Zero Trust Testing Checklist

https://www.linkedin.com/in/joas-antonio-dos-santos

Identity and Access

- Multi-factor Authentication (MFA) is implemented.
- Strong authentication policies are in place.
- There's a solution for identity management.
- Role-Based Access Control (RBAC) policies are in place.
- Regular verification of permissions and excessive privileges.

Backup and Recovery

- There's a backup and recovery strategy.
- Backups are regularly tested.

Endpoint Devices

- Endpoint security (e.g., antivirus, EDR) is implemented.
- Mobile Device Management (MDM) is in operation to control devices outside the network.

Training and Awareness

- Users are regularly trained on best security practices.
- They are aware of the Zero Trust model and its importance.

Integration with Other Solutions

- Integration with other security solutions, such as firewalls, antivirus, etc.

Principle of Least Privilege

- Users have the minimum necessary privileges to perform their functions.
- Mechanisms are in place to restrict access based on context (e.g., location, device type).

Encryption

- All data in transit is encrypted.
- All data at rest is encrypted.
- Encryption keys are managed and rotated regularly.

Integration with Cloud Infrastructure

- Security policies are extended and consistent in hybrid and cloud environments.

Application and Data Controls

- Policies are in place to ensure only trusted applications are run.
- Sensitive data is classified and protected accordingly.

Incident Response

- There's an incident response plan.
- Incident simulation exercises are regularly conducted.

Penetration Testing and Assessment

- Regular penetration tests are conducted.
- Vulnerability assessments are regularly carried out.
- Third-party evaluation of the Zero Trust implementation.

Updates and Patches

- There's an automated process for patching.
- Known vulnerabilities are promptly fixed.

Monitoring and Analysis

- Log records are maintained and monitored for suspicious activities.
- Alerts are generated for non-compliant activities.
- Behavioral analysis of users to identify anomalous activities.
- SIEM (Security Information and Event Management) solution or similar is in operation.

Network Segregation

- Micro-segmentation is implemented to isolate workloads.
- Devices and applications can only communicate with systems that are strictly necessary for their operations.