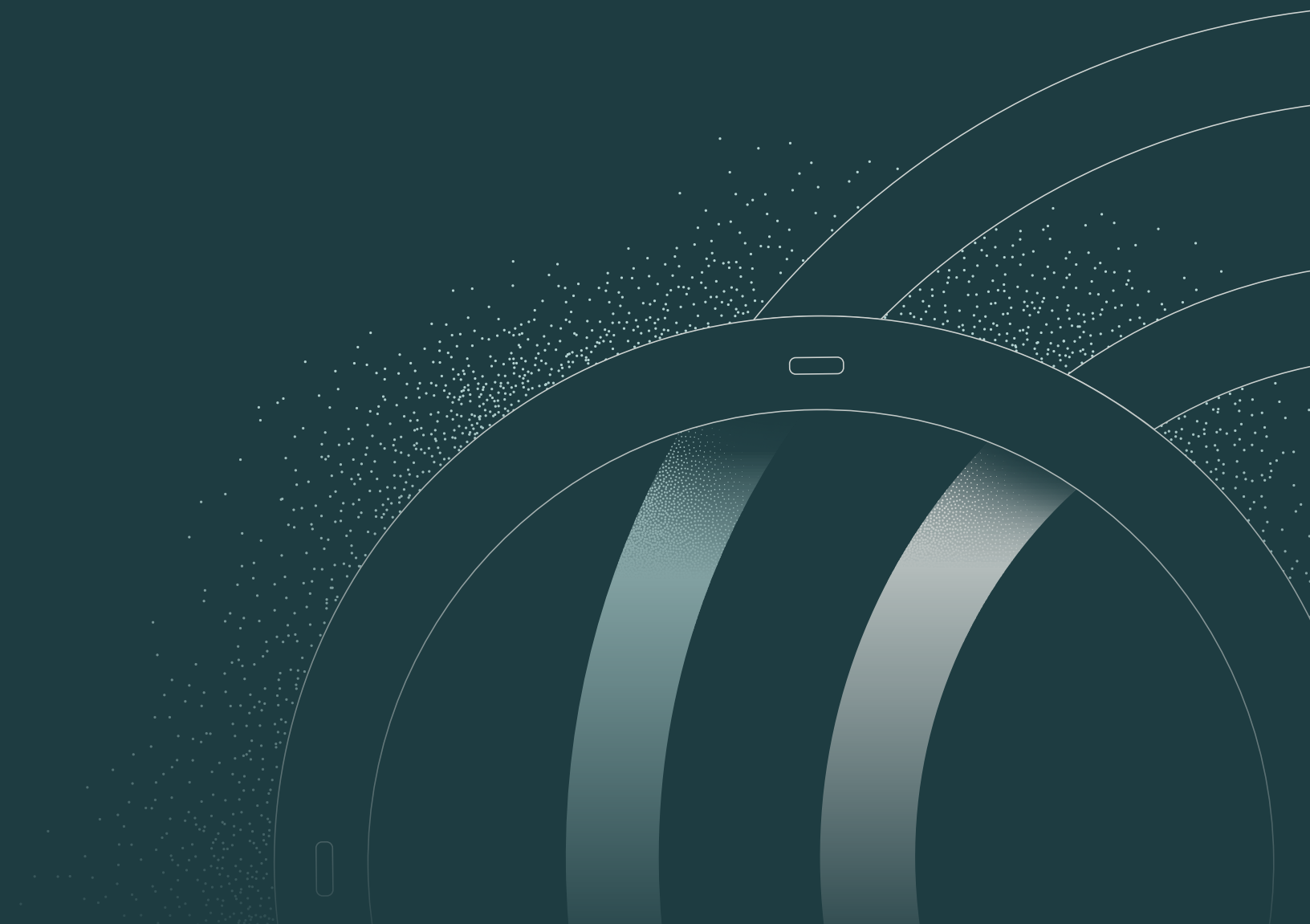
censys

CUSTOMER WORKBOOK

Operationalizing Censys in Your SOC



INTRODUCTION

About This Workbook

One intelligence layer. Every workflow.

