

KTH ROYAL INSTITUTE OF TECHNOLOGY · CYBERCAMPUS SWEDEN

# Annual Report 2025

**Dr. Emre Süren**

Researcher · Head, Royal Hacking Lab

*Proposal writing, consortium building, and collaboration — turning pitches into funded partnerships.*



GENERATED FROM [beyefendi.github.io](https://beyefendi.github.io) ACTIVITY LOG



## Dr. Emre Süren

RESEARCHER · HEAD, ROYAL HACKING LAB

Offensive security researcher specializing in LLM-driven vulnerability research and Cyber Threat Intelligence. Leads the Royal Hacking Lab at Cybercampus Sweden, supervises a growing group of PhD and master's students at KTH, and is a frequent advisor to Swedish government, defence, and industry stakeholders on AI-enabled cyber operations.

[kth.se/profile/emsuren](https://kth.se/profile/emsuren)

[scholar.google](https://scholar.google.com/citations?user=emsuren)

[github/beyefendi](https://github.com/beyefendi)

[linkedin/in/emresuren](https://linkedin/in/emresuren)

[youtube/@emresuren35](https://youtube/@emresuren35)

## The Year in Brief

FROM PITCHING TO FUNDED

2025 was the year the lab moved from pitching to funded: Dr. Süren secured his first four research grants as PI — headlined by CORTEX, a 2,000,000 SEK Digital Futures Research Pairs award for LLM-driven cyber threat intelligence, alongside Sweden's Cyber Threat Intelligence and two demonstration grants for vulnerability discovery and threat intelligence. Much of the year's effort went into writing proposals and pitching for consortium membership, reflected in the 30 talks: an EU Horizon Cluster 3 brokerage pitch in Brussels, an EU funding matchmaking pitch held online, a European Central Bank workshop in Frankfurt, expert-witness testimony in a Stockholm banking-fraud trial, and a steady stream of KTH Executive School and visiting-delegation sessions at the Royal Hacking Lab. One conference paper (FreeCAT) was published; PhD student Anton Israelsson continued into his second year, three master's theses concluded, and eleven more remained in progress. The Digital Forensics and Incident Response course (EP2780) ran its final year, capping a 2022–2025 run that involved a substantial hands-on creation from scratch. Service expanded with a Digital Futures faculty appointment, a new MSB advisory role, and continued ENISA, NordSec, and DFIRR committee duties.



*"Security has to move at the speed of the agents it protects."*

EMRE SÜREN

01 By the Numbers

COMPUTED FROM THE  
RECORD

30

Talks given

4

Grants secured · PI

15

Students supervised

1

Publication

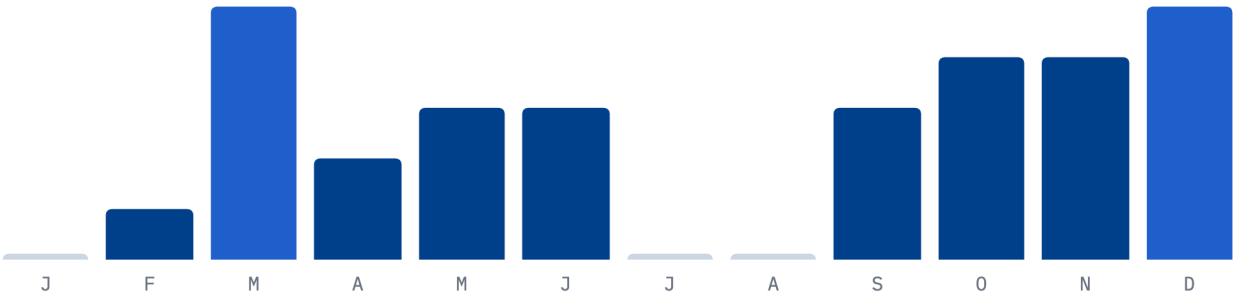
3

Countries visited

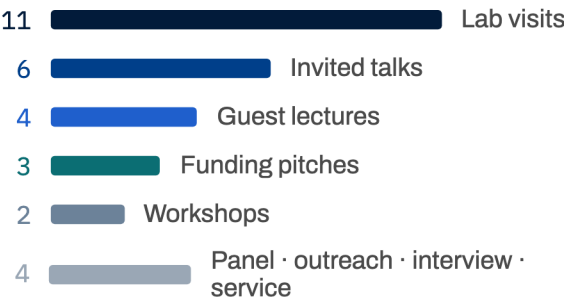
6

Proposals not funded

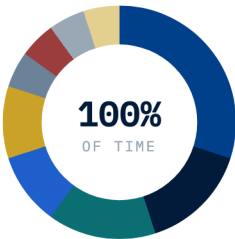
TALKS PER MONTH



ENGAGEMENTS BY TYPE



Thirty talks this year, but a fair share were funding pitches rather than research talks — eleven were visitors hosted at the lab, only three were pitches abroad. The balance needs to shift back toward research.



