

Alfa\_Group

# Tenable Attack Surface Management Report

# Report Description

Tenable Attack Surface Management generates routine snapshots of the organization's external attack surface, leveraging its patent-pending technology to map relationships between these assets to create an inventory of internet-accessible assets owned by a single organization. This report provides findings for all of the organization's external assets at the point in time when the report was generated.

## Background

Tenable Attack Surface Management captures not only DNS entries and IP addresses, but also the relationships between internet-accessible assets. This section describes details of the type of data captured by Tenable Attack Surface Management.

## Internet Snapshots

Each internet snapshot contains details about every known DNS entry and IP-addressable asset associated with the organization across the entire public internet. Snapshots are time-stamped, enabling Tenable Attack Surface Management to track changes of the organization's external assets over time.

## Data Sources

The captured internet snapshots are enriched with third-party data, including WHOIS databases, registered top-level domains, Autonomous System Number (ASN) information, listening ports, service banners, technology stack details, SSL/TLS certificate information, Realtime Blackhole Lists (RBL), email addresses, password dumps, vulnerability data, and more.

## Data Columns

Data collected about the organization's external assets in each internet snapshot potentially has up to 115 unique columns of data. These data columns, also referred to as asset meta-data, may include the web server distribution and major/minor version number, Content Management System (CMS) type, TLS certificate expiration date, geo-IP physical location, cloud or Content Delivery Network (CDN) provider, and more.

## Years

Tenable Attack Surface Management processes hundreds of terabytes of data, resulting in every imaginable computation problem, such as disk utilization, bandwidth, CPU, memory, and I/O processes. Processing internet snapshots requires a highly customized and purpose-built hardware and software platform split between public and private cloud.

# Total Assets

The total number of assets across all of Alfa Group's domain names.

**73**

# Total IP Addresses

The total number of Unique IPs Detected by Alfa Group.

51

# Total Domain Names

The total number of domain names owned by Alfa Group.

2

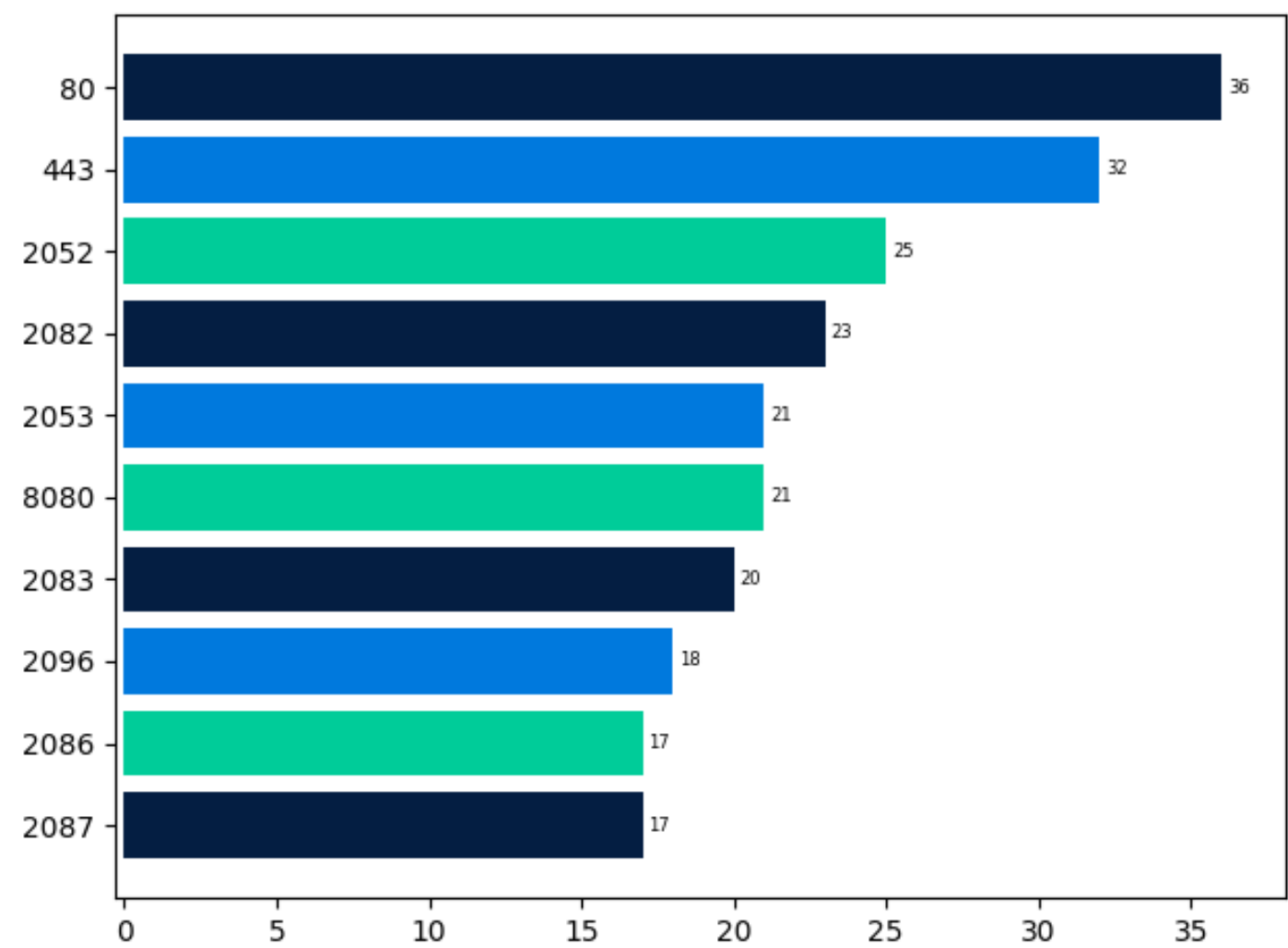
# Total Subdomains

The total number of subdomains owned by Alfa Group.

