

Start with the question you need to answer.

HIH SURFACE | PRODUCT, SOLUTION, RESEARCH, AND TECHNICAL BRIEFS

Explore the offer, inspect the public evidence, or go directly to the brief for your team. The technical and data briefs give the next level of detail.

HIH Surface is available through Early Access. Deployment is easy: hours, not months, operated by OHIIHO. ohiiho.com/contact.

UNDERSTAND THE PRODUCT	
Product Overview	p. 2-3
Company and Research	p. 24
INSPECT THE EVIDENCE	
Evidence from OHIIHO Research	p. 8-9
Post-Access Intelligence	p. 13-14
AI-Enabled Adversary Behavior	p. 15-16
APPLY IT TO YOUR TEAM	
HIH for MSSP and MDR Partners	p. 4-5
HIH for SOC and Threat Intelligence	p. 6-7
HIH for Financial Services	p. 17-18
HIH for CERT and Government	p. 19-20
Edge Exposure Intelligence	p. 11-12
PREPARE THE NEXT STEP	
Evaluate HIH Surface	p. 10
Architecture, Deployment, and Integration · A4	p. 21-22
Security, Data, and Responsibilities · A4	p. 23

LEARN MORE ohiiho.com/contact/

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. OHIIHO 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 OHIIHO's sensors. Only the behavior worth your time

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

OHIIHO 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.

Request a Finding walkthrough →

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.

Add first-party adversary intelligence to your managed service.

HIIH FOR MSSP AND MDR PARTNERS

Give clients observations they can investigate and evidence your team can explain. HIIH Surface adds a first-party source of adversary intelligence to your service. OHIIHO is the product: it deploys and operates the Surface in hours, not months. You are the service.

- **Enrich client investigations.** Bring access patterns, behavioral sequences, and supporting context into SOC triage.
- **Make briefings more concrete.** Explain what was observed, what it may mean, and what the client should check.
- **Build a focused offer.** Start with a client need and the intelligence output that would support it.

YOU ARE THE SERVICE

The client relationship, SOC workflow, integration, reporting, and the meeting rhythm.

OHIIHO IS THE PRODUCT

The managed Surface that receives and observes hostile activity, separate from production, with L3 support.

A BRIEFING YOUR TEAM CAN BUILD ON

An OHIIHO study linked SSH access-validation activity from many sources to one coordinated campaign through shared client characteristics. A client discussion can then focus on related access patterns in the client's own telemetry.

Published June 24, updated September 7, 2026. [Read the AsyncSSH analysis.](#)

[Discuss a partner use case →](#)

Choose the service your client needs first.

The HIIH partner model supports three service patterns. Start with the client’s question and the output your service will deliver.

WHAT IS REACHING THIS PROFILE?

Early-Signal Service

WHAT HAPPENS AFTER ACCESS?

Engagement & Evidence Service

WHAT SHOULD THE CLIENT UNDERSTAND?

Intelligence Briefing Material

OHIIHO	YOUR TEAM	YOUR CLIENT
Deploys and operates the Surface.	Owens the client service and L1/L2 workflow.	Chooses the mission and exposure.
Provides the platform and L3 support.	Retrieves results, reports, and escalates.	Supplies context and decides on actions.

Pick the first client deliverable: a triage finding, an engagement review, or an intelligence briefing. OHIIHO deploys the Surface in hours; your service does the rest.

Commercialization and redistribution rights are defined in the partner agreement.

[Start your first partner service →](#)

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 →](#)

Inspect the evidence behind the intelligence.

EVIDENCE FROM OHIIHO RESEARCH

OHIIHO Research publishes primary observations from controlled environments, with the analysis and evidence needed to examine the conclusions.

ACCESS VALIDATION

One exposed profile, one month

The study maps how access is validated and reused in the hostile activity reaching a single edge-appliance profile. For defenders, the value is in the behavior behind the volume.

[FortiBleed](#), June 24, 2026.

AI-ENABLED CAPABILITY

72 hours in one documented case

An operator dependent on agentic assistance obtained tooling to create and manage remote access. The analysis follows the workflow and the artifacts it produced.

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

POST-ACCESS BEHAVIOR

Encryption and propagation together

The analyzed Sorry-worm sample ran file encryption and SSH propagation concurrently in the same process. That relationship gives defenders a combined behavior to investigate.

[Inside Sorry-worm](#), May 1, 2026.



