



**Technische Hochschule
Brandenburg**
University of
Applied Sciences

Gefördert durch:



Bundesministerium
für Forschung, Technologie
und Raumfahrt

AI MODIFIED

AI-Empowered Cybersecurity in Healthcare: Joining Forces in the Digital Health Security Research Hub

Prof. Dr. Michael Pilgermann

11th eHealth Security Conference
07th Oct. 2026 | Nicosia, Cyprus



Agenda today

- 1) Status quo: AI potential for digital security in healthcare
- 2) Health cybersecurity research history
- 3) DHS-RH: the network in a nutshell
- 4) Overview: Horizon call
- 5) Get in touch with us



Your presenter



Prof. IT Security @ THB

- Computer Scientist with focus on IT security
- History in CI, network security and security monitoring
- Since 2021: Prof. IT-Security at UAS Brandenburg (THB)

MedSec & Research

- Head of MedSec: Research Group focussing IT Security of hospitals
- Cybersecurity & Microlearning (SCALE-C)
- DHS-RH

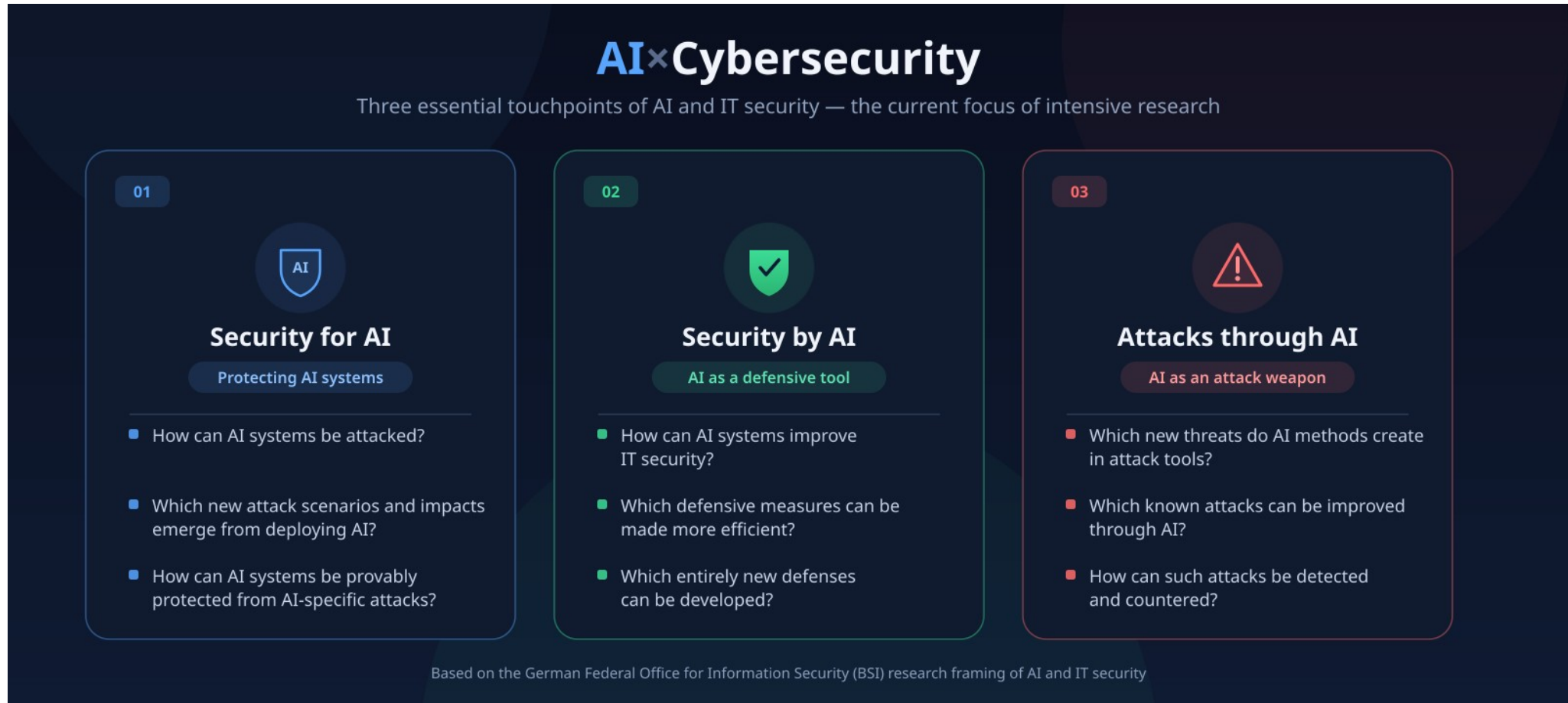
Spokesman UP KRITIS

- UP KRITIS = cooperation (industry and administration) for protection of CI (*2007)
- Around 1000 participants
- Spokesman since 2024