Most SOCs don't have an intelligence problem — they have an intelligence distribution problem. External context lives in one analyst's browser tab while the SIEM, SOAR, TIP, EDR consoles, and ticketing queues run on stale feeds and guesswork. The result: inconclusive alerts, slow investigations, and detections that lag the adversary.

This workbook operationalizes a different principle: make Censys Internet Intelligence a standing capability in security operations.

Not every workflow needs the same thing. Triage needs a fast, streamlined verdict on an external IP. Investigation needs to reconstruct a host as it was at the moment of an incident. Hunting needs to pivot from one indicator to a whole campaign. Defense needs Tools/TTP turned directly into detections, feeds, and blocklists. Censys feeds all four, but through different capabilities.

In this workbook, you'll stand up each of those four workflows, one phase at a time.

Core Topics

PHASE 1	Triage. Enrich every alert in the SIEM/SOAR with the Unlimited Enrichment API and triage with evidence, not guesswork.
PHASE 2	Investigate. Reconstruct any IP at the moment of the incident with point-in-time historical lookups in the platform.
PHASE 3	Hunt. Pivot from one indicator to the full campaign in Platform Search and monitor it continuously with Collections.
PHASE 4	Defend. Turn live adversary infrastructure into automated defense.
SIGN-OFF	A checklist to confirm Censys is wired into each workflow, plus your immediate next steps.

HOW TO USE THIS WORKBOOK

Each phase lists the actions needed to stand up one workflow, with sample API calls and queries. Jump to your discipline, or consider each sequentially to get a complete picture of the intelligence layer. Your Censys CSM can pair enablement sessions to each phase; note questions as you go and bring them to your next check-in.

IMPLEMENTATION ROADMAP

A phased path to full operationalization

Each phase follows the same pattern: enable the team, wire Censys into the tools they already use, and validate on live work before scaling.

Triage

Security Analysts

Provision platform and API access, connect the Unlimited Enrichment API to your SIEM/SOAR with a single REST call, and tune on live alerts.

Fewer inconclusive alerts · faster routine triage · higher-confidence escalations

Investigate

Forensics + IR

Enable IR on search, host profiles, and point-in-time historical views; wire historical lookups and pivot workflows into runbooks.

Investigations from hours to minutes · no tool-switching · confident incident declaration

Hunt

CTI + Advanced Threat Ops

Define hunt starting points, build Collections to map campaigns, and automate continuous monitoring of adversary infrastructure.

One IOC to full footprint in minutes · campaign infrastructure in real time

Defend

Detection + Security Engineering

Stand up webhooks for new infrastructure, generate blocklists and detection rules from live signatures, automate blocking via SOAR.

Block before the perimeter · fewer false positives · reduced dwell time

PHASE 1 · TRIAGE · SECURITY ANALYSTS

Enrich every alert with Internet intelligence

THE RISK

Roughly two-thirds of all alerts involve external IPs or domains, yet most are triaged with little or no external context. Analysts burn time on manual lookups across disconnected tools, alerts close as inconclusive, and real threats sit in the queue while adversary breakout times are measured in minutes.

THE STRATEGY

Make enrichment automatic, not optional — and make it cheap enough that you never have to ration it.

This is the job of the Unlimited Enrichment API: a lightweight, credit-free endpoint purpose-built for high-volume, automated lookups in SOC environments. Because its calls don't draw down your standard API credit balance, you can enrich every alert with an external indicator on ingest.

One call against an external IP returns a compact, standardized profile: the Censys Reputation Score with its level and evidence, detected threat name/type/tactic, host and service labels, service count with ports and protocols, WHOIS and ASN ownership, forward and reverse DNS, geolocation, and third-party context from GreyNoise, IPinfo, Mallory.ai, and others. The Unlimited Enrichment API is the quick glance — Phases 2–4 are the deep dive.

