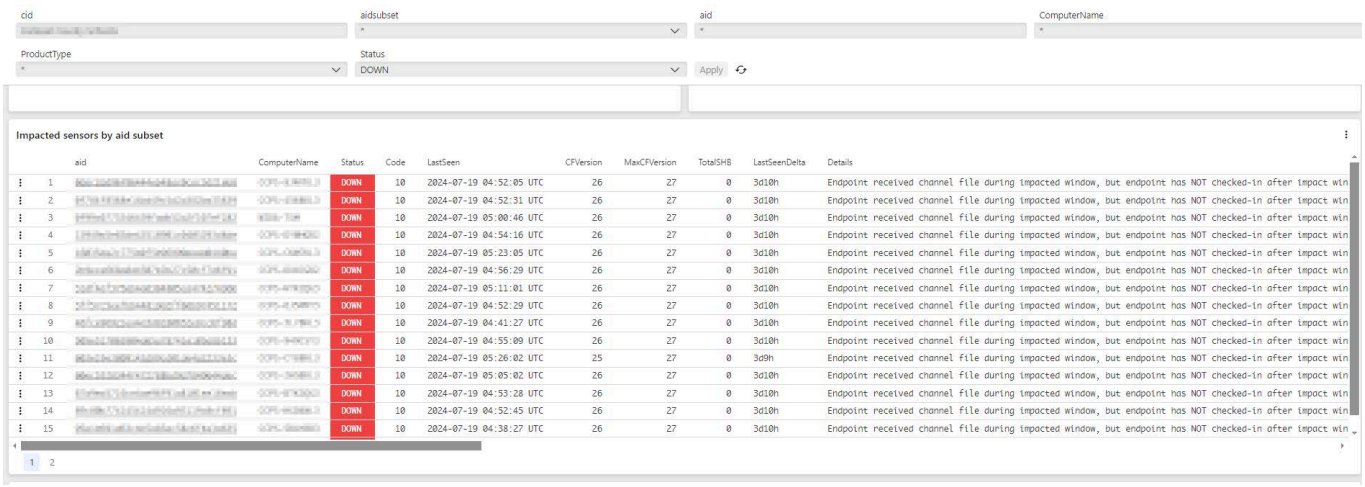
Hello -

Crowdstrike has created dashboards in the console that are designed to identify hosts still impacted by the widespread crashing issue on Windows hosts. This message briefly walks through how to access and interpret the information provided in these dashboards.

1. Access the dashboard, either via this link or by following the instructions below:
    a. Log into the Crowdstrike console, then go to Next-Gen SIEM>Dashboards (under 'Log Management').
    b. Find and click the 'hosts possibly impacted by windows crashes granular status' dashboard ('hosts possibly impacted by windows crashes' provides similar info but does not include the same level of visibility)
2. Select your CID (Organization Name) and aidsubset (choose *). You can also search for a particular status, for instance to find all hosts Crowdstrike is detecting as 'DOWN'.

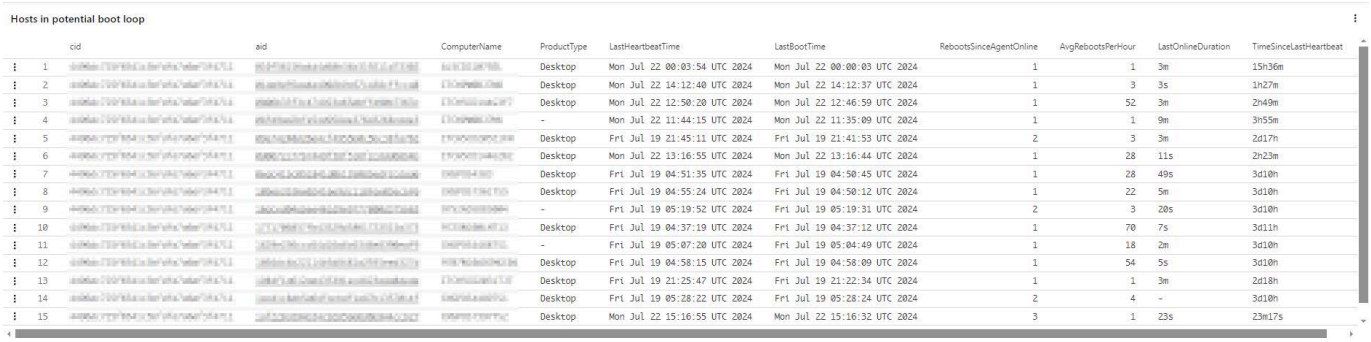
    Note: it can take a few seconds for the CID option to load, so if you see 'no suggestions available' wait for the load to complete.



