# Cylera Dashboard App Installation and User Guide For IBM QRadar Platform

This document describes how to install the Cylera Dashboard app on the QRadar platform and how to use it. The Cylera app (also referred to as an extension) on the QRadar platform enables the following capabilities:

- Install the Cylera Dashboard QRadar App to QRadar platform.
- Ingest all the syslogs from Cylera's server as events in QRadar.
- The events are used as data to generate the dashboard.
- The dashboard enables users to view the devices, vulnerabilities and threats from different perspectives.

---

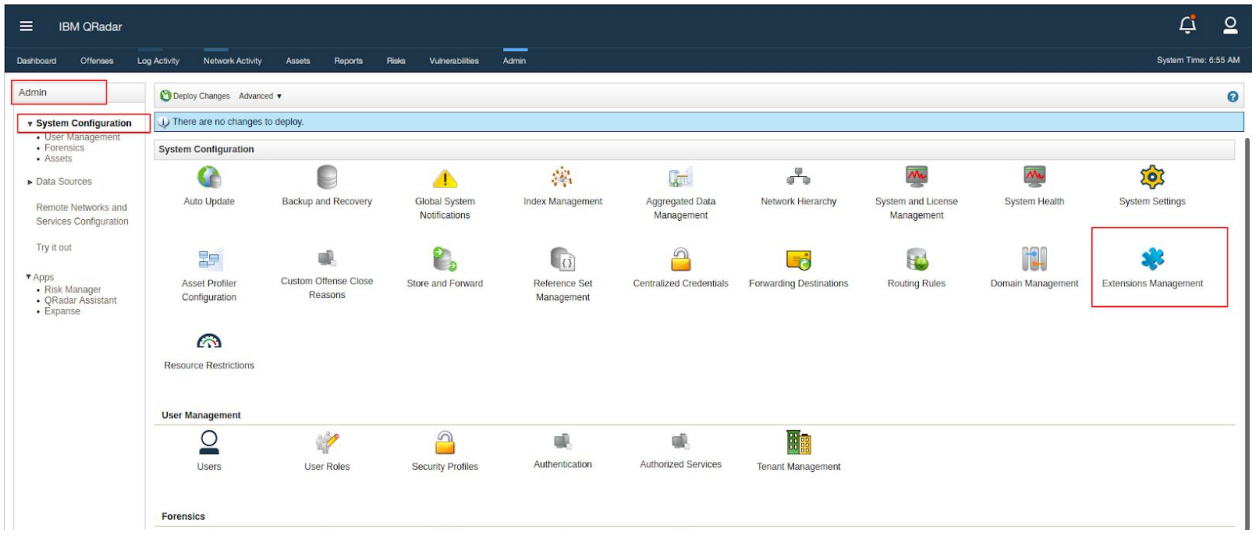
# Installing The Extension

Before beginning the installation, ensure that you meet the following prerequisites:

- Your QRadar platform is running one of the following versions or later:
    - IBM Security QRadar 7.3.2: Patch 7 (7.3.2.20190410024210)
- You have already downloaded the Cylera Dashboard App for QRadar file (cylera-dashboard.zip) from the IBM Security App Exchange.
- You can log in to QRadar with Master Administrator privileges.

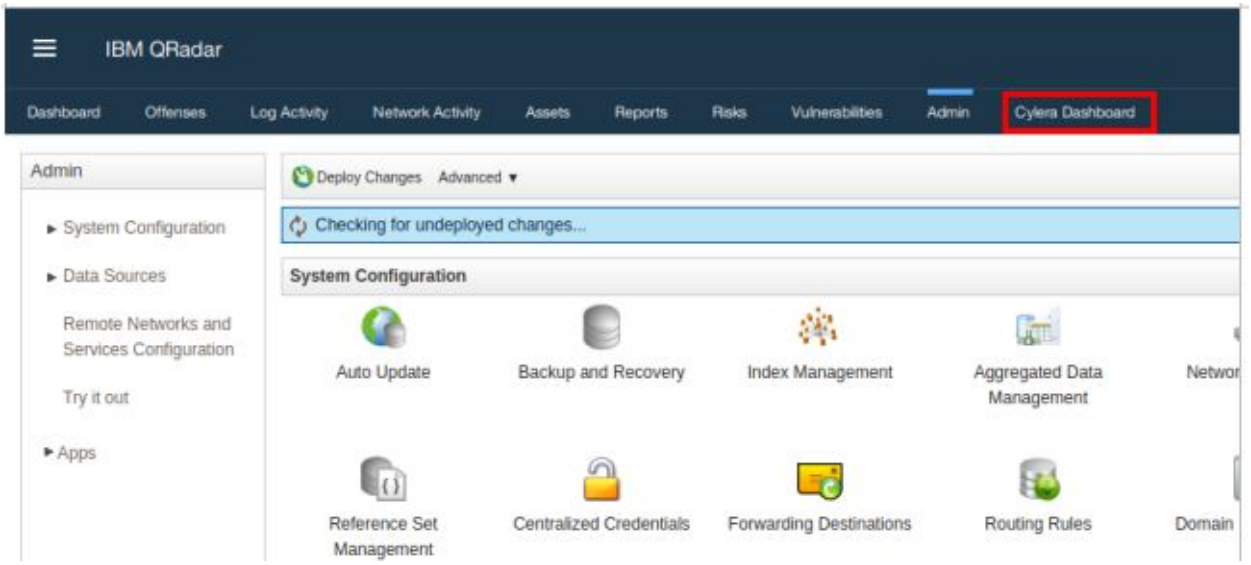
To install the Cylera Dashboard app on QRadar, perform the following steps:

1. Log in to the QRadar console with Master Administrator privileges and then click Admin in the navigation menu .
2. In the System Configuration section, click Extensions Management.




