# CYPHERNULLBYTE

## Security & Compliance Services

Fractional CISO leadership, offensive security, DevSecOps, incident response and security training, for teams that need real ownership of security, not just a slide deck of advice.

*Practitioner-led. Hands-on. Framework-agnostic.*

*Service overview: no pricing included, scoped per engagement.*

WHO WE ARE

# Security, run the way an in-house owner would run it

CypherNullByte is a practitioner-led security and compliance practice. Engagements are led personally by a senior security consultant, not handed off to a rotating account team, with vetted specialists brought in only when a specific engagement genuinely needs extra hands.

The working model is the same across every service line: find the real problem, hand over the exact fix, and stay accountable until it's actually closed out. Not a report that gets filed away, and not open-ended advice with no one on the hook for the outcome.

## What that looks like in practice

- Took an AI workflow orchestration platform through ISO 27001:2022 certification end to end, and is now building out ISO 42001:2022 AI governance on top of that same foundation.
- Ran enterprise vulnerability management across 20+ accounts and thousands of servers, containers and cloud workloads, including post-M&A environments, with zero critical SLA breaches.
- Re-engineered a national, SkillsFuture-funded cybersecurity training programme end to end: cut dropout from roughly 60% to 10%, lifted pass rates by around 20%, and built a train-the-trainer framework that kept 10+ facilitators delivering consistently across 10+ cohorts.
- Built automated threat-hunting and triage workflows that removed the need for an expensive third-party managed threat-hunting contract.

## Who this is for

AI-native and cloud-first startups facing their first enterprise security questionnaire or certification requirement, scale-ups that have outgrown ad-hoc security but aren't ready for a full-time CISO, and organizations that need a specific, bounded piece of work done properly: a penetration test, an incident investigated, a team trained.

CORE OFFERING

# Two ways to engage a vCISO

Every relationship starts with a short discovery conversation to find out which model actually fits, not a pitch for whichever is easier to sell. Both run on the same principle: advisory guidance is always included, your own team implements, and you stay the one accountable point of contact for the outcome.

### 1. Certification-Track vCISO: the 48-Day Path

*For teams with a live compliance deadline*

**Best fit:** A customer, prospect or partner has asked for SOC 2, ISO 27001, or a completed security questionnaire, and there's a real deadline attached.

- Phase 1, Readiness (diagnostic): ISMS scope definition, a full gap assessment against ISO 27001:2022 Annex A, an initial risk register, a draft Statement of Applicability, and a remediation roadmap that becomes the Phase 2 plan.
- Phase 2, Build: the full policy set, a finalized Statement of Applicability, and an independently coordinated internal audit, with control work across people & organizational security, physical security, application security, cloud & infrastructure, network security, and backup/business continuity, all mapped directly to ISO 27001:2022.
- Always-On vCISO (ongoing, can start alongside the build): continuous drift monitoring with a monthly report, unlimited security-questionnaire support for the sales team, first-call incident response, and guided implementation support, plus first right of refusal on whatever comes next (ISO 42001, SOC 2, or any other framework).

### 2. vCISO Foundations: ongoing ownership, no audit required

*For teams that aren't chasing a certification yet*

**Best fit:** There's no certification deadline, but leadership wants a real, accountable owner for security instead of it being nobody's job.

- Foundational setup: identity & access, encryption, logging, backup, and baseline hardening, so there's an actual foundation in place from day one.
- Continuous vulnerability management: not a one-off scan, a living, triaged list that gets tracked to closure.
- Ongoing cloud security (AWS/GCP/Azure) and network security review, folded into the standing relationship rather than billed as separate add-ons.
- A standing point of contact for anything security-related, including first-call incident response and the same guided-implementation model as the certification track.
- A natural on-ramp: if certification becomes a requirement later, the foundational work already done here shrinks the scope of that transition significantly.

*No pricing shown by design. Every engagement is scoped to the client's actual size, stack, and starting point before a number is discussed.*

FULL SERVICE MENU

# Beyond the vCISO retainer

Every service below is also available as its own scoped, standalone engagement, not everyone starting out needs a full retainer. This is the working menu of what's realistically offered across the security lifecycle.

