Startups & SMEs application form[1]

10th CYBER INVESTOR DAYS

1-2 December 2021 // Helsinki, Finland

European cybersecurity start-ups and scale-ups are invited to provide their company's profile and indicate whether they are looking for **access-to-finance** opportunities (B2B meetings with potential investors). Companies seeking **access-to-market** opportunities (B2B meetings with potential customers and partners, i.e. integrators, corporates etc) are also invited to apply.

IMPORTANT: The duly filled application form (pdf) and the 5-7 slides pitch deck (pdf) shall be sent to wg4_secretariat@ecs-org.eu.

DEADLINE: Monday, 18 October 2021, midnight CET.

ADVICE: Keep your application short and concise. Respect the indicated character limit.

[Insert company's name] *[Insert company's logo]*

COMPANY PROFILE	CONTACT DETAILS
Market Segment: to be identified in the table below Product Launch: *[insert]* Employees: *[insert]* HQ Address: *[insert]* Website: *[insert]*	Name, Surname: *[insert]* Email: *[insert]* Phone: *[insert]* +1 representative (name, surname, email): *[insert]*
YOUR INVESTORS	
[please list them down here]	

[1] Your personal data controller is the European Cyber Security Organisation (ECSO), registered at Rue Ducale 29, 1000 Brussels, Belgium. Please note that the data you provide in the application form will be used for the selection of the cybersecurity start-ups and SMEs to the Helsinki edition of the Cyber Investor Days, taking place on 1-2 December 2021. ECSO will use the provided contact details for the organisational purposes of the event: to update the participants about the selection results, the logistics and other event-related information. ECSO undertakes not to disclose the information and documents of any kind whatsoever. At any moment, you can email ECSO via wg4_secretariat@ecs-org.eu and ask for the removal of your data. To obtain detailed information about your rights, please contact us directly via wg4_secretariat@ecs-org.eu, or by posting a letter to: European Cyber Security Organisation (ECSO), Rue Ducale 29, 1000 Brussels, Belgium.

YOUR BOARD (CEO Funder, CTO Funder, etc):
[please list them down here]

UNIQUE VALUE PROPOSITION – Problem, Solution, Product	
Target Audience / Customer	*[insert]*
Statement of Need & Opportunity	*[insert]*
Product / Service Name	*[insert]*
Key benefits / Problem-solving capacity	*[insert]*
Primary Competitive Alternative	*[insert]*
Statement of Primary Differentiation	*[insert]*

MARKET & GO-TO-MARKET STRATEGY – 400 characters max (channels, geographies, segment priorities)
[insert, 400 characters max]

BUSINESS MODEL & USE OF PROCEEDS – 400 characters max (non-recurring vs. recurring; please quantify your use of proceeds – how much € & for what)
[insert, 400 characters max]

COMPETITION ON THE MARKET – 400 characters max (names & countries of your Top 5 contenders for the same customer budgets)
[insert, 400 characters max]

TEAM SIZE AND TEAM VISION – 400 characters max (relevant & well-rounded experiences, industry-specific skills, clear roles, notable advisors)
[insert, 400 characters max]

COMPANY COMPETITIVENES: TOP 3 ADVANTAGES – 400 characters max (p.s. 'we have the best team' will not count as a competitive advantage – it must be systematic advantages)

[insert, 400 characters max]

FINANCIAL INFORMATION

Current Stage: *[insert]*
Previous Capital: *[insert]*
Monthly Burn Rate: *[insert]*
Capital Seeking: *(does not apply for access-to-market opportunities)*: *[insert]*

ANNUAL FINANCIAL OVERVIEW *(in thousand euros, €)*

Financial year	2019	2020	2021	2022	2023
Revenues					
Expenditure					
Net profit					

MARKET SEGMENT
(mark the capabilities and categories that your company meets)

Capability	Solution Category	Company's market segment
IDENTIFY	Asset Mangement	
	Business Environment	
	Governance & Risk Management	
	Risk Assessment	
	Risk Management Strategy	
	Supply Chain Risk Management	
PROTECT	Identity Management & Access Control	
	Awareness and Training	
	Data Security	
	Information Protection Processes and Procedures	
	Maintenance	
	Protective Technology	
DETECT	Anomalies and Events	
	Security Continuous Monitoring	
	Detection Processes	
RESPOND	Response Planning	
	Communications	

	Analysis	
	Mitigation	
	Improvements	
RECOVER	Recovery Planning	
	Improvements	
	Communications	