Threat Hunting in Microsoft Sentinel

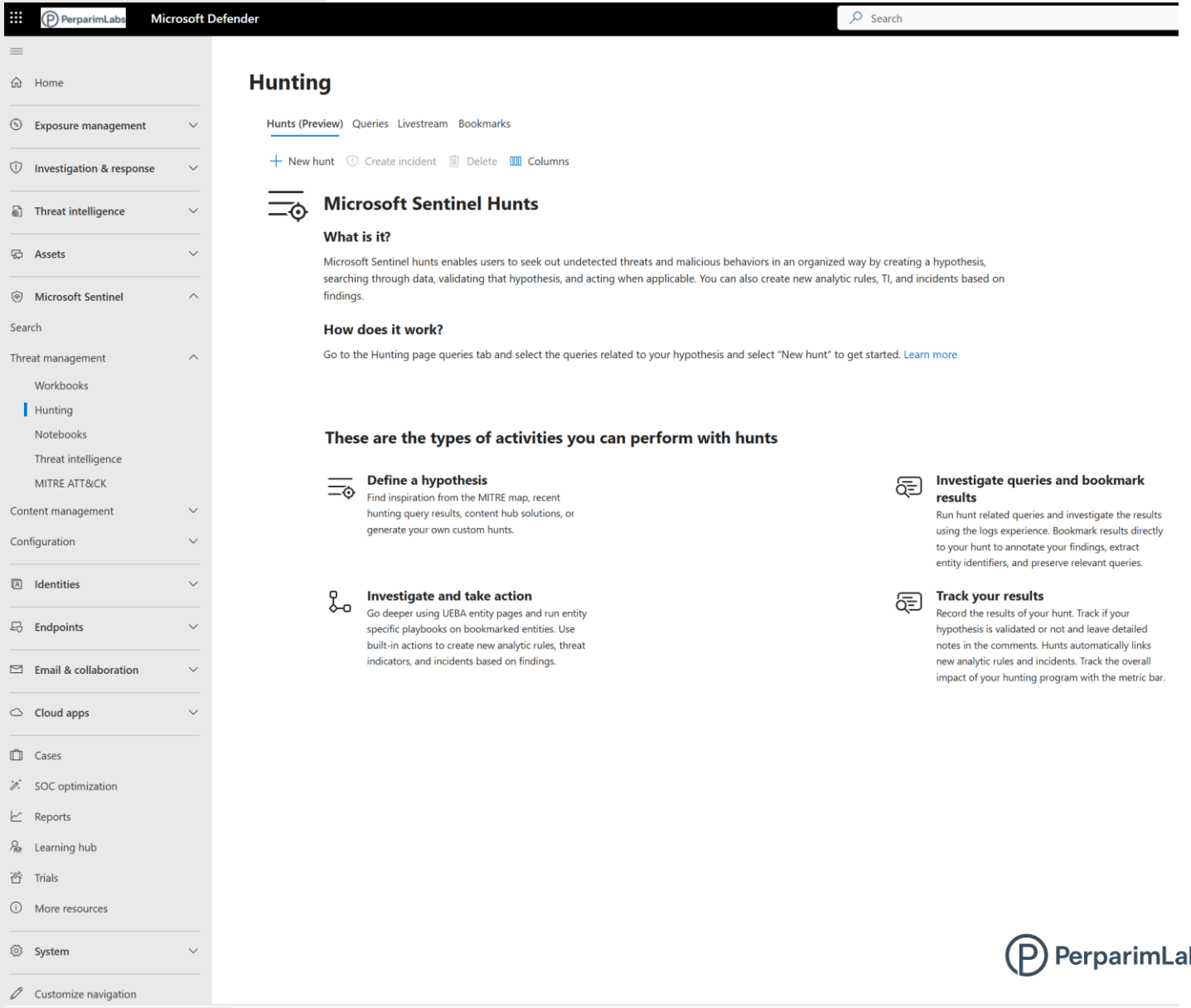
Using Built-in Queries to Detect Suspicious Activity

- Threat hunting = proactive search for threats that haven't triggered alerts.
- Sentinel leverages log data + built-in KQL queries.
- Goal: detect hidden attacks, lateral movement, open ports, or risky behaviors.