CYBER ARSENAL: CRIMEWARE RECOVERED FROM LIVE SESSIONS

CYBER ARSENAL

24 crimeware tools, dissected for defenders

Webshells, grabbers, and crackers dropped by real operators during live sessions, catalogued with detection signatures, the weaknesses of the tools themselves, and the backdoors their own distributors planted.

[Browse the Cyber Arsenal](#).

[Explore OHIIHO Research](#) →

From a captured Redis sequence to defensive content.

HYDRA BOT V5 | REDIS ACTIVITY OBSERVED FROM THE TARGET SIDE

One connection delivered artifacts associated with four Redis abuse patterns within 4.4 seconds. Four module-loading attempts followed, from about 10 seconds to the final attempt at 26.5 seconds.

0-4.4 s

Artifacts for four abuse patterns arrive over one TCP connection

About 10-26.5 s

Four module-loading attempts follow; none succeeds

All exploitation techniques were attempted; none succeeded against the sensor. The timing describes the observed sequence, not HIIH detection latency. Sequence, not to scale.

What the analysis used

Commands in sequence, a recovered stager, related artifacts, and infrastructure references.

What defenders can inspect

NIDS rules, YARA, Sigma, and IOC content, with hunting and hardening guidance. Review the reasoning and validate the material for your environment.

NIDS rules

YARA

Sigma

IOCs

requirepass

blocks all five vectors

bind 127.0.0.1

no external access

ACL deny

@admin · @dangerous

non-root

limits cron and SSH paths

firewall

block 6379 from the Internet

One prerequisite, unauthenticated Redis; one setting closes all five vectors. OHIIHO Research, September 1, 2026.

[Read the report and defensive content →](#)

Evaluate HIIH Surface against a question that matters.

LIVE IN HOURS | A TIME-BOXED EARLY ACCESS EVALUATION

OHIIHO deploys and operates a Surface exposed to real adversary activity, separate from your production assets, with no agents in your production. Your team reviews real Findings and decides.

01 Live in hours

OHIIHO deploys the Surface around your question. Nothing to install on your side.

02 Review the results

Your team examines real Findings and context in the Surface Console and records what they add to investigation, detection, or hardening work.

03 Decide

Compare the results with the criteria and choose what comes next.

LEARN MORE ohiiho.com/hiih/evaluate/

What your team contributes. One intelligence question, a receiving team, and time to review the results. The evaluation does not depend on a particular adversary appearing. Bring the question and the workflow that would use the answer.

Day one

CRITERIA FIXED BEFORE IT STARTS

WHAT THE EVALUATION MEASURES

- ☐ Time to first meaningful engagement.
- ☐ Intelligence your existing sources did not provide.
- ☐ Engagement depth reached.
- ☐ Findings your team could act on.
- ☐ Containment incidents: target none.

[Request an Early Access evaluation →](#)

See what adversaries test against a selected edge profile.

EDGE EXPOSURE INTELLIGENCE | A HIIH SURFACE MISSION

Scanners, access validators, and exploit automation can reach the same exposed service. A HIIH Surface provides a controlled observation point around a selected technology profile so your team can examine what those interactions reveal.

QUESTIONS A MISSION CAN INVESTIGATE

Access

What access material and validation patterns does the actor present?

Exposure

Which requests and exploitation paths does the actor test?

Engagement

What does the actor do when deeper interaction is available?

The target mix determines the interaction depth and available outputs.

RESEARCH EVIDENCE

One exposed edge-appliance profile, observed for one month, showed how access validation and reuse behave at scale. The analytical value came from the patterns, not the volume.

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

HIIH TARGETS

Hostile execution

On controlled targets, operated by OHIIHO.

SEPARATE

Your production

Outside the engagement path.

[Discuss an edge-exposure mission →](#)

Turn an exposure question into an analyst workflow.

ILLUSTRATIVE MISSION

“Which access-validation patterns reach this profile, and what should our SOC examine?”

01 Choose the profile

Pick the technology profile and exposure; OHIIHO deploys the matching targets.

02 Examine the activity

Review access sequences, repetition, timing, and available client characteristics.

03 Apply the result

Compare the observed pattern with production access logs and investigate exposed access paths.

A Contact Point records service-level interaction. Deeper questions call for a Live Host. OHIIHO deploys the right targets for your question, in hours.

