

Karin Patenge's GitHub repository with all sample code for this session can be found here:

**[https://github.com/karinpatenge/events/tree/main/
2026/09_AnDOUC](https://github.com/karinpatenge/events/tree/main/2026/09_AnDOUC)**



ANALYTICS AND DATA

TechCasts

Graph Analytics with Oracle AI Database 26ai and Linkurious Oigma

Karin Patenge, Senior Principal Product Manager, Oracle Spatial & Graph
Leo Nicolle, Linkurious Visualisation Engineer, Linkurious

Past & Future TechCasts:



August 20th

How and Where Oracle 26ai Beats Python for Data Preparation

Presented by Dr. Holger Freidrich



September 17th

Graph Analytics With Oracle AI Database 26ai and Linkurious Ogma

Presented by Karin Patenge & Leo Nicolle



October 15th

Not-to-Miss Sessions at Oracle AI World 2026

Presented by Keith Laker, Jamie Anderson, Ben Arnulf, & Melli Annamalai

TechCast Archive

2026	2025	2024	2023	2022	2021	
Date	Title			Presenter(s)	Replay	Download(s)
Aug 20	How and Where Oracle 26ai Beats Python for Data Preparation			Dr. Holger Friedrich, sumIT	Video	Slides
Jul 23	Temporal Data Lineage and Impact Analysis in Oracle Database: Evolution to Oracle Graph Architecture with Time-Travel Capabilities			Karin Patenge, Oracle & Tomislav Zarkovic, Koios	Video	Slides
Jun 25	Our Favorite Features of OAC: March & May 2026 Releases			Gautam Pisharam & Carter Beaton	Video	Slides
Apr 30	Pythian’s AI Journey with UMass: From AI Assistant to AI Agents!			Jon Mead & Ambili Thottathil, Pythian	Video	Slides
Apr 2	Build Practical AI Prototypes with Oracle Analytics (Even with a Small Team)			Dennis Gray & Adam Hume, Definian	Video	Slides
Mar 5	Fraud Stops with Oracle Database 26ai Vector Search + OML			Dr. Abigail Giles-Haigh	Video	Slides

