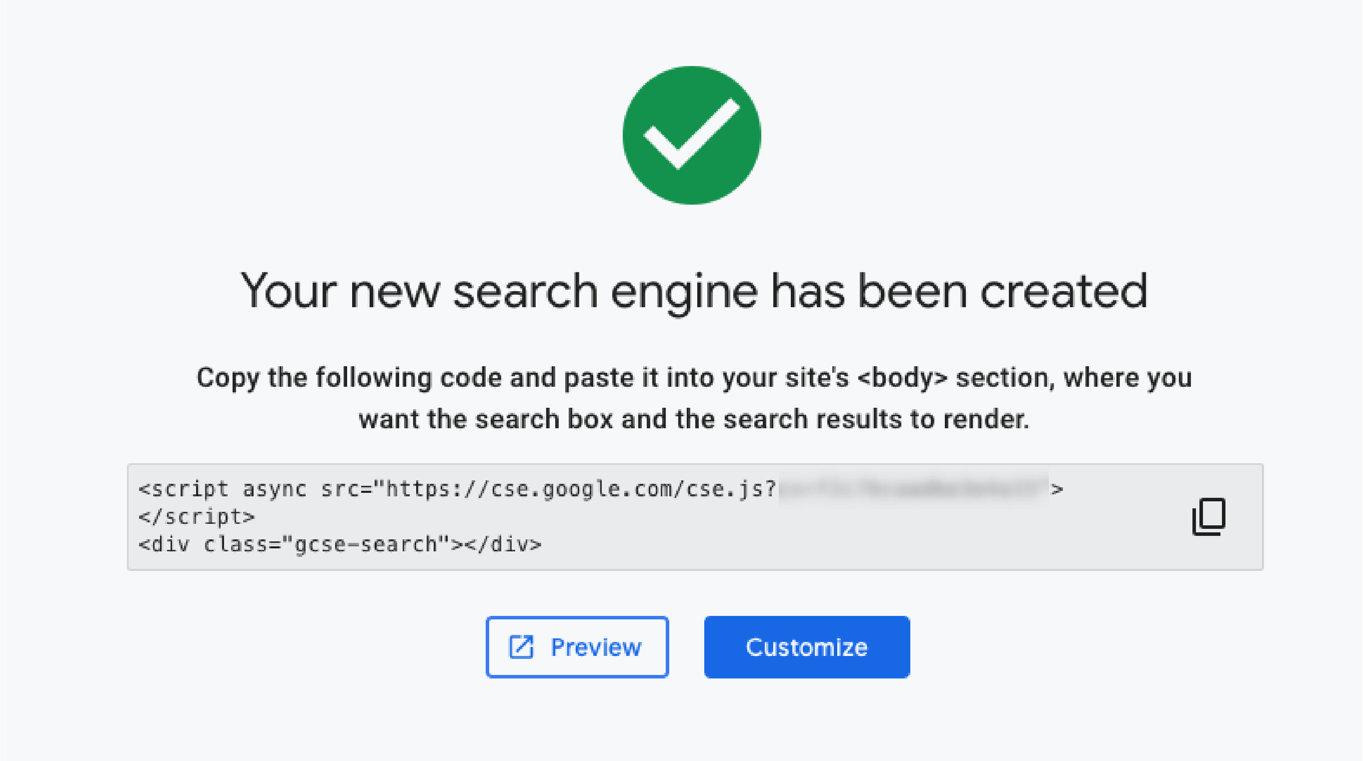
(The OSINT Workshop (1 of 5

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



Your new search engine has been created

Copy the following code and paste it into your site's <body> section, where you want the search box and the search results to render.

```
<script async src="https://cse.google.com/cse.js?[redacted]">
</script>
<div class="gcse-search"></div>
```

