secarma®
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Vulnerability Scanning

POWERED BY AppCheck
ACCURACY IS EVERYTHING

At Secarma our core services are focused around in-depth manual Penetration Testing and we aim to assist businesses develop their maturity towards advanced testing capabilities such as Red Teaming. However, Penetration Testing is a point in time approach and therefore work with AppCheck to deliver more regular security testing with their automated vulnerability scanning tool.

WHO IS IT FOR?

Vulnerability scanning software is for organisations who want to continually (or as and when required) test their applications and infrastructure to catch vulnerabilities before they cause an issue.

For organisations who need a quick, easy, flexible and affordable way to respond to and manage vulnerabilties, AppCheck offers unlimited testing 24 hours a day, 365 days a year. Its dashboard presents a fully configurable view of your current security posture, allowing you to track remediation, spot vulnerabilities

HOW CAN WE HELP?

An effective solution for identifying and reporting vulnerabilities throughout the year. Whilst it can't reach the same depth as a manual penetration test, it works particularly well alongside Penetration Testing to achieve a balance of depth and frequency. AppCheck can help with:

- **Quick & frequent vulnerability scanning:** Scans only take seconds to configure and start, and can be performed 24 hours a day, 365 days a year.
- **Security by design:** Perform scans throughout an applications lifecycle, ensuring it's secure before launching, and in the future.
- **Reporting & remediation:** Provides detailed reports with easy to follow remediation advice.
- **Vulnerability management dashboard:** A fully configurable view of your current security posture.

WHAT WE TEST

AppCheck has two distinct scanning engines designed to test web applications and computer systems for vulnerabilities:

- **Applications**

  For each URL configured with the scan, AppCheck will map out the application and mimic a typical application user. Methodical security testing will be performed to confirm the vulnerabilities

  Common vulnerabilities detected during the web application scan include; Injection flaws such as SQL, NoSQL, XML, Code, and command injection, cross-site scripting and hundreds of other vulnerability classes arising from insecure code.

- **Internal & External Infrastructure**

  The infrastructure scan identifies accessible services which are then probed for vulnerabilities.

  Common vulnerabilities detected during the infrastructure scanning phase include; missing operating systems patches, weak administrative passwords and access control vulnerabilities.