### S - Spoofing

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Rogue administrators

5. Malware or compromised systems

6. Insider threat (disgruntled employees)

7. Network eavesdroppers

8. Policy violations

9. Credential theft

10. Phishing attacks

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to spoof their identity to gain unauthorized access to the SFTP server.

- Likelihood: Moderate

- Impact: High

2. Internal attackers could also impersonate legitimate users to access sensitive data.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might attempt to impersonate trusted sources to inject malicious files into the system.

- Likelihood: Low

- Impact: Moderate

4. Rogue administrators could misuse their privileges to impersonate others.

- Likelihood: Low

- Impact: Moderate

5. Malware or compromised systems could spoof legitimate connections.

- Likelihood: Moderate

- Impact: Moderate

6. Insider threats might exploit their knowledge to spoof identities.

- Likelihood: Moderate

- Impact: High

7. Network eavesdroppers could attempt to intercept and manipulate traffic.

- Likelihood: Moderate

- Impact: Moderate

8. Policy violations could lead to unauthorized access.

- Likelihood: Low

- Impact: Low

9. Credential theft can result in unauthorized access.

- Likelihood: Moderate

- Impact: High

10. Phishing attacks may trick users into disclosing credentials.

- Likelihood: Moderate

- Impact: Moderate

### T - Tampering

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Malware or compromised systems

5. Data interception and modification

6. Network manipulation

7. Unauthorized system changes

8. Malicious software updates

9. Misconfiguration

10. Lack of data integrity checks

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to alter data during transmission or storage.

- Likelihood: Moderate

- Impact: High

2. Internal attackers could tamper with data to disrupt operations or steal sensitive information.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might send malicious files or tampered data.

- Likelihood: Low

- Impact: Moderate

4. Malware or compromised systems could introduce unauthorized changes.

- Likelihood: Moderate

- Impact: High

5. Data interception and modification during transit.

- Likelihood: Moderate

- Impact: Moderate

6. Network manipulation to tamper with data in transit.

- Likelihood: Moderate

- Impact: Moderate

7. Unauthorized system changes by administrators.

- Likelihood: Low

- Impact: Moderate

8. Malicious software updates compromising data integrity.

- Likelihood: Low

- Impact: High

9. Misconfigurations leading to vulnerabilities.

- Likelihood: Moderate

- Impact: High

10. Lack of data integrity checks allowing undetected tampering.

- Likelihood: Moderate

- Impact: High

### R - Repudiation

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Rogue administrators

5. Malware or compromised systems

6. Insider threats

7. Legal disputes

8. Lack of audit logs

9. Inadequate log protection

10. Incomplete or inconsistent logging

\*\*Threat Descriptions:\*\*

1. External attackers may gain access to the server and deny their actions.

- Likelihood: Moderate

- Impact: Moderate

2. Internal attackers could manipulate logs or erase evidence of their actions.

- Likelihood: Moderate

- Impact: Moderate

3. Third-party vendors might claim that they never sent certain files.

- Likelihood: Low

- Impact: Moderate

4. Rogue administrators may deny their unauthorized activities.

- Likelihood: Low

- Impact: Moderate

5. Malware or compromised systems might alter logs.

- Likelihood: Moderate

- Impact: Moderate

6. Insider threats could exploit their knowledge to deny actions.

- Likelihood: Moderate

- Impact: Moderate

7. Legal disputes may require non-repudiation evidence.

- Likelihood: Low

- Impact: Moderate

8. Lack of audit logs may hinder investigation.

- Likelihood: Moderate

- Impact: High

9. Inadequate log protection may allow tampering.

- Likelihood: Moderate

- Impact: High

10. Incomplete or inconsistent logging may lead to disputes.

- Likelihood: Moderate

- Impact: Moderate

### I - Information Disclosure

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Misconfiguration

5. Unauthorized software

6. Social engineering

7. Insider threats

8. Data leaks

9. Unencrypted backups

10. Unsanctioned devices

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to intercept and access sensitive data during transmission.

- Likelihood: High

- Impact: High

2. Internal attackers could exploit vulnerabilities to access confidential information.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might send sensitive files that get exposed.

- Likelihood: Low

- Impact: Moderate

4. Misconfiguration may inadvertently expose sensitive data.

- Likelihood: Moderate

- Impact: High

5. Unauthorized software could lead to data leaks.

- Likelihood: Moderate

- Impact: Moderate

6. Social engineering attacks may trick employees into disclosing sensitive information.

- Likelihood: Moderate

- Impact: Moderate

7. Insider threats might intentionally leak sensitive data.

- Likelihood: Moderate

- Impact: High

8. Data leaks through insecure backups.

- Likelihood: Moderate

- Impact: High

9. Unsanctioned devices accessing sensitive data.

- Likelihood: Moderate

- Impact: Moderate

10. Unencrypted backups being accessed by unauthorized individuals.

- Likelihood: Moderate

- Impact: High

### D - Denial of Service

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Malware or botnets

5. Natural disasters

6. Network failures

7. Power outages

8. Hardware failures

9. Software bugs

10. Resource exhaustion

\*\*Threat Descriptions:\*\*

1. External attackers may launch DDoS attacks to disrupt SFTP services.

- Likelihood: High

- Impact: High

2. Internal attackers could flood the server with requests to exhaust resources.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might unintentionally overload the server with large file transfers.

- Likelihood: Low

- Impact: Moderate

4. Malware or botnets may be used to launch coordinated DDoS attacks.

- Likelihood: Moderate

- Impact: High

5. Natural disasters, such as floods or earthquakes, could disrupt server operations.

- Likelihood: Low

- Impact: High

6. Network failures may result in service interruptions.

- Likelihood: Moderate

- Impact: High

7. Power outages may render the server inaccessible.

- Likelihood: Moderate

- Impact: High

8. Hardware failures could lead to service downtime.

- Likelihood: Moderate

- Impact: High

9. Software bugs or vulnerabilities may be exploited for DoS.

- Likelihood: Moderate

- Impact: High

10. Resource exhaustion due to inefficient resource management.

- Likelihood: Moderate

- Impact: High

### E - Elevation of Privilege

\*\*Threat Agents:\*\*

1. Internal attacker

2. Misconfiguration

3. Exploitable software vulnerabilities

4. Insufficient access controls

5. Rogue administrators

6. Social engineering

7. Unauthorized privilege escalation

8. Inadequate password policies

9. Insider threats

10. Weak encryption practices

\*\*Threat Descriptions:\*\*

1. Internal attackers may attempt to escalate their privileges to gain unauthorized access.

- Likelihood: Moderate

- Impact: High

2. Misconfigurations in the server or access controls could lead to unintended privilege escalation.

- Likelihood: Moderate

- Impact: High

3. Exploitable software vulnerabilities may be used to gain higher privileges.

- Likelihood: Moderate

- Impact: High

4. Insufficient access controls could allow unauthorized users to elevate their privileges.

- Likelihood: Moderate

- Impact: High

5. Rogue administrators might misuse their privileges.

- Likelihood: Moderate

- Impact: High

6. Social engineering attacks could trick users into granting elevated privileges.

- Likelihood: Moderate

- Impact: High

7. Unauthorized privilege escalation attempts.

- Likelihood: Moderate

- Impact: High

8. Inadequate password policies may lead to password-based privilege escalation.

- Likelihood: Moderate

- Impact: High

9. Insider threats intentionally elevating their privileges.

- Likelihood: Moderate

- Impact: High

10. Weak encryption practices leading to unauthorized data access.

- Likelihood: Moderate

- Impact: High