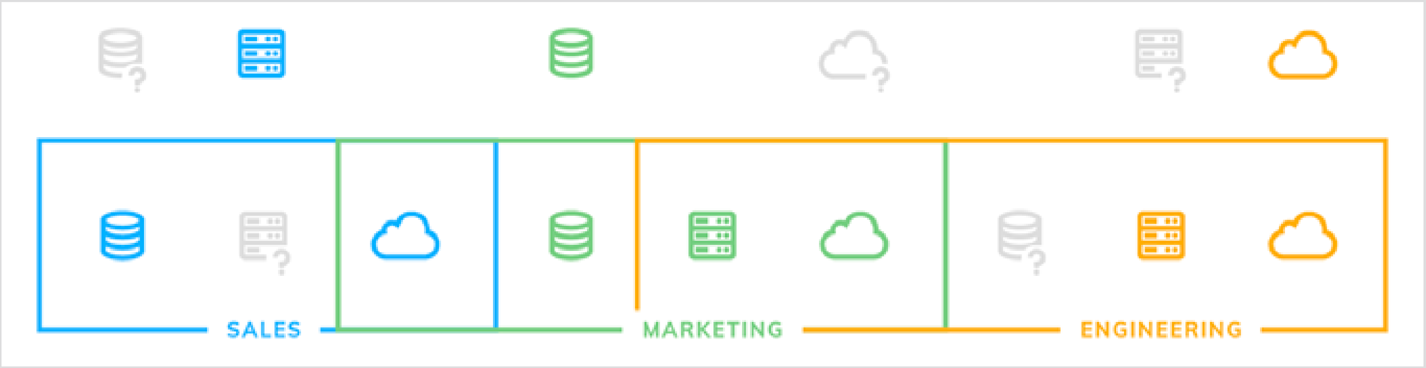
Why Internet Data Should be a Part of Your Security Strategy

censys

Censys.io

An introduction to protecting organizations with Internet security data

Censys provides access to 3 types of data sets: IPv4 Data, Certificate Data, and Alexa top 1M domains. With Censys Enterprise you'll have access to over 1,000 IPv4 ports, offline access, and flexible use for results returned per search.



It's not uncommon for business units to acquire infrastructure and cloud services outside of their organization's official IT processes

Today, protecting an organization requires both continually finding and monitoring traditional networks and external assets in close to real time. To protect distributed resources, proactive security groups have turned to Internet-wide scanning and other datasets that describe Internet host behavior. Internet-wide scanning is the process of connecting to and analyzing every known IP address, providing a global perspective of security data across the Internet.

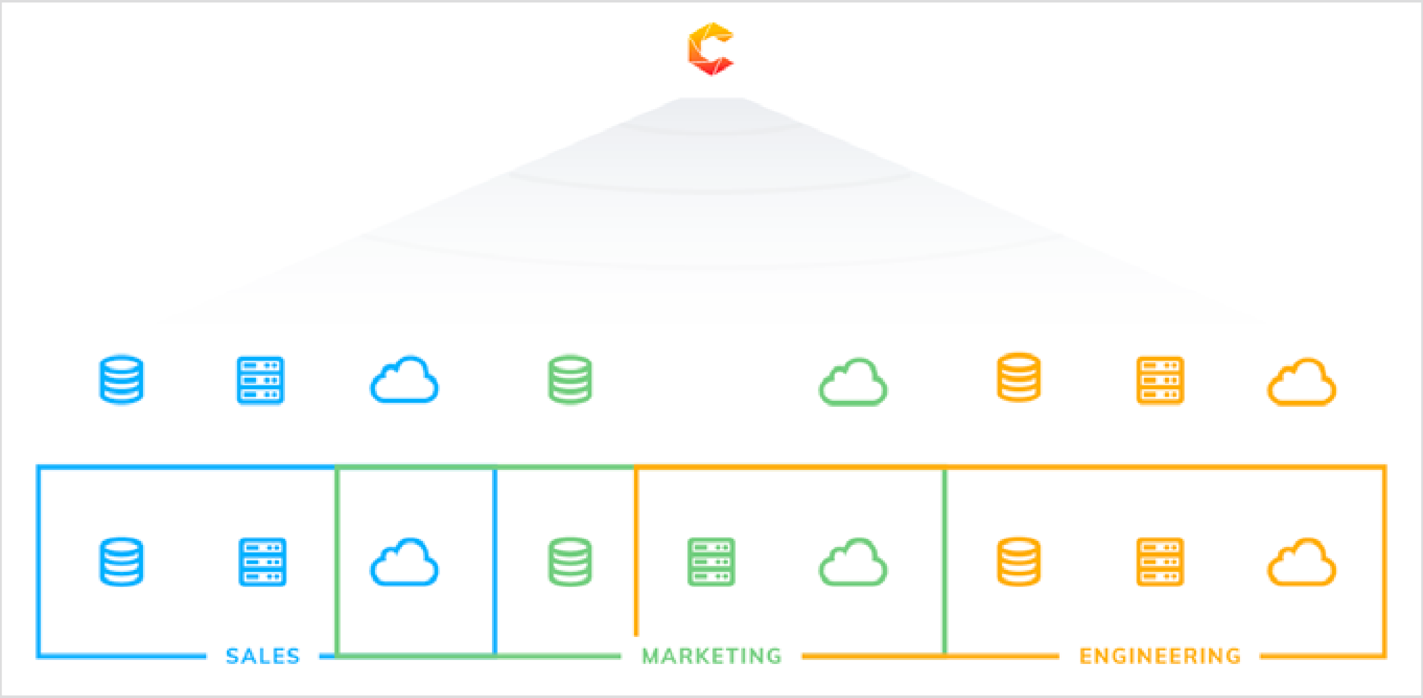
Previously, Internet-wide scanning was mostly used by security researchers and hackers to understand vulnerabilities at large scale, in order to track trends, malware behavior, and the time it takes administrators to patch vulnerable software. However, now that organizational assets are no longer contained within a single network, Internet-wide scanning can be used to provide the global perspective needed to find and protect assets outside of traditional network boundaries.