PHASE 1 · TRIAGE · CONTINUED

1

Provision platform & API access

Confirm seats for the analyst team, generate a service credential for the SIEM/SOAR, and identify the priority alert sources (firewall, IDS, EDR, proxy) that will be enriched first.

Frequency: Once, revisit as new alert sources are onboarded.

2

Connect enrichment to the SIEM / SOAR

Deploy the native Censys integration for your platform (Splunk ES, Microsoft Sentinel, Google SecOps, Palo Alto XSOAR, and more) or call the enrichment endpoint directly from a playbook so every alert with an external indicator is enriched on ingest.

Frequency: Once, then per new playbook.

3

Validate & tune on live alerts

Run enrichment against one high-volume alert queue for a week. Compare disposition speed and escalation quality against the prior baseline, tune which fields display in the analyst view, then roll out to remaining queues.

Frequency: Daily review, then weekly spot checks.

SAMPLE — SINGLE-CALL ALERT ENRICHMENT

```
curl -s
"https://api.platform.censys.io/v3/global/asset/enrichment/host/198.51.100.23" \
  -H "Authorization: Bearer $CENSYS_TOKEN"
# Returns: services, reputation score, threat labels (e.g. c2, tor-exit),
# certificates, WHOIS & DNS — one payload, ready for the SOAR playbook
```

PHASE OUTCOMES

- Fewer inconclusive alerts
- Faster triage on routine alerts
- Higher-confidence escalations

PHASE 2 · INVESTIGATE · FORENSICS + IR

Reconstruct the full picture of any incident

THE RISK

By the time IR gets an incident, the adversary's infrastructure has often changed — the C2 host is dark, the certificate rotated, the domain re-pointed. Investigating with only current-state data means reconstructing the incident from guesswork, switching between tools mid-investigation, and declaring (or dismissing) incidents without confidence.

THE STRATEGY

Extend enrichment backward in time. Censys point-in-time historical views answer the four questions every investigation turns on: What is this host? Who owns it? Has it changed? What else is linked? — for the exact moment of the incident, wired directly into the runbooks and log sources IR already uses.

PHASE 2 · INVESTIGATE · CONTINUED

1. **Enable the IR team on the platform**

   Run a working session with the IR/forensics team on Platform Search, host history timelines, and certificate/DNS pivots. Use a recent closed incident as the exercise so the team validates historical views against known ground truth.

   Frequency: Once, refresh when new investigators join.

2. **Wire historical lookups into runbooks**

   Add an at-time enrichment step to the top of each IR runbook: for every external indicator in scope, pull the host state at the incident timestamp, including services, certificates, labels, ownership and attach it to the case record automatically.

   Frequency: Once per runbook, then per new runbook.

3. **Establish pivot and investigation workflows**

   Document the standard pivot sequence: indicator → host profile → shared certificate or favicon → related hosts → netblock. Capture each pivot's results in the case so scoping decisions (contain one host vs. block a campaign) are evidence-backed.

   Frequency: Per investigation, reviewed monthly for new pivot types.

SAMPLE — POINT-IN-TIME HOST RECONSTRUCTION

```
# What was this IP running when the VPN log flagged it?
curl -s
"https://api.platform.censys.io/v3/global/asset/enrichment/host/203.0.113.7" \
  -H "Authorization: Bearer $CENSYS_TOKEN" \
  --url-query "at_time=2026-06-14T08:00:00Z"
# Compare against current state to answer: has it changed? what else is linked?
```

PHASE OUTCOMES

- Investigation time from hours to minutes
- No tool-switching mid-investigation
- Confident incident declaration

PHASE 3 · HUNT · CTI + ADVANCED THREAT OPS

Hunt adversaries across the Internet

THE RISK

Hunting from a single IOC against internal telemetry finds only what has already reached you. Adversary campaigns are built from dozens or hundreds of hosts that share fingerprints, certificates, JARM/JA4, favicons, hosting patterns, and banner signatures — stale threat feeds surface them long after the infrastructure has moved.

