


COOKBOOK

Cooking Up Queries

WITH censys


Your Guide to Savory Internet Searches (and Actual Recipes)




Have an appetite for detecting threats, uncovering vulnerabilities, AND tasty treats?

You've arrived at the right cookbook.

Welcome to the wild and wonderful world of the internet, where you never know what you might find and what might be lurking behind the firewall. Whether it's a hacked server, an exposed device, compromised critical infrastructure or something more sinister, as a security professional, we know you are always on the hunt. And to thwart the next bad actor, you need access to powerful data and tools.

Enter Censys Search. We provide security teams best-in-class data so you can proactively protect your organization against the bad guys. Censys Search leads the industry in scanning capabilities to provide the largest, most comprehensive dataset of internet intelligence available.

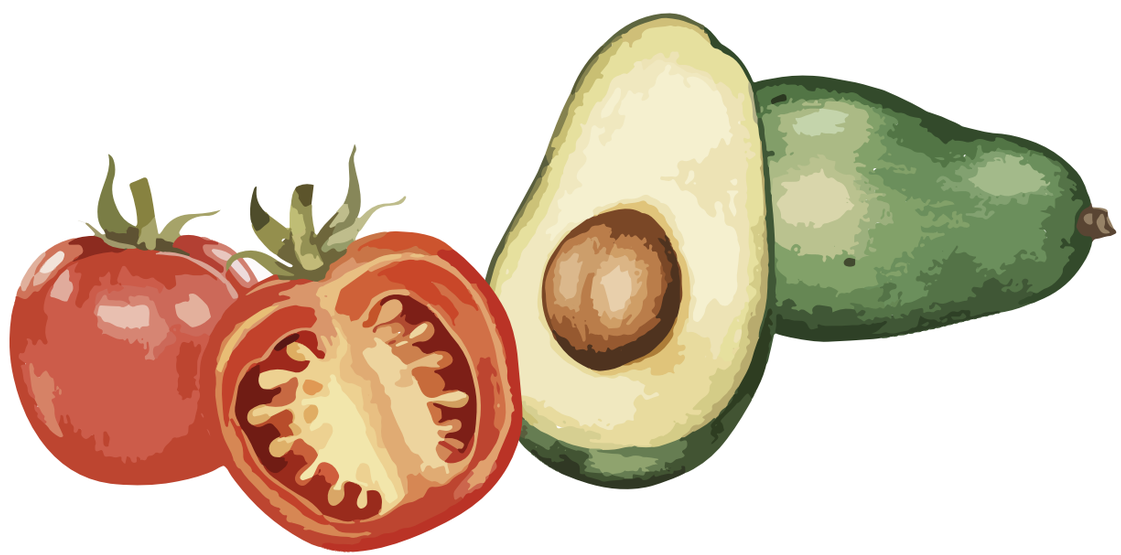
And the key to leveraging Censys Search to suss out the bad guys is cooking up the perfect query to investigate the biggest and baddest threats. Here at Censys, we think of our search queries a bit like recipes – combine the right search elements in the right order, and out pops the delectable details of the next big hack.

Which queries might you consider running on Censys Search? In this query cookbook, we'll walk through some of the most common ways security teams use Censys to conduct searches and gather important information about potential threats.

Follow our step-by-step query "recipes" and arrive at the information that will help you best protect your organization.

Then, reward yourself for all of your hard work with instructions for recipes you can actually eat, courtesy of our Censys home chefs. You didn't think our cookbook would forget about the food, did you?

Let's get cooking.



How to Deal with a Dreaded Zero Day

Let's kick things off with a recipe that'll take you from "oh no" to "no big deal" in no time. Because when a dreaded zero-day drops, it's all about how fast your team can whip up the right response.

What makes a zero-day such a race against time? It's a question of who will get to a publicly-disclosed vulnerability first: the good guys (your team) or the bad actors? As the certified good guys, it's your team's job to find out if the critical vulnerability is affecting your business, and if so, how severely. Once you know that, you can switch gears to patching so that you can keep greedy threat actors at bay.

But to win this race against time and keep your company protected, you need maximum visibility. Are your assets exposed? Which ones? Where do they live? After all, you can't protect what you can't see.

That's why in this recipe, we'll show you how to gain the visibility you need to act quickly and beat threat actors to the punch. Learn how you can leverage the Censys Search tool's queries and free dashboards, along with other actionable content and insights from our team.

Query Ingredients

- Access to search.censys.io
- The Cybersecurity & Infrastructure Security Agency website
- The Censys Blog
- Censys Search zero-day dashboards and queries
- Your Censys Customer Success point of contact
- Censys Twitter & LinkedIn profiles

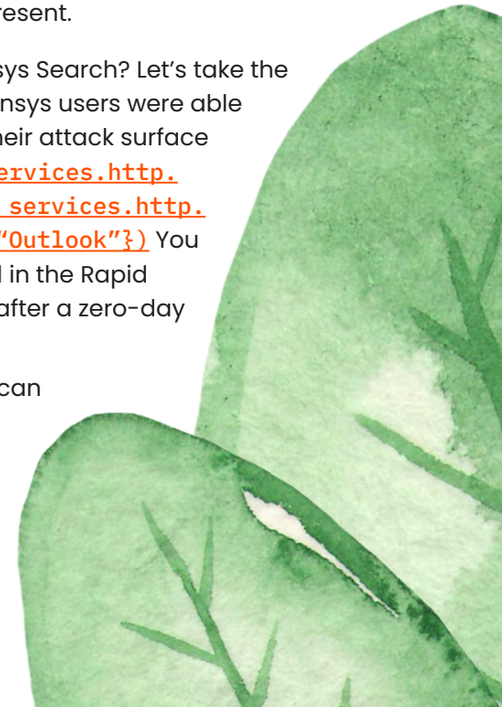
Query Recipe

1. If you're like most security teams, you probably first learn about a zero-day through the news, social media, or other folks in your network. Once you're aware of a zero-day, the first step is to read up on what's known about the Common Vulnerability and Exposure (CVE). We like to point folks in the direction of CISA (Cybersecurity & Infrastructure Security Agency), which is usually one the best places to get reliable, up-to-date information.

2. Next, you and your security team will need to figure out whether the CVE applies to your attack environment. Are your assets at risk? One way to reach your answer quickly is through the Censys Search tool, which you can find at search.censys.io. Here you can access our handy zero-day tracking dashboards and run specific zero-day queries about where the vulnerability is present.

    - Exactly what kind of query could you run on Censys Search? Let's take the latest ProxyNotShell vulnerability for example. Censys users were able to learn more about ProxyNotShell's impact on their attack surface by running the following query: `same_service(services.http.response.favicons.name: */owa/auth/* and services.http.response.html_title={"Outlook Web App", "Outlook"})` You can find queries specific to the zero-day at hand in the Rapid Response blogs that our team publishes shortly after a zero-day is announced (more on that below).