Submit a topic to share at <https://andouc.org/techcasts/>

Let's Connect



Website

<http://andouc.org/>



Chat with the Experts

<https://bit.ly/Join-ANDOUC-Slack>



Watch Previous TechCasts

<https://bit.ly/3qmGgHN>



<https://www.linkedin.com/company/analytics-and-data-oracle-user-community>



Spatial + Graph SIG

bit.ly/Spatial-Graph-LinkedIn



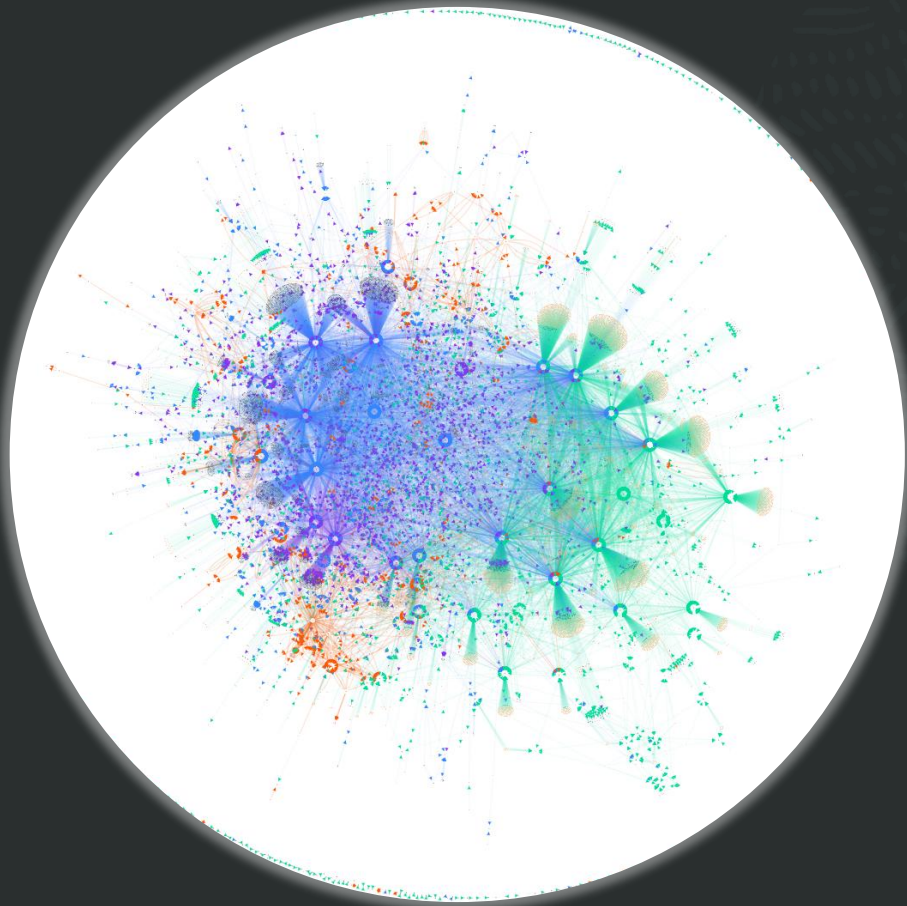
@analyticsndataouc.
bsky.social



SAVE THE DATE!
April 13-15, 2027

***Call for Papers
is OPEN!!***

Speakers



Karin Patenge

Product Manager @
Oracle

karin.patenge@oracle.com



Léo Nicolle

Visualization Engineer @
Linkurious

contact@linkurio.us

Agenda

Why Linkurious Ogma

About the Dataset

Explore SQL Property Graphs using Linkurious Ogma

Overview about Cyber Threat Scenarios

Graph Analytics applied to a Cyber Threat Scenario

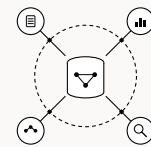
Take-Aways

Why Linkurious Ogma?

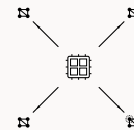


ogma-oracle-parser

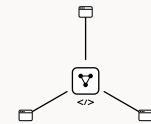
Linkurious is a leading Graph Visualization solution provider.



SQL Property Graphs in Oracle AI Database is an open ecosystem. Can easily be integrated with 3rd party specialized tools because of SQL/PGQ.



WebGL-based that leverages GPU acceleration for large, complex, and interactive graphs.

