1. Technical vulnerability assessment (core service selection)

Please select the type of the security test you would like us to perform	Infrastructure	Application
External	☐	☐
Internal	☐	☐
WiFi	☐	☐
Social engineering / phishing campaign	☐	☐
DDoS / performance assessment / stress test	☐	☐

2. Scope for external vulnerability assessment (if selected above)

Network domains to be tested (e.g., in.gr)		
Corresponding public IP network(s) of the domain above		
Number of "live" systems in the IP range (including network elements, VPN concentrators, FWs etc.)		
Are you using a public / hybrid cloud (e.g. AWS, Microsoft Azure) as IaaS for hosting any infrastructure services?	Yes ☐	No ☐
Number of "live" systems in the IaaS IP range (if applicable above)		
Website FQDNs or subdomains to be tested (i.e., www.in.gr)		

Website type	Type	Selection
	personal website	☐
	photo sharing website	☐
	authors website	☐
	community building website	☐
	mobile device website	☐
	Blogs	☐
	informational website	☐
	online business	☐
	directory website	☐
	e-commerce website	☐

VELOCITY CHECK

CLOSE THE LOOP

Is there a WAF present?	Yes ☐	No ☐
Is the website onramp a security CDN (e.g. cloudflare, Akamai etc.)?	Yes ☐	No ☐
Does the website have a test environment?	Yes ☐	No ☐
Does the website have a content management system (CMS) e.g. joomla, drupal, custom, wordpress?	Yes ☐	No ☐
What is the maximum duration of the external security test e.g. 2 weeks		

3.   Scope for Internal vulnerability assessment (if selected above)

IP network(s)		
Number of "live" systems in the IP range (including network elements, VPN concentrators, FWs etc.)		
Are you using a private / hybrid cloud (e.g. AWS, Microsoft Azure) as IaaS for hosting any infrastructure services?	Yes ☐	No ☐
Number of "live" systems in the IaaS IP range		
No of windows servers		
No of windows workstations		
No of Linux/Unix servers		
No and type of DBs		
No and type of special applications (e.g. CRM, ERP, ticketing, accounting, etc.)		
No and type of network elements (e.g. switches, routers, bridges, concentrators, NAS, SAN, nw-printers etc.)		
No and type of security gateways (e.g. FWs, IDS/IPS, NWAV, NAC etc)		
Offline password cracking?	Yes ☐	No ☐
What is the maximum duration of the internal security test e.g. 2 weeks		

4. Scope for WiFi vulnerability assessment (if selected above)

No of physical locations hosting WiFi APs		
No of SSIDs		
Type of SSIDs	Enterprise ☐	Guest ☐
Corresponding IP network(s)		
Number of "live" systems in the wireless IP range (including network elements, VPN concentrators, FWs etc.)		
Offline password cracking?	Yes ☐	No ☐

5. Scope of the phishing campaign (if selected above)

No of internal users to target		
Email messaging threshold e.g. 5		
Social network messaging e.g. linkedin, FB, Instagram etc	Yes ☐	No ☐
Is training / awareness required after the test?	Yes ☐	No ☐

6. Scope of the DDoS test (if selected above)

	Type	Selection
	Volumetric (infra)	☐
Please select the type of DDoS attacks	Email bombing (email server)	☐
	GET/POST requests (web server)	☐
	Amplification (application)	☐

IP Network / IP addresses	Subnet Mask	Whitelist IP addresses
Please list the IP network(s) or the host(s) IP addresses to be tested	Please list the network(s) subnet mask	Please list the IP addresses of 5 hosts or more their network traffic of which will be diverted during a DDoS attack