3. Your info gathering doesn't have to stop there. You can gain even more visibility and context about the zero-day by exploring additional Censys resources. When a zero-day hits, we update our community in a number of different ways.



Query Recipe Continued

a. For the Security Community at Large:

- The research team at Censys immediately starts digging into various data points to begin documenting the pervasiveness of the CVE. We clearly identify which assets are vulnerable to a new CVE within 8 hours of identification, and publish those on our Censys Blog to raise awareness and to share insights on how to best respond or mitigate. The blog is updated as new developments unfold, so you can always find the latest and greatest updates here. (Pro tip: Bookmark the blog so you can quickly check back in throughout day/week).

b. For Censys Users & Customers:

- Our Customer Success team provides exclusive alerts, puts boots and ears on the ground by looking at YOUR specific attack surface, and ensures you get the first insider scoop from your trusted source.

  1. The CS team will first package up the CVE information and distribute it to customers as soon as possible. This is done within hours of the publicly-known vulnerability release and occurs in conjunction with our research team's Rapid Response blog post.
     - Censys Attack Surface Management customers are able to immediately leverage Censys to scan their attack surface with queries provided by the Censys research team to begin remediation.
     - Censys Data customers are able to use their Censys Data accounts to query the internet and hunt for the vulnerabilities.
  2. Have a question or looking for a little one-on-one direction? The Customer Success team and Censys Support team are available 24/7 to help customers with any aspect of a zero-day response, whether it's discovering their vulnerabilities or figuring out the best course of action for remediation or patching.
  3. Once the dust has settled, the Customer Success team ensures organizational transparency by sharing risk reporting, providing customer attack surface trends, and offering future Rapid Response recommendations.

4. Finally, you'll want to monitor the patching of your zero-day vulnerability on an ongoing basis. Often, researchers and security professionals determine new or updated details about how the vulnerability may be exploited. Censys continually updates our blogs, even years after the original CVE. Bookmark the blog post for easy check-ins going forward.

Wrap-Up

When a zero-day drops, remember that you're not alone. You can rely on Censys to share the recipe for remediation and patching success within hours of the announcement, and as a customer, you can turn to our Customer Success team for real-time updates and personalized guidance on risk remediation.

APPETIZER RECIPE

Parmesan Spinach Balls

Just like dealing with a pesky zero-day, sometimes you need a quick, reliable recipe that's a surefire solution to getting you out of a jam. We've all been there before – maybe you forgot you agreed to bring an appetizer to tonight's dinner party, or perhaps you have a hungry audience in need of an after-school snack, but are tight on groceries. What could you throw together in short order to solve the issue? Allow us to introduce you to these oh-so-simple parmesan spinach balls. These spheres of savory flavor and cheesy goodness are a time-tested appetizer that checks all the boxes when you're in a pinch: quick to make, filling, and still easy to impress with.

PAIRS NICELY WITH
How to Deal with a Dreaded Zero Day
PAIRS NICELY WITH

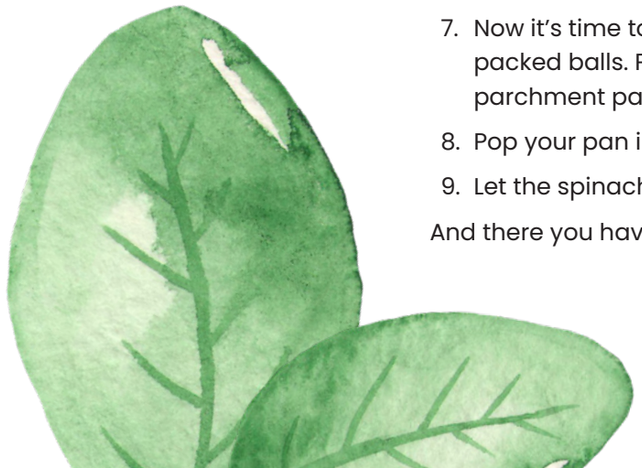
Ingredients

- 2 10 oz bags of frozen spinach
- 1 TBSP of minced onion
- 2 cups herbed seasoned stuffing croutons
- 1 cup parmesan cheese
- 2 beaten eggs
- 3 TBSP melted butter

Recipe

1. We'll start by preheating your oven to 375 degrees Fahrenheit.
2. You'll then want to combine your spinach (frozen) and minced onion in a pan and set heat to medium high. You can let this combo cook for about eight minutes or so (the spinach should be thawed and the onions, translucent).
3. Next, move your sauteed spinach and onion mixture to a colander over the sink and be sure to drain well. (This drainage step is key - you don't want any extra moisture).
4. Separately, whisk your two eggs together in a small mixing bowl.
5. Once drained, move your spinach and onions to a medium mixing bowl and gently fold in your remaining ingredients: stuffing croutons, parmesan cheese, beaten eggs, and melted butter.
6. Mix well until all ingredients are combined.
7. Now it's time to (literally) get your mixture into shape. Grab a small handful or spoonful and round out into 1-2 inch firmly-packed balls. Place your spinach balls a few inches apart on a shallow non-stick pan. You can also line your pan with parchment paper if preferred.
8. Pop your pan into the oven and let bake for about 15-20 minutes, or until you see a bit of crisping on the outside.
9. Let the spinach balls cool at room temperature for about 5 minutes.

And there you have it! Consider your appetizer dilemma remediated: you now have a tasty treat that's ready to share and enjoy.



Discovering Critical Infrastructure

Let's take a detour into the intriguing and high-stakes arena of critical infrastructure. What makes this particular corner of the internet worthy of a query recipe? For starters, there's a lot going on here – the majority of which we all rely on in some way, whether we realize it or not. Critical infrastructure includes essential services relevant to things like national security, economic security, and public health. You know, the services and networks that would create "kind of a big deal" if they weren't available. And because this space is (dare we say it) so "critical" to how we live our lives, it can also be an attractive ground for nefarious actors looking to wreak havoc.

For officials in government, those with national security roles, and folks in other related organizations, when essential services are on the line, being able to effectively monitor these infrastructures and detect the bad guys before they can act is paramount. That's where this query recipe comes in. Let's take a look at how we can use Censys Search to learn more about activity on critical infrastructures, and how to take action if we spot something unusual.

Query Ingredients

- Access to search.censys.io
- A goal for discovery: what kind of infrastructure are you looking to find?
- A location of interest

Query Recipe

1. Let's kick off this recipe by focusing on a location of interest. Where do you want to begin your search? You might already have a specific location in mind, or you may want to start broader and select a country of interest, and narrow your search from there. Pop into the Censys Search tool (search.censys.io) and navigate to the location field. Then, select country or country code, and from there, narrow down by province, city, and other options if you want to get more specific.

2. Once you've told Censys Search where you want to look, it's time to start unveiling what is hanging out in said location. Let's start by looking at hosts with ICS/SCADA/OT-related protocols. You can browse up to 1000 different protocols by location using the handy Report function. You can click on a protocol to view all hosts that are running that protocol in your area of interest, or you can query all ICS/SCADA/OT-related protocols that Censys discovers in your area of interest.