PerparimLabs

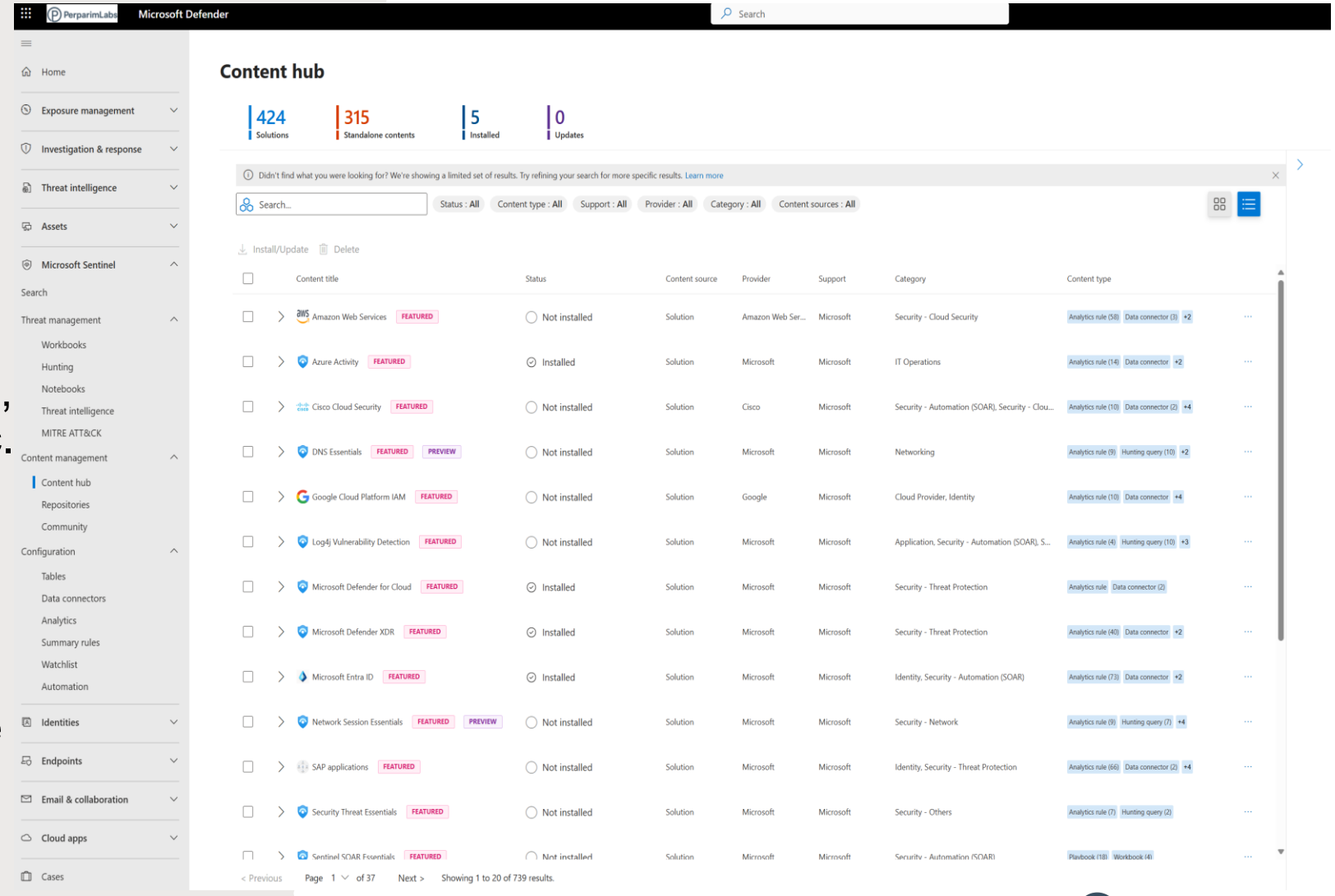
Hunting Entry

- Navigate to **Microsoft Sentinel > Hunting**.
- The Hunting blade centralizes all hunting queries from **Content Hub**.
- SOC teams use this to **test hypotheses**, investigate data, and take action.



