# Network Security Summary

F2F 50 - June 2020

# Overall Goals

# Major Goals of the NetSec Team

Move to Automated Security Provisioning

- Implies a defined configuration/deployment method
- Integrates well into general SIEM structures
- Less prone to the “insufficiently trained staff” explanation
- Easier to identify changed profiles caused by intended maintenance
    - Thus, easier to identify hostile changes as not fitting the profile

# Major Goals of the NetSec Team

- Replace outdated or poorly worded requirements
  - Threat technology has moved on
  - Requirements have too many “get out” clauses
  - Requirements are no longer effective given newer architectures
- Examples
  - Multifactor Authentication is available vs. Outdated password policies
  - Account Lockout after *n* bad password attempts
  - VMs/Containers run by Cloud providers, but controlled day-to-day by CAs

# Major Goals of the NetSec Team

- Close the Gaps
  - Identify where the NCSSRs don’t adequately address identifiable threats
  - Examine state of the art
  - Propose ballots to require best practice as described in current literature
  - Align better with the BRs

# Subgroups/Teams

# Pain Points Team

- Reviews comments received from the WebTrust Task Force
- Proposes ballots to remediate WebTrust comments
- Works on Outdated Requirements
- Adding Automated Security Provisioning where possible

# Threat Modelling Team

- Identifying threats and ranking them
- Reviewing NCSSRs for underlying rationale (i.e. threats)
- Use-case based approach (Offline CAs, online HSMs, Access Control, Patch Management, Account Management, Shared Accounts, etc.)
- Outdated Requirements
- Closing the Gaps

# Document Structuring Team

- Group focused on “structure” rather than “content”
- Proposing ballots in order to make big-picture improvements to the structure of the document
- Rewriting requirements to better address Offline CA systems
- Finalizing ballot to replace “zones” with separate logical access and physical security controls

# Ballots

| Ballot | Title | Status |
|---|---|---|
| SC29 | System Configuration Management | Passed |
| SC28 | Logging and Log Retention | Discussion |
| | Elimination of Zones | Drafting |
| | Offline CA Provisions | Drafting |
| | Account Management | Drafting |
| | Authentication Controls | Drafting |

# Thanks!

Mailing lists:

Main:
netsec@cabforum.org

Non-archived:
netsec-management@cabforum.org

Threat Modelling:
net-sec-threat-modeling@cabforum.org