Lemonade

CYBERSECURITY PROGRAM

A 3-YEAR PLAN

-- Priyadharshni Aruchami

Team 45

OBJECTIVE & PROGRAM GOALS

Present an overview of the cybersecurity program’s primary goals: securing customer data, ensuring regulatory compliance, and mitigating evolving threats.

Compliance with Regulatory Standards

Miitigate Risks

Secure Infrastructure

RISK ASSESSMENT & MITIGATION PLAN

Risk Area	Impact Level	Mitigation Strategy
Personally Identifiable Information (PII) Exposure	HIGH	Implement Data Encryption and access control
Phishing attacks	MEDIUM	Conduct regular security awareness training
Legacy Systems	HIGH	Move to cloud-based solutions to benefit from modern security measures, scalability, and vendor support
Third-party vendors	MEDIUM	Implement a vendor risk management program
Ransome Attacks	HIGH	Develop and Test an Incident Response plan

SECURITY PLAN PROPOSAL

MFA

Secure authentication methods to prevent unauthorized access

SOC2 Compliance

Compliance with SOC2 standards to ensure data integrity

AI Data Protection

AI-driven monitoring to protect customer PII

Legacy System Updates

Modernize legacy systems to reduce vulnerabilities

Continuous Training

Employee education on latest security protocols

Incident Response

Real-time threat detection and response

SSDLC

01. REQUIREMENTS

Clearly document security needs and expectations for the software from the beginning

02. DESIGN

Design system architecture with security in mind, considering data flows, network topology, and system boundaries

03. DEVELOPMENT

Following secure coding guidelines and treating security as a crucial aspect of code quality during coding and code reviews

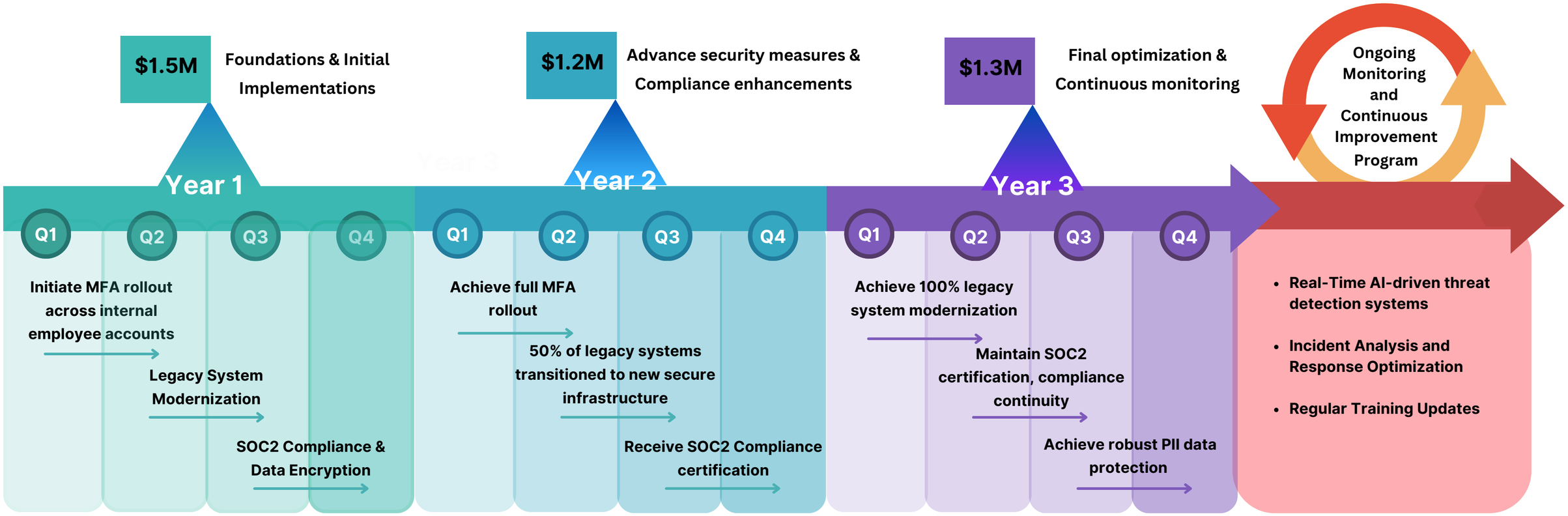
04. TESTING

Perform security testing, including static, dynamic, and interactive testing. Conduct penetration testing and vulnerability assessments to find potential issues.

