



# Unleash the Power of Censys Search

A Hassle-Free Handbook  
for Cyber Heroes



# Table of Contents



## Introduction

3



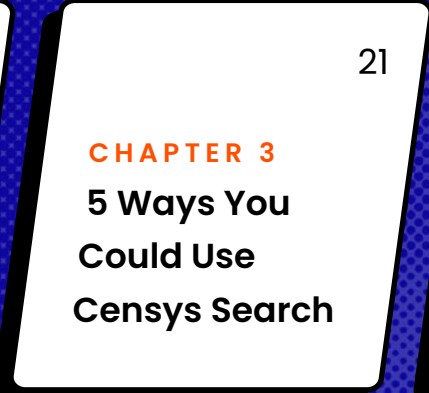
## **CHAPTER 1** The One Place to Understand *Everything* on the Internet

5



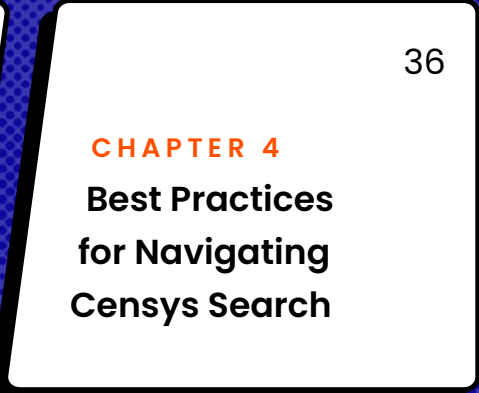
## **CHAPTER 2** Getting Started: Crafting Effective Queries

10



## **CHAPTER 3** 5 Ways You Could Use Censys Search

21



## **CHAPTER 4** Best Practices for Navigating Censys Search

36



## **CHAPTER 5** Other Capabilities You Should Know About

45



## **CHAPTER 6** Starting Your Censys Search Journey

54

# Welcome! We're So Glad You're Here.

Welcome to ***Unleash the Power of Censys Search***, your hassle-free handbook for mastering the powerful internet intelligence tool that is Censys Search.

As the global internet landscape has continuously evolved, so, too, has the complexity of cyber threats that organizations face. Attacks have become more frequent, adversaries, more sophisticated, and the consequences of a successful breach, more complicated.

Defenders on the frontlines of this harrowing threat landscape – the do-gooders who fight to protect their organization from attacks day in and day out – have been increasingly challenged to keep up.

What makes Censys Search the perfect sidekick for these cyber heroes? In short, it provides an unmatched

view of the global threat landscape. Powered by a proprietary dataset of internet intelligence, Censys Search offers access to data that's superior in coverage, context, accuracy, and freshness. This superiority is why Fortune 500 enterprises, international governments, and researchers from around the world use Censys Search to proactively identify threats, investigate IOCs, defend against known adversaries, monitor for exploits, track trends and behaviors, and so much more.

This unrivaled view is also why we say that Censys is the one place to understand everything on the internet.

Whether you're brand new to Censys Search or a current user, this handbook is designed to provide you with the instruction and insight you need to effortlessly make the most of Censys Search!

**Censys Search is the source of truth cyber heroes can rely on to gain an upper hand.**

## Throughout the handbook, we'll walk you through:

- **What Censys Search Is:** Get an introduction to the search-based platform from which users can access our proprietary internet intelligence.
- **How to Get Started in Censys Search:** Find step-by-step instructions on how to run queries in Censys Search and efficiently access the data you need.
- **Ways to Use Censys Search:** From tracking exposed assets and vulnerabilities in real-time to monitoring third-party risk, discover how Censys Search can be integrated into your cybersecurity strategy.
- **Best Practices:** Leverage the full potential of Censys Search with advanced querying capabilities and analytical tools that enable you to draw insightful conclusions and make informed decisions.

We hope you'll think of ***Unleash the Power of Censys Search*** as more than just a user manual, and instead, consider it your partner in navigating the complex world of internet security.

Let's get started!





## CHAPTER 1

# The One Place to Understand *Everything* on the Internet

TELL ME ABOUT CENSYS SEARCH

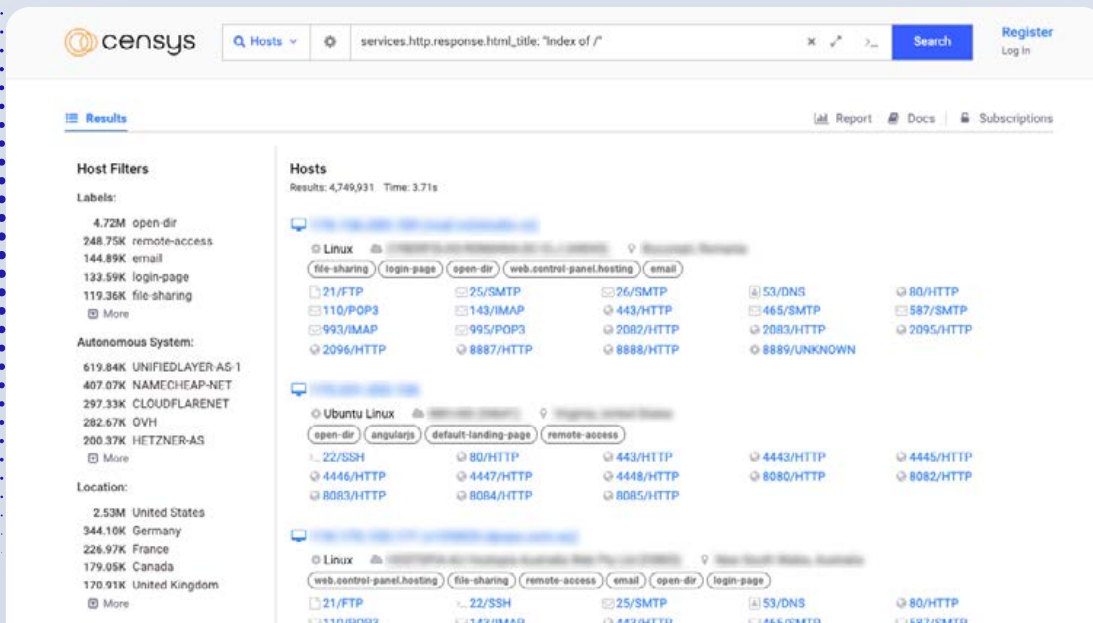
6

WHAT MAKES THIS DATA SO USEFUL?

7

WHY DO CYBER HEROES USE CENSYS SEARCH?

8



# Tell Me About Censys Search

Let's start with the basics and discuss Censys Search in its most fundamental terms. That means talking about the data that drives this powerful search engine.

Censys Search provides access to the most comprehensive, accurate, and up-to-date map of global internet infrastructure available. And we're not just talking in superlatives here for effect.

The proprietary dataset accessible within Censys Search is truly unmatched. Everything you might want to know about the structure of our public-facing internet – such as, how many hosts are

running in a specific province of China or how many TLS certificates associated with your organization or your vendors are expired – can be known from a query submitted to Censys Search.

Censys Search uses its proprietary scanning engine to scan the entire IPv4 and the majority of the IPv6 space for an unrivaled view of hosts and certificates, along with all of the hundreds of data points about software, services, and ASN, associated with each. You can learn more about how we passively scan the internet [here](#).



# What Makes This Data So Useful?

Unlike other sources of internet intelligence, Censys offers a deep, contextualized, attributed internet infrastructure map that supports multiple use cases. We don't just collect banners or detect service presence, we create a structured snapshot of every host and running service, down to the protocol level.

## Superior Coverage & Context

As a Censys Search user, you can tap into the most comprehensive and up-to-date visibility of hosts and services on the global internet. Censys:

- Provides multi-perspective scanning from 7 Tier-1 ISPs across 3 continents
- Identifies and scans websites by name, providing complete visibility into HTTP-based exposure and vulnerability
- **Is the *only* vendor conducting ML-based discovery of services across all 65k ports**
- Provides ~100 Deep Protocol Scanners and Automatic Protocol Detection to identify services running on unassigned ports
- Prioritizes cloud scanning to capture ephemeral cloud services
- Provides detailed visibility into open ports and running protocols, regardless of standard port assignment, to understand host intent **(we're the only vendor to do this)**
- Maintains the **world's largest x.509 certificate database** to identify related infrastructure and suspicious hosts
- Provides configuration and registration data to understand and determine ownership
- Includes device type labels to clearly identify host type (i.e. IoT, Database, VPN, etc.)

