Modern Advanced Cyber-Attacks in 2026 and the impact at the Threat Intel level

@ Vinterkonferansen 2026
by André Lima

Red Team Leader @ Telenor Cyberdefence

André Lima

- 15 years of experience: Portugal, Australia, Norway
- Researcher & Speaker in multiple conferences around Europe
  - Vinterkonferansen (2026)
  - Sikkerhetsfestivalen (2023,2024,2025)
  - Bsides Kristiansand (2025)
  - TIBER-EU Provider Conference (2024)
  - Bsides Oslo (2022,2023)
  - Bsides Lisbon (2022)
- Experienced in TIBER-EU/NO standard
- Malware developer and Defense/EDR Evasion specialist
- Certifications: OSED, OSCP, OSWP, eCRE, SLAE64, eWPTX

Agenda

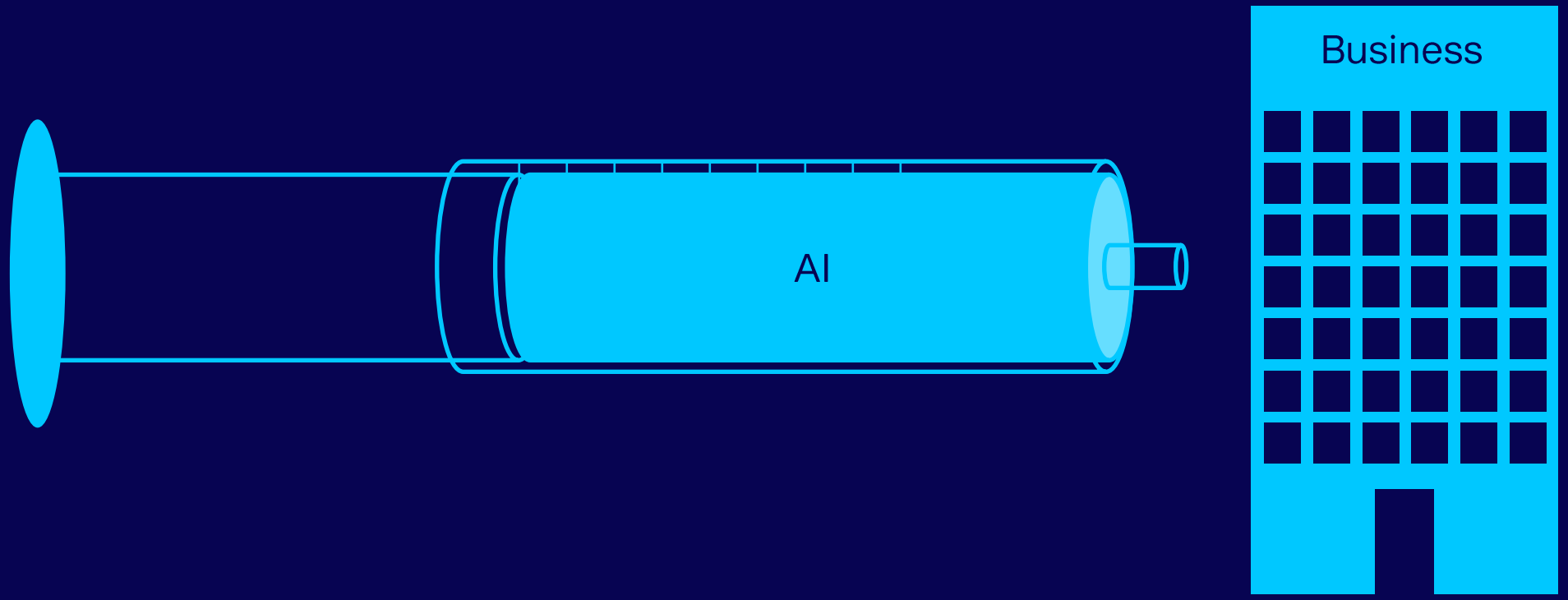
Intro / Context – What are MCP servers? How is that relevant?

A demo… to prove this is not just theoretical.

