Using Zetat™ — Zero Trust Analyzer Tool

Zetat maps your organization's security posture against the **NSA Zero Trust Implementation Guidelines (ZIG)**, the **DoD Zero Trust Framework**, and **NIST SP 800-207**. It tracks **42 current core capabilities** across 7 pillars and supports multiple phase memberships, phase-specific activities and outcomes, and a separate supplemental OT assessment. Two prior catalog entries are retained for compatibility but excluded from core scores.

Table of Contents

1. Navigating the Interface
2. Step 1 — Configure Your Organization
3. Step 2 — Dashboard Overview
4. Step 3 — Assess Capabilities
5. Step 4 — Gap Analysis
6. Step 5 — Technology Mapping
7. Step 6 — Reports & Exports
8. Step 7 — Snapshots (Progress Over Time)
9. Supplemental Assessments
10. Reference — Current Core Capabilities
11. Environment Variables
12. Production Deployment (AWS)

---

1. Navigating the Interface

The top navigation bar has seven sections:

Tab | Purpose |

|—|—|

Dashboard | Maturity overview, radar chart, phase progress, top gaps |

Capabilities | Current core capability assessment, multi-phase mapping, and activity/outcome tracking |

Gap Analysis | Colour-coded heatmap + prioritised open gap list |

Tech Mapping | Map NSA ZIG technology catalog (117 tools) to capabilities |

Supplemental | OT assessment overlay and retained legacy catalog entries |

Reports | Download HTML, gap, executive, and CSV reports |

About | How Zetat works and framework references |

All navigation is client-side (no page reloads).

---

2. Step 1 — Configure Your Organization

1. Click the **Settings icon** (settings) button in the top-right corner.
2. Enter your **Organization Name** — this appears on all reports.
3. Click **Save**.

Your org name is stored in the database and persists between sessions.

---

3. Step 2 — Dashboard Overview

When you open Zetat you land on the **Dashboard**. It shows:

- **Phase status strip** — Primer / Discovery / Phase One / Phase Two and completion percentages.
- **Four KPI cards** — Overall ZT Maturity %, Capabilities Complete, Open Gaps, Active Pillars (>50%).
- **7 Pillars bar chart** — horizontal maturity bars for each NSA ZIG pillar.
- **Maturity Radar** — pure-SVG spider chart of all 7 pillars overlaid.
- **Phase Progress bars** — Discovery, Phase One, Phase Two completion percentages.
- **High-Priority Gaps** — the first 8 open capabilities sorted by pillar/phase.

All scores update in real time as you save capability assessments.

How maturity is calculated:

```
Pillar %  = (Complete caps in pillar) ÷ (all caps in pillar excluding N/A) × 100

Overall % = (Total Complete caps) ÷ (Total caps excluding N/A) × 100
```

---

4. Step 3 — Assess Capabilities

This is the primary workflow. For each current core capability, record its status and applicable phase-specific activities and expected outcomes.

Opening the Capability Editor

1. Click **Capabilities** in the navigation bar.
2. Optionally filter by **Pillar**, **Phase**, or **Status** using the dropdowns.
3. Click any capability row (or its **Edit Edit** button) to open the edit modal.

Fields to Complete

Field | Options | Guidance |

|—|—|—|

Status | Not Started / In Progress / Complete / N/A | Set to `N/A` for capabilities outside your scope |

Priority | High / Medium / Low / — | Used to rank the gap list |

Owner | Free text (max 120 chars) | Person or team responsible |

Due Date | Date field | Target completion date |

Notes | Free text (max 2000 chars) | Evidence, blockers, or context |

Technologies | Multi-select from NSA ZIG catalog | Link deployed tools to this capability |

4. Add one or more activities within any mapped ZIG phase, and record the expected outcome, status, owner, due date, and evidence.
5. Click **Save** for the capability and **Save Activity** for each activity. Changes persist immediately.

Capability Statuses

Status | Meaning |

|—|—|

`Not Started` | No implementation work begun |

`In Progress` | Partially implemented or in active rollout |

`Complete` | Fully implemented and operational |

`N/A` | Capability not applicable to your environment |

> **Tip:** Work through the three phases in order — **Discovery** capabilities first (inventory, mapping, logging), then **Phase One** (foundational controls), then **Phase Two** (advanced automation and analytics).

---

5. Step 4 — Gap Analysis

Click **Gap Analysis** to see all capabilities that are not yet `Complete` or `N/A`.

Heatmap

- Each cell represents one capability, coloured by status:

- Green **Green** — Complete

- Yellow **Yellow** — In Progress

- Red **Red** — Not Started

- Grey **Grey** — N/A

- Cells are grouped by the **7 pillars** (columns).
- Hover or focus a cell to see a tooltip with the capability name, pillar, phase, and status.
- Click a cell to open the edit modal directly.

