protiviti®

Global Business Consulting

Cybersecurity Due Diligence

Pre- and Post-Acquisition Cybersecurity Support

Mergers and acquisitions are significant events for organizations looking to grow their business and expand their offerings. Organizations are discovering that simple due diligence questionnaires are no longer sufficient to assess the operational risk of integrating a new acquisition. Additionally, due to pre-close confidentiality, there may be difficulty in performing a full technical assessment of the acquisition while maintaining separation during the close process.

Protiviti's pre/post acquisition security packages quickly and effectively provide insight into target organizations that standard security audits or questionnaires do not achieve, while providing a level of separation between the two organizations. Upon completion of the assessment, Protiviti will provide a full report, including technical details and remediation steps, providing an organization with a much deeper understanding of the cybersecurity maturity of the acquisition target.

How Protiviti Can Help

Network Security Assessment

Conduct security testing to gain an understanding of the security posture of the target acquisition's networks and systems

Application Security Assessment

Assess the target acquisition's products and web/mobile applications to identify weaknesses which may allow an attacker to gain unauthorized access or sensitive data

Cloud Security Assessment

Review the cloud environments used by the acquisition target to identify possible misconfigurations which may present risk to the organization

Threat Assessment

Identify existing threats to the target acquisition by conducting threat intelligence assessments and executing "threat hunting" exercises

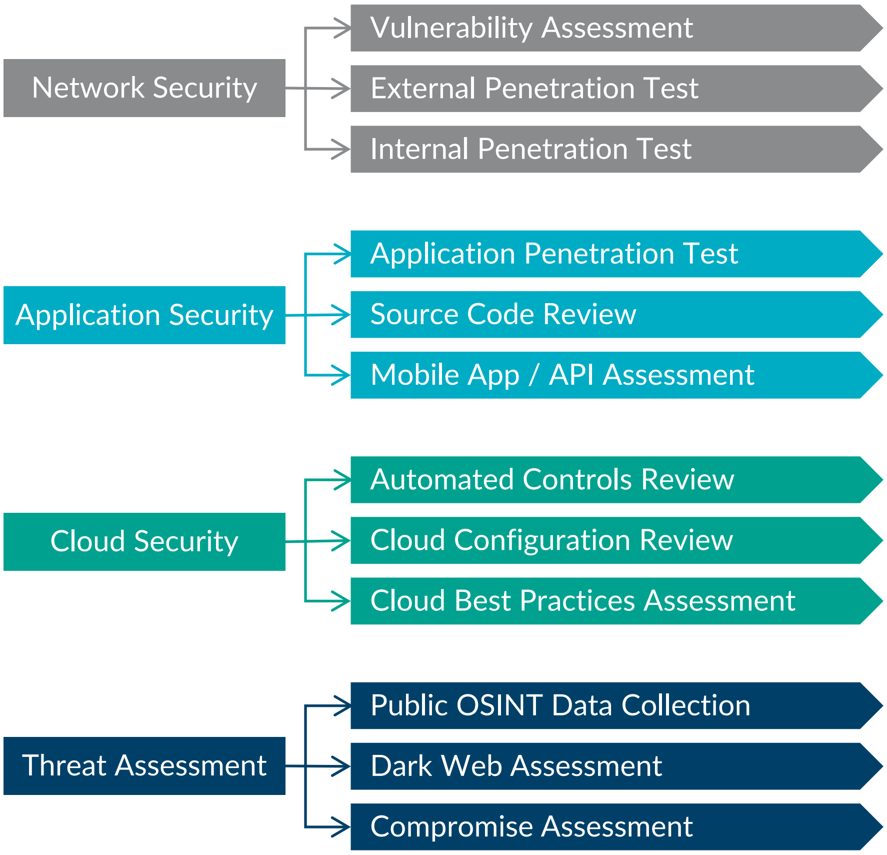
Business Outcomes

- Clear risk profile of an acquisition target
- Deep understanding of technical security posture
- Identification of past security threats and potential compromises
- Detailed list of recommendations needed to address identified issues

INNOVATE. TRANSFORM. SUCCEED.

Cybersecurity Due Diligence

Protiviti’s security assessments supporting due-diligence efforts typically focus on one, or many, of the following areas:



Network Security	Vulnerability Assessment	Where do we have known issues, vulnerabilities or misconfigurations?
	External Penetration Test	Can an external attacker breach our perimeter controls?
	Internal Penetration Test	If an attacker gains internal access, what would be impacted?
Application Security	Application Penetration Test	Can an attacker exploit our applications to gain access to sensitive data?
	Source Code Review	Are we following secure coding practices when developing applications?
	Mobile App / API Assessment	Have we exposed services that could be exploited to gain access to data?
Cloud Security	Automated Controls Review	Are there clear misconfigurations, exposing cloud environments to attack?
	Cloud Configuration Review	Is our cloud environment architected in a secure manner?
	Cloud Best Practices Assessment	Does our cloud have protections to detect and defend against attacks?
Threat Assessment	Public OSINT Data Collection	How much information about us is available on the clear web?
	Dark Web Assessment	How much information about us is available on the dark web?
	Compromise Assessment	Has a malicious threat actor compromised our environment?

Fortune 500
Technology Company

M&A Due Diligence Assessment

Business Requirement

A global technology company was looking to quickly pivot to a new line of business through a targeted acquisition. Given the importance and exposure of the acquisition, the company wanted a pre-close technical security assessment to understand the security posture of the networks, applications and cloud environments they would be integrating into their business.

Solution Delivered

Protiviti was able to quickly bridge the security teams between the two organizations and, in the limited time available, performed a full suite of penetration tests, application security assessments, cloud configuration reviews and threat assessment activities against the target company to gain an understanding of existing issues and threats facing the organization.

Business Results

Protiviti provided a summary report which clearly articulated the threats, risks and issues identified, which helped the acquiring company understand and plan for security controls, headcount and budget that would be necessary post-close to bring the acquisition up to their standards.

Protiviti.com/TechnologyConsulting **TechnologyConsulting@Protiviti.com** **TCblog.Protiviti.com**

protiviti®
Global Business Consulting