

See what AI assistance enables an operator to build.

Agentic assistance can help an operator work through technical obstacles, adapt failed attempts, and assemble tools. The defensive question is what capability the work produces and which observable traces it leaves.

OHHHO Research examined an operator dependent on agentic assistance who obtained working tooling to create and manage remote access.

AI WRITES THE LURE
where the debate looks

AI BUILDS INFRASTRUCTURE AND TOOLING
a capability problem: where the shift is

Two layers of AI misuse, not the same size. OHHHO Research, It Built the Business.

72

HOURS · ONE DOCUMENTED CASE

The case documents a specific workflow, not the prevalence of AI-enabled attacks. Controlled research can then test a narrower question about observable post-access behavior.

OHHHO Research, June 12, 2026. [Read It Built the Business.](#)

WHAT THE ANALYSIS EXAMINED

Requests

What the operator asked the assistance to accomplish.

Adaptations

How the workflow changed when attempts failed.

Artifacts

What the resulting tools and operating patterns reveal.

[Discuss an AI-related observation mission →](#)

Turn a controlled result into a testable defensive question.

OHIIHO ran approximately 1,000 LLM-driven intrusion trials across four controlled labs. In the 17-model persistence panel, every model added an SSH key to ~/.ssh/authorized_keys on the observed account.

17 of 17

MODELS · ADDED AN SSH KEY IN THE PERSISTENCE PANEL

OHIIHO Research, April 23, 2026. Controlled experiments; the persistence result applies to the 17-model panel. It is not a commercial detection rate. [Read the study.](#)

The defensive question

Which post-access changes would help your analysts investigate unauthorized persistence?

The analytical boundary

An SSH-key change is a persistence lead. It does not, by itself, identify an AI operator or a particular model.

The HIIH discussion

Start with an observable behavior, such as an unauthorized persistence change. See what the Surface records, then test how that evidence supports your analysts.

NAMING

disposable names · fresh hosting verification

ENDPOINT / BUILD

self-signed binary · control weakened after refusal

VIRTUALIZATION / NET

VM on a non-server · NAT and forwarding around it

WORKFLOW

fixes across unrelated layers: the tell

Defensive residue by layer: hunt the sequence of fixes, not IOCs. OHIIHO Research, It Built the Business.

Define an observation question →