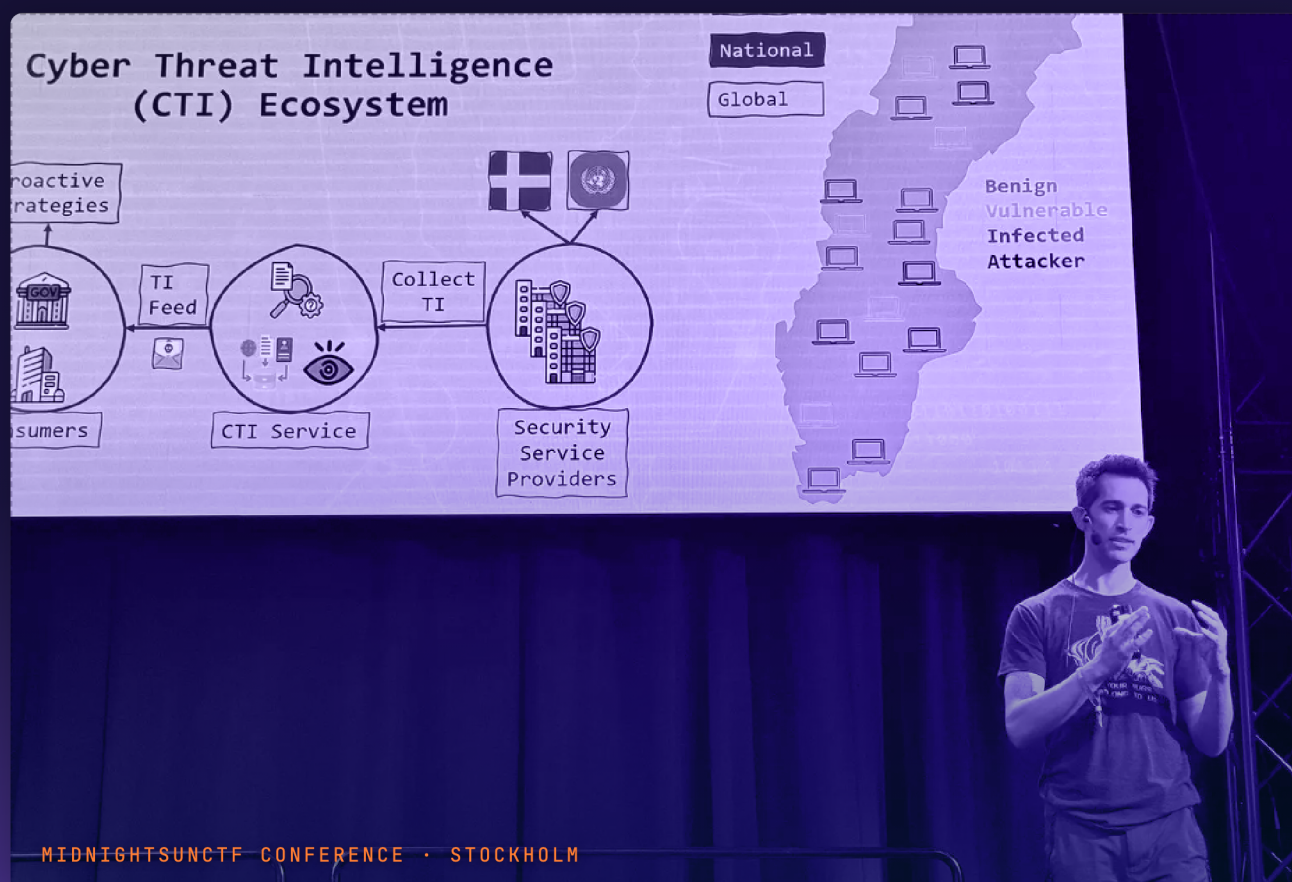


Annual Report 2024

Dr. Emre Süren

Researcher · Head, Royal Hacking Lab

Laying the groundwork — twelve talks, one country, and a lab introducing itself to Sweden.



