Reliance acsn

Penetration Testing: Service Hardening

Reduce attack vectors, condense the attack surface

Every network interface and software application is a potential attack vector into your organisation. Unnecessary instances of these greatly expand the available attack surface, which – coupled with master image build errors and misconfigurations – can leave your platforms and systems widely exposed to compromise.

Hardening these platforms and systems is the process of removing unnecessary connections and software, and remediating build and configuration errors, so that the overall attack surface is greatly condensed.

Reliance acsn's Service Hardening radically reduces attackers' opportunities to gain a foothold in your IT systems. It identifies a wide range of attack vectors, closes them down, and focuses defences more strongly where the business risk is greatest.

Attackers are faced with far fewer opportunities that might lead to objectives, and far more durable security to frustrate the methods they rely on to pursue them.

What Service Hardening delivers

Reliance acsn's Service Hardening is available both a standalone service and as part of a wider range of Penetration Testing offerings.

Using a combination of human security analysis expertise and industry-leading configuration audit tools, we comprehensively identify risks that could be remediated by Service Hardening on all platforms and services that constitute a principal business concern in your organisation.

Experts who know the tech

We choose specialists who have in-depth knowledge and experience of your specific platforms and services, so they can spot and fix issues faster.

Extensive attack vector audit

Includes non-essential programs, functions, applications, ports, permissions, access, and more, plus build and configuration errors.

Patch and update

We identify missing OS patches and review third-party software to ensure currency, as part of the process.

We secure what stays

We don't only remove what's not necessary – we configure the remaining software and other attack surfaces to maximise their security.

How our approach benefits you

At Reliance acsn, we understand that Service Hardening isn't something you do to tick a box, it's something you do to protect the areas of principal business concern to your organisation.

For this reason, we work closely with you to ensure that we're focusing our services where they'll best defend what's most important to you.

1 We help you achieve compliance

Hardening is a requirement of security compliance frameworks such as PCI-DSS and is typically included in ISO27001 adoption.

2 We deliver more, and flexibly

Service Hardening is just one part of a comprehensive Penetration Testing portfolio, and we can tailor delivery of any and every part of it to your organisation's needs.

3 We involve you in our conclusions

We can test the identified risks under controlled conditions to show you the business risk they represent to your organisation.

4 We're rapid and cost-effective

We can protect many hundreds of servers, workstations and other attack surfaces in a single deployment.

5 We have a proven track record

Government and enterprise clients alike across five continents rely on us to defend their systems against cyber threats.

6 We guide you through next steps

We give you clear recommendations to help address current and immediate vulnerabilities, and we're here to help you through the actions.

About Reliance acsn

Across five continents, enterprise and government clients depend on Reliance acsn to defend them against cyber threats like nobody else can.

Our managed security and consultancy services support organisations throughout the challenges of assurance, awareness, detection, response and prevention, 24 x 7, and focus on business risk – securing not just assets and data, but revenues, too.

- Reliance acsn's history goes back to 2003, with the founding of global cyber security specialist ACSN.
- In 2016, a merger created Reliance acsn in London, UK, to deliver real-time Managed Detection and Response (MDR)
- We've helped scores of the world's top brands plan, deploy and manage robust security solutions, in banking, telecoms, retail, government and insurance.
- Our people are accredited across all the major standards in IT security – including PCI, ISO27001, G-Cloud, CISSP, CREST, and many more – and accredited to support virtually any technology you have in place or are planning to procure.