# PACE Prototype Update

18 October 2021

Huntington Ingalls Industries

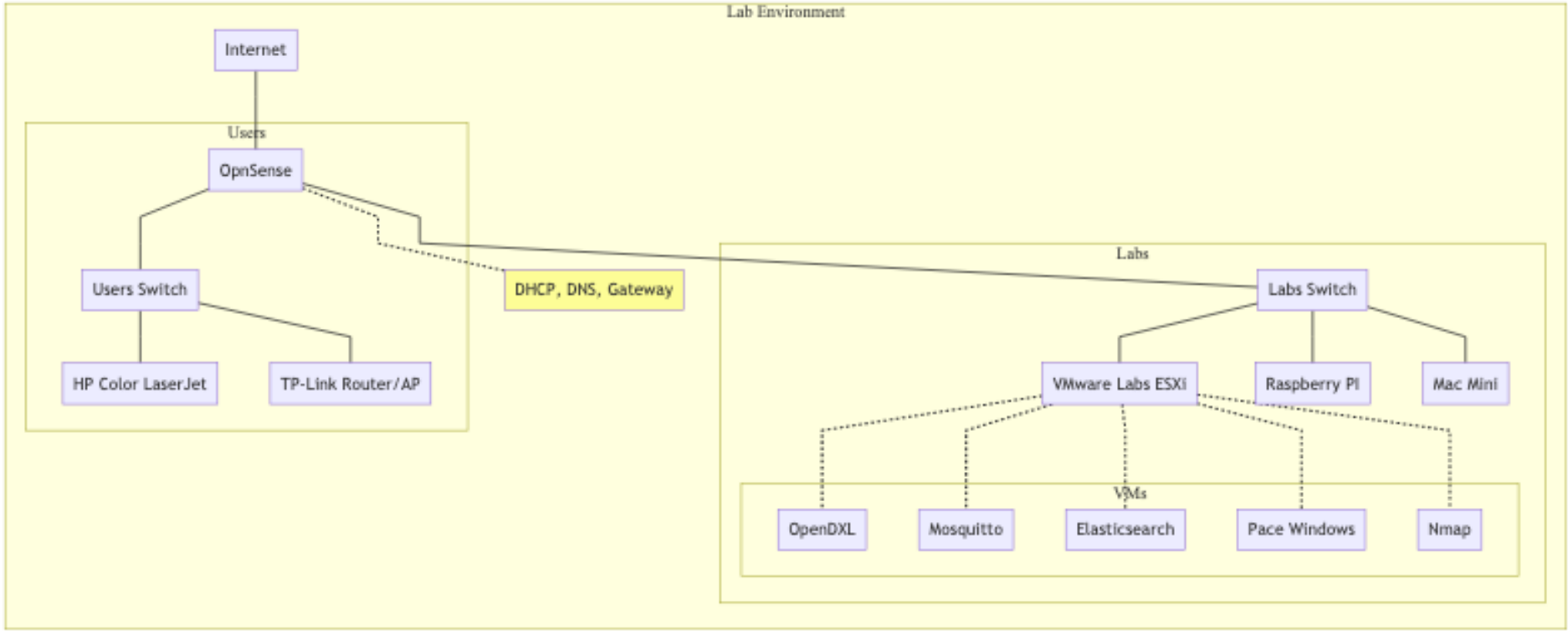
Hard Stuff Done Right™

# Prototype Components Mapping

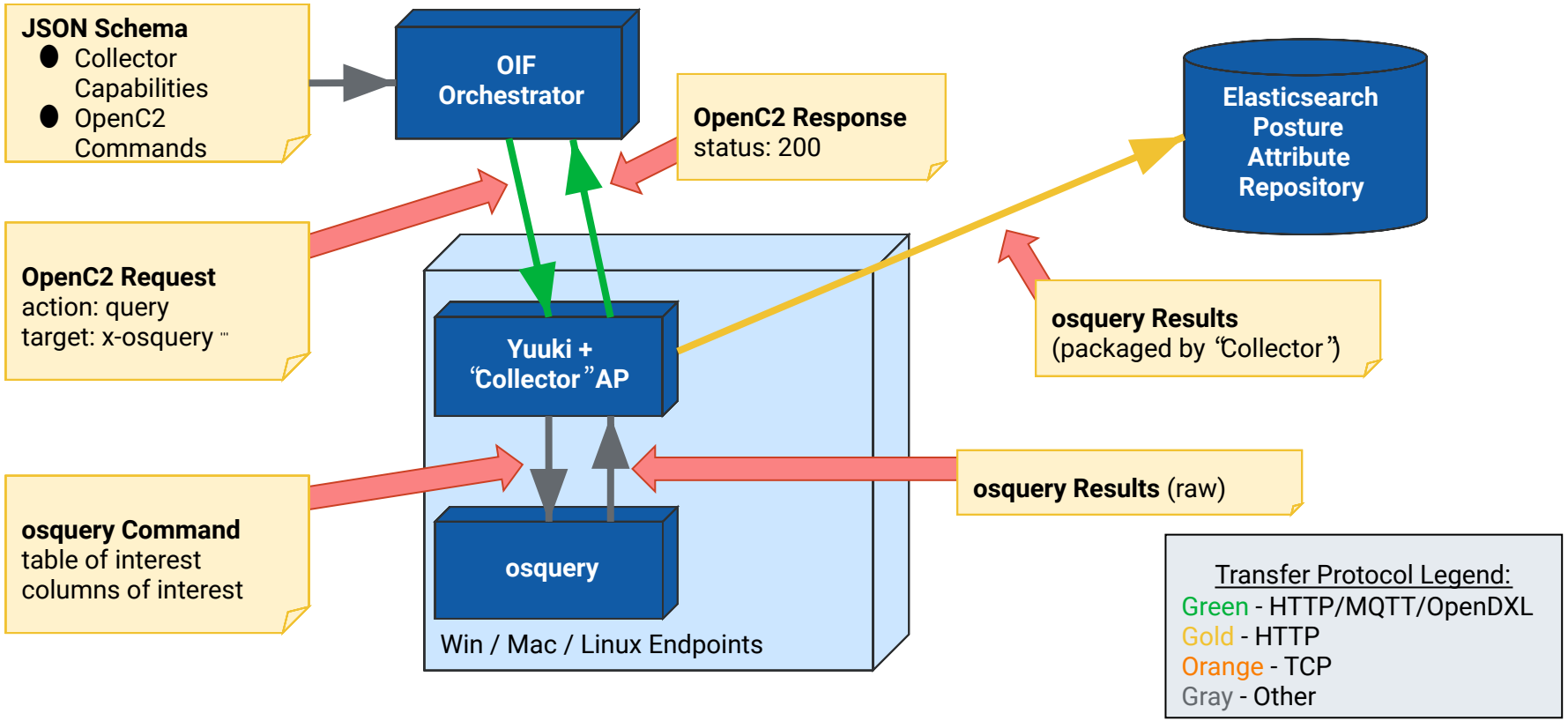
| SACM Components | PACE Components |
|---|---|
| Manager, Orchestrator | OIF-Orchestrator |
| PCS | Yuuki + “Collector” Actuator Profile(s)<br>*OIF-Device + “Collector” AP(s)* |
| Collection Engine | osquery, nmap |
| Posture Attribute Repository | Elasticsearch |
| Posture Evaluation Service | *(future - TBD)* |
| Endpoints | Windows, Mac OS, Linux, Raspbian,<br>*OPNSense, others TBD* |

