AegisShield Firewall

Fictional product discovery and controlled pilot case

Prepared by Eva Marquez

This case is fictional. The company, customer, research, costs, dates, board states, prototype, decisions, and outcomes are simulated for portfolio demonstration.

Contents

00-case-plan-and-codex-instructions - Case 02 - Plan and step-by-step instructions

01-sponsor-handoff-and-scenario - Document 01 - Sponsor Handoff and Scenario

02-product-discovery-and-business-case - Document 02 - Product Discovery and Business Case

03-discovery-findings-and-sponsor-decision - Document 03 - Discovery Findings and Sponsor Decision

04-project-brief - Document 04 - Project Brief

05-project-charter - Document 05 - Project Charter

06-product-scope-and-requirements - Document 06 - Product Scope and Requirements

07-stakeholder-register-and-communication-plan - Document 07 - Stakeholder Register and Communication Plan

08-kickoff-meeting-notes - Document 08 - Kickoff Meeting Notes

09-product-experience-and-prototype - Document 09 - Product Experience and Prototype

10-technical-approach-and-delivery-plan - Document 10 - Technical Approach and Delivery Plan

11-work-breakdown-structure - Document 11 - Work Breakdown Structure

12-raci-and-team-responsibilities - Document 12 - RACI and Team Responsibilities

13-product-backlog-and-estimates - Document 13 - Product Backlog and Estimates

14-budget-and-capacity-plan - Document 14 - Budget and Capacity Plan

15-project-schedule - Document 15 - Project Schedule

16-test-and-validation-plan - Document 16 - Test and Validation Plan

17-risk-register - Document 17 - Risk Register

18-data-protection-and-operational-readiness - Document 18 - Data Protection and Operational Readiness

19-execution-board-and-snapshots - Document 19 - Execution Board and Snapshots

20-issue-log - Document 20 - Issue Log

21-decision-and-change-log - Document 21 - Decision and Change Log

22-project-status-report - Document 22 - Project Status Report

23-pilot-test-results-and-bookeasy-acceptance - Document 23 - Pilot Test Results and BookEasy Acceptance

24-go-no-go-and-release-record - Document 24 - Go-No-Go and Release Record

25-stabilization-and-operations-handover - Document 25 - Stabilization and Operations Handover

26-project-closure-and-lessons-learned - Document 26 - Project Closure and Lessons Learned

27-portfolio-summary - Document 27 - Portfolio Summary

Case 02 - Plan and step-by-step instructions

Result

Create a fictional product case for AegisShield Firewall. The final case will include management documents, a visual prototype, simple diagrams, simulated execution evidence, and a printable document pack.

Important rules

- Keep this case separate from Case 01 - Cybersecurity Platform Modernization.
- Do not change the Case 01 PDF while building this case.
- Clearly label fictional customers, interviews, findings, costs, dates, and outcomes as simulated.
- Do not call a prototype a working security product.
- Do not assume that a delay must happen. A change request is recorded only if the fictional execution creates a reason for one.
- Use short, clear language and add a small vocabulary section to each document.
- Review each part before moving to the next one.

Prompt format for each step

Every implementation prompt should include:

- Objective - what this step is meant to decide or create.

2. Context - the facts and boundaries already approved. 3. Approved content - the exact information that must appear. 4. Deliverable - the file, page, prototype, or evidence to create. 5. Check - how we know the step is complete.

Stages

1. Define the initiative

Create the Sponsor Handoff and Scenario. Explain the product idea, the customer problem, the possible pilot, the relationship to the SIEM, the sponsor request, and the discovery boundaries.

2. Justify the product

Create the Product Discovery and Business Case. Compare competitors and alternatives, including continue, buy, resell, integrate, or build. Treat the value proposition, interviews, and findings as hypotheses until they are tested.

3. Record the discovery decision

Create Discovery Findings and Sponsor Decision. Record the simulated customer findings, options considered, recommendation, sponsor decision, approved boundary, and conditions for the next stage.

4. Define the first version

Create the Project Brief, Project Charter, product scope, roles, permissions, acceptance criteria, and the engineering investigation of an existing security engine.

5. Design the experience

Create the administrator journey and prototype screens. Show setup, rule configuration, event review, a blocked request, and correction of a rule that affected a legitimate booking. Use simulated data and state clearly that the prototype is not functional protection.

6. Plan the delivery

Create stakeholders, communication plan, kickoff, requirements, technical approach, WBS tree, RACI, backlog, estimates, budget, Gantt, and team capacity. Calculate the schedule from scope and proposed resources.

