Master Template: Cellular DFP

Dashboard Purpose: The training board develops Defense Force Protection by leveraging Network Survey device data. The dashboard focuses exclusively on cellular signals surveyed by operators surveying with NS devices. The purpose is to identify and highlight potential cellular anomalies in the area of interest, providing analysts with actionable insights to enhance situational awareness and threat detection with abnormal patterns that deviate from normal cellular behavior. Quickly allows an analyst to ID a time, location, and start point in the raw data for insight.

Within the Dashboard Links

https://view.seme.pro/kibana/app/dashboards#/view/194beae1-4a18-48e0-9b4c-f21919a69048?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15d,to:now))&_a=()

Included within Dashboard

Master Dashboard Template: Cellular DFP

| DFP Discover Template | SVIEW Sheets Template | Modify Map and Visualization Guide PDF |

DFP Cellular Template in Discover: Best for pulling and pivoting on large volumes of data, discover handles exporting queries above 10k records smoothly. Use when analysts need detailed records leading up to anomalies.
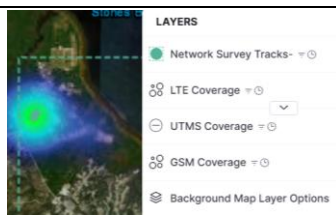
SVIEW Sheets Template: Optimized for quick pivots and lightweight analysis under 10k records. While focusing on location based searching. Best when speed and simplicity are needed for drilling into specific cellular anomalies.

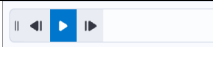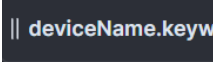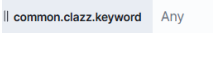## Modifying Filters on Dashboard using the Map and Filters

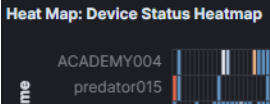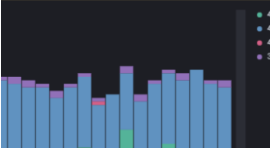|	
Search Bar	Free query the deviceName prefix example (*deviceName: predator** this filters the DB.
Add Filter	Choose Index, field, boolean (AND OR), and value to filter the dashboard.
Pinned Filters	Filters pinned when switching from discover, viz, or DB to carry over filters.
Load Query	Saved queries are saved with DTG filters and are accessible to all users.
Polygon Filter	In a Map, click **wrench**→ click **draw shape** → **save title** and view as a filter for the DB.
Time Range	Adjust the calendar: quick selection: the last 1 hour or the absolute date for firm dates.

Understanding Each Graph

Map: Network Survey Cellular Map **Purpose:** Identify cellular data from NS users of cellular structure and highlight potential anomalies in the area of interest, providing analysts with actionable insights to enhance situational awareness and threat detection. Broken out into cellular technologies.

	Network Survey Cellular Tracks: The survey route of an NS User
	LTE Coverage: LTE coverage in the area from LTE 4G cell towers.
	UMTS Coverage: UMTS coverage from UMTS 3G cell towers. (Less encryption)
	GSM Coverage: GSM coverage from GSM 2G cell towers. (Least encryption)
	Maps Included: ESRI Labels and ESRI Satellite Imagery

Filtering the Network Survey Index (NS) Results

Visualization Top to Bottom	Snapshot of VIZ	How to Modify it
Control-Range Slider: "Time Range Slider" This allows the user to filter for the time		Click Pen→ adjust Field OR Adjust Range
Control-Range Option: deviceName The user views a list of available deviceNames based on time filters and that index . A list is provided and the DB user can select specific end user and modify the dashboard to filter for only those selected users.	|| deviceName.keywo	Click Pen→ adjust Field → adjust selection
Control-Range Option: common.clazz This allows the user to view a list of technologies and select which technology they want to view (GSM, UMTS, LTE or/and NR)	|| common.clazz.keyword Any	Click Pen→ adjust Field → adjust selection

Current Visualizations in Dashboard: Purpose and Modifying		
Visualization Top to Bottom	**Snapshot of VIZ**	**How to Modify it**
Heat Map: "Device Status Heatmap" Purpose: Displays deviceName active with the filters used to identify active devices and how active those users are.	Heat Map: Device Status Heatmap ACADEMY004 predator015	Click ▫ → Edit Lens→ Modify deviceName → save & return→ SAVE DB
Bar Graph: "Drops in Service" Purpose: Use this graph to detect unexpected drops in the servicing technology.	NetworkSurveyUMTS NetworkSurveyLTE NetworkSurveyGSM NetworkSurvey5G	Click ▫ → Edit VIZ→ Modify deviceName in Set Filter → click Refresh→ save & return→ SAVE DB
Line Graph: "Cellular DFP Signal Strengthen" Purpose: Look for a significant spike in signal strength and/or false serving cells (neighbor cell) have a prolonged higher signal strength than the true serving cell (cell providing service). Note the circles are not indicators of anomaly behavior.	-40 -60 -80 -100 -120	Click ▫ → Edit VIZ→ Modify Set Filter → save and return→ SAVE DB
Bar Graph: "Cellular Anomaly Detection-MCC and MNC of Interest" Purpose: Analyst to identify potential towers of interest where it is not historically seen. Look for Mobile Country Codes (MCC) or Mobile Network Codes (MNC) that should not typically be seen in the surveyed area.	466 - 1 466 - 9 466 - 9 310 - 4	Click ▫ → Edit VIZ→ Modify deviceName in Set Filter → click Refresh→ save & return→ SAVE DB
Bar Graph: "Cellular Anomaly Detection-Neighbor List Present" Purpose: The analyst can ID potential towers of interest where there is a lack of neighbor cells reported, and only the serving cell can be a potential for an anomaly. Look for areas with no neighbor cells present (red color). Neighbor cells should always be part of the survey.	Serving Cell Neighbor	Click ▫ → Edit VIZ→ Modify deviceName in Set Filter → Click Refresh→ Save and return→ SAVE DB
Bar Graph: "Cellular Anomaly Detection-Rolling TAC/LAC Purpose: Shows over time, a user is switching TACS & LACs used to ID cellular anomalies. **1.** If the NS device is stationary & the LAC/TAC is rapidly switching. (Normal- on a LAC Border or Poor Signal strength.) **2.** If an NS device moves outside a LAC/TAC, it has only 1 LAC/TAC. **3.** If the device only surveys LAC (2g/3g) in a historically LTE area.	Rolling TAC/LAC abnormal changing of lacs and ta... LAC Count Tac Count 00 03:00 06:00 09:00 12:00 15:00 on.eventTime per 5 minutes	Click ▫ → Edit Lens→ Modify user prefix group in the search bar → click Refresh→ save & return→ SAVE DB.