

Security Testing & Assurance

Customer: PowerShield

Industry: Critical Infrastructure
Battery Monitoring

Services: Penetration Testing &
Security Assurance

Challenges:

- ▶ Securing a full product ecosystem across devices, embedded systems, and SaaS.
- ▶ Protecting critical infrastructure environments from cyber threats.
- ▶ Ensuring PowerShield products can be rolled out in highly secure critical infrastructure environments.

Outcome:

- ▶ Independently tested products prior to release.
- ▶ Strong security posture across platforms in critical infrastructure environments.
- ▶ Increased confidence and trust for customers, operators, partners and stakeholders.

PowerShield

PowerShield provides battery monitoring solutions for critical infrastructure environments. Its technology portfolio delivers secure visibility of battery performance across essential systems.

PowerShield solutions are deployed in environments where uptime and reliability are critical, making cyber security a fundamental requirement of both product design and operation.

The challenge

PowerShield operates in environments where high security is demanded and compromise can have significant operational consequences. As its product ecosystem expanded across connected devices, software, and cloud platforms, maintaining a consistently high level of cyber security across all components became increasingly important.

To ensure the integrity of their solution alongside broader applications and platform security, PowerShield required rigorous and independent validation.

The solution

PowerShield engaged CyberCX as a long-term partner to conduct regular penetration testing and independent security assessments across its product portfolio.

Testing includes:

- ▶ **Controllers and devices:** Security testing of embedded web interfaces and device-level access controls.
- ▶ **Assure SaaS platform:** Comprehensive web application penetration testing using industry best practice methodologies.
- ▶ **Software and integration layers:** Validation of software and platform interactions.

CyberCX applies industry best practices, including OWASP methodologies, supported by manual and automated testing techniques. Each engagement includes:

- ▶ **Executive reporting** for business-level assurance.
- ▶ **Technical reporting** with prioritised remediation actions.
- ▶ **Retesting cycles** to validate fixes and confirm risk reduction.

All findings are fed directly into PowerShield's development lifecycle, strengthening secure-by-design practices and continuously improving product resilience.

The outcome

Through its ongoing partnership with CyberCX, PowerShield has embedded independent security penetration testing into its core product development and release process, ensuring:

- ▶ Independent assurance that all products are rigorously tested before deployment;
- ▶ Strong security posture across devices, software, and SaaS platforms;
- ▶ Continuous improvement through structured remediation and regression testing; and
- ▶ Increased customer confidence in protecting critical infrastructure systems.

By partnering with CyberCX, PowerShield ensures its solutions remain secure, resilient, and trusted for deployment in critical infrastructure environments.

"PowerShield's engagement with CyberCX has delivered measurable improvements across both product security and the software development lifecycle, embedding security as a core discipline of development."

Paul Hectors, Chief Technical Officer
PowerShield

About CyberCX

CyberCX, part of Accenture, is the leading provider of professional cyber security services across Australia, New Zealand, UK and US. With a workforce of over 1,400 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents and build resilience in an increasingly complex and challenging threat environment.

Contact us to find out how CyberCX can boost the cyber security skills of your entire organisation.