**22**

# Detected Ports

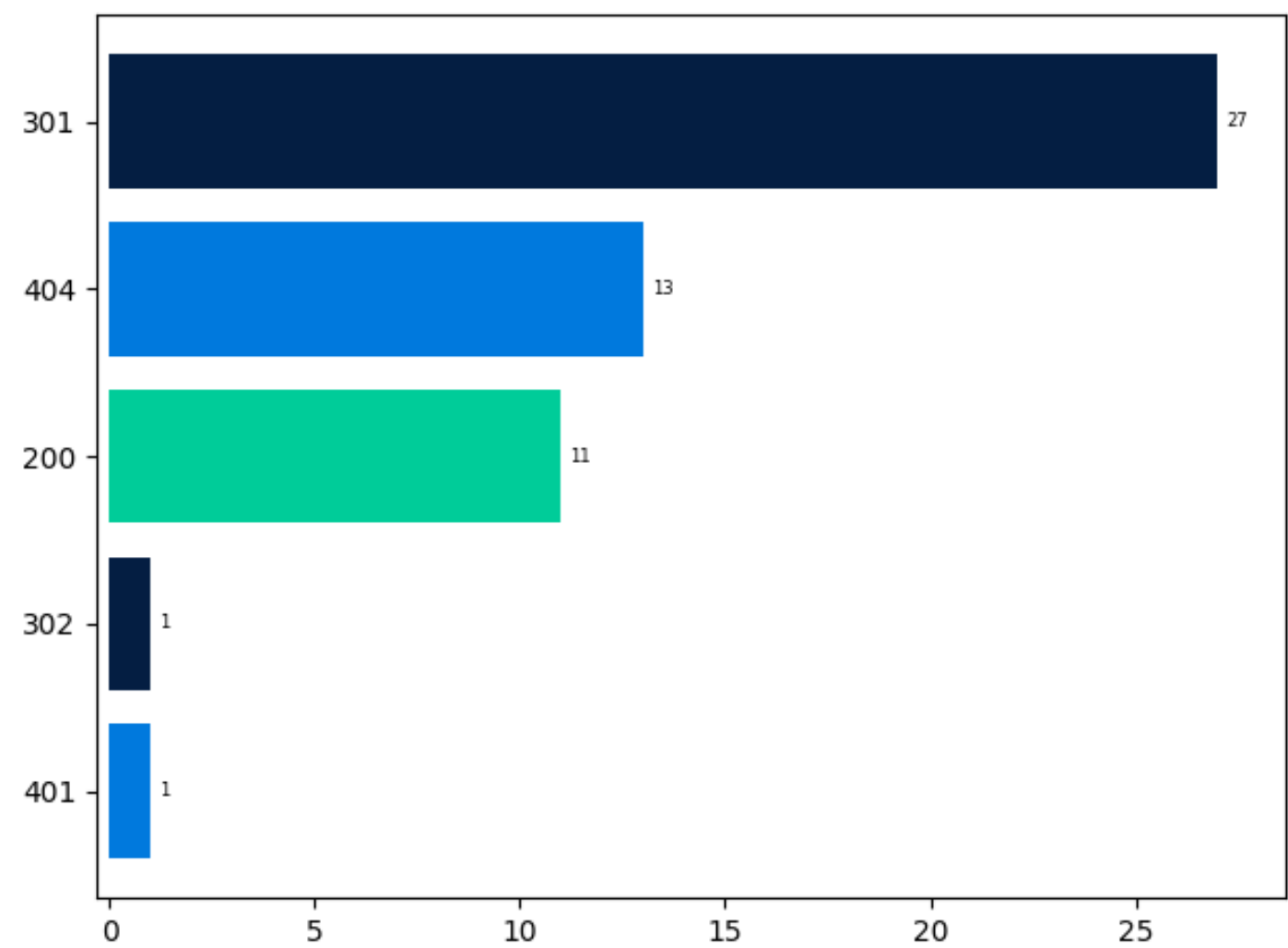
The Listening Ports widget provides details on the most common listening ports of the organization's internet- accessible assets.



Detected Ports	Count	Percent
80	36	49.32%
443	32	43.84%
2052	25	34.25%
2082	23	31.51%
2053	21	28.77%
8080	21	28.77%
2083	20	27.40%
2096	18	24.66%
2086	17	23.29%
2087	17	23.29%

# Response Code

The HTTP/S Response Codes for websites widget displays information about website status: if the site is OK; the page is redirecting; the content is not found; or an error is found.

