Shadow IT Detection Extension – Hackathon Brief

# 1. Executive Summary

Our project is a Chrome extension that helps companies detect and prevent Shadow IT – the use of unauthorized SaaS or cloud applications. It flags unapproved sites, displays risk information, suggests secure alternatives, and logs access events to an admin dashboard for IT visibility. It also includes malware scanning using the VirusTotal API to verify uploaded files before sharing them.

# 2. How the Product Works

• The extension detects domain visits and checks them against an approved/unapproved list.  
• If unapproved, a warning popup appears showing risk score, vulnerabilities, reasons, and suggestions.  
• All unapproved visits are logged to a backend dashboard for auditing.  
• A built-in file scanner using the VirusTotal API allows users to verify file safety before upload.

# 3. Role of Security in Preventing Shadow IT

Security teams are responsible for enforcing corporate IT policies and ensuring data safety. They play a key role in identifying Shadow IT risks by monitoring unauthorized app usage and blocking data exfiltration paths. Our tool empowers them with real-time visibility and action logs.

# 4. Competitors and Our Advantage

Competitors include platforms like Netskope, Zscaler, and Palo Alto Networks' Prisma.  
Our differentiators:  
• Lightweight, browser-based solution (ideal for SMEs and fast deployments).  
• Integrated risk intelligence (vulnerabilities, CVEs, and suggestions).  
• File upload malware scanning via VirusTotal.  
• Open source and customizable for internal security teams.

# 5. Monetization Opportunities

• SaaS Subscription for Admin Dashboard + Cloud Hosting.  
• Pro Features: Role-based access, real-time alerts, SIEM integration, API access.  
• Enterprise Tier: SOC2/ISO-compliant reporting, AI-based app detection.  
• Data-as-a-Service: Anonymous usage trends for benchmarking.

# 6. Sample Judge Questions & Answers

Q: What problem are you solving?  
A: Shadow IT exposes companies to data breaches, compliance risks, and security blind spots. We provide real-time visibility and control.  
  
Q: How is this different from other solutions?  
A: It's lightweight, open-source, privacy-conscious, and instantly deployable with malware scanning and CVE warnings built-in.  
  
Q: How do you validate what’s approved/unapproved?  
A: Admins define policies, and we plan to integrate dynamic reputation scoring using public threat feeds.  
  
Q: What’s your go-to-market strategy?  
A: Target SMBs and security-conscious teams with easy setup and pay-as-you-grow plans.