7. Plan tests and risks

Define tests for malicious requests, legitimate bookings, performance, permissions, data protection, monitoring, and recovery. Record risks such as false positives, service interruption, performance limits, and sensitive data in logs.

8. Represent execution

Create the execution board after the case is defined. Use real tool records only when they are ready, and label screenshots as simulated project evidence. If the fictional rule blocks a legitimate booking, record investigation, options, and the selected response. Add a change request only if the scenario supports one.

9. Validate, close, and publish

Prepare test results, BookEasy acceptance, launch decision, execution record, stabilization, operations handover, closure, lessons learned, and the portfolio page. Include the prototype, diagrams, screenshots, and printable documents.

Current progress

- Document 01 - Sponsor Handoff and Scenario: drafted.
- Document 02 - Product Discovery and Business Case: drafted.
- Document 03 - Discovery Findings and Sponsor Decision: drafted with simulated findings and a limited-stage recommendation.
- Documents 04-08: drafted in the authorization and product-definition phase.
- Document 09 - Product Experience and Prototype: drafted.
- Prototype: visual, non-functional, and uses simulated data.
- Documents 10-15 - delivery planning and technical design: drafted.
- Documents 16-18 - tests, risks, data protection, and operational readiness: drafted.
- Documents 19-27 - execution, issue resolution, pilot, release, handover, closure, and portfolio summary: drafted.
- Evidence repository: created and public, with the prototype, three GitHub Projects snapshots, and the case documents.
- Printable pack: created and checked as aegisshield-appprotect-case.pdf.
- Website page: published at https://www.by-evamarquez.com/portfolio/aegisshield-appprotect with links to the PDF, prototype, repository, and board evidence.

Document 01 - Sponsor Handoff and Scenario

Project: AegisShield Firewall Timing: Before project planning Status: Initial sponsor request

Business context

AegisShield is a fictional cybersecurity company. Its existing product is a SIEM, a service that collects security events and helps analysts investigate suspicious activity.

Leadership wants to expand the product portfolio with AegisShield Firewall, a web application firewall. AegisShield Firewall would inspect incoming web requests and could block requests that match configured security rules.

Customer problem to validate

BookEasy is an existing SIEM customer with an online scheduling application. Its booking and login functions must stay available to legitimate users while being protected from malicious requests.

For this fictional case, leadership identifies BookEasy as a possible pilot customer. Its needs, willingness to participate, and current protections still require confirmation.

Proposed product direction

AegisShield Firewall would be a separate service for configuring application protection, reviewing security events, and managing blocking rules.

The first direction is to use an established security engine and build the customer controls and service around it. Engineering must assess technical feasibility, licensing, and operational needs before a solution is selected.

Sponsor request

The CTO asks the Project Manager to coordinate an initial discovery and feasibility stage with Product, Engineering, Security, Design, and Operations.

The team must:

- Clarify customer needs.
- Compare competing solutions and build, buy, or integrate options.
- Propose a limited first release.
- Estimate resources, costs, and delivery time.

The sponsor will review this evidence before authorizing development and a BookEasy pilot.

Initial boundaries

AegisShield Firewall is a new product initiative. Changes to the existing SIEM are outside the initial discovery scope, except for assessing a possible event integration.

The proposed first release focuses on one BookEasy web application. Broader customer rollout, a proprietary security engine, and additional protection products require separate decisions.

Protection must be evaluated together with service availability. The team must consider how to prevent incorrect blocks from interrupting legitimate bookings.

Expected discovery outputs

A documented customer problem, proposed product scope, prototype, technical options, initial risks, estimated budget and schedule, and a recommendation for the sponsor's investment decision.

Key terms

SIEM: A service that collects security events to support monitoring and investigation.

Web application firewall: A security filter that inspects web requests and applies rules to allow or block them.

Web request: A message sent to an application, such as a request to log in or create a booking.

False positive: A legitimate request incorrectly identified as a threat.

Discovery: Early work to understand the problem and evaluate possible solutions.

Pilot: A limited trial with an agreed customer and scope.

Approval boundary

The sponsor authorizes investigation and proposal work only. Approval to build the product will come later, after enough information is available.

Document 02 - Product Discovery and Business Case

Project: AegisShield Firewall Stage: Discovery Status: Draft for evaluation

Business opportunity

AegisShield wants to evaluate a second product that complements its existing SIEM service.

AegisShield Firewall would inspect incoming requests to customer web applications and apply configured protection rules. Customers would manage the service through a dedicated administration panel.

Customer hypothesis

The proposed target is businesses that operate web applications and have limited internal security capacity.

The hypothesis is that some customers would value application protection configured and supported by AegisShield. This has not yet been validated.

