```
// Get ConfigStateUpdate and SensorHeartbeat events
#event_simpleName=/^(ConfigStateUpdate|SensorHeartbeat)$/
event_platform=Win
// Narrow search to Channel File 291 and extract version number; accept all
SensorHeartbeat events within impact window
| case{
    #event_simpleName=ConfigStateUpdate |
regex("\|1,123,(?<CFVersion>.*?)\|", field=ConfigStateData, strict=false) |
parseInt(CFVersion, radix=16);
    #event_simpleName=SensorHeartbeat | rename([[@timestamp, LastSeen]]);
}



| case{
    #event_simpleName=ConfigStateUpdate | @timestamp>1721362140000 AND
@timestamp < 1721366820000 | CSUcounter:=1;
    #event_simpleName=SensorHeartbeat | LastSeen>1721362140000 AND
LastSeen<1721366820000 | SHBcounter:=1;
    *;
}
| default(value="0", field=[CSUcounter, SHBcounter])
// Make sure both ConfigState update and SensorHeartbeat have happened
| selfJoinFilter(field=[cid, aid, ComputerName],
where=[{ConfigStateUpdate}, {SensorHeartbeat}])
// Aggregate results
| groupBy([cid, aid], function=([{selectFromMax(field="@timestamp",
include=[CFVersion])}, {selectFromMax(field="@timestamp",
include=[@timestamp]) | rename(field="@timestamp", as="LastSeen")},
max(CSUcounter, as=CSUcounter), max(SHBcounter, as=SHBcounter)]),
limit=max)
// Perform check on selfJoinFilter
| CFVersion=* LastSeen=*
// Calculate time between last seen and now
| LastSeenDelta:=now()-LastSeen
// Optional threshold; 3600000 is one hour
| LastSeenDelta>3600000
// Calculate duration between last seen and now
| LastSeenDelta:=formatDuration("LastSeenDelta", precision=2)
// Convert LastSeen time to human-readable format
| LastSeen:=formatTime(format="%F %T", field="LastSeen")
// Enrich aggregation with aid_master details
| aid=~match(file="aid_master_main.csv", column=[aid])
| aid=~match(file="aid_master_details.csv", column=[aid],
include=[FalconGroupingTags, SensorGroupingTags])
// Convert FirstSeen time to human-readable format
| FirstSeen:=formatTime(format="%F %T", field="FirstSeen")



// Move ProductType to human-readable format and add formatting
| $falcon/helper:enrich(field=ProductType)
| drop([Time])
| default(value="-", field=[MachineDomain, OU, SiteName,
FalconGroupingTags, SensorGroupingTags], replaceEmpty=true)
| case{
    CSUcounter=0 AND SHBcounter=0 | Details:="OK: Endpoint did not receive
channel file during impacted window. Endpoint was offline.";
```

```
    CSUcounter=0 AND SHBcounter=1 | Details:="OK: Endpoint did not receive
channel file during impacted window. Endpoint was online.";
    CSUcounter=1 AND SHBcounter=1 | Details:="CHECK: Endpoint received
channel file during impacted window. Endpoint was online. Endpoint has not
been seen online in past hour.";
```