HIIH FINDING

ACCESS

Illustrative example

CONFIDENCE  MEDIUM

OBSERVED ACTIVITY

Repeated access attempts, recurring client characteristics, and short interactions.

WHY IT MATTERS

Behavior consistent with automated access validation against the selected profile.

SUGGESTED ACTION

Check related access logs and investigate exposed access paths.

Illustrative example. An Internet-facing interaction alone does not establish customer-directed targeting.



The access-broker chain: HIIH observes the validation step. OHIIHO Research, FortiBleed.

[Start an edge-exposure mission →](#)

Understand what happens after access.

POST-ACCESS INTELLIGENCE | OBSERVED ON A HIIH LIVE HOST

On a HIIH Live Host, an actor's commands, files, tools, and search sequence can reveal what it considers valuable. OHIIHO operates the controlled target separately from your production assets.

- **Reconstruct the activity.** Examine the available session record and the order of actions.
- **Assess the likely objective.** Compare the observations with the explanations the evidence supports.
- **Develop a hunt.** Identify behaviors and artifacts to check in your own telemetry.

OBSERVED ON A HIIH LIVE HOST

Session established



Resource searches

files • tools • order of actions

YOUR ANALYTICAL WORKFLOW

Assess

the likely objective



Investigate

your own telemetry

A CASE WORTH FOLLOWING

An SSH botnet logged in, searched for resources, and disconnected without dropping a payload during the observed wave. The search sequence supported an assessment of host-value triage. The next page examines what the searches revealed and what they did not establish.

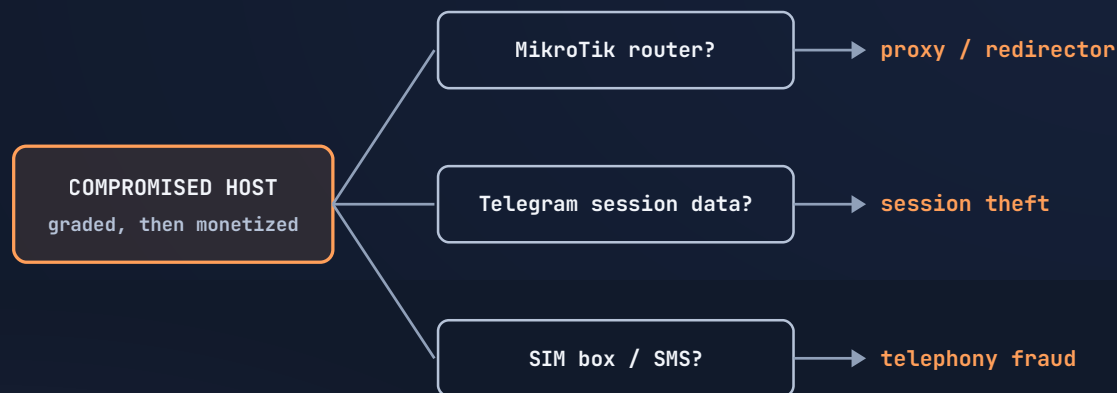
OHIIHO Research, June 12, 2026. [Read the host-triage study.](#)

Explore a post-access mission →

Assess the objective from the search sequence.

ONE OBSERVED WAVE | THE SAME SEARCH SEQUENCE, REPEATED FROM MANY SOURCES

The observed SSH activity searched for MikroTik router indicators, Telegram session data, and GSM/SMS-related resources, then disengaged. No payload was dropped during this wave.



Host-value triage: grade the asset, then monetize. OHIIHO Research, host-triage study.

RESEARCH CASE

OHIIHO Research

OBSERVED	Repeated post-access searches for the same categories of resources.
ASSESSED	Behavior consistent with evaluating a host's value before deciding how to use it.
DEFENSIVE USE	Hunt for the combination of searches and examine access to the relevant resources.

For your mission, name the behavior you want to understand. OHIIHO deploys the Live Hosts and delivers the session and artifact material your analysts examine.

OHIIHO Research, June 12, 2026. Wave observed June 11. Subsequent monetization or fraud was not demonstrated in this wave. [Read the evidence and analysis.](#)

[Discuss a post-access mission →](#)

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.

OHIIHO 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. OHIIHO 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.

OHIIHO 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 →](#)

Add direct evidence to your access-risk decisions.