MIDNIGHTSUNCTF CONFERENCE · STOCKHOLM



Dr. Emre Süren

RESEARCHER • HEAD, ROYAL HACKING LAB

Offensive security researcher specializing in LLM-driven vulnerability research, IoT Hacking, and Cyber Threat Intelligence. Heads the Royal Hacking Lab, supervises a growing group of master's students and teaches Digital Forensics at KTH. Focuses on research projects contributing to national security as well as the open source community, and volunteers as a researcher helping Swedish society become aware of the power of LLMs in cybersecurity.

kth.se/profile/emsuren

scholar.google

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

linkedin/in/emresuren

youtube/@emresuren35

The Year in Brief

LAYING THE GROUNDWORK

2024 was the year the Royal Hacking Lab found its voice in Sweden. Dr. Süren delivered twelve talks across the country — three media interviews, four lab demonstrations for visiting delegations, three invited talks at conferences and stakeholder events, a pitch, and a guest lecture — covering topics from medical IoT vulnerability research to LLMs in offensive security and national threat intelligence. One collaboration yielded a conference paper (ACM e-Energy 2025). No grants were secured in 2024; one proposal was submitted and rejected by VR (IoT VR, 1,395,000 SEK). Supervision was active: one completed master's thesis on memory corruption in IoT, and two bachelor theses were wrapped up. Three master's students extended into 2025. The Digital Forensics and Incident Response course (EP2780) ran for its third year. Service roles included a new seat on the NordSec program committee alongside continued ENISA membership and DFIRR program committee duty.



"You have to introduce yourself before anyone will let you in the room. In 2024, I introduced the lab and my research to all of Sweden."

EMRE SÜREN

01 By the Numbers

COMPUTED FROM THE RECORD

12

Talks given

0

Grants secured

8

Students supervised

1

Publication

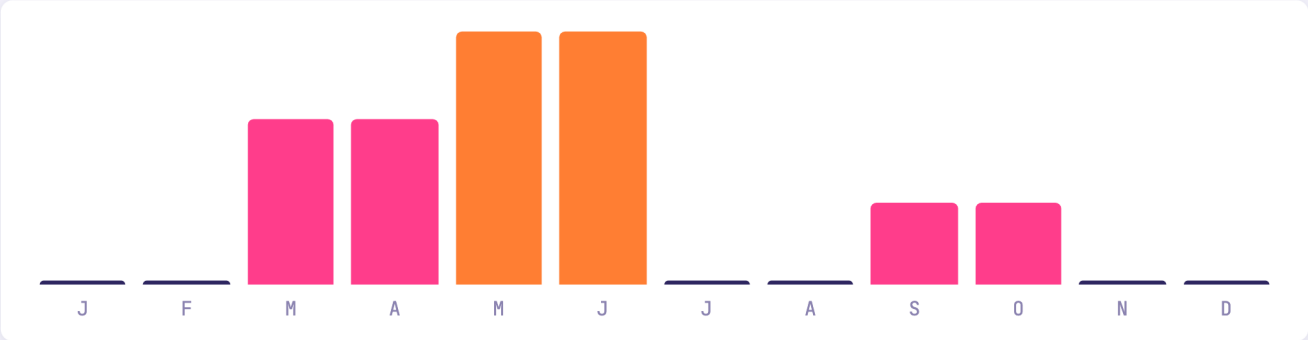
1

Country visited

1

Proposal not funded

TALKS PER MONTH

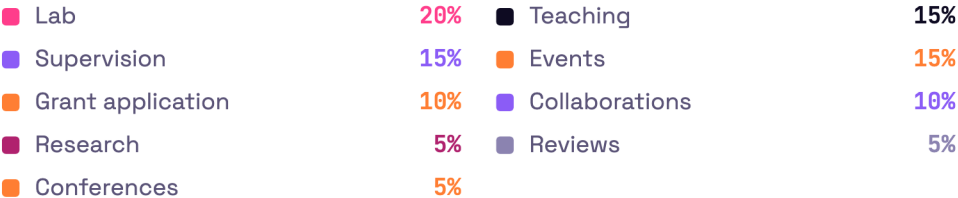
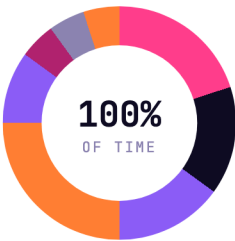


ENGAGEMENTS BY TYPE



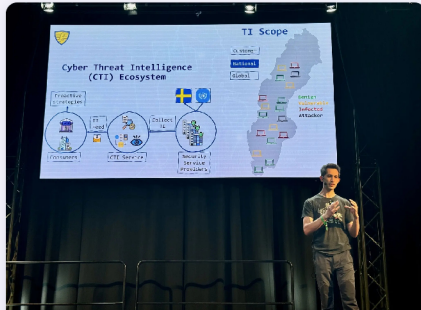
Twelve talks and every single one in Sweden. 2024 was about making the Royal Hacking Lab known at home first — I'd rather build a solid local reputation before trying to go anywhere else.