# Why Do Cyber Heroes Use Censys Search?

Censys Search operates as a user-friendly search engine, but it's so much more than that. It's an interactive, investigative tool with hundreds of filters and features that allow frontline defenders to refine results, pivot on findings, and dig into historical data. We have a dedicated chapter about different ways that you could use Censys Search (if you're ready to dive into those, head to Chapter 3). But let's talk broadly first.

**A security pro like yourself might use Censys Search because:**



## **You want to hunt for or investigate threats.**

Censys Search can be used to identify and gather credible evidence about cybersecurity threats. For example, a threat hunter could use Censys Search to proactively look for evidence of domain impersonation or suspicious IP addresses associated with their organization.



## **You want to understand if and how your organization is vulnerable.**

Let's say a zero-day has just hit and you need to know if your organization's assets could be affected. Or, you need to monitor when your TLS certificates expire. Censys Search can be used to help quickly identify and understand these vulnerabilities.



## **You want to observe activity and trends across the internet.**

In addition to enterprise security teams, security researchers also use Censys Search to track behavior across the internet. Historical data, location filters, and reports make it easy to look at activity in aggregate, while also maintaining the ability to drill down into assets. Our own research team frequently uses the tool to observe and report on the impact of new exploits.

For accomplishing these objectives and so many others, Censys Search has earned a reputation throughout the security community as a trusted source of reliable, accurate internet intelligence that's easy to access. Our growing [community](#) of hundreds of thousands of users is a testament to that trust!



A large, white, stylized quotation mark icon on a dark blue background.

**My favorite thing about Censys Search is its ability to provide a clear overview of my attack surface. It stands out from most internet scanners because it leverages numerous machine learning techniques, ensuring the data is refreshed daily. This is a significant advantage over other vendors, whose data can be outdated by weeks or even months. With Censys, I'm always informed about open ports and the software being used, thanks to its daily updates.**

**G2 Review from Verified Censys Search User,  
Non-Profit Management**



# Crafting Effective Search Queries

HOW TO WRITE A CENSYS SEARCH QUERY

12

YOUR QUERY STARTER PACK

17

EXPLORING ADVANCED QUERIES

18



**We've covered** what you can find in Censys Search – an unmatched dataset of global internet intelligence – now let's get into *how* to find it. This brings us to queries.

To access the data available in Censys Search, users run queries. Queries tell Censys Search what you're looking for. For example, your query might tell Censys Search to "show me all hosts with exposed RDP in Great Britain." When you submit a query, Censys Search evaluates every host or certificate in its dataset that matches your search, and returns that list to you in a results page. In this way, Search works much like other popular search engines you may be familiar with.

# How to Write a Censys Search Query

**Queries** are written in a specific syntax that's easy to learn, especially once you know the fundamentals. Rest assured that Censys Search has been used by thousands of individuals from across roles and industries who have picked up this syntax. You can, too! Let's walk through some essential query building blocks.

## Home Page View


Navigate to [search.censys.io](https://search.censys.io) and you'll be greeted with a simple **search toolbar**, as displayed below. Queries are entered into this toolbar. On the side, note that you can select "Hosts" or "Certificates." This tells Censys Search which **dataset** you'd like to query against. You can also use the **gear icon** to sort the order of results, adjust the number of results per page, and decide whether to include, exclude, or only view virtual hosts.






## Full Text Searches

One of the simplest queries to run is a **full-text search**. This is a query that doesn't specify a field and which searches across all text-based fields for the word or phrase submitted.


Example	Query
Query for hosts with any field that contains the term "hello"	hello 


You can search for a **multiple-word phrase** by surrounding it in **double quotes**.

Example	Query
Query for hosts with any field that contains the phrase "Hello World"	"hello world" 

## Field and Value Searches

You can also search **structured fields** for a **value** that's stored there. Fields reflect the nested structure of the host schema using dot notation to separate keys. Fields include host fields, identification and observation fields, service-name-specific fields, TLS fields and software fields.


Example	Query
Find all devices with a software product with the word "Windows" in it	services.software.product: Windows 


 **IMPORTANT:** If you want to search for an exact match (such as only the word "Windows" and nothing more), replace the colon between the field name and value with an equals sign (=).

## Wildcard Searches

**Wildcard symbols** are helpful for finding records where you know some part of a value, but not all.


Use the **asterisk symbol (\*)** to substitute zero or more unknown characters. Use the **question mark (?)** to substitute for exactly 1 unknown character.

Example	Query
<p>A query that specifies a value of "email" does not return records where the value is "e-mail," because it matches on tokenized words.</p> <p>In this instance, you can search for variations of email using the * wildcard</p>	<pre>services.http.response.headers: (key: server and value: e*mail) </pre>

 **NOTE:** Search does not support leading wildcard searches, for example, \*windows.


## Boolean Logic Searches


Who doesn't love a little **Boolean logic**? Censys allows the binary operators 'and', 'or', and 'not', as well as parentheses, to combine search criteria.

Type	Example	Query
OR	Return all hosts located either in the United States or Canada	<pre>location.country: Canada or location. country: "United States" </pre>




## Boolean Logic Searches (Continued)

Type	Example	Query
AND	Return hosts with port 443 open (with any service type) and an HTTP service (on any port)	<code>services.port: 443 and services.service_name: HTTP</code> 

 **IMPORTANT:** The search criteria applies to a host or certificate as a whole, unless specified. This query returns hosts with any service on port 443 and HTTP on any port.


## Nested Searches

You can use **nested query syntax** to apply multiple search criteria to a single object within a list of like objects, instead of to the entity as a whole. If you want certain criteria to all be true of a single service on a host, nest field/value pairs inside parentheses following the services field name.

Example	Query
Return hosts that are running an HTTP service on port 8888	<code>services: (port: 8888 and service_name: HTTP)</code> 

## Quotes

**Double quotes (")** search for a phrase instead of a single word. You can wrap whitespace-separated words in double quotes when searching for the phrase to be evaluated as a whole. Searches that specify a phrase for a field value are invalid without the double quotes.

Example	Query
Search for hosts and virtual hosts with an HTML title	<code>services.http.response.html_title:"your dashboard"</code> 

## Continue Learning



Head over to our Support site for more Censys Search query fundamentals!





# Your Query Starter Pack

Now that we have some query syntax ground rules covered, we can jump into some of the most frequently used Censys Search queries. These are foundational queries that can help you investigate common areas of interest faster.



## Services

Use Case	Query
I want to search for a service by service name.	<code>services.service_name:HTTP</code> 
I want to search for a service by port.	<code>services.port: 1337</code> 

## IP Addresses & Subnets

Use Case	Query
I want to search for a single IP.	<code>ip 1.1.1.1</code> 
I want to search for an IP by subnet.	<code>ip: 1.1.1.0/24</code> 

## Certificates







Use Case	Query
I want to search by certificate names.	<code>services.tls.certificates.leaf_data.names:"google.com"</code> 
I want to search for certificates by subject org.	<code>services.tls.certificates.leaf_data.subject.organization:"IBM"</code> 



# Exploring Advanced Queries

With basic queries conquered, you might be ready to conduct more detailed searches with queries that combine inputs or queries that serve as a starting point for threat investigations.

For example, using the **Boolean logic syntax** discussed above, rather than just looking for a certain type of service, you can look for that type of service in a specific location with the inclusion of "and." You could also search by ranges, or nested queries.

Example	Query
Services in a specific location	<code>services.service_name: MODBUS and location.country: Germany</code> 
Hosts based on geographic coordinates	<code>location.coordinates.latitude: 40.78955 and location.coordinates.longitude: -74.05653</code> 
Unexpired certificates for a specific domain	<code>labels='unexpired' and names: censys.io</code> 
Self-signed certificates observed in Censys host scans	<code>ever_seen_in_scan: true and labels: "self-signed"</code> 
Trusted certs from a specific CA expiring on specific day	<code>parsed.issuer.organization: "Let's Encrypt" and labels: "trusted" and parsed.validity_period.not_after: 2023-10-13</code> 
A specific service on a specific port	<code>services: (service_name: HTTP and port:1337)</code> 



## Investigating Threat Activity and Other Interesting Artifacts

Censys Search is frequently used for more advanced exploration into the global internet infrastructure, including for the purposes of threat investigation. Our own researchers have used Censys Search to uncover evidence of Russian ransomware, which you can [read about here](#). We'll get into more detail about how to use Censys Search for threat hunting investigations in the next chapter.