3. To upload the Cylera Dashboard app extension, click **Add > Browse**, browse to the downloaded file, , and then click **Add**.

4. To view the contents of the extension, select it from the extensions list and then click **More Details**.
5. To install the extension, select it from the list and then click **Install**.
6. Review the changes that the installation makes to the system and then select **Overwrite** or **Keep existing data** to specify how to handle existing content.
7. Review the installation summary and then click **OK**.
8. After the Installation is complete, navigate to the Toolbar section, click **Cylera Dashboard.**




This opens the Main Dashboard.

## Adding a Log Source

QRadar should be configured to have each Cylera appliance as a log source. The Cylera appliances use Syslog to send messages to QRadar.

**To add Cylera as a Log Source within QRadar:**

1. Login to the QRadar Console as Admin
2. Click on the Admin tab
3. Click "**Log Sources**" icon in the "**System Configuration**" area
4. Click "**Add**"
5. A form will then open. Complete the fields as follows:
    a. **Log Source Name:** Enter a unique log source name
    b. **Log Source Type:** Select Cylera
    c. **Protocol Configuration:** Select Syslog

    d. **Log Source Identifier:** Enter the IP Address of the Cylera appliance
    e. Uncheck the **Coalescing Events** checkbox
    f. Ensure the **Store Event Payload** checkbox is checked
    g. **Log Source Extension:** Choose the extension beginning with “CyleraCustom”
6. Click Save

After this, the log source has been successfully created. The final required step is to increase the maximum TCP payload size for Syslog messages:

1. Click on the Admin tab
2. Click “**System Settings**”
3. Click the “**Advanced**” button in the bottom-left of the popup window to switch to Advanced mode
4. Find the “**Max TCP Syslog Payload Length**” setting and set the value to **16384**
5. Click Save
6. Click the “**Deploy Changes**” button within the Admin tab and allow QRadar to restart