WHERE THE YEAR WENT



02 Talks & Invited Presentations

12 ENGAGEMENTS



2024-06-14 • INVITED TALK

Sweden's Threat Intelligence

MidNightSunCTF Conference · Stockholm



2024-04-25 • VISIT

Chat-GPT for Vulnerability Exploitation Demonstrated

Dakota State University · Royal Hacking Lab



2024-09-27 • VISIT

Smartwatch Hacking Demonstrated

KTH Rektor & Investment Committee

DATE	TITLE	VENUE	TYPE
2024-10-08	Vulnerability Research in the AI Era	Women4Cyber	invited talk
2024-09-27	Smartwatch Hacking Demonstrated	KTH Rektor and Investment Committee	visit
2024-06-14	Sweden's Threat Intelligence	MidNightSunCTF Conference · Stockholm	invited talk
2024-06-05	Large Language Models (LLMs) in Security Research	KTH Executive School Visit	visit
2024-06-01	Sweden's Threat Intelligence	Swedish Stakeholders Briefing · KTH ReaktorHallen	invited talk
2024-05-27	Hacking Lab Infrastructure and Collaboration Opportunities	SWITS'24 Seminar · Lund University	invited talk
2024-05-17	Large Language Models (LLMs) in Security Research	KTH Executive School Guest Lecture	guest lecture
2024-05-06	Offensive Security for Medical IoT Devices	HTM Matchmaking 2024 · SciLifeLab	pitch
2024-04-25	Chat-GPT for Vulnerability Exploitation Demonstrated	Dakota State University Visit	visit
2024-04-19	Beviset: Forum med militära hemligheter utsattes för intrång	SVT Radio	interview
2024-03-25	Hacking Lab Showcased for a Government Entity	A Three Letter Agency	visit
2024-03-22	Målet: Nya Cybercampus Sverige ska Stärka Hela Landets IT-säkerhet	NyTeknik	interview

Three interviews, four lab demonstrations, three invited talks, a pitch, and a guest lecture. Different formats, different rooms, different audiences — but the same year and the same country every time.

CONFERENCE • DEC 2024

Procedural Generation of Communication Networks in Power Systems

J. Weiss, L. Nordström, P. Hilber, E. Sören

16th ACM International Conference on Future and Sustainable Energy Systems (ACM e-Energy 2025)

One paper published, and it's about power-system network generation — not exactly my core focus. Most of the year's intellectual energy went into establishing the lab and pitching, not writing. The papers would have to wait.

OPEN SOURCE

FLAGSHIP github.com/beyefendi/awesome-memory-forensics

awesome-memory-forensics

Curated list of memory forensics tools, resources, and research.

github.com/beyefendi/penbook/tree/main/iot

penbook/iot

IoT penetration testing methodology and lab notes. Artifacts generated during my PatIoT paper.

More on github.com/beyefendi



Grants secured in 2024

No grants secured in 2024. One proposal was submitted to VR — IoTVR, 1,395,000 SEK — and was rejected (see Rejected Proposals).

REJECTED PROPOSAL

PI Vetenskapsrådet (VR)

1,395,000 SEK

IoTVR — IoT Vulnerability Research

Applied once, rejected once. IoTVR went to VR and came back empty. It was the first proposal I submitted as PI, and the lesson was immediate: one proposal is not a pipeline. You need to be sending something in every cycle.

IoTVR was a substantive proposal grounded in a genuine research need. VR ultimately declined to fund it. The amount itself was modest — 1.4M SEK would not have funded a single PhD student, let alone a group — which makes the outcome a useful data point: even proposals introducing a novel direction, such as applying LLMs to IoT hacking, are not guaranteed funding on merit alone. That outcome sharpened the plan for 2025 considerably.

Another significant development was the lab's move from KTH to Cybercampus this year. Given the lab's track record since inception, it was a natural fit for Cybercampus to host us, and in return the talks conducted all around Sweden helped introduce Cybercampus to a public that was largely unaware of the initiative in its early days. That contribution has not yet been matched by direct investment from Cybercampus in building out a research group under my supervision. A few proposals put to the management team this year also went unanswered, without a clear decision either way. Both outcomes fell short of what the lab's track record would suggest was warranted.

