IETF 86 - Orlando

Security Automation and Continuous Monitoring (SACM) Use Cases

Adam Montville, amontville@tripwire.com
David Waltermire, david.waltermire@nist.gov

URL: http://tools.ietf.org/html/draft-montville-sacm-asset-identification-04

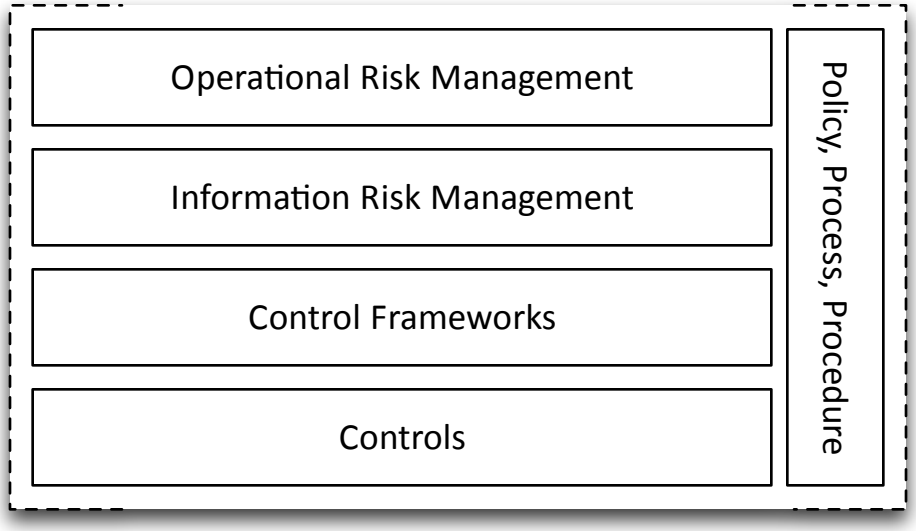
Abstract:

This document identifies use cases, derived functional capabilities, and requirements needed to provide a foundation for creating interoperable automation tools and continuous monitoring solutions that provide visibility into the state of endpoints, user activities, and network behavior. Stakeholders will be able to use these tools to aggregate and analyze relevant security and operational data to understand the organizations security posture, quantify business risk, and make informed decisions that support organizational objectives while protecting critical information. Organizations will be able to use these tools to augment and automate information sharing activities to collaborate with partners to identify and mitigate threats. Other automation tools will be able to integrate with these capabilities to enforce policies based on human decisions to harden systems, prevent misuse and reduce the overall attack surface.

Abstract has been updated to reflect altered scope.

