onsecurity

External Attack Surface Management Checklist

Feel confident in building a fortifying your external assets with OnSecurity's external attack surface management checklist.

Download and use this checklist to ensure your business is operating with a secure security strategy.

- □ **Audit your website** – Remove outdated login pages, technical documentation, and sensitive information revealing internal infrastructure
- □ **Lock down unused domains and subdomains** – Decommission or secure forgotten development servers and staging environments
- □ **Check for leaked credentials** – Search company email addresses on HaveIBeenPwned and enforce password resets for compromised accounts
- □ **Review cloud storage permissions** – Ensure S3 buckets, Azure blobs, and databases aren't publicly accessible
- □ **Scan code repositories** – Check GitHub and GitLab for exposed API keys, tokens, and credentials
- □ **Update employee social media guidance** – Provide clear policies on what staff should share on LinkedIn regarding technologies and internal projects
- □ **Monitor for brand impersonation** – Set up alerts for fake domains and fraudulent use of your brand

This resource is designed to help businesses become cyber reslient against emerging threats