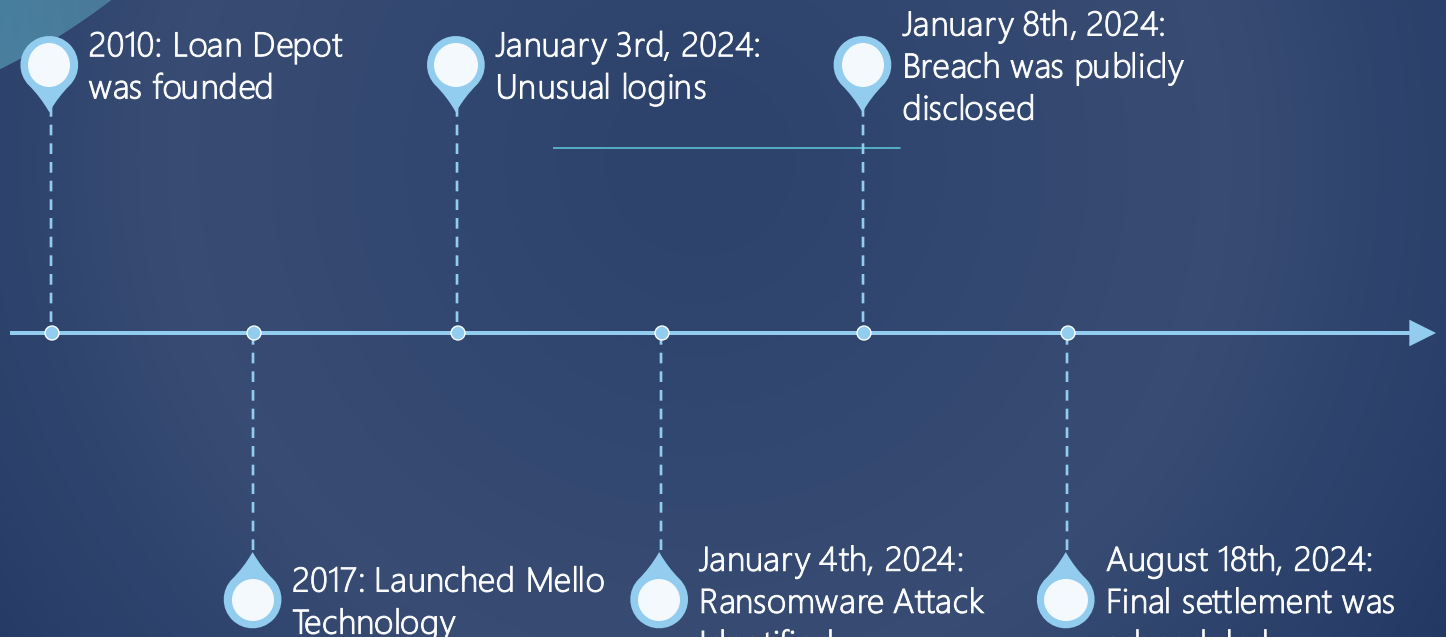
LOAN DEPOT RESPONSE PLAN

Team 6

Aydan Paul, Emma Lewis, TJ Field, Toshan Misir

LOAN DEPOT BACKGROUND AND BREACH



GOVERNANCE

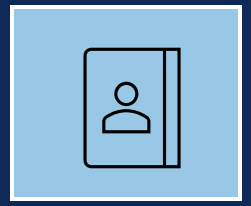
GV.OC

- Business-driven cybersecurity strategy

GV.RM

- Aligns NIST 2.0 framework with regulatory standards
- Quarterly risk assessments
- Adding cyber insurance

GV.RR

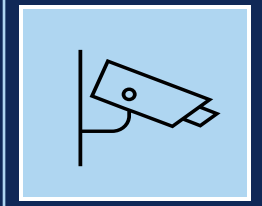


- CISO reports to teams depending of breach size.
- Integrating CRO responsibilities
- Coordinated incident response

GV.PO

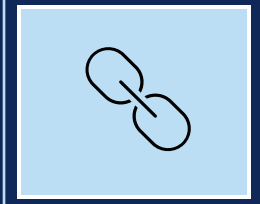
- Enforcing control standards
- Semi-annual audits
- Policies mapped to all key regulations

GV.OV



- Continuous monitoring
- Audits and breach simulations
- Reviewed by executives and board

GV.SC



- conduct annual audits and penetration testing
- Certifications and 24-hour breach notification

IDENTIFYING IMPACT

How Are Incidents Identified?




