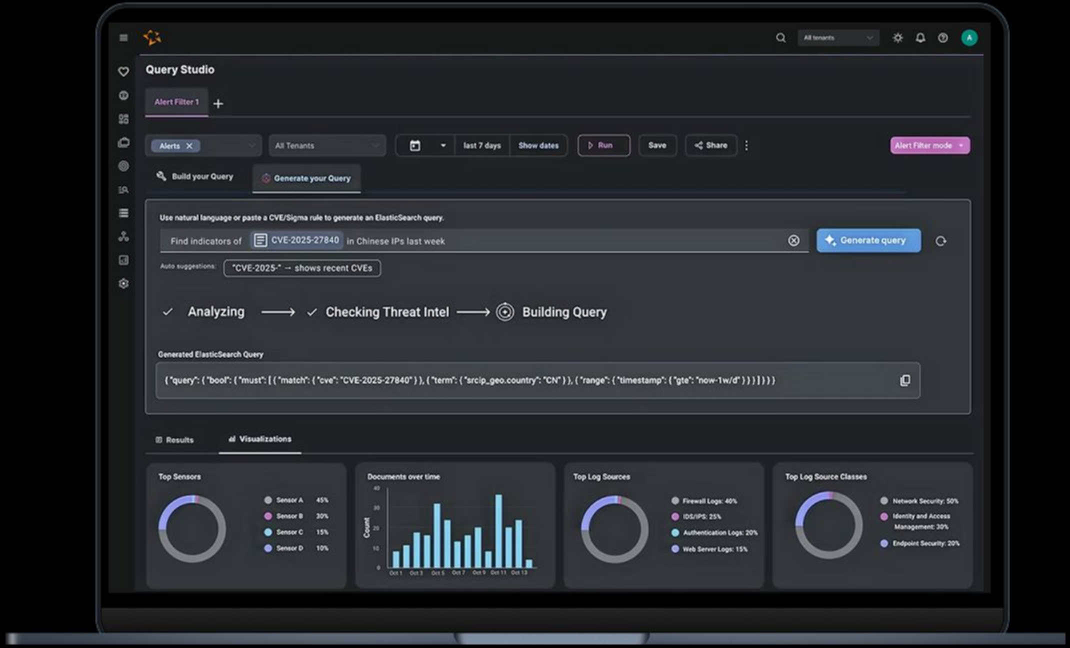
Background & Context

Query Studio: Empowering Analysts to 'Speak Security’



Use natural language or paste a CVE/Sigma rule to generate an ElasticSearch query.

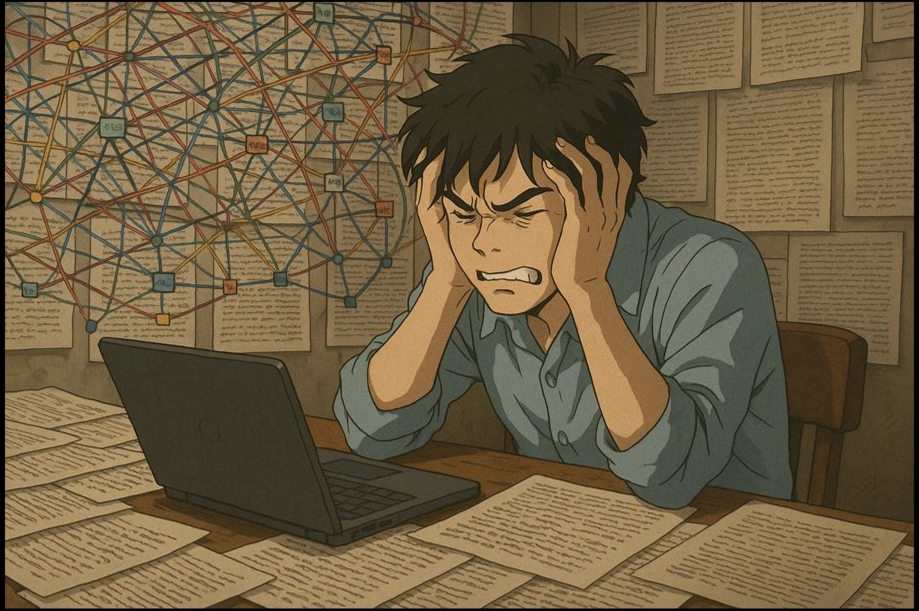
Find indicators of CVE-2025-27840 in Chinese IPs last week