**Queries that someone conducting an investigation into threat activity might find useful include:**

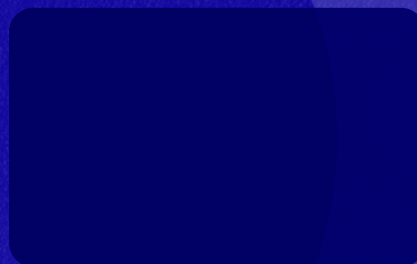
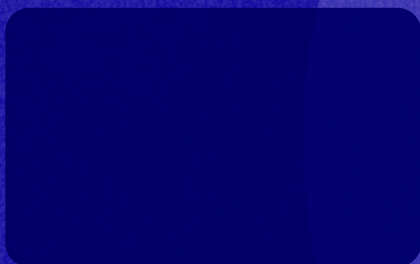
Example	Query
Open directories	<code>services.http.response.html_title: "Index of /" </code>
Cobalt Strike	<code>services.cobalt_strike: * </code>
Compromised MikroTik Routers	<code>services.service_name: MIKROTIK_BW and "HACKED" </code>
Services on port 53 that are not DNS	<code>same_service(services.port: 53 and not services.service_name: DNS) and services.truncated: false </code>
Network devices with exposed login pages	<code>same_service(labels:{network.device, login-page}) </code>
Deimos C2	<code>same_service((services.http.response.html_title="Deimos C2" or services.tls.certificates.leaf_data.subject.organization="Acme Co") and services.port: 8443) </code>

## Queries (continued)

Example	Query
Posh C2	<code>services.tls.certificates.leaf_data.subject_dn: "C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077"</code> 
Honeypot hosts	<code>services.truncated: true</code> 
RDP running on nonstandard ports	<code>services: (service_name="RDP" and NOT port=3389)</code>

## There's More to Explore

You can learn more about queries used to investigate threats and other unusual artifacts in these related reads from our Research Team!





# 5 Key Ways You Could Use Censys Search

TRACKING MALICIOUS INFRASTRUCTURE 23

IDENTIFYING VULNERABLE SERVICES 26

GAINING VISIBILITY INTO THIRD-PARTY RISK 29

MONITORING SSL/TLS CERTIFICATES 31

DISCOVERING OT/IOT DEVICES 33

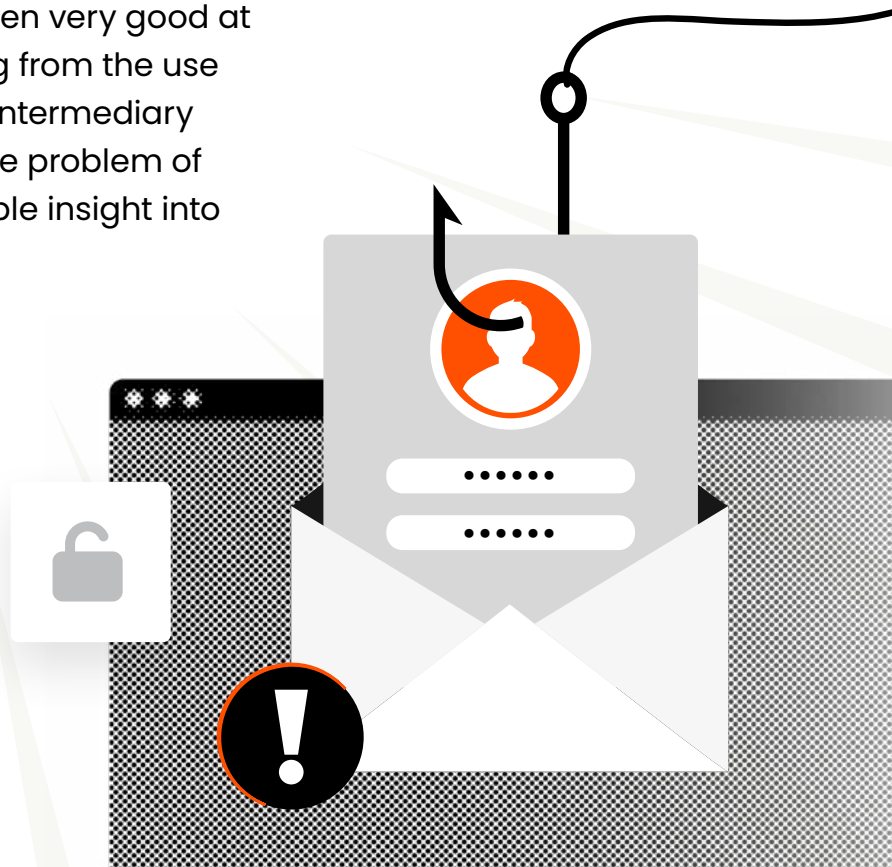
**With a view** of the entire public-facing internet at your fingertips, it isn't hard to imagine how many different interesting – and impactful – insights can be unearthed from Censys' massive dataset. In this chapter, we spotlight five popular ways that our users leverage Censys Search to support their cybersecurity objectives. **Though by no means an exhaustive list**, these examples are intended to provide a better sense of how Censys Search can be put into practice.



# 1

## Tracking Malicious Infrastructure

Proactively identifying adversary infrastructure is one of the most critical objectives for threat intelligence teams. However, tracking this infrastructure can be a particularly challenging objective, given that attackers who are intent enough on setting up things like C2 networks, phishing sites, and impersonated domains, are also, not surprisingly, often very good at hiding their tracks with tactics ranging from the use of proprietary VPNs to compromised intermediary services. Censys Search addresses the problem of source attribution by providing valuable insight into adversary operations.






## Follow Along

[Watch Tutorial >](#)


- 1 We could start in Censys Search by looking for evidence of malicious infrastructure in a certain geographic area. We can do this by combining a Censys Search location query with C2 and open directory labels. In doing so, we can identify assets in the U.K. that appear to be waiting for callbacks and offering a location to malware for storage.

```
(location.country: "United Kingdom") and labels:c2 and labels:open-dir 
```

- 2 On this query's results page, we spot a host that's running L3MON, which is well-known for being able to create fully undetectable payloads for Android phones. We can look at this use case in more detail by searching further for Cobalt Strike, which can fall into the wrong hands, using the service name qualifier.

```
services.service_name: 'COBALT_STRIKE' 
```

- 3 We see that 800 services with Cobalt Strike are returned. By adding the open directory filter back into our query, we can attempt to narrow our results.




```
services.service_name: 'COBALT_STRIKE' and labels: c2 and labels: open-dir 
```

- 4 We now see an interesting pattern: there is an ASN common across a couple of results. We'll pivot again, removing the open directory label to search for the ASN instead. This will give us hosts potentially originating from the same group.

```
services.service_name: 'COBALT_STRIKE' and autonomous_system.asn: 14061 
```

- 5 And with this, we arrive at just a few dozen hosts, likely related with similar configurations, all running from the same ASN! Check out the full tutorial for a closer look at this hypothetical investigation.

# Other Queries You Could Use to Track Malicious Infrastructure

Type	Query
AsyncRat C2	<code>services.software.product: asynccrat</code> 
Covenant C2	<code>services.software.product: covenant</code> 
Mythic C2	<code>services.software.product: mythic</code> 



I use it [Censys] daily and it has become an integral part of my toolset that I use to research and identify malicious infrastructure. The user interface is more intuitive, the pivoting options are better and simpler to use which makes hunting and research much simpler, and the query language is also easier to understand and use.

G2 Review from Verified Censys Search User,  
in Financial Services



# 2

## Identifying Vulnerable Services

Vulnerable services are low-hanging fruit for adversaries looking for entry points into the attack surface. However, the rapid pace of cloud sprawl, Shadow IT, and evolving digital infrastructure can make it challenging for already busy security teams to keep tabs on vulnerable services.


By querying specific service banners, software versions, or configurations in Censys Search, you can quickly pinpoint systems that require immediate patching or remediation.




