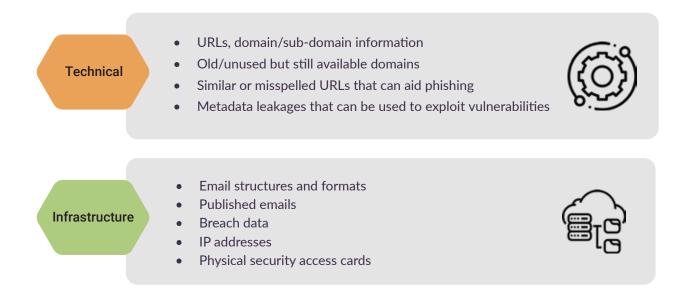# OSINT THREAT EXPOSURE ASSESSMENT

Our OSINT threat exposure review enables your business to know and understand the entire internet footprint of your assets and domains. It also ascertains the volume and nature of open-source information that can be used to profile and exploit key figures in your organization. Our analysis will allow you to understand how much of your sensitive business information malicious advisories can gather without actively engaging with your systems. And our recommendations detail the expected effort, along with guidelines & expenditure for implementation, enabling you to make measured and costed decisions about your security.

We will also check in the public domain and on the Dark Web leaked sensitive information and suggest remediation including the areas that need focus and prioritization. Our OSINT Risk Assessment is an extension to your standard business risk assessments. Our team will take the same paths that a threat actor might take when researching your business.

The first step to any targeted cyber-attack is research - and we do our research really well

Some of the areas we cover for investigation

Technical
- URLs, domain/sub-domain information
- Old/unused but still available domains
- Similar or misspelled URLs that can aid phishing
- Metadata leakages that can be used to exploit vulnerabilities

Infrastructure
- Email structures and formats
- Published emails
- Breach data
- IP addresses
- Physical security access cards

![activebytes innovations logo]

Business
- Public financial records
- News and press releases
- Key employee profiles and contacts
- Documents, papers, articles (published and leaked)

Social and Personal
- Social media accounts and personal details
- Family member posts and photographs
- LinkedIn and other messaging platforms

Benefits

- Aid in discovering unnoticed vulnerabilities in infrastructure
- Understand threat landscape and prioritize their risks
- Reduce attack surface
- Ensure security of public facing interfaces or applications
- Safeguard employees from phishing attacks