Generate query
Auto suggestions:
"CVE-2025-" → shows recent CVEs
✓ Analyzing ⟶ ✓ Checking Threat Intel ⟶ Building Query
Generated ElasticSearch Query

```
{ "query": { "bool": { "must": [ { "match": { "cve": "CVE-2025-27840" } }, { "term": { "srcip_geo.country": "CN" } }, { "range": { "timestamp": { "gte": "now-1w/d" } } } ] } } }
```

Problem

The Challenge: Bridging the Gap Between Human Intuition and Machine Data



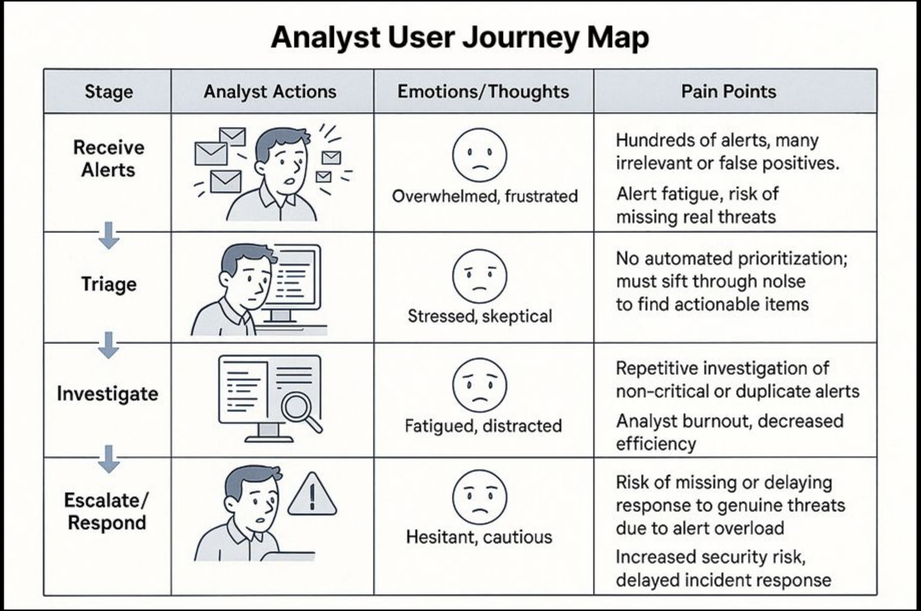
ChatGPT 4o *Prompt: A revised visual representation of data overload (e.g., a chaotic network diagram, a wall of text, a frustrated analyst). Adult Anime or full length Japanese animation movie style*

Problem:

- Data overload hinders threat identification.
- Complex tools slow investigations.
- Analysts need natural language queries.

Research & Insights

Understanding Analyst Needs: From Data to Decisions



Analyst User Journey Map

Stage	Analyst Actions	Emotions/Thoughts	Pain Points
Receive Alerts		Overwhelmed, frustrated	Hundreds of alerts, many irrelevant or false positives. Alert fatigue, risk of missing real threats
Triage		Stressed, skeptical	No automated prioritization; must sift through nolse to find actionable items
Investigate		Fatigued, distracted	Repetitive investigation of non-critical or duplicate alerts Analyst burnout, decreased efficiency
Escalate/ Respond		Hesitant, cautious	Risk of missing or delaying response to genuine threats due to alert overload Increased security risk, delayed incident response

Research & Insights:

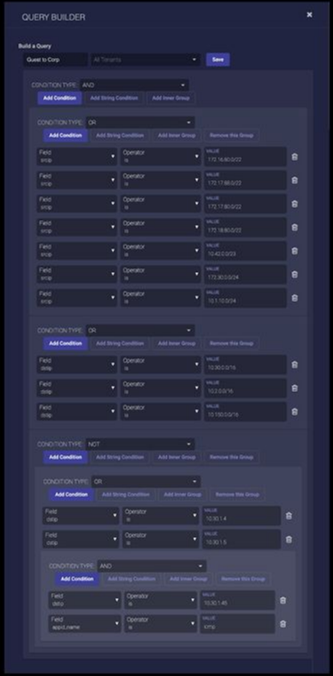
- Analysts spend too much time writing/ debugging queries.
- Visualizing data is crucial for fast pattern recognition.
- Seamless pivoting between data sets is essential.

