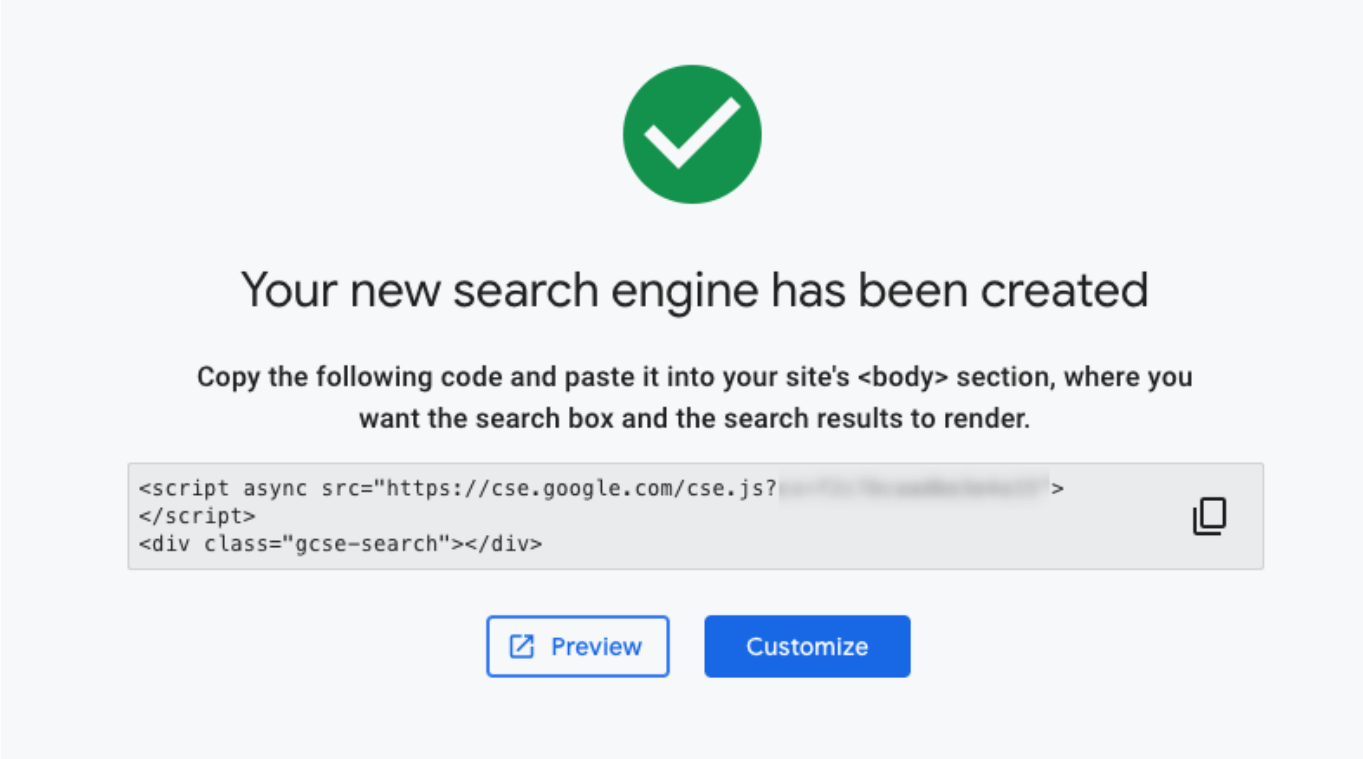
The OSINT Workshop (1 of 5)



By Mario Rojas, Senior Security Researcher

Effective threat intelligence is all about staying one step ahead of potential threats. By leveraging the right tools, organisations can proactively identify and mitigate cyber risks before they become critical issues.



Welcome to The OSINT (Open-Source Intelligence) Workshop, where we will be delving into the art and science of building custom search engines tailored for OSINT. Much like skilled craftsmen in a workshop, participants will learn to design and refine tools that enhance your threat intelligence capabilities.