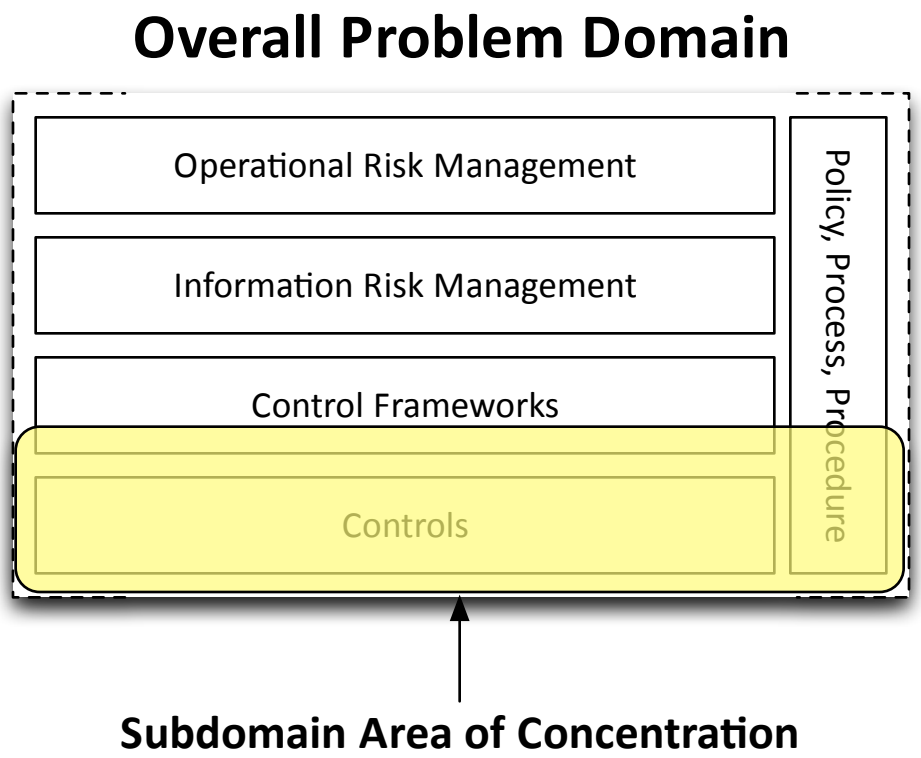
Frame Of Reference

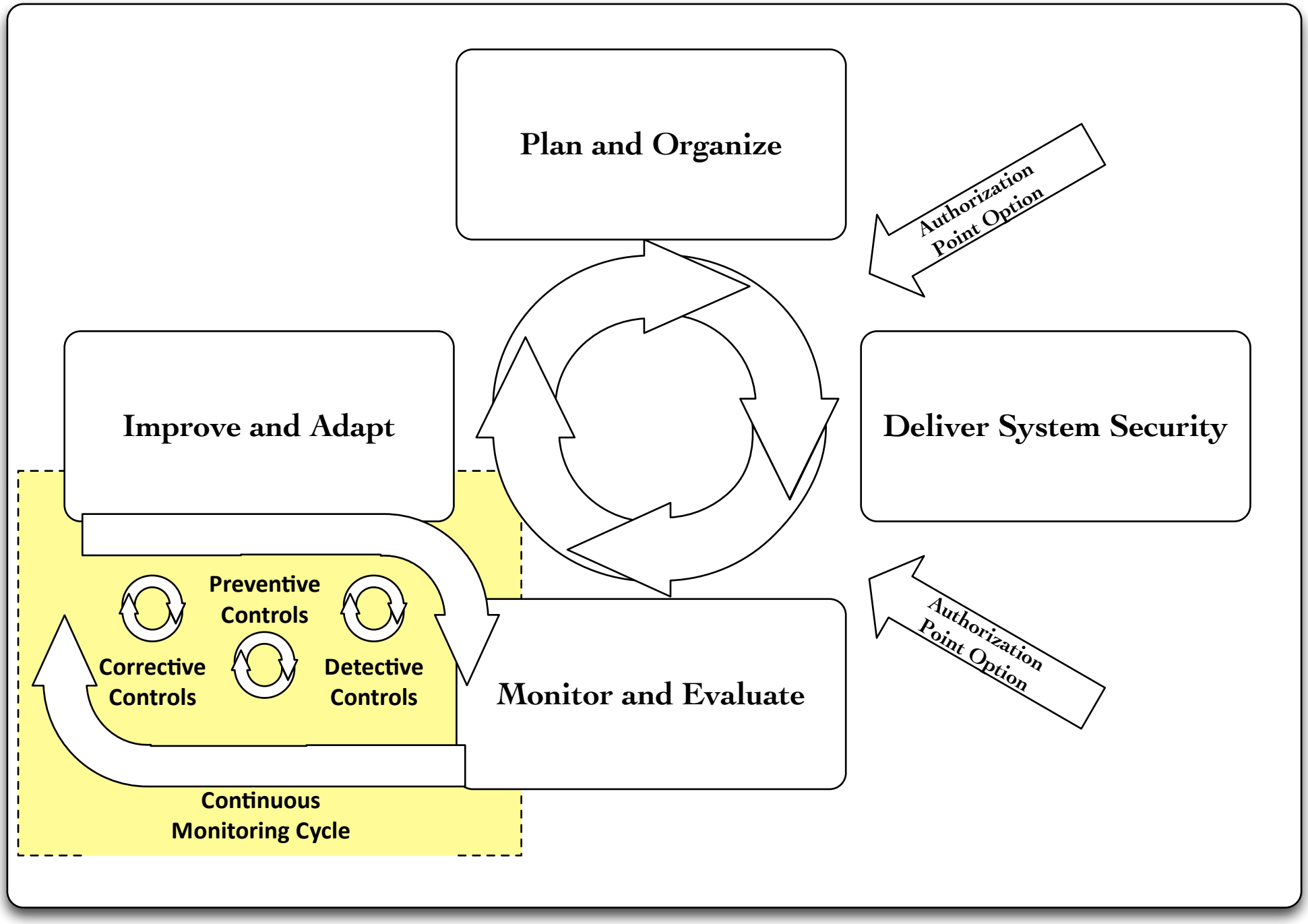