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

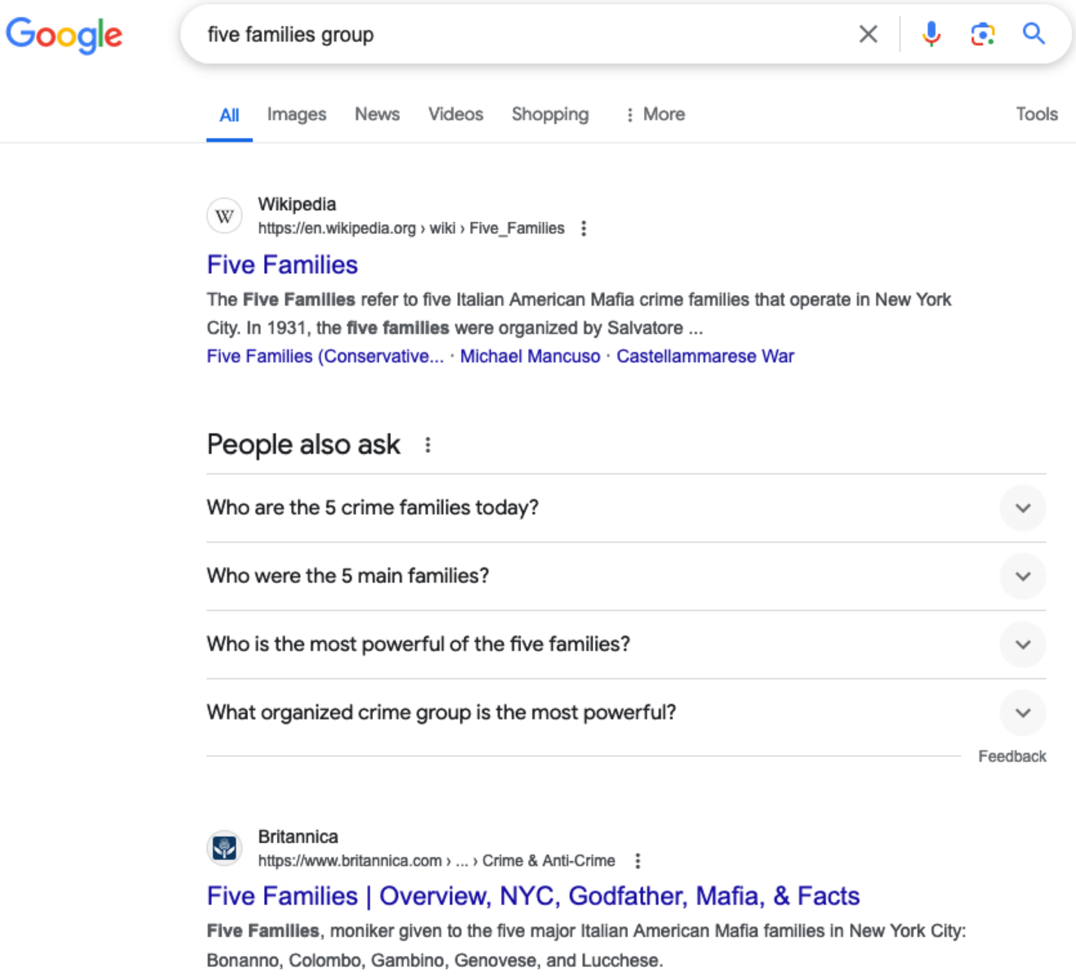
Join us as we guide you through each step of creating powerful custom search engines to .boost your OSINT proficiency

?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



Wikipedia
https://en.wikipedia.org › wiki › Five_Families

Five Families

The **Five Families** refer to five Italian American Mafia crime families that operate in New York City. In 1931, the **five families** were organized by Salvatore ...

Five Families (Conservative... · Michael Mancuso · Castellammarese War

People also ask

Who are the 5 crime families today?

Who were the 5 main families?

Who is the most powerful of the five families?

What organized crime group is the most powerful?