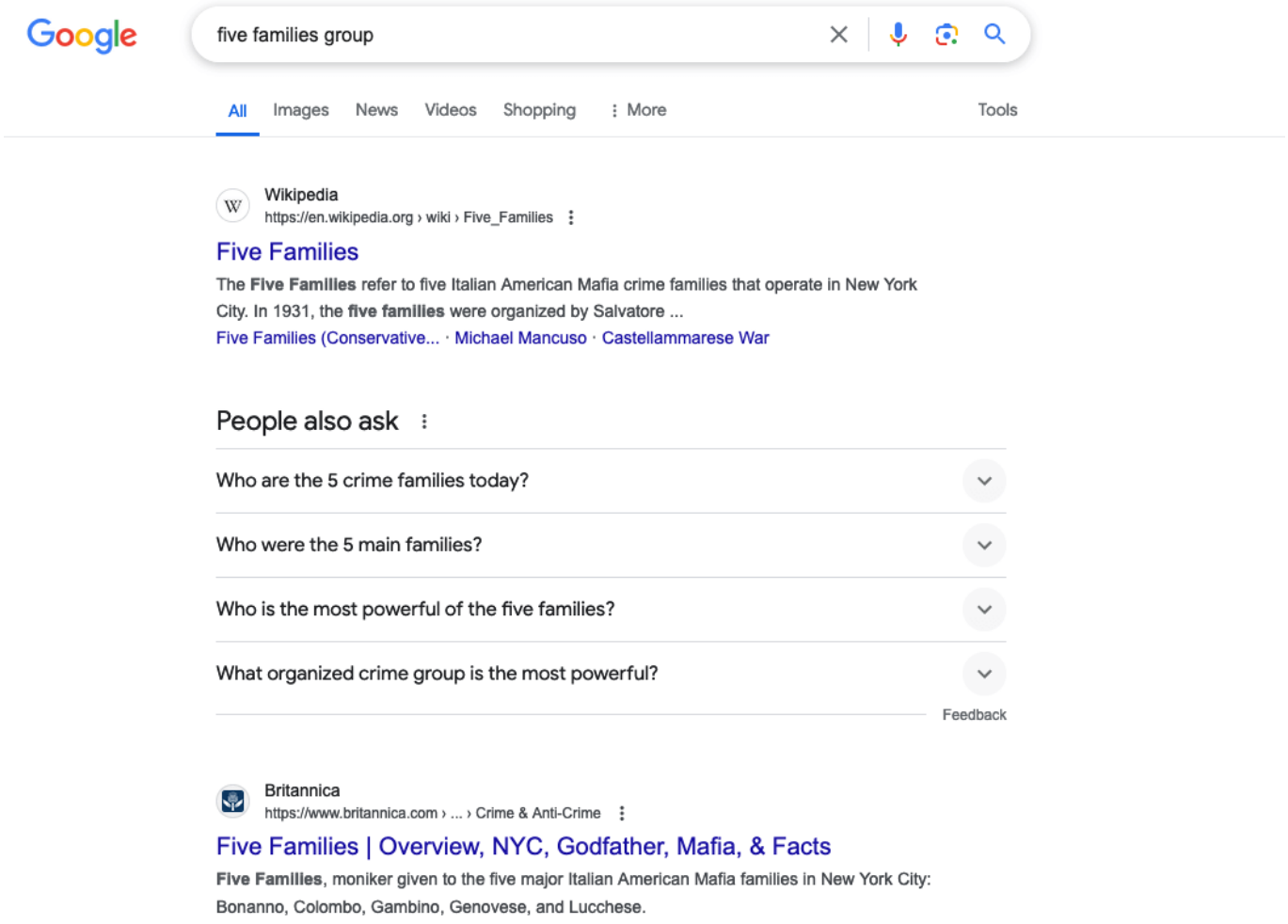
Join us as we guide you through each step of creating powerful custom search engines to boost your OSINT proficiency.

What is a Google Custom Search Engine?

A powerful yet often overlooked tool is the Google Custom Search Engine (CSE). A CSE allows you to refine or pre-filter Google search results to specific sites or types of results, making it easier for organisations to gather Open-Source Intelligence (OSINT) from various web sources while eliminating irrelevant results. This targeted approach provides enhanced control over search outcomes, which is essential for specialised fields such as threat intelligence.