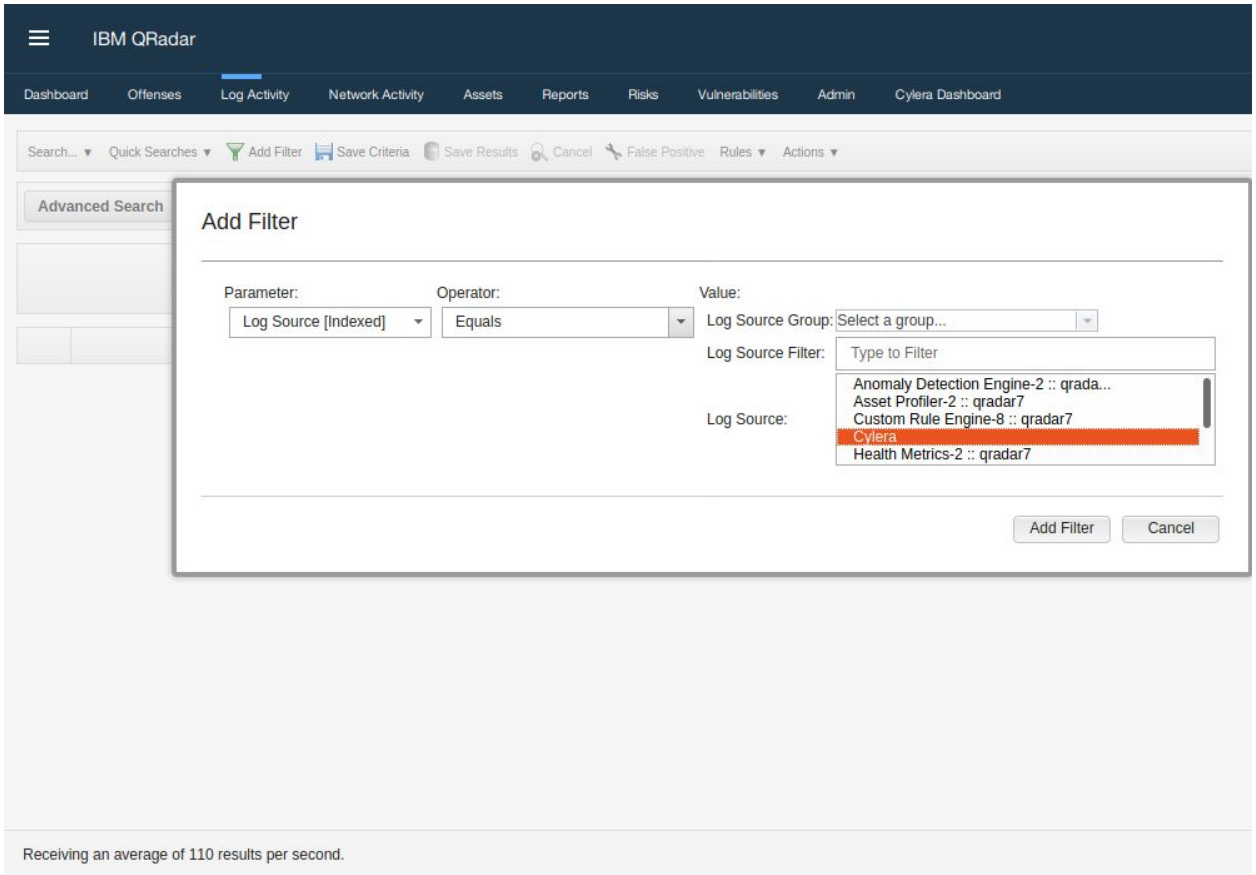
## Using the Extension

The integration enables the following functionality within the QRadar console:

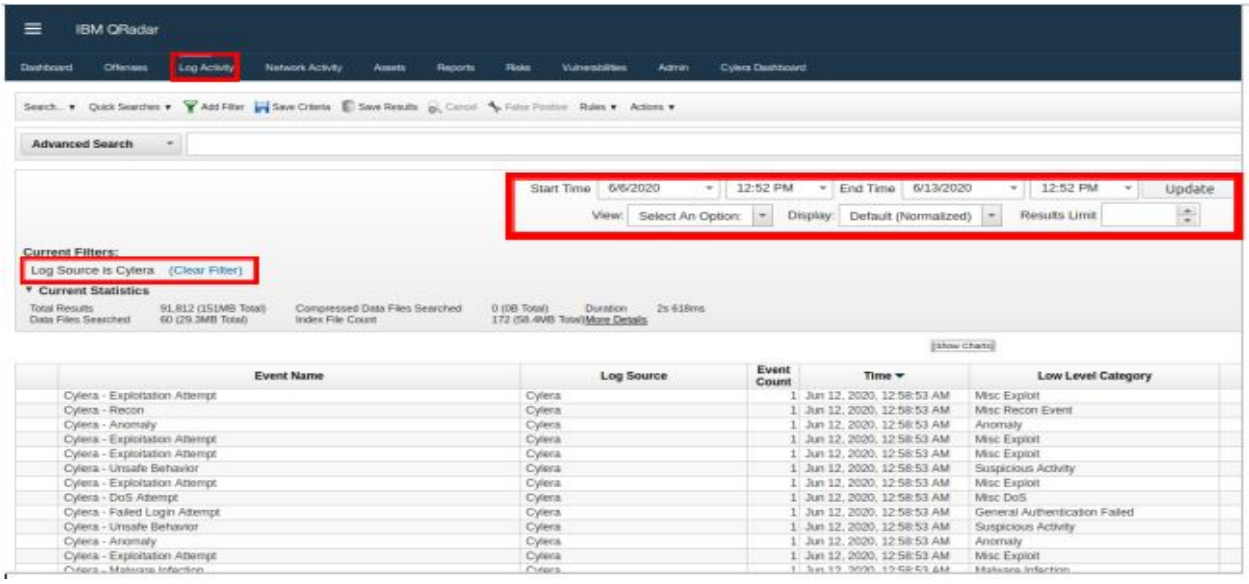
- View events in the QRadar *Log Activity* section as a part of the dashboard.
- Summary views for risks, alerts and inventory.
- Individual detailed views for asset, vulnerability and threat.

## Log Activity Events

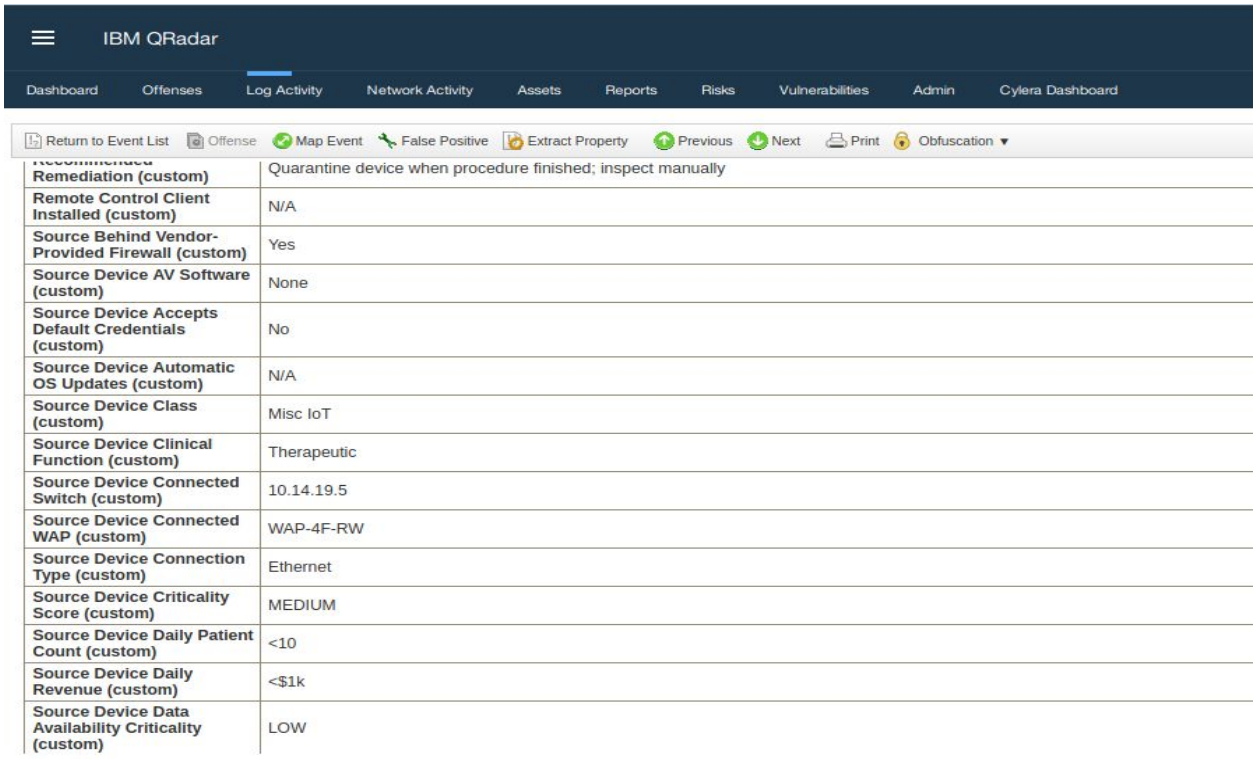
After the QRadar and Cylera Dashboard integration is complete, the Cylera Dashboard app will start ingesting events from the Cylera server and displaying them as QRadar events. Navigate to the **Log Activity** tab and filter the log source to show entries from “Cylera”.
**To apply a filter – Click Add Filter, select Log Source [Indexed] and select Cylera.**