BookEasy is a proposed discovery participant and possible pilot customer. Participation does not imply a purchase commitment.

Discovery questions

- What protection does the customer already use?
- Which problems remain unresolved?
- Who configures security rules and investigates incorrect blocks?
- What would justify purchasing another service?
- Who makes the purchasing decision, and what budget could support it?

Alternatives to evaluate

- Continue using the customer's existing protection.
- Purchase or resell an established service.
- Build an AegisShield product around an existing security engine.
- Develop a proprietary engine. This option needs separate justification because of its technical and operational demands.

Proposed value to test

AegisShield would offer application protection with guided setup, understandable event records, and support for investigating incorrect blocks.

These are proposed benefits, not established competitive advantages. Discovery must determine whether customers value them and whether existing products already meet their needs.

Discovery activities

- Product leads customer interviews and competitor analysis.
- Engineering and Security evaluate technical options and protection limits.
- Design prepares a prototype of setup, event review, and rule management.
- Operations assesses hosting, monitoring, support, and recovery needs.
- The Project Manager coordinates activities, dependencies, estimates, and the sponsor review.

Commercial and delivery assessment

The team estimates development costs and ongoing costs for infrastructure, licensing, security rule maintenance, and customer support.

Product proposes a pricing hypothesis. The team evaluates whether potential revenue could support those costs.

All figures used in this educational case must be identified as simulated assumptions.

Decision criteria

Recommend a limited development stage only if discovery identifies a clear customer problem, a credible reason to choose AegisShield Firewall, a feasible technical approach, and an acceptable estimate of costs and risks.

Otherwise, recommend further investigation, a partnership, or stopping the initiative.

Sponsor decision

Pending completion of discovery.

The decision record will identify the evidence reviewed, selected option, approved funding boundary, and conditions for the next stage.

Key terms

Business case: The reasons, costs, expected benefits, and risks used to assess an investment.

Customer hypothesis: An assumption about customer needs that must be tested.

Build versus buy: A comparison between developing a solution and obtaining an existing one.

Operating costs: The ongoing cost of running and supporting the product.

Decision gate: A review where the sponsor decides whether and how work should continue.

Document 03 - Discovery Findings and Sponsor Decision

Project: AegisShield Firewall Stage: Discovery decision gate Status: Simulated findings and recommendation for sponsor review

> *All findings in this document are simulated for portfolio use. They are not real customer research or competitive research.*

Discovery evidence used

The team reviewed a simulated BookEasy interview summary, a short competitor comparison, an initial technical assessment, an operating-cost estimate, and a prototype review.

Simulated customer findings

Area	Simulated finding	What it means
Current protection	BookEasy uses a basic hosted protection service and reviews alerts in more than one place.	A simpler view could be useful, but the value is not proven for every customer.
Main pain point	The team needs to understand why a request was blocked and restore a legitimate booking quickly.	Event details, rule explanation, and a safe exception path are important for the first version.
Ownership	Engineering configures protection today, while support receives the first customer questions.	The product needs clear roles, permissions, and an escalation path.
Pilot interest	The simulated BookEasy representative is open to reviewing a limited pilot if booking traffic is protected and rollback is ready.	The pilot is possible, but it is not a purchase commitment.
Buying reason	The strongest proposed reason is guided setup and support from the existing AegisShield team.	The value proposition should stay focused instead of promising a full security platform.

Simulated options comparison

Option	Summary	Assessment
Continue with current protection	Do not add an AegisShield product now.	Lowest delivery cost, but does not address the visibility and support gap found in discovery.
Buy or resell an existing service	Offer another vendor's service to customers.	Faster path, but less control over the customer experience, data flow, and product direction.
Build around an existing security engine	Use an established engine and create the AegisShield setup, event, exception, and support experience.	Recommended for a limited first version, subject to licensing, technical, and performance checks.
Build a proprietary engine	Create the detection and blocking engine inside AegisShield.	Not recommended for the first version because the cost, risk, and support burden are too high.

Recommendation

Authorize a limited product-definition and technical validation stage for AegisShield Firewall. The first version should use an established security engine and focus on one BookEasy web application.

The first version should cover:

- Registering one application.
- Configuring a small set of protection rules.
- Viewing requests and rule matches.
- Blocking a request in a controlled test setting.
- Creating and reviewing an exception for a legitimate booking.
- Recording security events for the existing SIEM integration if the technical assessment supports it.

The first version should not include a proprietary engine, broad customer rollout, or a promise of protection against every threat.

