Black Start
Critical service recovery
Prepare for the Nightmare Scenario

DEV/NULL

Imagine waking up to find every system that keeps your business alive; identity, network, authentication, firewalls, monitoring, and backups has been wiped out. Whether through ransomware, sabotage, network outage, zero-day vulnerability, or hardware failure, everything is now encrypted or unusable.

Slow recovery is an existential threat.

This is a *black start* scenario: The organisation's entire digital nervous system must be rebuilt from bare metal, trusting nothing that remains online.

Black Start Resilience Framework

Delivers a battle-ready recovery that lets you jump back into business. Fast. Clean. Audit-ready.

- **Reliable, secure rebuild** of your most business-critical systems. Your key network, servers, and applications automatically recovered in parallel.
- A **tamper-proof inventory** of assets and settings. All baseline configurations are digitally signed and offline. A **clean source of truth**.
- **Ready to use recovery scripts**. Build scripts, verified images, and emergency recovery kits.
- **Regulator-aligned, provable recovery processes**. Documented, auditable, and compliant.

This gives confidence that your organisation can accelerate its return to business-critical operation.

The outcome

A hardened, auditable foundation that turns a 'what if' into a 'how we will':

- A trusted **source of truth**
- A regulator ready, **proven capability**
- **Proactive resilience**
- **Accelerated, automated, and simultaneous restoration** capability

On the worst possible day for the organisation, this approach ensures it is not the end of operations, just the start of a structured recovery.

How do we deliver the service?

We employ a three-phase approach:

1. **Assessment and validation of current Disaster Recovery (DR) capability**
   - Prove what works, and what fails, under black start conditions
   - Identify critical system dependencies and trust gaps
2. **Design and prove a Black Start Recovery Process**
   - Produce business-ready recovery playbooks
   - Engineer a bare-metal rebuild processes for identity, network, and business-critical services
3. **Black Start Support**
   - Support from expert crisis engineers to rapidly restore business-critical services.

Signs you will find value

This approach is particularly helpful if you are worried about:

- **Uncertain system settings**: If you can't be sure that your core configurations (like user accounts, network rules, firewalls, etc.) are correct, you'll benefit from a clear, trusted reference.
- **At-risk backups**: Backups that might be lost, corrupted, or tampered with by ransomware, insider actions, or hardware failures can cripple recovery.
- **Missing recovery plan:** If your incident-response team doesn't have a clear, tested procedure for wiping and rebuilding an entire environment quickly and securely, this service fills that gap.

By using unchangeable, digitally verified data, you can cut the time your organisation spends out of action and speed up the return to normal operations.

Why choose Security?

A blackout is not just an IT outage. It is a crisis, requiring:

- Zero trust in existing systems
- Forensic assurance of configuration integrity
- Immutable evidence of clean baselines
- Anti-tamper controls, insider threat protection, and cryptographic validation

Black start is fundamentally a security capability, not an operational one.

Complementary roles:

- IT Operations excels at availability during normal conditions.
- Security excels at ensuring trust, integrity, and resilience against adversary actions.

A security-led approach provides:

- Independent governance and dual control protection
- Cryptographically signed baseline configurations
- Immutable ledgers and offline, tamper-proof storage
- Defensive engineering for catastrophic, adversarial events

When the entire estate is untrusted, Security holds the keys to recovery.

Why Dev/Null?

Precision:

Superior analytical skills to identify weaknesses, assess risks accurately, and recommend effective solutions based on real-world scenarios and proven best practices.

Reliability:

A consistent ability to meet deadlines, deliver high-quality work, and provide clear communication throughout the engagement process.

Security expertise:

Comprehensive understanding of security tools, methodologies, and industry standards, ensuring accurate assessments and effective recommendations.

Trust:

Building trust through transparent communication, reliable delivery, and proven expertise in security assessment and management.

Innovation:

The ability to bring new ideas, innovative approaches, and creative solutions to traditional security challenges, ensuring clients stay ahead of emerging threats.

Collaboration:

Fostering open dialogue, active listening, and effective communication to ensure the best possible outcomes for your security needs.

Book a conversation with one of our consultants to explore how Black Start can protect you.

info@devnullsecurity.co.uk