Identity Security Maturity Model

Delinea

	PHASE 0: HIGH RISK	PHASE 1: FOUNDATIONAL Get visibility & reduce attack surface	PHASE 2: ENHANCED Integrate policies & limit overprivileged users	PHASE 3: ADAPTIVE Increase automation & intelligence
GRC **Governance, Risk and Compliance**	→ No centralized inventory of assets → No easy way to report on user access permissions and privileges → Manual employee onboarding, changes and termination → No automatic disabling of accounts → Manual provisioning of applications	→ Establish roles and access rules along with a control library with mitigating controls (IGA) → Establish an accurate inventory of privileged accounts and their credentials. (Vault, ITDR) → Detect account take over (ATO) threats and send to SOC (ITDR) → Identity Lifecycle Management for all users and named privileged accounts (IGA)	→ Cross-app risk monitoring for critical business apps (IGA) → Implement real-time session monitoring & security access control policies for endpoints. → Enforce host-based session, file, & process auditing → Integration with ITSM for change control approvals → Automate Identity Lifecycle Management for core business applications (IGA) → Access request workflows enhanced with risk analytics (IGA) → Access Review Certificate Campaigns (IGA) → Self-service personal profile management (IGA)	→ Integration with IGA for attestation reporting and risk-based approvals. → Automate Identity Lifecycle Management for all users and business applications (IGA) → Leverage audit data, ML analytics, and automation to detect, track & alert to any threats (ITDR, Integrate with SIEM). → Implement service account discovery, provisioning, and governance across identity and cloud service providers. → Audit critical business apps for sensitive config and data changes and all access grants (IGA) → Automate identity, access and risk reporting with review and signoff (IGA) → Automate attack response (ITDR) → Enhance SOC productivity with Identity Threat information (ITDR)
PA **Privileged Administration**	→ No PAM vault – Secrets manually managed, may be on spreadsheets → Admins access using local admin accounts. → Users may be admins of their own workstations. → Workstation security cannot be trusted. → May be using domain admin for Windows Servers. → May be managing local accounts on each UNIX/Linux system.	→ Discover, vault & automate periodic rotation for all administration and shadow admins accounts. (Vault, ITDR) → Establish a secure admin environment for both local & remote sessions. (RAS) → Establish initial privileged access workflows (IGA, ITSM)	→ Discover, classify, & manage local accounts, groups, roles, & security config files that might grant privileges across all assets. → Discover non-admin privileged access (ITDR) → Establish basic privilege elevation policies for all. → Establish just-in-time, just-enough privileges (IGA, ITSM) → Expand remote access control to vendors & contractors without creating AD accounts. → Enforce basic least privilege for apps (CIEM, IGA)	→ Establish more granular least privilege policies. (PAM, CIEM) → Automate onboarding of new managed assets. → Fix deep posture and privilege escalation paths (ITDR)
IAM **Identity and Access Management**	→ No centralized access controls. → Near impossible to tell who has access and what privileges they have. → Identity management may not be centralized.	→ Enforce MFA for access to Vault, including secrets check out and remote session initiation. → Establish named privileged accounts to prevent using public identities (IGA) → Discover and remediate identity posture issues (ITDR)	→ Clean up stale accounts and unused admins (ITDR) → Enforce MFA at endpoints for direct log-in and privilege elevation. → Eliminate local accounts via identity consolidation for UNIX and Linux Servers. → Remove hardcoded credentials and config data from applications and scripts. → Automate privilege security in DevOps workflows and tooling.	→ Increase MFA from NIST Authenticator Assurance Level (AAL) 1 to NIST AAL2. → Enhance conditional access with risk scoring for identities and targets (ITDR, IGA) → Restrict privileged access to only registered and company-owned endpoints. → Prohibit privileged access by any client system that is not known, authenticated, properly secured, and trusted. → Require dual authorization for privileged operations on critical or sensitive systems.