Approach & Key Decisions

Empowering Analysts with Intuitive Tools

- Redesigned UI with a new name: Query Studio (formerly Queries and Filter Builder)
- Added optional Natural Language Query input
- Enhanced alert filters with automated score adjustments

OLD UI



QUERY BUILDER

Build a Query

Guest to Corp | All Tenants | Save

CONDITION TYPE: AND

CONDITION TYPE: OR

Field srcip | Operator is | VALUE 172.16.80.0/22
Field srcip | Operator is | VALUE 172.17.88.0/22
Field srcip | Operator is | VALUE 172.17.80.0/22
Field srcip | Operator is | VALUE 172.18.80.0/22
Field srcip | Operator is | VALUE 10.42.0.0/23
Field srcip | Operator is | VALUE 172.30.0.0/24
Field srcip | Operator is | VALUE 10.1.10.0/24

CONDITION TYPE: OR

Field dstip | Operator is | VALUE 10.30.0.0/16
Field dstip | Operator is | VALUE 10.2.0.0/16
Field dstip | Operator is | VALUE 10.150.0.0/16

CONDITION TYPE: NOT

CONDITION TYPE: OR

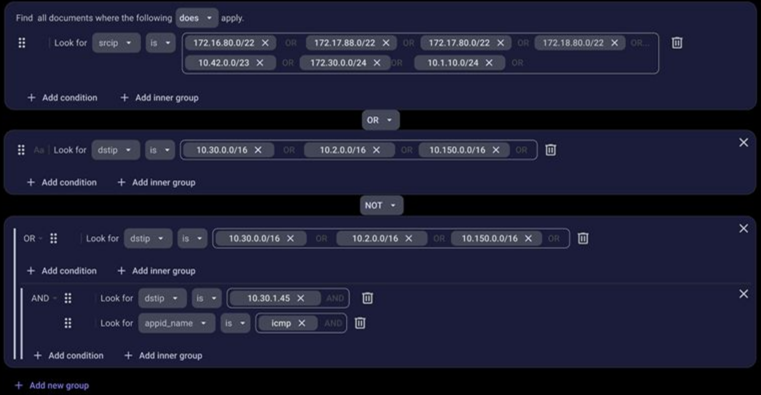
Field dstip | Operator is | VALUE 10.30.1.4
Field dstip | Operator is | VALUE 10.30.1.5

CONDITION TYPE: AND

Field dstip | Operator is | VALUE 10.30.1.45
Field appid_name | Operator is | VALUE icmp

→

NEW UI



Find all documents where the following does apply.

Look for srcip is 172.16.80.0/22 OR 172.17.88.0/22 OR 172.17.80.0/22 OR 172.18.80.0/22 OR... 10.42.0.0/23 OR 172.30.0.0/24 OR 10.1.10.0/24 OR