Gap List

Below the heatmap, open gaps are listed sorted by pillar and phase. Each row shows:

- Capability ID and name
- Pillar and phase
- Current status
- Priority and owner

Use this list to assign owners and due dates to the highest-priority items.

---

6. Step 5 — Technology Mapping

Click **Tech Mapping** to see the NSA ZIG Technology Catalog — 117 commercial and open-source security tools organised into 7 categories.

Category | Examples |

|—|—|

Identity & Access | Okta, Azure AD/Entra ID, CyberArk PAM |

Device & Endpoint | CrowdStrike Falcon, Microsoft Defender XDR, Tanium |

Network | Palo Alto NGFW, Zscaler ZPA/ZIA, Illumio |

Application | Cloudflare WAF, Snyk, Veracode, Apigee |

Data | Microsoft Purview, Varonis, Forcepoint DLP |

Automation | Splunk SOAR, Open Policy Agent, ServiceNow SecOps |

Visibility | Splunk SIEM, Microsoft Sentinel, Recorded Future |

Mapping a Technology to a Capability

1. In **Tech Mapping**, click a technology name in the left panel.
2. The right panel shows which capabilities it is currently assigned to.
3. To link the technology to a capability, open that capability via **Capabilities** → edit modal → **Technologies** field → select the tool.
4. Save. The Tech Mapping panel updates to show the new assignment.

This lets you answer **"which capabilities does our Okta deployment satisfy?"** and identify tools you are paying for but have not mapped to any ZIG capability.

---

7. Step 6 — Reports & Exports

Click **Reports** to access four export formats.

Report | Button | Format | Contents |

|—|—|—|—|

Full Assessment | **Download Full Report (HTML)** | `.html` | All 42 current core capabilities: ID, name, pillar, phases, status, priority, owner |

Gap Report | **Download Gap Report (HTML)** | `.html` | Only open gaps with notes included |

Executive Summary | **Download Executive Summary (HTML)** | `.html` | KPI cards + per-pillar maturity bars; suitable for leadership briefings |

Raw Data | **Export CSV** | `.csv` | All 42 current core capabilities, including phase memberships, technologies, and notes |

Generating a Report

1. Click the relevant **Download** button.
2. The file downloads immediately — no server-side storage.
3. Open the HTML file in any browser for a formatted view, or import the CSV into Excel / Google Sheets.

---

8. Step 7 — Snapshots (Progress Over Time)

Snapshots capture your overall and per-pillar maturity at a point in time so you can track progress across assessment cycles.

Taking a Snapshot

1. Click the **Snapshot icon Snapshot** button (top right, next to Settings).
2. Enter a label (e.g., `Q2 2026 Baseline`).
3. Click **Save Snapshot**.

Viewing Snapshots

The snapshot list on the Reports page (or via the snapshot modal) shows each saved snapshot with its label, date, and overall maturity score. Use this to compare quarter-over-quarter progress.

> **Tip:** Take a snapshot before and after each major implementation sprint so you have a before/after comparison.

---

9. Supplemental Assessments

The **Supplemental** tab keeps two non-core areas separate from the ZIG maturity score:

- **Operational Technology:** Initial prompts based on NSA's October 8, 2026 OT Zero Trust guidance. They are a planning overlay, not a complete transcription of the CSI. Open the full CSI or NSA's release summary.
- **Retained legacy entries:** `5.5 DNS Security` and `5.6 Encrypted Traffic Inspection` remain available for existing assessments but do not contribute to current core scores.

Source note: NSA's Discovery overview states 14 core capabilities, while its current phase page visibly links 13 capability IDs. Zetat maps the explicitly listed IDs pending clarification. See the NSA ZIG portal and Discovery page.

---

10. Reference — Current Core Capabilities

The Phase column lists every current phase membership for each capability. A capability may appear in more than one phase.

Pillar 1 — User (9 capabilities)

ID | Phase | Capability |

|—|—|—|

1.1 | Discovery | User Inventory |

1.2 | Phase Two | Conditional User Access |

1.3 | Phase One | Multi-Factor Authentication (MFA) |

1.4 | Phase One, Phase Two | Privileged Access Management (PAM) |

1.5 | Phase One, Phase Two | Identity Federation & User Credentialing |

1.6 | Phase Two | Behavioral, Credentialing & Biometrics |

1.7 | Phase One | Least Privilege Access |

1.8 | Phase One, Phase Two | Continuous Authentication |

1.9 | Phase Two | Integrated ICAM Platform |

Pillar 2 — Device (7 capabilities)