Once the filter is added, Cylera events will be visible after providing the time range in the **View real time events.** Click **View** to choose various time ranges, else by default that will be set to 'Real Time Events'.



Double-click on the logged event to see all the fields related to the event




| | |
|---|---|
| Remediation (custom) | Quarantine device when procedure finished; inspect manually |
| Remote Control Client Installed (custom) | N/A |
| Source Behind Vendor-Provided Firewall (custom) | Yes |
| Source Device AV Software (custom) | None |
| Source Device Accepts Default Credentials (custom) | No |
| Source Device Automatic OS Updates (custom) | N/A |
| Source Device Class (custom) | Misc IoT |
| Source Device Clinical Function (custom) | Therapeutic |
| Source Device Connected Switch (custom) | 10.14.19.5 |
| Source Device Connected WAP (custom) | WAP-4F-RW |
| Source Device Connection Type (custom) | Ethernet |
| Source Device Criticality Score (custom) | MEDIUM |
| Source Device Daily Patient Count (custom) | <10 |
| Source Device Daily Revenue (custom) | <$1k |
| Source Device Data Availability Criticality (custom) | LOW |

# Events

Events has following custom fields, some of which can be seen in the final screenshot shown in the previous section. The full list of custom fields are:

1. Behind Vendor-Provided Firewall
2. CVSS
3. Current Device State
4. Device AV Software
5. Device Accepts Default Credentials
6. Device Automatic OS Updates
7. Device Class
8. Device Clinical Function
9. Device Connected Switch
10. Device Connected WAP
11. Device Connection Type
12. Device Criticality Score
13. Device Daily Patient Count
14. Device Daily Revenue

15. Device Data Availability Criticality
16. Device Data Confidentiality Criticality
17. Device Data Integrity Criticality
18. Device Dependencies
19. Device Dependents
20. Device FDA Class
21. Device First Seen
22. Device Functional Availability Criticality
23. Device Functional Integrity Criticality
24. Device ID
25. Device Intra-Site Location
26. Device Model
27. Device Next Scheduled Usage Time
28. Device Open Ports
29. Device Owner
30. Device Risk Score
31. Device Runs EOL OS
32. Device Serial
33. Device Site
34. Device Spare Availability
35. Device Type
36. Device Typical Active Days
37. Device Typical Active Hours
38. Device Vendor
39. Device Version
40. Dual-Homed
41. Exposed to Internet
42. Management Client Installed
43. Message
44. On Guest Network
45. Operating System
46. Outdated Firmware
47. Recommended Remediation
48. Remote Control Client Installed
49. Source Behind Vendor-Provided Firewall
50. Source Device AV Software
51. Source Device Accepts Default Credentials
52. Source Device Automatic OS Updates
53. Source Device Class
54. Source Device Clinical Function
55. Source Device Connected Switch

56. Source Device Connected WAP
57. Source Device Connection Type
58. Source Device Criticality Score
59. Source Device Daily Patient Count
60. Source Device Daily Revenue
61. Source Device Data Availability Criticality
62. Source Device Data Confidentiality Criticality
63. Source Device Data Integrity Criticality
64. Source Device Dependencies
65. Source Device Dependents
66. Source Device FDA Class
67. Source Device First Seen
68. Source Device Functional Availability Criticality
69. Source Device Functional Integrity Criticality
70. Source Device ID
71. Source Device Intra-Site Location
72. Source Device Model
73. Source Device Next Scheduled Usage Time
74. Source Device Open Ports
75. Source Device Owner
76. Source Device Risk Score
77. Source Device Runs EOL OS
78. Source Device Serial
79. Source Device Site
80. Source Device Spare Availability
81. Source Device Type
82. Source Device Typical Active Days
83. Source Device Typical Active Hours
84. Source Device Vendor
85. Source Device Version
86. Source Dual-Homed
87. Source Exposed to Internet
88. Source Management Client Installed
89. Source On Guest Network
90. Source Operating System
91. Source Outdated Firmware
92. Source Remote Control Client Installed
93. Source State
94. Source Uses Internet
95. Source VLAN
96. Source VLAN Type