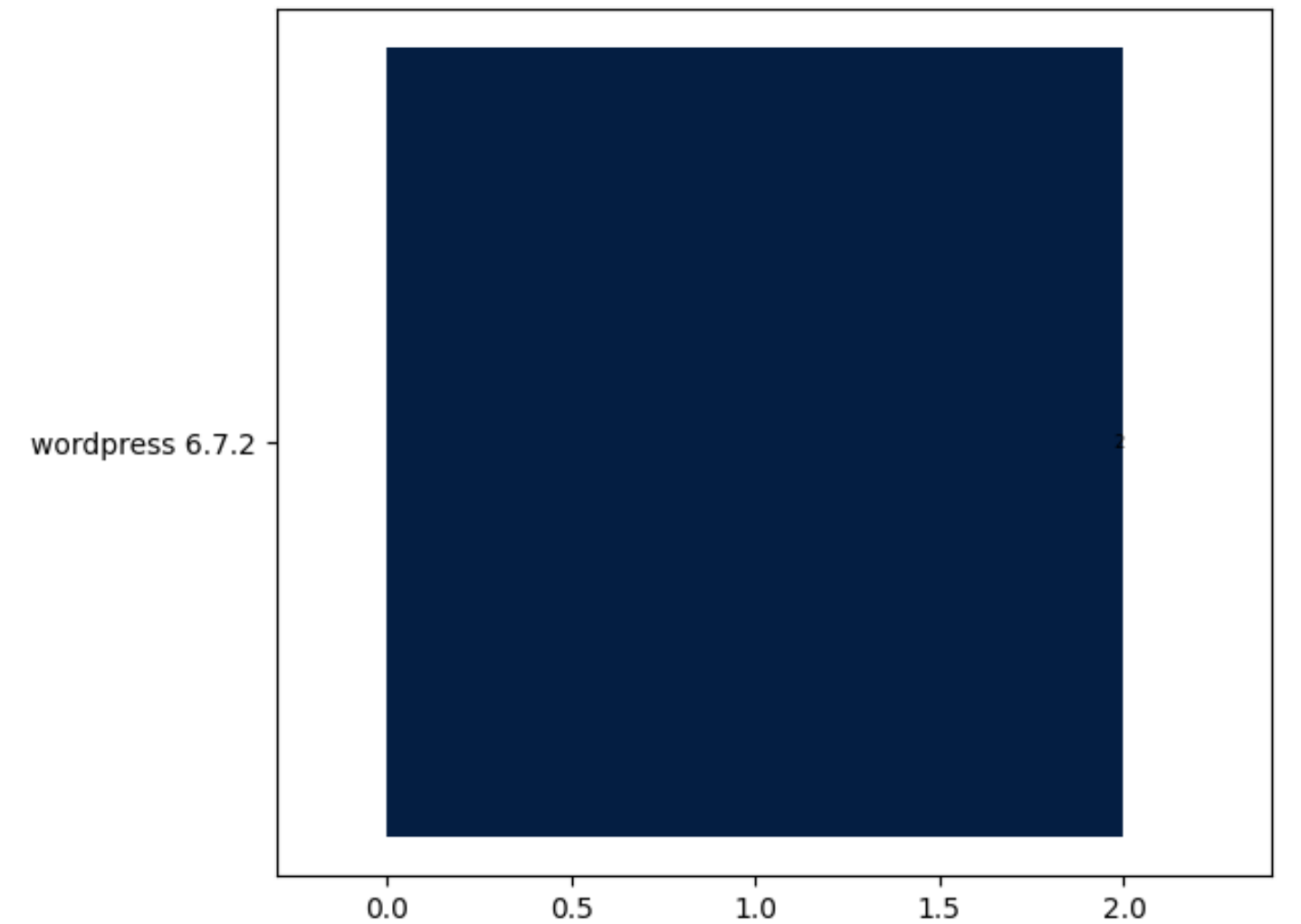


Response Code	Count	Percent
301	27	36.99%
404	13	17.81%
200	11	15.07%
302	1	1.37%
401	1	1.37%