OR

Look for dstip is 10.30.0.0/16 OR 10.2.0.0/16 OR 10.150.0.0/16 OR

NOT

OR Look for dstip is 10.30.0.0/16 OR 10.2.0.0/16 OR 10.150.0.0/16 OR

AND Look for dstip is 10.30.1.45 AND

Look for appid_name is icmp AND

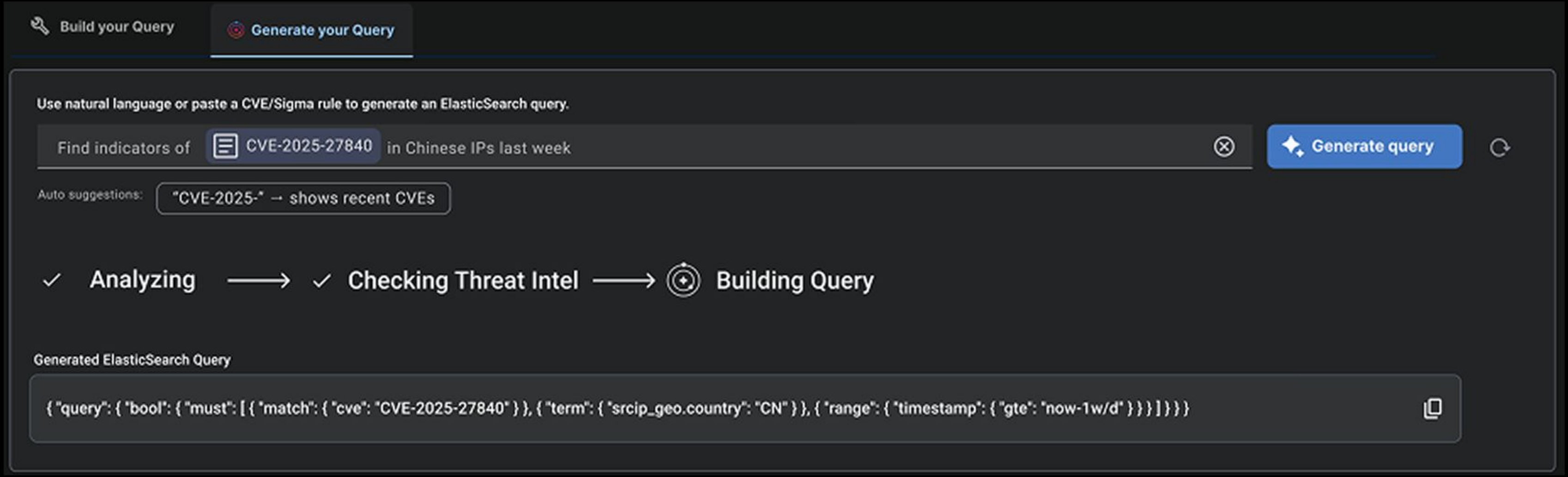
~~Query& Filter Builder~~

NEW! Query Studio

Solution: Natural Language to Queries

Making Queries Intuitive

Enable natural language search.



Use natural language or paste a CVE/Sigma rule to generate an ElasticSearch query.

Find indicators of CVE-2025-27840 in Chinese IPs last week

Auto suggestions: "CVE-2025-" → shows recent CVEs

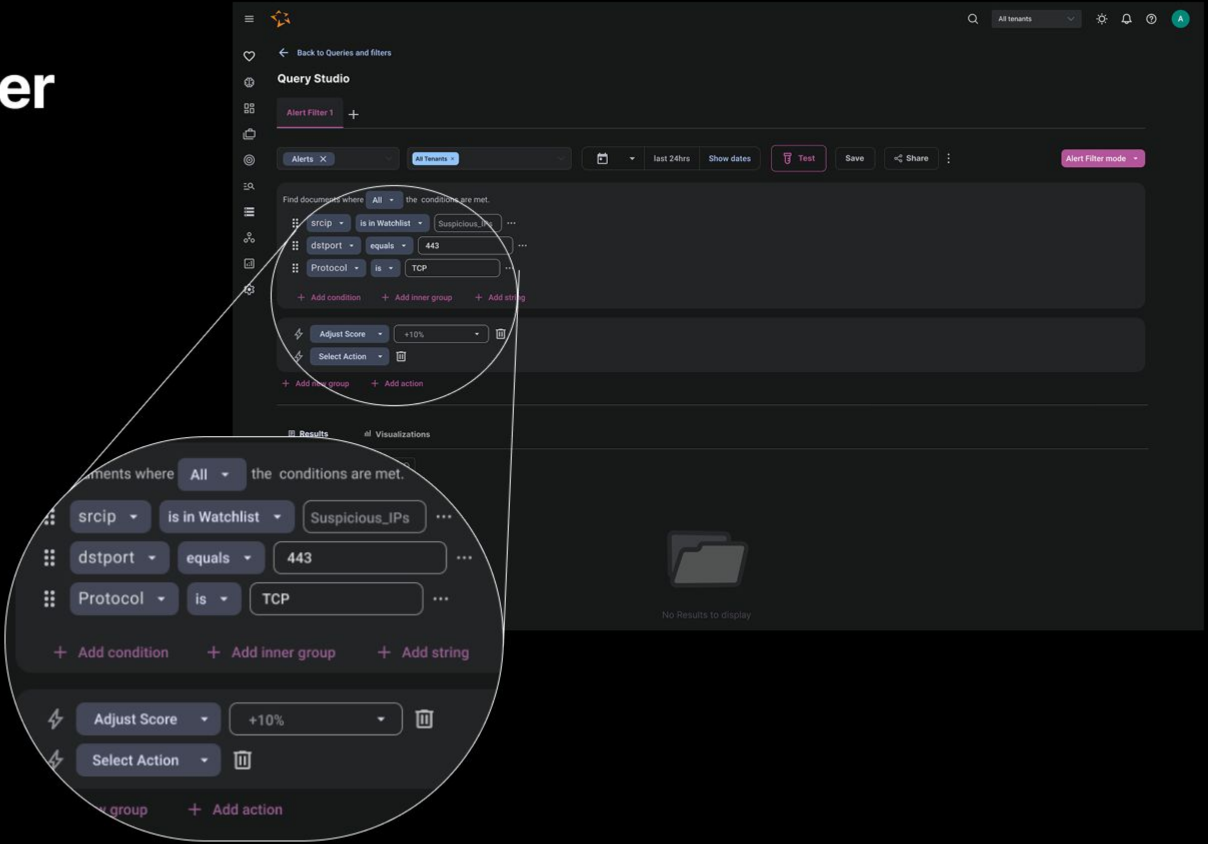
✓ Analyzing ⟶ ✓ Checking Threat Intel ⟶ Building Query

Generated ElasticSearch Query

```
{ "query": { "bool": { "must": [ { "match": { "cve": "CVE-2025-27840" } }, { "term": { "srcip_geo.country": "CN" } }, { "range": { "timestamp": { "gte": "now-1w/d" } } } ] } } }
```

Solution: Alert Filter Actions

Enhanced Alert Filter Actions



Query Studio

Find documents where All the conditions are met.

