CHECKLIST

API SECURITY

Essentials For Organisations

1. **Implement secure authentication and authorisation methods**
   Use secure protocols like OAuth and OpenID Connect to authenticate and authorise API users; use access tokens to control access to resources.

2. **Input validation**
   Validate all input passed to the API to ensure it conforms to the expected format and does not contain any malicious code.

3. **Encryption**
   Use HTTPS to encrypt all communications between the API and clients to protect against eavesdropping and man-in-the-middle attacks.

4. **Use an API Gateway**
   API Gateways act as a reverse proxy for API requests and provide features such as authentication, rate limiting and caching to protect against common API attacks.

5. **Monitor and log API activity**
   Use monitoring and logging tools to track API activity and detect any suspicious activity.

6. **Regularly update and patch the API**
   Keep the API and the underlying systems updated with the latest security patches to protect against known vulnerabilities.

7. **Conduct regular Penetration testing**
   Regularly conduct penetration testing to identify and remediate vulnerabilities in the API and the connected systems.

8. **Train employees on API security**
   It’s important to educate employees on API security best practices and raise awareness of the risks associated with APIs.

www.distology.com

Distology.