Content Hub Providers

- Hunting queries are powered by installed **solutions/connectors**.
- Each provider (Microsoft Entra ID, Defender XDR, Azure Activity, etc. brings:
  - Prebuilt queries
  - Data connectors
  - Analytics rules
- Installing these ensures you have the **queries + data** needed.



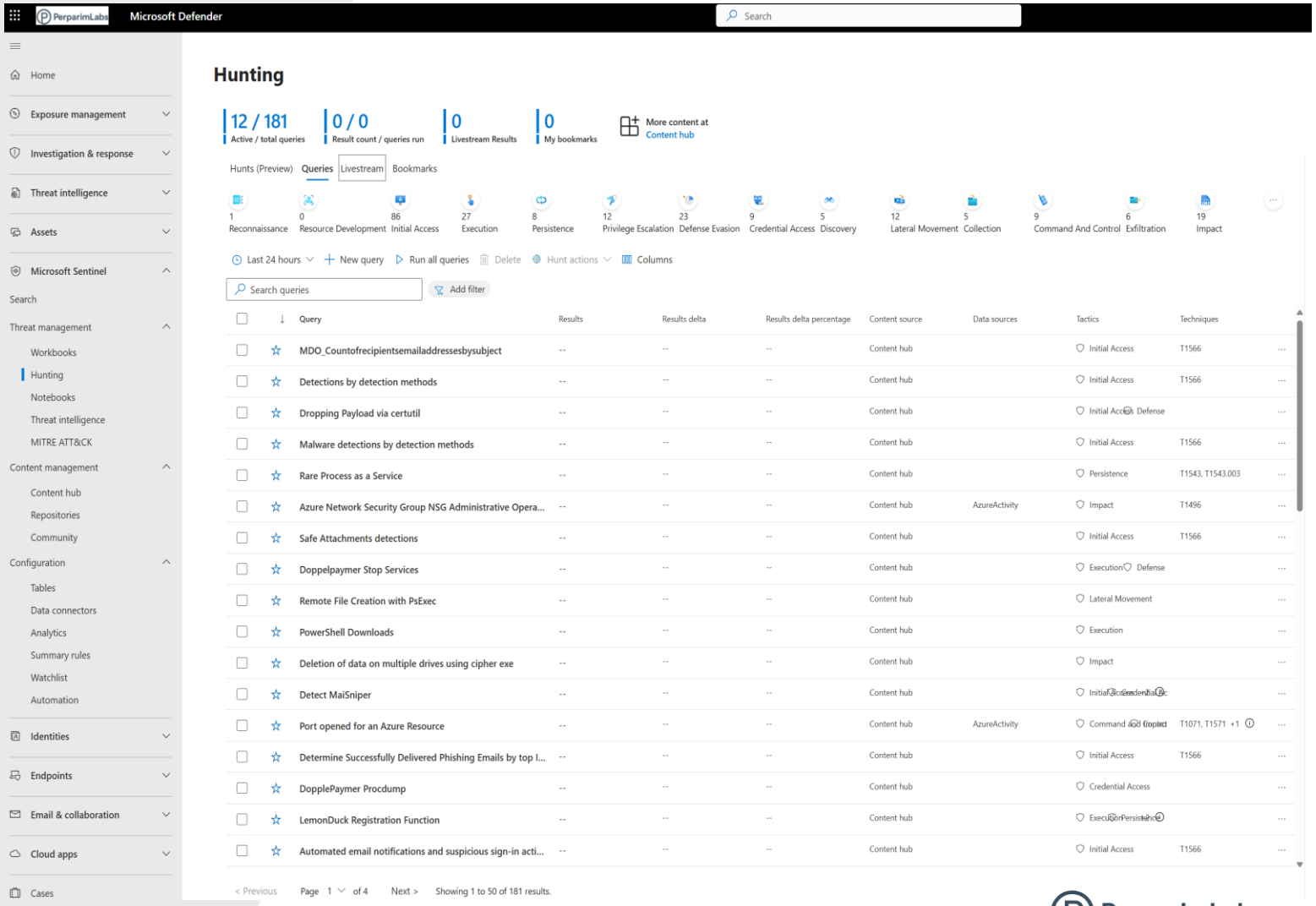
💡 Tip: More connectors = richer hunting capability.