3. You'll next want to find ICS/SCADA/OT assets by asset type. You can search for specific ICS/SCADA/OT assets by name (ex: `Honeywell XL Web Controller`) or by keyword (ex: `Siemens`) within host responses via queries such as HTML Title, Telnet banner or other ICS/SCADA/OT response fields. If your overall search goal is broad, you might try a number of different asset types here. But if you know exactly the kind of infrastructure you're looking for (such as operational tech in the utilities space), this is where you can get specific and turn results faster.

4. If your goal was to identify where critical infrastructure is present, give yourself a pat on the back! You've just accomplished that in Step 3. However, if you're interested in figuring out which infrastructure might be home to suspicious activity, this is where the investigation continues. You can keep digging by narrowing your resulting hosts by likelihood of exposure. Too many hosts to investigate individually? Not a problem. Just add HTTP, Telnet and/or other protocols to your query string. Adding other

Query Recipe Continued

protocols that are likely to elicit a login prompt, a product type, an admin panel, or provide other insights can indicate possible exposures.

5. From here you can investigate individual hosts for exposures by examining their responses on various ports/protocols (including HTTP, Telnet, Modbus, BACnet and more) for login prompts, serviced location information, model numbers, manufacturers, admin panels, and more.

6. Now it's time to research uncovered device information. For this step, we'll hop out of the Censys Search tool and use a search engine like Google to look up the makes and models discovered in the previous step. This will give us a more precise understanding of the host's function and allow us to see if known exposures exist (e.g.: default credentials in online user manuals).

7. Let's say you do in fact spot something that looks like an exposure. After confirming its criticality (function + location) and confirming that an exposure exists on the host, you'll want to document your findings. The easy part here? You can capture your key findings right within the Censys Search tool! Use document key aspects like function, make/model, owner, and location serviced by the asset. The tool's tags also let you quickly return to hosts and track your progress. Additionally, you can use the COMMENT section at the bottom of the host summary page to detail exposures and add context to share with your colleagues. Note: Tags & Comments are only visible to your team, so no need to worry about exposing sensitive findings.

   » Did you find a make/model in a parsed field like HTML Title or Modbus vendor? Capture it and build a list of known devices to query en masse later.

8. Now that you've discovered a criticality and exposure, it's time to take action. This is arguably THE most important step of the process – if you think critical infrastructure is in jeopardy, the right parties need to know. As soon as you have your findings documents, you'll want to contact the owner or authorities in the served location and let them know about the exposure. You can find more information on how to report a vulnerability below! If you're able to, recommend remediation with the host owner or authorities to make the asset less publicly accessible and/or to increase redundancy of the asset's functions. After all, sharing what you know could help keep the infrastructure safe from bad actors going forward.

Wrap-Up

And just like that, you've played a part in helping to keep the ever-important world of critical infrastructure a little safer. All it takes is deciding where to start your search, using simple queries on the Censys Search tool, and following your sleuthing instincts to dig deeper into suspicious host activity. And with convenient document tags and comment features, you can make sure that you capture all of the right details from your findings, and even share them with other members of your security team. Most importantly, you'll have a concrete trail of evidence you can point to when you alert the host owner or agency of an exposure. How's that for a day's work?

Chef's Note

To report an ICS, IoT, or medical device vulnerability, please email central@cisa.gov or call 1-888-282-0870. When sending sensitive information to the CISA via email, we encourage you to encrypt your messages. Download the CISA ICS public key.

For more questions on this topic or CISA in general, please contact Central@cisa.gov. To report anomalous cyber activity and/or cyber incidents 24/7 email report@cisa.gov or (888) 282-0870. To report an IT Vulnerability, please use this form: https://www.kb.cert.org/vuls/report/

APPETIZER RECIPE

Sausage Stuffed French Bread

Since we've been focused on critical infrastructure, let's draw inspiration from an appetizer with an infrastructure we could also say is "critical" to its success as a party favorite. This dip recipe forgets the traditional serving bowl approach and instead nestles its spicy sausage and cream cheese filling within the soft and toasty walls of an extra-wide loaf of French bread – an infrastructure meant to be enjoyed with the dip it contains. Bake your French bread to golden perfection and let this hearty appetizer be the centerpiece of your next party spread. The bonus? No clean-up necessary; we can bet your loaf will be devoured by night's end.

PAIRS NICELY WITH
Discovering Critical Infrastructure
PAIRS NICELY WITH

Ingredients

- 1 wide loaf of French bread
- 1 pound breakfast sausage
- 2 ½ TBSP of jalapenos, chopped
- ½ cup green onions, chopped
- 1 cup green peppers, chopped
- 8 oz package of cream cheese
- 8 oz sour cream
- 8 oz cheddar cheese, grated
- 1 ½ TSP of New Orleans Cajun or Creole seasoning
- Tortilla chips

Recipe

1. You know the drill - let's preheat that oven. You can set yours to a standard350 degrees Fahrenheit.
2. While your oven heats up, take your extra-wide loaf of French bread and lengthwise, cut the top quarter off of it. Hollow out the center until the loaf's walls are about a half-inch thick. Set aside for now.
3. Next, brown the sausage in a medium skillet and break up any clumps.
4. Add your vegetables to the skillet (jalapenos, green peppers, green onions) and let them cook for about 5 minutes, stirring occasionally.
5. Next, add in your cream cheese, sour cream, and cheddar cheese right into the skillet and stir until melted.
6. Now it's time to add in your seasoning (for those looking for an extra kick, add in another dash).
7. Take your French bread loaf and fill it with the sausage-cheese mixture.
8. Next, place the loaf on a cooking sheet and let it bake for about 45 minutes, or until the loaf is crusty on the outside and the dip is warm.
9. Now it's time to enjoy: gather your tortilla chips for dipping and dig in! Once you've made it through the chips, use pieces of the bread loaf itself to finish off the remaining dip.

Identifying a Russian C2 Network Using Censys Search

Here at Censys, we recently found a Russian ransomware group just casually hanging out on the internet. Normally, to find and investigate cyber threats, researchers have to rely on the artifacts of a cyber attack, like clues left behind at the scene of a crime. We found this group by simply keying in on suspicious software (Metasploit - a widely available exploit tool) on hosts, narrowed down in Russia. Initially, this is like finding a van with burglary tools inside: not conclusively indicative of a crime, but enough suspicion to keep digging.

So dig we did - and eventually found two Russian hosts with more specific malware and tools, as well as direct ties to two other Russian Bitcoin hosts, along with historical evidence of the malware kits outfitted with direct links to the MedusaLocker group, as disclosed in CISA Alert (AA22-181A). This is like finding a copy of a ransom/robbery note in a criminal's apartment along with the bank accounts they use to deposit their spoils and all of the tools needed for a robbery.

