VANDERBILT UNIVERSITY

Creating and Managing Secure Research Environments

Heather Mitchell and Allen Karns
Vanderbilt University

Leveraging the cloud for secure and compliant research environments

- First request in 2018 – ITAR, GovCloud, and a long wait
- 2019 -- a repeatable, pre-approved template
  - Infrastructure-as-Code
  - NIST 800-171
  - Vanderbilt Internal Audit blessed
  - Up in an afternoon
  - Default for all accounts

Intake Process

- Many paths
  - Sponsored Programs Administration > VUIT Security
  - Relationship Managers
  - Other researchers
- Determining the level of compliance
  - Data Use Agreement
  - Other grant terms
  - Our default

Technical Approach: Setup

- SRE template account
  - Used for testing
  - Hosts scripts, tools, reports
- CloudFormation stacks
  - BitBucket repository
  - Future = CI/CD pipeline, Terraform
- CIS benchmarking
  - Windows – UserData, GPO, run-once script
  - Linux -- UserData

UserData:

mkdir Assessor-CLI && cd Assessor-CLI

aws s3 sync s3://ssre-userdata-files/Linux/Assessor-CLI ./

chmod 755 Assessor-CLI.sh && ./Assessor-CLI.sh -b /benchmarks/CIS_Amazon_Linux_2_Benchmark_v1.0.0.1- xccdf.xml –html

cd /Assessor-CLI

aws s3 sync reports/ s3://ssre-userdata-files/Reports --exclude "*" --include "*.html"

aws s3 sync /var/log/ s3://ssre-userdata-files/Reports --exclude "*" --include "user-data.log"

Ongoing Monitoring

- Initial CIS Assessor report
- Splunk – different alerting threshold
- Rapid7
- Microsoft Defender ATP