
ONTOLOGY
Some thoughts

What is a finding

- The term **finding** is used to describe the result of an analytic. The word finding is emerging as a common classifier across the industry to discuss the results of security based tools.

- For example:
  - In a SOC: “We are working through 23 findings since lunch”
  - In a red team: “Our report details 23 findings as a result of our pen test”
  - …

Q: What should a good findings object do?

- Assist the consumer in understanding the data to be consumed.
- Present all information in a logical construct.
- Reduce duplication, combined with a solid ontology become a single point of truth.
- Limit callbacks to source by generating complete data sets at the point of consumption.

NIST – An ontology that's open to assist in finding classification

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

DXL Ontology Example 1

- findings_de.ae_siem_*mostRecentFinding*

An ontology topic that will deliver a *finding* that describes *anomalies and event data* from *a siem* that concern *mostRecentFinding*

Structural

Semantic

This approach allows us to group findings, relate findings in a hierarchy and subdivide findings

Ontology in use

Access Topic: findings

Returns all findings.

Access Topic: findings_de.ae

Returns all findings that relate to anomalies and events

Access Topic: findings_de.ae_siem

Returns all findings that relate to anomalies and events that originate from the SIEM

Topic: findings_de.ae_siem_mostRecentFinding

Returns the most recent single finding that relates to anomalies and event data that originated from the SIEM.

Growing ontology

- /findings_de.ae_siem_ mostRecentFinding
- /findings_de.ae_siem_ mostRecentFindings
- /findings_de.ae_siem_ mostRecentFindingsByIP
- /findings_de.ae_siem_ mostRecentFindingsByFileHash
- /findings_de.ae_siem_ mostRecentFindingByURL
- /findings_de.ae_siem_ mostRecentFindingByDomainName

individual

groupset

DXL Ontology (special character use)

/ used to identify hierarchical leap in filtering.

-(dash) used to indicate source (combination) finding genus.

.(dot) used to indicate shorthand representation.

notifications/findings/<nistIdentifier>/<source>/<discriptionOfActivity>