

Give your analysts the sequence behind the signal.

HIIH FOR SOC AND THREAT INTELLIGENCE

HIIH Surface records adversary activity on controlled targets and turns selected observations into structured Findings. OHIIHO deploys and operates it in hours, with no agents in your production. Your team gains a direct source to examine alongside its own logs and threat intelligence.

- **Triage the behavior.** Examine whether repeated access activity is consistent with scanning, access validation, or deeper engagement.
- **Develop a hunt.** Use the sequence and available client characteristics to define what to look for in your telemetry.
- **Inform detection engineering.** Turn an assessed behavior into a candidate detection and a controlled test.

ILLUSTRATIVE OBSERVATION SEQUENCE

TIMING	ACCESS BEHAVIOR	CLIENT CONTEXT
First contact	Several access attempts against the same account	One client signature across the attempts
Repeated activity	Similar client characteristics and short intervals recur	Same source context
Connection ends	No post-access activity in this illustrative sequence	Connection closed by the source

Illustrative observation sequence. No timestamps or addresses from a live sensor.

RESEARCH EXAMPLE: ACCESS VALIDATION

An OHIIHO SSH study linked activity from many sources to one coordinated access-validation campaign through repeated client characteristics and behavior.

[Read the AsyncSSH analysis.](#)

The analyst's next task is to assess the evidence and test its relevance against the organization's own activity.

[Request an analyst walkthrough →](#)

From a Finding to an analyst decision.

HIIH FINDING

ACCESS

Illustrative example

CONFIDENCE  MEDIUM

OBSERVED ACTIVITY	Repeated access attempts followed by short interactions and disengagement.
MISSION RELEVANCE	Profile-specific; the pattern alone does not establish actor identity or customer-directed targeting.
WHY IT MATTERS	Automated access validation against a profile like yours is a lead for your own access logs.
SUPPORTING MATERIAL	Access sequence, timing, source context, and available client characteristics.
SUGGESTED ACTION	Review related edge access activity and assess exposed access paths.

01 Inspect

Review the observed facts, assessment, confidence, and supporting context in the Surface Console.

02 Correlate

Compare the pattern with your edge logs, identity telemetry, exposure context, and other intelligence.

03 Decide

If the pattern appears in your telemetry, investigate the account and its exposure. If it does not, record the hypothesis and monitor for recurrence.

API and authorized MCP paths support retrieval into your tools. Start with one Finding type and one destination, then verify which fields and supporting context reach the analyst.

Illustrative analyst view, not a live Console export.

[Review your first workflow →](#)