HIIH FOR FINANCIAL SERVICES

Illustrative use case. A financial-services security team is assessing access-validation activity against a relevant remote-access profile. A HIIH Surface, live in hours, provides controlled observations to examine alongside the organization's access logs and exposure context. The decision to support: does the observed pattern justify an identity investigation, a monitoring change, or continued observation of the selected profile?

- **For the SOC.** Investigate related access patterns and exposed access paths.
- **For threat intelligence.** Assess the behavior and document the evidence supporting the interpretation.
- **For security and risk stakeholders.** Explain what was observed, what remains uncertain, and which defensive checks are justified.

Your partner or integrator tailors the service to your team; OHIIHO deploys and operates the Surface.

RESEARCH EVIDENCE

A published OHIIHO study examined access validation and reuse patterns against one exposed edge-appliance profile.

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



The access-broker chain: HIIH observes the validation step. OHIIHO Research, FortiBleed.

[Discuss a financial-services use case →](#)

What your security, data, and procurement teams get.

Start with one intelligence question and the team that will use the answer. Security, data, and procurement stakeholders find what they need in one brief.

AREA	WHAT YOU GET
Mission and owner	One question, one receiving team, one decision the intelligence supports.
Exposure and execution	Your chosen profiles; hostile execution stays on HIIH targets, outside your production.
Analyst workflow	Findings with evidence in the Surface Console, retrievable through the API and authorized MCP paths.
Data and access	Documented hosting, retention, authorized users, minimization, and export conditions.
Evaluation	A time-boxed Early Access evaluation with criteria fixed before day one.

Deployment is easy: hours, not months, operated by OHIIHO. Your partner or integrator handles the tailored service around it.

For more detail, see [Architecture, Deployment, and Integration](#) and [Security, Data, and Responsibilities](#). A technical edition of each brief is available on request.

HIIH TARGETS

Hostile execution
On controlled targets, operated by OHIIHO.

SEPARATE

Your production
Outside the engagement path.

[LEARN MORE](#) ohiiho.com/solutions/industries/financial-services/ • ohiiho.com/company/trust/data-and-responsibilities/

Request an Early Access evaluation →

Build primary evidence for a defined sector question.

HIIH FOR CERT, GOVERNMENT, AND CRITICAL INFRASTRUCTURE

Incident reports and external intelligence provide essential context. A HIIH Surface adds controlled observation around selected technology and exposure profiles, deployed around your mission in hours.

- **Define the question.** Identify the recurring behavior or technology profile the team needs to understand.
- **Collect primary material.** Examine hostile interactions and supported post-access activity outside member production assets.
- **Prepare a useful output.** Give authorized CERT, SOC, and analytical recipients qualified observations and defensive checks.

Defined question

behavior or technology profile



Controlled collection and analysis

selected profiles • HIIH Surface



Operational brief for authorized recipients

CERT • SOC • analytical workflows

RESEARCH EVIDENCE

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

The study describes deployed collection points, not national or sector-wide coverage. [Read the AsyncSSH analysis.](#)

[Discuss a sector intelligence mission →](#)

Define the brief your recipients need.

Name the question and the recipients. OHIIHO deploys the collection and delivers the evidence and defensive checks the brief must contain.

ILLUSTRATIVE OPERATIONAL BRIEF	
QUESTION	What recurring SSH access behavior should recipients examine in their own telemetry?
OBSERVED	Recurring SSH access activity from multiple sources, with similar client characteristics and behavior across several collection points.
ASSESSED	The recurring characteristics and behavior support an assessment of coordinated access validation.
DEFENSIVE CHECKS	Review related access patterns in recipients' own telemetry and assess local relevance.
LIMIT	Collection geography does not establish actor origin or sector-wide targeting.

Editorial example based on the published [AsyncSSH study](#). It is not a customer-delivered brief.

Hosting, retention, and export are documented for your program. OHIIHO Sovereign Programs follow a separate eligibility-reviewed path; this brief covers the commercial HIIH Surface.

[LEARN MORE](#) ohiiho.com/solutions/industries/government/

Collection

Profiles, exposure, placement, and engagement depth.

Analysis

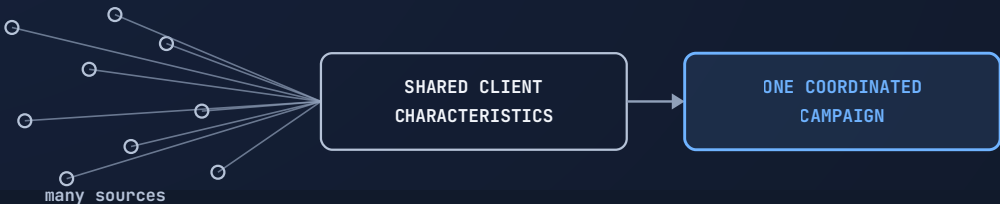
Evidence needed to support the assessment.