In the 1990s, many administrators performed basic network scans to identify servers and devices on their corporate networks. Those tools are reliable for scanning small, private networks to locate vulnerabilities and misconfigurations. However, thanks to virtualization, cloud, and data center advancements, well-defined networks have become a thing of the past.

Where it used to be possible to know everything on a corporate network within those limited borders, a new challenge has emerged in asset and infrastructure management. Today, some of the most important and most vulnerable assets are externally hosted, but contain sensitive data and pose a risk to organizations.

Over the past decade, security researchers have developed tools that make Internet-wide scanning practical. They have also published data created from network scans for systems administrators, allowing them to query for assets they may not have otherwise known about. With these new tools, researchers and systems administrators alike were able to query the Internet for certain types of devices, locate vulnerabilities worldwide, and understand the attributes of every device on the Internet.

This whitepaper explains the practical application of using Internet security data to help security professionals get a holistic view of all of their infrastructure — even devices and hosts that are not in known corporate networks — so they can locate potential threats and security gaps.



Censys and other Internet-wide scanners index every publicly accessible server on the Internet, which helps IT and security teams locate their organization's assets without needed to know where every server is physically located

How Organizations Use Internet Security Data to Defend Themselves

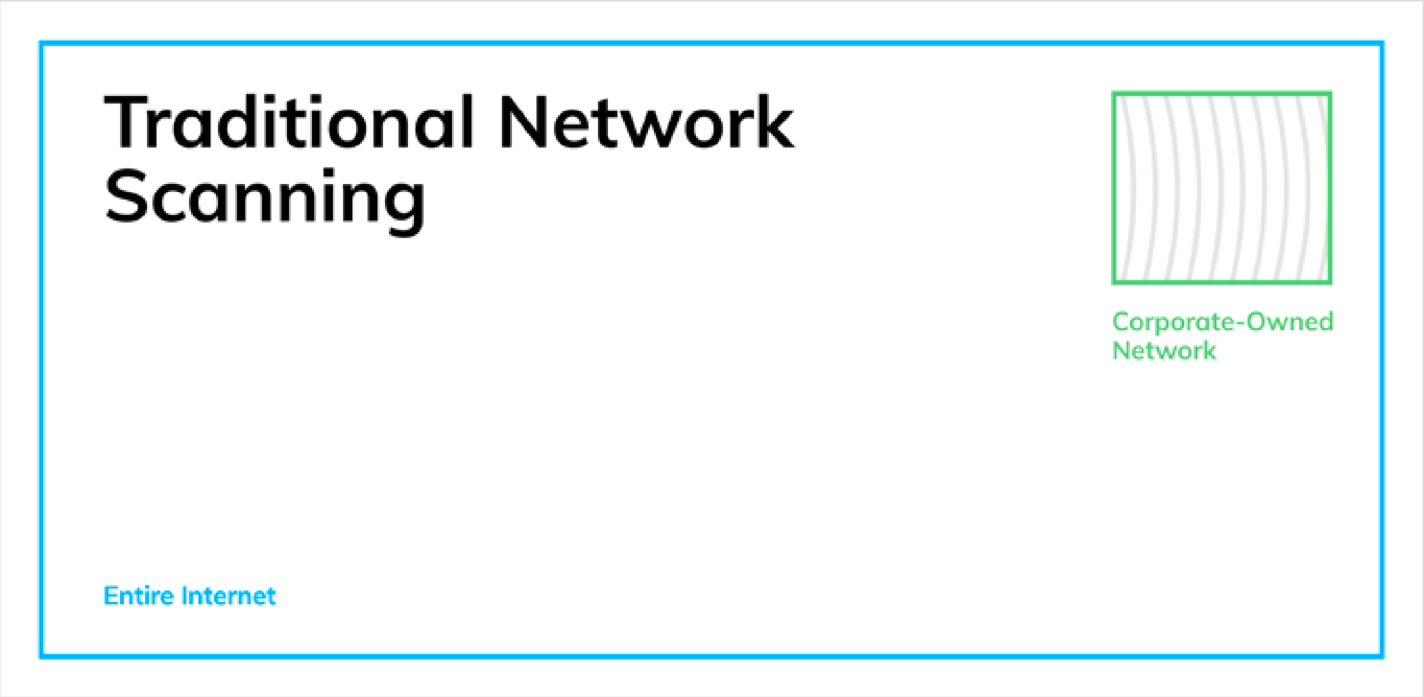
The advancements and usability improvements of Internet-wide scanning make it an appropriate tool for:

1. Infrastructure discovery and continuous monitoring
2. Preventing phishing and brand impersonation
3. Threat hunting to prevent targeted attacks

Infrastructure Discovery and Continuous Monitoring

Security administrators and IT teams often use Internet security data—especially Internet-wide scan and certificate transparency data—to locate vulnerable servers and to provide a complete view of Internet-facing assets. Network scanning has been advocated since the mid-1990s and is now part of compliance security checks, making its use a requirement for most organizations.

