censys

Securing Healthcare Infrastructure

Protecting Vital Protocols and Systems from Cyber Threats

With unmatched internet visibility and accuracy, Censys provides access to billions of services, hosts, and certificates. Whether leveraging **Censys Attack Surface Management (ASM)** to conduct searches on assets in your organization's external attack surface or using **Censys Search** for visibility into the entire internet, knowing which resources and identifiers to use is essential for advanced threat detection and response efforts, and mitigating threats in real-time. This reference guide provides a comprehensive list of essential healthcare systems, protocols, and labels for effective use in your daily operations with Censys.

Critical Healthcare IT Systems & Protocols Censys Identifies:

HL7 (Health Level 7)
Identify and secure HL7 to prevent unauthorized access to sensitive patient information, ensuring compliance and data protection.

FHIR (Fast Healthcare Interoperability Resources)
Detect and secure FHIR to protect sensitive health information, to avoid data breaches and maintain patient trust.

DICOM (Digital Imaging and Communications in Medicine)
Identify and secure DICOM to safeguard patient privacy and maintain data integrity.

PACS (Picture Archiving and Communication System)
Ensure the security of PACS to protect medical images and reduce the risk of data breaches.

RIS (Radiology Information System)
Secure RIS to maintain patient privacy and protect radiology data from unauthorized access.

HIS (Hospital Information System)
Secure HIS to protect administrative, financial, and clinical information, maintaining hospital operations integrity.

LIS (Laboratory Information System)
Implement security measures for LIS to protect patient test results and laboratory data, ensuring privacy and compliance.

EHR (Electronic Health Records)
Secure EHR to prevent unauthorized access and data breaches, protecting extensive patient health information.

Leveraging Labels for Streamlined Detection

Censys uses labels to categorize and identify various systems and services within IT environments. By leveraging these labels, you can streamline the detection and security of critical components. Below are the key labels and their significance:

- **Medical Device (medical-device) Label** - Categorizes systems such as EMR/EHR, DICOM-enabled imaging devices, PACS servers, and Smart Operating System Controllers. Securing these devices is crucial to avoid operational disruptions and protect patient privacy.
- **Remote Access (remote-access) Label** - Identifies services like RDP, SSH, VNC, VPN, TeamViewer, and AnyDesk. Securing these services prevents unauthorized access to networks and systems handling PHI, supporting HIPAA, HITECH, GDPR, NIST, and ISO 27001 compliance.
- **Database (database) Label** - Covers systems like SQL Databases, NoSQL Databases, Key-Value Stores, and Document Stores. Protecting these databases prevents unauthorized access and data breaches of PHI, aligning with HIPAA, HITECH, GDPR, NIST, ISO 27001, and SOC 2 standards.
- **File Sharing (file-sharing) Label** - Includes services such as FTP, SFTP, SMB, and cloud-based platforms. Securing these services prevents unauthorized access and data breaches involving PHI, aiding HIPAA, HITECH, GDPR, NIST, ISO 27001, and PCI DSS compliance.
- **Netscaler (netscaler) Label** - Refers to hosts using Citrix NetScaler (Citrix ADC). Securing these hosts prevents unauthorized access and service disruptions, protecting PHI and supporting HIPAA, HITECH, NIST, and ISO 27001 standards.

How to Detect Protocols and Systems in Censys Search

Censys Search empowers you to proactively identify and mitigate threats across the global internet infrastructure. Below are examples of the different types of queries you can run to detect various protocols and labels:

Use Case	Query
Identify Hosts by Service Name Find hosts that provide a specific service.	`services.service_name: DICOM`
Identify Hosts by Service Banner Find hosts based on specific text found in the service banner.	`services.banner: HL7`
Identify Hosts by Label Find hosts with the Medical Device label.	`labels: “medical-device”`
Identify Hosts by Multiple Labels Find hosts with the Medical Device, Remote Access, Database, File Sharing or Netscaler label to detect hosts.	`labels: {medical-device, remote-access, database, file-sharing, netscaler}`

Querying Censys Search for internet-exposed hosts labeled as ‘medical-device’ revealed nearly 23,000 instances.

How to Detect Protocols and Systems in Censys ASM

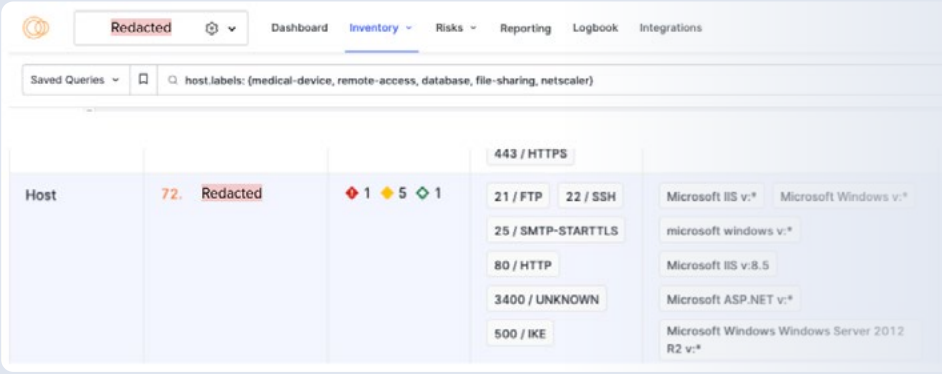
Censys ASM enables you to detect these protocols and labels specific to assets identified in your external attack surface. Below are examples of the different types of queries you can run to detect various protocols and labels.

Use Case	Query
Identify Hosts with Services by Name Find hosts that provide a specific service.	`host.services.service_name: DICOM`
Identify Hosts with a Service Banner Find hosts based on specific text found in the service banner.	`host.services.banner: HL7`
Identify Hosts by Label Find hosts with the Medical Device, Remote Access, Database, File Sharing or Netscaler label.	`host.labels: {medical-device, remote-access, database, file-sharing, netscaler}`

Learn More

Leverage Saved Query Automation to receive notifications for these queries in real-time, enabling you to take immediate action on potential threats.

See the Demo



Leveraging Censys ASM to identify hosts categorized under critical protocol and system labels.

Censys for Healthcare

In an era where cyber threats are increasingly sophisticated and healthcare data is more vulnerable than ever, Censys provides the comprehensive visibility and actionable intelligence needed to protect your critical infrastructure. Trust Censys to be your partner in building a resilient, secure, and patient-centric digital environment.

censys

VISIT censys.com

CONTACT hello@censys.com

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.