97. Source Vulnerability Count
98. Source Workstation-Like
99. Title
100. Urgency
101. Uses Internet
102. VLAN
103. VLAN Type
104. Vulnerability Count
105. Workstation-Like
106. Destination Device AV Software
107. Destination Device AV Version
108. Destination Device Active Days
109. Destination Device Active Hours
110. Destination Device Auto OS Updates
111. Destination Device Browsing Behavior
112. Destination Device Class
113. Destination Device Clinical Function
114. Destination Device Connected Switch
115. Destination Device Connected Wap
116. Destination Device Connection Type
117. Destination Device Creates ePHI
118. Destination Device Current State
119. Destination Device Daily Patient Count
120. Destination Device Daily Revenue
121. Destination Device Data Availability Impact
122. Destination Device Data Confidentiality Impact
123. Destination Device Data Integrity Impact
124. Destination Device Default Creds
125. Destination Device Dependencies
126. Destination Device Dependents
127. Destination Device Dual Homed
128. Destination Device Eol Operating System
129. Destination Device FDA Class
130. Destination Device First Seen
131. Destination Device Functional Availability Impact
132. Destination Device Functional Integrity Impact
133. Destination Device Guest Network
134. Destination Device Hostname
135. Destination Device Hours Past 7d
136. Destination Device ID
137. Destination Device IP

138. Destination Device Impact Score
139. Destination Device Impact Score Number
140. Destination Device International Traffic
141. Destination Device Known Open Ports
142. Destination Device Location Category
143. Destination Device Location Name
144. Destination Device Location Source
145. Destination Device MAC
146. Destination Device Management Client
147. Destination Device Model
148. Destination Device Next Scheduled Time
149. Destination Device Operating System
150. Destination Device Outdated Firmware
151. Destination Device Owner
152. Destination Device Physically Segmented
153. Destination Device Receives ePHI
154. Destination Device Remote Control Client
155. Destination Device Risk Score
156. Destination Device Risk Score Number
157. Destination Device Segmentation Type
158. Destination Device Serial
159. Destination Device Site Name
160. Destination Device Spare Availability
161. Destination Device Stores ePHI
162. Destination Device Transmits ePHI
163. Destination Device Type
164. Destination Device Uses Internet
165. Destination Device Vendor
166. Destination Device Vendor Firewall
167. Destination Device Version
168. Destination Device Vlan
169. Destination Device Vlan Type
170. Destination Device Vuln Count
171. Destination Device Workstation Like
172. Destination Port
173. Device AV Software
174. Device AV Version
175. Device Active Days
176. Device Active Hours
177. Device Auto OS Updates
178. Device Browsing Behavior

179. Device Class
180. Device Clinical Function
181. Device Connected Switch
182. Device Connected Wap
183. Device Connection Type
184. Device Creates ePHI
185. Device Current State
186. Device Daily Patient Count
187. Device Daily Revenue
188. Device Data Availability Impact
189. Device Data Confidentiality Impact
190. Device Data Integrity Impact
191. Device Default Creds
192. Device Dependencies
193. Device Dependents
194. Device Dual Homed
195. Device Eol Operating System
196. Device FDA Class
197. Device First Seen
198. Device Functional Availability Impact
199. Device Functional Integrity Impact
200. Device Guest Network
201. Device Hostname
202. Device Hours Past 7d
203. Device ID
204. Device IP
205. Device Impact Score
206. Device Impact Score Number
207. Device International Traffic
208. Device Known Open Ports
209. Device Location Category
210. Device Location Name
211. Device Location Source
212. Device MAC
213. Device Management Client
214. Device Model
215. Device Next Scheduled Time
216. Device Operating System
217. Device Outdated Firmware
218. Device Owner
219. Device Physically Segmented