Running hunts is free; **data ingestion** is billed via Log Analytics.

PerparimLabs

Query Library

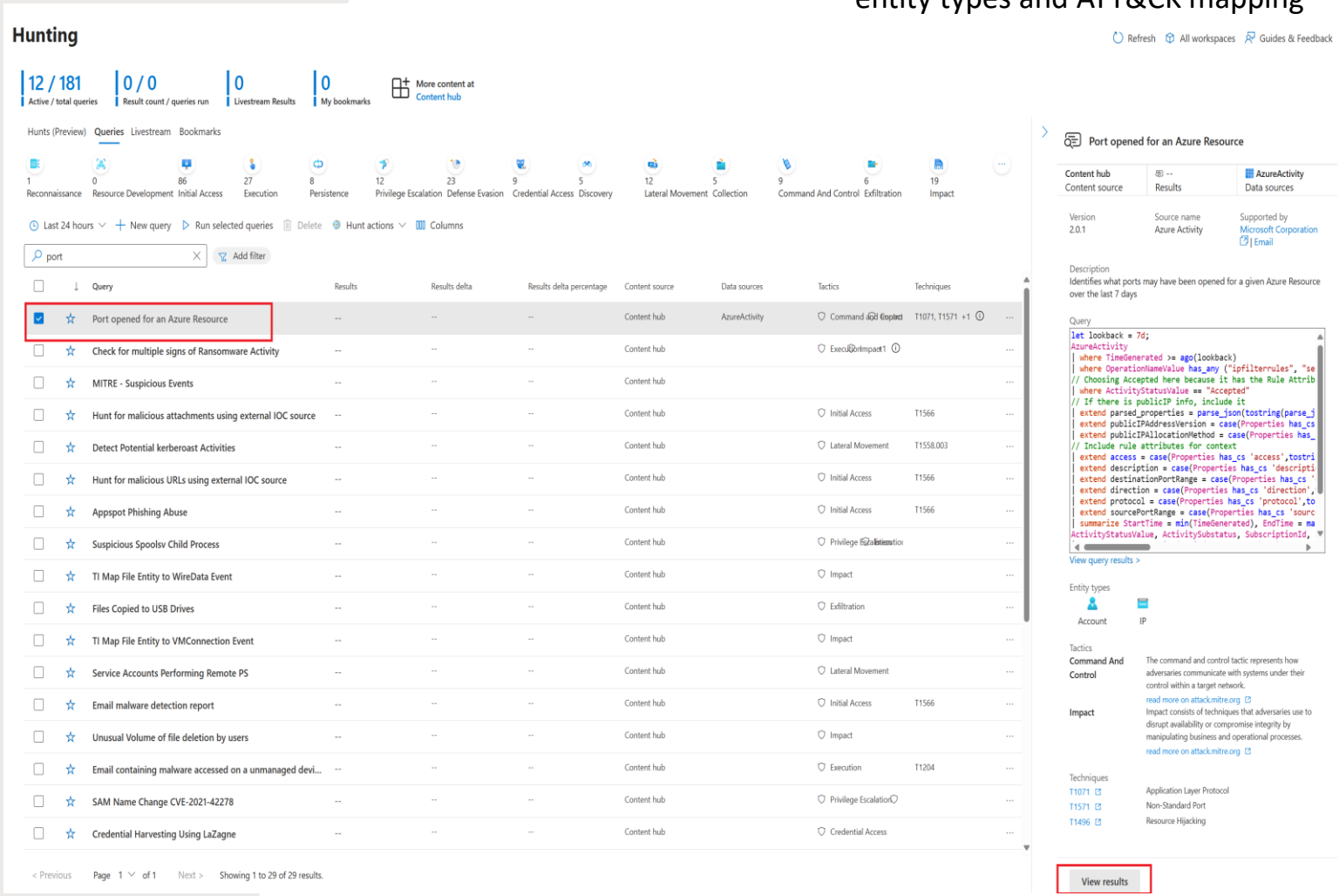
- Sentinel provides **181+ hunting queries** mapped to MITRE ATT&CK tactics.
- Examples:
  - Port scanning activity
  - Phishing attempts
  - Lateral movement detection
- Queries are categorized by **tactics (Initial Access, Persistence, Impact, etc.)**.