WHERE THE YEAR WENT

- Grant application
- Events
- Teaching
- Reviews
- Lab

- Supervision
- Collaborations
- Research
- Conferences

## 02 Talks & Invited Presentations

30 ENGAGEMENTS ·  
SELECTED HIGHLIGHTS



2025-12-08 · WORKSHOP

### Practical Adversarial GenAI for Red Teamers

European Central Bank · Frankfurt

Hands-on workshop on prompt injection, jailbreaking, and autonomous penetration-testing agents for ECB staff.

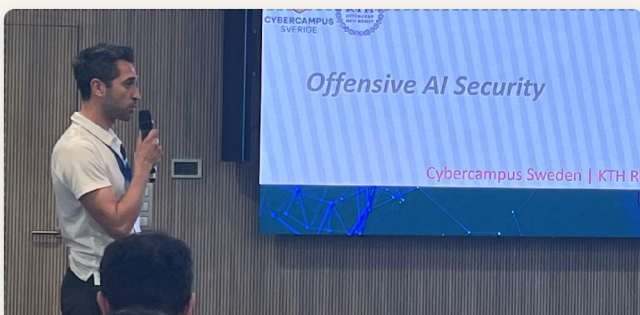


2025-12-12 · PUBLIC SERVICE

### Digital Forensics Expertise Testimony

Criminal Court (Tingsrätt) · Stockholm

Expert witness in a high-profile banking-fraud case, presenting forensic analysis findings to the court.



2025-06-12 · PITCH

### Proposal: Offensive AI Security

EU Horizon Cluster 3 Brokerage · Brussels

Pitched a consortium proposal on generative AI for vulnerability research to ~200 participants among 25 ideas.



2025-12-02 · INVITED TALK

### AI in Offensive Security: LLM-Driven Research

State of Cybersecurity 2025 · Stockholm

A practical framework for building LLM agents for penetration testing, with a live multi-step exploitation demo.