# Content Management Systems (CMS)

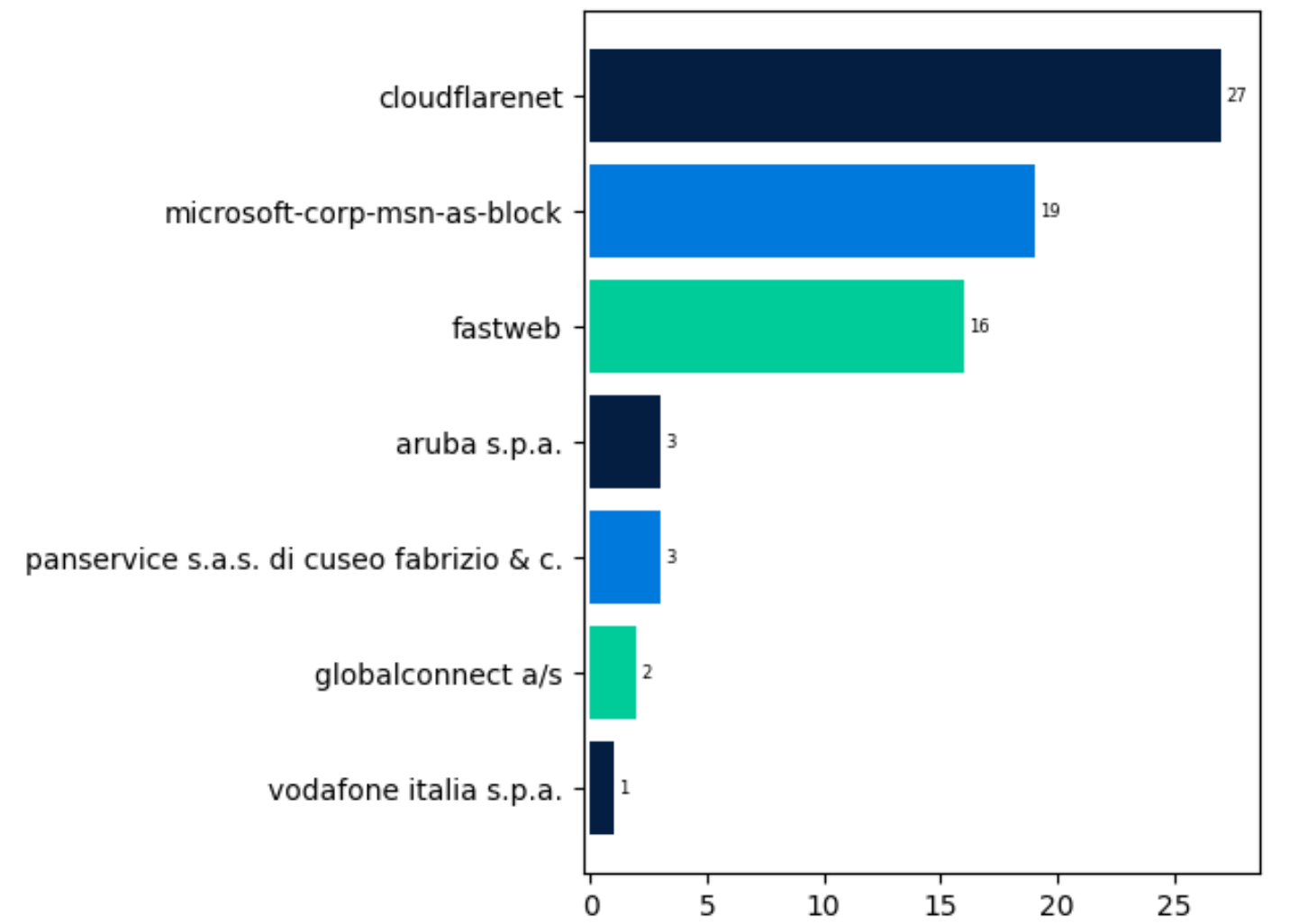
Content Management Systems (CMS) are software applications that are used to manage the creation and modification of digital content. The Content Management Systems widget displays information about what Content Management Systems have been detected for the organization.



Content Management Systems (CMS)	Count	Percent
wordpress 6.7.2	2	2.74%

# Autonomous System Numbers (ASNs)

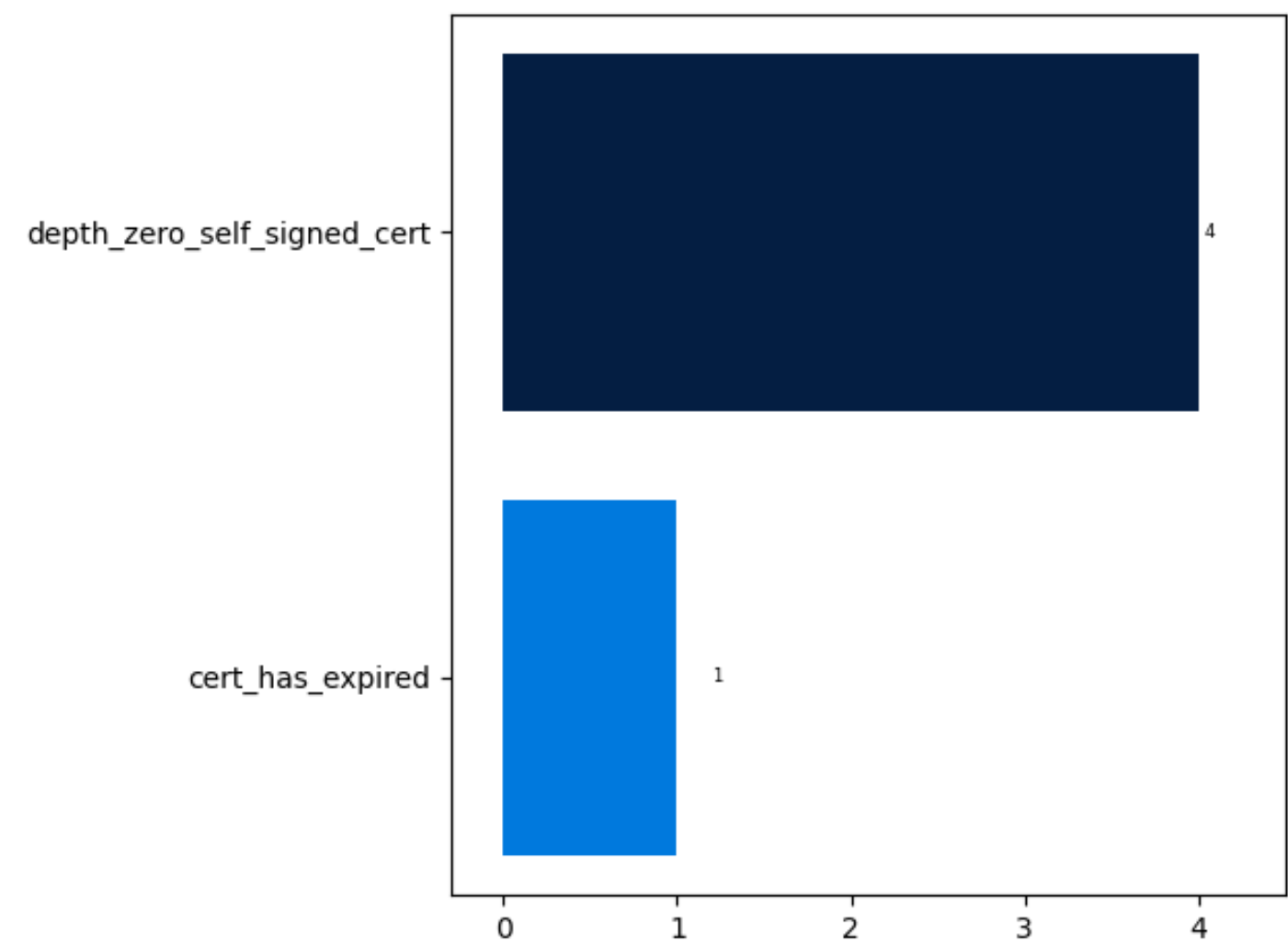
The Autonomous System Numbers (ASNs) widget displays where internet-accessible assets are located by IP address range. ASNs are unique numbers that are available globally to identify autonomous systems and enable systems to exchange exterior routing information with other neighboring autonomous systems.