After considering the evidence, we think our findings on these Russian hosts can be considered either a "smoking" or "loaded gun." What's even more significant: if it is the latter, that means we may have found these hosts before they could launch another attack. And in doing so, we've landed on a technique that will allow cyber investigators to proactively hunt cyber criminals. Just how did we go about our investigation? Read on for a recipe you can cook up to find ransomware on your own.

Query Ingredients

- 4,779,321 Russian hosts
- Access to search.censys.io

Query Recipe

1. Where to begin when looking for signs of ransomware? It helps to start with a location of interest. In our case, we felt Russia could be a good jumping off point, given recent geopolitical and current events. Once you know where you want to look, jump into the Censys Search tool (search.censys.io) and conduct an initial search for all the hosts that are located in your country of interest (in our case, Russia). Your query should look something like this: `location.country= `Russia``

2. Next, using the Censys "Report" function, show the top 1000 software products available on all hosts in Russia that Censys sees. This will be built off of the previous query. Your query for this step should look like this: `Report: location.country= `Russia` + services.software.product (1000 results)`

3. You'll now want to think about the type of exploit tool you want to search for. When it came to our investigation, we set our sights on Metasploit. This is an exploit tool used by penetration testers and other hackers, which is why we felt it would be a worthy lead into a ransomware investigation. We selected Metasploit software from the results of the previous Censys report. This will show all hosts in Russia with Metasploit on them that are available for connection and, therefore, available for an attack. Query: `(location.country= `Russia`) and services.software.product=`Metasploit``

4. From here, you'll want to search for all hosts in the world that Censys observes as matching the Deimos C2 (this is a Command and Control tool that's used by penetration testers and hackers to automate management of compromised hosts) JARM TLS fingerprint. Query: `services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687`

5. Then, generate a historical snapshot of your original host in question – in our case, Russian Host A (our prime suspect) –) with Metasploit and Deimos C2. This is where

Query Recipe Continued

you'll really want to put on your detective hat as you look for anomalies in the host from this historical view. What seems out of place? Are there certificates that appeared suddenly on the host, but then disappeared just as quickly? In our case, we came across the certificate of another C2 tool - Posh C2 (removed and replaced with Deimos C2). You can see what our query turned up here: PoshC2 certificate discovery on 30 May 2022 on Host A

6. The search doesn't stop here. With whatever unusual host activity you uncover from your own historical view, you'll next likely need to dive a layer deeper. In our investigation, the discovery of the PoshC2 certificate was a key turning point, and it led us to search for all hosts in the world that Censys observes presenting the PoshC2 certificate.

As a result of this search query, we discovered two MORE Russian hosts (which we called Hosts F and G) with malware packages, domain links to CISA Alert AA22-181A detailing indicators of compromise (IOCs) for the Medusa Locker group, and IP addresses to Russian Bitcoin hosts I and J for ransomware payment. In other words, we landed on our ransomware, thanks to a proverbial jackpot of evidence that we were pretty confident could be considered very, very suspicious. You can check out what we uncovered here: `services.tls.certificates.leaf_data.subject_dn=`C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077`

Wrap-Up

There's no "secret sauce" to our findings. Any threat hunter can follow our recipe on their hunt for ransomware and other nefarious activity. We simply explored the Censys worldwide, 24/7 scan dataset, while keeping a sharp lookout for suspicious findings like the penetration testing tool "Metasploit " and the presence of "C2" (Command and Control) software.

We then dug deeper in time with our History tool, while corroborating our findings through external sources like Google to confirm our suspicions. Since Censys interacts with every publicly-facing host on the internet, we can see not only which software and configurations hosts are currently running, but what they were running in the past (it's kind of like having our very own time machine), and pivot for similar, suspicious items like C2 tools, to see where else in the world they are being used.

In the same way analysts might use satellite imagery to detect a Russian tank on a Ukrainian border, and then judge the movement from one orbit to the next, so too can we leverage our global scan points to learn more about the disposition and changes of hosts over time, and with that info – locate vulnerabilities or hostile actors BEFORE they act. And that's a pretty handy threat hunting recipe to have in your back pocket, if you ask us.

MAIN COURSE RECIPE

Tender Beef Rouladens

Now that your search for foreign ransomware is complete, let's stay in the region and set our sights on a delicious favorite from Germany. As with our ransomware expedition, this traditional German dish also has an unusual ingredient that requires a little "digging in" to uncover. Wrapped tightly within the rouladen's juicy layers of beef and bacon you'll find slices of the tangy (and sometimes divisive) pickle. At-a-glance, you might not suspect this crunchy ingredient would be burrowed inside such a tender exterior; but as with ransomware, we know things aren't always as they seem! Warm up on a chilly winter's night with this hearty suppertime staple – and be ready to surprise and delight your guests with your rouladens' briny interiors.

PAIRS NICELY WITH
Identifying a Russian C2 Network
PAIRS NICELY WITH

Ingredients

- Slices of thin, top round beef (about ¼ of an inch each). They should be about the size of a 4x6 photo.
- The same number of slices of thick-cut smoked bacon
- Dill pickles
- 1 chopped onion
- Salt and black pepper
- 1/3 cup brown mustard
- 1 TBSP butter
- 1 TBSP olive oil
- 1 clove of garlic, minced
- 2-3 TBSP water dissolved in ¼-½ cups water
- Toothpicks

Recipe

1. We'll begin by getting a crockpot set up in your cooking space and setting to slow cook.
2. Next, lay out your beef slices on a cutting board and spread a thin layer of your brown mustard, salt, and pepper atop each.
3. Next, place one strip of the thick-cut smoked bacon lengthwise in the center of each beef slice.
4. Add your slices of pickles (also lengthwise) and your chopped onions.
5. Roll up each slice and secure with toothpicks (usually 2-3 toothpicks are needed).
6. Generously add oil to the crockpot so that it coats the entire bottom of the pot., Place your rouladens within and cover with the lid. It's time to let these rollups get nice and tender!
7. Your rouladens will need to cook for about four hours on slow heat. It's not a bad idea to check in halfway through to turn them and add a half cup of water (if you think they're looking a little dry).
8. Once four hours have passed and your rouladens are looking nice and tender, it's chef's choice on the final touches: maybe you want to add in a dash more salt, pepper, or oil to round them off.
9. It's now time to remove your rouladens from the crockpot, plate, and enjoy!

Pro tip: Consider removing 1 or 2 of your toothpicks from each rouladen before plating or biting in. While helpful for holding everything together during the cooking process, the toothpicks might pose an obstacle when sitting down to eat.

Finding Hacked Web Servers

So far we've covered recipes on some pretty juicy corners of the security world: compromised critical infrastructure, ransomware lurking on foreign hosts. But now let's switch things up and turn our attention to a recipe that deals with an all-too-common aspect of cybersecurity: the hacked web server. According to the 2022 Verizon Data Breach Investigations Report, web servers are the asset most commonly impacted in breaches. This isn't exactly surprising given that web servers typically make up the bulk of an organization's internet-facing infrastructure, and are therefore more likely to be exposed than other types of digital assets. Translation: hacked web servers are common and easy points of entry for bad actors.