## 02 Full List

| DATE       | TITLE                                                 | VENUE · TYPE                                                           |
|------------|-------------------------------------------------------|------------------------------------------------------------------------|
| 2025-12-18 | LLMs in Offensive Security                            | Cicor Group · KTH Nymble · <a href="#">workshop</a>                    |
| 2025-12-12 | Digital Forensics Expertise Testimony                 | Criminal Court · Stockholm · <a href="#">public service</a>            |
| 2025-12-08 | Practical Adversarial GenAI for Red Teamers           | European Central Bank · Frankfurt · <a href="#">workshop</a>           |
| 2025-12-04 | Research Vision on Offensive AI Security              | Forum for Adjunct Professors · <a href="#">invited talk</a>            |
| 2025-12-02 | AI in Offensive Security                              | State of Cybersecurity 2025 · Stockholm · <a href="#">invited talk</a> |
| 2025-11-20 | Dr. Sören's Research Vision                           | MSB · <a href="#">visit</a>                                            |
| 2025-11-20 | Crime Prevention in Hyperspaces                       | Safeplaces Network & Digital Futures · <a href="#">panel</a>           |
| 2025-11-04 | Most Impactful Discoveries in the Lab                 | Three Letter Agency · <a href="#">visit</a>                            |
| 2025-11-03 | Interview with Dr. Emre Sören                         | Framtidens Karriär · <a href="#">interview</a>                         |
| 2025-10-22 | When Language Models Go Offensive                     | Tech Talks Unplugged · Detectify · <a href="#">invited talk</a>        |
| 2025-10-09 | Dr. Sören's Research Journey                          | KTH Executive Program · <a href="#">guest lecture</a>                  |
| 2025-10-08 | Contribution to the National Security                 | KTH Board · <a href="#">visit</a>                                      |
| 2025-10-06 | Dr. Sören's Research Vision                           | KTH Innovation · <a href="#">visit</a>                                 |
| 2025-09-26 | Dr. Sören's Research Vision                           | American Congressmen Delegation · <a href="#">visit</a>                |
| 2025-09-24 | Dr. Sören's Research Vision                           | MSAB · <a href="#">visit</a>                                           |
| 2025-09-19 | Dr. Sören's Research Vision                           | Ministry of Education · <a href="#">visit</a>                          |
| 2025-06-27 | Proposal: AGI for Offensive Security                  | EU Cybersecurity Funding · online · <a href="#">pitch</a>              |
| 2025-06-12 | Proposal: Offensive AI Security                       | EU Horizon Cluster 3 · Brussels · <a href="#">pitch</a>                |
| 2025-06-03 | Dr. Sören's Research Vision                           | SWITS'25 Seminar · <a href="#">invited talk</a>                        |
| 2025-05-16 | Dr. Sören's Research Vision                           | Nanyang Technological Univ. · <a href="#">visit</a>                    |
| 2025-05-14 | Proposal: Offensive AI Security for National Security | CS4S Matchmaking · <a href="#">pitch</a>                               |
| 2025-05-08 | Dr. Sören's Research Vision                           | Nackademin & IT-Högskolan · <a href="#">visit</a>                      |
| 2025-04-29 | AI vs. AI: Battlefield of Offensive Security          | Diplomatprogrammet · <a href="#">guest lecture</a>                     |
| 2025-04-10 | Offensive Security in the AI Threat Landscape         | Cybersäkerhet Nätverk · Altinget · <a href="#">guest lecture</a>       |
| 2025-03-27 | Dr. Sören's Research Vision                           | KTH Fusion Career Fair · <a href="#">outreach</a>                      |
| 2025-03-20 | Offensive Security in the AI Revolution               | OWASP Meetup · Detectify · <a href="#">invited talk</a>                |
| 2025-03-20 | Offensive AI in Cybersecurity: A Research Outlook     | KTH Executive School · <a href="#">guest lecture</a>                   |
| 2025-03-03 | When AI Hunts AI                                      | Stellar Capacity Masterclass · <a href="#">invited talk</a>            |
| 2025-03-03 | Fundraising for AI Research                           | Swedish Philanthropist · KTH Rektorshuset · <a href="#">visit</a>      |
| 2025-02-20 | Smartwatch Hacking                                    | Univ. of Strathclyde Visit · <a href="#">visit</a>                     |

CONFERENCE · MAR 2025

## FreeCAT — A Framework for Resilience and Evolution by Code Analysis Tools

S. Hacks, C. Artho, R. Guanciale, R. Künnemann, D. Malakhova, E. Süren

*International Conference on Evaluation and Modeling Methods for Systems Analysis and Development*

NOT ACCEPTED · NORDSEC

## SvenDroid: A Dynamic Instrumentation Study Locating Swedish Mobile App Vulnerabilities

This year I spent a lot of time on proposal writing and attending events, and it left too little time for publications. NordSec — whose program committee I happen to sit on — rejected one of our submissions, “SvenDroid.” Reviewing for a venue and getting rejected by it in the same year is a special kind of humbling — more so when a paper on the very same topic made it in.

OPEN SOURCE

FLAGSHIP

[github.com/ReverseSecLabs/spikee](https://github.com/ReverseSecLabs/spikee)

TogetherAI support

### spikee

A toolkit for testing LLM apps and guardrails against prompt-injection and jailbreak attacks.

[github.com/beyefendi/prompt-injection-playground](https://github.com/beyefendi/prompt-injection-playground)

### prompt-injection-playground

Systematically testing open-source prompt-injection kits against LLMs, guardrails, and LLM-powered applications.

More on [github.com/beyefendi](https://github.com/beyefendi)

PI Digital Futures Research Pairs · KTH-RPROJ-0146472

2026–2027 (Awarded 2025)

**CORTEX — An LLM-Driven Framework for Enhanced CTI through AI**  
2,000,000 SEK (~0.18M €)

PI NAISS 2025/6-50

2025

**Sweden's Cyber Threat Intelligence**  
1,500 GiB storage (in-kind)

PI NAISS 2024/5-651

2025

**Discovering Software Vulnerabilities with LLMs**  
500 GPU-h / month (in-kind)

PI Digital Futures SRI · KTH-RPROJ-0146472

2025

**Swedish Cyber Threat Intelligence Demo**  
120,000 SEK (~10,982 €)

For every grant I won this year, I lost more than one — four funded, six rejected. Proposal writing was the real engine room of 2025, even if the win rate doesn't show it.