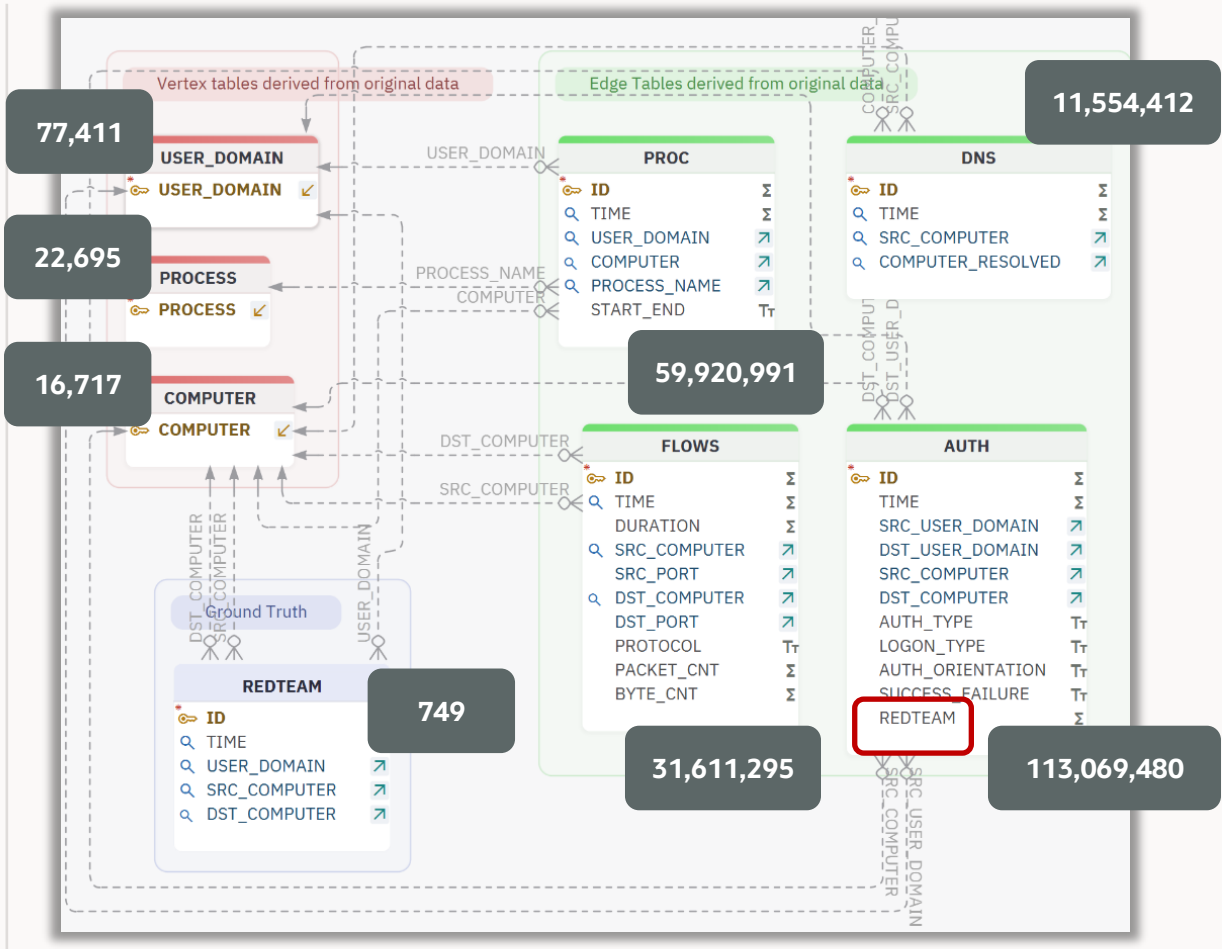


Developer-friendly by design — offers native framework support and low-code integration, letting teams build sophisticated graph visualizations with minimal overhead.

Overview about Cyber Threat Scenarios

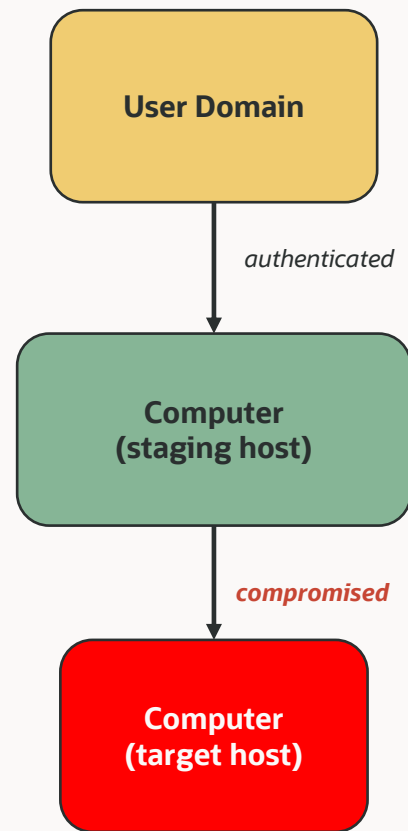
Mapping the Dataset to Vertices & Edges

File	Mapping to Vertices & Edges
auth.txt	Vertices ➡ User Domains, Computers Edges ➡ User Domain ➡ Computer, Computer ➡ Computer
proc.txt	Vertices ➡ User Domains, Computers, Processes Edges ➡ User Domain ➡ Computer, Computer ➡ Process
flows.txt	Vertices ➡ Computers Edges ➡ Computer ➡ Computer
dns.txt	Vertices ➡ Computers Edges ➡ Computer ➡ Computer
redteam.txt	Vertices ➡ User Domains, Computers Edges ➡ User Domain ➡ Computer, Computer ➡ Computer

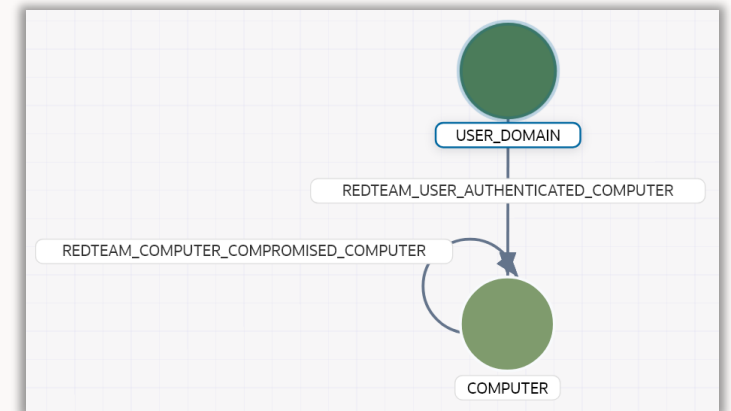


The Ground-Truth Graph

REDTEAM as a 2-hop attack chain



```
-- Ground-truth graph based on REDTEAM data
CREATE PROPERTY GRAPH IF NOT EXISTS lanl_ground_truth_graph
  VERTEX TABLES (
    user_domain
    KEY ( user_domain )
    LABEL user_domain PROPERTIES ARE ALL COLUMNS,
    computer
    KEY ( computer )
    LABEL computer PROPERTIES ARE ALL COLUMNS,
    process
    KEY ( process )
    LABEL process PROPERTIES ARE ALL COLUMNS
  )
  EDGE TABLES (
    redteam AS redteam_user_authenticated_computer
    KEY ( id )
    SOURCE KEY ( user_domain ) REFERENCES user_domain ( user_domain )
    DESTINATION KEY ( src_computer ) REFERENCES computer ( computer )
    LABEL authenticated
    PROPERTIES ( id, time, user_domain, src_computer ),
    redteam AS redteam_computer_compromised_computer
    KEY ( id )
    SOURCE KEY ( src_computer ) REFERENCES computer ( computer )
    DESTINATION KEY ( dst_computer ) REFERENCES computer ( computer )
    LABEL compromised
    PROPERTIES ( id, time, user_domain, src_computer, dst_computer )
  )
```



