Advanced Features and Customisations for Your Google Custom Search Engine (3 of 5)

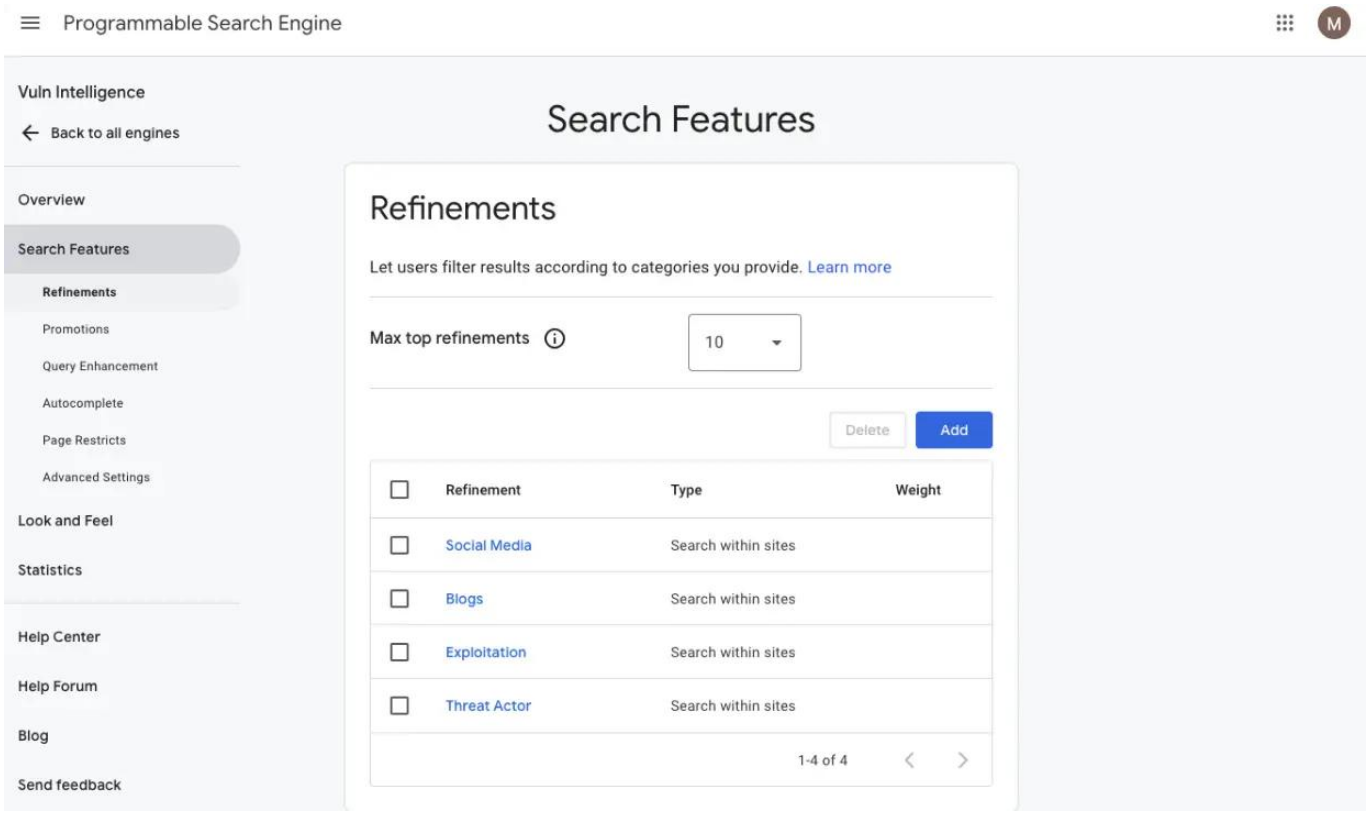


By Mario Rojas, Senior Security Researcher

Creating and Configuring Your Google Custom Search Engine
So far in this series, we've covered the basics of creating and configuring a Google Custom Search Engine (CSE) tailored to your open-source intelligence (OSINT) and threat intelligence needs. Now, it is time to explore advanced features and customisations that will help fine-tune your CSE.
These enhancements will improve search relevance, streamline research, and integrate your CSE seamlessly into your workflows.