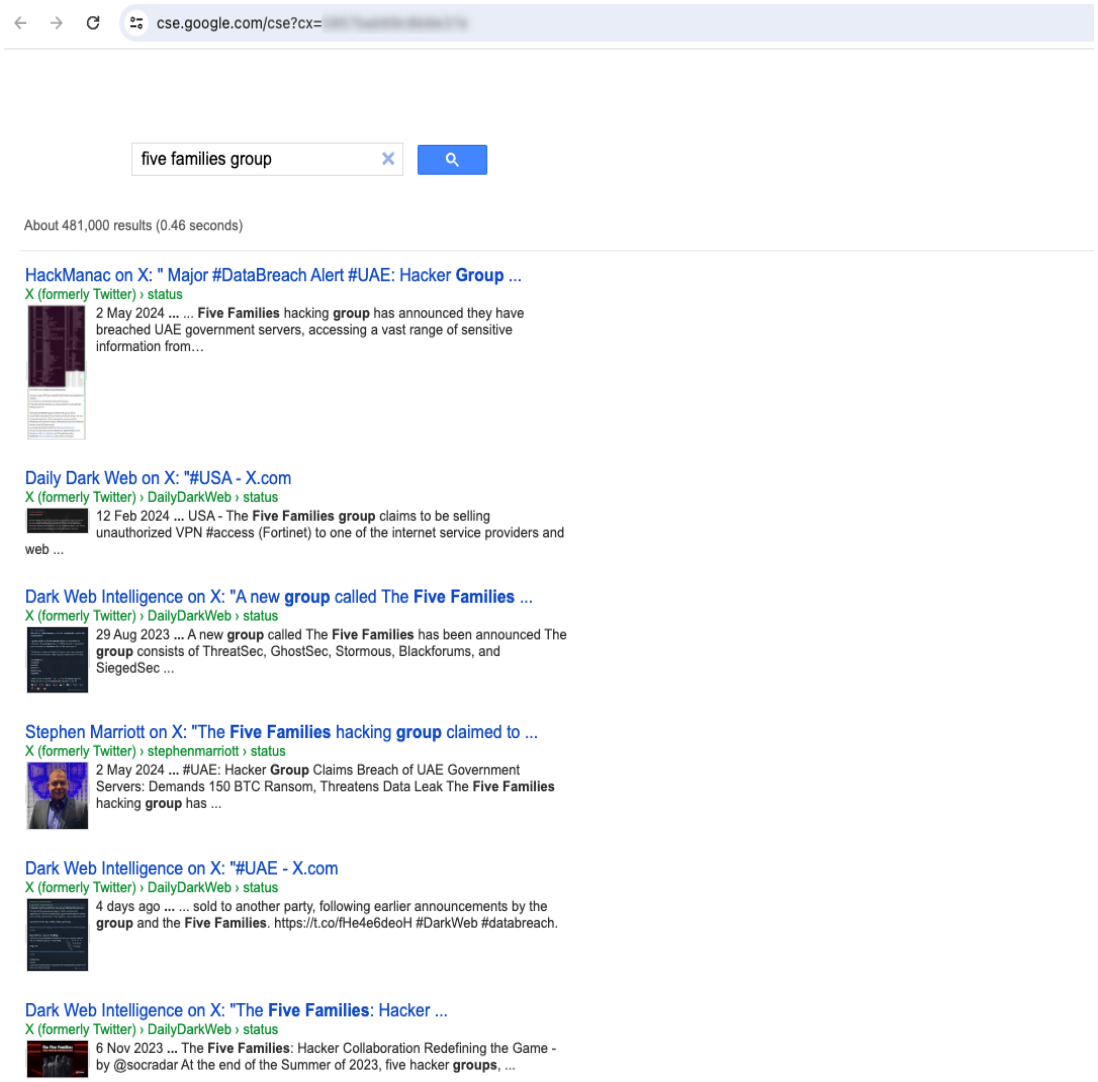
For instance, conducting a test search for the infamous ’Five Families’ hacker group, known for its recent large-scale ransomware attacks against various UAE organisations, reveals the effectiveness of a CSE.

Using a standard Google search for the ’Five Families’ group returns no relevant results, as illustrated in the image below.



In contrast, a CSE tailored to relevant websites and pages yields highly applicable results, therefore demonstrating improved relevance and accuracy.

This adjusted outcome is significantly more actionable for a threat intelligence analyst – as shown in the following image.



Why Use Google CSE for OSINT?

Understanding the tactical advantages of Google CSE can significantly enhance your security operations in environments where precise information-gathering makes a significant difference, such as in our previous example.

Here’s how it can fit into your strategy for gathering intelligence:

- **Targeted Information Gathering**: Customise searches to focus on specific sectors, geographies, or types of information relevant to your security needs.
- **Reduced Noise in Search Results**: By narrowing the scope of your searches, you filter out irrelevant information, making it faster and easier to find what you need.
- **Integration Capabilities**: Easily integrate with other tools and systems for enhanced data analysis and utilisation.

Pros of Using Google CSE

Google CSE provides several benefits when used appropriately within a comprehensive threat intelligence framework. Let’s examine these benefits:

- **Customisation**: Tailor search engines to target the exact sources of information you

need.
- **Cost-Effective**: Depending on the scale, Google CSE can be a cost-effective solution compared to other commercial search tools.
- **User Experience**: Improve the search experience for users by providing more relevant results, which is key when time and accuracy are critical.

Cons of Using Google CSE

It's also important to be aware of the potential challenges when integrating new tools into your operations. Here are some considerations for Google CSE:

- **Setup Complexity**: Initially, setting up and customising your CSE can be complex, requiring a good understanding of search parameters and configurations. Our upcoming guides will help simplify this process.
- **Query Limits**: Be mindful of the daily query limits in the free tier; exceeding these could incur costs.
- **Maintenance**: Continuous adjustments are necessary to ensure the search engine remains effective as the digital landscape evolves.

Conclusion

The potential use of Google CSE for OSINT purposes in corporate security settings should form part of a calculated and carefully thought-out decision process, requiring a thorough understanding of both its strengths and limitations.

Our next blog posts will provide detailed steps and best practices for setting up and maintaining a Google CSE tailored to your needs.