CDX 2015 Directive Change Summary

Directive (to v1.0)

All: Changed 2014 to 2015, revised wording and grammar for clarity, and emphasized the modules
1.1: Added clarification of the overall structure of the module types and listed proposed options
2.0: (Timeline) updated timeline; added virtual infra avail.; added challenge modules event timeline
3.1: Added descriptions of the module types as executed by Blue Cells
3.2.3: Formally mentioned that White Cell will monitor Red Cell
3.4: Gray Cell will operate inside BLUENETS remotely from HQ
4.1.4: Mentioned a listing of penalties in the Scoring Spec
4.1.5: Emphasized scoring with formatting
4.2.1: Added overview of scoring breakdown
4.2.3.2: Emphasized requiring tokens on each required service and each required user workstation
4.2.5: Emphasized scoring with formatting
4.2.5.3: Added an outline of expectations regarding forbidden unrealistic insider threat mitigations
4.3.1: (VPN) Adapted to include the virtualized infrastructure option
4.3.1.5: (VPM) Emphasized that CDX-connected devices shall not connect to the Internet
4.3.2.1: (IP addrs) Added RMC Undergraduate team and CDDP team to BLUENET IP layout
5.1.2: Gray Cell requires RDP from HQ
6.0: Removed duty hours special rules from CDX 2014
8.0.1: (CNA by students) Amended definition of forbidden actions to add White Cell discretion and decrease the severity of the penalty (while still potentially completely crippling a violator's score)
Page 16: Added tentative descriptions of five proposed challenge modules

Network Specification

2.1.3: Added RMC-U and CDDP
2.1.13: (future change) Gray Cell must somehow have RDP access to the Gray Cell workstations
2.6: Will we kill or keep VOIP?
2.6.3: Virtual infrastructure schools will use soft VOIP phones?
2.7.4: Do we still require the web forum app? What web app would we change it to?
2.11.3: Gray Cell requires RDP from HQ
3.0.2: No more Windows XP
2.0.2,3: Blue Cells must advise White Cell of suspected malware to remove from HQ-provided images
3.0.8: Blue Cell cannot add software to HQ-provided images without telling White Cell
4.0.2: Gray Cell requires RDP from HQ
5.1: Adapted to include the virtual infrastructure

Scoring Specification

1.1.2: Adjusted score weighting to make room for the expanded challenge modules
1.1.2: Changed White Cell scoring to an adjustment of the total score
3.3.2: Removed duty hours special rule for C&I scoring from CDX 2014
4.1.3: Defined the new White Cell Adjustments aspect of scoring

Red Cell Rules of Engagement

2.9: Forbade Red Cell use of RDP port 3389 on Gray Cell user workstations