Conditions before development approval

- Engineering confirms that the selected engine can meet the pilot needs.
- Product confirms the first-release scope and customer validation scenarios.
- Security reviews data handling, access control, rule safety, and audit needs.
- Operations confirms monitoring, support, recovery, and escalation requirements.
- Finance or the sponsor reviews the simulated budget and ongoing operating-cost assumptions.
- BookEasy confirms the pilot boundary and agrees how legitimate bookings will be protected during testing.

Sponsor decision

Simulated decision: Approve the limited product-definition and technical-validation stage.

Decision owner: CTO / Project Sponsor.

Approved boundary: One BookEasy web application, an established security engine, a limited set of rules, a controlled test environment, and a pilot-readiness recommendation.

Not approved: Production protection, broad customer rollout, a proprietary engine, or a full AegisShield Firewall launch.

Next step

Use this decision to prepare the Project Brief and Project Charter. The Charter will define the approved stage, authority, resources, milestones, and success criteria before detailed delivery planning begins.

Key terms

Finding: Information learned during discovery. In this case, a simulated customer need or constraint.

Option: A possible path the sponsor could choose, such as buy, integrate, or build.

Recommendation: The option the team supports after reviewing the evidence.

Decision gate: The point where the sponsor decides whether the work can move to the next stage.

Approved boundary: The clear limit of what the decision allows the team to do.

Document 04 - Project Brief

Project: AegisShield Firewall Stage: Product definition and technical validation Status: Draft for Charter approval Customer: BookEasy pilot, fictional

Purpose

Turn the discovery recommendation into a small, testable product stage. The team will define the first AegisShield Firewall experience, confirm technical feasibility, and prepare a safe pilot recommendation.

Problem

BookEasy needs to protect an online scheduling application without making legitimate login and booking requests fail. Its current protection and alert review are spread across more than one place. The team needs a clearer way to understand blocked requests and correct a rule when it affects a real customer action.

Objective

Define and validate a limited AegisShield Firewall first version for one BookEasy web application. The stage must show how an administrator registers the application, configures basic rules, reviews events, tests a block, and creates a safe exception for a legitimate booking.

Proposed scope

Included

- One BookEasy web application in a controlled test environment.
- Application registration and basic protection settings.
- A small set of rules for common request patterns.
- Request and rule-match event review.
- Controlled block testing.
- Exception management for an approved legitimate request.
- Roles, permissions, audit records, monitoring, and recovery planning.
- Technical assessment of an established security engine.

Excluded

- Production protection for BookEasy.
- Rollout to other customers.
- A proprietary detection or blocking engine.
- A complete SIEM redesign.
- A promise to detect every type of attack.
- Automated rule changes without an approval step.

Main deliverables

- Approved product brief and charter.

2. Product scope, requirements, and acceptance checklist. 3. Administrator journey and clickable visual prototype. 4. Technical option, licensing, and operating-cost assessment. 5. WBS, RACI, backlog, estimates, schedule, risks, and test plan. 6. Pilot-readiness recommendation and sponsor decision.

Assumptions and constraints

- The company and customer are fictional.
- Customer interviews and competitor findings are simulated.
- A security engine may be licensed or integrated, but its terms must be reviewed.
- The prototype uses simulated data and is not a working firewall.
- Legitimate login and booking must remain available in the pilot test.
- The first stage uses a part-time cross-functional team.

Success criteria for this stage

- The first-release boundary is approved.
- The main customer journey is clear and understandable.
- Engineering confirms at least one feasible technical path.
- Security and Operations identify the controls needed for a pilot.
- BookEasy confirms the pilot scenarios and the safe way to test blocks and exceptions.
- The sponsor has enough evidence to decide whether to authorize pilot build work.

Methodology

This stage uses a hybrid approach. The plan controls scope, decisions, risks, budget assumptions, and gates. The team uses short discovery and design loops to test the product idea, learn from findings, and adjust the first version before approval.

Key terms

First version: The smallest product scope that can test the main customer problem.

Pilot readiness: Evidence that the team can test the product with the agreed customer and controls.

Operating cost: The ongoing cost to host, monitor, license, and support the product.

Scope boundary: What the team is allowed to include and what it must leave out.

Document 05 - Project Charter

Project: AegisShield Firewall Stage authorized: Product definition and technical validation Status: Simulated sponsor approval Sponsor: CTO

Authorization

The CTO authorizes the Project Manager to coordinate a limited product-definition and technical-validation stage for AegisShield Firewall. This authorization does not approve production protection or a broad product launch.

Business need

AegisShield wants to evaluate a second product that can complement its SIEM. The first version must solve a clear customer problem without creating a new source of service interruption or unsafe blocking.