Selecting a Query

- Example query: **Port opened for an Azure Resource.**
- Purpose: detects ports opened on VMs or Arc-enabled servers.
- Shows KQL script on the right-hand pane.
- You can **run as-is** or **customize KQL** (e.g., change timeframe).

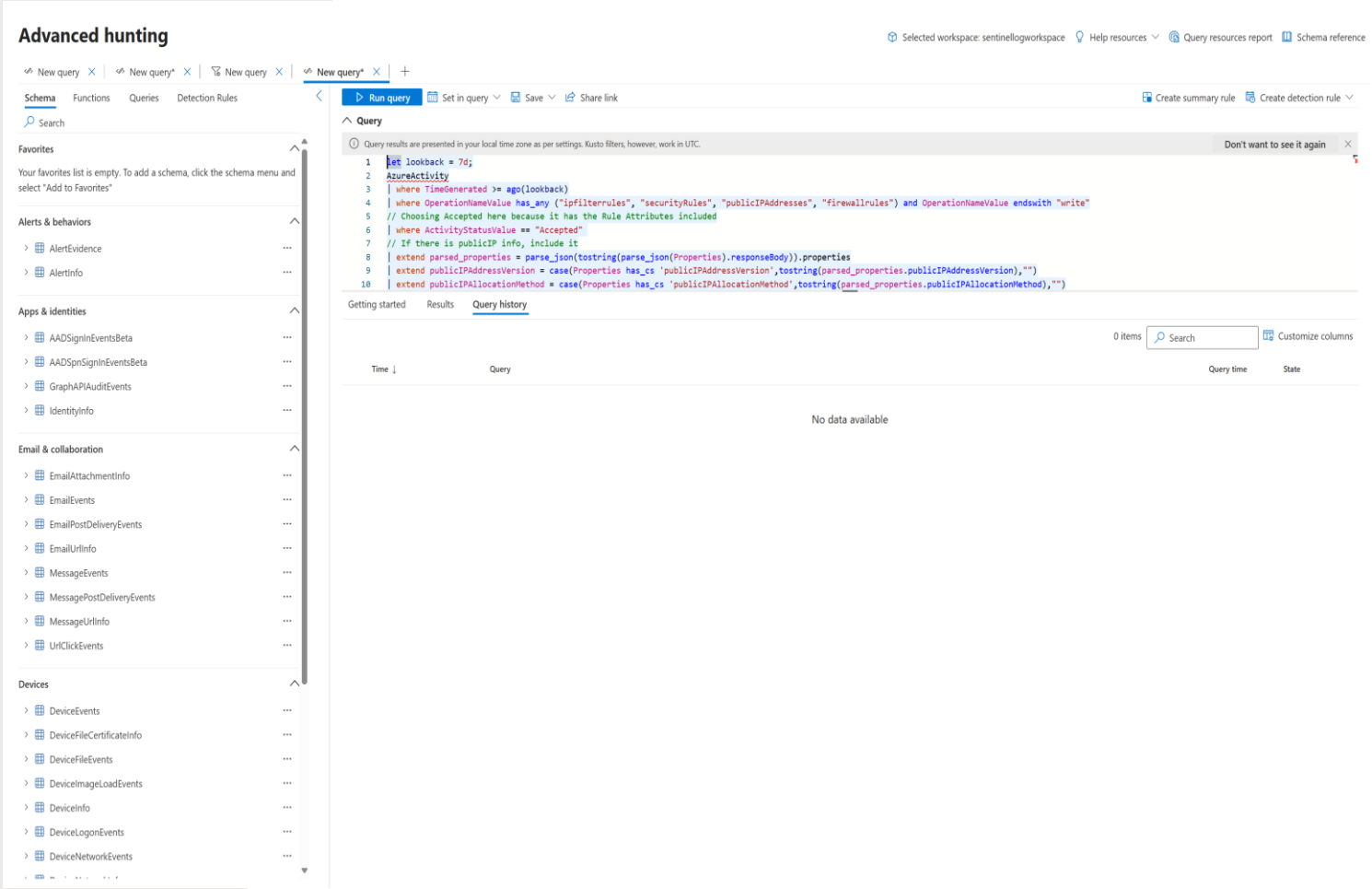
Right pane shows KQL + related entity types and ATT&CK mapping