However, traditional tools only scan small, well-defined networks. They are not designed to find corporate data and assets exposed elsewhere on the Internet, such as those put there by employees operating outside of official IT procedures and audits, sometimes referred to as Shadow IT. As such, security teams have inherited the rather daunting task of securing every single domain and server used within their organizations, regardless of where they are hosted—or who in the organization setup the server.



Traditional scanning only finds assets on the networks explicitly specified by the organization

With many services living in the cloud and with distributed workforces and global office locations, this can be a particularly time-consuming challenge. It's easy for employees to simply add a server to the Internet in an effort to get a task done that they will often bypass the organization's process, often unintentionally. Unfortunately, each of those instances can pose a threat to the security of the entire organization unless they are known, monitored, updated, and secured. That's where Internet-wide scan data comes in—it offers those teams a quick, automated way to determine if any new corporate assets are made accessible on the Internet.

> Internet security data helps IT prevent attacks rather than being stuck in the unproductive cycle of reacting to attacks

Modern Network Scanning
Corporate-Owned Network
Entire Internet

Internet-wide scanning helps organizations find their assets across known and unknown networks

Continious Exposure Monitoring Complements Annual Security Audits

Many organizations rely on annual or quarterly pentesting audits to measure their security risk, maintain compliance, and uncover new risks. But adversaries are continuously scanning for weaknesses in that network—often finding targets within hours.

Now that data from Internet scanning services is readily available, security practitioners can get the value of “mini pentests” on a daily basis to understand their risk and secure their organizations against attacks in real time by patching vulnerable servers or taking them offline and locating attacker infrastructure before attacks are launched.

While volumes of data are available to collect on every single port, most analysts consume only high-level details to understand the entirety of their attack surface. One of the biggest challenges is making the determination of which areas and types of infrastructure warrant daily scanning and a bit of regular time from security analysts. Similar to how a security team might work with a pentesting organization to determine what the parameters of an annual audit would be, the goal is to pinpoint the areas most at risk and use limited resources (analysts and security team members) wisely.

