Discussion of the Security Concepts at NHR@Göttingen from 1000 Feets

Hendrik Nolte
Security Onion NHR@Göttingen

- Security Onion with 4 Layers
- Most sensitive systems at the top
- `ssh` access to admin nodes only
  - from an isolated admin-network
  - using sk keys on the JumpHost
- Only Movement downwards permitted
  - Enforced via node-local firewalls
Security Onion NHR@Göttingen - Layers

- **Layer 0**
  - Most sensitive Systems
  - JumpHost, Syslog Server, etc.
  - Administration via special clients

- **Layer 2**
  - Management Nodes with daemons
  - e.g. slurmctld, licenses, filesystems

- **Layer 1**
  - Everything between Layer 0 and 2
  - e.g. Admin Master

- **Layer 3**
  - user nodes
Islands and Networks

- Admin (T0-T2) and user nodes (T3) are separated into islands
- Each islands has 4 LANs:
  - PXE
  - BMC
  - User
  - Management
- User and admin LAN’s are, if required, routed
- Port isolation can be enforced on externally managed switches
- High-Speed interconnects, e.g. OPA, or Infiniband, are treated additionally
Compliance Checking

- Compliance checking on all nodes
  - Continuously during runtime
- Methodology
  - Create security concept for each node
  - Derive legitimate system state
  - Determine critical components
  - Check them via Icinga/Nagios
    - Simple checksum
- Components
  - iptables, ssh files, kernel modules
- Purpose
  - Not for intrusion detection
  - Proactively prevent vulnerability due to under-coffinated admin

Components:

- iptables
- ssh files
- kernel modules