MVP Threat Model

One page. 60 minutes. Three controls before launch.

Project / Feature		**Date**	
Participants		**Sprint #**	

1. Assets (Crown Jewels)

What are we protecting? List 5–7 items.

2. Entry Points

Where can attackers reach the system?

3. Abuse Paths

Format: "Attacker does X via Y to cause Z." Score 1–3 each. ***1–2 = monitor · 3–4 = next sprint · 6–9 = pre-launch action***

#	Abuse Path	Likelihood	Impact	Score
1				
2				
3				
4				
5				

4. Impact (per top-scored path)

User harm · Trust damage · Operational impact · Cost spike · Contractual or legal exposure

5. Controls — Top 3

Pick the smallest control that closes the biggest hole. Each gets one owner, one due date, one acceptance test.

#	Control	Owner	Due Date	Acceptance Test
1				
2				
3				

Now / Next / Later

Pre-launch / Next sprint / Documented debt with re-evaluation trigger.

Now (this sprint)	Next (sprint+1)	Later (debt + trigger)

Pre-Launch Eligibility Checklist

Any "no" → ticket with owner and due date before release.

☐	Token lifetime and revocation policy documented	Yes	No	N/A
☐	Object-level authorization tested on top 3 APIs	Yes	No	N/A
☐	Webhook signatures verified and replay-protected	Yes	No	N/A
☐	Sensitive data redacted in analytics payloads	Yes	No	N/A
☐	Admin actions produce audit log entries (B2B/enterprise only)	Yes	No	N/A

The 60-Minute Sprint

0–10 min Define crown-jewel assets — what hurts users fastest if it leaks?

10–25 min Map the top three user journeys — onboarding, checkout, admin changes

25–40 min Brainstorm realistic attacker moves — "Attacker does X via Y to cause Z"

40–50 min Score risk fast — likelihood × impact, 1–3 scale each

50–60 min Pick top 3 mitigations — assign owner, due date, acceptance test

Free template by GRC Vitrix · grcvitrix.com
Practical SOC 2, security, and AI guides for early-stage SaaS teams.