



Automating the Hell out of Vulnerability Management

Florian Ruechel¹

¹*Atlassian*

Scanning for network vulnerabilities is a well understood practice for hardening an organisation. It's not about finding the latest 0day, but ensuring there is no low-hanging fruit. However, in practice implementing vulnerability scanning in a modern organisation presents big challenges. How do you integrate a 'old-school' approach into a modern, cloud-based company? How does your approach scale to tens of thousands of hosts?

See how our engineers evolved scanning from using yet-another-web-interface and sending e-mails to service owners (hoping for the best) to an automated, scalable solution that makes a measurable impact. This approach scales, it handles risk management, false positives, regressions and various other details that used to make scanning hard. And it decouples the actual scanner from the process - swapping out for a different solution is minimal effort.

Our solution isn't limited to your run-of-the-mill security scanners either. It can be easily re-used to address other issues within your organisation, too - anything that is a security risk can leverage the same solution (open S3 buckets, dangling DNS names, misconfiguration). And your compliance team will be happy too!