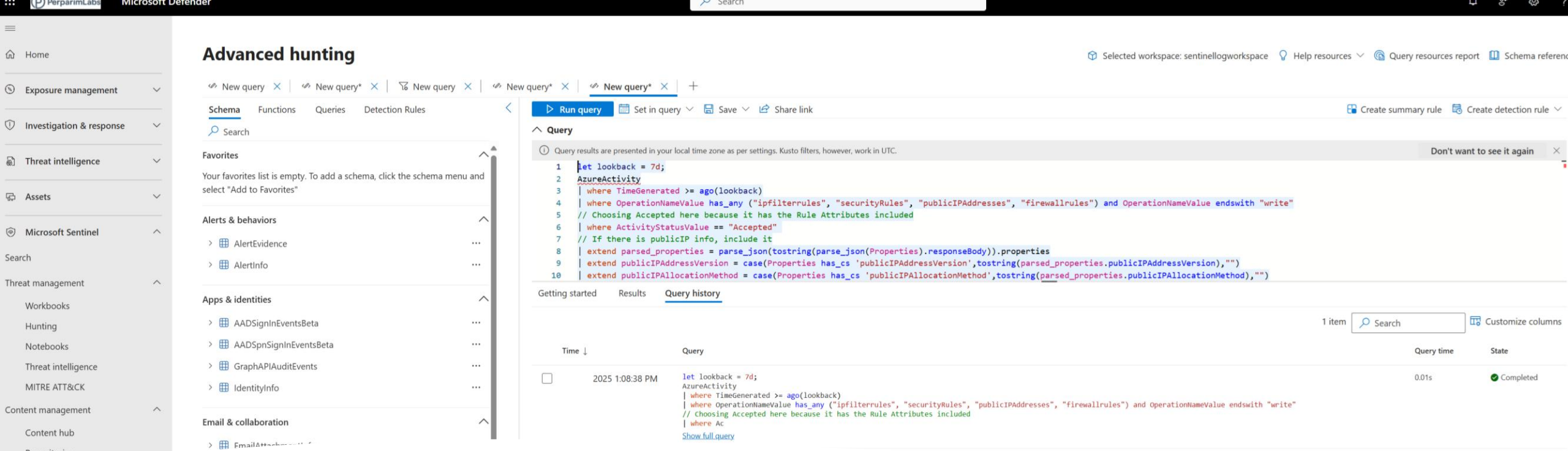
Running the Query

- Run queries directly in **Advanced Hunting**.
- Output: list of matching activities (if detected).
- Even with **no results**, this demonstrates:
  - Query syntax
  - Data sources checked
  - Baseline validation
- **Time range matters** (retention + lookback window control what you see).

💡 *Tip:* In real SOC, lack of results still validates your baseline security posture.



PerparimLabs



Query History

- All executed hunts are logged in **Query History**.
- **Save / Share link** to reuse with your team or convert to a detection rule later.
- Useful for:
  - Tracking which hunts were performed
  - Sharing queries with SOC teams
  - Building repeatable playbooks

PerparimLabs

Key Takeaways

- Threat hunting = proactive defense.
- Sentinel gives **prebuilt KQL queries** from Content Hub.
- You can:
  1. Run & customize queries.
  2. Investigate suspicious activity.
  3. Feed results into **alerts, incidents, or playbooks**.
- Hunting complements **automation & analytics** for complete SOC coverage.
- Convert useful hunts to **analytics rules** or **automation** (SOAR) for continuous coverage.

PerparimLabs