## Follow Along

[Watch Tutorial >](#)

- 1 Let's say we want to understand whether or not any of our telnet services have exposures. We could start with a Censys Search query that searches for all services of that name.

```
services = telnet 
```

- 2 Of the millions of results that are returned, we refine our search by looking for exposed services with the words like "username" in the banner.

```
(services = telnet) and services.banner: 'username' 
```

- 3 However, we know that our service banners don't just include words like "username," we know they include the exact words "username." To narrow results further, we'll swap our colon (which gave us a fuzzy match) for an equal sign, which gives us an exact match. We've now narrowed our results from millions of telnet services to just 300.

```
(services = telnet) and services.banner='username' 
```

- 4 From here, you can apply your specific IP range to identify the specific telnet services belonging to your organization.

- 5 We took a stepwise approach to identifying services of interest, but you could also use this complete query from the start:

```
services=telnet and services.banner = 'username' and ip = add own IP range
```





What sets Censys apart is its ability to provide a real-time view of the assets as they appear on the internet, coupled with detailed metadata that can be crucial for effective risk assessment and mitigation. With Censys, users can easily navigate through a wealth of data to pinpoint specific vulnerabilities, understand their impact, and prioritize remediation efforts accordingly.

G2 Review from Verified User,  
Computer & Network Security



# 3

## Gaining Visibility into Third-Party Risk

The average modern enterprise maintains a vast ecosystem of third-party vendors and partners. It's the name of the game in an increasingly digital, highly-interconnected world. Understanding the security posture of these many partners is incredibly important, as gaps in their security can pose real risk to your organization.

In Censys Search, you can proactively monitor whether vendors or service providers are adhering to security standards and configurations specified in their agreements. Censys' daily scanning cadences and contextualized attribution provide the full visibility needed to understand third-party risk in real-time.



## Follow Along


[Watch Tutorial >](#)

- 1 Let's say you'd like to apply some scrutiny to a potential acquisition target (*Censys Search can be a tool for understanding risk from both current and future partners*).


You could start with a search for a vendor, like Microsoft Corporation. Services parsed subject queries can be delineated for specific organizations.

```
services.tls.certificate.parsed.subject.organization: `Microsoft Corporation` 
```


- 2 Next, you could refine your search with a nested query that looks for vendor certificates with information about the relative strength of their TLS certificates.

```
services: (tls.certificate.parsed.subject.organization: `Microsoft Corporation` AND tls.version_selected: {TLSv1_0, TLSv1_1}) 
```

- 3 On a similar theme, you could continue building on this query by looking for assets with weak encryption algorithms, like 3DES. Ideally, you want third-party partners to be using modern encryption standards like AES.

```
services: (tls.certificate.parsed.subject.organization: `Microsoft Corporation` AND tls.cipher_selected: {"TLS_RSA_WITH_3DES_EDE_CBC_SHA", "TLS_RSA_WITH_RC4_128_SHA"}) 
```

- 4 Additionally, you could look for exposed Managed File Transfer servers related to your vendor and all of the associated vulnerabilities that they introduce.

```
services.tls.certificate.parsed.subject.organization: `Microsoft Corporation` AND labels: managed-file-transfer 
```



# 4

## Monitoring SSL/TLS Certificates

Expired and misconfigured certificates pose all sorts of problems for organizations, from application functionality issues to attacker exploitation, using techniques like POODLE attacks.

As we mentioned in Chapter 1, **Censys has the largest database of x.509 certificates in the world** (20 terabytes, or 17B+ certificates and counting). This makes Censys Search a great resource for understanding your certificates. Use the tool to track SSL/TLS certificates to prevent use of expired or misconfigured certificates, identify certificate authorities used, and ensure that an organization's certificates are secure.



## Follow Along

[Watch Tutorial >](#)

- 1 Let's pretend you're on the lookout for expired certificates tied to your organization. We can start with a query that uses regular expression (regex) to enumerate your search for certificates with a high degree of fidelity. In this hypothetical, we'll say your organization's name is ACME.

```
((services.tls.certificate.names=/(.*)acme.(.*)/ or name=/(.*)acme.(.*)/ or dns.names=/(.*)acme.(.*)/ or dns.reverse_dns.names=/(.*)acme.(.*)/))
```



- 2 From here, we can add a clause that looks at the validity length of the returned certificates. Let's choose one that has no life left at all.

```
((services.tls.certificate.names=/(.*)acme.(.*)/ or name=/(.*)acme.(.*)/ or dns.names=/(.*)acme.(.*)/ or dns.reverse_dns.names=/(.*)acme.(.*)/)) and services.tls.certificate.parsed.validity_period.length_seconds=0
```



- 3 This returns all of our exposed certificates. However, we can still look further. Which certificate issuers are you using? We'll add another clause that excludes certificates from your approved issuer. In this hypothetical, we'll say it's Let's Encrypt.

```
((((services.tls.certificate.names=/(.*)acme.(.*)/ or name=/(.*)acme.(.*)/ or dns.names=/(.*)acme.(.*)/ or dns.reverse_dns.names=/(.*)acme.(.*)/)) and (services.tls.certificate.parsed.validity_period.length_seconds=0) and not (services.tls.certificate.parsed.issuer.organization: encrypt)))
```



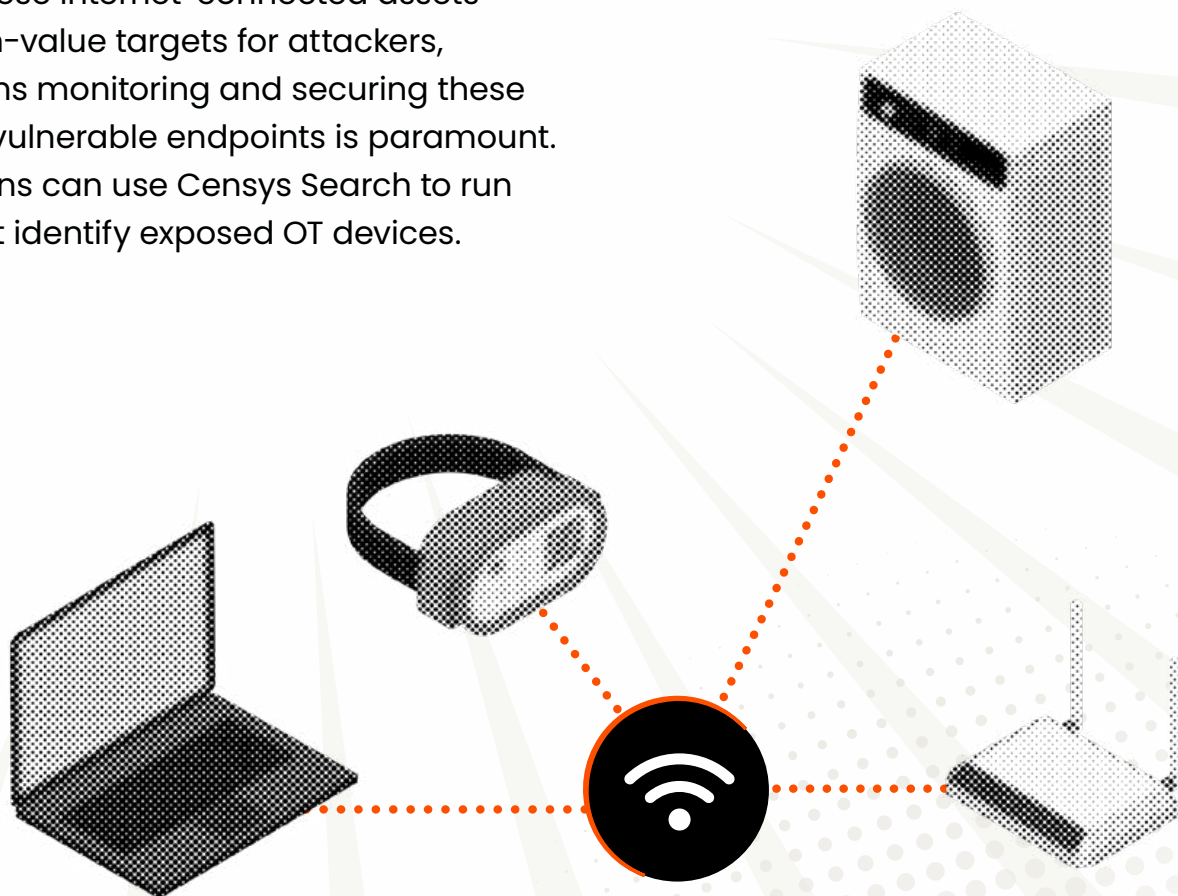
- 4 With just three queries, we've now successfully narrowed down 20 terabytes of certificate data into the small handful of certificates that are relevant to your security objectives.