*italics indicates future work / capability*

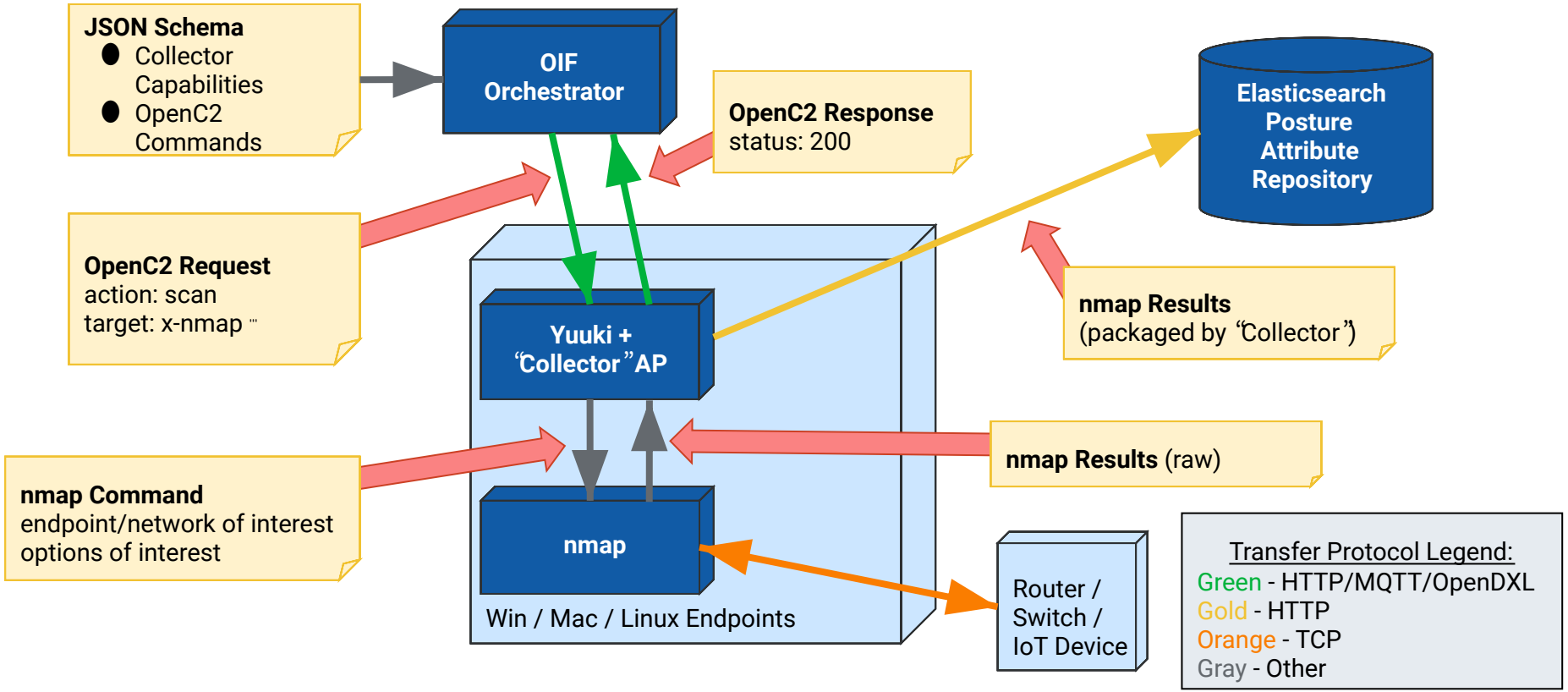
# PACE Prototype Demonstration Network



# Example Information Flow Using osquery



# Example Information Flow Using nmap



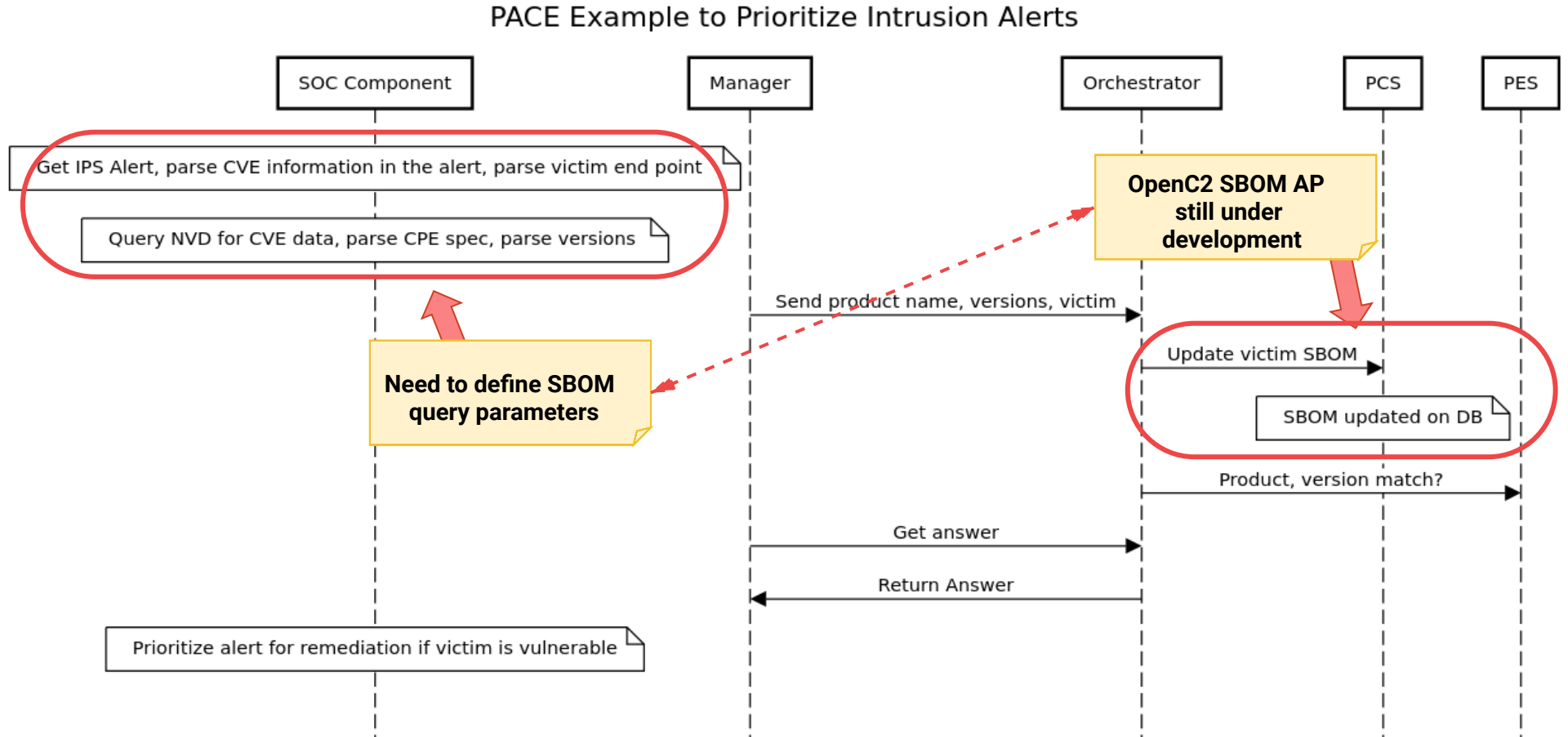
# Current Activities

- Actuator Profile Definition
  - for osquery
  - for nmap
- JSON Schema Development
  - Required OIF-Orchestrator for Command Construction, Response Validation
  - Need schema content for osquery tables
    - 277 total tables available
    - 51 tables common to all supported OSes

# Pending Activities

- Integration with McAfee-supplied use cases
  - Need to define interface(s), information flow
  - Need to convert trigger information into posture query parameters
- Add Posture Evaluation
  - Need Posture Evaluation capability
  - Possible OpenC2 Language Extension
- Create Use Case Contributions to OpenC2 Language Development

# McAfee IPS Use Case



# McAfee STIX Use Case