

A threat indicator tells you something looks bad. HIIH Surface shows you what adversaries really do.

HIIH SURFACE | MANAGED ADVERSARY ENGAGEMENT INTELLIGENCE PLATFORM

HIIH Surface is a managed deployment of controlled targets, separate from your production assets. Deployment is easy: you just add an engagement surface for adversaries. Access-validation botnets, ransomware, worms, criminals, APT actors, and AI-assisted operators engage with them. OHIHO operates the environment and turns selected observations into actionable Findings your team can examine and integrate.

- **See the behavior, not just the indicator.** Access material presented, commands run, and files dropped, in order, on supported targets.
- **Investigate with the sequence.** Each Finding links observed facts to its assessment and supporting material.
- **Hunt from observed activity.** Turn what adversaries actually did into hypotheses and candidate detections.



Millions of hostile interactions every month across OHIHO's sensors. Only the behavior worth your time

Analysis filters what reaches the targets; your team receives the behavior worth examining. A published OHIHO study turned one month of activity against an exposed edge-appliance profile into how access is validated and reused.

OHIHO Research, June 24, 2026. [Read the FortiBleed study.](#)

[Request a Surface walkthrough →](#)

Inspect the facts. Understand the assessment. Choose the next step.

A HIIH Finding connects observed activity with its assessment, confidence, supporting material, and suggested action. Your analysts inspect it in the Surface Console; your tools retrieve available Findings and context through the API and authorized MCP paths.

WHERE IT FITS

SOURCE	WHAT IT ADDS
Threat intelligence feeds	External indicators and context from broader collection and reporting.
EDR and production telemetry	Activity and detections from the systems you operate.
HIIH Surface	Direct observations from controlled targets, deployed around your mission and separate from production.

Choose the depth the question needs. Contact Points record service-level interaction. Live Hosts support deeper observation of commands, files, and post-access activity on supported targets.

You bring the question and use the intelligence. OHIIHO deploys and operates the Surface: hours, not months, no agents in your production. Bring one question and the workflow that would use the answer.

HIIH FINDING

ACCESS

CONFIDENCE

MEDIUM

Illustrative example

OBSERVED ACTIVITY	Repeated access attempts with recurring client characteristics and timing, ending without deeper interaction.
MISSION RELEVANCE	Profile-specific; relevance to your organization requires correlation with its exposure and telemetry.
WHY IT MATTERS	Shows what is being validated against a profile like yours before any deeper engagement.
SUPPORTING MATERIAL	Access observations, timing, source context, and available client characteristics.
SUGGESTED ACTION	Compare the pattern with edge and identity telemetry, investigate exposed access paths, and monitor recurrence.

Illustrative analyst view, not a Console export. Customer-directed targeting is not established by this pattern alone.

Request a Finding walkthrough →