AI potential for digital security in healthcare

Touchpoints of AI and IT security

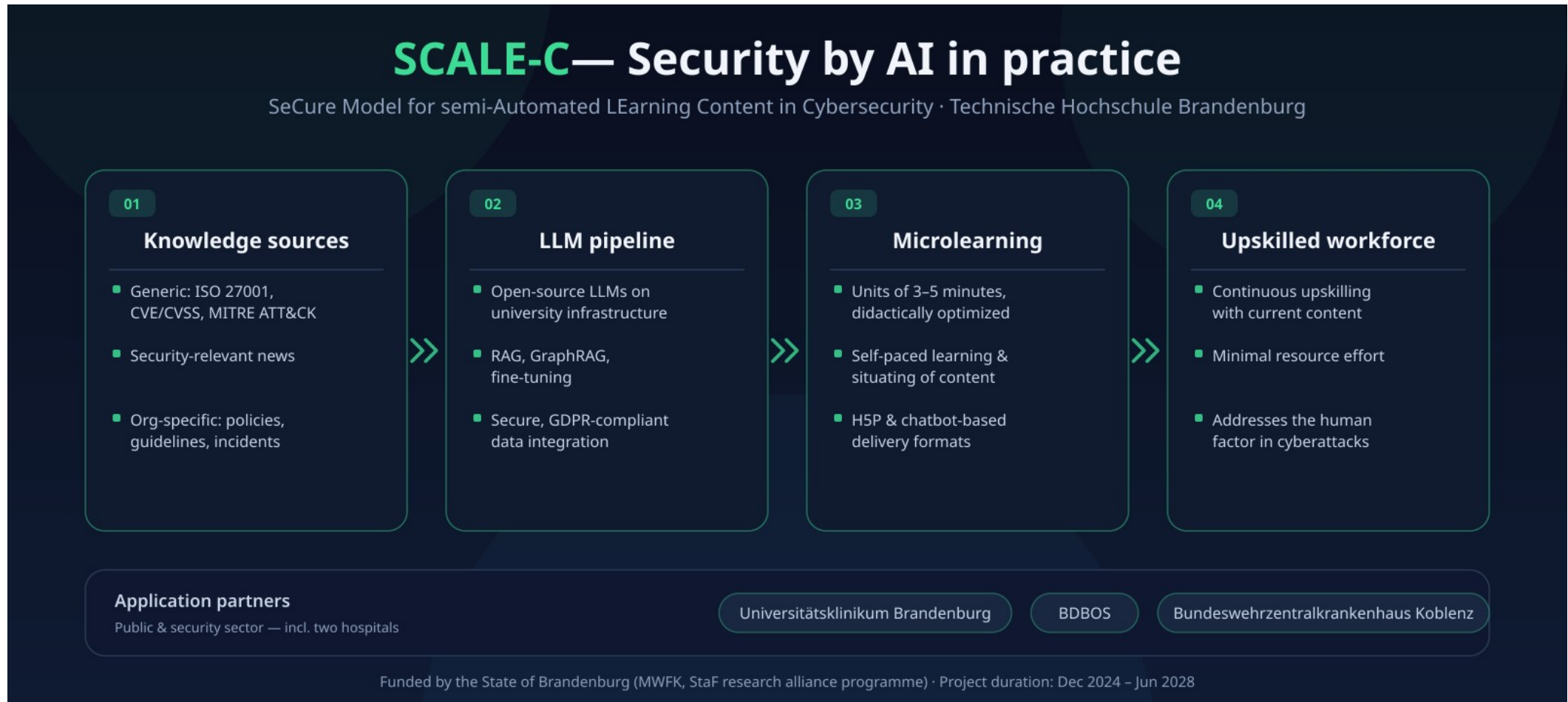


https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html



AI potential for digital security in healthcare

Specific use case: SCALE-C



<https://www.th-brandenburg.de/forschung-und-kooperation/scale-c/>



AI potential for digital security in healthcare

Security by AI	Attacks through AI
<p>Recent research results</p> <ul style="list-style-type: none">• NLP(CTI)2STIX• AI agents for SOC functionality (detection / response), e.g.<ul style="list-style-type: none">• Triage• Alert enrichment• Domain specific LLM honeypots• LLM-Assisted Vulnerability Analysis of Medical Devices• Deep compliance	<p>Full range of improvements:</p> <ul style="list-style-type: none">• Phishing E-Mails• Vulnerability Scans• Recent AI attacks
→ adapt to healthcare environments	→ even faster detection and response

<https://informatik.th-brandenburg.de/medsec>



Health cybersecurity research history

EU Projects· Cybersecurity in Healthcare

Platforms for cyber threats in the health sector — focus, approach and lessons learned

01

AI4HealthSec

Horizon 2020

Improved detection & analysis of cyberattacks and threats on Health Care Information Infrastructures

AI-driven, self-organized swarm intelligence framework · models for risk and trend analysis

02

CyberSANE

Horizon 2020

Incident handling, warning & response system for critical information infrastructures

One of three pilots: medical devices & information systems in a healthcare context
Risk information gathered by local software agents was shared only reluctantly due to its criticality

03

SEPTON

Horizon Europe

Cybersecurity toolkit for protecting networked medical devices (NMDs) in hospitals

Use case on networked medical technology with a dedicated focus on vulnerability handling
Young project — preliminary results suggest analysis within the organizations' own IT (cf. CyberSANE)

04

SECANT

Horizon 2020

Collaborative threat intelligence collection, analysis & sharing — validated in healthcare pilots

Threat Intelligence Module (TIM): groundwork on relevant formats & sources for CTI