Autonomous System Numbers (ASNs)	Count	Percent
cloudflarenet	27	36.99%
microsoft-corp-msn-as-block	19	26.03%
fastweb	16	21.92%
aruba s.p.a.	3	4.11%
panservice s.a.s. di cuseo fabrizio & c.	3	4.11%
globalconnect a/s	2	2.74%
vodafone italia s.p.a.	1	1.37%

# SSL/TLS Errors

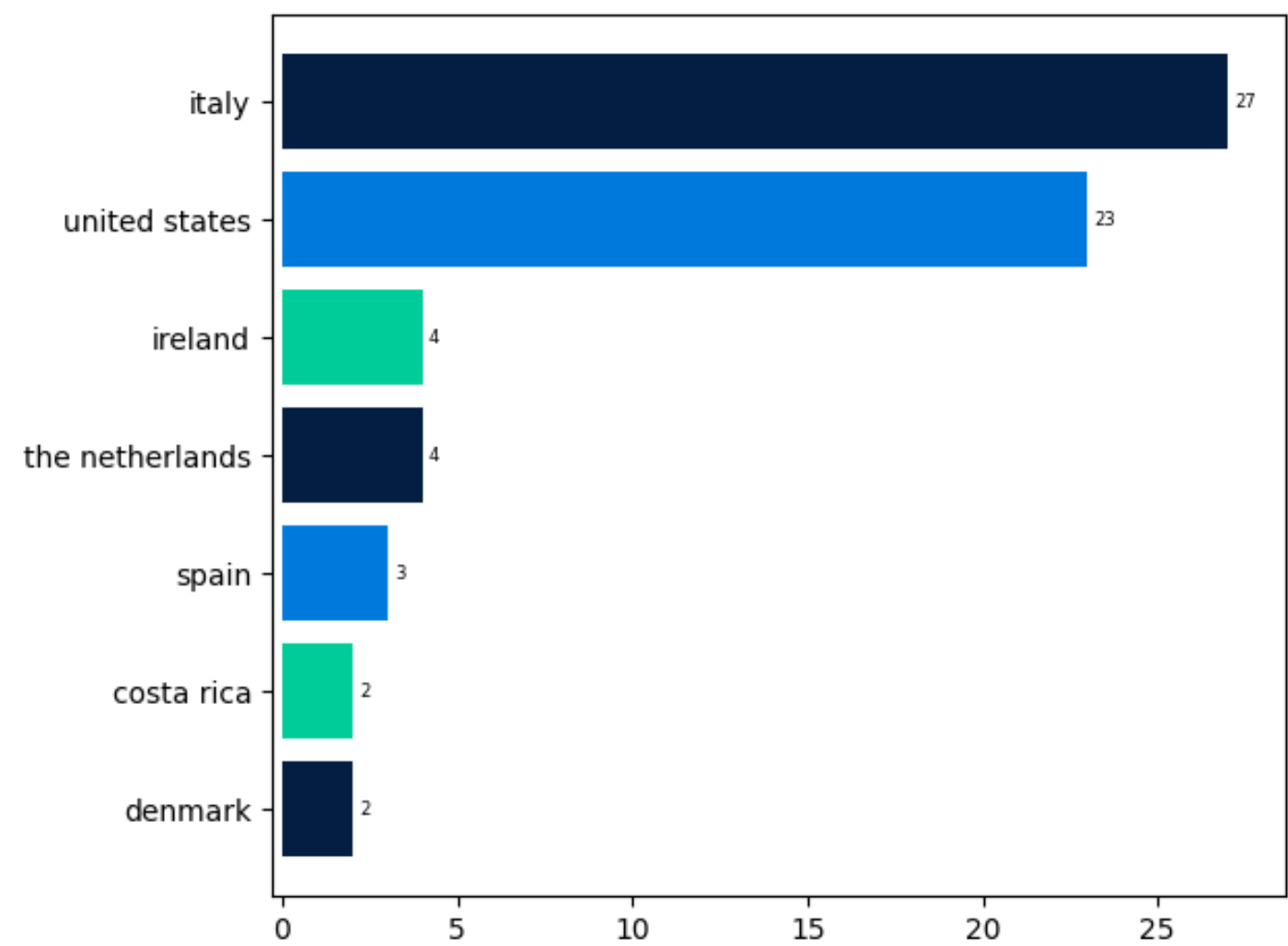
The SSL/TLS Errors widgets display data about errors that are found on scanned websites and seen by a web browser, such as Google Chrome.