Feedback

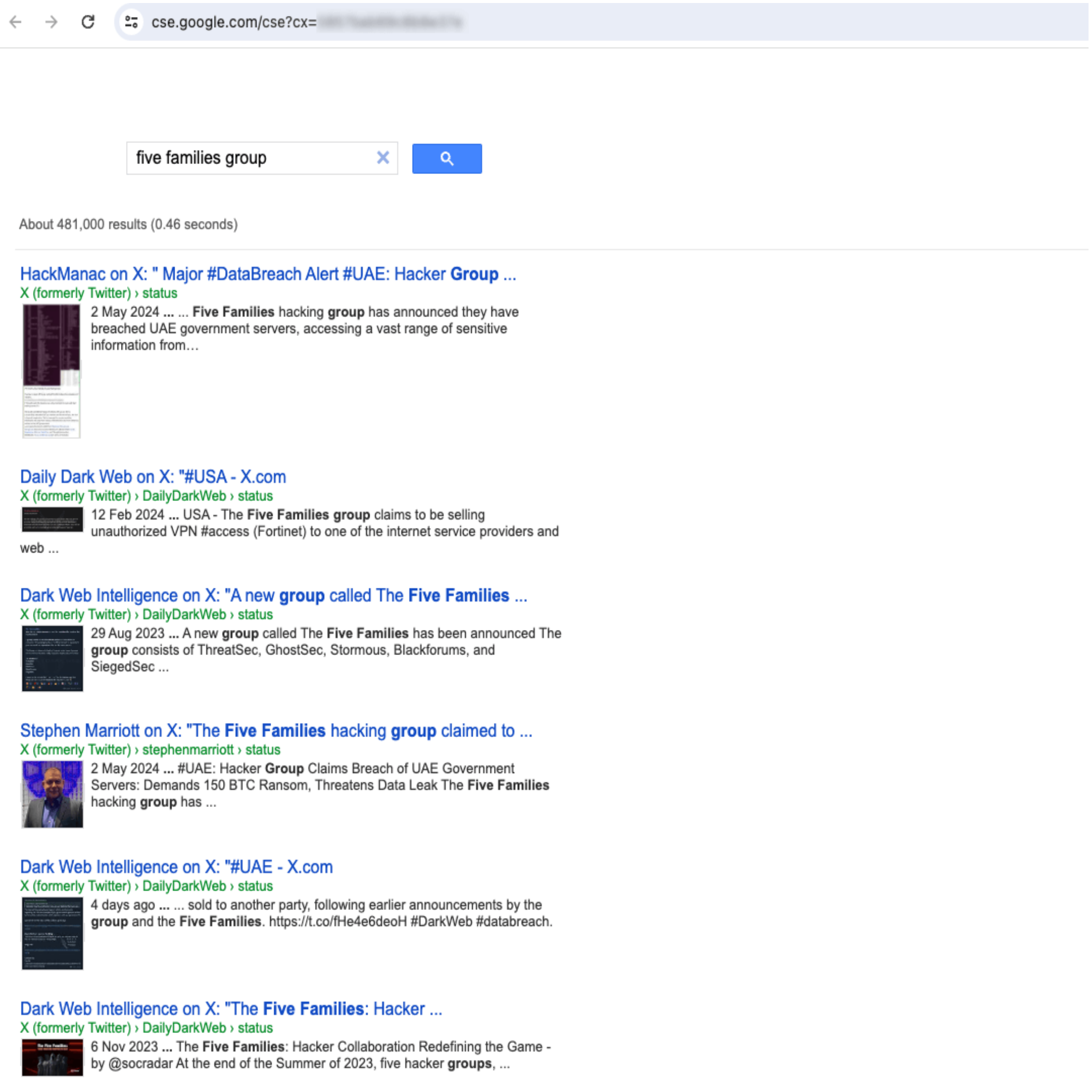
Britannica
https://www.britannica.com › ... › Crime & Anti-Crime

Five Families | Overview, NYC, Godfather, Mafia, & Facts

Five Families, moniker given to the five major Italian American Mafia families in New York City: Bonanno, Colombo, Gambino, Genovese, and Lucchese.

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



cse.google.com/cse?cx=[redacted]

five families group

About 481,000 results (0.46 seconds)

HackManac on X: " Major #DataBreach Alert #UAE: Hacker **Group** ...
X (formerly Twitter) › status
2 May 2024 **...** ... **Five Families** hacking **group** has announced they have breached UAE government servers, accessing a vast range of sensitive information from…

Daily Dark Web on X: "#USA - X.com
X (formerly Twitter) › DailyDarkWeb › status
12 Feb 2024 **...** USA - The **Five Families group** claims to be selling unauthorized VPN #access (Fortinet) to one of the internet service providers and web ...

Dark Web Intelligence on X: "A new **group** called The **Five Families** ...
X (formerly Twitter) › DailyDarkWeb › status
29 Aug 2023 **...** A new **group** called The **Five Families** has been announced The **group** consists of ThreatSec, GhostSec, Stormous, Blackforums, and SiegedSec ...

Stephen Marriott on X: "The **Five Families** hacking **group** claimed to ...
X (formerly Twitter) › stephenmarriott › status
2 May 2024 **...** #UAE: Hacker **Group** Claims Breach of UAE Government Servers: Demands 150 BTC Ransom, Threatens Data Leak The **Five Families** hacking **group** has ...

Dark Web Intelligence on X: "#UAE - X.com
X (formerly Twitter) › DailyDarkWeb › status
4 days ago **...** ... sold to another party, following earlier announcements by the **group** and the **Five Families**. https://t.co/fHe4e6deoH #DarkWeb #databreach.

Dark Web Intelligence on X: "The **Five Families**: Hacker ...
X (formerly Twitter) › DailyDarkWeb › status
6 Nov 2023 **...** The **Five Families**: Hacker Collaboration Redefining the Game - by @socradar At the end of the Summer of 2023, five hacker **groups**, ...

?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