CERBERUS**SENTINEL**

The Necessity of Cybersecurity Assessment During M&A

Cerberus Sentinel brings both the experience and expertise to support the M&A lifecycle.

Preliminary Due Diligence

Review historical penetration test reports:
High-level identification of red flags

Review historical risk assessment reports:
High level identification of cyber assets and liabilities

Dark Web Scan:
Identification of any exfiltrated data, compromised credentials, and other sensitive corporate information currently in the hands of cyber attackers

Synergy and Value Qualification

In-depth Penetration Test with detailed report:
Full-access security testing on all areas of the target environment to uncover key vulnerabilities that attackers can exploit

In-depth Risk Assessment with detailed report:
Assessment of target's cybersecurity controls to identify gaps and prioritize remediation plan

Itemized Cost Analysis:
Provide estimated remediation costs for integration planning and/or negotiations

Remediation of Security Gaps

Example Activities Include:

- Update patching and vulnerability management
- Security monitoring (MDR, XDR, SIEM)
- Update cybersecurity policies and procedures
- Security awareness training
- Vendor reviews to mitigate 3rd party supply chain risk
- Backup and recovery architecture
- Firewall audit and update
- Identify architectural weaknesses
- Secure code review

CERBERUS SENTINEL