	aid	ComputerName	Status	Code	LastSeen	CPVersion	MaxCPVersion	TotalSHB	LastSeenDelta	Details
1	[redacted]	[redacted]	DOWN	10	2024-07-19 04:52:05 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
2	[redacted]	[redacted]	DOWN	10	2024-07-19 04:52:31 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
3	[redacted]	[redacted]	DOWN	10	2024-07-19 05:00:46 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
4	[redacted]	[redacted]	DOWN	10	2024-07-19 04:54:16 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
5	[redacted]	[redacted]	DOWN	10	2024-07-19 05:23:05 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
6	[redacted]	[redacted]	DOWN	10	2024-07-19 04:56:29 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
7	[redacted]	[redacted]	DOWN	10	2024-07-19 05:11:01 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
8	[redacted]	[redacted]	DOWN	10	2024-07-19 04:52:29 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
9	[redacted]	[redacted]	DOWN	10	2024-07-19 04:41:27 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
10	[redacted]	[redacted]	DOWN	10	2024-07-19 04:55:09 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
11	[redacted]	[redacted]	DOWN	10	2024-07-19 05:26:02 UTC	25	27	0	3d9h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
12	[redacted]	[redacted]	DOWN	10	2024-07-19 05:05:02 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
13	[redacted]	[redacted]	DOWN	10	2024-07-19 04:53:28 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
14	[redacted]	[redacted]	DOWN	10	2024-07-19 04:52:45 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win
15	[redacted]	[redacted]	DOWN	10	2024-07-19 04:38:27 UTC	26	27	0	3d10h	Endpoint received channel file during impacted window, but endpoint has NOT checked-in after impact win

1 2

3. The dashboard will generate a report of 'Impacted sensors by aid subset', showing assets that meet the criteria you defined above. They also provide a report on 'Hosts in potential boot loop' which shows hosts that may not be able to start up successfully, which may be related to these assets being impacted by this issue.



	cid	aid	ComputerName	ProductType	LastHeartbeatTime	LastBootTime	RebootsSinceAgentOnline	AvgRebootsPerHour	LastOnlineDuration	TimeSinceLastHeartbeat
1	[redacted]	[redacted]	[redacted]	Desktop	Mon Jul 22 00:03:54 UTC 2024	Mon Jul 22 00:00:03 UTC 2024	1	1	3m	15h36m
2	[redacted]	[redacted]	[redacted]	Desktop	Mon Jul 22 14:12:40 UTC 2024	Mon Jul 22 14:12:37 UTC 2024	1	3	3s	1h27m
3	[redacted]	[redacted]	[redacted]	Desktop	Mon Jul 22 12:50:20 UTC 2024	Mon Jul 22 12:46:59 UTC 2024	1	52	3m	2h49m
4	[redacted]	[redacted]	[redacted]	-	Mon Jul 22 11:44:15 UTC 2024	Mon Jul 22 11:35:09 UTC 2024	1	1	9m	3h55m
5	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 21:45:11 UTC 2024	Fri Jul 19 21:41:53 UTC 2024	2	3	3m	2d17h
6	[redacted]	[redacted]	[redacted]	Desktop	Mon Jul 22 13:16:55 UTC 2024	Mon Jul 22 13:16:44 UTC 2024	1	28	11s	2h23m
7	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 04:51:35 UTC 2024	Fri Jul 19 04:50:45 UTC 2024	1	28	49s	3d10h
8	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 04:55:24 UTC 2024	Fri Jul 19 04:50:12 UTC 2024	1	22	5m	3d10h
9	[redacted]	[redacted]	[redacted]	-	Fri Jul 19 05:19:52 UTC 2024	Fri Jul 19 05:19:31 UTC 2024	2	3	20s	3d10h
10	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 04:37:19 UTC 2024	Fri Jul 19 04:37:12 UTC 2024	1	70	7s	3d11h
11	[redacted]	[redacted]	[redacted]	-	Fri Jul 19 05:07:20 UTC 2024	Fri Jul 19 05:04:49 UTC 2024	1	18	2m	3d10h
12	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 04:58:15 UTC 2024	Fri Jul 19 04:58:09 UTC 2024	1	54	5s	3d10h
13	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 21:25:47 UTC 2024	Fri Jul 19 21:22:34 UTC 2024	1	1	3m	2d18h
14	[redacted]	[redacted]	[redacted]	Desktop	Fri Jul 19 05:28:22 UTC 2024	Fri Jul 19 05:28:24 UTC 2024	2	4	-	3d10h
15	[redacted]	[redacted]	[redacted]	Desktop	Mon Jul 22 15:16:55 UTC 2024	Mon Jul 22 15:16:32 UTC 2024	3	1	23s	23m17s

Status Information
'DOWN' is a high confidence assessment that an asset is still impacted, 'OK' is a high confidence assessment that the machine was not impacted or has been remediated, and the other statuses are low or medium confidence assessments based on the available data. Here is a full breakdown of the available status definitions:

- **DOWN**: a high confidence assessment where remediation is likely to be required
    - Endpoint has channel file version of 0 and has not checked-in after impact window.
    - Endpoint received the channel file during impact window, but endpoint has NOT checked-in after impact window.

- **VERIFY**: a low to medium confidence assessment
    - Endpoint received the channel file during impact window and has checked-in after impact window.

- **RECOVERY_LIKELY:** a medium confidence assessment
    - Endpoint received channel file during impact window and has checked-in after impact window with a total reported uptime of 5-10 hours.

- **RECOVERY_VERY_LIKELY:** a medium to high confidence assessment
    - Endpoint received channel file during impact window and has checked-in after impact window a total reported uptime of 10-20 hours.

- **UNKNOWN:** there is not enough available data to form an assessment
    - Cannot determine endpoint status based on available telemetry.

- **OK:** a high confidence assessment
    - Endpoint running version of Falcon sensor that is not impacted.
    - Endpoint has the latest channel file and is operational.
    - Endpoint was offline and did not receive the channel file during impact window.
    - Endpoint was online and did not receive the channel file during impact window.

For additional information, please reference this support article released by Crowdstrike (no login required).