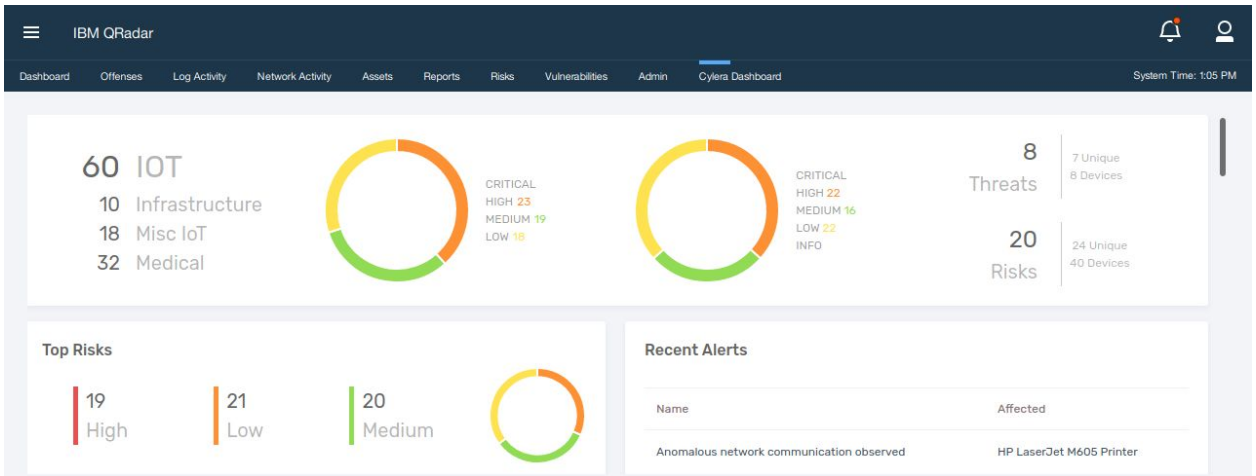
220. Device Receives ePHI
221. Device Remote Control Client
222. Device Risk Score
223. Device Risk Score Number
224. Device Segmentation Type
225. Device Serial
226. Device Site Name
227. Device Spare Availability
228. Device Stores ePHI
229. Device Transmits ePHI
230. Device Type
231. Device Uses Internet
232. Device Vendor
233. Device Vendor Firewall
234. Device Version
235. Device Vlan
236. Device Vlan Type
237. Device Vuln Count
238. Device Workstation Like
239. Message
240. Network Timestamp
241. Protocol
242. Source Device AV Software
243. Source Device AV Version
244. Source Device Active Days
245. Source Device Active Hours
246. Source Device Auto OS Updates
247. Source Device Browsing Behavior
248. Source Device Class
249. Source Device Clinical Function
250. Source Device Connected Switch
251. Source Device Connected Wap
252. Source Device Connection Type
253. Source Device Creates ePHI
254. Source Device Current State
255. Source Device Daily Patient Count
256. Source Device Daily Revenue
257. Source Device Data Availability Impact
258. Source Device Data Confidentiality Impact
259. Source Device Data Integrity Impact
260. Source Device Default Creds

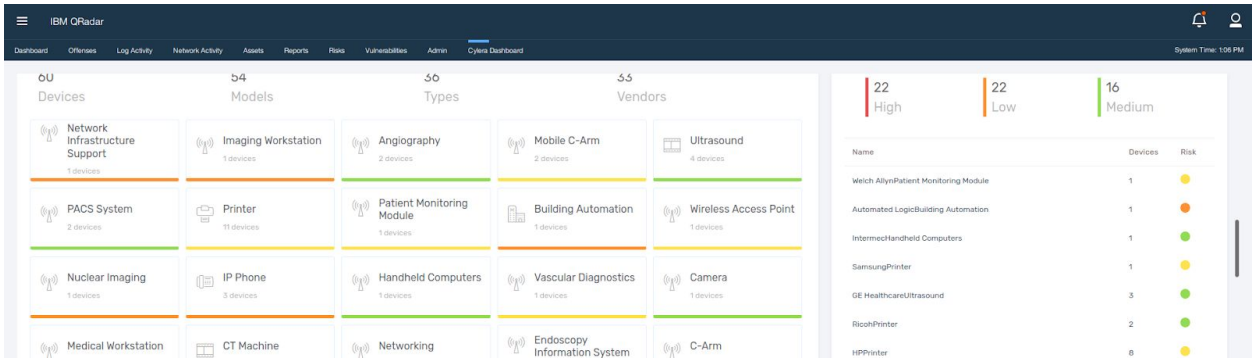
261. Source Device Dependencies
262. Source Device Dependents
263. Source Device Dual Homed
264. Source Device Eol Operating System
265. Source Device FDA Class
266. Source Device First Seen
267. Source Device Functional Availability Impact
268. Source Device Functional Integrity Impact
269. Source Device Guest Network
270. Source Device Hostname
271. Source Device Hours Past 7d
272. Source Device ID
273. Source Device IP
274. Source Device Impact Score
275. Source Device Impact Score Number
276. Source Device International Traffic
277. Source Device Known Open Ports
278. Source Device Location Category
279. Source Device Location Name
280. Source Device Location Source
281. Source Device MAC
282. Source Device Management Client
283. Source Device Model
284. Source Device Next Scheduled Time
285. Source Device Operating System
286. Source Device Outdated Firmware
287. Source Device Owner
288. Source Device Physically Segmented
289. Source Device Receives ePHI
290. Source Device Remote Control Client
291. Source Device Risk Score
292. Source Device Risk Score Number
293. Source Device Segmentation Type
294. Source Device Serial
295. Source Device Site Name
296. Source Device Spare Availability
297. Source Device Stores ePHI
298. Source Device Transmits ePHI
299. Source Device Type
300. Source Device Uses Internet
301. Source Device Vendor