A Comprehensive View of Known Vulnerabilities

When product security updates are released, or when a web server certificate is a month from expiring, think of a countdown clock starting. Those patches are public information and smart attackers know that they can use this information to determine that those unpatched versions are officially insecure until they're updated. The responsibility to update and secure those unpatched servers lies with the security and IT teams. Any help these teams can can get to quickly locate them to create a priority list is essential. Data from continuous scanning also makes it easier for organizations to analyze any changes that have occurred over time within their infrastructure, which could potentially flag a security vulnerability or otherwise signal that the team should investigate.

The reality is that threat actors are able to see everything on the Internet, too, so they know when software is losing security support, or when other defenses may be down. As an example, Censys researchers found that attackers began scanning for the Heartbleed vulnerability within 22 hours of its disclosure, hoping to exploit the bug and victimize organizations. To complicate this problem further, known vulnerabilities are often published before the vendor is able to offer a fix or patch to their users, leaving all those hosts open to attack until such an update is released.

> Threat actors began scanning for the Heartbleed vulnerability within 22 hours of its disclosure

Assets exposed to the Internet with known vulnerabilities are an easy target for attackers. Continuous monitoring not only helps IT teams identify unknown assets, but it can also be used to keep tabs on vulnerabilities and server software versions on known assets. This isn't a replacement for existing vulnerability scanners, but it can help prioritize what needs to be patched first.

How to Find Vulnerable Hosts that Require Immediate Updates

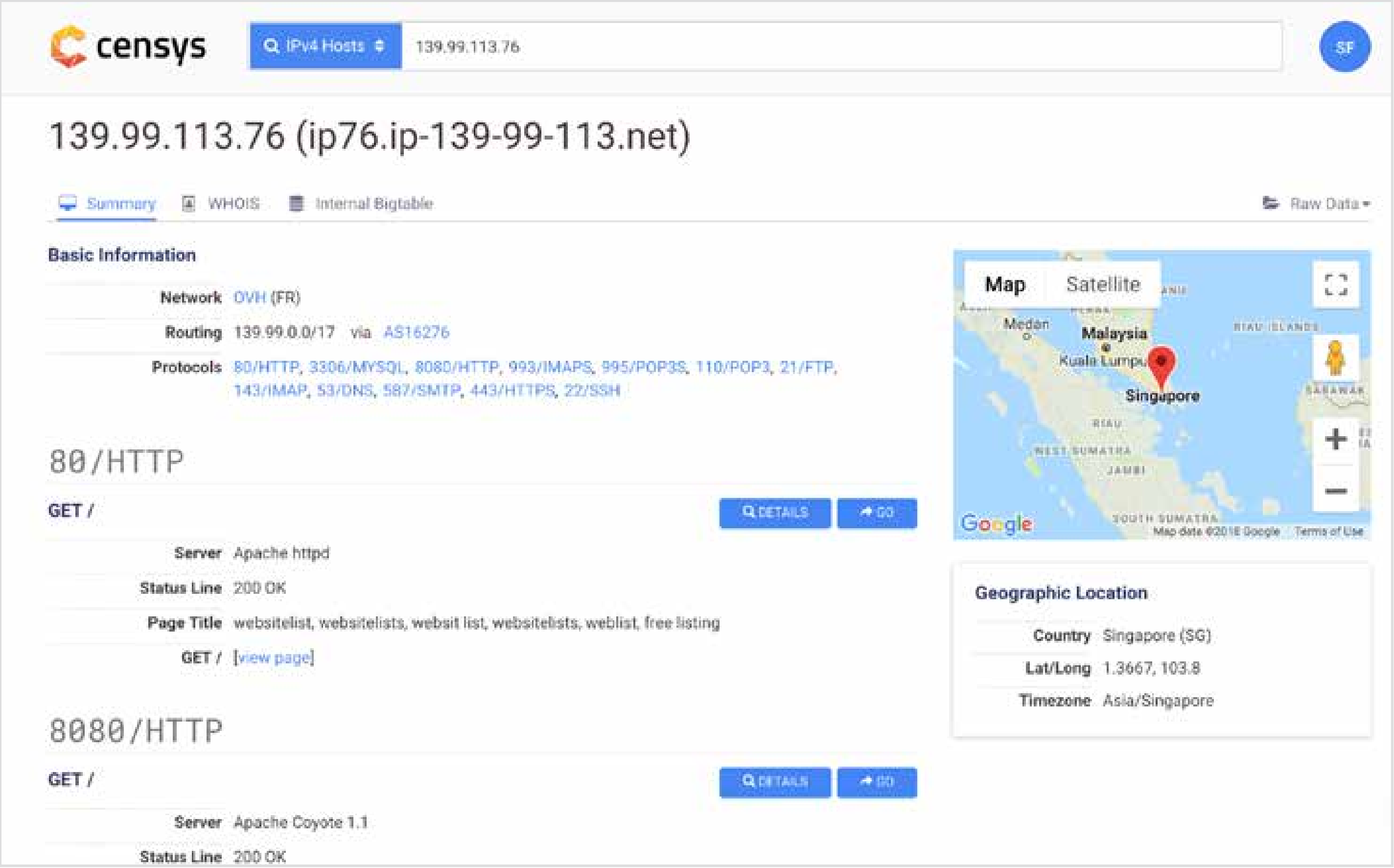
Another typical use case for security teams is to find software within their organization that needs patching or updating. Many security professionals subscribe to critical vulnerability and exposure