# 5

## Discovering OT and IOT Devices

### Operational Technology Devices

Operational Technology (OT) devices connected to an organization's network are crucial for maintaining the security and integrity of critical industrial control systems. However, these internet-connected assets can be high-value targets for attackers, which means monitoring and securing these potentially vulnerable endpoints is paramount. Organizations can use Censys Search to run queries that identify exposed OT devices.





## Follow Along


[Watch Tutorial >](#)

- 1 We can start with simple searches for OT protocols. Let's choose BACNet.

BACNet 

---

- 2 A good start, but lots of results. We can narrow down to our interest in a manufacturer like Siemens. Perhaps in this hypothetical, their devices have been the target of a recent vulnerability.

BACNet and siemens 

---

- 3 You can see how even rudimentary queries can give insight into OT architecture. We want to keep digging though, so we apply a search for HTTP on these devices. Exposed HTTP could be evidence of an HMI that's visible to the outside world.

BACNet and siemens and services.port= 80 

---

- 4 And there we have it - we find devices with exposed HTTP that we can continue to investigate.


## Internet of Things Devices

As with OT devices, Internet of Things (IoT) devices are particularly high-value targets for adversaries looking to wreak havoc on organizations and governments. It doesn't take much imagination to recognize the implications of a nation state using exposed IoT devices to say, take control of their adversary's power grid. Censys Search can be used to find and protect these sensitive IoT devices.

### Follow Along

[Watch Tutorial >](#)

- 1 We can start by using the 'IoT' label - one of many labels in the tool that groups devices by functionality. We'll combine this label with a geographic area of interest, based on recent geopolitical events.

```
labels: iot and location.country: "Ukraine" 
```

- 2 Thousands of results are returned, so to add some granularity, let's look specifically at cameras that are running real-time streaming.

```
labels: iot and location.country: "Ukraine" and services.service_name: RTSP 
```

- 3 Now we have our specific subset of interesting devices that we can parse through and further refine!

## Other Ways You Could Use Censys Search

Looking for more inspiration? Censys Search can be used for all sorts of additional security objectives, including identifying instances of domain spoofing and discovering rogue assets. Check out our [10 Ways to Use Censys Search Cheat Sheet](#) to learn more, or visit our [Resources Hub](#) to view more tutorials!



## CHAPTER 4

# Navigating Censys Search

GAINING PERSPECTIVE WITH HISTORICAL DATA 38

WORKING SMARTER WITH MATCHED SERVICES 39

COLLABORATING WITH TAGS & COMMENTS 41

PIVOTING STRATEGICALLY WITH THE EXPLORE FEATURE 42

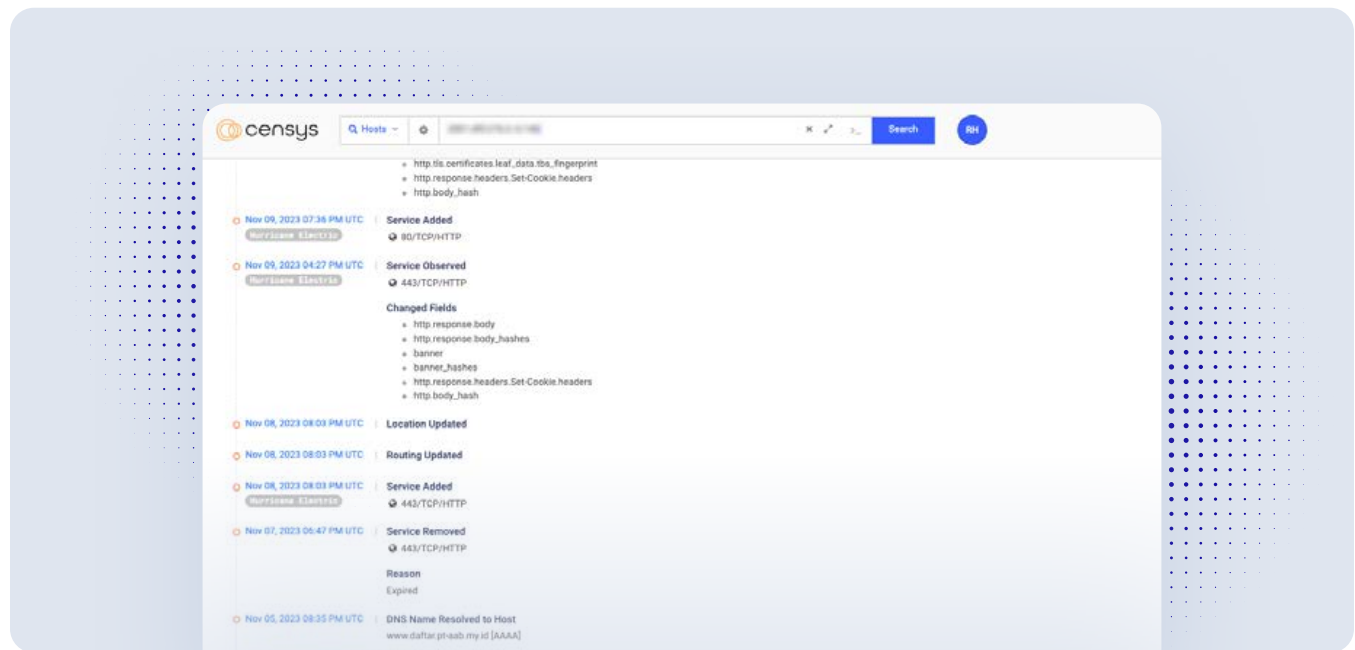


**We've introduced** how you can use queries to conduct searches for various security objectives – it's now time to highlight the additional features and capabilities within Censys Search that can advance your exploration! These best practices will help you find exactly what you're looking for in Censys Search, faster, and more efficiently.

# Gaining Perspective with Historical Data

Historical data is an incredibly valuable resource for today's cyber heroes. The ability to credibly identify threats, map adversary tactics, and create detailed incident reports often depends on being able to look back at activity that occurred at a previous point in time.

**In Censys Search, you can access up to two years of history about hosts.**



## How to Go Back in Time with Censys Search

On any host page in Censys Search, you'll see **"Host History"** in the top navigation bar. This displays a chronology of events related to host activity, like when services are added and locations are updated.

To see all of the observations Censys made of a host's services, open the **History** tab and toggle the **"See All Observations"** button to blue. To compare activity from two points in time, tick the boxes on the left-hand side of the activity you want to compare and click the **"Compare"** button. A comparison could be useful when trying to determine if and how a host may have been impacted by a zero-day.

## Historical Data in Practice

The Censys Research Team recently used the host history function in Censys Search to facilitate an investigation into **NTC Vulkan infrastructure** related to offensive cyber tools. The team used historical analysis to identify a GitLab server that NTC Vulkan may have previously been using to develop tools for a cyber unit of Russia's military intelligence service. Investigating the history of NTC Vulkan's hosts helped the team learn more about the core functions of the hosts and the organization itself.

### Further Reading

Check out our [Discovery of NTC Vulkan Infrastructure](#) article for a full analysis of what our research team uncovered.

---

## Working Smarter with Matched Services

Guesswork and manual effort are two things today's cybersecurity teams simply don't have time for. The matched services feature in Censys Search helps ensure you avoid both.