THE STRATEGY

Hunt the adversary's infrastructure, not just your logs. Seed each hunt with a fingerprint, expand it across the Internet with Censys Platform, then convert the hunt into a Collection — a standing query that continuously surfaces new assets matching the pattern the moment they appear.

1

Define hunt starting points

With CTI, pick the campaign families that matter to your org and record their seed artifacts. Censys ARC's threat dataset can get you started. Keep a shared hunt register so work isn't duplicated.

Frequency: Weekly hunt planning session.

2

Build Collections to map campaigns

For each seed, pivot outward in Platform Search and save the resulting query as a Collection. Twenty hunts a month compounds fast — a year of steady hunting yields hundreds of continuously monitored infrastructure clusters.

Frequency: Per hunt, target 3–5 new Collections per week.

3

Automate continuous monitoring

Enable events on each Collection so additions and changes flow to the stack automatically — Slack or Teams for analyst awareness, the TIP for scoring, the SIEM for correlation. The hunt keeps running after the hunter moves on.

Frequency: Once per Collection, review noisy patterns monthly.

SAMPLE — CAMPAIGN PIVOTS IN PLATFORM SEARCH

A pivot runs several moves deep. Each query narrows or expands the set — the payoff is what the expansion exposes.

1 — Seed from ARC threat data, then narrow by geography:

```
(host.services.threats.name = "AsyncRAT" or web.threats.name = "AsyncRAT")
and host.location.country = "China"
```

2 — Pivot on a shared favicon fingerprint (~300 hosts, Internet-wide):

```
host.services.endpoints.http.favicons.hash_sha256 =
  "10dc6e7a6b5a0b86167994767dd0bc652eb04aba06c18d1410d0761da470b00a"
```

3 — Read the cluster for what doesn't fit: one host geolocated to Mountain View, US serves a Chinese-language, food-delivery-themed lure. The favicon says it belongs to the campaign; the geography-versus-content mismatch says it warrants a hard look. Save the query as a Collection and the cluster keeps reporting new members as they appear.

PHASE OUTCOMES

- Spend time hunting, not querying tools
- Find campaign infrastructure in real time
- One IOC to full footprint in minutes

PHASE 4 · DEFEND · DETECTION + SECURITY ENGINEERING

Defend at the campaign level

THE RISK

Blocklists built from static feeds describe where attackers were, not where they are. Adversaries rotate infrastructure faster than feeds refresh, so defenses generate false positives on recycled IPs while live campaign hosts pass clean, and detection engineering spends its time maintaining stale rules instead of writing new ones.

THE STRATEGY

Close the loop from the hunts you built in Phase 3. Every Collection tracking live adversary infrastructure becomes a defensive control: webhooks announce new hosts as they appear, blocklists and detection rules generate from live signatures, and SOAR playbooks act automatically — resulting in blocking at the campaign level.

PHASE 4 · DEFEND · CONTINUED

1

Stand up webhooks for new infrastructure

Attach a webhook to each high-confidence Collection so asset-added and asset-changed events post to the SOAR, SIEM, or messaging channel in real time. Route by severity: C2 clusters to the SOAR, lower-confidence patterns to an analyst review channel.

Frequency: Once per Collection.

2

Generate blocklists & detection rules

Export each Collection's current membership as a live blocklist for the firewall, proxy, and DNS layers, and translate its fingerprints (certificates, JARM/JA4, banners) into SIEM detection rules. Regenerate on Collection change events so rules track the campaign.

Frequency: Automated on change, human review weekly.

3

Automate blocking & response

Wire webhook events into SOAR playbooks that validate, push the indicator to enforcement points, and sweep recent logs for prior contact. A single certificate pivot can surface hundreds of linked hosts — automate the bulk block, keep a human on the approval gate.

Frequency: Continuous, tune approval thresholds monthly.

