Last modified 16 minutes ago

CFE Event Log

date	Round	Ref	description
Wed Aug 3 02:35:45 UTC 2016	n/a	Vidas	event plan commitment hashes exported
Wed Aug 3 02:45:26 UTC 2016	n/a	Vidas	set of challenge CSIDs (shortname) given to zhivich
Wed Aug 3 17:12:32 UTC 2016	n/a	Vidas	Byrd unplugged CRS TI and IDS cables for each team; verified by Vidas
Wed Aug 3 18:38:19 UTC 2016	n/a	Vidas	Decision to not perform additional sparring in relation to recent FAQ entries. (unanimous: Walker, Eagle, Caswell, Thompson, Vidas)
Wed Aug 3 18:45:00 UTC 2016	n/a	Caswell	Cable cut by I2O deputy director
Wed Aug 3 20:37:51 EDT 2016	n/a	Caswell	Brought in the following media from competitors for re-installation procedures: TechX (1 CD), Codejitsu (1 CD), Shellphish (2 CDs), Forallsecure (1 Blueray). Delivered by Frantzen
Thu Aug 4 07:26:06 PDT 2016	n/a	Vidas	Caswell cfe reset; complete (observed by Vidas, Eagle)
Thu Aug 4 07:36:27 PDT 2016	n/a	Vidas	Andrew's air gap robot discs returned to Andrew
Thu Aug 4 07:42:24 PDT 2016	n/a	Vidas	Byrd plugged in CRS TI and IDS cables for each team; verified by Vidas
Thu Aug 4 07:42:29 PDT 2016	n/a	Vidas	Caswell cfe setup; complete (observed by Vidas)
Thu Aug 4 07:55:12 PDT 2016	n/a	Vidas	1430 (prior to airgap) yellow node 36, reported by Pat
Thu Aug 4 07:57:49 PDT 2016	n/a	Vidas	yellow node 36 verified to have been shutdown by the team via the administrative interface
Thu Aug 4 07:59:58 PDT 2016	n/a	Vidas	CFE official CS schedule export to Ben Price and Frantzen (confirmed by Caswell)
Thu Aug 4 15:04:20 UTC 2016	n/a	Vidas	MAC link check to HPC confirmed by Holt
Thu Aug 4			

15:07:45 UTC 2016	n/a	Vidas	Link negotiation confirmed by Vidas
Thu Aug 4 15:10:15 UTC 2016	n/a	Vidas	Andrew confirms that the numbered discs have been placed in the Air Gap Robot
Thu Aug 4 15:16:10 UTC 2016	n/a	Caswell	Andrew identified the backup robot failed. Tvidas attempting to fix the software failure
Thu Aug 4 15:18:27 UTC 2016	n/a	Caswell	Backup robot software failure was re-classified as a hardware failure by TVidas. Switching to Primary robot
Thu Aug 4 15:21:40 UTC 2016	n/a	Vidas	PM notified of Air Gap robot failure, decision to have Josh (referee shirt) attempt to repair the secondary robot. suspense: 1530 UTC
Thu Aug 4 15:21:40 UTC 2016	n/a	Vidas	Primary Air Gap Robot test appears successful via highside logs
Thu Aug 4 15:27:38 UTC 2016	n/a	Vidas	recentered robot echo 'N4' > /dev/ttyUSB0 at SPAWAR request
Thu Aug 4 15:23:28 UTC 2016	n/a	Vidas	followed by several requests for M4, N6, M6, N2, M2... etc
Thu Aug 4 15:33:55 UTC 2016	n/a	Vidas	Backup repair called by SPAWAR. Cable returned to Primary. Primary Air Gap Robot tested again. appears successful
Thu Aug 4 16:00:33 UTC 2016	n/a	Vidas	launch status check complete, all teams go
Thu Aug 4 16:00:45 UTC 2016	0	Vidas	CFE start
Thu Aug 4 16:05:31 UTC 2016	0	Vidas	All CRS confirmed to be interacting with TI API; all CRS IDS links confirmed to be transferring data (Caswell, Vidas)
Thu Aug 4 16:07:19 UTC 2016	1	Vidas	AGR software appeared successful (Vidas) and visually observed (Eagle)
Thu Aug 4 16:19:46 UTC 2016	1	Vidas	Observed approx 300 second delay in round 1 start. Root cause appears to be ssh setup time for forensics setup, remedied by Caswell by established persistent connection
Thu Aug 4 16:29:12 UTC 2016	4	Vidas	~~Observed (Eagle) that all teams have thrown at least one successful PoV~~
Thu Aug 4 16:37:10 UTC	5	Vidas	Observed that HPC lost LPC monitoring on purple (Pat). Deemed to not be critical enough to re-cable. Pat will visually monitor the display on the front of the HPC racks for ALL teams.