The Cyber Graph

-- Cyber graph combining AUTH, DNS, FLOWS, and PROC
CREATE PROPERTY GRAPH IF NOT EXISTS **lanl_cyber_graph**

VERTEX TABLES (

user_domain

KEY (user_domain) LABEL user_domain PROPERTIES ARE ALL COLUMNS,

computer

KEY (computer) LABEL computer PROPERTIES ARE ALL COLUMNS,

process

KEY (process) LABEL process PROPERTIES ARE ALL COLUMNS

)

EDGE TABLES (

dns AS dns_computer_resolved_computer

KEY (id) SOURCE KEY (src_computer) REFERENCES computer (computer) DESTINATION KEY (computer_resolved) REFERENCES computer (computer)

LABEL resolved PROPERTIES (id, time, src_computer, computer_resolved),

flows AS flows_computer_connected_computer

KEY (id) SOURCE KEY (src_computer) REFERENCES computer (computer) DESTINATION KEY (dst_computer) REFERENCES computer (computer)

LABEL flows_connected PROPERTIES (id, time, duration, src_computer, src_port, dst_port, dst_computer, protocol, packet_cnt, byte_cnt),

proc AS proc_user_authenticated_computer

KEY (id) SOURCE KEY (user_domain) REFERENCES user_domain (user_domain) DESTINATION KEY (computer) REFERENCES computer (computer)

LABEL proc_connected PROPERTIES (id, time, user_domain, computer),

proc AS proc_computer_runs_process

KEY (id) SOURCE KEY (computer) REFERENCES computer (computer) DESTINATION KEY (process_name) REFERENCES process (process)

LABEL ran PROPERTIES (id, time, computer, process_name, start_end),

auth AS auth_src_user_authenticated_src_computer

KEY (id) SOURCE KEY (src_user_domain) REFERENCES user_domain (user_domain) DESTINATION KEY (src_computer) REFERENCES computer (computer)

LABEL auth_src_authenticated PROPERTIES (id, time, src_user_domain, src_computer, auth_type, logon_type, auth_orientation, success_failure, **redteam**),

auth AS auth_dst_user_authenticated_dst_computer

KEY (id) SOURCE KEY (dst_user_domain) REFERENCES user_domain (user_domain) DESTINATION KEY (dst_computer) REFERENCES computer (computer)

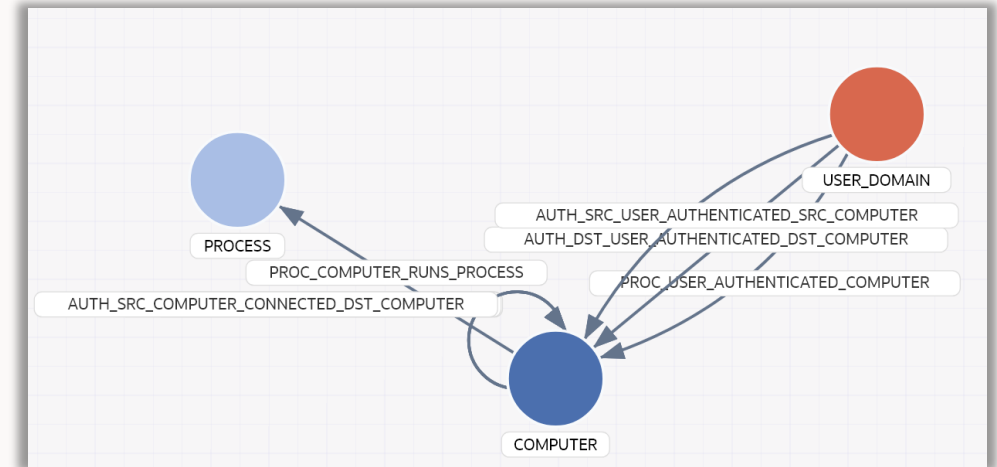
LABEL auth_dst_authenticated PROPERTIES (id, time, dst_user_domain, dst_computer, auth_type, logon_type, auth_orientation, success_failure, **redteam**),

auth AS auth_src_computer_connected_dst_computer

KEY (id) SOURCE KEY (src_computer) REFERENCES computer (computer) DESTINATION KEY (dst_computer) REFERENCES computer (computer)