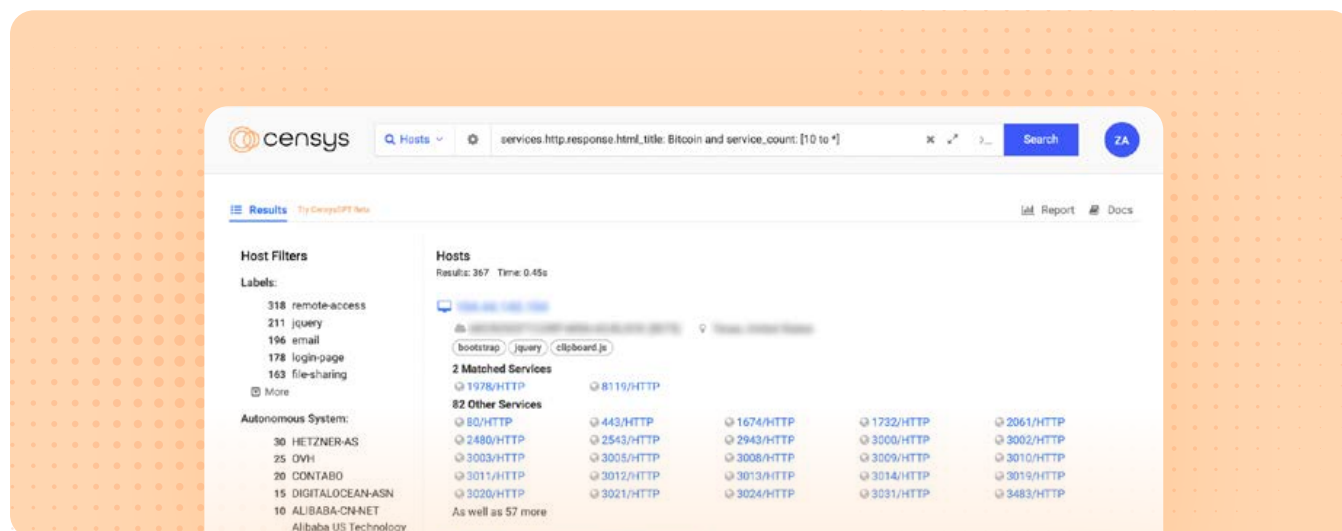
**When users perform a query on a host with multiple services, the matched services function highlights exactly which services on the host meet the search criteria.** This helps users quickly pinpoint the relevant services, without manually sifting through *all* of the services that a host may run.



## Matched Services in Practice

We know that a host can have multiple HTTP services, all running on different ports. When each of these services is scanned, each HTTP service returns a response, which can be unique or the same. Matched services can save users significant time investigating each of those responses by identifying which HTTP service running on a host matches the query.

**In the example below, we're looking for a host with an HTML title that includes "Bitcoin" and more than 10 services running on it.**



Results page for the query: [services.http.response.html\\_title: Bitcoin and service\\_count: \[10 to \\*\]](#).

Rather than clicking into the 82 other services, all of which are on the same HTTP service, users only need to investigate the two matched services.

This kind of precise matching is crucial for cybersecurity teams who need to identify and address specific vulnerabilities or compliance issues efficiently. In other words, if you aren't using matched services, you're missing out!

# Collaborating with Tags and Comments

Cyber heroes can't do it alone! The tags and comments features within Censys Search recognize this reality, and serve as useful ways to better organize your work, jump back into investigations, and collaborate with other team members.

## Staying Organized with Tags

Tags are custom markers that make it possible to quickly categorize and filter data. **Importantly, tags make it easier to return back to the things you found interesting in Censys Search.**

When you come across a host or certificate in Censys Search that you want to earmark, you can add your own custom tag to the host or certificate page. This opens the door to a whole new level of customization and personalization within Censys Search.

### Tags in Practice

Create a tag by navigating to the top right corner of a host or certificate page and clicking the **"Add Tag"** button. A display box will pop up to enter your tag name. Once you click "Add Tag," your tag will appear on the host or certificate page any time you return to it. The Add Tag box can also show you tags that have been previously created by your team, so that you can work from existing tags and follow a shared tagging structure if you choose. (And don't worry, nobody outside of your organization can see your tags.)

## Communicating with Comments

Comments further extend the functionality of tags by allowing team members to annotate specific hosts or certificates with insights, context, or follow-up actions. In doing so, teams can create their own shared knowledge base. This collaborative approach ensures that all team members have access to the same information. Comments are a great option when you have more to say about a finding than what could be conveyed through a custom tag.

### How to Leave a Comment

Comments can be found at the very bottom of a host or certificate page. There, you'll see a box with a prompt to enter text. You and your team have the ability to type as much or as little as you'd like. You can include links and images for additional context in your write-up, too.

---

## Pivoting Strategically with the Explore Feature

The ability to pivot is one of the most critical skills in threat hunting! By pivoting effectively, you can uncover hidden relationships, patterns, and attack paths, allowing them to trace the entire attack chain and gain a holistic view of the threat landscape.

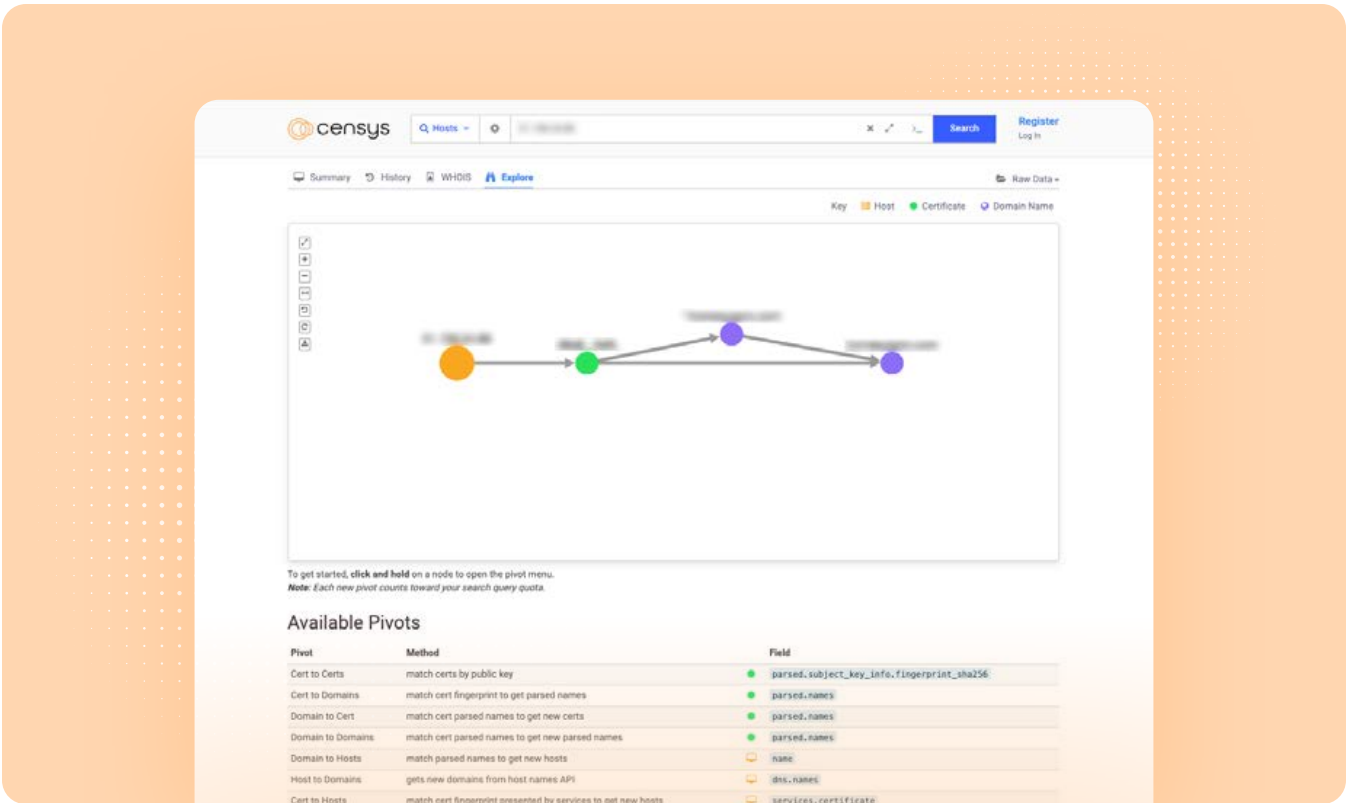
### Explore in Censys Search

In addition to pivoting as you come upon new and interesting information, you can *also* use the Explore feature in Censys Search to fast track your next move. This feature provides recommendations about related hosts, certificates, and domain names that may be worth exploring next.



# How It Works

On any host or certificate page, find the “**Explore**” tab in the top navigation bar. Click to see a nodal map of hosts, certificates, and domain names that are related to the host or certificate you’re viewing. To learn more about a specific node on the map, click and hold on the node. An icon will appear that will allow you to jump into a new tab to view more detailed information about the node, or jump to more information about its related certificate, host, domain details.



Below the map, you’ll also see a list of these same pivot opportunities, with details about the type of pivot, the method, and the corresponding field in Censys Search.

Use the **Explore** feature to gain one, consolidated view of all potential pivots to make your next move strategically!