Finding hacked web servers can be useful for a number of reasons:

- Defenders can track threat actors as they're working, meaning they can quickly locate the affected hosts and immediately take action before any further damage is done.
- Researchers can track insecure servers and monitor trends in adversary behavior and methodology, learning from these attacks in order to hopefully prevent similar future attacks.

Whether defender or researcher, you can identify hacked web servers quickly using straightforward queries on the Censys Searh tool. Let's show you how.

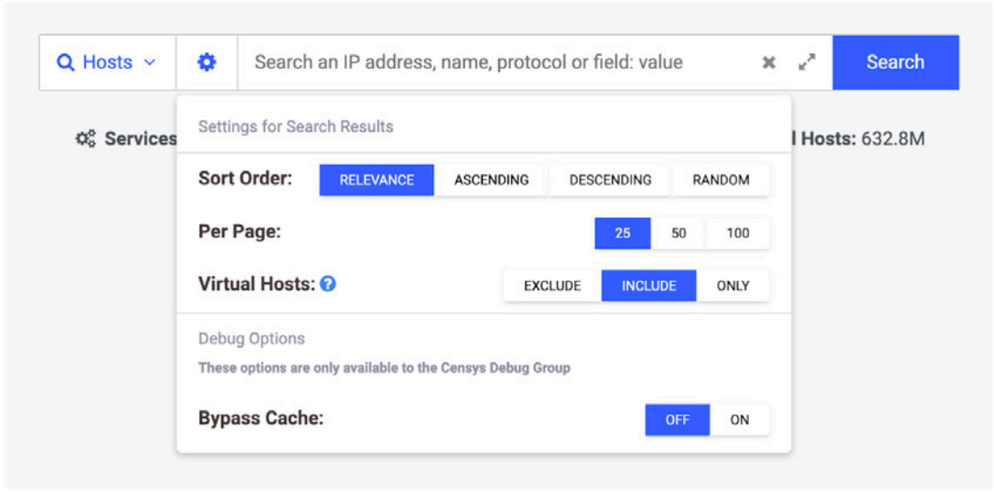
Query Ingredients

- Access to search.censys.io
- A hacking goal: are you a defender or a researcher?

Query Recipe

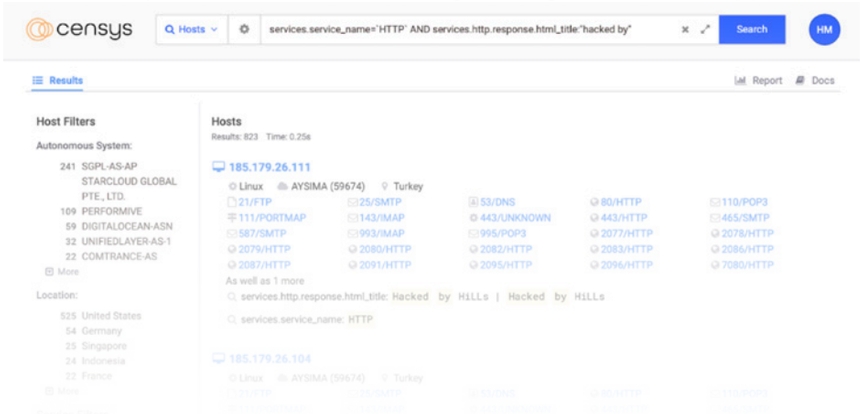
1. We'll begin with one of the simplest ways to find defaced web servers: searching for the string "hacked by" in the Censys Search tool. Threat actors commonly "sign their work" by leaving a message on a website, such as "Hacked by [actor handle]." Luckily these signatures help defenders and researchers who are hunting for affected web servers. We can use Censys to search for these affected sites all over the world simply by looking for defacements. Hackers might think they're being cheeky leaving their calling cards, but for folks like us who have the right data and tracing tools at their fingertips, these calling cards give away more than hackers might realize.

2. Our simple query will restrict results to Censys-visible HTTP servers that include the string "hacked by" on their web interface. We can include virtual hosts in these search results by first toggling the gear icon on the search homepage and selecting "Virtual Hosts: Include" as seen below.



Query Recipe Continued

3. Next, we can run our search by typing in this query and clicking "Search": services.service_name='HTTP' AND services.http.response.html_title:'hacked by'. This will grab all Censys-visible hosts running HTTP, regardless of which TCP port it's running it on. Based on the search results that come back and the highlighted text, you can immediately see that we're uncovering some gems with this approach!



4. We can narrow down these results further based on what we're interested in. Some additional filters you may want to add in specific use cases include:
   - If you run a network (for example a university, a hosting company, or an Internet Service Provider) or need to triage reports for your clients, you can constrain this query.For example, if you work at a national CSIRT organization you can filter by the "location.country" attribute (e.g. just add "AND location.country: [your country]" to the above query).
   - If you're working for a state government and helping your organization identify successful hacking events, you can filter by the "location.city" attribute.
   - If you're running an Internet Service Provider, you can filter by your autonomous system number using the "autonomous_system.asn: [your asn]" attribute. Using the API you can make these calls on a regular basis and keep updated as we find these servers.

Defender Flavor

For Defenders: What to do if you find hacked servers tied to your organization?

Let's say you've just discovered you've been breached, so you're in defense mode. If you're doing damage control, you have a bit of a challenge ahead of you. However, there are a lot of helpful guides and tools from people who've been in your shoes before (and there are many who have). Let's take a look at how you might go about finding these servers in defense mode, using helpful resources along the way.

1. Initially, you'll need to remove the problematic content, restore the site from a backup, close security gaps that you've uncovered after tracking the attack(s), and add some security tooling around it in order to prevent future issues. Ideally, you'd want to react by reinstalling your breached systems onto an updated, secured platform, but we realize that's very often not a realistic option for most companies. **As Censys never attempts to gain access to any of the hosts across the internet (we strongly believe in good internet citizenship), we don't collect any data on how a server is hacked.**

2. However, Censys data can help you identify the possible routes that a bad actortook to access your system. An example would be that perhaps an attacker left FTP on, which you would be able to see with a bit of forensic analysis. This creative analysis is key so that you can determine what happened to close the security gap and prevent it from happening again. Censys can give you the critical visibility into Internet-exposed services that you need in your threat hunting efforts and help you find attacker trails and behaviors in order to track, pivot, and protect your organization.

3. Without the knowledge that you have hacked web servers tied to your organization, threat actors could continue damaging your systems for years to come. So even though finding that you've been affected by adversaries can feel like a defeat, you've still done the work to locate those problematic hosts and address the security gap before it gets any bigger. And in our book, that's something to give yourself credit for!