- srcip · is in Watchlist · Suspicious_IPs
- dstport · equals · 443
- Protocol · is · TCP

- Adjust Score · +10%
- Select Action

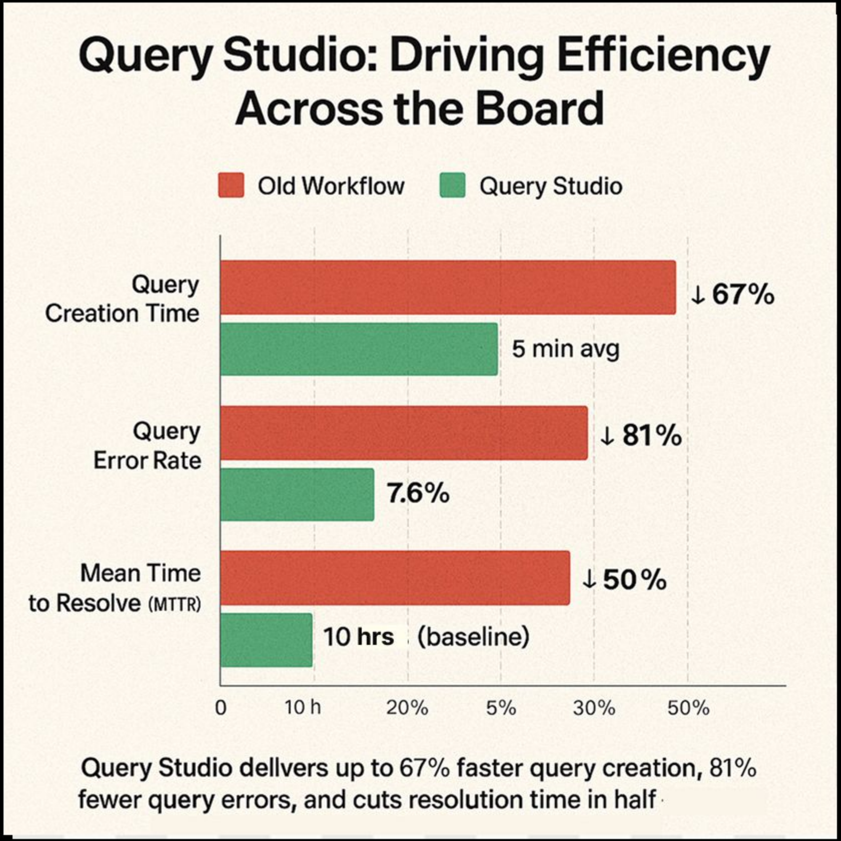
Streamlining Alert Management

- Automatically suppress irrelevant alerts.
- Reduce alert fatigue and focus on critical events.
- Showcase the workflow of creating and applying filters, including automating alert score adjustments.

Solution: Key Features

Key Features: Designed for Impact

The new UI transformed a complex, error-prone process into a streamlined, powerful, and accessible tool—enabling faster, more accurate threat detection and response. The redesign led to:



Query Studio: Driving Efficiency Across the Board

Query Studio dellvers up to 67% faster query creation, 81% fewer query errors, and cuts resolution time in half

Lessons Learned and Future Iterations

Lessons Learned: Continuous Improvement

Key lessons:

- The power of natural language in complex domains.
- The importance of balancing power with usability.
- The importance of effective alert management, including flexible alert scoring.

Future Iterations:

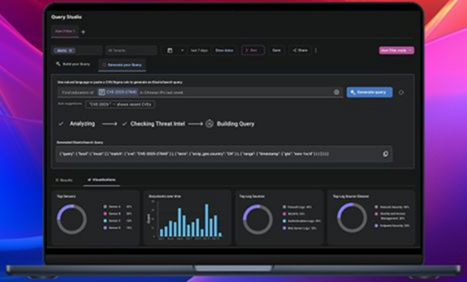
- Deeper AI integration to automate more tasks.
- More contextual, guided investigation workflows.

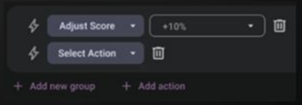
~~Query& Filter Builder~~

NEW!

Query Studio

AI Query Authoring





Alert Filter Actions

Threat Hunting Visualizations