But: strong focus on internal sources · no mapping to treatment processes · no recommended measures

All projects funded by the European Union under Horizon 2020 / Horizon Europe

Cyber Threat Intelligence for Hospitals ^a

A Systematic Literature Review

Benedikt Michaelis^{b,1,2}, Carina Schwabe^{c,1,2}, Stefan Stein^{d,1}, Michael Pilgermann^{c,1}

¹Department of Computer Science and Media, Brandenburg University of Applied Sciences, Magdeburger Straße 50, 14770 Brandenburg an der Havel, Germany

²Department of Mathematics and Computer Science, Freie Universität Berlin, Arnimallee 14, 14195 Berlin

Abstract Hospitals provide indispensable services to individuals and society. The urgent need for continuous service and the high value connected with the associated data make them attractive targets for cyberattacks. Consequently, lives depend on sufficient cybersecurity measures. Cyber Threat Intelligence allows hospitals to implement proactive strategies and measures, and is therefore recommended in research on cybersecurity for hospitals. This article examines research findings in the field of Cyber Threat Intelligence specifically for hospitals and correlates the findings with generic findings regarding issues and proposed solutions. Despite the criticality of hospital operations and a currently insufficient preparation against cyberattacks, research specifically on Cyber Threat Intelligence for hospitals is limited. The review identified seven publications. The research examined is characterized by investigations on the collection and processing of intelligence as well as suitable sharing. The problems described in generic research are also present here. This includes the persisting discussions on CTI and key terminology as well as a missing organizational perspective. Consequently, the article proposes a short definition of key terminology related to CTI and proposes the leading factors for research specifically for hospitals. This includes that presented solutions must match an acceptance level under practitioners and match requirements of data protection and cyber security. In addition, medical devices as a common source of intelligence have to be thoroughly researched, as well as the implementation

