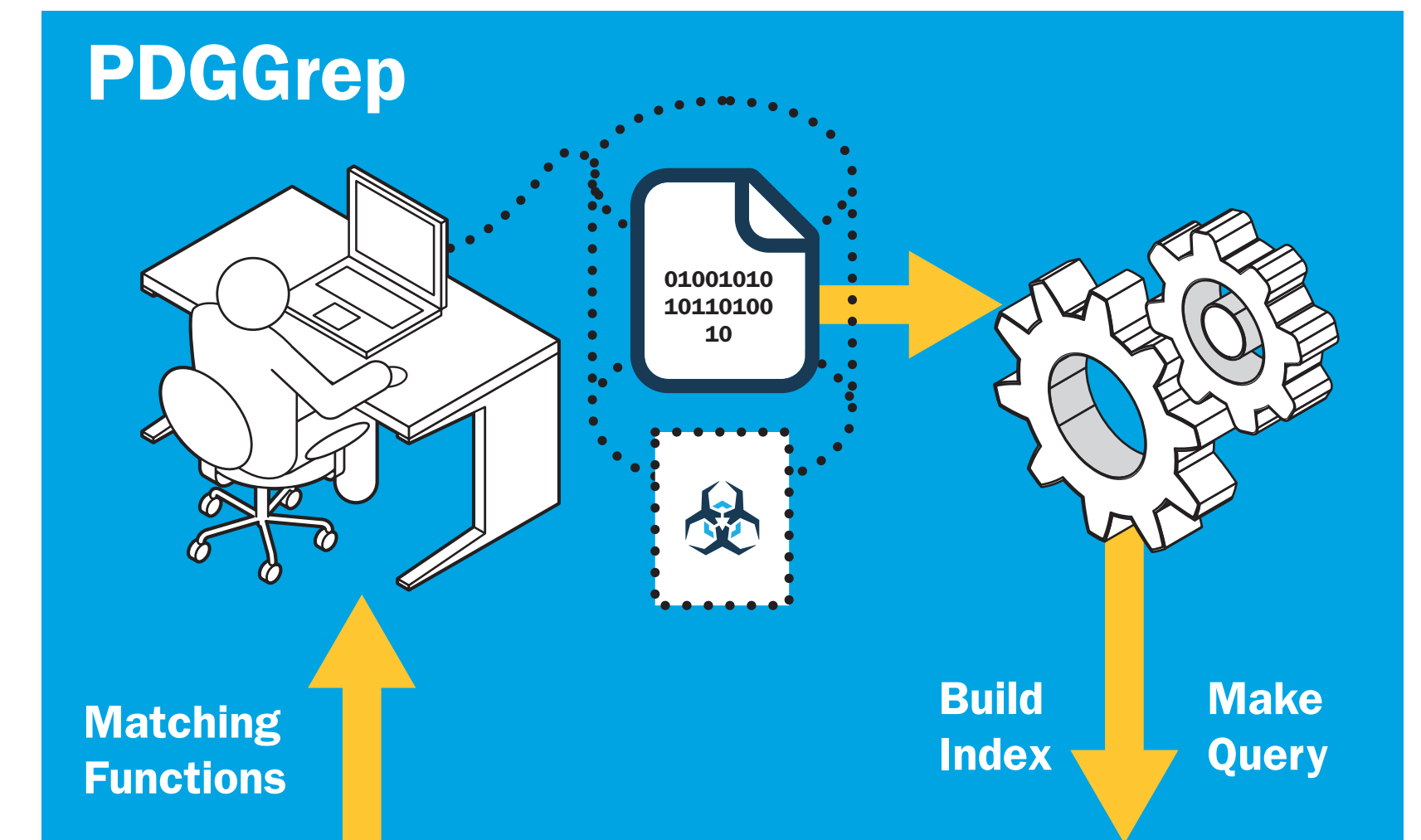
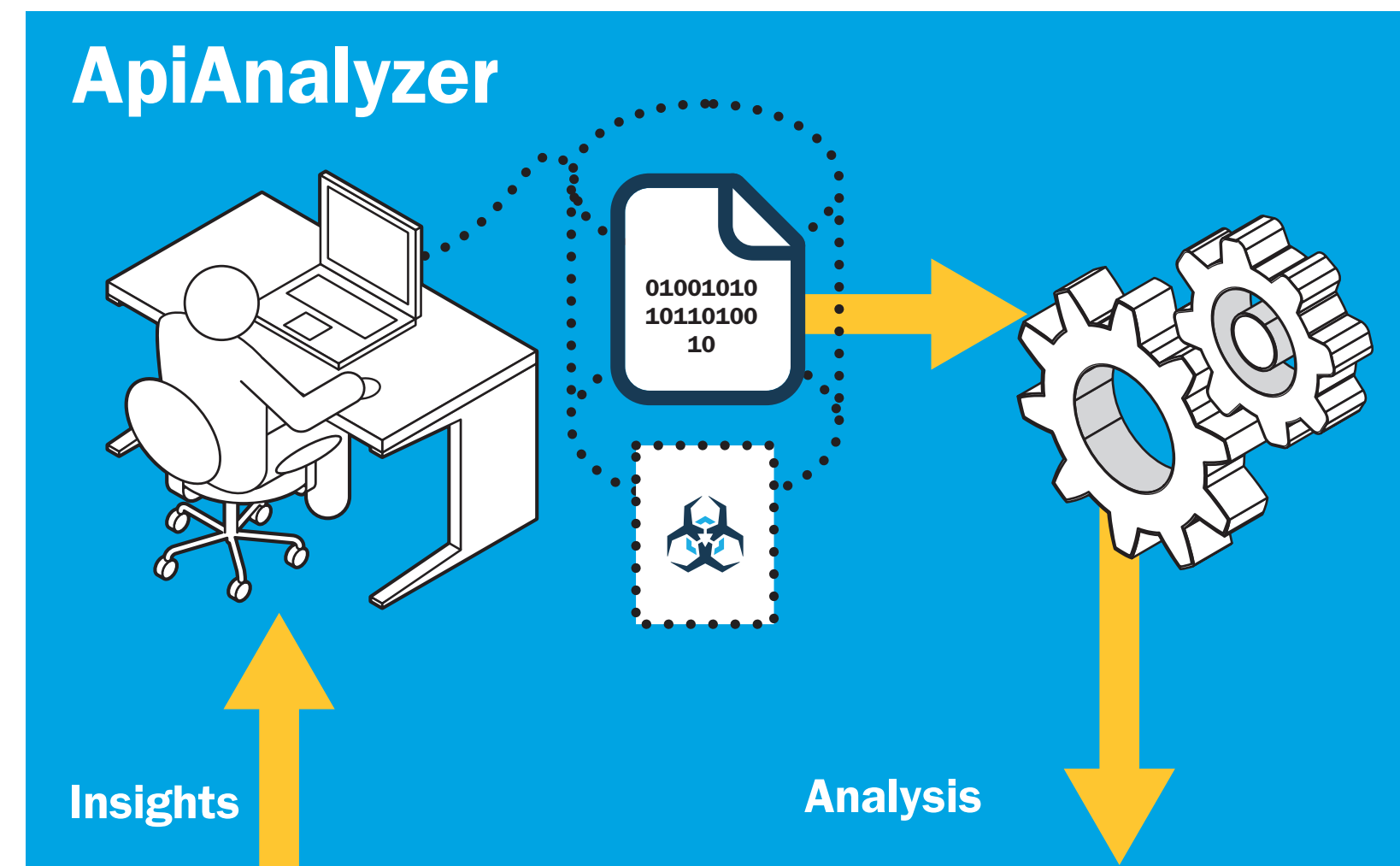
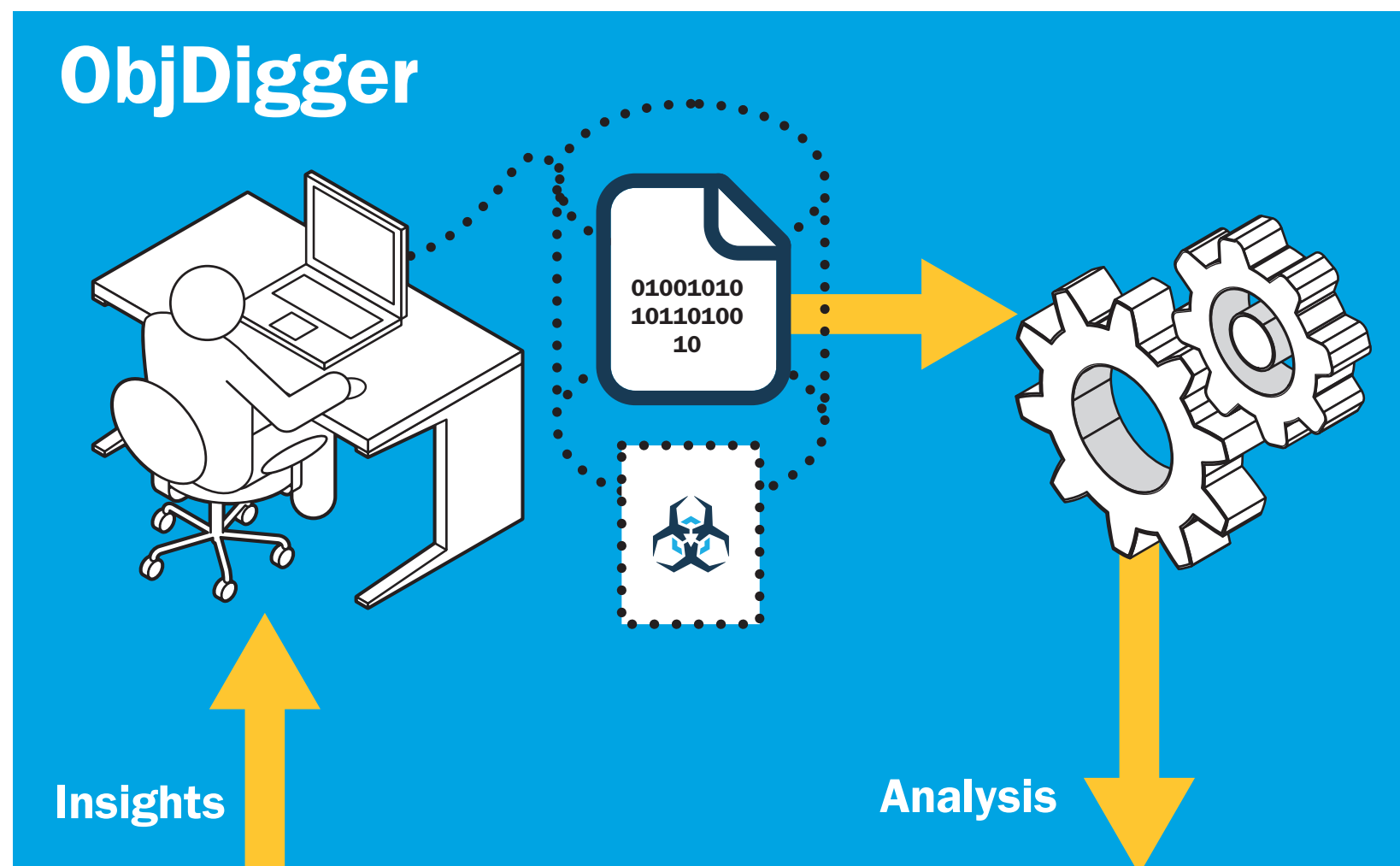


Pharos Static Analysis Tools



Analyzes OO (Object-Oriented) program and finds:

- **Classes with members**
- **Methods for each class**
- **Virtual function tables**
- **Member accesses**
- **Virtual function calls**

Analyzes API call graph:

- **Reads EXE and signatures**
- **Simplifies CFG (just API calls)**
- **Searches CFG recursively**
- **Substitutes subgraphs in CFG**
- **Returns signature matches**

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

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by Department of Defense and Department of Homeland Security under Contract No. FA8721-05-C-0003 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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Defense and Department of Homeland Security or the United States Department of Defense.

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.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

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

DM-0002833