ShadowMap Reconnaissance Technical Report

Version 1.0 — September 2025

SHADOWMAP

Prepared by: Mohammad Abir Abbas aka uknowwho

Confidential – For Internal Security Review Only

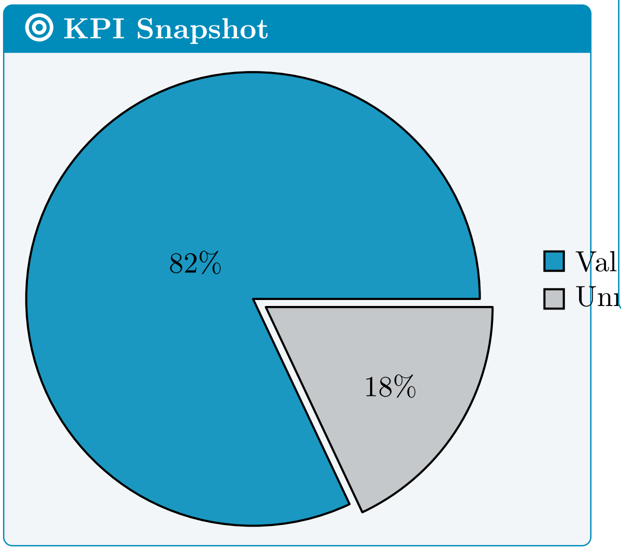
🕒 *Generated on: October 11, 2025*

Executive Dashboard

Discovery Overview

Total Subdomains: 118
Validated (Live): 97
Validation Rate: 82%
CORS Issues: 10
Takeover Flags: 1
Unique Open Ports: 2

KPI Snapshot



Exposure Summary

✗ Atlassian takeover surface identified
! 9 CORS issues on *bkash.com*
✓ *bybit.eu* footprint hardened
Repeatability verified across runs

Governance Actions

- DNS takeover remediation sprint scheduled.
- CORS policy automation to be enforced in CI/CD.
- Integration with CMDB and observability stack planned.

Figure 1. Executive Summary Dashboard – Reconnaissance KPIs, Sept 2025

Executive Summary

ShadowMap executed six reconnaissance runs (7–10 Sept 2025), identifying 118 subdomains and validating 82% as live. Detected issues include one potential Atlassian takeover surface and recurring CORS misconfigurations on *bkash.com* and *canva.com*. Bybit's infrastructure showed minimal exposure with two open ports requiring fingerprinting.

Objectives

- Quantify reconnaissance coverage and service validation accuracy.
- Highlight exploitable surfaces for rapid remediation.
- Provide governance-aligned KPIs for risk reduction.

Methodology

1. Discovery Orchestration

ShadowMap aggregates certificates, normalizes domains, and deduplicates sources.

2. Validation and Enrichment

Assets undergo DNS resolution, TLS fingerprinting, and heuristic takeover detection.

3. Output Management

Structured exports (CSV, JSON, TXT) feed downstream analytics.

4. Security Posture Alignment

Findings are mapped to enterprise governance and compliance guidance.

Data Overview

Table 1: *

Reconnaissance Summary 2ShadowLightwhite

Target (UTC Run)	**Discovered**	**Validated**	**CORS**	**Takeover**	**Open Ports**
atlassian.net (2025-09-07)	6	5	0	1	0
bkash.com (2025-09-07)	42	33	5	0	0
bkash.com (2025-09-08)	44	34	4	0	0
bybit.eu (2025-09-10)	1	1	0	0	2
canva.com (2025-09-08)	24	23	1	0	0
example.com (2025-09-07)	1	1	0	0	0
Totals	118	97	10	1	2

Key Findings

- **Atlassian Takeover Risk:** DNS ownership validation pending.
- **CORS Misconfigurations:** Recurrent across payment-related domains.
- **Bybit Exposure:** Two open ports, no CORS or takeover flags.
- **Operational Stability:** Repeat runs demonstrate consistency.

Recommendations

1. Coordinate DNS and certificate remediation via governance sponsors.
2. Enforce automated CORS testing in CI/CD aligned with the Data Security Strategy.
3. Integrate validated inventories into CMDB and observability pipelines.
4. Automate SBOM-based recon scans for continuous visibility.

Appendix A — Compliance Mapping

⚖ Framework Alignment

Framework Control	ShadowMap Correlation
NIST CSF PR.AC-1	Reconnaissance ensures access control hygiene by validating live subdomain exposure.
ISO 27001 A.12.6.1	CORS findings inform application-level security hardening.
CIS Control 1.4	Asset discovery automation supports continuous inventory management.
NIST CSF DE.CM-8	Network monitoring extended via open port intelligence from ShadowMap.
ISO 27002 8.1.1	Governance recommendations map to asset ownership and tracking.

Observations

This compliance mapping ensures that ShadowMap's outputs directly contribute to enterprise cyber governance, enabling audit traceability and proactive risk management.

Appendix B — Version Control & Repository Link

Repository: https://github.com/ShadowMapOrg/recon-reports

QR code embeds the latest version tag for version-controlled verification.