ID | Phase | Capability |

|—|—|—|

2.1 | Discovery, Phase One, Phase Two | Device Inventory |

2.2 | Phase Two | Device Detection & Compliance |

2.3 | Discovery, Phase Two | Device Authorization |

2.4 | Phase One, Phase Two | Remote Access |

2.5 | Phase One | Automated Asset, Vulnerability & Patch Management |

2.6 | Phase One, Phase Two | Unified Endpoint Management (UEM) & MDM |

2.7 | Phase One, Phase Two | EDR & XDR |

Pillar 3 — Application & Workload (4 capabilities)

ID | Phase | Capability |

|—|—|—|

3.1 | Discovery | Application Inventory |

3.2 | Phase One, Phase Two | Secure Software Development & Integration |

3.3 | Phase One, Phase Two | Software Risk Management |

3.4 | Phase One, Phase Two | Resource Authorization & Integration |

Pillar 4 — Data (7 capabilities)

ID | Phase | Capability |

|—|—|—|

4.1 | Discovery | Data Analysis |

4.2 | Phase One, Phase Two | Enterprise Data Governance |

4.3 | Phase One, Phase Two | Data Labeling & Tagging |

4.4 | Discovery, Phase One, Phase Two | Data Monitoring & Sensing |

4.5 | Phase One, Phase Two | Data Encryption & Rights Management |

4.6 | Phase One, Phase Two | Data Loss Prevention (DLP) |

4.7 | Phase Two | Data Access Control |

Pillar 5 — Network & Environment (4 current core capabilities)

ID | Phase | Capability |

|—|—|—|

5.1 | Discovery, Phase One | Data Flow Mapping |

5.2 | Discovery, Phase One, Phase Two | Software-Defined Networking (SDN) |

5.3 | Phase One, Phase Two | Macro-Segmentation |

5.4 | Phase One, Phase Two | Micro-Segmentation |

Pillar 6 — Automation & Orchestration (6 capabilities)

ID | Phase | Capability |

|—|—|—|

6.1 | Discovery, Phase One, Phase Two | Policy Decision Point (PDP) & Orchestration |

6.2 | Discovery, Phase Two | Critical Process Automation |

6.3 | Phase Two | Machine Learning (ML) |

6.5 | Discovery, Phase One | SOAR |

6.6 | Discovery, Phase One, Phase Two | API Standardization |

6.7 | Phase One, Phase Two | SOC & Incident Response (IR) |

Pillar 7 — Visibility & Analytics (5 capabilities)

ID | Phase | Capability |

|—|—|—|

7.1 | Discovery, Phase One, Phase Two | Log All Traffic |

7.2 | Phase One, Phase Two | SIEM |

7.3 | Phase One, Phase Two | Common Security & Risk Analytics |

7.4 | Phase Two | User & Entity Behavior Analytics (UEBA) |

7.5 | Phase One, Phase Two | Threat Intelligence Integration |

---

11. Environment Variables

Variable | Default | Description |

|—|—|—|

`SECRET_KEY` | random (auto-generated) | Flask session signing key — **set this in production** |

`DB_PATH` | `zetat_data.db` (next to `app/`) | Absolute path to the database file |

`ORG_NAME` | `My Organization` | Default organisation name (overridden by Settings UI) |

`RECAPTCHA_SITE_KEY` | configured in app | Public reCAPTCHA key used on registration and login |

`RECAPTCHA_SECRET` | configured in app | Server-side reCAPTCHA verification secret |

`RECAPTCHA_ENABLED` | inferred from cookie security | Explicitly enable or disable reCAPTCHA |

---

12. Production Deployment (AWS)

The live site uses an EC2 backend behind the existing Nginx edge at **https://zetatcyber.com**.

- Nginx terminates TLS, redirects HTTP and `www` to the HTTPS apex, and enforces ModSecurity with the OWASP CRS.
- The Flask/Gunicorn container is bound to a private interface only; the edge security group is the only permitted source on its application port.
- SQLite data persists in the `zetatcyber-data` Docker volume. The runtime container uses a read-only root filesystem and dropped Linux capabilities.
- The environment file, including Flask session and reCAPTCHA settings, is root-readable only. Preserve the existing `SECRET_KEY` across deployments so active sessions remain valid.
- Certbot manages the apex/`www` certificate and automatic renewal. Check it with `sudo certbot certificates`; test renewal with `sudo certbot renew --dry-run`.

The Terraform files under `zetat_web/terraform/` describe an alternate ECS/Fargate architecture; they do not describe the current live EC2 deployment.

Basic deployment checks:

```
docker ps --filter name=zetatcyber-app

curl -fsS https://zetatcyber.com/health

sudo nginx -t
```

```
sudo certbot renew --dry-run
```

Keep the backend port private. Do not publish it to `0.0.0.0/0`.

Zetat™ v1.0 — Antibody Cyber Technology, LLC · Aligned with NSA ZIG · DoD ZT Framework · NIST SP 800-207