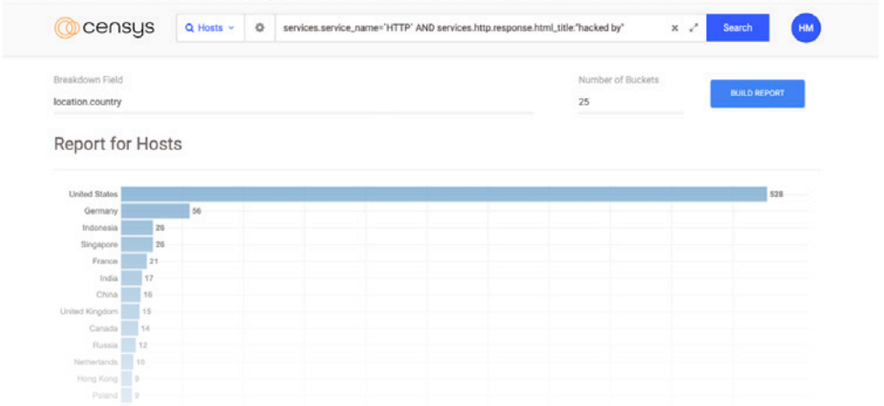
Researcher Flavor

For Researchers: What to do if you're trying to discover and track trends across the internet?

If you're a researcher, the types of security trend data you can uncover in Censys can be highly useful for existing research projects and for brainstorming new projects. Data from our Search tool can help bring an entirely new perspective to your efforts.

1. A suggested first step is to begin exploring interesting Internet-wide security trends by analyzing data on a global scale with Censys searches, relying on our report builder function.

2. Let's build a report from the search results we uncovered earlier, aggregating by the country each web server is hosted in using the "location.country" field. We can make the data more or less granular by adjusting the "Number of Buckets" field.

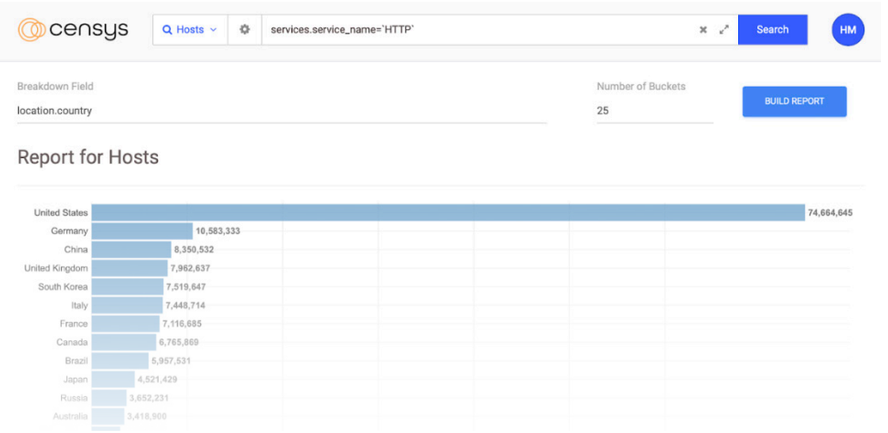


This report reveals that the United States dominates, with 3.46% of hacked servers hosted in the U.S.

But this chart on its own is misleading. If all you were to do is to take those results at face value and make interpretations around it, you'd likely draw some false conclusions. An important distinction to make in this report is that hosts aren't distributed evenly around the world. The U.S. hosts a good deal of the IPv4 address space, so this trend data may be unfairly skewed toward that country. Think about it this way: if two countries each have 20 servers reporting "hacked by", but the first country has 100 servers and the second has 10000, that's a 20% rate vs a 0.2% rate of "hacked by" instances.

3. What you'll want to do from here is start adding context into the picture. In this example, we'll tie together two sets of results from Censys:

   - The number of HTTP servers with the string "hacked by" by country
   - The number of total hosts running HTTP by country (see the figure below)

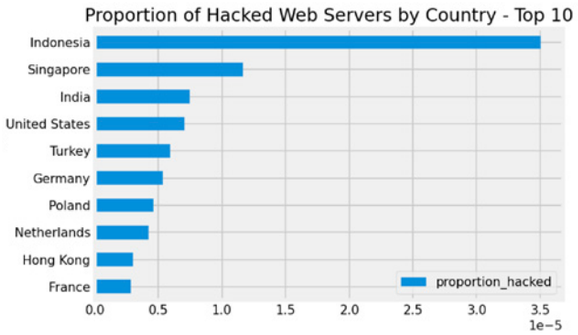


When we scale the "hacked by" values (the first data set) by the number of web servers in each country (the second set), filtering out countries where the former value is trivially small (n<5), we see a different picture.

Researcher Flavor Continued

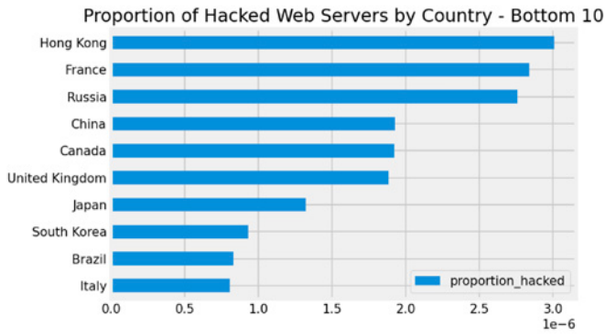
Tables 1 and 2 break down the top 10 and bottom 10 instances of "hacked by" per capita web servers for those countries. Surprisingly, Indonesia leads the pack as a percentage of population at a rate of about triple the second-place country Singapore, but that may be due to the smaller web server population in that country compared to Singapore.

Table 1: Top 10 Most Affected Countries per Capita Web Servers



Italy, by contrast, has the lowest rate of defaced web servers from our perspective. It's interesting to study various factors that may explain these findings, which may point to the opportunity for a broader study.

Table 2: Least 10 Affected Countries Per Capita Web Servers



4. These data points can lead us to a larger question: what attributes, regulations, and social trends could potentially impact why Indonesia or Iceland, for instance, would have more hacked websites per capita than other countries? As you can imagine, internet data alone isn't enough to demonstrate causation, but it can be used to pull together interesting data trends to support a huge variety of research projects.

Wrap-Up

There's so much to explore and uncover in the world of internet data, and this recipe is just one way to get to the bottom of a particular, all-too-common corner of it.

And whether you're a defender or a researcher, when it comes to gathering intel, it's all about having access to the right tools so that you can act quickly and confidently. With a tool like Censys, there are endless possibilities to get creative with your future investigations, whether they're related to hacked web servers or any number of other areas of interest. Happy searching!