SAMPLE — COLLECTION WEBHOOK FEEDING THE SOAR

```
# Webhook payload on new asset in a tracked C2 Collection
{ "collection": "campaign-c2-cluster-014",
  "event": "asset.added", "asset": "198.51.100.88",
  "labels": ["c2", "remote-access"], "first_seen": "2026-07-11" }
# SOAR playbook: validate -> block at firewall/proxy/DNS -> retro-hunt logs
```

PHASE OUTCOMES

- Block threats before they reach the perimeter
- Fewer false positives
- Reduced dwell time

OPERATIONALIZE

Connect Censys Across the Stack

Censys is most useful when the intelligence reaches each team where they work, which means picking the right surface for each workflow rather than forcing every team through one interface. Censys connects six ways.

REST API

Current and historical lookups, searches, and aggregations over high-speed REST APIs — the backbone of alert enrichment and runbook automation.

Webhooks

Monitor changes in Internet infrastructure and push notifications to any destination the moment they happen.

Integrations

Native connectors bring Censys intelligence into your SIEMs, SOARs, and TIPs with no custom code.

Web Search Interface

Explore Censys data, experiment with queries, and build investigations in the browser.

CLI / SDKs

Script Censys intelligence into your tooling with the command-line tool and SDKs.

MCP Server

Query the Platform in natural language — secure, fully governed access for AI-assisted workflows.

Native Integrations Across the SOC

SIEM · SOAR · SOC AI — Palo Alto Networks XSIAM · Google SecOps (Chronicle) · Microsoft Sentinel · Cisco Splunk Platform · Palo Alto Networks Cortex XSOAR · Cisco Splunk SOAR · Cyware

Threat Intelligence — Maltego · OpenCTI (Filigran) · Dataminr · ThreatConnect · Vertex Synapse · Securonix · ThreatQuotient

Asset Management (CMDB) — Axonius · ServiceNow

See the full, current list at censys.com/resources/integrations.

FINAL SIGN-OFF

Confirm Censys is live across the stack

Work through this checklist with your team. Every unchecked box is an agenda item for your next Censys CSM session.

Phase 1 · Triage

- [ ] Platform org, roles, and API credentials provisioned; priority alert sources identified
- [ ] Unlimited Enrichment API wired into the SIEM/SOAR; every alert with an external indicator enriched on ingest
- [ ] Live-alert validation complete; analyst view tuned and rolled out to all queues

Phase 2 · Investigate

- [ ] IR team enabled on search, host profiles, and point-in-time historical views
- [ ] At-time lookup step added to every active IR runbook (cross-referenced with logs)
- [ ] Standard pivot workflow documented and in use

Phase 3 · Hunt

- [ ] Hunt register established with seed indicators and fingerprints per campaign family
- [ ] Collections built for priority campaigns and reviewed in weekly hunt planning
- [ ] Continuous monitoring events routed to Slack/Teams, TIP, and SIEM

Phase 4 · Defend

- [ ] Webhooks live on high-confidence Collections, routed by severity
- [ ] Live blocklists and fingerprint-based detection rules regenerating on change events
- [ ] SOAR playbooks blocking and retro-hunting automatically, with approval gates tuned

