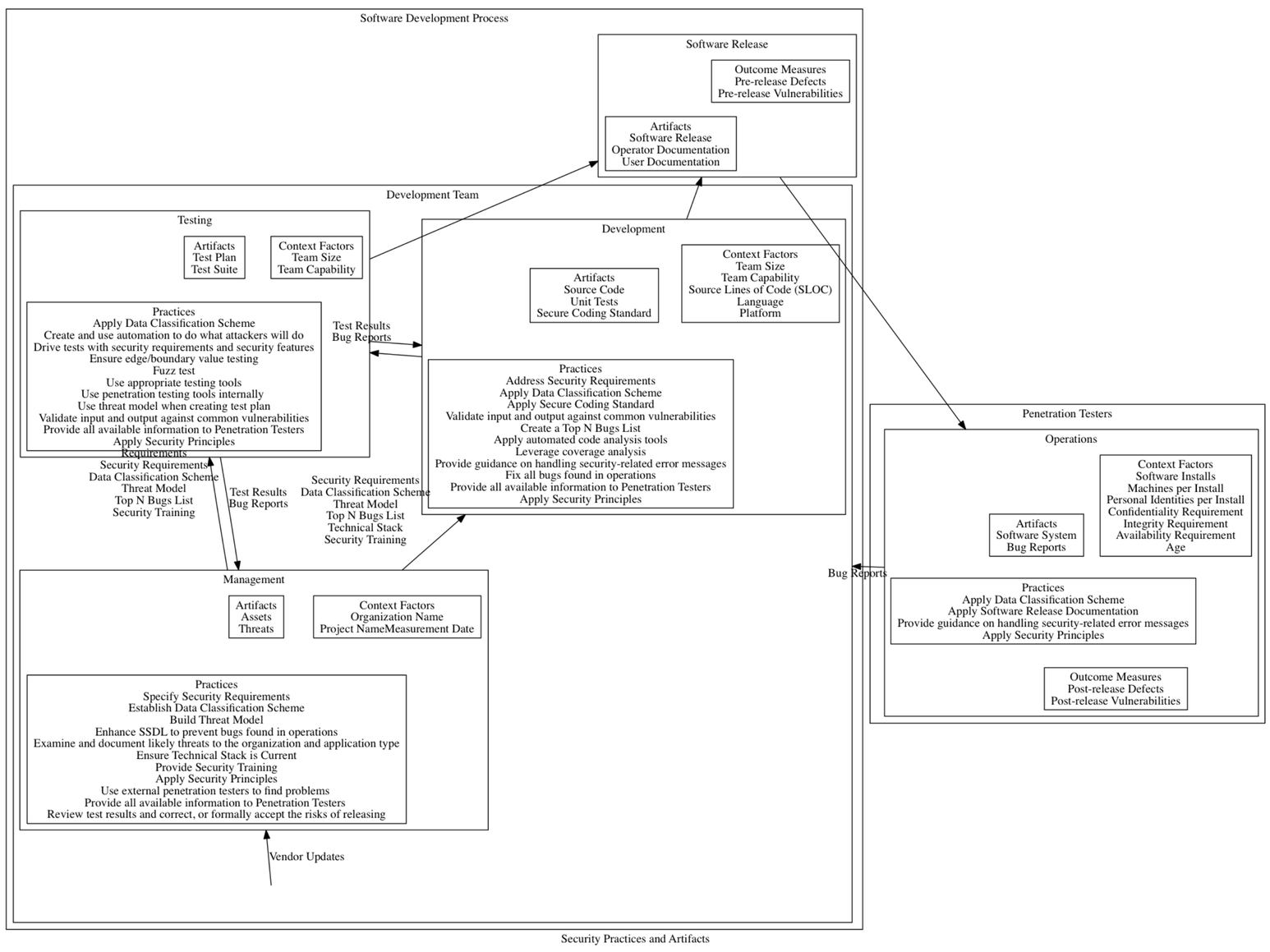
Building a Security Practices Evaluation Framework

Patrick Morrison, Laurie Williams
Department of Computer Science
North Carolina State University
pjmorris@ncsu.edu, williams@csc.ncsu.edu



Practice Adherence Metrics

- Practice
  - Usage - How often is this practice applied?
  - Ease of Use - How easy is this practice to use?
  - Utility - How much does this practice assist in providing security?
  - Training – Has the practice been taught?
- Artifact
  - Channel – How is this artifact delivered?
  - Source – Who created this artifact?
  - Type – How rigorous is this artifact?
  - Assurance – How is this artifact's use checked?
  - Revision – How often is this artifact revised?

Impact

- The Security Practices Evaluation Framework (SP-EF) supports empirical measurement of software development security practices and their effect on security outcomes.
- Teams can used the collected data to drive practice selection, prediction, and process improvement.
- SP-EF based replication and accumulation of data across projects and environments supports cross-project validation.

Schedule

- Now: Two case studies of open source projects are being conducted using the SP-EF data elements and guidebook.
- The year to come: Conduct studies in industrial environments, validate model, iterate over framework based on data collected. We have begun discussions with industrial partners.

http://hot-sos.org/

The Science of Security initiative is funded by the National Security Agency.