302. Source Device Vendor Firewall
303. Source Device Version
304. Source Device Vlan
305. Source Device Vlan Type
306. Source Device Vuln Count
307. Source Device Workstation Like
308. Source Port
309. Threat Context
310. Threat Description
311. Threat Name
312. Threat Remediation
313. Threat Risk Score
314. Threat Risk Score Number
315. Threat Type
316. Vuln Cvss Score
317. Vuln Cvss Vector
318. Vuln Description
319. Vuln ID
320. Vuln Name
321. Vuln Remediation
322. Vuln Risk Score
323. Vuln Risk Score Number
324. Vuln Status

# The Main Dashboard

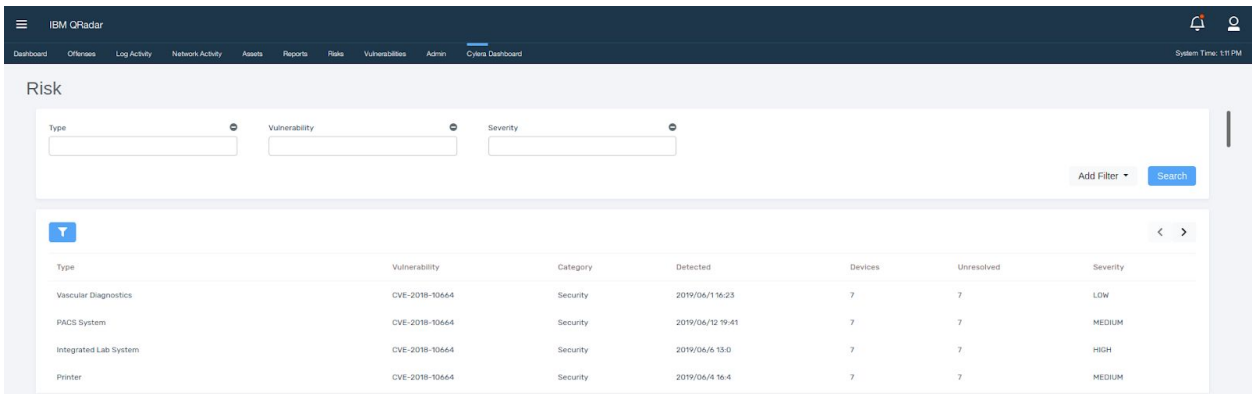
The Main Dashboard consists of Summary, Top Risks, Recent Alerts, Inventory and Riskiest Devices sections.



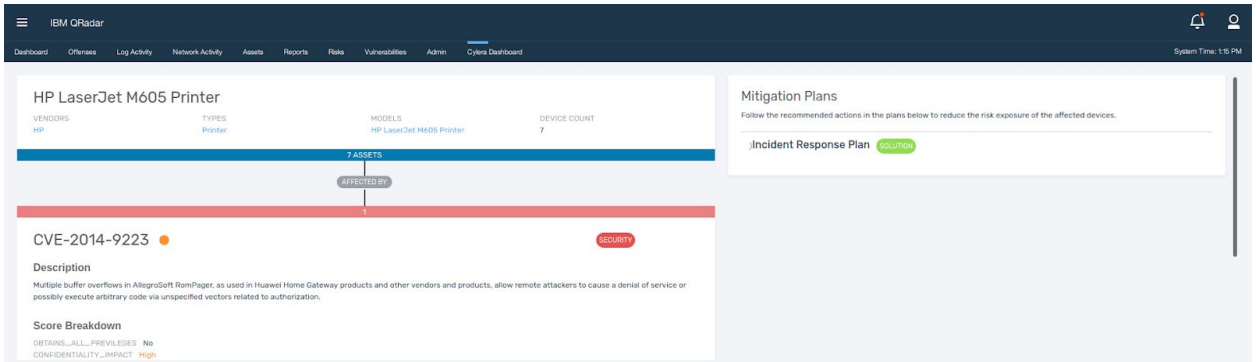



# Risks List and Vulnerability Details

In the Top Risks section 8 vulnerabilities are visible at a time but if the user wishes to see all the risks then he can simply click on ‘view all’. Also the same behaviour can be seen from the top right section of the Summary which shows the number of risks and upon clicking it takes the user to the risks list.

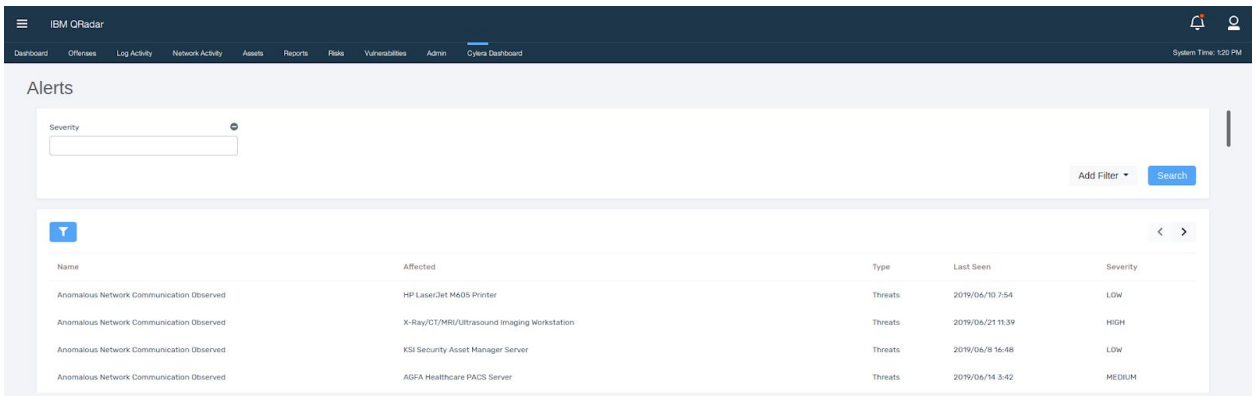



Each row depicts the individual risk so if one of the rows is clicked then the user can see the Vulnerability Detailed View. Below is the example for the same.

