The Secure Offboarding Checklist: Non-Negotiable Actions

Secure Offboarding: What Every Employee Departure Says About Your Cyber Maturity

Whaller

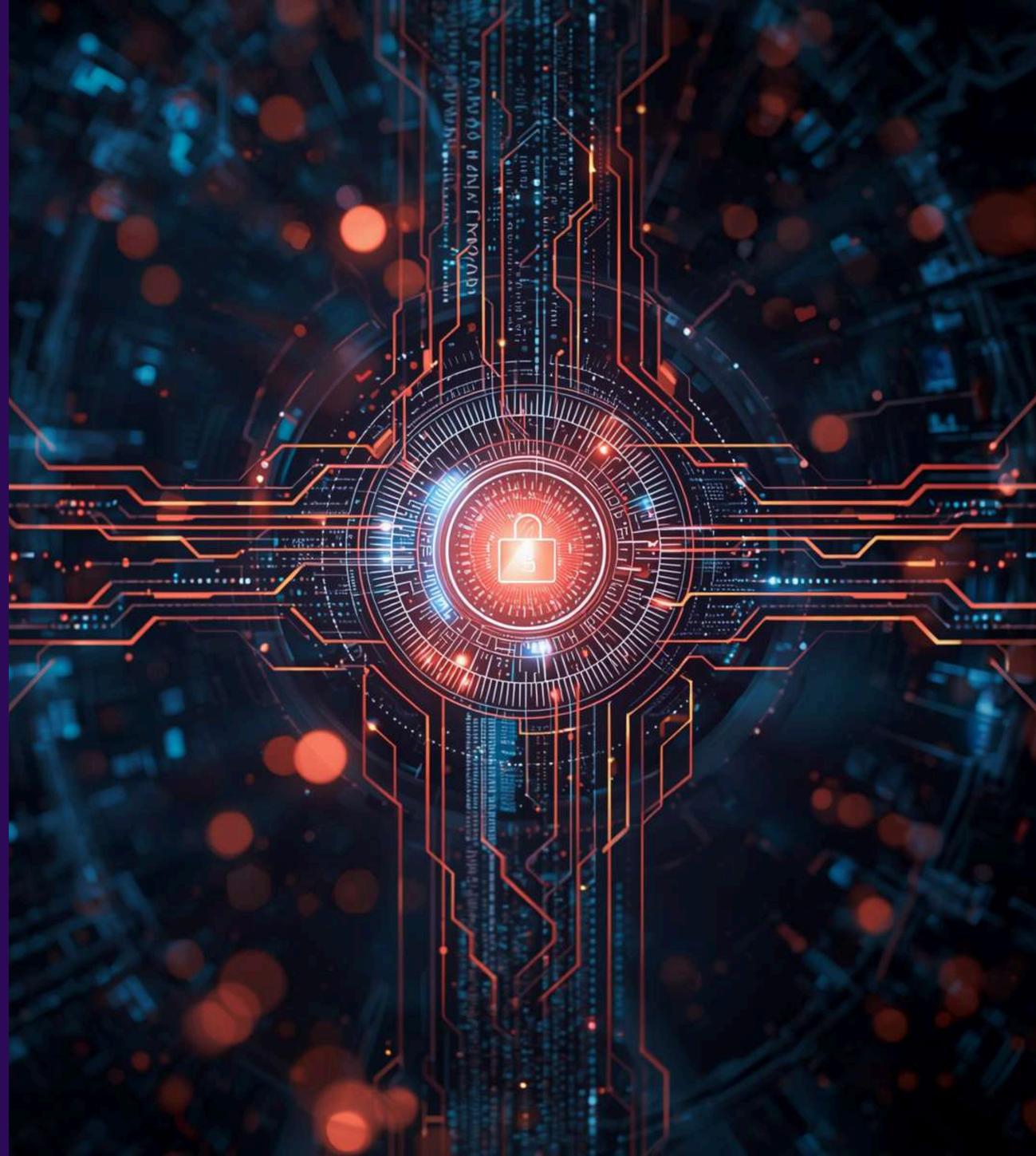
Physical Access

- Recover the building access badge on or before the last day — no exceptions
- Disable alarm codes and any biometric access linked to the employee
- Recover physical keys, car park passes and hardware tokens
- Recover all professional equipment: laptop, smartphone, tablet, removable storage media

Whaller

Information System Access

- Disable the Active Directory / LDAP account immediately — before the notice period ends if the employee has left the premises
- Revoke all VPN credentials and remote connections
- Disable the professional email account set up a time-limited forwarding rule if continuity requires it
- Remove or deactivate accounts on all SaaS tools: CRM, ERP, project management, collaborative platforms…
- Revoke access to shared storage: file servers, drives, document repositories
- Remove source code repository access if the employee was a developer
- Revoke API tokens and any programmatic access credentials generated by the employee