2016			
Thu Aug 4 16:41:05 UTC 2016	6	Caswell	set icinga2 monitoring of external switches to known down, as we are now within the airgap
Thu Aug 4 17:19:37 UTC 2016	13	Vidas	Pat reports that as of 1712 UTC, red-47 was administratively powered off by the CRS
Thu Aug 4 17:21:56 UTC 2016	13	Vidas	Revised observation (Eagle) that all teams had thrown at least one successful PoV by **round 5**
Thu Aug 4 17:53:52 UTC 2016	20	Vidas	Observed that CFE is 1/2 way to 40 scored rounds. Frantzen asked to notify Walker
Thu Aug 4 18:34:26 UTC 2016	27	Vidas	Pat reports that at 1825 blue gateway lost link momentarily (only a few seconds, not action required by HPC). Hypothesis: possibly a bad cable.
Thu Aug 4 19:41:09 UTC 2016	40	Vidas	40 scored rounds have completed
Thu Aug 4 13:36:43 PDT 2016	50	Vidas	exported round 43 viz export data, as requested by visualization team. Visually authenticated cadet Adam VanProoyen?, who caught the USB drive
Thu Aug 4 21:11:54 UTC 2016	56	Caswell	JWright found an execution divergence that prevents execution in public decree running within VMWare, but works in our framework. Information delivered to Visualization for story finding. CB: aad614cb087c4adca1a873190759751b0e4f10b2c3c6ee1c52c2be7b3a42ccd8.rcb
Thu Aug 4 21:31:50 UTC 2016	60	Caswell	One of the two water pumps failed. The full system must be taken down to troubleshoot, as such no action will be taken. Game continues with only one water pump.
Thu Aug 4 22:16:47 UTC 2016	67	hso	ForAllSecure? has contacted with the following concern: Our CRS should always submit PoVs. On every round, every CS, against all teams. Data at defcon.cgc.com shows that we have not. Can you confirm that is the case? If we have been submitting PoVs for a few rounds, we request a full reboot.
Thu Aug 4 22:18:52 UTC 2016	68	Caswell	Identified POVs with invalid CSIDs being uploaded by FAS. An exemplar from the logs, "2016/08/04 22:17:08 invalid csid: invalid csid field: not in map (as hex: 32383033333832323531)". This timestamp should fall in the middle of round 68. CSID decodes as 2803382251. This CB exited the schedule in round 51. We will monitor the CSIDs used for the next round to correlate with the schedule.
Thu Aug 4 22:26:24 UTC 2016	70	Caswell	Continued investigation of FAS POV issue. Identified the last 300 POV failures, extracted the FAS provided CSID. None are in the current challenge set.
Thu Aug 4 22:33:45 UTC 2016	71	Caswell	Game paused per Walker to ensure root cause of the FAS POV issue
Thu Aug 4 22:48:18 UTC 2016	71	Caswell	Validated that cfe-api configs match across all teams modulo team number and team password as expected (Confirmed cseagle). Validated that consensus files for round 52 through 55 are the same between team 1 (who is successfully uploading POVs) and FAS (who is not). This was confirmed by tvidas.
Thu Aug 4 22:54:29 UTC 2016	71	Caswell	Restarted game as per 20 minute delay requirement requested by Walker. Consensus: TVidas, HSO, Caswell, CSEagle

