Vendor Security Assessment Threat Modeling Guide

For Security Engineers/Analysts

Author: Kat Fitzgerald

March 2025

1. Introduction

This guide provides a structured approach to threat modeling during Vendor Security Assessments (VSAs), specifically focusing on data sharing scenarios involving Google Workspace, Gmail, and similar email systems like Microsoft 365. The threat modeling process helps security engineers go beyond questionnaire responses to evaluate comprehensive security risks.

2. Pre-Assessment Data Gathering

2.1 Data Flow Understanding

- Document all entry and exit points for Google data
- Map data flow between Google systems and vendor systems
- Identify data storage locations and retention periods
- Document authentication mechanisms for data access
- Map integration points with email systems

2.2 Access Control Mapping

- Document user roles and permission levels
- Identify administrative access points
- Map service account permissions
- Document OAuth scopes and permissions
- List third-party integrations

3. Threat Categories

3.1 Data Exfiltration Threats

- Unauthorized data downloads
- Email forwarding rules
- Browser extensions with data access
- Screen capture/sharing risks
- API abuse scenarios
- Data export functionality
- Clipboard risks

3.2 Authentication/Authorization Threats

- Session hijacking
- OAuth token theft
- Credential stuffing
- Password spraying
- MFA bypass attempts
- Service account compromise
- Privilege escalation

3.3 Email-Specific Threats

- Phishing through vendor systems
- Mail rule manipulation
- Email retention policy bypass
- DLP bypass scenarios
- Attachment malware delivery
- Email forwarding chains
- BEC (Business Email Compromise) risks

3.4 Integration Threats

- API endpoint vulnerabilities
- Webhook abuse
- SSO implementation flaws
- Directory sync issues
- Third-party plugin risks
- Cross-tenant data leakage
- Integration chain attacks

4. Risk Assessment Matrix

4.1 Impact Levels

- Data breach scope
- Operational disruption
- Regulatory compliance
- Reputational damage
- Financial impact
- User privacy impact
- Service availability

4.2 Likelihood Factors

- Technical complexity
- Required access levels
- Detection capabilities
- Existing controls
- Attack surface size
- Historical precedents
- Attacker motivation

5. Control Evaluation Framework

5.1 Preventive Controls

- Access management
- Authentication methods
- Data encryption
- Network segregation
- Input validation
- API rate limiting
- DLP implementation

5.2 Detective Controls

- Logging mechanisms
- Alert systems
- Audit trails
- User activity monitoring
- Anomaly detection
- DLP monitoring
- Access reviews

5.3 Responsive Controls

- Incident response plans
- Account lockout procedures
- Data recovery processes
- Communication protocols
- Forensic capabilities
- Vendor SLAs
- Breach notification

6. Specific Scenarios Analysis

6.1 Google Workspace Integration

- Document sharing risks
- Drive sync scenarios
- Calendar integration risks
- Meet/Chat security
- Admin console risks
- Directory risks
- Domain-wide delegation

6.2 Email System Integration

- Mail flow security
- Attachment handling
- Header manipulation
- SPF/DKIM/DMARC
- Email encryption
- Distribution lists
- Archive access

7. Vendor-Specific Considerations

7.1 Architecture Review

- Cloud infrastructure
- Network design
- Application architecture
- Database design
- Backup systems
- DR capabilities
- Security monitoring

7.2 Development Practices

- SDLC security
- Code review process
- Deployment security
- Change management
- Security testing
- Vulnerability management
- Third-party code

8. Mitigation Strategies

8.1 Technical Controls

- API security requirements
- Authentication standards
- Encryption requirements
- Network controls
- Monitoring requirements
- Access restrictions
- Data handling rules

8.2 Procedural Controls

- Access review process
- Change management
- Incident response
- Security training
- Audit procedures
- Documentation requirements
- Communication protocols

9. Continuous Assessment

9.1 Monitoring Requirements

- Security metrics
- Performance indicators
- Compliance checks
- Access reviews
- Threat intelligence
- Incident tracking
- Control effectiveness

9.2 Periodic Review Criteria

- Control assessment
- Risk reassessment
- Threat landscape changes
- Compliance updates
- Technology changes
- Business changes
- Integration changes