Whaller

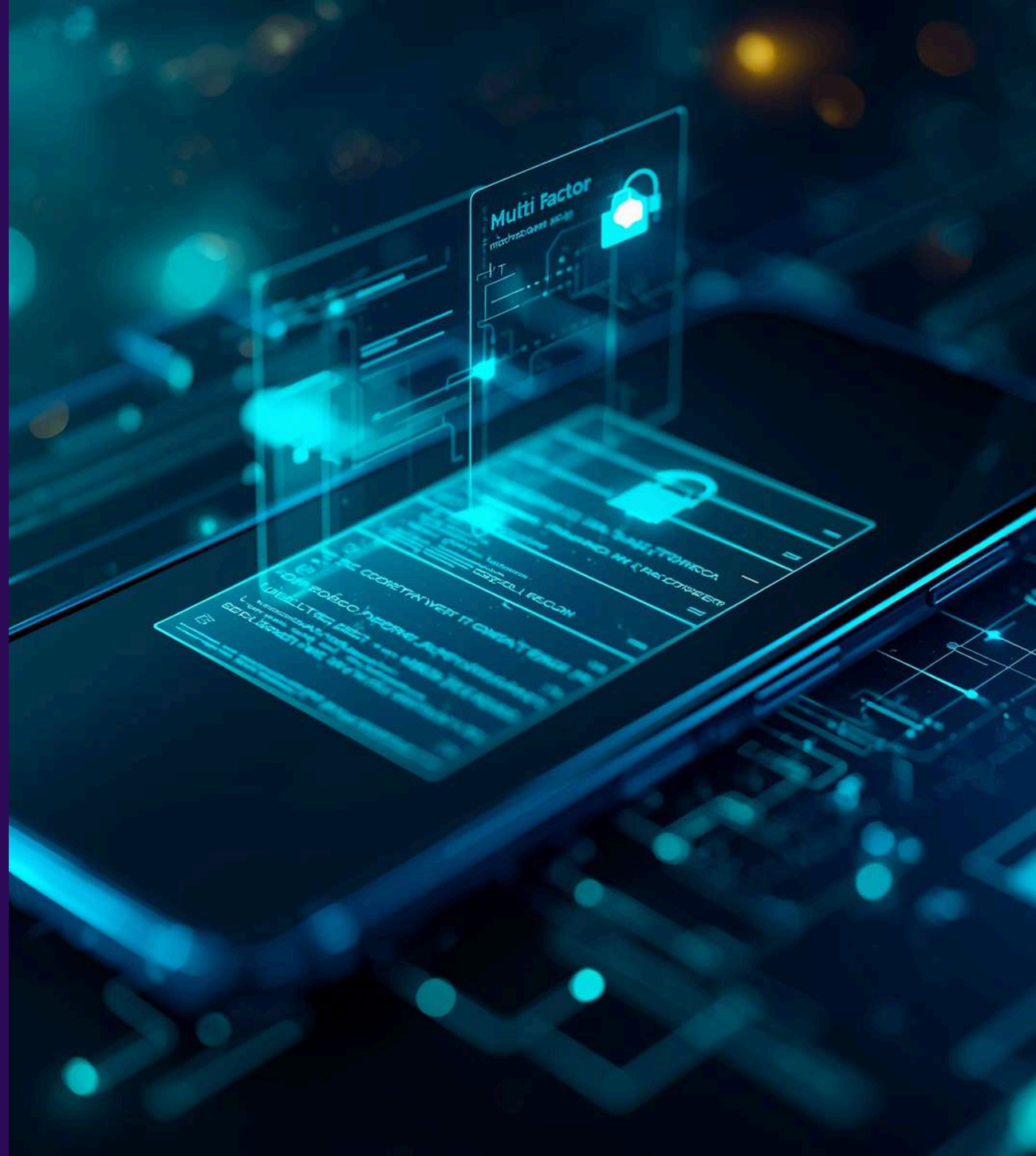
Shared Passwords & Secrets

- Identify every application accessed with shared credentials (generic inboxes, company social media, shared supplier logins…)
- Systematically rotate all shared passwords without exception
- Revoke access to team password managers if the employee had access
- Change Wi-Fi network passwords if access credentials were shared with the employee

Whaller

Multi-Factor Authentication (MFA)

- Deactivate authenticator apps linked to the employee's professional accounts (Google Authenticator, Microsoft Authenticator…)
- Revoke personal phone numbers registered as a second factor on professional applications
- Regenerate MFA backup codes on all sensitive accounts that were accessible to the departing employee



Whaller

Privileged Accounts: Special Vigilance Required

- Revoke administrator rights before the employee's physical departure — not after
- Transfer privileges and responsibilities to another authorised individual
- Change service account passwords managed by the departing employee
- Audit actions on critical systems carried out in the days leading up to the departure

Whaller

After the Departure: Monitor, Audit, Document

- Monitor connection attempts using the former employee's credentials
- Set alerts on any suspicious activity linked to recently deactivated accounts
- Verify that temporary email forwarding rules have not been redirected to an unauthorised external address
- Carry out a full audit across all systems to confirm no residual access has been overlooked

Whaller

Whaller

PÔLE D'EXCELLENCE CYBER

Email: contact@whaller.com Tel: +33 1 47 92 82 18 Website: whaller.com/fr