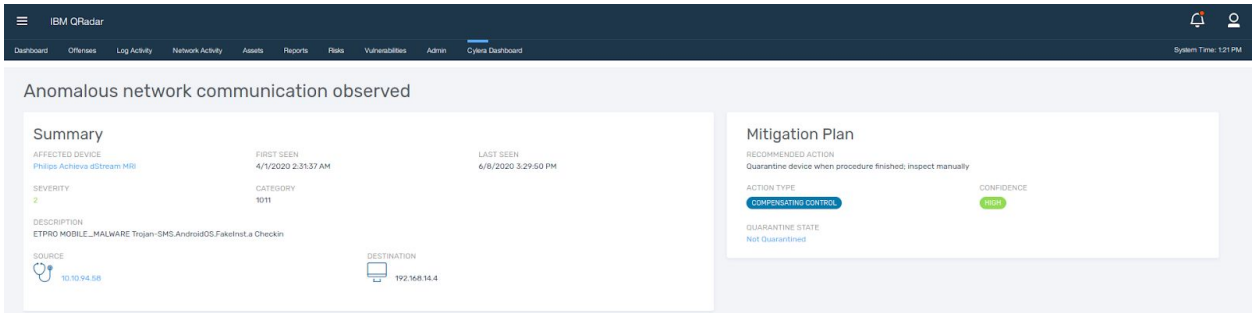


# Alerts List and Threats Details

The Recent Alerts section has 10 threats visible at a time but if the user wishes to see all the threats then he can simply click on ‘view all’.

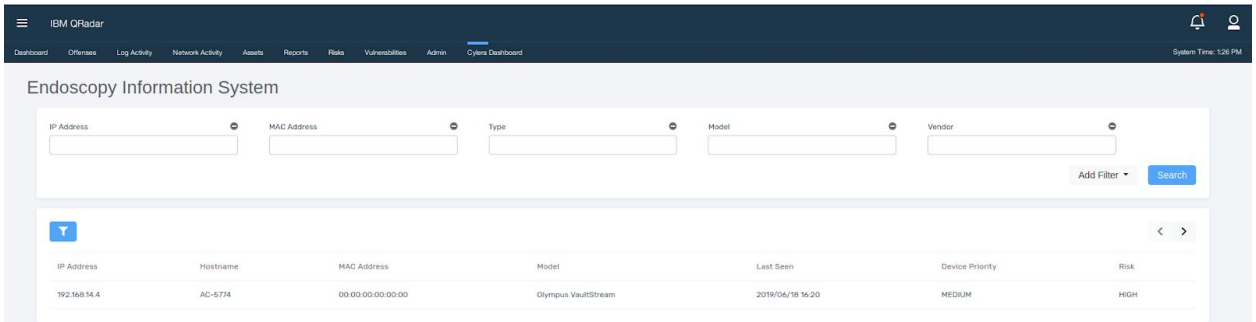



Each row depicts the individual threat so if one of the rows is clicked then the user can see the Threat Detailed View. Below is the example for the same.

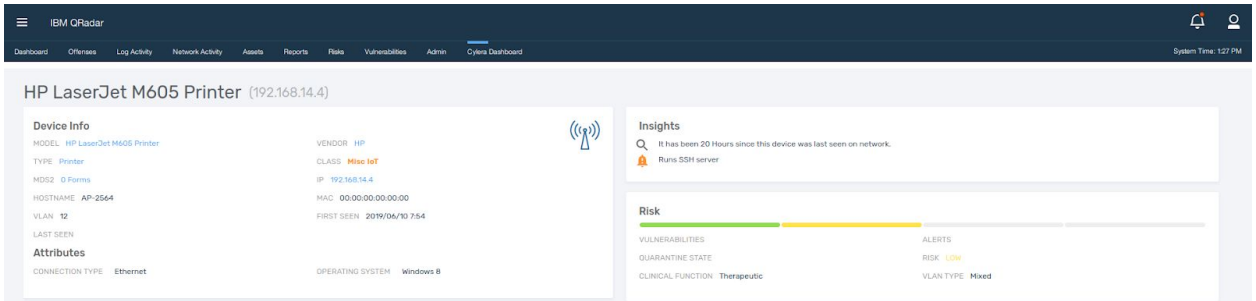



# Inventory Summary List and Individual Asset View

The Inventory section shows Device Count based on the Device Types  along with the risks associated with those devices, the user can see the Inventory Summary List if he clicks on one of the devices.



The same behaviour as Risks and alerts follows here as well, if the user wishes to see the Individual Asset then he can see it by clicking one of the rows and the following view can be seen.




Note that all these table views allow users to view, add or remove filters upon their wish.