keypoint

Solution spotlight
Red teaming

How secure are your organisation, applications and networks – and your physical security?

Red teaming - a multi-blended, simulated attack orchestrated from the perspective of a malicious actor - helps find security loopholes and gives clients a 360-degree perspective - without the pressure of a headline-causing cyber security breach.

Red team overview

Red team tests realistically simulate a virtual and physical security attack, attempting to uncover security vulnerabilities that might otherwise be discovered by bad actors and offering a genuine overview of the risks and vulnerabilities threatening your technologies, people and physical assets.

Red teaming covers your applications, networks, social engineering and physical security:

Technology
including networks, applications, routers, switches and appliances

People
such as staff, independent contractors, departments and business partners

Physical assets
from offices and warehouses to substations, data centres and buildings

A selection of work products

- High-level non-technical summaries for executives and senior-level management
- Detailed technical report for security professionals - with step-by-step information that sets out our findings
- Fact-based risk analysis linking critical findings to specific assets
- Tactical recommendations for immediate improvements
- Strategic recommendations for longer-term improvement

For more information, please contact Keypoint IT Consulting.

Srikant Ranganathan
Senior Director, IT consulting
T +973 17206827
srikant.Ranganathan@keypoint.com

Sagar Rao
Assistant Manager, IT consulting
T +973 17206802
sagar.rao@keypoint.com