Internal Detection	Vendor Notification	Customer Reports	External Disclosure

Impact Levels:

HIGH (SEVERE) IMPACT	MEDIUM IMPACT	LOW (MINOR) IMPACT
Ex: Ransomware, BEC, Vendor Breach, Payment Compromise Response: CISO, Cybersecurity & Oversight Committee, IT Security, Legal	Ex: API Exploit, Cloud Exposure, Insider Misuse, Loan Fraud Response: IT Security, CISO Notified	Ex: DDoS, Policy Violation Response: IT Security Teams

DETECTION

We recommend implementing:

Protect and retain public data;

Identify risks

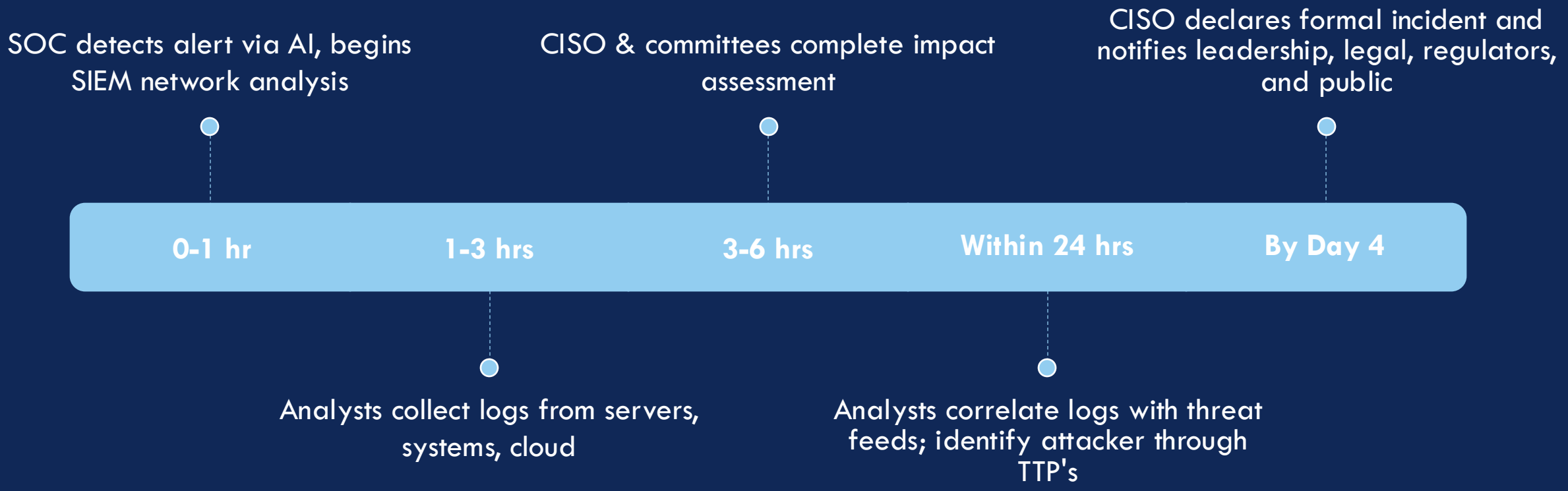
AI real time monitoring to pinpoint root causes

CISO-led cybersecurity oversight committee

Annual cybersecurity training

Vendor data-use agreements required

RESPONSE PACE



PROTECT

Identity & Access: Centralized accounts, MFA for all, least-privilege, and time-limited admin access.

Awareness & Training: Ongoing cyber training and phishing simulations, with tracked completion.

Data Security: Classify GLBA data, encrypt at rest/in transit, DLP, masked test data, and immutable backups.

Platform Security: Hardened systems, regular patching, EDR, WAF/API protection, and segmented networks.

Infrastructure Resilience: Geo-separated backups, highly available core services, and tested recovery plans.

RESPONSE

Incident Management	Incident Analysis	Communication	Mitigation
• Activate CIRT • Isolate affected systems • Engage DFIR • Notify leadership	• Identify attack vectors • Privilege escalation • Impacted systems and exposed PII & SPII	• Provide internal updates • Prepare SEC 8-K and state/federal	• Rebuild from clean baseline • Rotate credetials • Enforce MFA • Patch vulnerabilities

RECOVERY

Recovery Plan Execution

- Restore systems in phases aligned with business continuity
- Validate integrity using hashing/log analysis

Recovery Communication

- Deliver final forensic report to execs/board
- Share recovery updates with customers

SOURCES

- Center for Security and Privacy Controls. (n.d.). *ID.RA-10 – Critical suppliers are assessed prior to acquisition (NIST Cybersecurity Framework v2.0).* CSF.Tools. https://csf.tools/reference/nist-cybersecurity-framework/v2-0/id/id-ra/id-ra-10/
- Dynatrace. (n.d.). *loanDepot customer story.* Dynatrace. https://www.dynatrace.com/customers/loandepot/
- International Journal of Innovative Science and Research Technology. (2025, April). *Cybersecurity GRC framework analysis report [PDF].* IJISRT. https://ijisrt.com/assets/upload/files/IJISRT25APR1107.pdf
- Jewish Federations of North America. (n.d.). *Cyber-security incident response template.* https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf
- loanDepot, Inc. (n.d.). *Privacy policy.* loanDepot, Inc. https://www.loandepot.com/privacypolicy
- loanDepot, Inc. (2025, March 13). *Form 10-K: Cybersecurity GRC – Board Cybersecurity.* loanDepot, Inc. https://www.loandepot.com/
- Red Canary. (n.d.). *Incident response and readiness guide.* https://resource.redcanary.com/rs/003-YRU-314/images/IncidentResponse-and-Readiness-Guide__RedCanary.pdf

THANK YOU