



Product Presentation

June 2022









Why Continuous Security Testing?

Digital transformation & Agile working environment

Stay in compliance (ISO, SOC2, OWASP)

Signifies solid risk management

Save cost by finding security bugs early in the cycle

Boosts customer confidence & reputation

Practice secure development practices

Stay a step ahead of hackers

Real Challenges



Problem 1

Penetration testing is complex and lengthy process



Problem 2

Penetration testing is not agile, while 80% of all app development happens using agile methodology



Problem 3

Penetration testing is short-lived and expensive (operational overhead inclusive). Often performed under time pressure

Traditional Penetration Test Approach

• Requirement • Selection of tools Resource intensive for both Gathering • Repeated process for each Manual review of pentest vendor and customer • SoW writing & scan results customer signoff Repeated process False positive • No visibility to customer on Takes 2-4 weeks Resource allocation removal scan results Takes 1-2 days Automated Scoping & Vulnerability Scheduling Scanning Manual Report Penetration Writing & Resource skill-level Delivery Testing • Time-consuming, lengthy limitation and repeated process to Often no exploitation Checklist based • Peer Review & generate a report performed approach **Quality Assurance** Massive copy/paste Performed under time Vulnerability • One-off report activities pressure exploitation delivery Takes 1-2 days Takes 5-7 days

One-off testing, repeated process & no cost savings – Always expensive due to costly resource + hidden management fees

Solutions



Solution 1

Deploy own SAST & vulnerability scanning tools but that picks only low hanging issues and you still need pentest



Solution 2

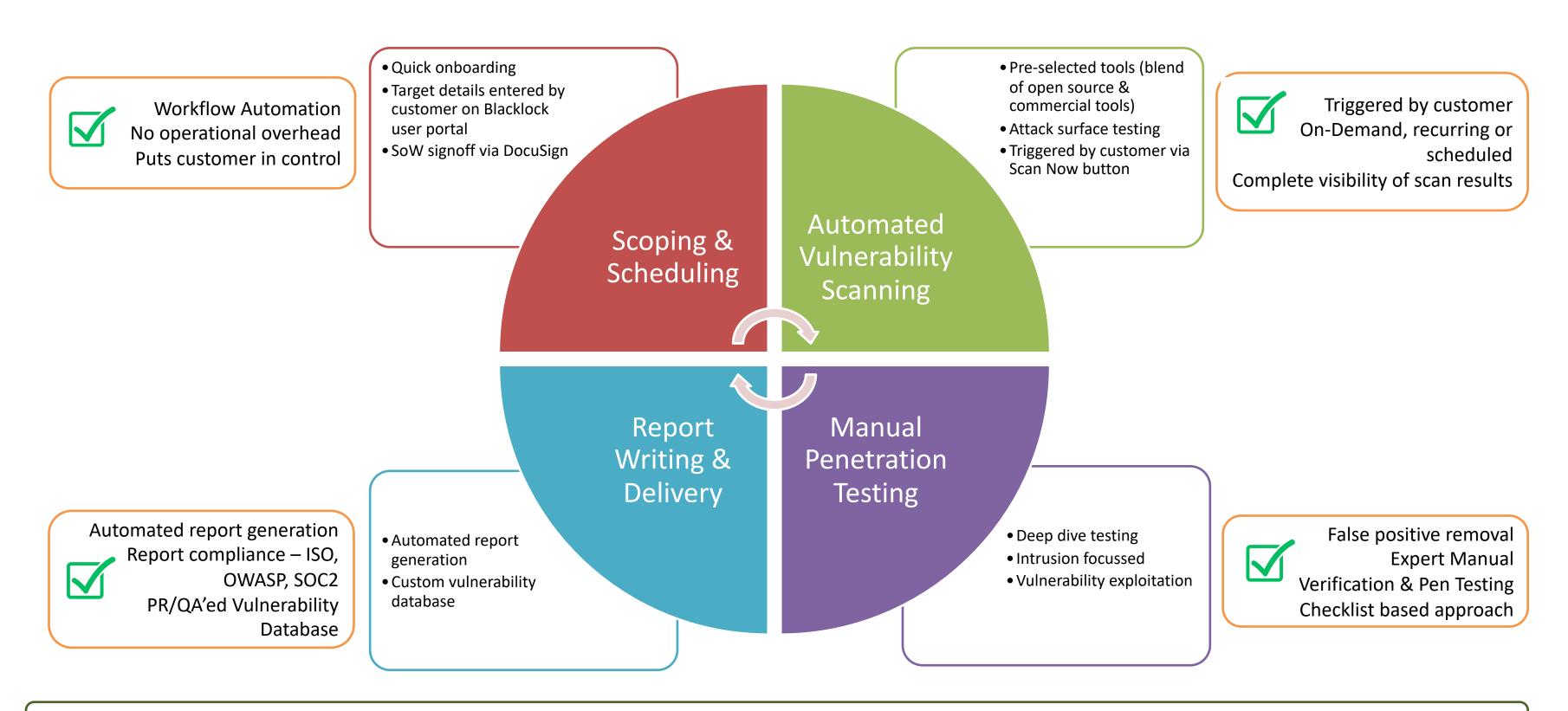
Hire your own pentest team; take 6+ months to make new qualified hires



Solution 3

PTaaS - Adopt a holistic approach to continuous security testing and vulnerability management

Blacklock PTaaS Approach



Continuous Security Testing & Cost Savings through Automation

How is Blacklock different?

Simple, scalable, secure and a cost-effective way to perform continuous security testing

Process automation and tool integration leads to reduced overheads and costs

Dynamic Application Security Testing (DAST)

Platform Independent API for DevOps

Trigger security vulnerability scanning with expert manual validation

Single platform delivery, vulnerability management & reporting

Blacklock Benefits

Reduced Costs - Workflow Automation

Puts YOU in Control - Shifting the control from pentester to YOU

Faster Turnarounds - Pentesters are intrusion-specialists; not just the skilled tool operator

Continuous Security Testing - On-Demand, Recurring, Scheduled or directly from your DevOps pipeline or Blacklock account

Single Delivery Platform - No more tracking of vulnerabilities through PDFs, emails or shared drives

Standout Features

Single Delivery Platform

Dashboard & Security Posture

Vulnerability
Management &
Tracking

Unlimited Vulnerability Scanning

Integrations

CI/CD Integration for DevOps

JIRA – Automated Ticket Creation

Slack – Blacklock Scan & Vulnerability Updates

Reporting

Management & Developer Report

OWASP, ISO, SOC2 Compliant Report

Add your team

Allow developers and managers to view/action vulnerabilities

Role-based access to Blacklock portal

Integrations







Blacklock listings & recognitions



https://aws.amazon.com/marketplace/pp
/prodview-rospeedggwsa4





https://owasp.org/wwwcommunity/Vulnerability_Scanning_Tools

Our Team & Recognitions

20+ years of pentesting experience Industry recognised certifications, CREST CRT, CPSA, CISSP, OSCP, OSCE, CEH.

Technical Advisory Board with ex-Google and veteran cybersecurity members

Dedicated team of pentesters and developers

Executed 200+ pentesting jobs across all major industries

Winner - Reseller's 2021 NZ Innovation Awards Give it a go with 14-day free trial ...





Contact Us

+64 04 280 7403

hello@blacklock.io

www.blacklock.io

Follow us on <u>Linkedin</u> & <u>Twitter</u>