Overall Problem Domain



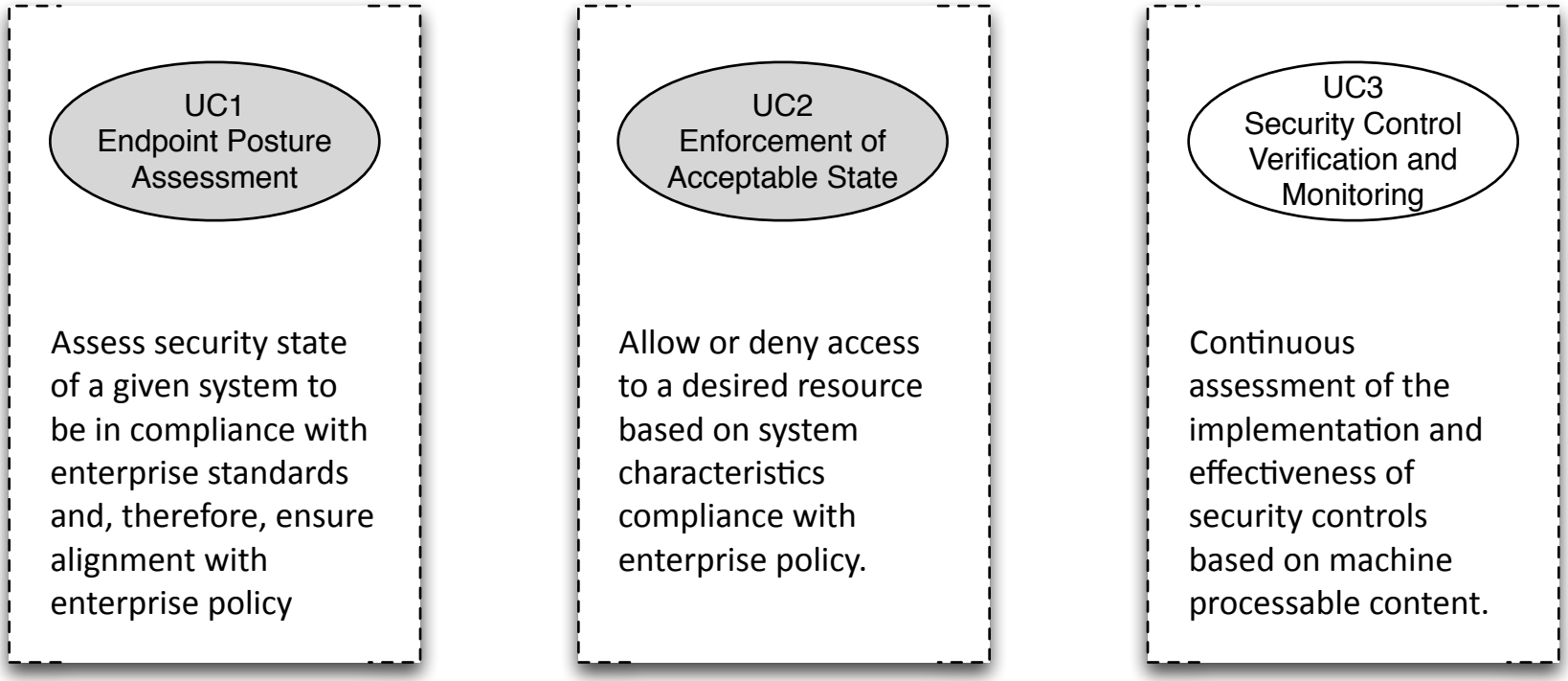
A refresher from our Atlanta BoF...