STUDENT(S)	THESIS	LEVEL	STATUS
Erik Mickols	Memory corruption in IoT: Extending PatIoT to hunt memory corruption bugs · KTH	MSc	completed 2024
Edward Norberg	Design and Evaluation of Memory Analytics Measures for Windows 11 Forensics · KTH	MSc	ongoing
Roni Henareh	Fine-Tuning Small Open-Weight LLMs for Cybersecurity · KTH	MSc	ongoing
Peter Daniel	Triggering false alarms in computer networks · KTH	MSc	ongoing
Gergo Emin Tarcheh & Nina Shamaya	Smart home infrastructure for penetration testing and national cyber ranges · KTH	BSc	completed 2024
Hjalmar Höglund & Roni Henareh	Collaboration platform for penetration tests enhanced with machine learning · KTH	BSc	completed 2024

The thesis on memory corruption wrapped, and two bachelor theses crossed the finish line. A decent harvest for a lab that was still setting up its own infrastructure. The students coming in now will have a much more equipped environment than the ones who joined first.

GRADUATE COURSE EP2780

2022-2025

Digital Forensics and Incident Response

A required course for the KTH master's program in Cyber Security, covering forensic analysis and incident response for compromised systems, with weekly hands-on labs and a Capture-the-Flag format.

Third year of the digital forensics course that I've built from nothing, and the hands-on labs are genuinely good. Whether that shows up in feedback is a different story — one I was still trying to resolve when the year ended.

ADMIN

ENISA

CEI Listed expert

2023–current

TPC

NordSec

Program-committee member

2024–current

TPC

DFIRR

Program-committee member

2023–current

Joined NordSec's program committee for the first time in 2024. It felt like the right moment — the lab had enough of a profile that a TPC seat made sense, and I could finally contribute something to a unique Scandinavian venue rather than just submitting to it.

The plan for 2025 is straightforward: get funded, get PhD students, get published. Everything else — the talks, the collaborations, the pitches — feeds into those three. 2024 proved you can't build a group on visibility alone.

WHAT 2024 TAUGHT ME

Funding is the critical bottleneck for group development. Without external grants, recruiting and retaining PhD students is not possible at the pace the lab's trajectory requires. One good proposal is not enough — the pipeline has to run continuously.

Students are showing more reluctance to attend the lab in person compared to previous years, gravitating instead toward conducting their studies remotely. Worth watching as supervision plans for 2025 take shape.

Cybercampus has not yet matched the lab's track record with direct investment, and proposals put to the management team this year went unanswered. The more productive path forward is to keep converting public visibility into a concrete case for that investment, rather than waiting on a decision.

THE PLAN FOR 2025

- 01 Apply for research funding aggressively in 2025, targeting at least 10M SEK across multiple calls.
- 02 Convert this year's visibility into a direct funding conversation with Cybercampus, translating public presence into a concrete investment case.
- 03 Recruit at least two PhD students to build a stable research core.
- 04 Build active collaborations with international research labs and pitch for consortium membership in EU-funded projects.
- 05 Improve EP2780 so that student satisfaction reflects the investment made in the course's hands-on design; re-record lectures with AI support, including the voice-over.
- 06 Write and submit at least two research papers; aim for at least one acceptance.

09 2024 in Photos

NINE HIGHLIGHTS

Beyond the headline conference talk — the interviews, lab demonstrations, and stakeholder visits that made up the Royal Hacking Lab's first full year finding its footing in Sweden.



SVT RADIO INTERVIEW • APR



DAKOTA STATE UNIVERSITY VISIT • APR



WOMEN4CYBER • OCT



HTM MATCHMAKING • SCILIFELAB • MAY



SWITS'24 • LUND UNIVERSITY • MAY



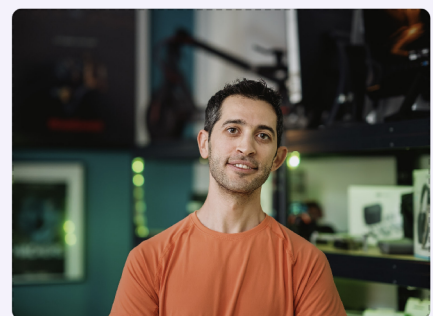
KTH EXECUTIVE SCHOOL GUEST LECTURE • MAY



KTH EXECUTIVE SCHOOL VISIT • JUN



GOVERNMENT ENTITY VISIT • MAR



NYTEKNIK INTERVIEW • MAR