## 05 Supervision

1 PhD · 14 MSc · 3 DONE  
/ 12 ONGOING

| STUDENT             | THESIS                                                                                | LEVEL | STATUS           |
|---------------------|---------------------------------------------------------------------------------------|-------|------------------|
| Anton Israelsson    | Privacy-preserving ML services through hybrid homomorphic encryption · RISE & Uppsala | PhD   | ongoing · 2nd yr |
| Rahila Kundan       | Penetration Testing & Vulnerability Analysis of Swedish apps · KTH                    | MSc   | completed 2025   |
| Yamini Balannagari  | Static/Dynamic Analysis & Reverse Engineering for Mobile App Vulnerabilities · KTH    | MSc   | completed 2025   |
| Peter Daniel        | Triggering false alarms in computer networks · KTH                                    | MSc   | completed 2025   |
| Hassan El Ghamri    | Exploiting vulnerabilities in the Raspberry Pi compute module · KTH                   | MSc   | ongoing          |
| Roy Dolonius        | Penetration testing methodologies for embedded systems · KTH                          | MSc   | ongoing          |
| Ísak Arnar Kolbeins | Penetration testing security weaknesses in embedded devices · KTH                     | MSc   | ongoing          |
| Hávar Sigurðarson   | De-obfuscating & clustering malicious JavaScript on Swedish webpages · Stockholm U.   | MSc   | ongoing          |
| Siwei Zhang         | Fine-tuning DeepSeek LLM for vulnerability research · Stockholm U.                    | MSc   | ongoing          |
| Yanxiang Du         | Fine-tuning LLaMA LLM for vulnerability research · Stockholm U.                       | MSc   | ongoing          |
| Marco Campione      | Fuzzing Matter(s): stateful black-box fuzzer for Matter devices · KTH                 | MSc   | ongoing          |
| Anton Rådberg       | Investigating fileless malware in Windows operating systems · KTH                     | MSc   | ongoing          |
| Edward Norberg      | Memory Analytics Measures for Windows 11 Forensics · KTH                              | MSc   | ongoing          |
| Gabriel Gerdin      | LLMs for Software Vulnerability Discovery & Exploitation · Karlstad U.                | MSc   | ongoing          |
| Roni Henareh        | Fine-Tuning Small Open-Weight LLMs for Cybersecurity · KTH                            | MSc   | ongoing          |

Eleven ongoing master's students by year's end is a sign of a fast-growing group — and exactly why I'm tightening how I screen new students going forward, rather than accepting everyone who's interested.



GRADUATE COURSE EP2780

2022–2025

## Digital Forensics and Incident Response

Created from scratch around more than 100 hands-on lab exercises in a Capture-the-Flag format — its final year after a 2022–2025 run. The build took substantial overtime and a pause on research to prioritize the student experience.

The student feedback didn't fully reflect that investment, which informed my decision not to continue teaching the course beyond 2025.

## 07 Professional Service

8 ROLES

|          |                                                                                                  |              |
|----------|--------------------------------------------------------------------------------------------------|--------------|
| ADMIN    | <b>Digital Futures</b><br>Faculty                                                                | 2025–current |
| ADMIN    | <b>Stockholm District Court</b><br>Digital forensics expert witness, banking-fraud investigation | 2025         |
| ADMIN    | <b>EU Commission — MSB</b><br>Advisor on cyber risks of connected & automated vehicles           | 2025         |
| ADMIN    | <b>ENISA</b><br>CEI Listed expert                                                                | 2023–current |
| TPC      | <b>NordSec — Nordic Conf. on Secure IT Systems</b><br>Program-committee member                   | 2024–current |
| TPC      | <b>DFIR Review (DFIRR)</b><br>Program-committee member                                           | 2023–current |
| REVIEWER | <b>World Wide Web journal</b><br>Reviewer                                                        | 2025         |
| REVIEWER | <b>Journal of Computer Virology &amp; Hacking Techniques</b><br>Reviewer                         | 2025         |

2025 was the year I started showing up on the institutional side as much as the research side — a Digital Futures faculty seat, an MSB advisory role on connected-vehicle cyber risk, ENISA's expert roster, and NordSec's program committee.

## 08 Rejected Proposals

6 NOT FUNDED

PI EU Horizon · HORIZON-CL3-2025-02-CS-ECCC-01

14M € total

### GENSHIELD — Generative-AI Self-Healing Cybersecurity & Compliance for IIoT

Scored 12.5/15 (Excellence 4.5, Impact 3.5, Implementation 4.5) but not selected for funding.

