



# Building from the Pilot Effort... Next Steps

# Next Steps

## Mature the Common Event Record

- Solicit input on completeness of version 1.0
- Must be able to morph to new CER formats and providing backward compatibility
- Address scaling issues with respect to the record size and consider other data representation formats
- Include second order events such as Measurement/Performance
- Incorporate a mechanism for more granular correlation of events

# Next Steps

## Scale the diagnostic backplane

- Adopt a real Authz/Authn methodology
  - We use certificates at this time, but management is an issue
  - Shibboleth non-web version ready
- Provide an anonymization API to provide capability to satisfy policy where necessary
- Transport method evolution (to SOAP?)
  - Remove the dependency of SCP
  - Add real-time flow capability
- Migration from Python or offload compute intensive areas to another language
- Management and Configuration
  - Centralized configuration
  - Keep the configuration work on the clients hands free

## Add Applications

- Domain specific
  - Work with middleware application, network, system, security groups to build focused apps based on what we've learned from scenario writing process
  - Discuss performance/measurement with external groups
- Mature and establish a base application with GUI interface for forensics and reporting
  - Reporting – feed appellations like cricket and crystal reports
  - Forensics – need a client GUI interface that is ported to Linux, Mac and Windows

## Add Applications

- Build simple but high value tools that extract information from the archive and not the DB
  - Summaries of events
  - For retrieving data that is not sent to the DB
- Verson1 of the Event API
  - Acquiring a real-time event flow from any node
  - Simple data locator service (where can I find this data)
  - Querying data repositories directly but be conscious of future capabilities where agents may mine data over multiple repositories

# Next Steps

Getting traction with other groups has been difficult but...

- Assemble a ccBay early adopters group
- Composed of key I2 campus stakeholders
  - CMU and Duke thus far
- Soliciting feedback from others on new and existing features
- Involve members in development efforts
  - Retrofitting existing diagnostic applications to use backplane
    - OWAMP, SurfNet Detective, UT
  - Build new normalization agents to provide more granularity of the event and consider a mechanism for registering them
  - To assist in developing core components