MAIN COURSE RECIPE - MADE TWO WAYS

Tikka Masala Tater Tot Hotdish

Since you've been spending time thinking about "hacks," why not try a creative hack for a traditional casserole dish? The tater tot hotdish has long been a favorite in the American Midwest, often brought as a dish-to-pass at social gatherings and family events. Though it may not seem synonymous with gourmet, the tater tot hotdish does serve up a delightful combination of flavors that are the definition of "comfort food." Another great thing about this dish? It leaves ample room for interpretation. In this iteration of the tater tot hotdish, we'll draw inspiration from Indian cuisine with the addition of Tikka Masala simmer sauce. Swap the hotdish's traditional cream of mushroom with Tikka Masala simmer sauce for a bolder bite that brings original flavor and a little more spice. Like finding hacked web servers for both defensive and research purposes, you can also go about this dish two ways; choose the meat lover's option with ground turkey, or go the vegetarian route with hearty lentils.

PAIRS NICELY WITH
Identifying a Russian C2 Network
PAIRS NICELY WITH

Ingredients

- ¼ cup olive oil
- 1 yellow onion, finely chopped
- 1 pound lean ground turkey OR ¾ cup lentils (vegetarian version)
- 2 cups frozen green beans, thawed
- 1 ¾ cups frozen corn, thawed
- 1 cup chopped frozen broccoli, thawed
- ~20 oz of Tikka Masala simmer sauce
- 1 pound frozen potato tots
- Salt and black pepper

Recipe

1. We'll get started by preheating your oven to 350 degrees Fahrenheit.
2. In a large skillet, heat the olive oil on medium heat and add in your onions.
3. Stir occasionally until the onions begin to brown. This should take you about 15 minutes.
4. Once the onions are soft and starting to brown, add in your ground turkey and mix together. Season with salt and pepper as desired.
5. After the turkey is cooked through (it should look a little golden brown), pour your turkey and onion mixture into a 9x13 inch baking dish.
6. On top of the turkey and onion mixture, spread your thawed green beans, corn, and broccoli.
7. In this next step, we'll depart from a traditional hot dish ingredient (cream of mushroom soup) and swap in our Tikka Masala simmer sauce. Layer on the Tikka Masala until all of the surface is covered.
8. Round out your dish with a top layer of tater tots (still frozen).
9. Place your delicious, layered concoction in the oven and bake uncovered for 60 minutes, or until you see that the tater tots are crispy on top.
10. Let your hot dish cool slightly (no burnt tongues, here) and serve!

Vegetarian Option: Follow the same instructions as above but swap your ground turkey for lentils. As your yellow onions saute on the stovetop, rinse the lentils well in a colander and add to a pot with 3 cups of water. Bring to a boil, cover, reduce the heat, and let simmer until the lentils are tender. This should take about 15-20 minutes (about the same time as the onions). Once cooked, combine with onions and continue on with the remainder of the recipe.

TAKING THE NEXT STEP

Censys Attack Surface Management

Individual search queries like the ones we've just shared recipes for are great ways for to dive deep into specific areas of threat detection. However, you might be looking for a complement to individual query efforts – perhaps something like an automated, scalable threat detection solution? If you're not already familiar, allow us to introduce you to Attack Surface Management.

Just what is Attack Surface Management (ASM)? ASM solutions are great because they continuously monitor and identify assets across the entirety of your attack surface, including assets tied to your organization you didn't even know existed. ASM is a proactive approach to threat detection and remediation that helps you see your attack surface from an attacker's point of view, while also helping you increase efficiency and control the costs of cloud sprawl and Shadow IT. The Censys Attack Surface Management Platform happens to be the industry's leading solution, because we serve up a comprehensive profile of internet assets, and empower defenders like you with the visibility and the insights they need to stay ahead of bad actors.

Companies of all sizes turn to Censys Attack Surface Management for proactive threat detection they can trust. What could your security team expect when they join the Censys community? Read on for our seamless customer onboarding recipe!

ASM Ingredients

- 1 kickoff call
- 2-3 training sessions
- 1 Censys Academy & support docs
- 1 cloud connector
- (Optional) 1SAML & 1 ticketing system

ASM Recipe

1. Start by gathering your Censys contract and signing off on your "ingredients" from the list above.
2. You'll want to get things "preheating" with your sales contact by providing a few important points of information, including your team's top attack surface priorities, success metrics, and the key stakeholders who should be involved in the onboarding process.
3. Next, launch your newly-formed partnership with a top-notch kickoff call, led by your Censys Customer Success Manager (CSM). Be sure to have any relevant key stakeholders from your organization attend the call as well.
4. Once your kickoff call is complete, fold in 2-3 training sessions provided by your Censys CSM that are focused on platform overview, technical integration questions, and additional documentation. You can also access more information about these topics at any time from Censys Support Docs and the Censys Academy.
5. Once your first training session is folded in, you'll next want to stand up your cloud connectors and integrations. Carefully make sure that each piece is connected, working, and integrated. Additional training sessions can be folded in once this is completed. The above steps complete your onboarding and integration portion with Censys!
6. To further gauge your enterprise adoption, you'll want to monitor your instance of the platform for at least 90 days to make sure it's the right consistency (i.e. – everything is set up in a way that best meets your organization's needs). Log in to check on your attack surface daily to ensure correct seeds are listed and that critical/high risks are remediated. This will be a key time to clean up any dirty dishes and prep for the next

ASM Recipe Continued

step. If seeds are present and they shouldn't be, please be sure to remove them or tag accordingly.

7. Your Censys CSM will periodically check in with you to inquire about the status of the attack surface work previously completed. It's important that you lean into their partnership to answer any questions you have or provide additional support.

8. After your first 90 days on the platform have passed, you'll meet with your Censys CSM to review your platform usage, workflows, and key use cases to be measured. At this time, your attack surface is ready for the final step: reporting. This can be done by selecting "reporting" at the top of the platform's console. Once reports are generated, feel free to make adjustments to your attack surface based on the trends you obtain from the reports.

Wrap-Up

The Censys onboarding process is designed to ensure that joining the Censys community is as seamless as possible. Who likes complexity anyways? Not us. That said, onboarding can also be as customizable as you need it to be. Need an extra training session? Want to learn more about a specific feature that's particularly relevant to your users? That's what our Customer Success Team is here for! The Success Team is also committed to optimizing your Censys experience well beyond the onboarding process; we're here for you as your team's needs evolve, as our platform evolves (we're always working on exciting new features), and as critical risks and vulnerabilities are uncovered that require you to take action. Know that atCensys, we're committed to partnering with you on your attack surface management efforts on an ongoing basis.

DESSERT RECIPE

No-Bake Cookies

In the spirit of keeping things easy and minimizing effort, let's end on a note of supreme simplicity. The no-bake cookie is the minimalist baker's dream: just a few common baking ingredients you'll likely already have on hand and a cookie sheet. For this recipe, you don't even need to turn on your oven! Like onboarding to the Censys ASM platform, once you've provided the key ingredients, you can let the cookies do the rest on their own – and spend your time focused on more pressing matters at hand.