LABEL auth_connected PROPERTIES (id, time, src_computer, dst_computer, **redteam**)

)



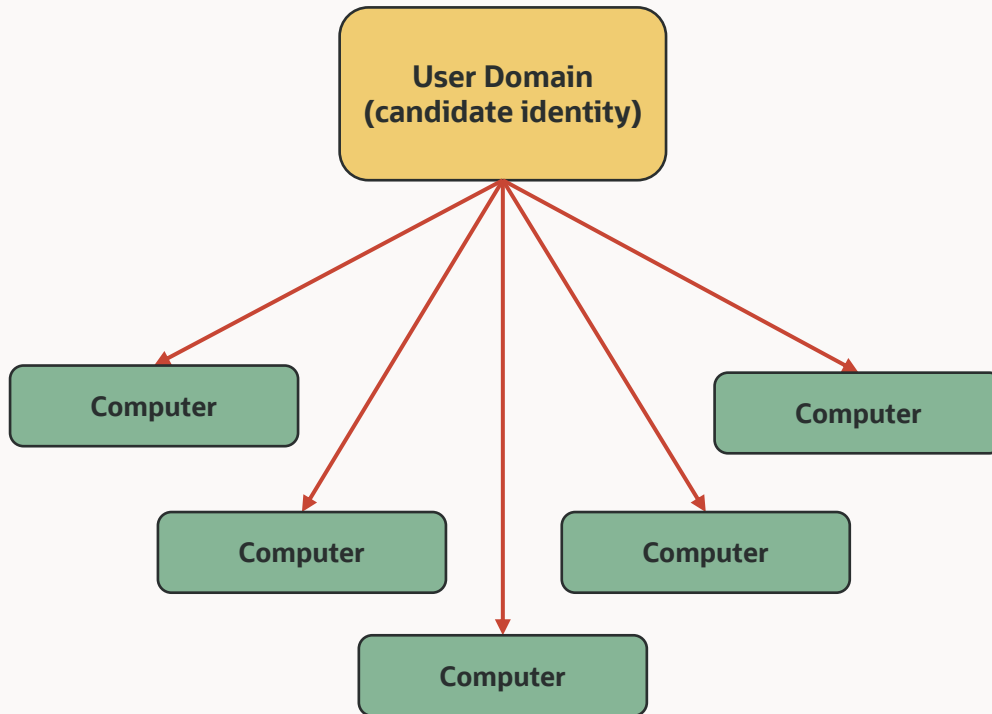
The following scenarios and scripts were created, tested, refined, and documented using:

- Codex (GPT 5.6 Luna Extra High)
- [Oracle AI Database Skills](#) (incl. SQL Property Graph skills)
- SQLcl MCP Server

Graph Analytics on Cyber Threat Scenarios

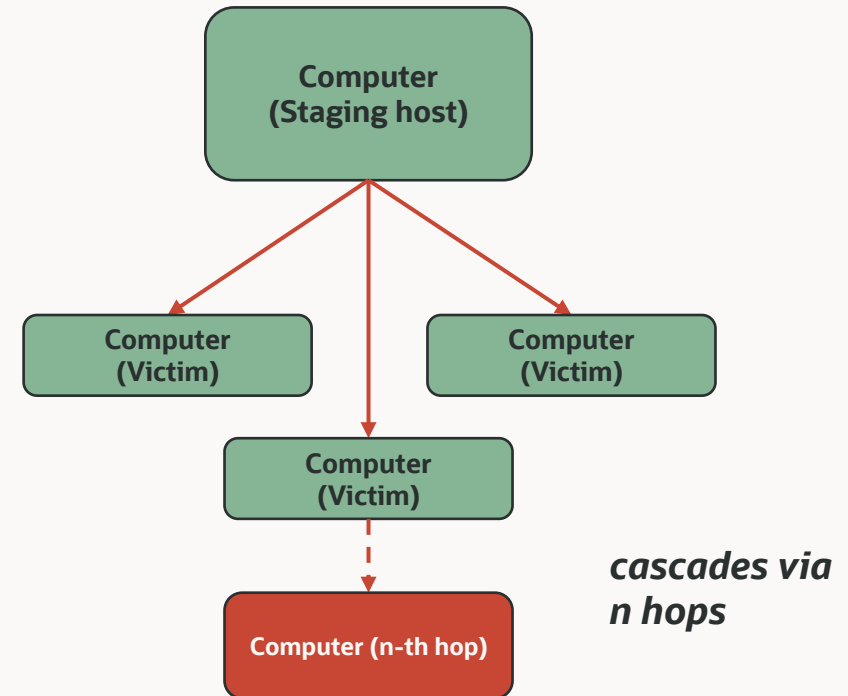
Start with Hypothesis

Hypothesis 1: Credential Theft (“Impossible Travel”)



