2022-05-16 Meeting notes

Date

16 May 2022

Attendees

- Daniel Lyons
- Andrew Kapuscinski [X]
- Nathan Bockisch [X]
- Sam Kagan
- Stephan Witz
- Thomas Chamberlin
- Adriana Escobar De La Torre
- Michael Brice
- Pat Murphy
- Wade Craig
- Matt Chauta

Goals

- Incident response
- Dependency management
- Secret storage
- Security policies in general
- Plan future collaboration between these groups and CIS/Security

Discussion items

Time	Item	Who	Notes
	Introduction	Stephan Witz	

Notes

- If there is a security incident, inform your supervisor and email iso@nrao.edu.
- For the master security policy, read the CIS pages; it's part of the annual policy documentation
- CIS has no official secret manager or secret storage platform
- Instead of setting a big shared destination, enumerate some wrong practices and provide alternatives
- Guidance about where to put passwords should be part of onboarding in each group (even if the answers are different)
- When passwords need to be shared between humans, put them in a file and upload to astrocloud with a short expiry
- Vulnerability testing will be performed with Rapid7 Insight
  - An agent process collects metrics and makes reports
  - Wade will share a link to the rapid7 agent installer for containers
  - Need to collaborate with Wade about informing him of expiring containers so that licenses can be freed
- When a new public-facing system is brought online, make a helpdesk ticket to request a public security test
- Each group should deploy a password check-in prevention tool
  - Git Guardian, there is another one
  - It can be a plugin for gitlab
- Dependency checking can be automated with dependabot (which can be a plugin for gitlab)
- We will provide some kind of class on different attacks/vulnerabilities
  - There will be a joint presentation from SSA and CIS on this later on
- SonarQube can also be used to perform automated security scans of the code, along with other aspects of the code
- Need a clearinghouse for platform-specific knowledge transfer between groups (like Django)

Action items

□ Wade Craig Share a link to the Rapid7 agent installer

□ Daniel Lyons Collaborate with Patrick Murphy on a vulnerability presentation

□ Every developer: try out these tools