IMMEDIATE NEXT STEPS

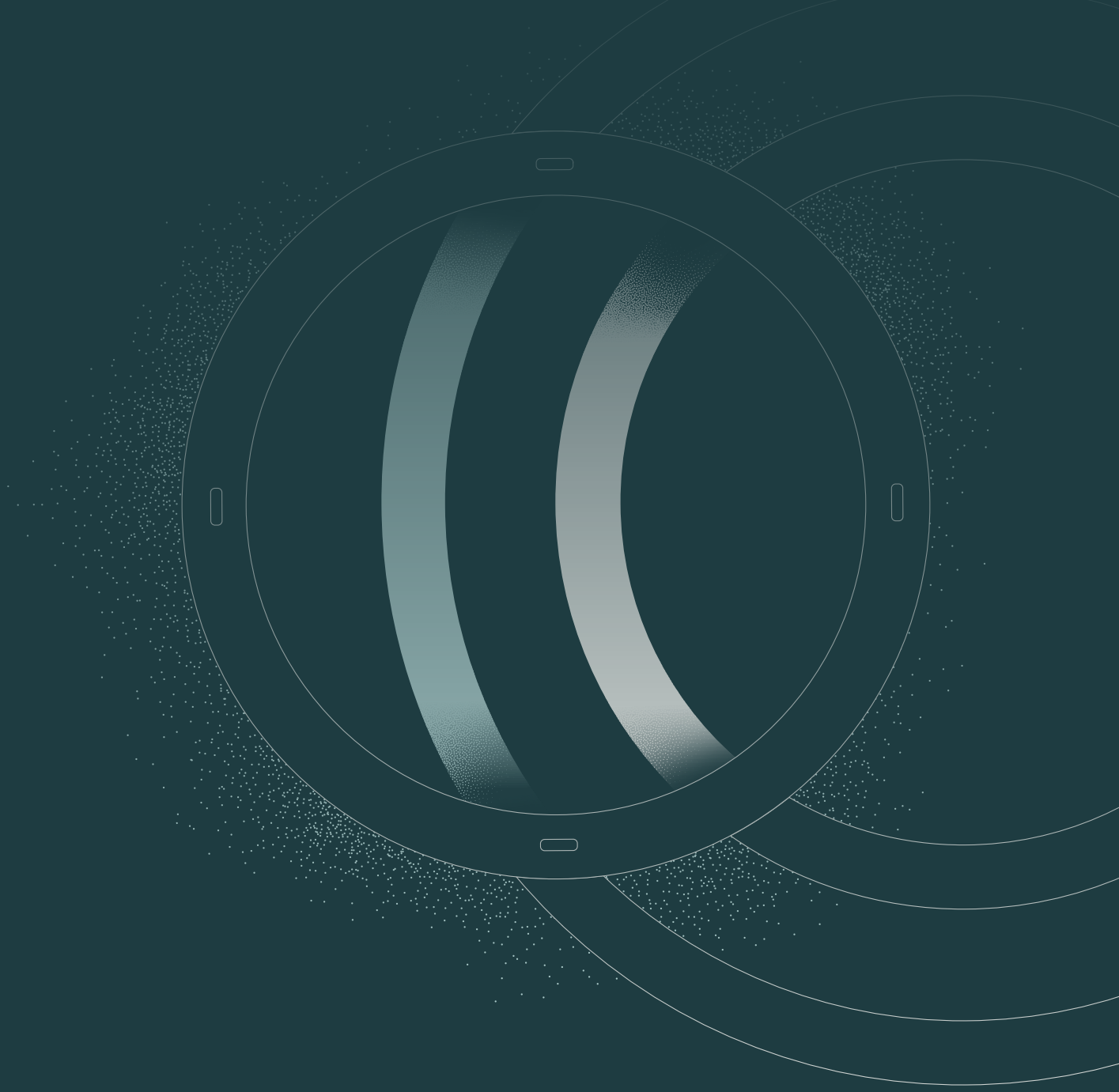
1. Confirm platform access and your priority alert sources
2. Schedule per-phase enablement sessions with each team
3. Align with your CSM on the success metrics you'll measure against

WHERE TO GO FROM HERE

The Foundational Data Layer for Modern Security Operations

Censys maintains the most comprehensive, up-to-date map of the Internet — every host, service, certificate, and domain, continuously scanned and enriched with threat context. Security teams worldwide rely on Censys Internet Intelligence to triage with evidence, investigate with history, hunt at Internet scale, and defend at the campaign level.

Ready to operationalize Censys? Contact your Censys Customer Success Manager to schedule your Phase 1 enablement session, or visit censys.com/integrations to explore connectors for your stack.



censys

Censys is the authority in Internet intelligence and insights. Delivering the most comprehensive, accurate, and up-to-date global map of Internet infrastructure, Censys provides the real-time external visibility organizations need to accelerate security operations, investigate threats, and understand Internet exposure. Global governments, Fortune 500 companies, and security providers trust Censys to uncover risks faster and respond more effectively.

VISIT
censys.com

CONTACT
hello@censys.com