## 1. Governance, Risk & Compliance

- **ISO 27001:2022 certification readiness:** full ISMS build, Annex A gap mapping, Statement of Applicability, internal audit coordination.
- **SOC 2 (Type I & II) readiness:** control design and the operating-evidence window Type II requires.
- **Privacy & data protection alignment:** GDPR and HIPAA gap assessment and control mapping (legal review and DPA drafting stay with your counsel).
- **Risk assessment & risk register management:** methodology, scoring, and an actively maintained register, not a one-time spreadsheet.
- **Policy & procedure development:** written to match how the organization actually operates, not copy-pasted templates.
- **Third-party / vendor risk assessments (TPRM):** running your vendor questionnaires, or standing in the vendor's seat to answer a customer's TPRM questionnaire and produce the evidence behind it.
- **Internal audit coordination:** sourcing and managing an independent auditor to keep certification-audit independence clean.

## 2. AI Security & Governance

- **ISO 42001:2022 AI management system design:** for teams shipping AI features or using AI in regulated workflows.
- **AI governance and AI-risk awareness training:** tied into ISO 42001 work where relevant.
- **Practical, model-agnostic AI-tool usage guidance:** the discipline isn't which AI you use, it's how your people use it, verify its output, and stay accountable for it. Humans remain the end controllers.
- **Standalone or bundled:** fits naturally alongside ISO 27001 / SOC 2 work, or stands alone as its own scoped engagement.

## 3. Offensive Security / VAPT

- External and internal network penetration testing
- Web application and API penetration testing
- Cloud environment penetration testing and configuration review
- Point-in-time and ongoing vulnerability assessments
- Remediation verification and re-testing, so findings actually get closed, not just logged

## 4. Application Security & DevSecOps

- Secure SDLC design and threat modeling for new features and high-risk workflows
- SAST, DAST and SCA integration into the existing development workflow
- CI/CD pipeline security automation and container/Kubernetes controls
- Secrets management architecture (e.g., HashiCorp Vault) across cloud and on-prem, including CI/CD integration
- Infrastructure-as-code review and cloud security posture management

## 5. Cloud & Network Security

- Cloud security architecture and hardening across AWS, GCP and Azure
- Network segmentation, firewall and access-control review
- Zero-trust and secure remote-access design
- Backup, disaster recovery and business continuity design, including restore validation and runbooks

## 6. Security Operations & Vulnerability Management

- Vulnerability management programme design and day-to-day operation (VMDR lifecycle)
- SOC advisory: detection engineering guidance and MITRE ATT&CK-aligned monitoring
- Threat hunting and triage workflow design
- Executive risk dashboards and board-ready reporting on posture, remediation and incident trends

## 7. Incident Response & Investigations

- Incident response readiness: runbooks, playbooks and tabletop exercises
- First-call triage and containment coordination
- Breach and incident investigation support
- Digital forensics support and evidence handling
- Post-incident review and lessons-learned facilitation

## 8. Training & Enablement

- Security awareness training for all-staff audiences, built around how the organization actually works
- Technical curriculum design and delivery: network security, ethical hacking, digital forensics, security monitoring, and applied AI-in-security
- Train-the-trainer programmes to scale delivery across multiple facilitators without losing consistency

GETTING STARTED

# How an engagement begins

Every new conversation starts the same way: a short discovery discussion to understand the actual situation, a live deal blocked on a security ask, a desire for real ownership with no deadline attached, or a single bounded need like a penetration test, an incident, or a training session.

## From there

- A live deadline (customer, prospect or auditor asking for something specific) routes toward the Certification-Track vCISO.
- No deadline, but a need for standing ownership, routes toward vCISO Foundations.
- A single, bounded need (a pentest, an investigation, a training session, a policy set) is scoped and quoted as its own engagement. No retainer required to get started.

## What every engagement includes, regardless of size

- Advisory is always included: the problem is found, the exact fix is written, your team implements it.
- A single accountable owner, not a rotating team, from discovery through delivery.
- No vendor lock-in: recommendations stay framework- and platform-agnostic.

---

**CYPHERNULLBYTE**

Security & Compliance Services

contact@cyphernullbyte.com
+91 6396701030, WhatsApp (Text only)