Step 1: Leveraging Refinements for Focused Searches

Refinements in Google Custom Search Engine (CSE) allow you to create predefined filters that guide users to specific categories or sections within the search results. When you set up refinements, they appear as clickable tabs or sections above the search results, enabling users to quickly toggle between different areas of focus. This organisation not only improves the relevance of search results but also gives users an at-a-glance view of specialised data.



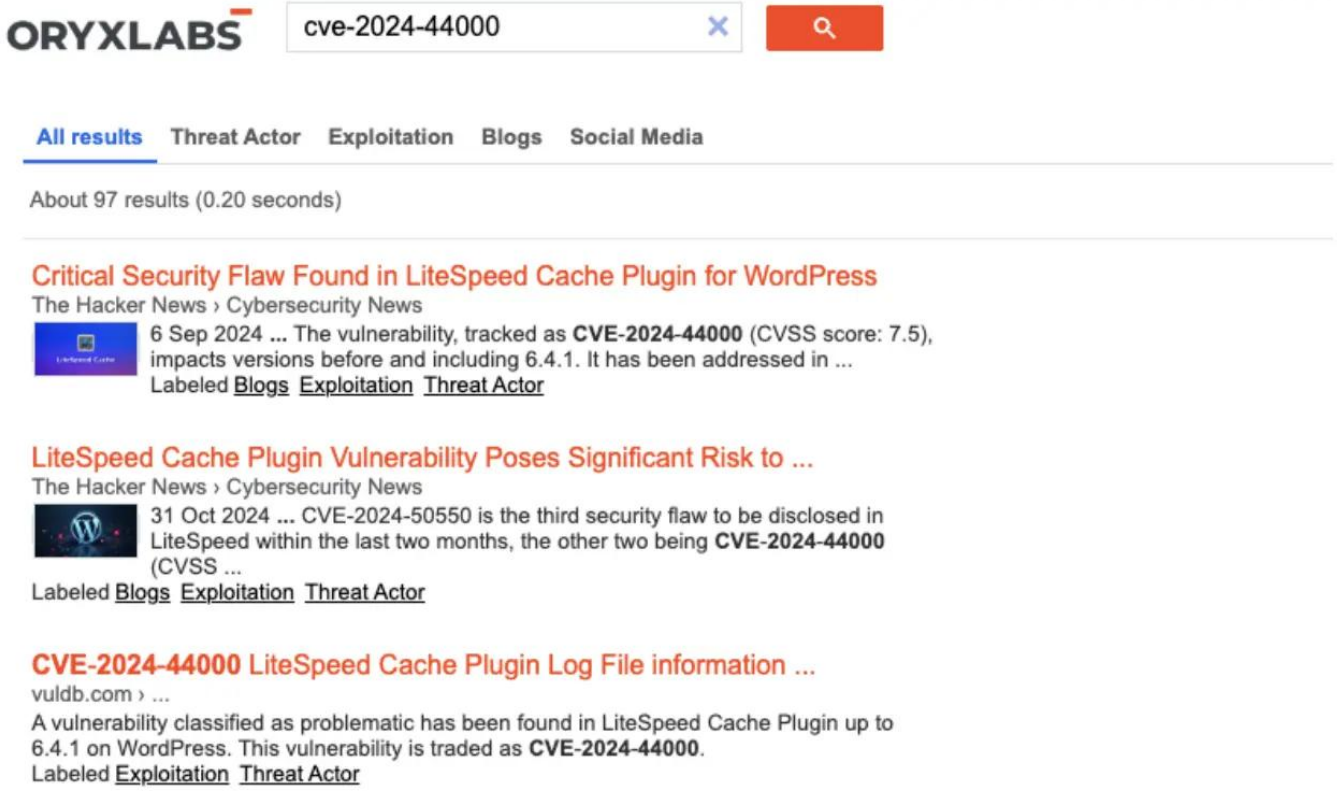
Create a refinement:

- From the list of search engines, select the search engine you want to edit.
- Under Overview, scroll down and click on Search features.
- Under the Refinements section. Click Add.
- Enter a name for the refinement and choose either "search within sites with this refinement" or "change priority of sites with this refinement".
- Select the sites you want to be included during the search.
- (Optional) You can further narrow down the search results by adding optional words which will be added to the user's query when they search within the label by clicking on Advanced.
- Click Save.