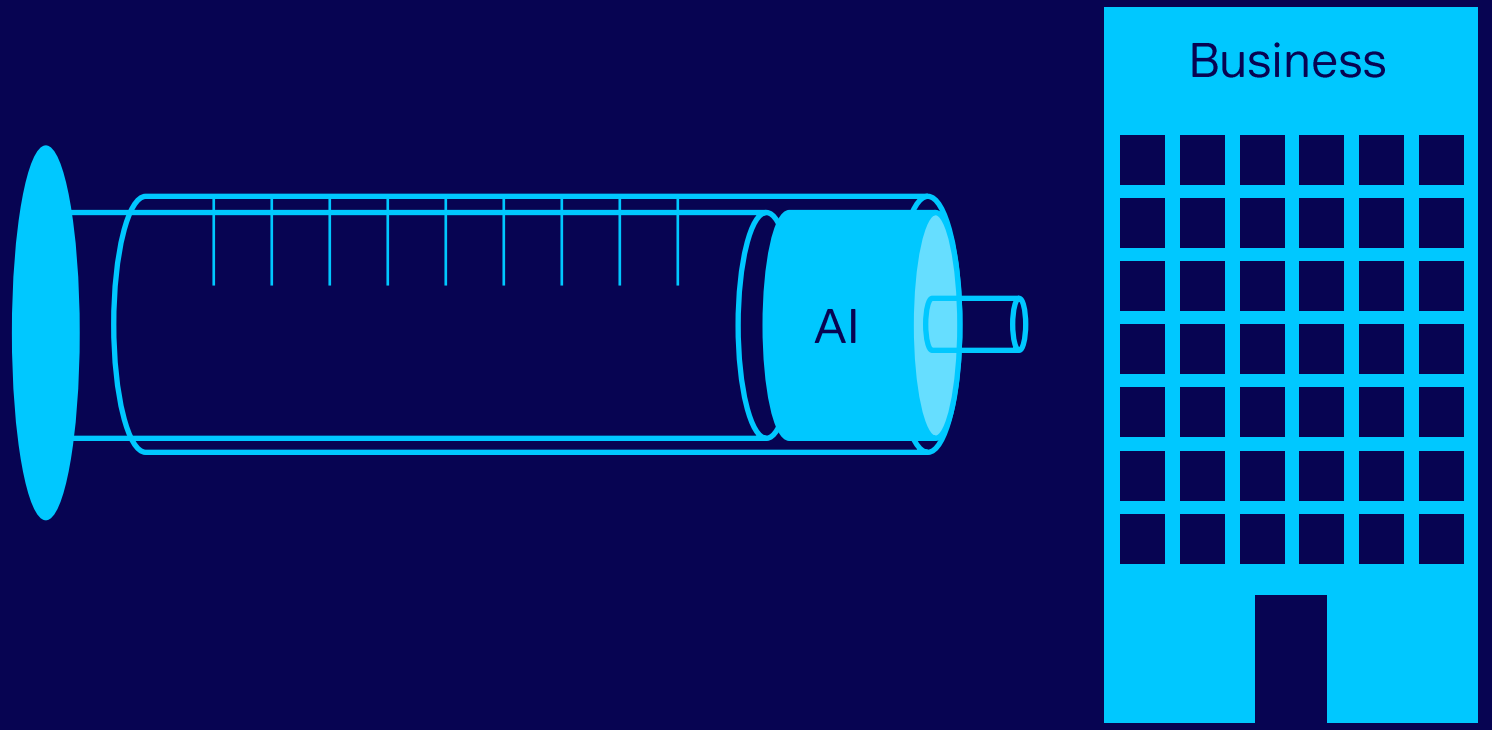
Impact for Cyber Threat Intel

Conclusions

Intro / Context



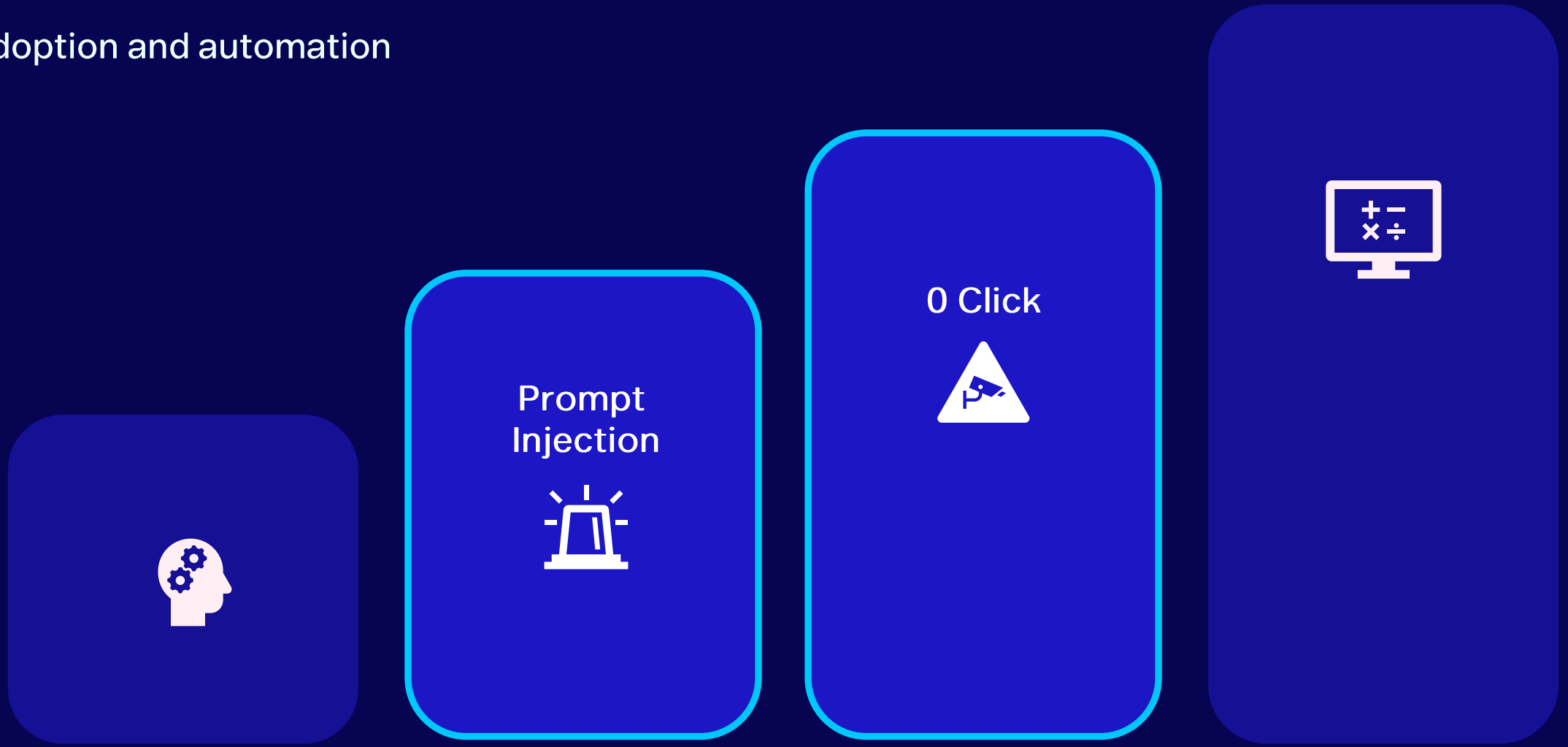
Intro / Context



Intro / Context – New attack surface / vectors

Intro / Context – New attack surface / vectors

- AI adoption and automation



Intro / Context – New attack surface / vectors

- Vibe-coding

Intro / Context – New attack surface / vectors

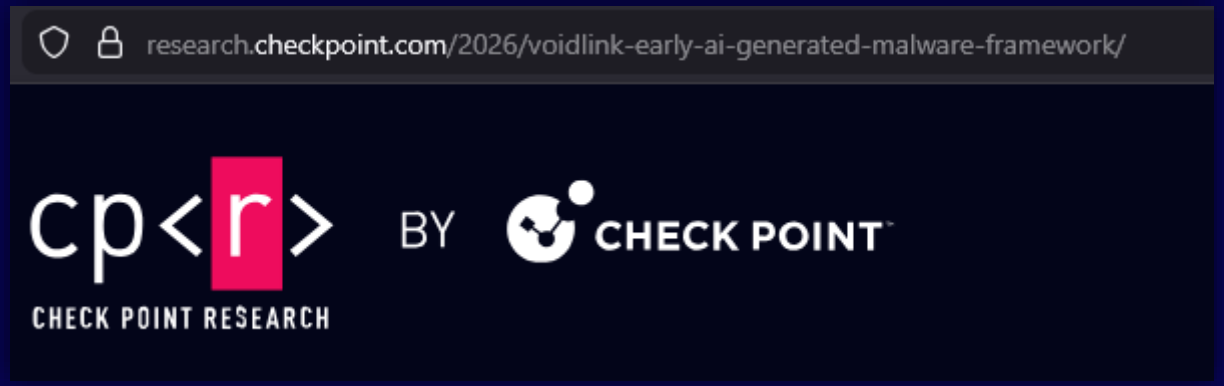
- AI deception will improve

Intro / Context – Bigger problem…

- APTs (the focus of this presentation)

Intro / Context – Bigger problem…

- APTs (the focus of this presentation)



Intro / Context – Bigger problem…

- APTs (the focus of this presentation)

research.checkpoint.com/2026/voidlink-early-ai-generated-malware-framework/

VOIDLINK: EVIDENCE THAT THE ERA OF ADVANCED AI-GENERATED MALWARE HAS BEGUN

January 20, 2026

Key Points

Check Point Research (CPR) believes a new era of AI-generated malware has begun. VoidLink stands as the first evidently documented case of this era, as a truly advanced malware framework **authored almost entirely by artificial intelligence**, likely under the direction of a single individual.

Until now, solid evidence of AI-generated malware has primarily been linked to inexperienced threat actors, as in the case of FunkSec, or to malware that largely mirrored the functionality of existing open-source malware tools. VoidLink is the first evidence based case that shows how **dangerous AI can become in the hands of more capable malware developers.**

Intro / Context – Bigger problem…

- APTs (the focus of this presentation)

Intro /

- APTs (the f

AI-Guided Malware

Home » Artificial Intelligence (AI)

