# Audit Report

# Solh Streffie

Audited on September 24, 2025

Reported on September 24, 2025

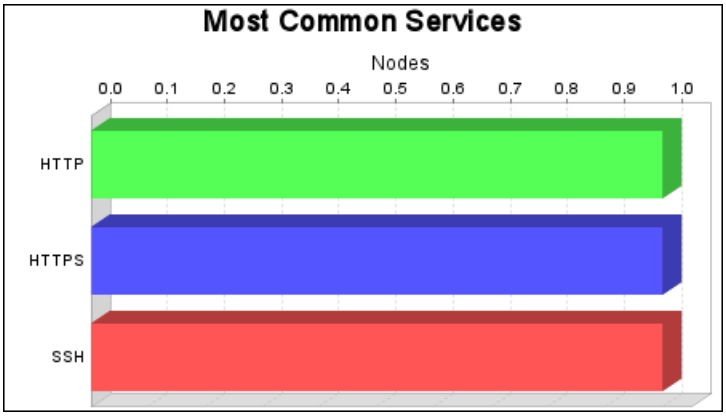
# 1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

| Site Name | Start Time | End Time | Total Time | Status |
|---|---|---|---|---|
| Solh Streffie | September 24, 2025 15:51, IST | September 24, 2025 15:53, IST | 2 minutes | Success |

**There is not enough historical data to display overall asset trend.**

The audit was performed on one system which was found to be active and was scanned. No vulnerabilities were found during this scan.
One operating system was identified during this scan.
There were 3 services found to be running during this scan.




The HTTP, HTTPS and SSH services were found on 1 systems, making them the most common services.

# 2. Discovered Systems

| Node | Operating System | Risk | Aliases |
|---|---|---|---|
| 52.66.61.253 | Ubuntu Linux | 0.0 | •ai.solhapp.com |

# 3. Discovered and Potential Vulnerabilities

# 4. Discovered Services

## 4.1. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

### 4.1.1. General Security Issues

*Simple authentication scheme*

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

### 4.1.2. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 52.66.61.253 | tcp | 80 | 0 | •OpenResty 1.27.1.2<br>•http.banner: openresty/1.27.1.2<br>•http.banner.server: openresty/1.27.1.2 |

## 4.2. HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

### 4.2.1. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 52.66.61.253 | tcp | 443 | 0 | •OpenResty 1.27.1.2<br>•http.banner: openresty/1.27.1.2<br>•http.banner.server: openresty/1.27.1.2<br>•ssl: true<br>•ssl.cert.issuer.dn: CN=E5, O=Let's Encrypt, C=US<br>•ssl.cert.key.alg.name: EC<br>•ssl.cert.not.valid.after: Sun, 19 Oct 2025 17:45:03 IST<br>•ssl.cert.not.valid.before: Mon, 21 Jul 2025 17:45:04 IST<br>•ssl.cert.selfsigned: false<br>•ssl.cert.serial.number: |

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| | | | | 528695334347752058186710286422514149636261<br>•ssl.cert.sha1.fingerprint: d126b374a11b291d3497d80098f9865e5f95b3c8<br>•ssl.cert.sig.alg.name: SHA384withECDSA<br>•ssl.cert.subject.alt.name-1: ai.solhapp.com<br>•ssl.cert.subject.alt.name-count: 1<br>•ssl.cert.subject.dn: CN=ai.solhapp.com<br>•ssl.cert.validchain: true<br>•ssl.cert.version: 3<br>•ssl.protocols: tlsv1_2,tlsv1_3<br>•ssl.supportsInsecureRenegotiation: true<br>•sslv2: false<br>•sslv3: false<br>•tlsv1_0: false<br>•tlsv1_1: false<br>•tlsv1_2: true<br>•tlsv1_2.ciphers: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256<br>•tlsv1_2.extensions: RENEGOTIATION_INFO,EXTENDED_MASTER_SECRET,EC_POINT_FORMATS,SERVER_NAME<br>•tlsv1_3: true<br>•tlsv1_3.ciphers: TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256<br>•tlsv1_3.extensions: SERVER_NAME |

## 4.3. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

### 4.3.1. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 52.66.61.253 | tcp | 22 | 0 | •OpenBSD OpenSSH 9.6p1<br>•ssh.algorithms.compression: none,zlib@openssh.com<br>•ssh.algorithms.encryption: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com<br>•ssh.algorithms.hostkey: rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519<br>•ssh.algorithms.kex: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-s,kex-strict-s-v00@openssh.com<br>•ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1<br>•ssh.banner: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11<br>•ssh.protocol.version: 2.0 |

# 5. Discovered Users and Groups

No user or group information was discovered during the scan.

# 6. Discovered Databases

No database information was discovered during the scan.

# 7. Discovered Files and Directories

No file or directory information was discovered during the scan.

# 8. Policy Evaluations

No policy evaluations were performed.

# 9. Spidered Web Sites

No web sites were spidered during the scan.