Here are some examples

Refinement	Site	Keywords
Blogs	www.thehackernews.com www.securityweek.com www.helpnetsecurity.com www.darkreading.com	
Exploitation	www.krebsonsecurity.com otx.alienvault.com www.thehackernews.com www.securityweek.com www.helpnetsecurity.com www.darkreading.com www.reddit.com/r/cybersecurity/ www.reddit.com/r/netsec/ x.com	Exploited
Social Media	www.reddit.com/r/cybersecurity/ www.reddit.com/r/netsec/ x.com	
Threat Actor	www.krebsonsecurity.com otx.alienvault.com www.thehackernews.com www.securityweek.com www.helpnetsecurity.com www.darkreading.com www.reddit.com/r/cybersecurity/ www.reddit.com/r/netsec/ x.com	gang actor

We can quickly test the new refinements by searching for something like “CVE-2024-44000”. Here you should get new tabs for each one of the refinements.

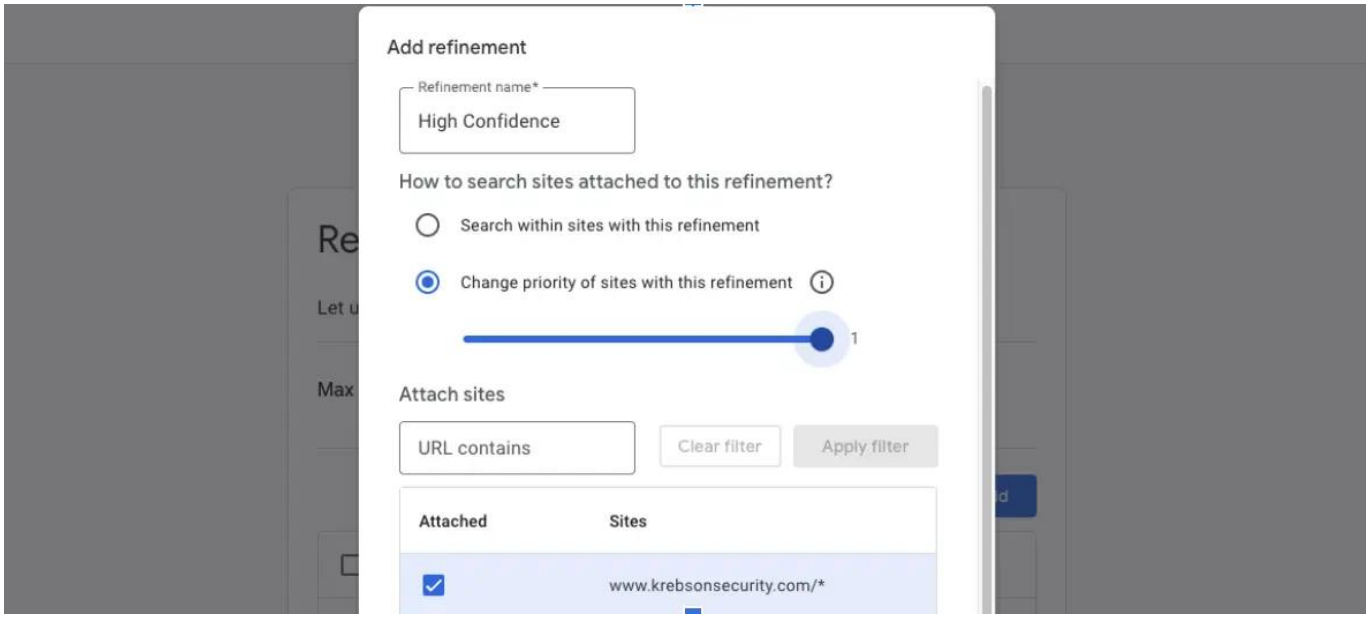


This structured approach enhances usability by allowing users to stay within their specific research context without re-entering search terms or manually sifting through irrelevant results. It also gives you flexibility in tailoring the CSE to cover multiple research needs within a single search interface.