PI Swedish Research Council (VR)

5,768,000 SEK (~0.53M €)

### VORTEX — Vulnerability-Oriented Retrieval and Tuning for Exploitation

Reviewers concluded the applicant's profile was not a sufficient match for the proposed work.

PI KTH Int'l Partner University · Joint Doctoral Funding

4.4M SEK

### Artificial Honeypot Architectures for Critical-Infrastructure Threat Intelligence in Scandinavia

The partner university's co-applicant did not submit required documents in time, leaving the joint application incomplete.

WP leader EU Horizon · HORIZON-CL3-2024-CS-01-01

5.5M € total / 0.8M € own

### FreeCAT — Framework for Resilience and Evolution by Code Analysis Tools

Innovation aspects of the project were not registered enough to be considered for funding.

WP leader Digital Europe · DIGITAL-ECCC-2024-DEPLOY-CYBER-07

2.8M € total / €122,435 own

### EU VISTAR — European Repository for Research on Vigilance, Situational Awareness and Threats

Not selected for funding; reviewers did not find the proposal sufficiently interesting.

PI Cybercampus Sweden · Direct application

### AI-Secure — Advancing Sweden's Cybersecurity through AI-Driven Vulnerability Research

Submitted directly to Cybercampus Sweden by email — the open call's eligibility rules ruled out a formal application — and was not considered for funding.

*2026 is mostly about saying no more often —  
fewer research topics, fewer talk invitations, more finished papers.*

## WHAT 2025 TAUGHT ME

Accepted nearly every collaboration and funding offer in the rush to build the research group and recruit PhD students, which consumed significant time that could have gone toward research itself.

Spread effort across too many research topics at once — including a significant investment in digital forensics (the memotopsy project) and broad IoT hacking work — which slowed progress on higher-priority research.

## THE PLAN FOR 2026

- 01 Kick off CORTEX — the LLM-driven CTI framework — as a primary research focus for 2026–2027.
- 02 Seek funding for research on adversarial attacks against MCP servers using Guardian Agents.
- 03 Extend the existing NAISS grant to continue LLM-driven vulnerability-discovery research.
- 04 Submit the long-awaited Swedish CTI paper (SwedTI).
- 05 Submit 10 papers in 2026, targeting at least 5 acceptances.
- 06 Keep IoT-hacking research at a maintenance-only level, not a primary line.
- 07 Submit the memotopsy paper as the closing chapter of digital-forensics research.
- 08 Conclude teaching DFIR (EP2780) after 2025.
- 09 Turn current research output into new courses: AI Agents for Pentesting, Prompt Injection & Jailbreaking.
- 10 Launch a YouTube channel to share research and educational content.
- 11 Decline talk invitations that don't justify the time investment.
- 12 Recruit five new master's students for LLM-driven honeypots and guardian-agent evasion.
- 13 Apply stricter screening of new students and collaborations — fit over urgency.

## 10 2025 in Photos

NINE HIGHLIGHTS

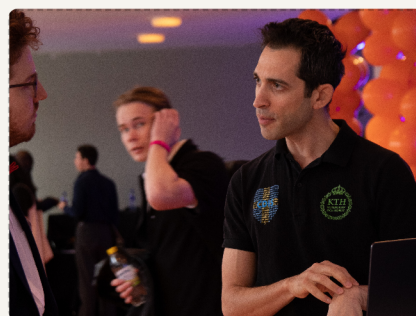
Beyond the headline engagements — the meetups, guest lectures, lab visits, and matchmaking events that filled out the year at the Royal Hacking Lab and around Stockholm.



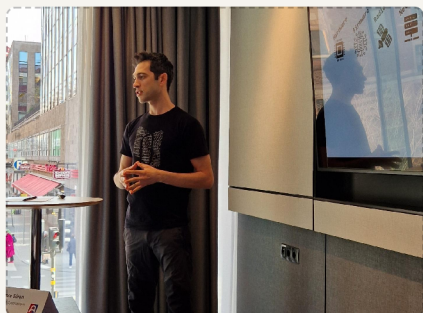
KTH EXECUTIVE SCHOOL • MAR



OWASP MEETUP • MAR



KTH FUSION CAREER FAIR • MAR



CYBERSÄKERHET NÄTVERK • APR



DIPLOMAT PROGRAM • APR



CS4S MATCHMAKING • MAY



NTU SINGAPORE VISIT • MAY



TECH TALKS UNPLUGGED • OCT



MSB • SWEDISH CIVIL CONTINGENCIES • NOV