5+ distinct computers, all within 1 hour

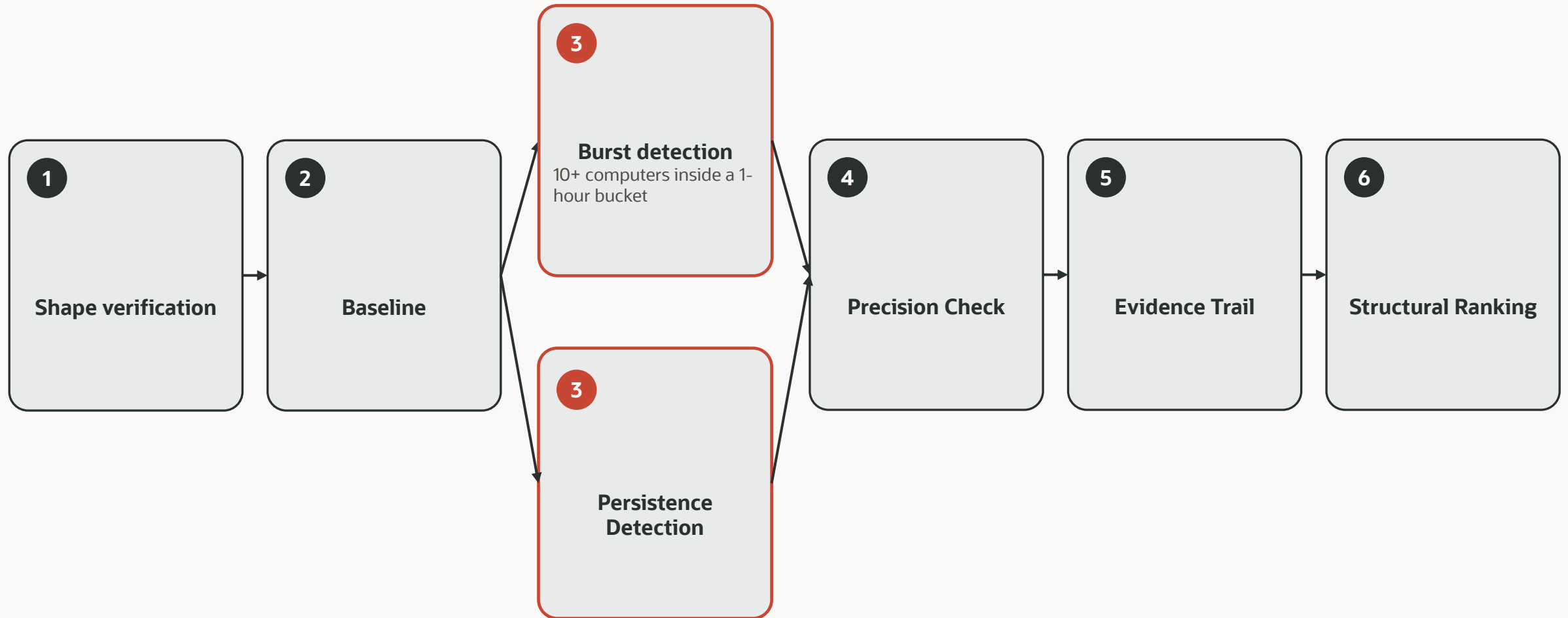
Hypothesis 2: Lateral Pivot



5+ distinct targets, all within 1 hour

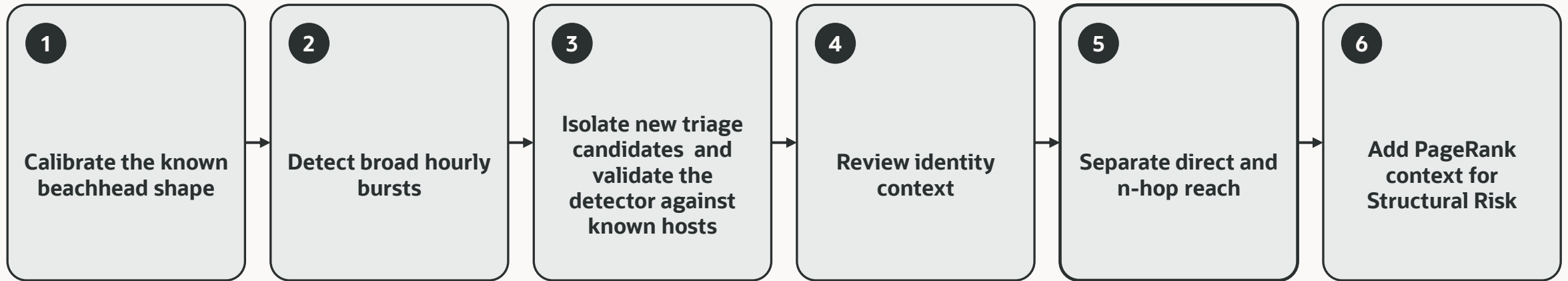
Proposed Workflow: Credential Theft

Fraudulent cross-computer authentication ("impossible travel")