Leah Siskind
Director of Impact and AI Research Fellow

Maria Riofrio
Research Assistant

Mariam Lomtadze
Intern

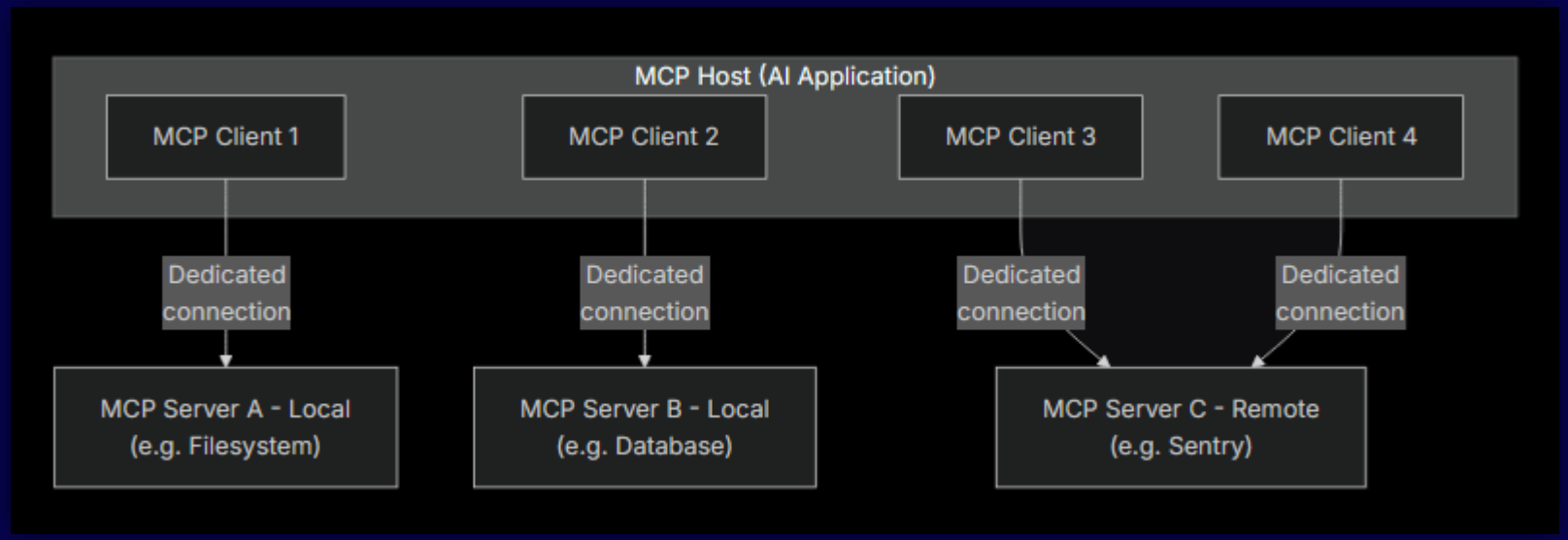
Listen to analysis
6 min

Hackers are now using AI to guide attacks in real time. In a statement that initially attracted little attention among Western analysts, Ukraine's national cybersecurity agency **warned** on July 17 that a Russian cyber threat group, known as **APT28**, is using AI in a novel way as part of its cyberattacks. Once the hackers gain access to their target, the AI instructs the malware how to move through the network and disrupt, destroy, or steal information. This more adaptive methodology makes it harder for defenders to detect and thwart attacks.

