Search Variable Support - Preliminary Requirements Summary

Ask

- Search variables in a search clause will allow users to specify a set of values for specific use-cases enabling re-usability in dashboards and other search use-cases

NDR Use-case

Generate this dashboard, by supporting variables, such as a homenet variable that can be populated using a generate search syntax.

Homenet variable would gather all homenet information stored in the NIDS schema

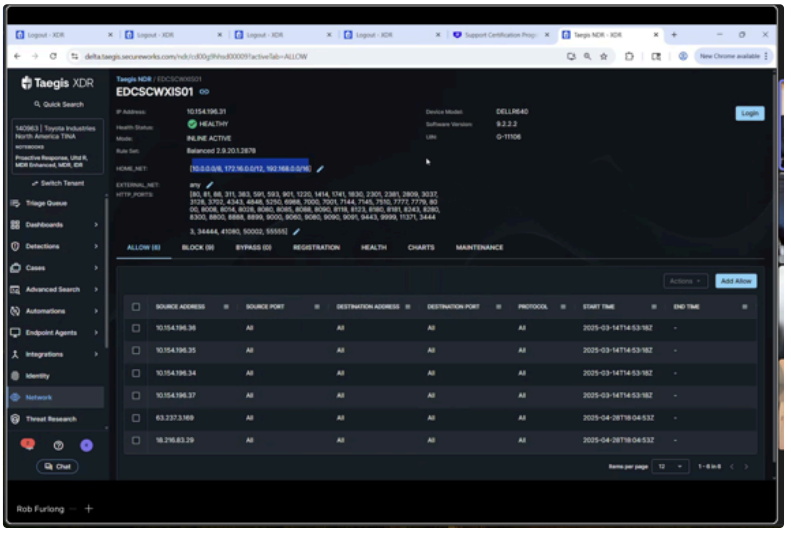
Allows for generic block, value-add dashboard to show NDR value

NDR iSensor Value Prop Report generated by CSMs

Directionality	Source	Dest	Total
Internal to Internal	Home_Net	Home_Net	228,706
Inbound	External_Net	Home_Net	148,669
External to External	External_Net	External_Net	301
Outbound	Home_Net	External_Net	2,139,105
Grand Total			2,516,781

- This requires bespoke queries and planning for each NDR instance and each customer
- Variable would allow generic dashboards deployed to Taegis by default showing this information

Taegis Network Console



Query

FROM nids WHERE ((sensor_type = 'isensor' AND blocked = 2) AND ((((sensor_id = 'iSensor_India' AND source_address IN ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16', '182.71.197.82/31', '182.71.197.84/30', '182.71.197.88/30', '182.71.197.92/31', '182.71.197.94/32')) AND destination_address !IN ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16', '182.71.197.82/31', '182.71.197.84/30', '182.71.197.88/30', '182.71.197.92/31', '182.71.197.94/32')) OR ((sensor_id = 'iSensor_AUS' AND source_address IN ('139.130.128.110/30', '110.174.237.126/29')) AND

destination_address !IN ('139.130.128.110/30', '110.174.237.126/29'))) OR ((sensor_id IN ('iSensor_Brazil', 'isensor_Hayward_10G', 'iSensor_Mexico', 'iSensor_Pembroke', 'iSensor_Scotland', 'iSensor_SouthAfrica') AND source_address IN ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16')) AND destination_address !IN ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16')))) EARLIEST='2026-01-05T00:00:00.000Z' AND LATEST='2026-01-11T23:59:59.000Z'

Competitor SIEM Examples

SumoLogic

Filtering Dashboards with Template Variables | Sumo Logic Docs

MS Sentinel

Let statement - Kusto

Timing

- Requirements and technical review discussion mid-Feb
- Possible Q3 deliverable

TODO

- Gather addtional variable use-cases
- Gather technical requirements
- Gather UX/UI updates (if any)
- Gather value prop for NDR

Raw Notes

- Add a variable for homenet for NDR
  - Where do variables go?

    - From NIDS schema
- Don’t have variable support in the language
    - patterns
    - Any other requirements
    - File for this
    - Search for reqs
- Create the dashboard shown using the variable
    - Homenet variable make it more standardized
    - How to build a custom dashboard
- Medium effort
- Impact statement
- NDR 21.5 million, larger impacts on NDR; stop other services
    - Tied to larger dollars
    - Move my MDR
    - Self-serve, customer stance
- Mid February requirements and use-cases