(CVE) feeds, which notify them immediately when a service is known as vulnerable to a specific type of attack or exploit. With that feed informing them, security professionals can find the affected software and version that's at risk and needs to be patched. Here's an example of how a systems administrator could find Apache Tomcat servers that are affiliated with their organization.

Censys IPv4 Hosts Search for Tomcat servers on the Internet

Then, filter the list down by replacing the following example ("ibm. com") with any domain name to only see Tomcat servers that might be associated with a particular organization:

Censys IPv4 Hosts Search: "you've successfully installed Tomcat. Congratulations" AND 443.https.tls.certificate.parsed.names: ibm.com



139.99.113.76 (ip76.ip-139-99-113.net)

Basic Information

Network OVH (FR)
Routing 139.99.0.0/17 via AS16276
Protocols 80/HTTP, 3306/MYSQL, 8080/HTTP, 993/IMAPS, 995/POP3S, 110/POP3, 21/FTP, 143/IMAP, 53/DNS, 587/SMTP, 443/HTTPS, 22/SSH

80/HTTP

GET /

Server Apache httpd
Status Line 200 OK
Page Title websitelist, websitelists, websit list, websitelists, weblist, free listing
GET / [view page]

8080/HTTP

GET /

Server Apache Coyote 1.1
Status Line 200 OK

Geographic Location

Country Singapore (SG)
Lat/Long 1.3667, 103.8
Timezone Asia/Singapore

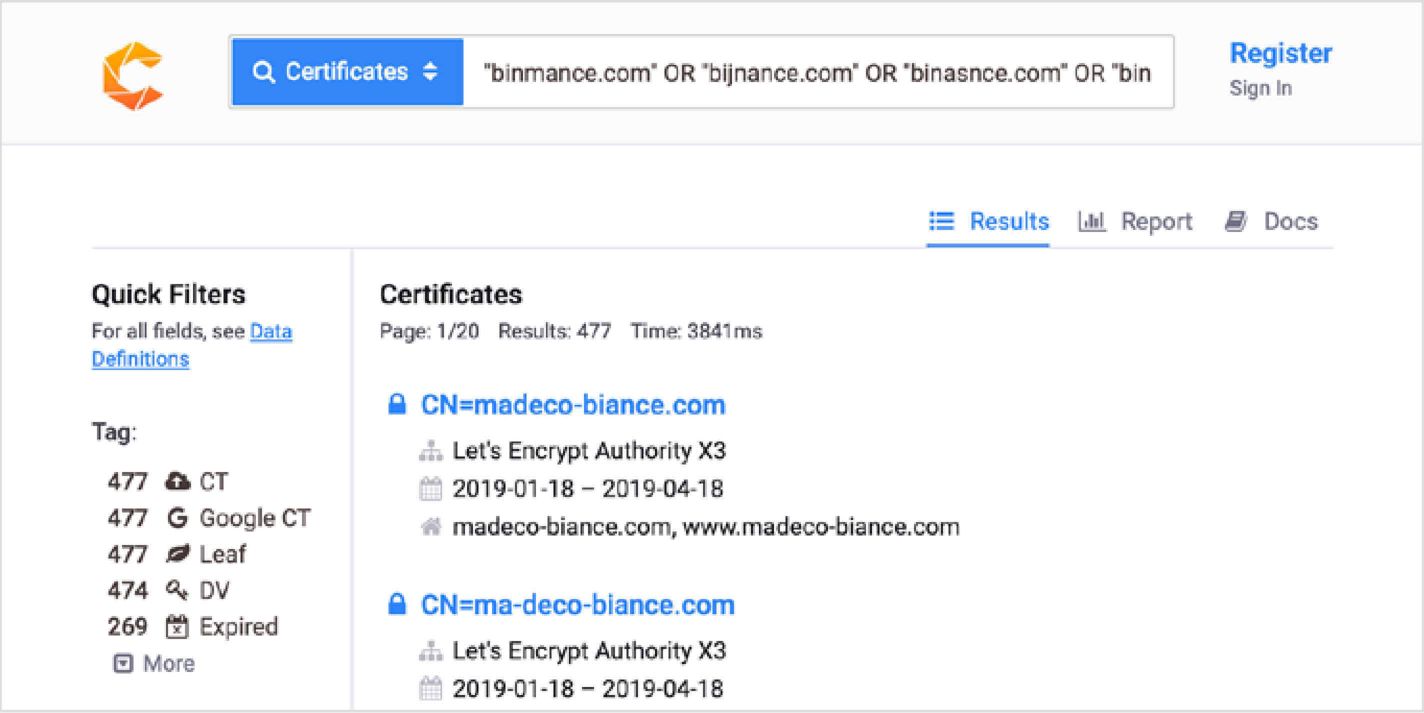
We've chosen domains associated with bug bounty programs for our examples here. This server is no longer online, but this screenshot shows you what Internet security data would be collected on this potentially vulnerable server.

