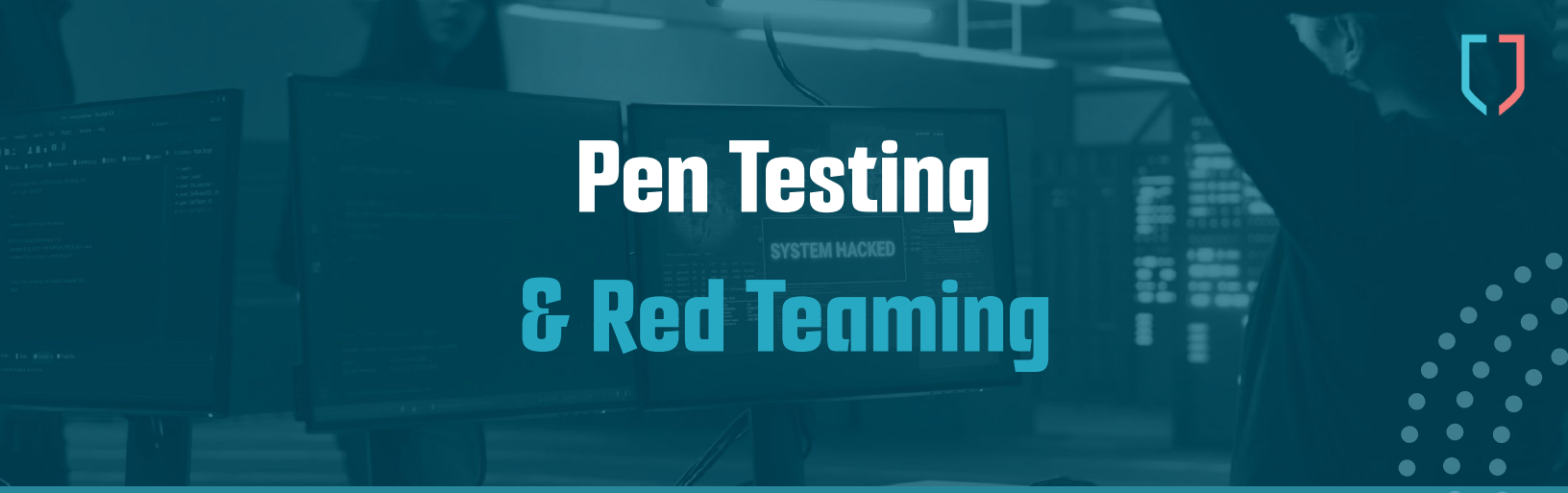

Pen Testing & Red Teaming

Ihre Systeme wirken stabil, aber Angreifer müssen nur eine einzige Schwachstelle finden. Ein offener Port, ein falsch konfigurierter Service, ein unachtsamer Klick – und Fremde können sich unbemerkt in Ihrem Netzwerk bewegen.

Penetrationstests und Red Teaming geben Ihnen Klarheit darüber, wie widerstandsfähig Ihre Umgebung wirklich ist – unter realistischen Bedingungen und aus der Perspektive eines Angreifers.

Was ist Pen Testing & Red Teaming?

Pen Testing:
Wir prüfen Systeme, Anwendungen, Netzwerke, Cloud-Dienste und Prozesse auf verwertbare Sicherheitslücken – so, wie echte Angreifer es tun würden.

Ihr Nutzen:

- Klare Sicht auf technische Schwachstellen
- Priorisierte Empfehlungen nach Risiko und Geschäftsrelevanz
- Validierung von Sicherheitsmaßnahmen und Konfigurationen
- Schutz Ihrer Systeme vor bekannten Angriffswegen

Red Teaming:
Wir simulieren einen vollständigen Angriff: Social Engineering, physische Tests, initial access, lateral movement und Datenexfiltration – unauffällig, mehrstufig und realitätsnah.

Ihr Nutzen:

- Realitätsgetreue Einschätzung Ihrer gesamten Sicherheitslage
- Messung der Effektivität von Logging, Detektion und Reaktion
- Sichtbarkeit über echte Angriffswege in Ihrer Umgebung
- Stärkung von Incident-Response-Teams und Sicherheitsprozessketten

Warum AwareTec®?

Erfahrene Offensive-Sicherheitsspezialisten – Unser Team besteht aus deutschen und israelischen zertifizierten Pen Testern und Threat-Analysten mit Erfahrung in echten Angriffsszenarien.

Ergebnisse mit echtem Mehrwert – Sie erhalten klare Prioritäten, aussagekräftige Risikoanalysen und konkrete Maßnahmen, die sofort umsetzbar sind.

Unterstützung für technische Teams und Führungskräfte – wir helfen Ihren technischen Teams ebenso wie Ihren Entscheidern. So gewährleisten wir, dass sowohl technische Maßnahmen als auch Kommunikations- und Compliance-Anforderungen Hand in Hand gehen.