



When acquiring or divesting a business, there is risk for all parties involved. Our Merger & Acquisitions (M&A) Transition Support service helps organisations manage cyber risk across the entire merger, acquisition, and divestiture lifecycle.

More detail

Pre-Deal Cyber Due Diligence

- Rapid, time bound cyber risk assessment of acquisition or divestment targets.
- Prioritised and actionable report of hidden risks to support deal decisions, valuation discussion and risk acceptance.

Strategic Integration

- Develop pragmatic cybersecurity integration strategies aligned with enterprise risk appetite and business priorities.
- Define governance, policies, and operating models for the merged entity.
- Establish clear ownership, accountability, and reporting structures during transition.
- Align short-term controls with long-term security strategy.

Secure Transition & Day-1 Readiness

- Implement interim security controls to protect critical assets during transition.
- Implement secure connectivity, identity management, and data protection from Day-1 for merged environments.
- Maintain continuity of operations while longer-term integration or separation activities are delivered.

Benefits

This service is particularly beneficial for organisations who would like:

- Cybersecurity to be a key enabler of successful business consolidation and growth.
- A structured assessment of current states to be merged.
- Visibility into inherited risks.
- Integration, and transformation support.
- Mature cybersecurity operations across newly combined entities.

What's included in the Dev/Null service?



Initial Consultation:

Initial consultation to understand your objectives and environment.



Current State Review:

A comprehensive view of the current state of the target business security architecture.
Identify control gaps and uplift in technology requirements.



Risk Assessment:

Rapid and detailed assessment of risk due to organisational change to understand potential impact

Identify the security posture, vulnerabilities and compliance gaps. This will include taking inventory and analysis of the IT Assets, infrastructure to identify known active breaches.



Executive-level reporting:

Executive-level reporting with actionable recommendations on critical findings and priorities for day-1 controls



Supply Chain Assessment:

Perform detailed review of third, fourth party relationships and review the security posture and identify any risks they may possess.



Strategic integration:

Advice on how to transition services in the best way possible, including go/no go inputs
Develop a detailed integration plan with a focus on securely combining systems and data.
Advice on necessary security measures to protect against future cyberattacks.
Post-transition support from our expert team

Why Dev/Null?



Responsive:

We stay flexible and adapt to your priorities, whether that means shifting focus within a project or responding to an emerging threat to provide the best security for you. Our fast-turnaround, communication, and flexible engagement models keep you moving forward without delays.



Evolving:

Continuous learning is at the core of our culture: we routinely assess, refine, and re-engineer our processes, tools, and skills to stay ahead of the threat landscape. This mindset translates into more effective, efficient, and resilient solutions for you.



Sustainable:

We design security architectures and practices that endure, focusing on long-term resilience rather than quick fixes. By embedding best practices, automating controls, and aligning with your business roadmap, we foster a culture of continuous improvement.



Established:

Our team brings deep operational experience developed across a broad range of industries and security domains, backed by proven industry and vendor certifications, and a portfolio of real-world successes. That depth of knowledge lets us solve complex problems with confidence and speed.



Enabling:

Beyond delivering services, we actively coach your staff, sharing best practices, conducting workshops, and providing hands-on training to mature your capability. The result is an empowered internal team that can sustain and expand the gains we deliver.



Actionable:

Complex cybersecurity concepts are distilled into plain language, ensuring every stakeholder, from executives to engineers, understands the risks, options, and recommended actions. This clarity drives informed decisions and smooth collaboration across your organisation.

Who to choose

Choosing the right partner for your Cybersecurity M&A Transition Support is essential to making informed decisions and protecting your business. At Dev/Null, we understand that every M&A activity carries unique risks, especially in today's complex threat landscape. Our role is to help you see beyond the surface, to uncover hidden vulnerabilities, to assess cyber maturity, and to identify integration challenges before they become costly issues.

We bring together decades of collective experience across all facets of cybersecurity, from governance and compliance to threat detection, response, and technical operations.

By combining hands-on operational experience with clear, executive-ready insight, we ensure cybersecurity enables the transaction rather than delaying it.

Book a conversation with one of our consultants to explore how we can help with M&A Support.

info@devnullsecurity.co.uk