Quickly detect and resolve vulnerabilities with an automated testing solution by SecureQuest

Free your IT team from time-consuming, repetitive testing

Penetration testing is an essential component of modern security, ensuring your infrastructure can withstand even the most inventive attacks. Yet the extensive planning and analytics associated with this form of testing can also quickly overwhelm your IT team. Even when some components are automated, most organisations still rely heavily on manual analysis and investigation by skilled IT professionals. As well as affecting productivity, this also increases the risk of error and the likelihood vulnerabilities will fall through the cracks.

SecureQuest (Questronix's Cybersecurity Team), can help you overcome these challenges with automated vulnerability scanning and penetration testing, enabled by the RedHat Ansible Automation Platform (Ansible).

Simplify, streamline and consolidate your testing approach

SecureQuest can work closely with your organisation to integrate the security tools you require, as well as provide the Ansible playbooks required to automate laborious and repetitive tasks such as in vulnerability scanning and penetration testing.

This can deliver a range of benefits:

- **Speed and efficiency** — reliably execute a vast number of tests much faster than manual processing allows

- **Enhanced security** — quickly and easily identify security vulnerabilities that might be missed by manual testing.

- **Save time and resources** — take the burden of conducting repetitive tasks away from your IT team, freeing them to focus on other areas.

- **Continuous testing** — we can help you integrate a range of automated security tools into your DevSecOps environment, ensuring security testing is performed consistently throughout the entire development process, 24/7.

- **Alleviate complexity** — automating your security processes can streamline even the most complex of testing tasks, including performing multi-layered iterative attacks before software is released into the market.

Why choose SecureQuest Services for your automated testing?

- **Fully customisable** — our team can adapt a range of security testing tools to work with Ansible, based on your organisation's specific use cases.

- **Ongoing support** — the SecureQuest team will work with you at every step, ensuring the optimal design, deployment, and maintenance of your solution.

- **Cost effective** — pay for your solution under a highly flexible software-as-a-service arrangement.

- **Robust and secure** — SecureQuest's solution integrates with industry-standard security tools which could help your organization improve its security posture.
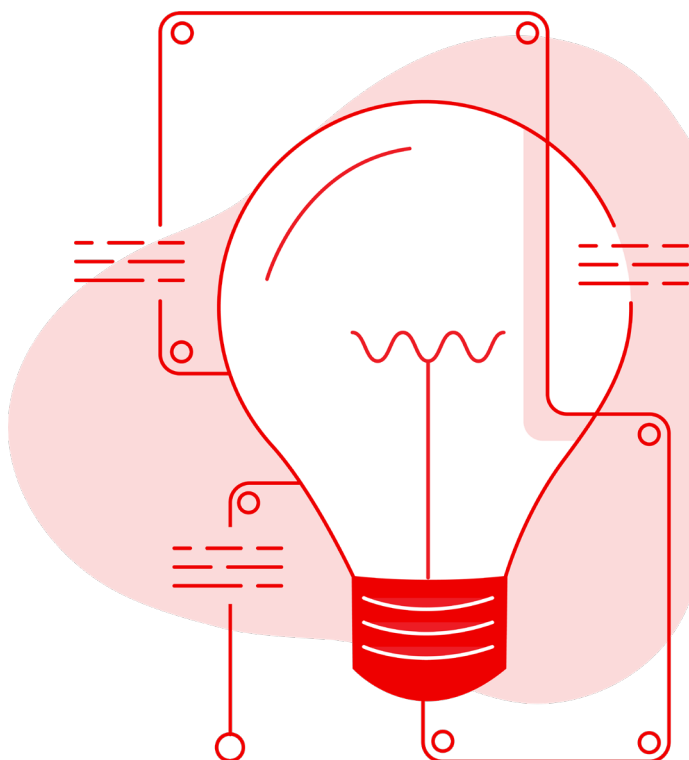
How SecureQuest helped a major financial services organisation

This large bank in Asia processes missions of transactions every day across a diverse branch network, making robust security absolutely critical. Yet maintaining regular and reliable testing processes was proving to be a major drain on the bank's internal resources.

