**需求1**

1 高级别数据指的是什么？在哪个接口有体现？

Answer:

1.A graph for summarizing alerts via priority. 通过优先级汇总alerts的图表, 目前可以通过多次调用 `/alerts/fetch-alerts-priority` 来完成, 但现在他们写了一个更好的router，就不需要多次调用了。

2. 基于组的所有设备throughput的图表 – 给你新写的router。

3. 基于throughput的前10个设备的图表 – 给你新写的router。

4. verdicts – 已有，在quickwins。

**Router:**

FetchAlertPriorityCounts

{

1: 24,

3: 15,

5: 17,

9: 43

}

TopTenLocksThroughput

// dictionary 的value是那个lock的所有设备的throughput. 用table来表示。

{

"LockOne": 1323123,

"LockTwo": 12341234,

"LockThree": 44444

}

//最多再增加七个锁，总计十个。router返回前十个，不需要你进行计算哪些构成前十名。如果总共少于十个，例如，如果只存在四个锁，那么JSON中将只返回四个项目。

//这个route 返回MAC 地址 (设备) 还有他们throughput的总和. 用柱形图表示

TopTalkers

{

"MACAddress": 141414,

"MACAddressTwo": 55555

//At MAXIMUM, EIGHT more devices, totalling to 10. Same as above where if there are less than 10 devices, you will receive a dictionary containing two items

}

2 事件数量的接口在已提供的接口文档没找到

FetchDashBreakdown

[

{

"type": "Whitelisted SSH,

"count": 150

},

{

"type": "External SSH",

"count": 100

},

{

"type": "Blacklisted SSH",

"count": 75

}

]

FetchDashHistory

[

{

"day": "2024-01-01",

"count": 12

},

{

"day": "2024-01-02",

"count": 15

},

{

"day": "2024-01-03",

"count": 8

},

{

"day": "2024-01-04",

"count": 20

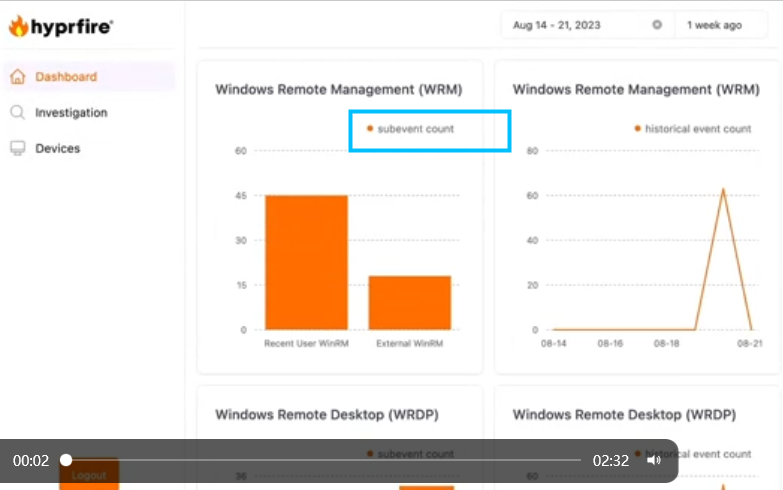
}

]

3 “最活跃通讯者”“最活跃通讯网络”的概念？ 以及对应的接口

**录屏：**

1. window remote management(WRM)以及WRDP INF SSH PSC中 subevent count指的什么含义 新版dashboard页面还需要这些图表？



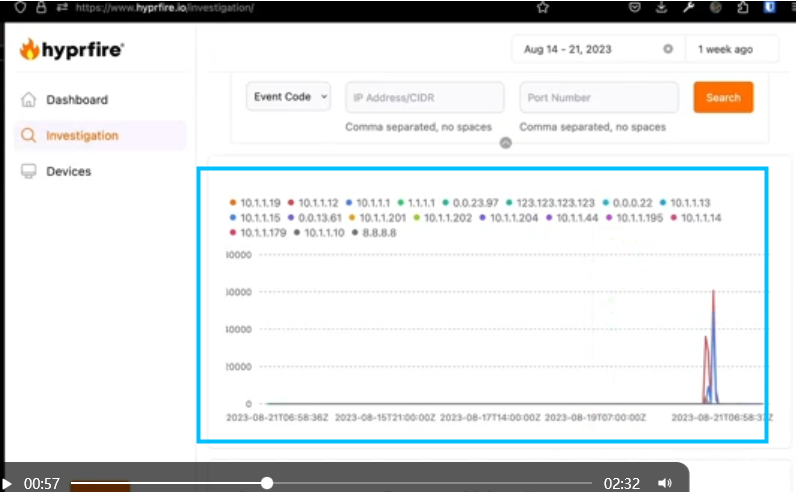
WRM代表Windows远程管理的类别。subevent count构成了整个类别。

例如，对于WRM，subevent count是 WRM001, WRM002, WRM003, WRM004, WRM005。

对于WinRDP，subevent count是 WRDP001, WRDP002, WRDP003, WRDP004, WRDP005。

（如果还不清晰我就去要subevent count 类型列表）

1. investigation中的包含ip地址和时间的折线图表呈现的含义，event code下拉的数据包含哪些是前端硬编码还是后端接口获取来的



Answer：

都是后端接口获取，表示在某时间段内不同IP地址count

FetchInvestigativeLogs

[

{

"date": "2024-02-01T00:00:00Z",

"type": "SomeType",

"priority": 1,

"message": "SomeMessage",

"info": "SomeInfo"

},

{

"date": "2024-02-01T00:01:00Z",

"type": "SomeType2",

"priority": 3,

"message": "SomeMessage2",

"info": "SomeInfo2"

}

]

FetchInvestigativeGraphs

[

{

"ip": "1.2.3.4",

"count": 200

},

{

"ip": "2.3.4.5",

"count": 180

},

{

"ip": "3.4.5.6",

"count": 160

},

{

"ip": "4.5.6.7",

"count": 140

},

//More objects would go here to reach 20 at MAXIMUM

]

**接口文档**

在quickwins中的3个接口返回数据结构没提供。