Preventing Phishing and Brand Impersonation

Internet security data, particularly digital certificates issued to web servers, can be used to locate fraudulent domains intended for phishing attacks. Adversaries will often use techniques like typo-squatting — creating domains similar to a legitimate brand domain, but with a commonly-used typo in place (for example Paypsl.com instead of Paypal.com). Corporate security teams can take advantage of Internet security data by searching the adversary breadcrumb trail as they stand up phishing domains. There are some open-source tools to help in these efforts, for example DNS Twist, which auto-populates a list of customized potentially fraudulent domains. With these domains in hand, IT teams can search the Internet for sketchy domains that are likely planted by adversaries to enable phishing attacks.

Here's an example of how this might work in Censys:

Search Censys for fraudulent domains tied to Binance.com



"binmance.com" OR "bijnance.com" OR "binasnce.com" OR "bin

Quick Filters

For all fields, see Data Definitions

Tag:

477 CT
477 Google CT
477 Leaf
474 DV
269 Expired

Certificates

Page: 1/20 Results: 477 Time: 3841ms

CN=madeco-biance.com
Let's Encrypt Authority X3
2019-01-18 – 2019-04-18
madeco-biance.com, www.madeco-biance.com

CN=ma-deco-biance.com
Let's Encrypt Authority X3
2019-01-18 – 2019-04-18

These tools help IT teams get a head start on potential attacks and block them before they're a problem. While these fraudulent domain searches aren't a complete solution for fighting phishing, they help IT teams locate and block or takedown accounts that were likely under the radar prior to analyzing Internet security data.