Thu Aug 4 23:10:20 UTC 2016	74	Vidas	informed PM. Direction is to continue investigation under the assumption that there may be an infrastructure bug and to operate at a heightened level of caution (more liberal with extending unscored portions of rounds when investigation is warranted).
Thu Aug 4 23:16:52 UTC 2016	75	Caswell	Paused game, as we identified the official request by FAS for the above POV issue states "If we have not been submitting POVs for a few rounds, we request a full reboot." TVidas went to explain the full ask to Walker to discuss. Will wait until TVidas returns to continue.
Thu Aug 4 23:19:56 UTC 2016	76	Caswell	Restarted game, per tvidas
Thu Aug 4 23:21:26 UTC 2016	76	Caswell	HPC confirms hardware for FAS is operating at 100%. Per CFE Event plan, there is no opportunity to restart the CRS to the competitors.
Thu Aug 4 23:41:49 UTC 2016	78	Caswell	API test developed by Caswell, confirmed by cseagle and tvidas before execution: * Developed a test to prove to the API config is correct. * We developed a "fake" POV upload that would be rejected by the API but show that current CSID map is loaded correctly. The webserver validates the fields in the following order: csid, team, throws, file. As such, we used an invalid team (0), an invalid throw count (100), and a valid CSID for the current round under test. * This was run against the FAS team interface, using the sparring partner credentials. * The web server responded with the following: '2016/08/04 23:31:50 127.0.0.1:55276 400 POST /pov - {"hash":"01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b","file":"bmc-fake-pov.pov","error": ["invalid team","invalid throws"]}'. This record shows that the team interface accepted the CSID, but rejected the team and throws. This test confirms that the team interface is properly mapping the current round's CSIDs, which is the error indcated by the FAS CRS below: '2016/08/04 23:37:53 192.168.1.10:44322 400 POST /pov - {"hash":"12d8733f48efea58c788fcc20af544009e107701e14c793887add1c7b3320391","file":"FAKER_00000.pov","error":invalid csid?}'. This result was validated by Caswell, TVidas, and CSEagle as to confirming the csid map loads appropriately in the team interface.
Thu Aug 4 23:51:43 UTC 2016	81	Vidas	Informed PM of continuing investigation and absence of any evidence of infrastructure error. PM decision to permit team to reboot CRS as they requested (e.g. human input into the autonomous system), iff all teams vote to permit Mayhem to reboot.
Fri Aug 5 00:10:31 UTC 2016	85	Vidas	Informed by PM that (1) result of team vote is to not permit reboot of Mayhem (2) if and when TI logs from infrastructure are made available, ForAllSecure? will be given first access, and (3) ForAllSecure? will be granted first access to already established CFE data extraction process.
Fri Aug 5 00:16:14 UTC 2016	86	Vidas	Observed that Mayhem continues to upload valid RCBs
Fri Aug 5 01:13:17 UTC 2016	95	Vidas	CFE has ended based on rounds
Fri Aug 5 01:52:29 UTC 2016	n/a	Vidas	Observed that Mayhem has successfully uploaded a PoV in round 95
Fri Aug 5 02:15:30 UTC 2016	n/a	Caswell	Disabled access to the team interfaces via "cfe --task disable_crs", interfaces confirmed down by hso, tvidas
Fri Aug 5 02:17:45 UTC 2016	n/a	Caswell	Game archive task started via "cfe --task archive"
Fri Aug 5 04:15:17 UTC 2016	n/a	Caswell	Attempt to create CFE game archive failed as it filled the GS1 disk. Started CFE archive using gxy as the destination. Using same command using a different destination to create the archive. Confirmed by cseagle, hso)
Fri Aug 5 04:24:54 UTC	n/a	Caswell	Identified the archive ETA of compression would be beyond time of the stage deconstruction. Using the same command without compression. Confirmed by cseagle, hso, wright