Step 2: Adding Context with Labels

Labels can highlight or de-emphasise certain websites or domains within your search. This can be done by assigning labels like "High Confidence" or "Medium Relevance" to control the weight of specific sources in results.

In Figure 3 (above), you may have noticed that each result contains labels at the bottom that match names found in our refinements. We can create new refinements and use the “Change priority of sites with this refinement” to assign different weights (0-1) to specific sites.



These new labels will help analysts access the most valuable information first, minimising the time spent sorting through lower-quality sources.

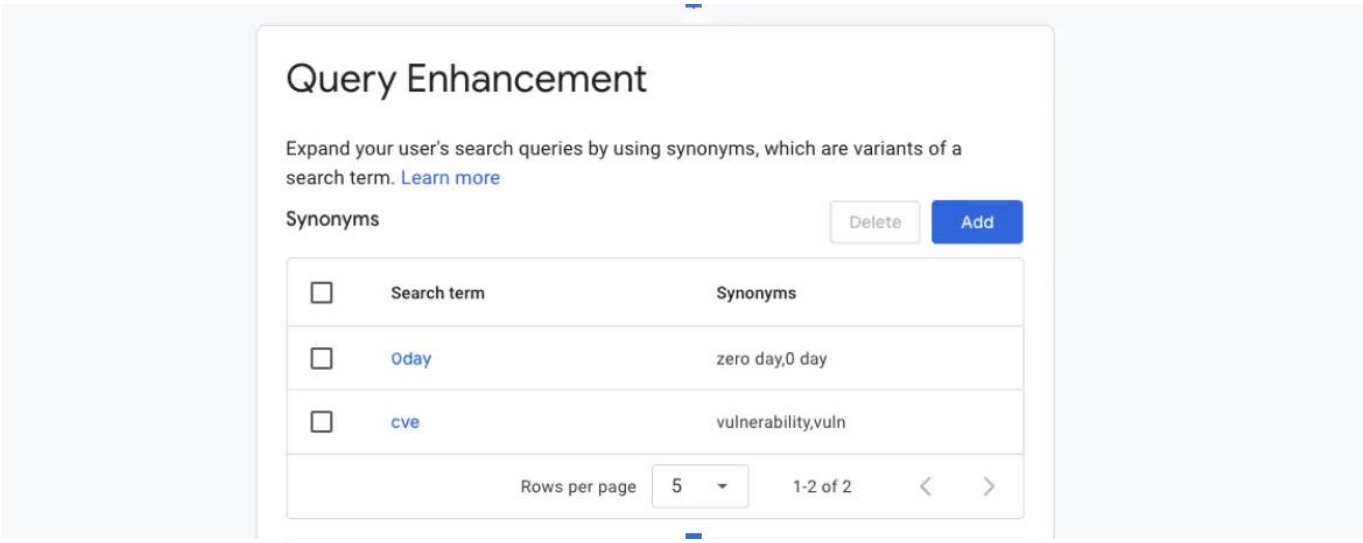
Step 3: Enhancing Searches with Synonyms and Query Additions

Query enhancements allow you to make your Google Custom Search Engine (CSE) smarter by defining synonyms and adding query parameters to improve the search experience. These features help users find what they’re looking for more effectively, especially when dealing with industry-specific terminology or preferences for search result presentation.