Proposed Workflow: Lateral Pivot

Fraudulent “beachhead” reuse, cascading across hops

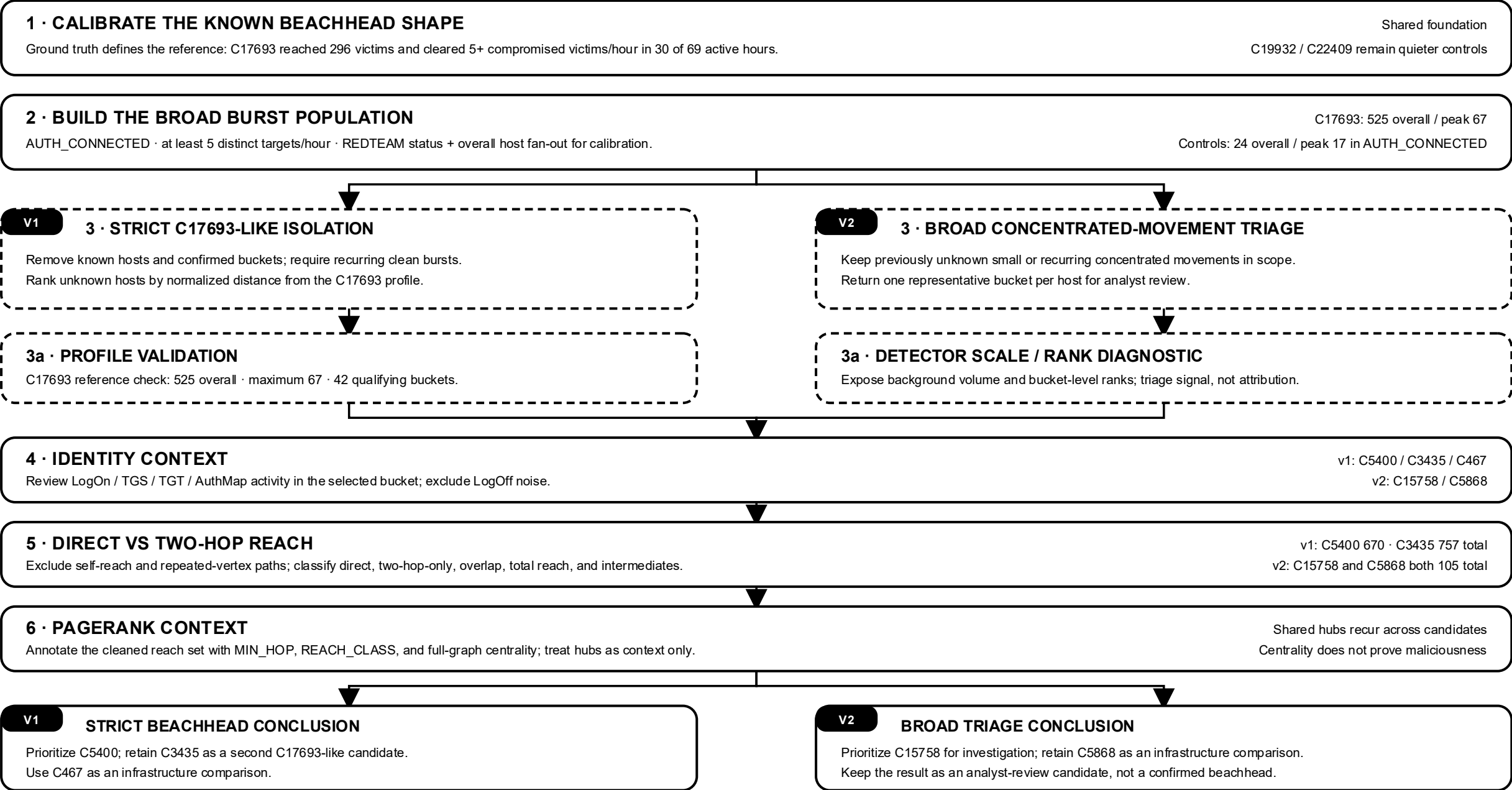


Explanation:

A beachhead is the one staging computer an attacker reuses repeatedly to pivot outward to many victims, with the pivot cascading across several hops rather than stopping at direct targets.