AI Is Reshaping the Cyber Threat Landscape

Intro / Context – new APTs

- MCP servers concepts



https://modelcontextprotocol.io/docs/learn/architecture

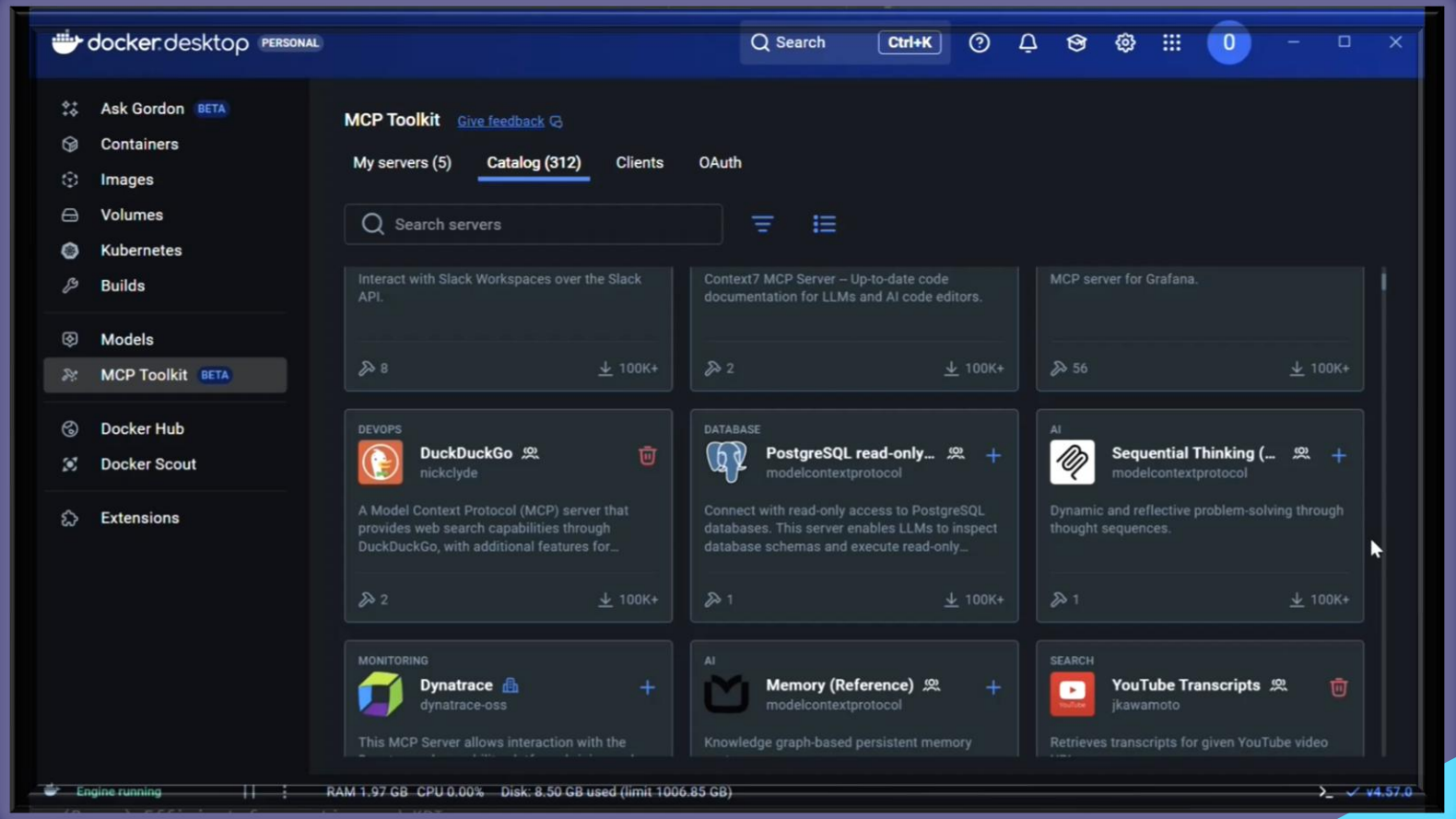
Intro / Context – new APTs

- MCP servers
  - **Transport layer**: Defines the communication mechanisms and channels that enable data exchange between clients and servers, including transport-specific connection establishment, message framing, and authorization.
    - **Stdio transport**
    - **Streamable HTTP transport (Server-Sent Events - SSE)**

Intro / Context – new APTs

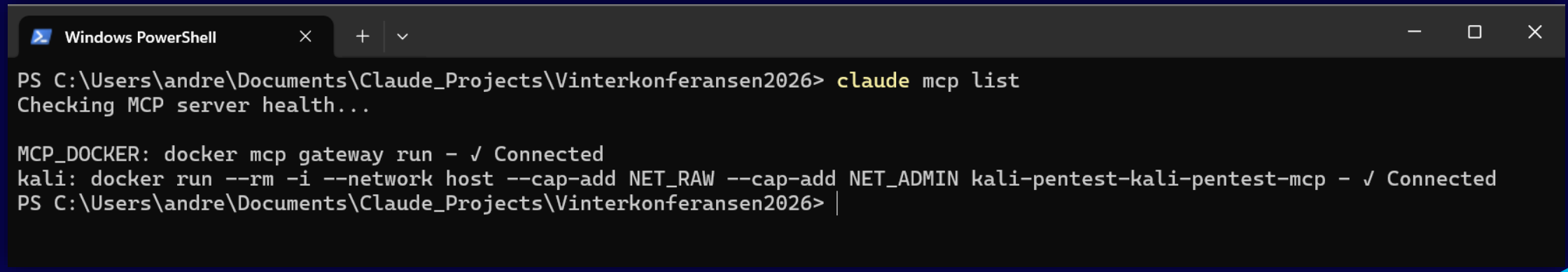
- MCP defines three core **primitives** that servers can expose:
  - **Tools**: Executable functions that AI applications can invoke to perform actions (e.g., file operations, API calls, database queries)
  - **Resources**: Data sources that provide contextual information to AI applications (e.g., file contents, database records, API responses)
  - **Prompts**: Reusable templates that help structure interactions with language models (e.g., system prompts, few-shot examples)

Intro / Context – new APTs



Intro / Context – new APTs

- My custom MCP server…



Demo

Impact for Threat intel

Attribution
gets foggier

Static IOCs
They already age like yogurt, MCP makes them spoil instantly

Threat modelling
changes

Detection Engineering
must adapt

🖳 So... what should I be looking for? 🤔

Some things to track in 2026...

Some things to track in 2026…

Track #1

Network shape.

Timing symmetry, consistent TLS configurations, predictable domain-registration churn, subtly similar HTTP header stacks, or the same C2 URI grammar.

Track #2

Track #3

Some things to track in 2026...

Track #1

Track #2

Behavioural signatures.

MCP engines chain TTPs based on internal logic: discovery → escalation → pivot → collection → exfil. The exact commands change, but the high-level sequence doesn't.

Track #3

Some things to track in 2026...

Track #1

Track #2

Track #3

Orchestration footprints.

MCP systems call out to themselves, their orchestration APIs, or their own provisioning modules.

Thank you for coming... 😊

https://www.linkedin.com/in/aflima/

0x4ndr3

https://0x4ndr3.github.io/

telenor | cyberdefence