Pentest Readiness Checklist

Bytium LLC

1. Scope & Objectives

- Define in-scope assets: apps, APIs, environments, IP ranges, cloud accounts, physical sites.
- Document testing goals: vulnerability discovery, compliance verification, exploit
- validation, or full adversary simulation.

2. Legal & Approvals

- Written authorization letter with explicit scope and testing window.
- Point of contact list, escalation tree, and on-call availability.
- Third-party hosting approvals (e.g., cloud, CDN, WAF vendors) if required.

3. Environment & Change Freeze

- Production vs. staging: confirm which is to be tested and data sensitivity.
- Change freeze or change-communication plan during the test window.
- Backups and rollbacks confirmed for critical systems.

4. Access & Test Data

- Test accounts per role (user, admin, support, API keys) and MFA expectations.
- Masked or synthetic data for non-prod; data minimization guidance for prod.
- VPN/allowlisting details, jumpbox info, or bastion access if applicable.

5. Applications & APIs

- Base URLs, versions, mobile app build/link, API specs (OpenAPI/Swagger) if available.
- List of critical user journeys: auth, payments, file upload, admin flows.
- Known hardening: WAF rules, rate limits, bot defenses, anti-automation.

6. Infrastructure & Network

- Public IP ranges, domains, subdomains, and known third-party services.
- Internal ranges and access method for internal testing.
- AD/SSO details, network segmentation, crown-jewel systems.

7. Cloud Accounts

- Cloud provider(s), account IDs, org structure, and landing zones.

- IAM approach: roles, least privilege, break-glass accounts, access keys usage.
- Security tooling: Config rules, GuardDuty/Defender/SCC, logging sinks.

8. Compliance & Data Handling

- Regulatory context (PCI DSS, HIPAA, GDPR, ISO 27001) and data residency.
- Evidence retention policy, handling of credentials/tokens, and report classification.
- Vulnerability disclosure policy and SLAs for remediation.

9. Logging, Monitoring & Safety

- SIEM/EDR/IDS in place; notify SOC to avoid false incident escalation.
- List detections you want validated (e.g., auth brute force, SSRF, exfil).
- Safety constraints: DoS limits, social-engineering rules, phishing approvals.

10. During the Engagement

- Slack/Teams channel for daily updates and real-time questions.
- Daily or midpoint sync to review preliminary findings and adjust scope.
- Secure evidence handoff (encrypted archive or shared vault).

11. Reporting & Retesting

- Report format expectations: executive summary + technical details + repro steps.
- Severity model (CVSS or custom) and business impact mapping.
- Retest window and criteria; fixes tracked with IDs/links.

12. Aftercare

- Knowledge transfer session for engineers and leadership.
- Optional hardening backlog and roadmap recom