SCENARIO 2 — LATERAL PIVOT WORKFLOW

Combined view: v1 C17693-like beachhead search + v2 broad concentrated-movement triage



Both workflows identify candidates for review; additional evidence is required to confirm a beachhead.

Demo:

SQL-Based Graph Analytics

Using Visual Studio Code + SQL Developer Extension
(+ SQL Developer Graph Visualization Extension)

Final Step: Result

First 7 Rows

	COMPUTER	ROLE	MIN_HOP	REACH_CLASS	PAGERANK_SCORE
1	C586	REACHED	2	TWO_HOP_ONLY	0.04000134953389035
2	C612	REACHED	2	TWO_HOP_ONLY	0.03067915198494771
3	C529	REACHED	2	TWO_HOP_ONLY	0.030524342419061896
4	C625	REACHED	2	TWO_HOP_ONLY	0.02815230258829418
5	C467	REACHED	1	DIRECT_AND_TWO_HOP	0.027391278936998362
6	C457	REACHED	1	DIRECT_AND_TWO_HOP	0.026705827204715434
7	C1065	REACHED	2	TWO_HOP_ONLY	0.025190767835493295

Findings

Scenario 2

The 5+ Target Burst Is a Triage Signal,
Not a Beachhead Classifier

C15758 Is the Stronger Broad-Triage
Candidate

Multi-Hop Reach and PageRank Are
Strongly Hub-Driven



Scenario 2 identifies candidates for analyst review — **not confirmed beachheads**.

Take-Aways

Applying Graph Analytics is an iterative process. SQL has all techniques to do the analysis.

AI and Skills can help derive analytical scenarios, generate or refine queries, interpret the results, and document them.

Visualizing results helps a great deal in detecting & understanding patterns

SQL/PGQ removes barriers for the integration with (specialized) 3rd party graph visualization solutions



Thank You

Work In Progress:

LiveLabs Workshop – Stay tuned !

Past & Future TechCasts:



August 20th

How and Where Oracle 26ai Beats Python for Data Preparation

Presented by Dr. Holger Freidrich



September 17th

Graph Analytics With Oracle AI Database 26ai and Linkurious Ogma

Presented by Karin Patenge & Leo Nicolle



October 15th

Not-to-Miss Sessions at Oracle AI World 2026

Presented by Keith Laker, Jamie Anderson, Ben Arnulf, & Melli Annamalai

TechCast Archive

2026	2025	2024	2023	2022	2021
Date	Title	Presenter(s)		Replay	Download(s)
Aug 20	How and Where Oracle 26ai Beats Python for Data Preparation	Dr. Holger Friedrich, sumIT		Video	Slides
Jul 23	Temporal Data Lineage and Impact Analysis in Oracle Database: Evolution to Oracle Graph Architecture with Time-Travel Capabilities	Karin Patenge, Oracle & Tomislav Zarkovic, Koios		Video	Slides
Jun 25	Our Favorite Features of OAC: March & May 2026 Releases	Gautam Pisharam & Carter Beaton		Video	Slides
Apr 30	Pythian's AI Journey with UMass: From AI Assistant to AI Agents!	Jon Mead & Ambili Thottathil, Pythian		Video	Slides
Apr 2	Build Practical AI Prototypes with Oracle Analytics (Even with a Small Team)	Dennis Gray & Adam Hume, Definian		Video	Slides
Mar 5	Fraud Stops with Oracle Database 26ai Vector Search + OML	Dr. Abigail Giles-Haigh		Video	Slides

Submit a topic to share at <https://andouc.org/techcasts/>



SAVE THE DATE!
April 13-15, 2027

***Call for Papers
is OPEN!!***

Helpful Links –

ORACLE ANALYTICS VIDEOS:

<https://www.youtube.com/@OracleAnalytics/videos>

OAC MARCH AND MAY 2026 NEW FEATURES VIDEOS BY ORACLE:

<https://bit.ly/OACMar26Features>

<https://bit.ly/OACMay26Features>

OAC NEW FEATURES DOCUMENTATION BY ORACLE:

<https://docs.oracle.com/en/cloud/paas/analytics-cloud/acswn/index.html#GUID-CFF90F44-BCEB-49EE-B40B-8D040F02D476>

ORACLE ANALYTICS COMMUNITY:

<https://community.oracle.com/products/oracleanalytics>

ORACLE ANALYTICS LIBRARY/EXAMPLES:

<https://www.oracle.com/business-analytics/data-visualization/examples/>

ORACLE ANALYTICS LIVE DEMOS:

<https://www.oracle.com/business-analytics/data-visualization/demos/>