Frame Of Reference



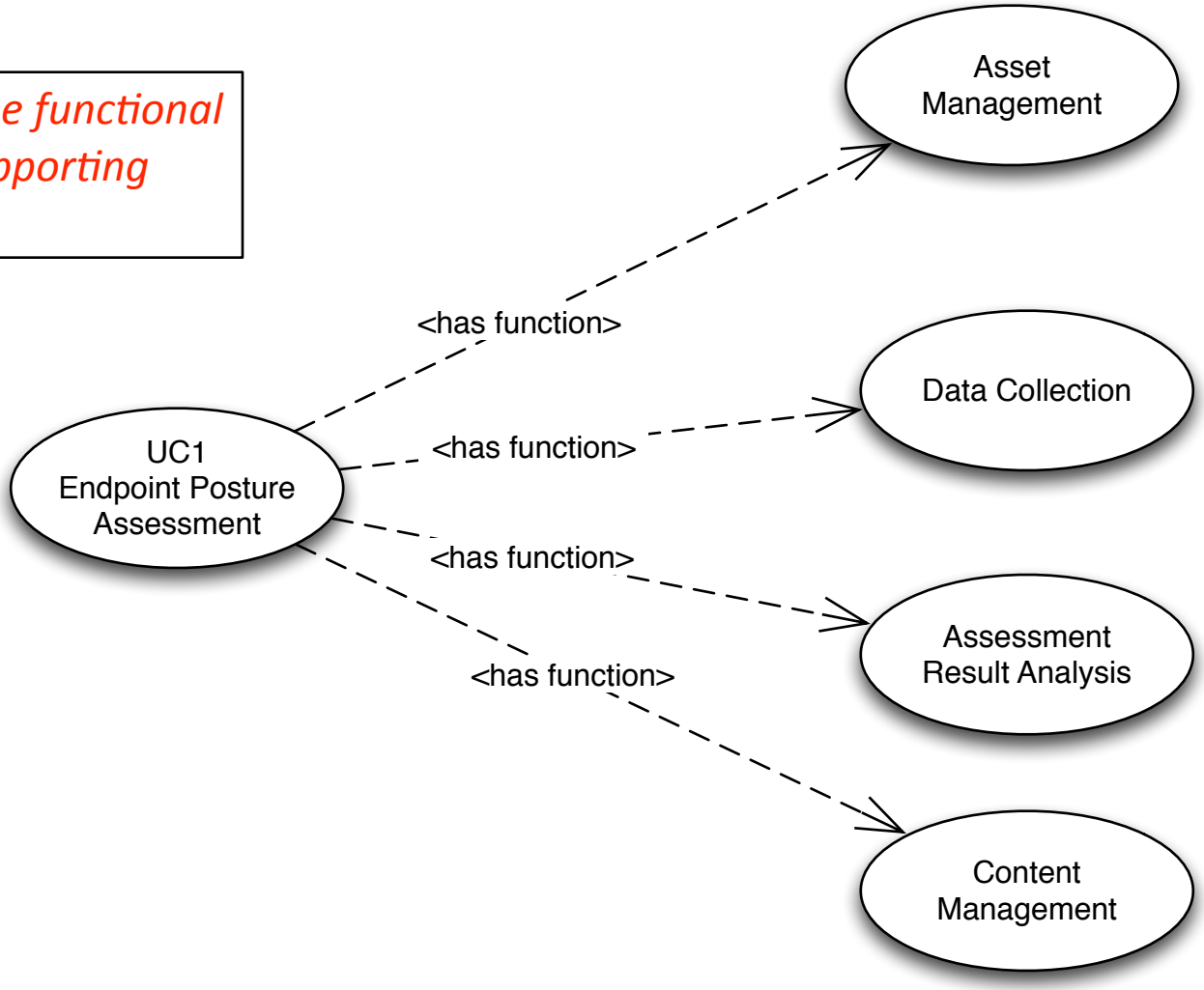

Plan and Organize
Authorization Point Option
Improve and Adapt
Deliver System Security
Preventive Controls
Corrective Controls
Detective Controls
Monitor and Evaluate
Authorization Point Option
Continuous Monitoring Cycle

Use Case focus has changed slightly for UC1 and UC2, but pretty much the same.