2016			
Fri Aug 5 06:44:16 UTC 2016	n/a	Caswell	Archive command completed, appears to be appropriate size (checked by hso, validated by Caswell). Archive finished at 08/05-05.09.26.
Fri Aug 5 07:16:03 UTC 2016	n/a	Caswell	MD5 of archive: a039ed6390ce2fea604c6c0499bcb7e3
Fri Aug 5 14:05:45 UTC 2016	n/a	Vidas	Infrastructure referees are investigating potential divergence from CFE scores and verification team, between team ranked 3rd and 4th, relating to PoVs in NRFIN_00063, CROMU_00051, KPRCA_00065, CROMU_00073, and NFRIN_00052. This is reportedly localized to rounds 55-63, 66-74, 25 27-37, 24-33, and 80-90 respectively. PoVs are reportedly 100% failure on CFE infrastructure and 100% pass on verification.
Fri Aug 5 14:21:51 UTC 2016	n/a	Vidas	Correction on rounds in question, typo on reported round and indexing adjustment by verification team: 52-62, 65-73, 24 26-36, 23-32, and 79-89
Fri Aug 5 15:34:10 UTC 2016	n/a	Vidas	Frantzen reports that NRFIN_00051 (round 73) and NRFIN_00052 (round 89) are also divergence examples
Fri Aug 5 16:15:27 UTC 2016	n/a	Vidas	Confirmed expected results (invalid PoV flag data) for multiple CS and Rounds via public vs private test (Jason), CFE round re-creation (Eagle), CFE logs (bmc), Forensics (Thompson). Frantzen reports that there is a verification team bug that tests incorrect CBs in some cases, and that ranks 1 and 2 are still confirmed by verification team. It will take the verification team 16 hours to test PoVs for ranks 3 and 4.
Fri Aug 5 17:15:00 UTC 2016	n/a	Vidas	Frantzen reports that verification team has confirmed the bug in their system in writing.
Sat Aug 6 02:05:06 UTC 2016	n/a	Vidas	Byrd observed that air gap had been broken recently (in the last 70 minutes) as there is a 2' square power distribution box just inside the airgap wall near team 6. The power source is a floorbox under the stage below team 6 CRS, power cables are then routed out between two glass airgap wall panels to AV equipment.
Sat Aug 6 02:53:28 UTC 2016	n/a	hso	After discussion with Troy Jessup (DEF CON Liason), Josh Byrd, and AV Tech (Encore), Josh called Walker and discussed the current state of the situation regarding the power distribution box. Walker told Josh that the box can stay, but all future events related to the box need to be logged and Josh needs to be present when any work is done with the box. The box is expected to be removed tomorrow morning by Encore with Josh present.
Sat Aug 6 18:18:53 UTC 2016	n/a	Vidas	Verification team has identified another bug and another, smaller PoV-based divergence. Revised eta is "this evening" (e.g. less then 12 hours). No tasks for the infrastructure team / referees.
Sun Aug 7 06:29:11 UTC 2016	n/a	Vidas	Frantzen reports that verification is done and that third and fourth place teams will be notified soon.

Signed CFE Archive File Hashes

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

cfe-final.tar hashes:

md5sum:
a039ed6390ce2fea604c6c0499bcb7e3

sha512sum:
a5d9b42e43cf92ec18879754c37861e5132b3826210af08a5b3659a98d2fe727778046739d1c86d13da17ca29b4b6640ce43f9c
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)

iQIcBAEBAgAGBQJXpmnlAAoJEM2yIO9cDptEslwQAKVPLF0b5k59pWLrhNp0oX1k
UEpLdkotTC9JFG+dKEOz+gFF6MVZEpSJj7SLP7Zeflpx8SPuKA1/nm4DU2UQGoXh
thjiEml2WmWQo82j3NCYPMxT3QbE50nvxGsRBZyTyjjyl6jKvwC7W1r4a2Lo8bmR
rTumRJezbhC5cbr9/pTcwEjk3B4tAqVOYcdA0h4DEYXl3anIre8FfMHce+aC36lh
oWDwWFXGPUFBb4nG0lYZdibQAsLBKdTyUWJcBdEgci1ouhvGN+e/zSaAZVwWC54i
```

```
Gi9hYqHOOr5NPvc1MO+c0G29z0jAtKxi91HVgUBRlCW0ITAZ8zjAdfdBgWab5BHd
buZA2x4mXpqjUBxkECawqWFfkH0Bzpn/dT/GIqv9E1EcGn0X205r8uuTqwqC1jms
LaBuOalt92ZEqOnk21fAJsKJm60fL3Ml87JYI+tk3eyuMIukQhZRTLZ/Q55O3huT
IQvhl1yIEe3Tpk+gvc5eIqJwpAZM0t3v6o1dbIhdM61z/uJBkiVK7Fa0PPobivNE
nHPI7SjPjMPYsFTSnOYNGn28r+z+0VjEFfzv/waD+beqPiutk2m1BH9DEyNn0vc0
wzXLLB6I2moiI0G0jz5elGrjO99UbrBXt9omz+h35gTwi1V1g3NZ/eaiJnu6vpr+
UKNhcxCMvqerc316+peh
=n/WQ
-----END PGP SIGNATURE-----
```