**I really like that I am able to tie together multiple elements and pivot points to include the number of services, specific services, ASN data, response headers etc., to identify very specific infrastructure.**

G2 Review from Verified Censys Search User,  
Enterprise Company



# Other Capabilities You Should Know About

USING REGEX QUERIES TO IDENTIFY PATTERNS

47

ACCELERATING SEARCHES WITH CENSYSGPT

49

INTUITIVE SEARCHING WITH MAP TO CENSYS BETA

50

INTEGRATING CENSYS DATA INTO  
YOUR SECURITY ECOSYSTEM

52




**But wait! *There's more.*** We've covered the essentials, but there's still a treasure trove of Censys Search insights to unpack. While we won't be able to get through all of it in this one humble handbook, we *will* spend this chapter highlighting a handful of additional capabilities that we think are worth your attention!


# Identifying Patterns with Regex Queries

**Regular expression (regex) queries** unlock advanced search capabilities by providing more flexibility to define your search criteria. Rather than submitting a query limited to a single static string, users can run regex queries that ask Censys to identify patterns in the data.




For example, without regex, you might run a query that asks:


Example (without regex)	Static string query
"Which (unnamed) hosts with an HTTP service contain a reference to any string containing .js?"	<code>services.http.response.body:*.js*</code> 

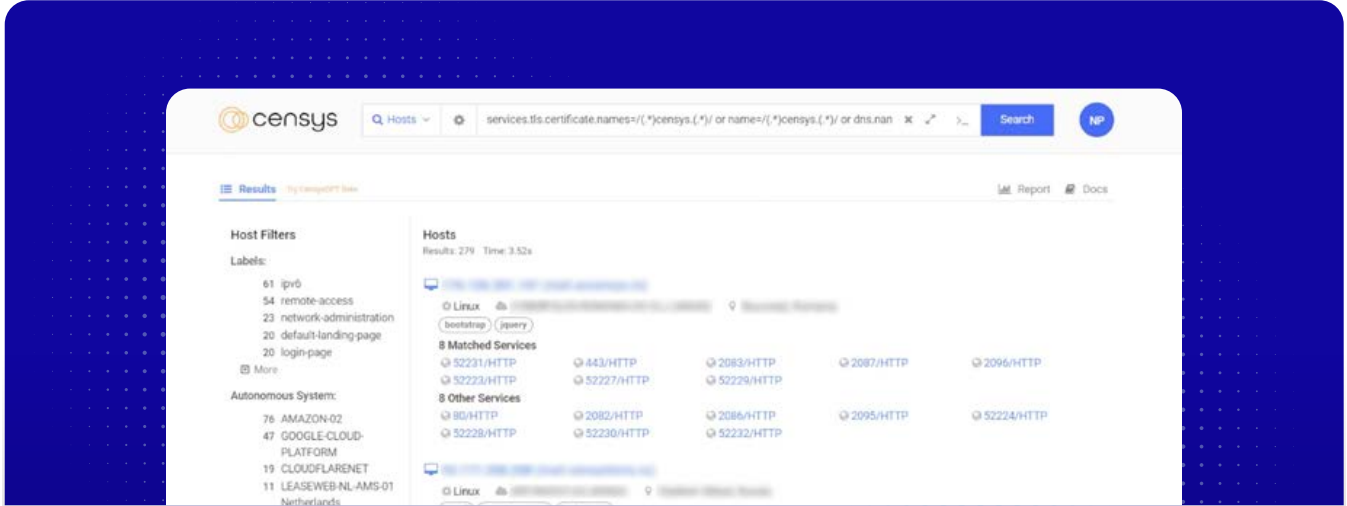
With a **regex query**, you could broaden your criteria with a query that asks:

Example (with regex)	Regex query
"Which hosts have an HTTP location header that includes the sequence ../ (which is vulnerable to directory traversal attacks), followed by one of the more common executable page types like .js, .php, or .asp?"	<code>services.http.response.headers.location=/(.*(\\.\\.\\/))+.*(\\.asp \\.php \\.js \\.cgi).*/</code> 

**Regex queries** are best used when simple pattern matches won't suffice, and are ideal for fields whose values are long strings. Popular hosts to write regex expressions for are **"http.response.body"** and **"services.banner."**

Additional examples	Regex queries
HTTP responses originating from behind a proxy	<code>services.http.response.headers.x_forwarded_for: /.*,.*/</code> 
Certificates that contain an eTLD+4-formatted subdomain of censys.io:	<code>names: /.*\...\censys\.io/</code> 
Hosts with a service serving a Hook URL	<code>/.*\:3000\hook\.js.*/</code> or <code>services.banner=/.*\:3000\hook\.js.*/</code> 

 **TIP:** You can find a guide to regex query syntax that explains how to use all of the backslashes, periods, and other placeholder characters, [here](#).





# Accelerating Searches with CensysGPT

We've talked about running searches with queries. But there's actually another way to find what you're looking for.

**With our AI-powered CensysGPT, a beta feature of Censys Search, you can translate natural language queries into Censys Search queries.** This means you can bypass query syntax altogether and find what you're looking for *even faster*. CensysGPT is particularly ideal to use when you have a more complicated question in mind that might require advanced query building. Simply ask CensysGPT your question in your own words!

We also know that while Censys offers the *best* view of the internet, it's not the only view. If you're familiar with other query languages, you can use CensysGPT to automatically convert your queries into Censys queries. You can access CensysGPT right from the Censys Search home page.

## Simplify your query building

With **CensysGPT**, there's no need to let the nuances of query language slow down your investigation!

### CensysGPT Beta

CensysGPT beta simplifies building queries and empowers users to conduct efficient and effective reconnaissance operations. The tool enables users to quickly and easily gain insights into hosts on the internet, streamlining the process and allowing for more proactive threat hunting and exposure management. We're continually improving CensysGPT and value your feedback!

Enter your search query here:

e.g. Find hosts running Apache

Generate Query ↗

Try one of these examples:

Russian hosts running RDP or FTP ↗

Services in Brazil with the html title "Index of /" ↗

Translate a Legacy Censys Query:

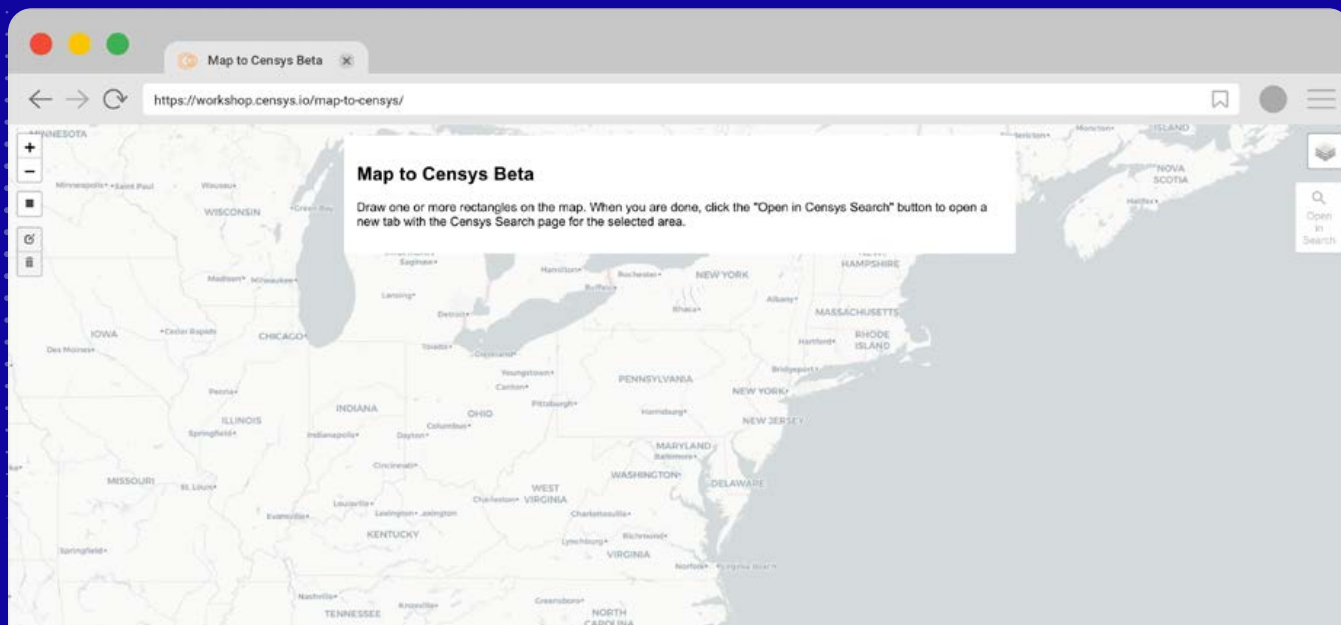
80.http.get.headers.server: squid ↗

443.https.get.body: "kubernetes" ↗

Translate a Shodan, ZoomEye, BinaryEdge, or other query:

os:Windows port:2077 ↗

text:'PRTG Network Monitor' AND port:80,443 ↗



## Intuitive Searching with Map to Censys Beta

Searching by geolocation can significantly narrow the scope of a threat hunting investigation, transforming the overwhelming expanse of global internet infrastructure into a manageable field relevant to your objectives.

