Funding program	Opslag	Målgruppe	Beskrivelse	Deadline for ansøgning
Digital Europe	Strengthening the SOC Ecosystem	National SOCs, Cross-Border SOC Platforms and other relevant stakeholders	This topic complements other actions in this and the previous Work Programme, which are building up National SOCs and Cross-Border SOC platforms. It will empower SOCs which are linked to National SOCs, and to a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms, leading to an increased data sharing and better detection capability for cyber threats. This should in particular foster interoperability, identifying what data can be shared, how this is shared and in what format, requirements and sharing agreements, and ways to enable better exchange. Links to the actions funded under the Cybersecurity Skills Academy (in the main Digital Europe work programme) can also be envisaged.	21/01-2025
Digital Europe	Development and Deployment of Advanced Key Technologies	The target stakeholders are technology companies, especially SMEs, working to provide and support other private and public organisations with cyber threat detection and CTI feeds.	Breakthroughs in Key Digital Technologies such as Artificial Intelligence (including generative AI and adversarial AI), Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking, create new opportunities for advancing cybersecurity in the areas of vulnerability detection, threat detection and rapid response, reducing the window of opportunity for attackers to exploit these vulnerabilities. Furthermore, they may enable new possibilities to protect data security and privacy. 27 The objective is to enable European cybersecurity actors to take advantage of these new breakthroughs, improving detection and prevention capabilities, efficiency, scalability, and facilitating data sharing and regulatory compliance.	21/01-2025

Digital Europe	Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations	This topic targets in particular industrial players, national cybersecurity authorities, national cybersecurity competence centres, National Coordination Centres, private entities and any other relevant stakeholders.	This mechanism aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.	21/01-2025
Digital Europe	Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)	This topic targets relevant industrial stakeholders, including SMEs and start-ups.	The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555)34, the Cybersecurity Act35 , and the Directive on attacks against information systems (Directive 2013/40)36. It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous Digital Work Programme.	21/01-2025
Digital Europe	Enlarging existing or Launching New Cross-Border SOC Platforms	Public bodies acting as National SOCs linked to a “call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU”.	This action aims at new cross-border SOC platforms, as well as supporting those that were already launched under the previous DIGITAL work programme (2021-2022). While the main focus of this action is on processes and tools for prevention, detection and analysis of emerging cyber-attacks, it also foresees in particular the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU.	21/01-2025
Digital Europe	National SOCs	Public bodies acting as National SOCs linked to a “call for	The objective is to create or strengthen National SOCs, in particular with state-of-theart tools for	21/01-2025

		expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU".	monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs. They will also, where possible, benefit from information and feeds from other SOCs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis.	
Horizon Europe	Mitigating new threats and adapting investigation strategies in the era of Internet of Things	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	There are a number of implications particular to IoT devices, which have been consistently highlighted by researchers and Police Authorities. IoT devices may represent a threat that goes beyond the digital world, i.e. they may become an increasingly physical threat, since they find applications in, e.g., industry and infrastructure, as well as in building smart cities. Therefore, the successful proposal should help Police Authorities understand the implications of the fast-developing IoT environment in order to keep pace with the evolution of its applications, recognise and tackle the emerging (digital and especially physical) threats that this may pose.	20/11-2024
Horizon Europe	Lawful evidence collection in online child sexual abuse investigations, including undercover	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	Research in this area should tackle legislative frameworks to collecting evidence in online, including undercover, investigations of child sexual abuse, leading to guidelines and manuals that would make the capability available across the EU to target these offenders more effectively. The results of this research topic (training, manuals guidelines) should be shared among all European Police Authorities, notably via CEPOL, provided that the Agency opts out from applying for funding under this topic.	20/11-2024

Horizon Europe	Resilient and secure urban planning and new tools for EU territorial entities	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	The proposals should include a high level of confidence in data management and sharing, provide solutions on cybersecurity issues and take on board new type of threats. The proposed solutions should suggest trusted shared architectures, trusted data collection, secure computation on the data and management processes, modelling capabilities, hypervisor supporting global situational awareness with open and trusted API's, trusted data processing engines and, e.g., artificial intelligence tools.	20/11-2024
Horizon Europe	Advanced real-time data analysis used for infrastructure resilience	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	Resilience of smart cities is marked by a set of specific requirements taking into account most notably aspects from the integration considering user centred approaches as well as social and ethical aspects of Industrial Internet of Things (IIoT), AI/ Machine Learning approaches for real-time data analytics, ensuring transparency, sufficient knowledge and their operational challenges in this area.	20/11-2024
Horizon Europe	Approaches and tools for security in software and hardware development and assessment	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	Software is at the foundation of all digital technologies and, as such, at the core of IT infrastructures, services, and products. The EU should be able to rely on software and hardware that can be verified and audited as to their security. In particular, the potential security implications of using open-source software and hardware, and security auditability in that context, should be further explored. Software is subject to continuous update, so the security posture cannot be assessed once and for all, hence methods and tooling to perform continuous assessments of security are needed. In addition, security and privacy regulations also	20/11-2024

			evolve, having to be factored in compliance approaches.	
Horizon Europe	Post-quantum cryptography transition	Læs nærmere herom i opslaget og Annex B for arbejdsprogrammet.	Post-quantum resistant cryptographic algorithms should be deployable in a dynamic manner in order to quickly react to new quantum computer developments. Recommendations for post-quantum cryptography have already been published, but have to be maintained up-to-date. Proposals received under this topic should contribute to developing coordinated European recommendations for the transition to post-quantum cryptography across the EU.	20/11-2024
SMV:Digital	Digital ansvarlighed: It-sikkerhed og dataetik - Tilskud til privat rådgivning på 50.000 kr. | SMV:Digital (smvdigital.dk)	Ansøgninger åbner 31. okt 2024, og midler tildeles efter først-til-mølle princippet.	Søg om tilskud på 50.000 kr. og få hjælp til at styrke din virksomheds digitale sikkerhed eller til at tænke dataetik ind i måden, din virksomhed behandler data på.	n/a