Threat Hunting to Prevent Targeted Attacks

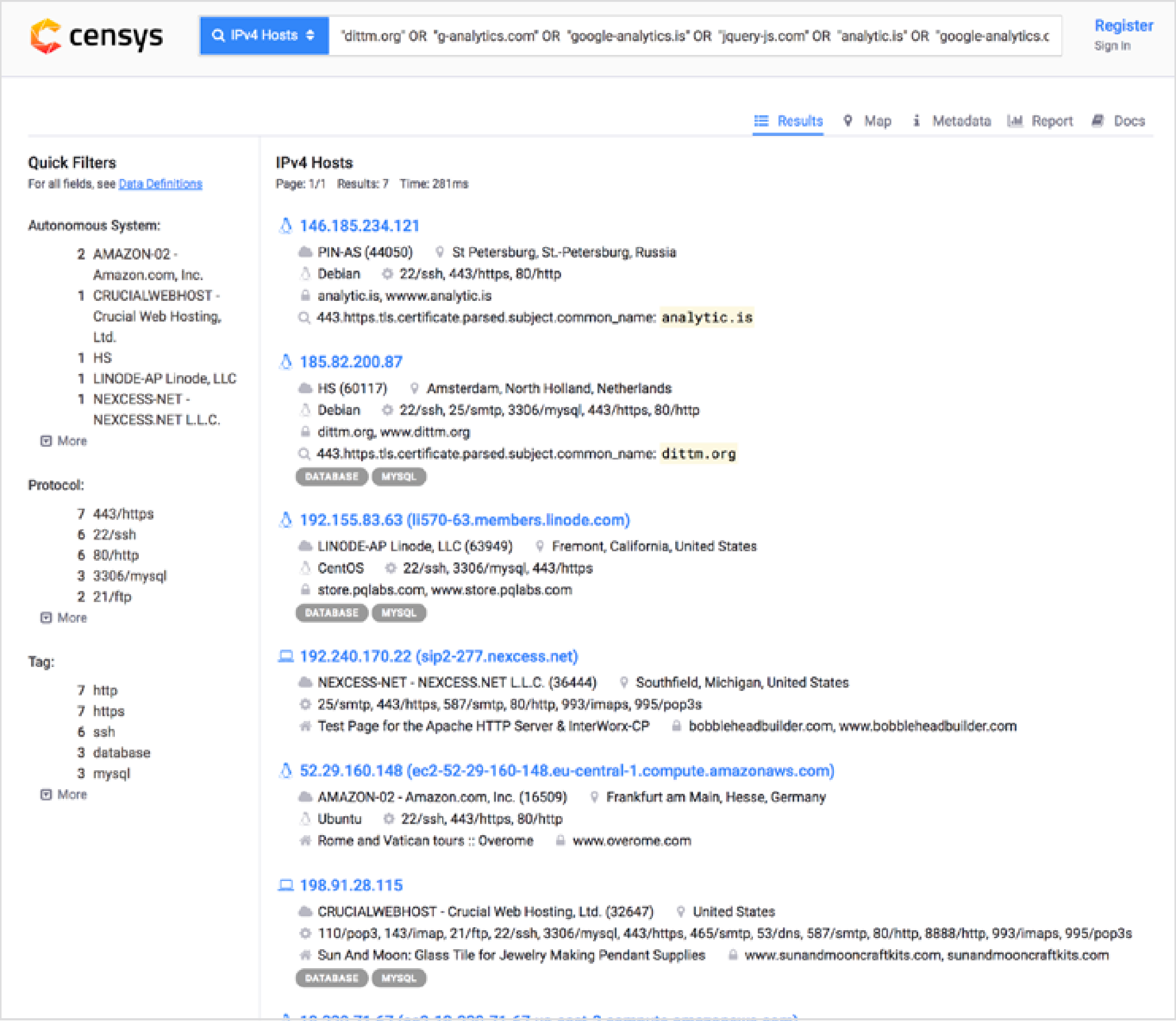
Some large enterprise organizations have highly specialized security teams that utilize Internet security data to prevent targeted phishing and malware from having a negative impact on their business.

Threat hunters typically use Internet data to track known adversaries and their infrastructure, block phishing attacks and other brand impersonation techniques, and locate and block malware sitting dormant on their systems, waiting for an attacker to exploit. An example we'll use here is how a threat hunting team might track known malware, like Magecart, which is the malware used to attack British Airways and Ticketmaster back in 2015. Despite the news coverage and many online discussions about Magecart, the malware is still actively in use by attackers and leading to large data breaches. Threat hunting teams might be interested in understanding how prevalent instances of Magecart are and, more importantly, if their organization or client is at risk of an exploit using Magecart.

Because Magecart operates by injecting malicious Javascript on the root page of websites, threat hunters can search for infected websites through Censys by looking for the known malicious code in the raw HTML. They could compile a list of domains associated with Magecart (for instance, from the Magecart domain list from this OTX pulse) and then search for them with the following query:

Search Censys for domains associated with Magecart malware

Then, the threat hunter would manually inspect the results of this query to ensure the root HTML retrieved from each webserver contains a script link to one of those domains. Those filtered search results of affected IP addresses are below:



"dittm.org" OR "g-analytics.com" OR "google-analytics.is" OR "jquery-js.com" OR "analytic.is" OR "google-analytics.c

Quick Filters
For all fields, see Data Definitions

Autonomous System:

2	AMAZON-02 - Amazon.com, Inc.
1	CRUCIALWEBHOST - Crucial Web Hosting, Ltd.
1	HS
1	LINODE-AP Linode, LLC
1	NEXCESS-NET - NEXCESS.NET L.L.C.