Synonyms for Consistent Results
Synonyms enable your CSE to interpret different terms as equivalent, ensuring relevant results are returned no matter which variation is used. For example:

- Define "CVE" and "vuln" as synonyms so searches for either term yield similar results.
- Map "0 day" and "zero day" together to account for stylistic variations in how vulnerabilities are referenced.

Adding synonyms is particularly useful in OSINT research, where standard and shorthand terms are often used interchangeably. To set them up, navigate to the Search Features > Query Enhancement section of your CSE dashboard, and add your synonym mappings under the Synonyms tab.



Query Additions for Customised Searches
Query additions allow you to append specific parameters to every user query, tailoring the results to match your needs automatically. For instance,

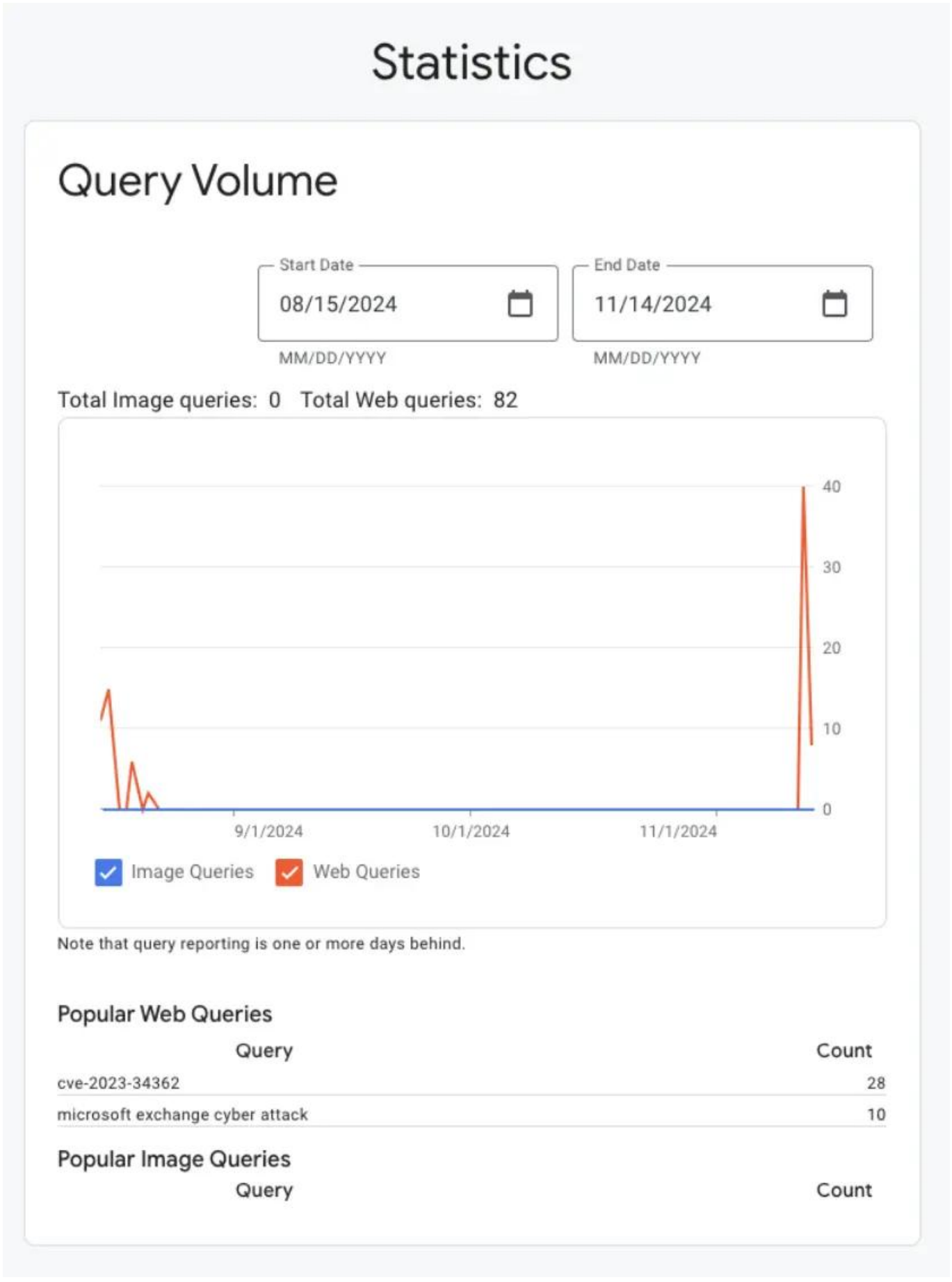
- Append the parameter num=100 to display 100 results per page instead of the default 10, reducing the need for pagination during research.