SSL/TLS Errors	Count	Percent
depth_zero_self_signed_cert	4	5.48%
cert_has_expired	1	1.37%

# Country

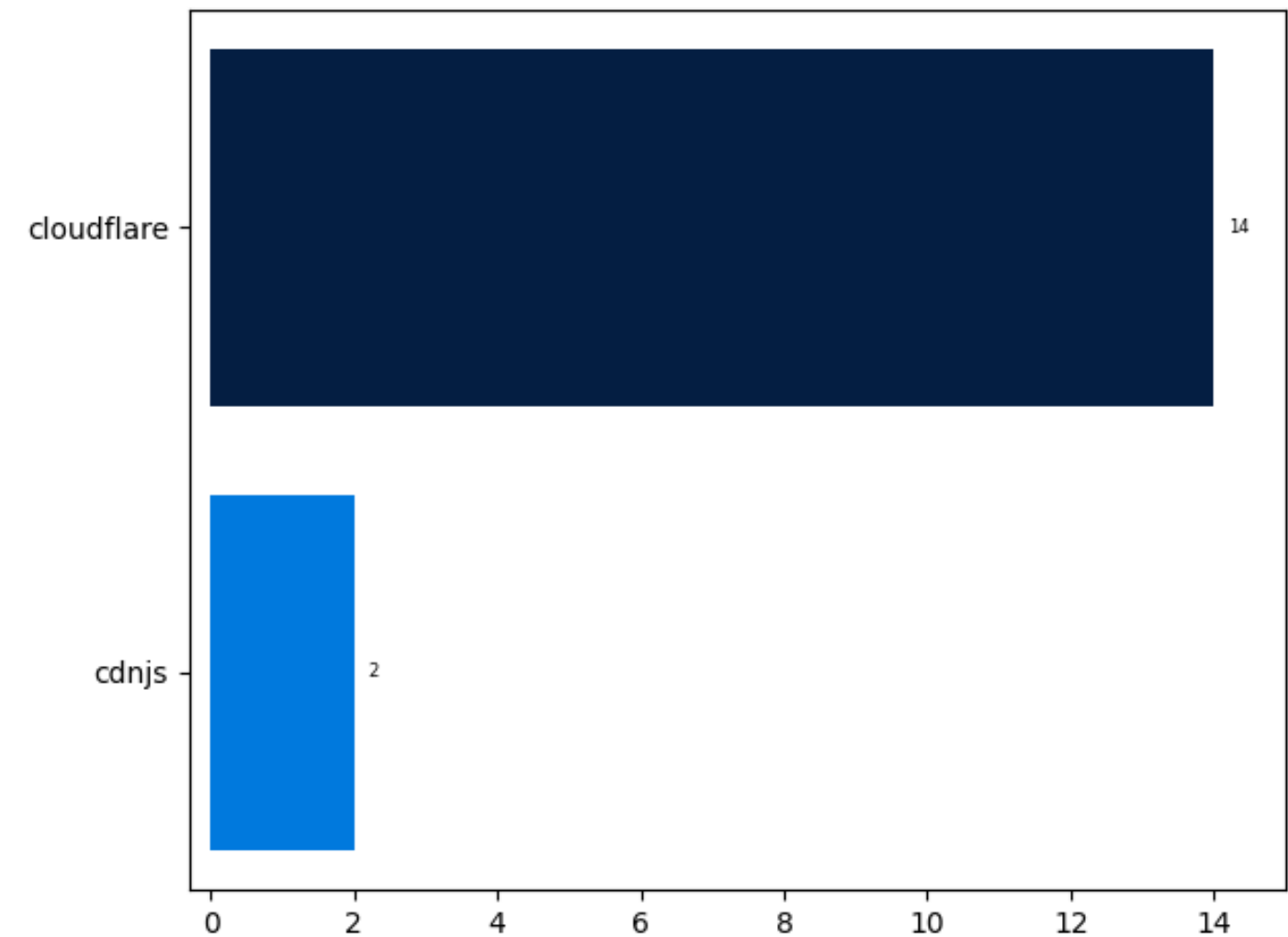
The Hosting Countries widgets display where the organization's internet-accessible assets are physically located, as determined by third-party geolocation of IP address ranges.