Delivery

Receiving team, output format, and retrieval path.

Sharing

Authorized recipients, redaction, and redistribution rights.



Many sources, one campaign, linked through shared client characteristics. OHIIHO Research, AsyncSSH study.

Start a sector intelligence mission →

How a HIIH Surface turns interaction into intelligence.

A HIIH Surface is a managed environment built to be engaged by real adversaries, separate from your production assets. OHIIHO operates it around your mission; your team receives Findings with their evidence.



Engagement Adversaries reach credible targets prepared for the mission: Contact Points for service-level interaction, Live Hosts for deeper observation on real operating systems.

Observation and analysis What adversaries bring and do is recorded as evidence. Selected activity is analyzed and qualified into Findings; not every observation becomes a Finding.

Authorized retrieval Your analysts inspect results in the Surface Console. Your tools retrieve available results through the API and authorized MCP paths.

Engagement Gateway OHIIHO's engagement layer. It governs how each hostile interaction is engaged across the Surface, and what is recorded.

Controlled operation Outbound activity is governed by the operating policy and deployment controls. OHIIHO deploys and operates the platform: hours, not months, no agents in your production.

Functional view, not a network topology. The detailed architecture and the integration worksheet are provided in the technical edition of this brief, on request.

LEARN MORE ohiiho.com/hiih/surface/anatomy-and-assets/

Choose the retrieval path your workflow needs.

HIIH uses pull-based delivery. The same Finding identity is preserved across Console, API, and MCP representations; available fields and supporting detail depend on the path and permissions.

PATH	INTENDED USE	WHAT YOU GET
Surface Console	Inspect Findings and available context.	Users, related observations, artifacts, and available replays.
API	Retrieve available results programmatically.	Authenticated access, documented fields, and your destination.
MCP	Query selected Findings and context through authorized tooling.	Permissions, accessible context, and tool behavior.
STIX 2.1 over TAXII 2.1	Retrieve structured objects through the CTI path.	Available by mission; object content and destination support.

Today. The Access Finding family is live and inspectable in the Surface Console; other families and evidence depths are being populated.

WHAT YOUR DEPLOYMENT INCLUDES

WHAT YOU GET	DOCUMENTED IN YOUR DEPLOYMENT
Mission	Question, receiving team, and intended use.
Exposure	Your profiles and access paths; placement and change handling.
Operations	OHIIHO, customer, and partner roles; contacts and change handling.
Data and delivery	Hosting, retention, authorized users, export conditions, and integration owner.

Start with one result and one destination; your partner or integrator connects the rest. A supported format does not, by itself, establish a tested production connector.

LEARN MORE ohiiho.com/hiih/delivery/ · ohiiho.com/hiih/findings/research-and-limits/



SCAN TO CONTACT OHIIHO

Request the technical edition →

Separate adversary engagement from production.

The Surface exposes only the profiles and targets selected for the mission. Adversaries interact with HIIH Contact Points or Live Hosts while customer production assets remain outside the hostile execution path.

Outbound activity is governed by the operating policy and deployment controls. This separation does not mean that every attack against production is diverted to HIIH: existing production controls remain in use.

RESPONSIBILITIES

OHIIHO

Deploys and operates the Surface, collects and structures results, and implements the controls.

Partner, where applicable

Runs the client service, L1/L2 workflow, reporting, and service obligations.

Customer

Brings the mission, names authorized users, and uses the results.

AREA	PRINCIPLE
Collection	Follows the target and the engagement depth. Material presented by an adversary may concern third parties, so access and reuse require explicit controls.
Access and retention	Hosting, retention, authorized users, minimization, and export conditions are documented for your deployment.
Separation	Customer-specific evidence and outputs are logically separated. Any cross-Surface correlation requires a separately governed path.
Research	Publication requires review and sanitization; it is not an automatic downstream use of customer data.

The technical edition of this brief details the data classes and the responsibility model. It is provided on request, as a nominative copy.

