Insider Threat Workshop Synopsis

SPONSORED BY DOD HPCMP, NIST, NSA, NSF

DECEMBER 12, 2017

LORTON, VA

Workshop Genesis & Overview

- Insider threat is the primary of the top three security concerns within NSF, DoD, and NSA HPC communities.
- Participants were generally a mix of government, military, and academic system owner/sponsors.
- One day workshop to develop a system owner perspective for HPC systems. Objectives included:
  - Understand the nature and extent of the threat
  - Identify challenges and gaps associated with threat mitigations
  - Highlight potential actions and best practices to protect HPC environments

Major Takeaways

1. Insider threat and anomalous behavior are continuing and critical problems affecting HPC agencies
2. Most agencies have insufficient protocols, processes, systems and personnel in place to mitigate the threat in any meaningful way
3. There is no common definition of Insider Threat / Anomalous Behavior across federal HPC agencies
4. Individual agencies have not identified most probable use-cases and certainly not "Black Swan" (high impact, high surprise) use-cases
5. Developing effective monitoring and counter-insider threat strategies is futile without first attending to item 4 above
6. An effective first step in a program to more aggressively manage the risks would be to define agency-specific use cases and exploit these as the basis for planning an effective response