^aThis work was funded by Brandenburg University of Applied Sciences.

^be-mail: benedikt.michaelis@th-brandenburg.de

^ce-mail: carina.schwabe@th-brandenburg.de

^de-mail: stefan.stein@th-brandenburg.de

^ee-mail: michael.pilgermann@th-brandenburg.de

of sharing networks that incorporate adjacent organizations like emergency services and medical offices.

1 Introduction

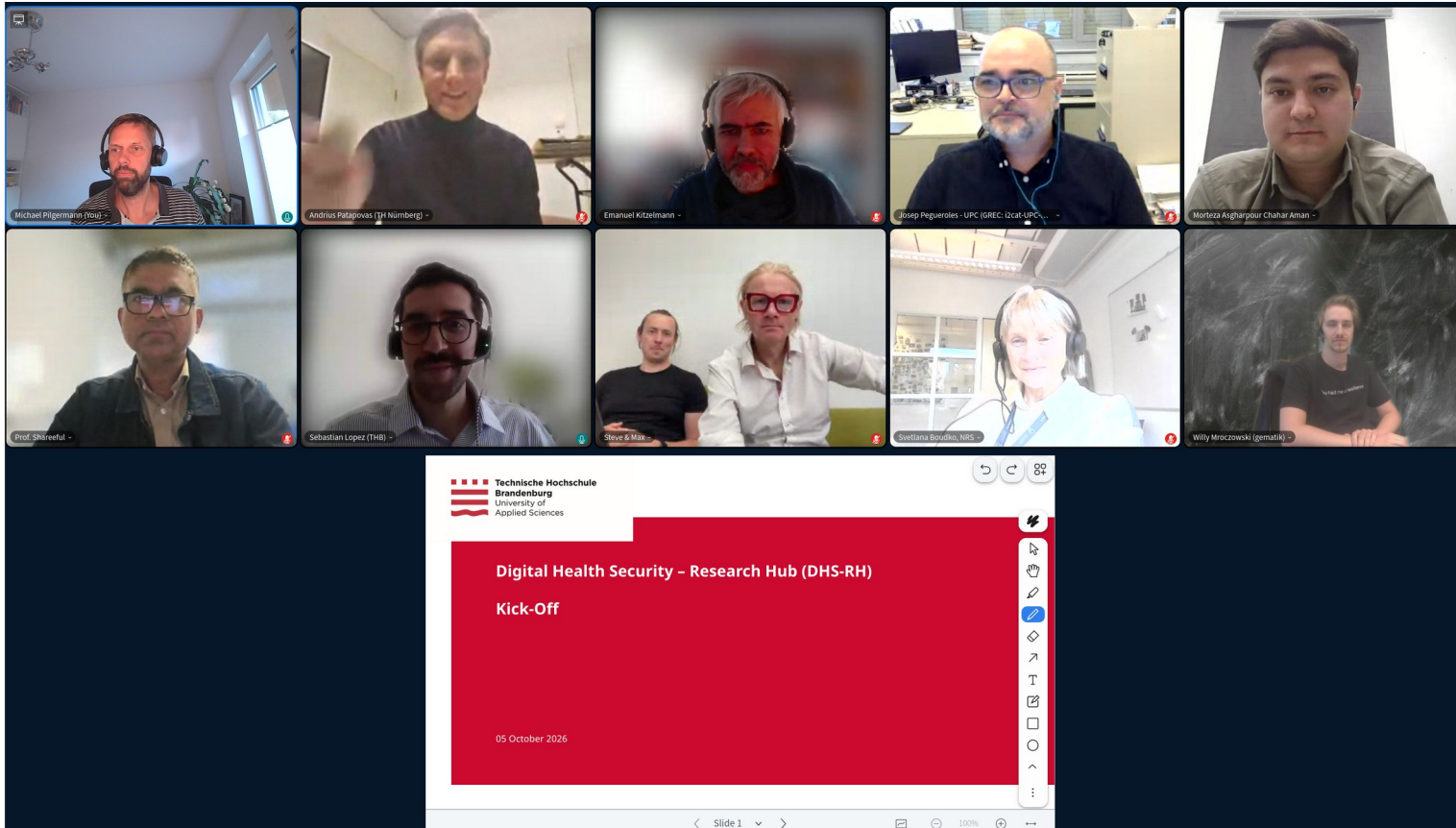
Advances in medicine are a factor that contributes, among others, to a doubled life expectancy in Germany since the 19th century [1]. Improvements in medical care have been accompanied by technological advances in medicine. From monitoring vital signs to electronic implants and robots that assist in surgery, the daily routines of patients and medical professionals are versatily characterized by technical devices [2]. The essential services that hospitals provide for both individuals and society demand the mandatory requirement to protect them from attacks. The attacks themselves may cause malfunctions or failures that can cost lives and cause financial damage. In addition, the ruling of hospitals as critical infrastructure in different states, such as Germany [3] and the United States of America [4] honors the importance of hospitals. It is inherently clear that medical systems must function flawlessly. Every single case of patient outcomes that are negatively influenced by failing technical systems is one case too many. The observed lack of protection against cyberthreats in hospitals [5] urges the need to strengthen the protection strategies used.