Country	Count	Percent
italy	27	36.99%
united states	23	31.51%
ireland	4	5.48%
the netherlands	4	5.48%
spain	3	4.11%
costa rica	2	2.74%
denmark	2	2.74%

# Hosted by Content Delivery Networks (CDNs)

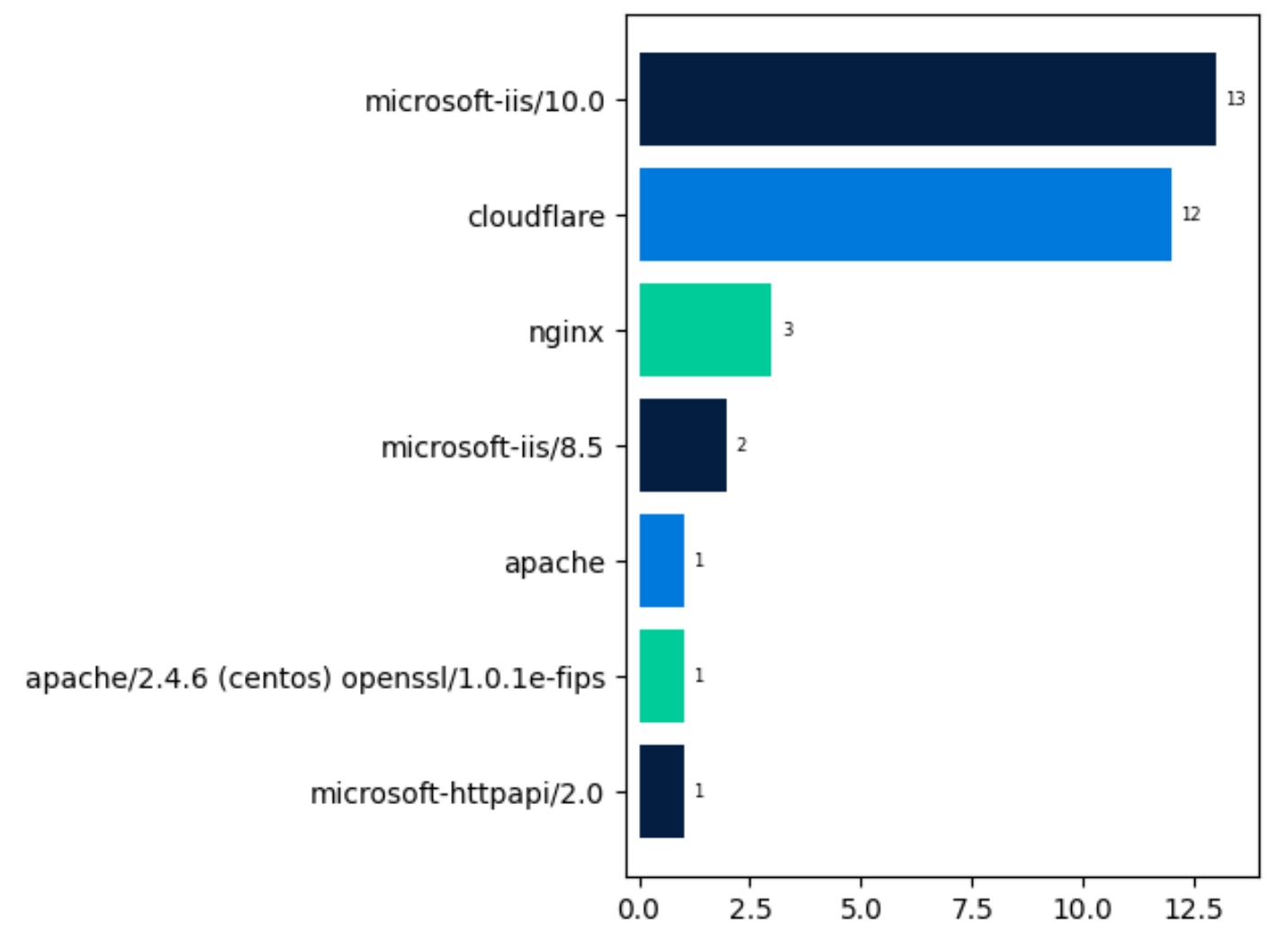
Content Delivery Networks (CDNs) are a geographically distributed groups of servers that work together to provide fast delivery of internet content. The Hosted by CDNs widgets display counts of the organizations assets that are hosted by CDNs along with the name of the hosting CDN.



Hosted by Content Delivery Networks (CDNs)	Count	Percent
cloudflare	14	19.18%
cdnjs	2	2.74%