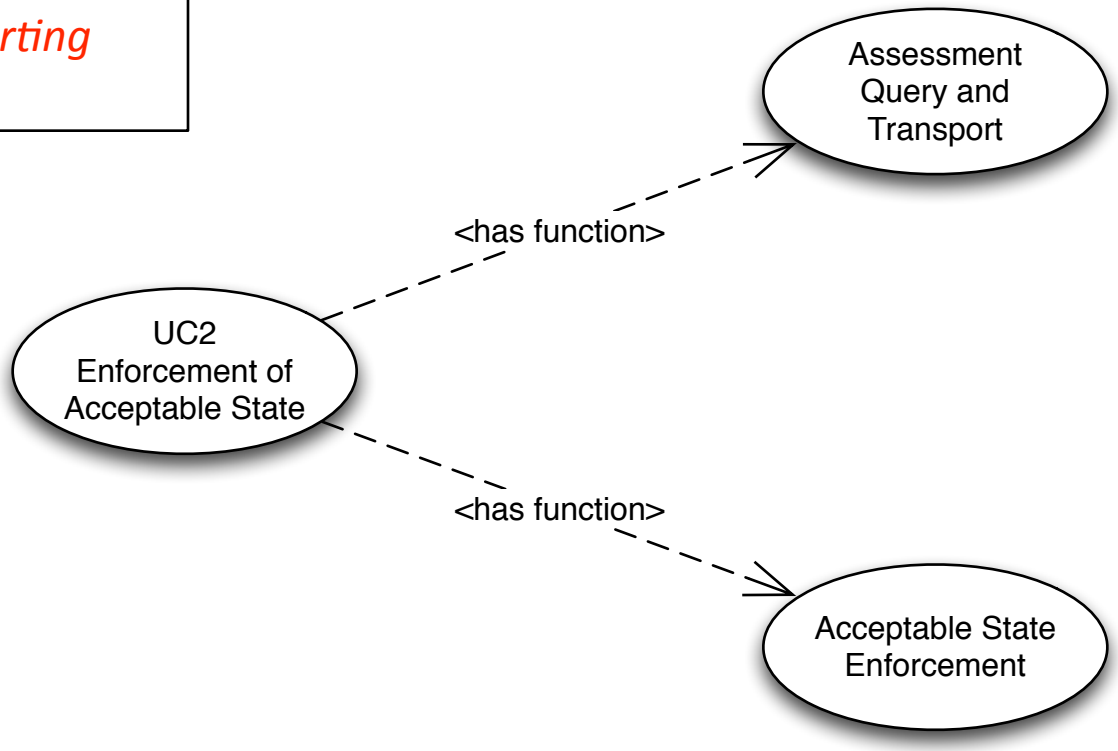


Possibly change "Asset Management" to "Asset Scoping"

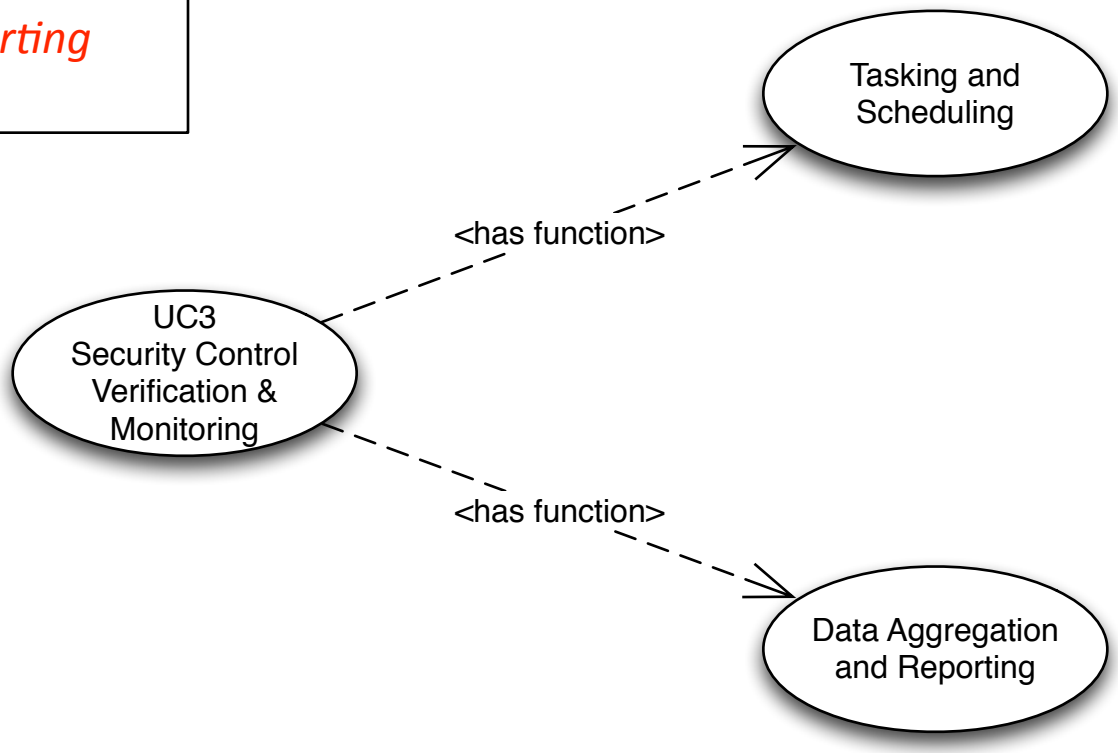
Streamlined the functional capabilities supporting UC1.



Streamlined the functional capabilities supporting UC2.



Streamlined the functional capabilities supporting UC3.



Open Issues:

1. Are updated use cases sufficiently narrow?

2. Are updated use cases aligned with draft charter?

3. Thoughts around renaming "Asset Management" to "Asset Scoping"?