Security SIG Update

- **Charter was revised and voted on.**
  - We’re legit!
  - We’re also open to everyone! #hpc-security in the CUG Slack!
- **Leadership was voted on.**
  - Chair: Aaron J. Scantlin
  - Deputy Chair: Alden Stradling
- **Poll for meeting frequency in Slack – go vote!**
  - Monthly, every other month, or quarterly Zoom meetings?
- **We have a mailing list! Ask questions!**
  - security-sig@lists.cug.org
- **Initial round of content ideas solicited.**

Initial Round of Content Ideas

Discussion of TLP:RED discussions

  - Vendors are very uncomfortable with discussion of pre-disclosure embargoed and NDA material coming through insecure channels.
  - TLP:RED is mostly removing attribution for reputational or other preference reasons All CUG attendees and invited CUG-adjacent parties can participate in the SIG discussions
  - Getting momentum behind initiatives that are NDA or embargoed can be more complex, but using SIG participation to find like-minded folks with similar needs can help get things started even if direct discussion in SIG meetings and channels remains impossible.

Discussion of what the SIG will do, what its use cases and patterns will be

- **Victor Holanda (CSCS): Allow organic growth — don't limit it artificially**
  - Alden: Agreed — looking for seeds of what we're shooting for, not constraints on the scope
- **V: Want discussions of secure development lifecycle and zero trust techniques and processes**
- **V: IOC — Indicatiors of Compromise monitoring**
- **V: Training and user awareness are central to security.**
  - A: Joint training and shared information about trainers and vendors that do a good job. Discussion of Kubecon experience with Kube security pros
- **SOAR**
- **Dennis Walker: Addressing integration friction: address site baselines, but site threat models vary greatly. Site-specific baselines are something that would be nice to have**
- **Prentice Bisbal: Security vs performance, security vs. usability**
- **Larry Kaplan + Dennis Walker: Issue curation — what's most important to the majority of the customers?**
  - Launches a discussion of how to get the SIG behind real security requests — setting up a SIG-wide issue numbering system to allow for voting on issues and giving a common reference for CASTs to be binned together for high priority
  - Use Box.com subscription somehow for shared doc?
- **Dennis Walker: Sharing security mitigation techniques and even code when possible**
- **Paul Tomlinson (AWE): Addressing concerns with timezones in regional support**
- **Establish secure channel on Slack?**
  - No — just too much effort and risk to maintain invites and curation
- **V: Communicate about regional standards and how they interact, like with the NIST + UNZA standards releasing next week**