LEARN MORE ohiiho.com/company/trust/separation-and-containment/ · ohiiho.com/company/trust/data-and-responsibilities/



SCAN TO CONTACT OHIIHO

Request the technical edition →

Research-led intelligence. Built and operated by OHIIHO.

OHIIHO | ADVERSARY ENGAGEMENT INTELLIGENCE

OHIIHO builds and operates HIIH Surface. Our tech founder brings three decades of offensive and defensive cybersecurity practice. The company is headquartered in Singapore, with a European entity in Estonia.

PRODUCT

Managed Surfaces turn selected hostile interactions into Findings and supporting context for defined security missions.

OPERATIONS

OHIIHO runs the specialized engagement environment. Customer and partner teams use the results in their own security processes.

RESEARCH

Published studies let customers examine the observations, reasoning, and defensive content behind the approach.



GOVWARE 2026 TECH TALK, SINGAPORE, OCTOBER 13, 2026: LAURENT OUDOT ON STAGE IN FRONT OF A FULL ROOM

PUBLIC CONTRIBUTION

Laurent Oudot spoke at GovWare 2026 (Singapore, October 13, 2026): Counter-Intelligence Against Agentic AI Attackers. [View the program](#) · [Explore OHIIHO Research](#).

Discuss your mission with OHIIHO →

Five things to remember.

HIIH SURFACE | KEY POINTS OF THIS COLLECTION

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

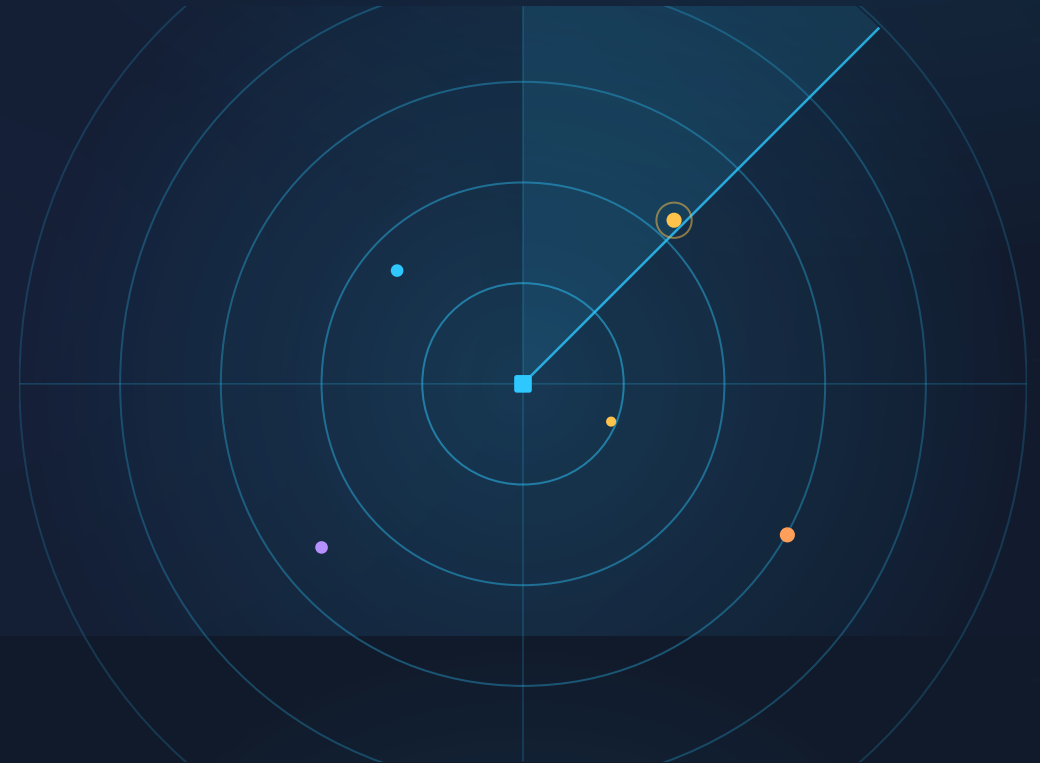
Separate from production. Controlled targets, deployed in hours and operated by OHIIHO, around the question you bring.

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

Findings, not feeds. Your analysts inspect them in the Surface Console; your tools retrieve them through the API and authorized MCP paths.

Public evidence. The studies cited in this collection are published by OHIIHO Research and open to your review.

Bring one question and the workflow that would use the answer.



[Request a Surface walkthrough →](#)