To configure query additions, go to the Search Features section and use the Query Additions tab

Step 4: Monitoring and Analysing Usage with the CSE Dashboard

The CSE dashboard offers analytics to understand user behaviour, making it easier to adjust your CSE to better serve its purpose.

- Using Analytics for Insights: View metrics like search term popularity, click-through rates, and top-performing sources. This can reveal trends in user behaviour, helping you refine your search parameters.
- Refining Based on Data: Use these insights to adjust labels, refine site inclusions, or even add/remove domains.
- Example for Threat Intel Teams: If certain searches are frequent, you may consider adding new sites or refining existing ones to match emerging OSINT needs.



Step 5: Managing Multiple CSEs for Diverse Research Needs

Creating multiple Google Custom Search Engines (CSEs) is a practical strategy when you

need to address a wide range of research topics. By segmenting your search needs into separate CSEs, you can maintain clarity, optimise search performance, and simplify workflows for yourself or your team.

Benefits of Multiple CSEs

Managing varied research requirements can become overwhelming when everything is crammed into a single CSE. By creating dedicated CSEs for specific areas, you gain:

- Better Focus: Each CSE targets a distinct area of research, eliminating the noise that comes from irrelevant sources.
- Improved Usability: Users don’t need to toggle between refinements or filters, they can simply access the right CSE for the task.
- Custom Features: Each CSE can have its own set of refinements, synonyms, and query additions tailored to its unique focus.

For example, an OSINT practitioner might create separate CSEs for:

- Phishing Domains: Focused on identifying malicious domains, phishing kits, and related indicators of compromise.
- Ransomware Research: Tracking ransomware families, ransom demands, and attack techniques across blogs and security feeds.
- Threat Actor Profiles: Aggregating profiles, tools, and techniques associated with known threat groups.

Tips for Organisation

Managing multiple CSEs requires a systematic approach to ensure ease of use and accessibility:

- Naming Conventions: Use descriptive and consistent names like “OSINT –Ransomware” or “OSINT – Threat Actors” to make it clear what each CSE is for.
- Documentation: Maintain a central document or dashboard listing all your CSEs, their purposes, and direct links to access them. This can be shared with your team for collaboration.
- Review and Maintenance: Regularly review each CSE to update sources and refine parameters as research needs evolve.

Example Scenarios

Let’s say you’re researching vulnerabilities and exploits:

- Ransomware Research CSE: Includes domains like bleepingcomputer.com and kaspersky.com/blog to track emerging ransomware campaigns and their indicators of compromise.
- Threat Actor CSE: Focuses on sources like darkreading.com and securityweek.com, combined with keywords such as "APT" or "gang," to retrieve detailed profiles and activity reports.

By separating these areas into different CSEs, you can work more efficiently, reduce irrelevant results, and streamline research for both you and your team.

Conclusion

With these advanced features and strategies, your Google Custom Search Engine becomes a powerful and flexible tool tailored to your OSINT and threat intelligence workflows. Refinements and query enhancements ensure precision, while features like synonyms, labels, and query additions save time and provide deeper customisation. By creating multiple specialised CSEs, you can tackle diverse research needs without cluttering your searches.

As you continue to refine and adapt your CSEs, you'll discover new ways to optimise your workflow and uncover actionable insights faster. In the next post, we'll dive into using the Google CSE API to programmatically retrieve results and integrate them into your automated threat intelligence processes.