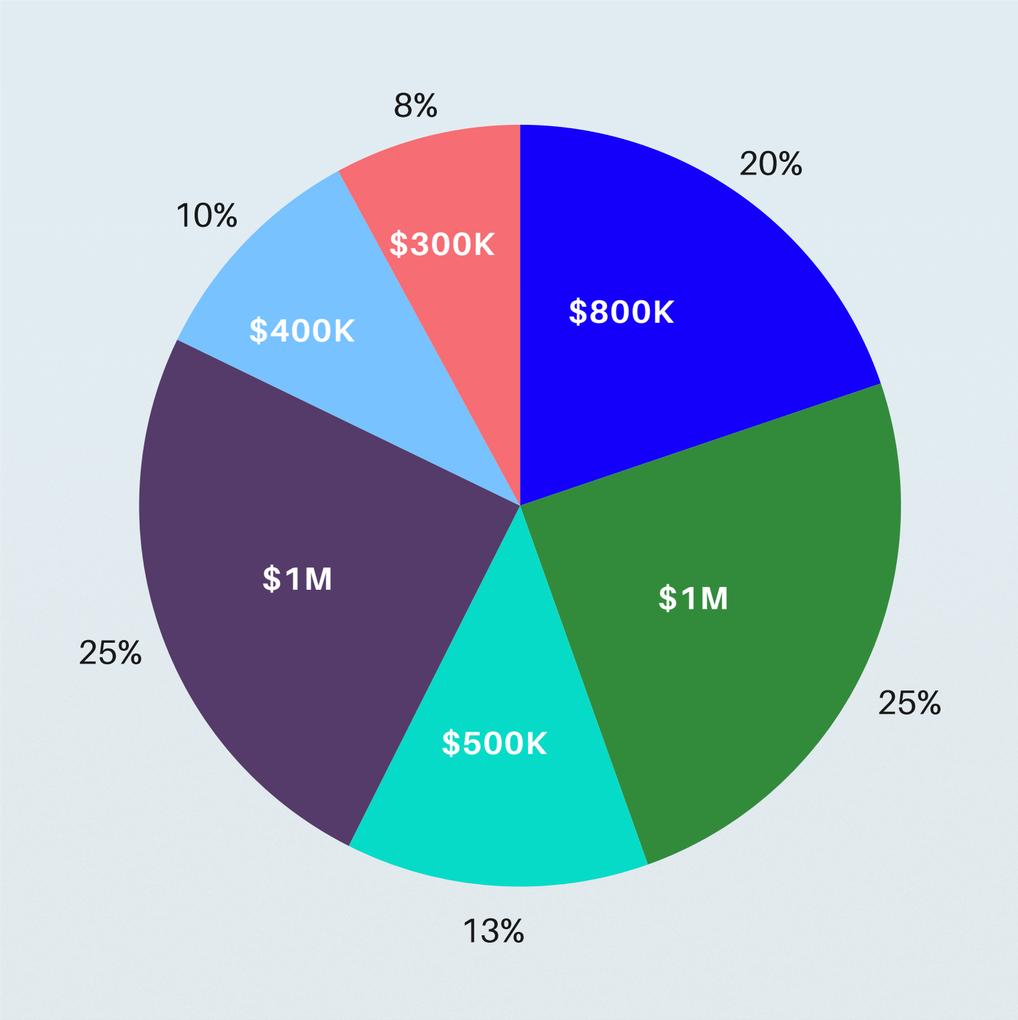
05. DEPLOYMENT

Implement a secure deployment process with configuration management.Monitor applications for security incidents and vulnerabilities post-deployment.

PROGRAM ROADMAP



BUDGET ALLOCATION



- MFA
- Legacy Systems
- SOC2 Compliance
- PII Data Security
- Training
- Contingency

STAKEHOLDER MATRIX

Stakeholder	Role	Primary Priority	Key Focus
CTO	Technology Strategy	Innovation	AI adoption, secure processing
CIO	Security Oversight	Risk Reduction	Compliance, access controls
IT Team	Technical Implementation	Operational Efficiency	System updates, encryption
Clients	Service Users	Data Privacy & Trust	Transparency, data protection
Regulatory Bodies	Compliance Enforcement	Compliance	Audit, adherence to standards

KEY TAKEWAYS FOR CYBERSECURITY PROGRAM

1

Comprehensive Three-Year Plan

The program addresses both current and potential vulnerabilities across critical areas, including employee access controls, data protection, and incident response

2

Strategic Alignment with CTO and CIO Goals

Directly supports CTO goals (innovation, scalability) by enabling secure infrastructure for tech advancements, and aligns with CIO objectives (risk management, compliance) to uphold regulatory and security standards

3

Investment in Resilience and Compliance

A $4 million investment is allocated across resources, technology, and training, emphasizing Lemonade’s commitment to a resilient and secure environment for employees and customers

CONCLUSION

This 3-year cybersecurity roadmap provides a structured, executive-focused framework for addressing Lemonade’s most critical security priorities. By aligning each initiative with specific goals, the roadmap highlights a phased, adaptive approach designed to strengthen Lemonade’s cybersecurity posture in a scalable, resource-efficient manner.

THANK YOU!

CTO

NELL CRAIN

CIO

RHEA RIPLEY