PAIRS NICELY WITH
Censys Attack Surface Management
PAIRS NICELY WITH

Ingredients

- ½ cup butter
- 1 and ¾ cup sugar
- ½ cup milk
- ½ cup unsweetened cocoa powder
- 1 TSP vanilla extract
- 2/3 cup peanut butter
- 3 cups quick oats

Recipe

1. Get started by lining your cookie sheet with parchment paper so you have that ready to go when the time comes.
2. Next, combine your sugar, cocoa powder, butter, and milk into a saucepan and turn to medium heat on the stove. Stir this often, and raise to a boil.
3. Once you've reached a boil, let the mixture bubble for a full minute without any stirring.
4. Remove the saucepan from your stovetop, place on a safe surface, and add in your oats, peanut butter, and vanilla.
5. Stir together until all of the oats and peanut butter are fully folded into the mixture.
6. Next, use a large spoon to scoop the mixture into balls and place onto your parchment paper. How big you make your cookies is of course up to you, but just keep in mind that they will spread slightly, so be sure to keep some distance between them on the tray.
7. Let your cookies set out at room temperature for about 20-30 minutes. Your cookies should be firm on the outside. (If they're not, let them continue hardening).
8. Remove your cookies from the parchment paper and voila! You have an indulgent treat ready to devour.

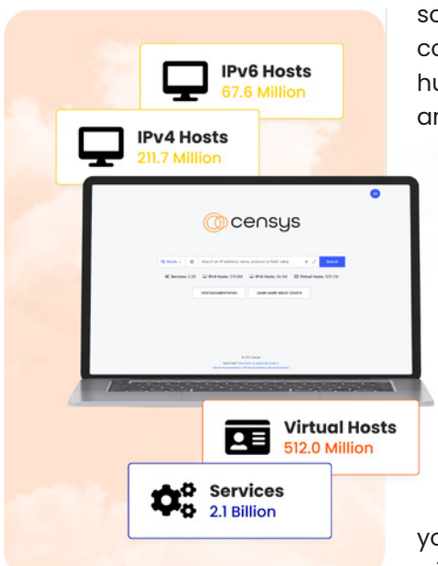
HUNGRY FOR MORE?

About Censys Search

There are endless query recipes to explore with Censys! Get started on our community version of Censys Search (free to the public) at search.censys.io, or request a demo to learn more about how companies of all sizes benefit from Pro, Pro Plus, and Enterprise user packages. We can't wait to see what you "cook" up!

What is Censys Search?

Give your security program access to the best internet intelligence on the market with Censys Search. Our global scanning infrastructure collects information on more of the internet (and at a higher frequency) than any other tool, and our ground truth scan data is enriched with multiple internal and external sources to provide complete context on each asset's configuration and level of exposure. And, your threat hunting exercises can become more pointed with an easy-to-use query language and 1500+ parsable data fields, giving you the flexibility you need to locate attack infrastructure, write risk detections, and identify compromised hosts.



Censys Search also continuously scans 101 protocols across the top 3,500+ ports on the full IPv4 address space and the top 100 IPv4 ports daily (that's 2x more than the nearest competitor) to produce a high-resolution map of the public internet, providing best-in-class visibility to threat hunters, attack surface managers, and other security professionals. With Censys Search, your team can understand and investigate threats with greater accuracy.

Why is Censys Search Superior?

- **Structured data and advanced search**: Find structured data with detailed information that's indexed and searchable about each protocol and certificates associated with hosts. Ingest data into whichever workflows already exist within your organization, whether you're leveraging the UI or API.
- **More internet hosts and services:** Automatic protocol detection, through which Censys identifies services independently of ports, means your team will have visibility into services running on non-standard ports.
- **Multi-perspective scanning:** Censys data gives you visibility into 99% of active IPv4 hosts on the internet, thanks to scanning from five Tier-1 service providers from separate locations around the world.
- **Detailed historical host data:** All users have access to historical data via UI and API, with significantly more detailed information than our competitors.
- **Fast lookup API:** Utilize Censys data programmatically via the Censys API, which provides detailed information about current or historical assets.

Learn more about Censys Search at: https://censys.io/data-and-search/

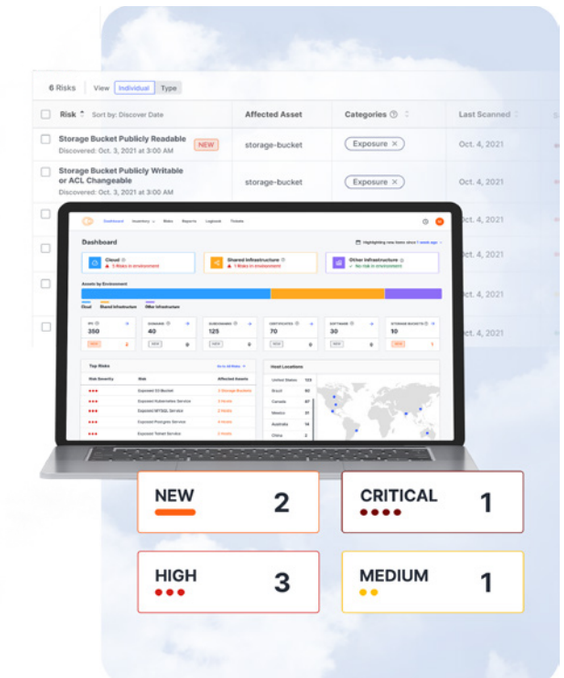
HUNGRY FOR MORE?

About Censys Attack Surface Management

What is Censys ASM?

Did our bonus recipe on automated Attack Surface Management catch your attention?

Attack Surface Management is a proactive cybersecurity approach that provides automated asset discovery, management, inventory, and risk prioritization across your organization's entire attack surface. It's a way to gain a comprehensive view of everything your organization owns on the internet, and see it all from an attacker's point of view so that you can better protect and defend against threats before they occur.



What Makes Censys Attack Surface Management the Leading Solution?

- **Daily Asset Discovery:** Achieve near real-time visibility with daily updates to your attack surface.
- **Asset Inventory:** Search across your attack surface data with the agility and accuracy of a threat hunter leveraging 1400+ parsable data fields.
- **Cloud Connectors:** Get total visibility in the cloud and keep up with changes by the hour.
- **Rapid Response:** Understand your overall exposure to zero-day and headline vulnerabilities in minutes instead of days or weeks.
- **Click to Rescan:** Rescan any asset for its known services to "trust but verify" remediation work has been successful.
- **Logbook:** Keep track of 2 years of changes to each asset, or your attack surface as a whole.
- **End-to-End Customer Control:** Manage every data point in your attack surface without filing support tickets or billing professional services hours.

Learn more about Censys Attack Surface Management at: https://censys.io/attack-surface-management/

censys

The one place to understand everything on the internet.

For security pros who protect the organization, Censys is the best at finding exposures attackers will exploit. Our industry-leading Internet scanning platform and >9.1B certificate database (the world's largest) enable us to provide 63% more service coverage than our nearest competitors. Founded by the creators of ZMap, at Censys we've made it our mission to make the Internet a more secure place for everyone.

hello@censys.io
www.censys.io