Our innovative [Map to Censys Beta feature, available in the Censys Search Workshop](#), streamlines geolocation searches by eliminating the need for manual location-based queries.

## Here's how to leverage this powerful tool:



### ACCESS

Navigate from the [Censys Search home page](#) to the [Search Workshop](#) and select "[Map to Censys Beta](#)."

---



### INTERACTIVE MAPPING

Upon selection, a world map appears. You can zoom in to continents or drill down to townships and streets. To define your search area, use the rectangle tool from the toolbar to draw a region. For instance, draw over the Eastern Seaboard to capture a broad yet significant area.

---



### EDIT AND REFINE

Adjust the shape of your drawn rectangle with the pencil tool to fit the exact geographical outline you need.

---



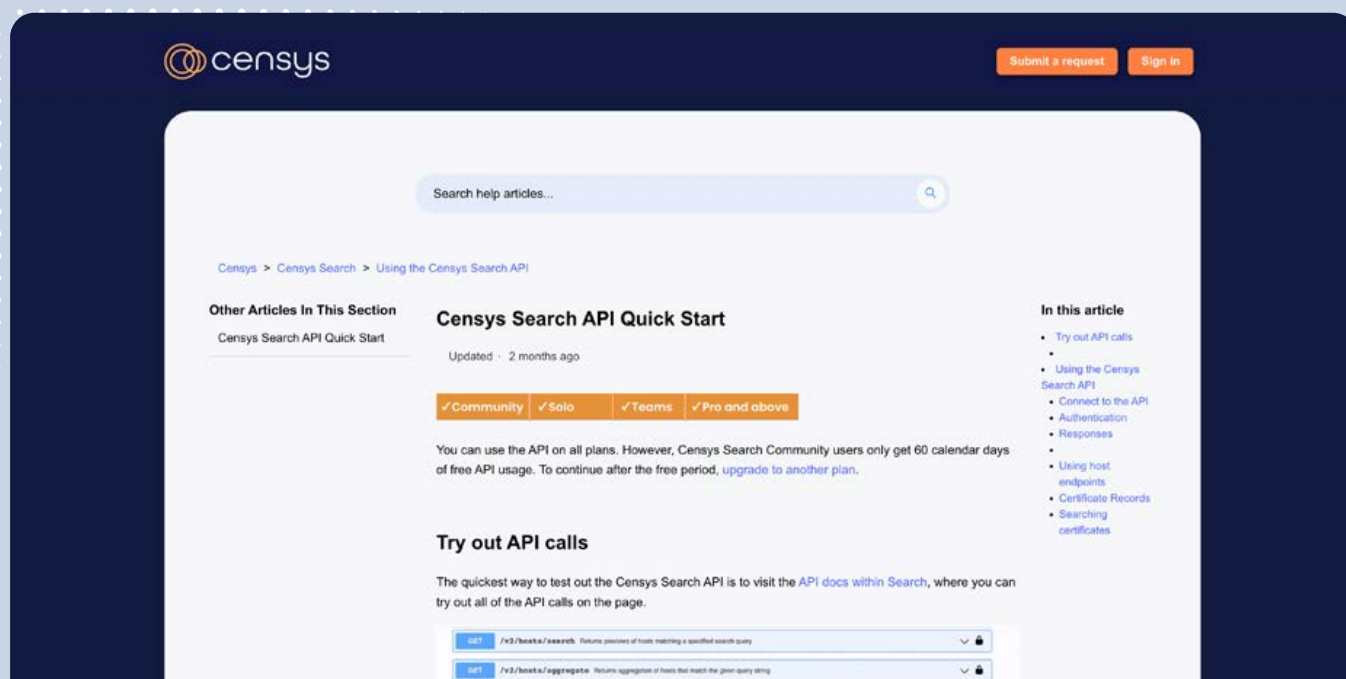
### SEARCH AND ANALYZE

Once your area is highlighted, click "**Open in Search.**" A new tab will display all hosts in your selected region, offering a granular view of potential threats and anomalies.

## Multi-Regional Searches and Additional Views

[Map to Censys Beta](#) isn't just for single-region searches. You can select multiple areas and view aggregated data for all selected regions. And for a different perspective, switch between various display filters like the Esri World Imagery for satellite visuals or OPNVKarte for public transport routes.





# The Censys API: Bringing Censys Data into Your Security Ecosystem

Censys Search data can also be retrieved through our API. The Censys API makes it possible for users to conveniently integrate Censys data into their own applications, security tools, and scripts. For example, many organizations use the API to enrich their SIEM tools and augment their threat intelligence feeds.

## **Getting started with the Censys API is simple.**

You can navigate to [search.censys.io/api](https://search.censys.io/api) to access the Censys Search endpoints.

Once there, you'll see that every call to the API requires authentication with HTTP basic auth using the API ID and secret key shown on the My Account page.

## Host Endpoints & Certificate Records

You can use the API to search for, compare, and view hosts and certificates in their current state or at a historical point in time, and more:

Use Case	Query
<b>Search</b> Search for hosts using the Censys Search Language.	(/v2/hosts/search)
<b>Aggregate</b> Generate a report about the frequency of values seen for a specified field across all hosts matching a search.	(/v2/hosts/aggregate)
<b>View</b> View a host as it is known to Censys currently or at a historical point in time.	(v2/hosts/{id})
<b>Hosts by Cert</b> Lists the hosts that are currently presenting a certificate.	(v2/certificates/{fp}/hosts)
<b>Search</b> Search for certificates using the Censys Search Language.	(v2/certificates/search)
<b>Report</b> Generate a report about the values for a specified field across all certs matching a search.	(v2/certificates/aggregate)

If you choose to use the Censys Search API, the **custom field selection** feature is a great way to optimize your searches! Custom field selection host previews aren't limited to default fields; instead, only the specific fields you request will display. You can read further about custom field selection in [our blog article](#), and to learn more about how to get started with the Censys API, visit our [API Quick Start Guide](#).



# Starting Your Journey with Censys Search



**Congratulations!** You've made it to the final chapter of *Unleash the Power of Censys Search*. You're now familiar with the fundamentals, have best practices in your back pocket, and should feel ready to start searching with confidence! Before you jump in (or back in) to the tool, let's talk about which version of Censys Search might be the best fit for you, and ways you can access ongoing support.

# Staying Connected with Censys

Your Censys Search learning journey doesn't have to stop here. You can find even more instructions, insights, and practical tips from Censys when you visit:



## [The Censys Community Forum](#)

Connect with other Censys users and industry experts on the Censys Community Forum! Ask questions, start discussions, learn from others, access documentation, and more. Anyone with a Censys account can join.



## [The Censys Knowledge Base](#)

This is your go-to destination for technical documentation, where you can find detailed information about topics like our query language, API, and host and certificate fields.



## [The Getting Started Site](#)

This is where a more focused collection of new user resources lives. Quick links take you to essential resources like our "Search Query Fundamentals" article.



## [The Censys Resources Hub](#)

Find the latest and greatest security thought leadership content here.



## [Censys on Social](#)

We regularly publish user content on [LinkedIn](#), [X](#), [Reddit](#), and [Mastodon](#). Follow us for updates and to connect with other users!

# The Power of Censys Search Is In Your Hands

We've covered how Censys Search's unparalleled insights into global internet infrastructure can empower you to be the cyber hero your organization needs.

*It's now up to you to make the most of it!*

We hope that the knowledge and techniques shared in this handbook will enhance your ability to leverage Censys Search to its fullest potential. Embrace this powerful tool, continue exploring its features, and join an expansive community of professionals dedicated to advancing the frontiers of internet security.

**Happy searching! Get started today at [search.censys.io](https://search.censys.io)**



Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.

[hello@censys.com](mailto:hello@censys.com)    [www.censys.com](https://www.censys.com)