edgescan

Case Study

Case Study: Global Telecom Company

Scope:
Web Applications: 450
Internet Facing Servers: 12,789

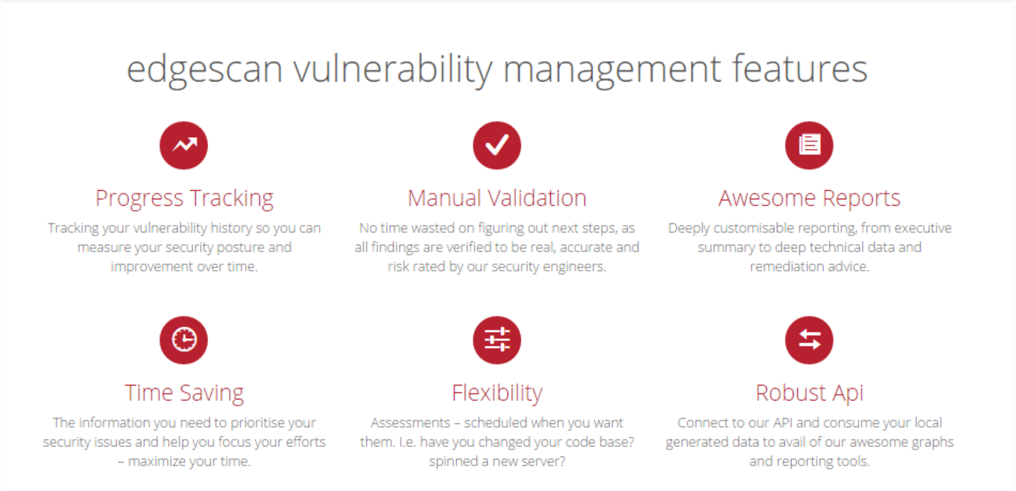
The scope of this engagement consisted of delivering continuous vulnerability management of 450 web applications and 12 thousand servers distributed across the globe for a global telecoms manufacturer and operator based in the USA:

- The client company required a continuous assessment of its entire global Internet facing cyber-estate in order to detect current security issues and detect new issues into the future.
- The client required a false positive free list of actionable findings which they could simply assign and fix.
- They required the assessment to continue to assess the sites so they could track progress and mitigation of discovered security risks.

Onboarding:
The onboarding phase consisted of validating each site and server for stability and criticality such that the continuous assessment could provide coverage and depth of testing as expected. Once an application is onboarded technical assessment can commence and the application is subject to technical security assessment on an ongoing basis.

Continuous Assessment
Edgescan provided continuous assessment on an ongoing basis for the 450 web application and 12789 IP servers under management. All of the vulnerabilities discovered are manually validated helping our client focus on issues which cause a real risk. Assessments occurred on a scheduled and an ad-hoc basis as required by the client.

Outcome
Within the first 7 days edgescan discovered, validated and published 233 high risk issues on the clients edgescan portal. The client proceeded to fix the discovered issues over the coming months and the fixes were verified and closed by edgescan. The client could display the improvement of its security posture over time. The client could request an assessment when required to retest for vulnerabilities and maintain a secure posture.



edgescan vulnerability management features

Progress Tracking
Tracking your vulnerability history so you can measure your security posture and improvement over time.

Manual Validation
No time wasted on figuring out next steps, as all findings are verified to be real, accurate and risk rated by our security engineers.

Awesome Reports
Deeply customisable reporting, from executive summary to deep technical data and remediation advice.

Time Saving
The information you need to prioritise your security issues and help you focus your efforts – maximize your time.

Flexibility
Assessments – scheduled when you want them. I.e. have you changed your code base? spinned a new server?

Robust Api
Connect to our API and consume your local generated data to avail of our awesome graphs and reporting tools.