More

Protocol:

7	443/https
6	22/ssh
6	80/http
3	3306/mysql
2	21/ftp

More

Tag:

7	http
7	https
6	ssh
3	database
3	mysql

More

IPv4 Hosts
Page: 1/1 Results: 7 Time: 281ms

146.185.234.121
PIN-AS (44050) St Petersburg, St.-Petersburg, Russia
Debian 22/ssh, 443/https, 80/http
analytic.is, wwww.analytic.is
443.https.tls.certificate.parsed.subject.common_name: analytic.is

185.82.200.87
HS (60117) Amsterdam, North Holland, Netherlands
Debian 22/ssh, 25/smtp, 3306/mysql, 443/https, 80/http
dittm.org, www.dittm.org
443.https.tls.certificate.parsed.subject.common_name: dittm.org
DATABASE MYSQL

192.155.83.63 (li570-63.members.linode.com)
LINODE-AP Linode, LLC (63949) Fremont, California, United States
CentOS 22/ssh, 3306/mysql, 443/https
store.pqlabs.com, www.store.pqlabs.com
DATABASE MYSQL

192.240.170.22 (sip2-277.nexcess.net)
NEXCESS-NET - NEXCESS.NET L.L.C. (36444) Southfield, Michigan, United States
25/smtp, 443/https, 587/smtp, 80/http, 993/imaps, 995/pop3s
Test Page for the Apache HTTP Server & InterWorx-CP bobbleheadbuilder.com, www.bobbleheadbuilder.com

52.29.160.148 (ec2-52-29-160-148.eu-central-1.compute.amazonaws.com)
AMAZON-02 - Amazon.com, Inc. (16509) Frankfurt am Main, Hesse, Germany
Ubuntu 22/ssh, 443/https, 80/http
Rome and Vatican tours :: Overome www.overome.com

198.91.28.115
CRUCIALWEBHOST - Crucial Web Hosting, Ltd. (32647) United States
110/pop3, 143/imap, 21/ftp, 22/ssh, 3306/mysql, 443/https, 465/smtp, 53/dns, 587/smtp, 80/http, 8888/http, 993/imaps, 995/pop3s
Sun And Moon: Glass Tile for Jewelry Making Pendant Supplies www.sunandmooncraftkits.com, sunandmooncraftkits.com
DATABASE MYSQL

With those search results, threat hunters would be able to take necessary steps to mitigate the risk of Magecart, and other malware that behaves in a similar manner or is built with a similar architecture, in their organization.

Incorporating Internet Security Data into a Strong, Defensive Strategy

Here are a few recommendations to effectively incorporate the data, tools, and processes outlined above into an organization's security strategy.

1 **Pull Together Multiple Sources of Internet Security Data**

Typically, security teams will analyze WHOIS information, domain registration, DNS, network scanning, and digital certificates. Thankfully, today there are products and tools that help automate the ingestion of relevant security data in order to make this more practical for organizations of all sizes.

2 **Build your System to Easily Add and Remove Datasets**

Be agile enough to adapt and to ingest new types of Internet security data as it becomes available.

3 **Create a Repeatable Process for Investigation**

Security leaders should develop a process to investigate and add context to Internet security data discoveries. Some obvious targets will surface and can be used to immediately inform security teams about security gaps, however getting insights from the bulk of data will require dedicated time from analysts.

4 **Prioritize your Findings**

Often, analysts are surprised by the number of unknown hosts that they discover in the search results on their first few scans and the next steps of how to address those results seem daunting. The key to securing the organization is in determining which hosts/issues/vulnerabilities to prioritize based on the level of risk each domain presents. This would be a similar task that those familiar with pentests might be familiar with — rating, according to severity and risk, what issues are addressed first.

The business use for Internet security data was not made practical until recently, but with the advent of security data search engines and automation tools, this information is much more actionable for corporate security teams. The strategy behind putting Internet security data into use in an organization should start with gaining a global perspective of everything tied to a business, rather than simply monitoring and tracking what infrastructure lives within the traditional IT network.

Ready to Get Started?

LEARN MORE	CONTACT SALES	SUPPORT
censys.io	sales@censys.io	support.censys.io