Therefore, efforts to protect hospitals from cyberattacks are vital in an emerging area of attacks against hospitals. According to the European Network and Information Security Agency (ENISA), healthcare is the third largest sector targeted by ransomware attacks in the European Union (EU) [6]. This totals to 309 reported incidents affecting cybersecurity in the health sector in the EU in 2023 [7] and 389 successful ran-

<https://doi.org/10.21203/rs.3.rs-10457606/v1>



DHS-RH: Kick off Monday this week



5th Oct. 2026 – 19 experts from

- Germany
- Spain
- Greece
- Norway
- UK

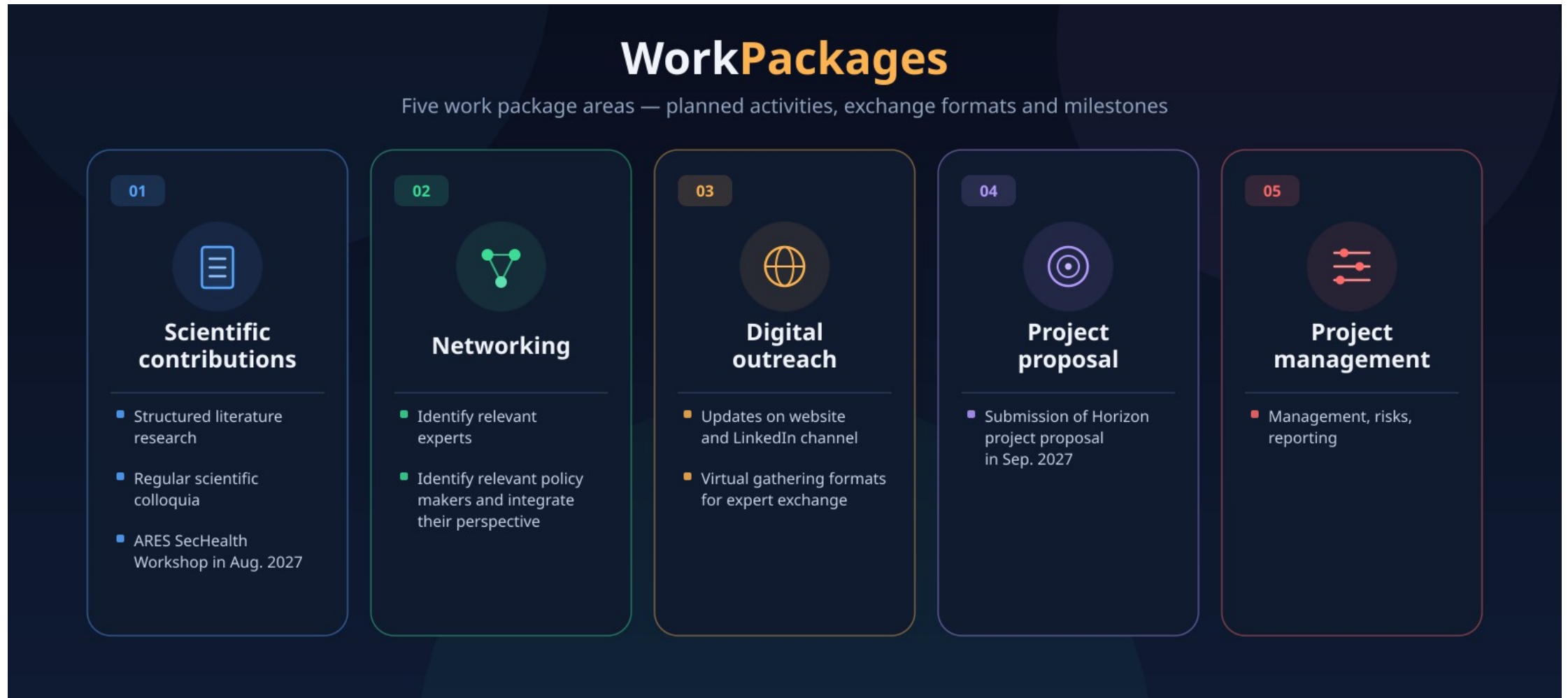


DHS-RH : Background

- Topic: **AI** for **Applied Cybersecurity** (Security Monitoring and Response) in **Healthcare**
- German federal government provides funding in order to establish the network of experts
- Duration: 12 months (Sep. 26 – Sep. 27)
- Objective:
 - Network of (academic) experts
 - Horizont submission in Sep. 2027
- Develop perspective to continue network after initial funding



DHS-RH: work packages





Overview: Horizont call

EU Horizon Call: Artificial Intelligence for Cybersecurity applications

- Budget: 24.8 Mio EUR (**5-6 projects; each 4-5 Mio EUR**; lump sum)

Important dates

- Opening of the Call: 2 March 2027
- Deadline: 15 September 2027

Expected Outcome

- AI-driven solutions for **real-time cyber threat detection**;
- Advanced **adaptive** AI systems that **evolve with dynamic cybersecurity challenges**;
- Contribute to drastically **reduce reaction time** for the recovery of systems

Concrete Requirements

For a Horizon Europe proposal on AI-driven cybersecurity

01

Real-Time Threat Detection

- Novel ML techniques to detect anomalies, malicious activity and AI-powered threats
- Improves situational awareness & response times

02

Adaptive AI Systems

- AI that continuously learns from new cyber threats and emerging attack patterns
- Maintains robustness and explainability

03

Enhanced SOC's & Cyber Hubs

- AI-enhanced SOC frameworks with predictive analytics, automation & threat intelligence
- Strengthens proactive defence measures

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2027-02-cs-eccc-01>



Get in touch

Web site	LindedIn Group
https://dhs-rh.eu	https://www.linkedin.com/groups/40609158/
	

Vielen Dank für Ihre Aufmerksamkeit

**“Sicher ist, dass nichts sicher ist.
Selbst das nicht.”**
(Joachim Ringelnatz)

<mailto:dhs-rh@th-brandenburg.de>