censys

CHEATSHEET

10 Ways to Use Censys Search

Accurate and up-to-date internet data is the lifeblood of effective threat hunting. It allows security professionals to stay ahead of the constantly evolving threat landscape, respond promptly to potential threats, and reduce the risks associated with cybersecurity incidents.

Threat hunters can utilize Censys Search for various use cases to enhance their cybersecurity efforts. Read on to learn more about the top 10 ways to leverage Censys Search.

1

Identify Vulnerable Services:

Identify devices or services with potential vulnerabilities. By querying specific service banners, software versions, or configurations, they can pinpoint systems that require immediate patching or remediation.

2

Discover Rogue Assets:

Search for devices and services that do not belong to the organization's known inventory. This helps identify rogue or unauthorized assets that may pose a security risk.

3

Monitor SSL/TLS Certificates:

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.

4

Identify Open Ports and Services:

Search for open ports and services that are exposed on the internet. This information is valuable for ensuring that only necessary services are running and no unauthorized or unnecessary ports are open.

5

Investigate Geographical Anomalies:

Enrich connection logs to detect access attempts from hosts in unusual locations, with strange profiles, and more.

6 **Find Devices with Weak Encryption:**
By searching for devices that use outdated encryption protocols or weak cryptographic configurations, you can identify security weaknesses that need immediate attention.

7 **Discover IoT Devices:**
Discover Internet of Things (IoT) devices connected to an organization's network. This is essential for monitoring and securing these potentially vulnerable endpoints.

8 **Track Vendor or Provider Compliance:**
Monitor whether vendors or service providers are adhering to security standards and configurations specified in their agreements.

9 **Search for Sensitive Data Exposure:**
Identify potentially exposed sensitive data, such as databases with open ports or web services misconfigured to expose critical information.

10 **Identify Malicious Infrastructure:**
Find malicious infrastructure, such as command and control servers, phishing websites, and other suspicious domains or IP addresses.

These specific use cases illustrate how Censys Search can be a valuable tool for threat hunters to identify and respond to a wide range of security threats and vulnerabilities within an organization's network and beyond.