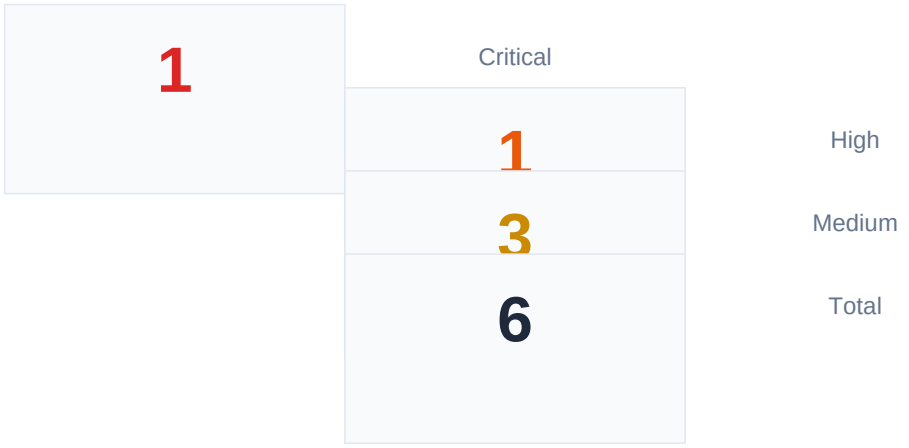
THREAT INTELLIGENCE REPORT

Demo Corp (Sample) | Report ID: demo_20260927 | September 27, 2026

THREAT LEVEL: CRITICAL

Executive Summary



Detailed Findings

[CRITICAL] Leaked .env file with database credentials on GitHub

Source: github | URL: https://github.com/example/repo/blob/main/config.env

A public GitHub repository contains a .env file with what appears to be database credentials and API keys associated with the client domain. The repository appears to be a development fork that was ma

[HIGH] Credential dump on Pastebin mentions client domain

Source: paste_site | URL: https://pastebin.com/abc12345

A paste on pastebin.com contains what appears to be a list of email addresses and password hashes. Several entries use the democorp.example domain, suggesting a potential credential leak from the orga

[MEDIUM] Discussion on r/cybersecurity about Demo Corp security practices

Source: reddit | URL: https://reddit.com/r/cybersecurity/comments/example

A thread on r/cybersecurity discusses Demo Corp's recent security practices. The thread includes some criticism of their incident response time and mentions potential vulnerabilities in their web infr

[MEDIUM] New SSL certificate issued for api.democorp.example

Source: certificate_transparency | URL: https://crt.sh/?q=democorp.example

A new SSL certificate was issued for api.democorp.example via Let's Encrypt. This may be legitimate but should be verified as no corresponding deployment was announced.

[LOW] John Demo mentioned in netsec thread about executive credentials

Source: reddit | URL: https://reddit.com/r/netsec/comments/example2

A post on r/netsec mentions executive John Demo in the context of a broader discussion about credential reuse among C-suite executives. No direct credential leak identified, but the mention creates re

[MEDIUM] New subdomain detected: dev-democorp.example

Source: domain_monitor | URL: DNS: democorp.example

A new DNS record was detected for dev-democorp.example. This subdomain was not previously registered and resolves to an external IP address. Possible subdomain takeover risk.