SecureQuest worked with the bank to implement an automated testing solution — streamlining key processes, and reducing human intervention. The bank now has a fully protected, automated and controlled testing environment, leaving their IT team free to focus on implementing more high-value innovations.
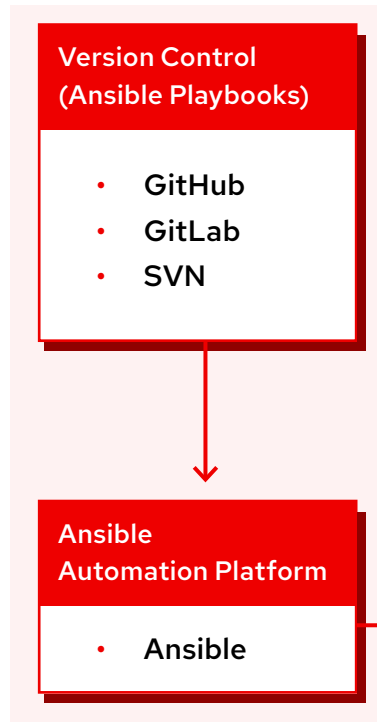
> "Security automation is the #1 automation priority for organisations in 2023."
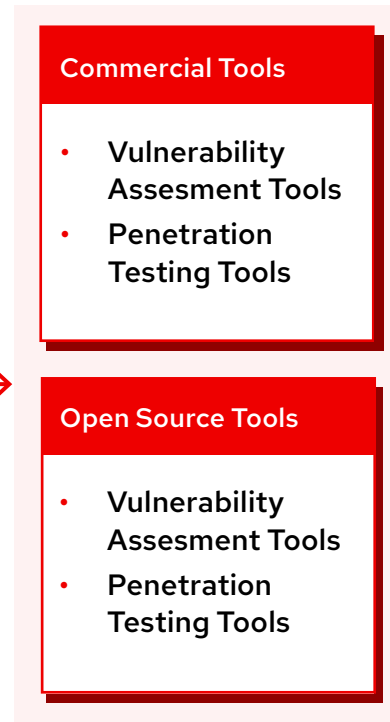
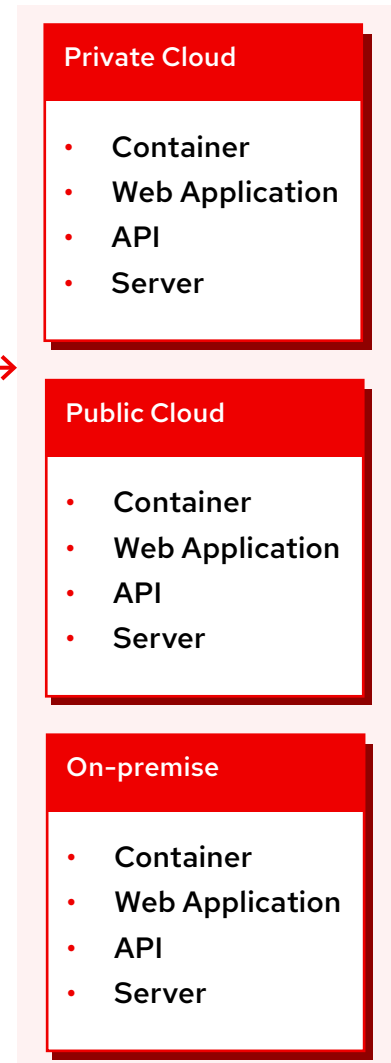Source: Red Hat Global Customer Tech Outlook, 2022

Solutions Overview

Automation

Version Control (Ansible Playbooks)

- GitHub
- GitLab
- SVN

Ansible Automation Platform

- Ansible

Security Tools

Commercial Tools

- Vulnerability Assesment Tools
- Penetration Testing Tools

Open Source Tools

- Vulnerability Assesment Tools
- Penetration Testing Tools

Environments

Private Cloud

- Container
- Web Application
- API
- Server

Public Cloud

- Container
- Web Application
- API
- Server

On-premise

- Container
- Web Application
- API
- Server