# Servers

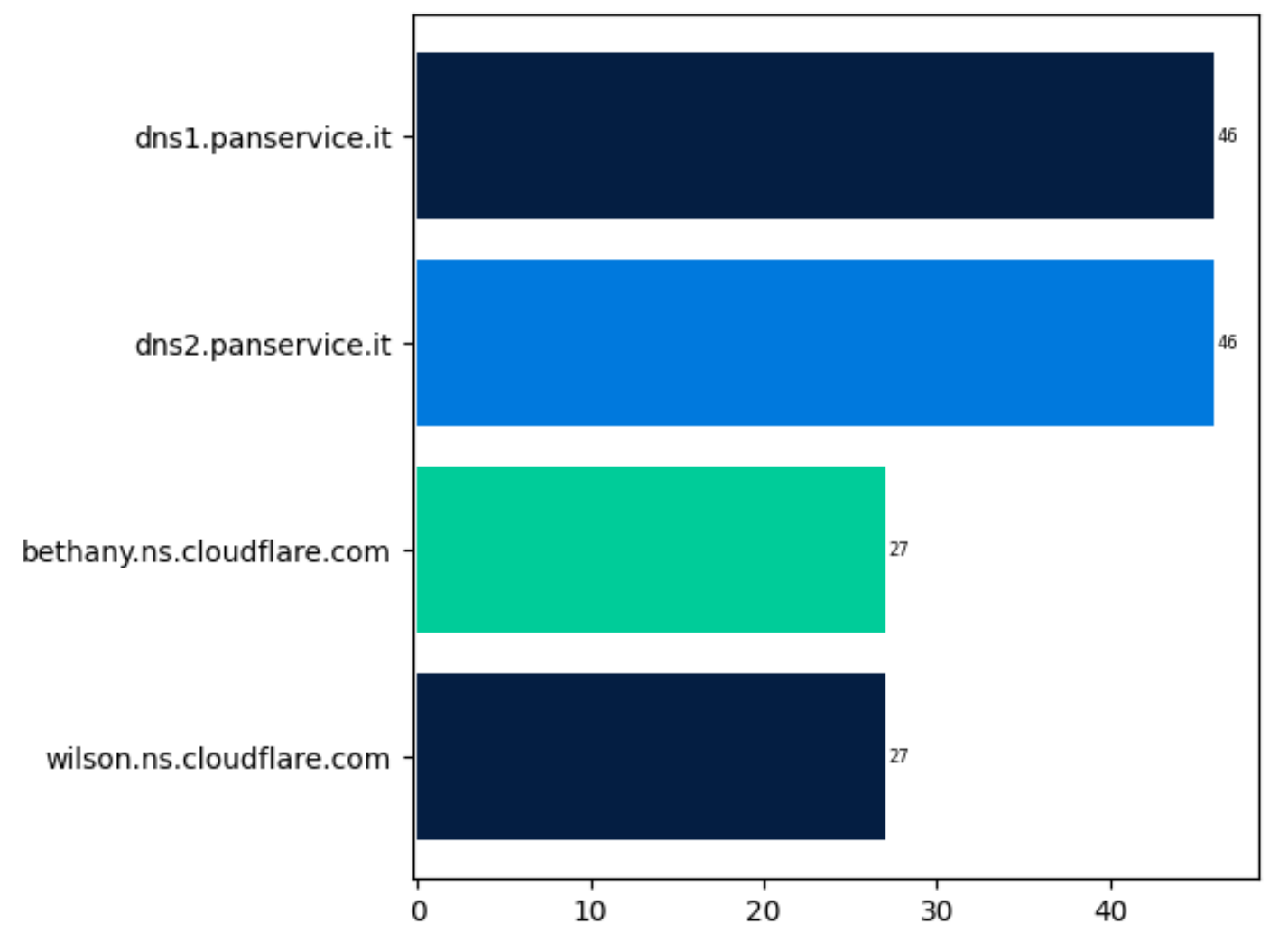
The Servers widgets display counts of the organization's assets that are running web servers, along with the type of server.



Servers	Count	Percent
microsoft-iis/10.0	13	17.81%
cloudflare	12	16.44%
nginx	3	4.11%
microsoft-iis/8.5	2	2.74%
apache	1	1.37%
apache/2.4.6 (centos) openssl/1.0.1e-fips	1	1.37%
microsoft-httpapi/2.0	1	1.37%

# Nameservers

The Nameservers widgets display data about the detected Nameservers that were detected by Tenable Attack Surface Management.



Nameservers	Count	Percent
dns1.panservice.it	46	63.01%
dns2.panservice.it	46	63.01%
bethany.ns.cloudflare.com	27	36.99%
wilson.ns.cloudflare.com	27	36.99%

# Lexicon

## Asset

A domain name, subdomain, or IP addresses and/or combination thereof of a device connected to the Internet or internal network. An asset may include, but not limited to web servers, name servers, IoT devices, network printers, etc. Example: foo.tld, bar.foo.tld, x.x.x.x

## Asset Inventory

A complete collection of an organization's assets and associated metadata of each asset.

## Asset Management

Asset management refers to monitoring, configuring, and maintaining of assets.

## Attack Surface

From the network perspective of an adversary, the complete asset inventory of an organization including all actively listening services (open ports) on each asset.

## Autonomous System Number (ASN)

An ASN is a unique number that's available globally to identify an autonomous system and which enables that system to exchange exterior routing information with other neighboring autonomous systems.

## Content Delivery Network (CDN)

A CDN refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content.

## Discovery

Discovery refers to the act of identifying assets.

## Domain Name

A domain name is a label that identifies a network domain. Domain names are used to identify Internet resources, such as computers, networks, and services, with an easy-to-remember text label that is easier to memorize than the numerical addresses used in the Internet protocols.

## External

Refers to the accessibility of an asset that can be connected to from across the Internet.

## Host

A device connected to a network that communicates with other hosts on the network.

## Hostname

A unique name given to any device that is connected to a specific computer network, typically appended to a domain name, and resolves to an IP-address using the Domain Name System (DNS).