Objective

Prepare enough product, technical, operational, financial, and customer evidence for the sponsor to decide whether to authorize a controlled BookEasy pilot.

Approved boundary

The team may define and validate AegisShield Firewall for one BookEasy web application. It may assess an existing security engine, create a visual prototype, define rules and exceptions, estimate resources and costs, and prepare pilot controls.

The team may not deploy production protection, roll out to other customers, build a proprietary engine, or redesign the existing SIEM.

Deliverables

- Product brief and scope.
- Requirements and acceptance criteria.
- Administrator journey and prototype.
- Technical option and licensing assessment.
- Stakeholder, communication, and kickoff records.
- WBS, RACI, backlog, estimates, budget, Gantt, and capacity view.
- Test, risk, data-protection, monitoring, and recovery plan.
- Pilot-readiness recommendation and sponsor decision.

Methodology

The project uses a hybrid approach:

- Planned controls for scope, approvals, risks, budget assumptions, dates, and release gates.

- Short discovery and design loops for interviews, prototype feedback, technical checks, and requirement changes.

In simple terms, the team agrees on the limits first, then learns and improves the first version in small steps.

Initial milestones

Milestone	Target
Charter and first-release scope approved	Week 2
Prototype and requirements reviewed	Week 4
Technical and cost options assessed	Week 5
Pilot test plan and controls ready	Week 7
Sponsor decision on pilot build	Week 8

Authority

- The CTO approves scope, budget boundary, major risks, and the decision to authorize pilot build work.
- Product owns customer value, first-release priorities, and acceptance scenarios.
- Engineering owns technical feasibility, engine evaluation, estimates, and implementation options.
- Security owns security controls, data protection, and rule-safety review.
- Operations owns monitoring, support, recovery, and handover requirements.
- The Project Manager coordinates the plan, records decisions, tracks risks, and escalates blockers.

Resources and budget assumption

The fictional plan assumes part-time availability from Product, Engineering, Security, Design, Operations, QA, Customer Success, and the Project Manager. Budget figures will be labeled as simulated planning assumptions and will be reviewed by the sponsor before any build authorization.

Success criteria

The stage succeeds when the sponsor receives a clear scope, evidence of a real customer problem, a feasible technical path, a safe test approach, an initial cost and schedule view, and a recommendation with conditions.

Simulated approval

Decision: Approved for product definition and technical validation. Date: April 6, 2026 (simulated). Approver: CTO / Project Sponsor. Next gate: Sponsor decision on controlled pilot build.

Key terms

Charter: The document that authorizes the work and sets its limits.

Gate: A review point where the sponsor decides whether work can move forward.

Pilot build: A limited build prepared for controlled customer testing.

Release approval: Permission to put a product change into an agreed environment.

Document 06 - Product Scope and Requirements

Project: AegisShield Firewall Stage: Product definition Status: Draft baseline for review

Product goal

Help a customer protect one web application, understand why requests were blocked, and correct a rule when a legitimate booking is affected.

First-release scope

Area	Included in the first version	Not included
Application	Register one BookEasy web application	Multiple customer applications
Rules	Create, enable, disable, and test a small rule set	Automatic rule creation
Events	Review request details, matched rule, action, and time	Full security analytics platform
Blocking	Run controlled block tests in a non-production environment	Unsupervised production blocking
Exceptions	Add an approved exception and record who changed it	Permanent bypass without review
Access	Admin and viewer roles	Complex enterprise role design
Integration	Assess an event feed to the existing SIEM	Rebuild the SIEM

Requirements and acceptance

ID	Requirement	How we will check it
APR-01	An admin can register one BookEasy web application.	The application appears with name, environment, owner, and status.
APR-02	An admin can create and change a basic protection rule.	A rule can be saved, enabled, disabled, and shown with an audit record.
APR-03	The service records request and rule-match events.	Test events show time, action, matched rule, and a safe request identifier.
APR-04	An admin can review why a request was blocked.	The event view explains the rule and shows the request details approved for display.
APR-05	A controlled test can block a request in the test environment.	A known test request is blocked and the result is recorded.
APR-06	An approved admin can create an exception for a legitimate booking request.	The request passes after the exception, the change is logged, and the exception can be removed.
APR-07	Viewer users cannot change rules or exceptions.	Permission tests show that a viewer can read allowed events but cannot edit controls.
APR-08	The product can show its service health and failed delivery attempts.	Operations can see a health state and receive an alert for a simulated failure.

ID	Requirement	How we will check it
APR-09	Sensitive request data is protected in the product and test records.	Security confirms masking, access control, retention, and no credentials in logs.
APR-10	A pilot can return to the prior safe configuration.	The team rehearses rule rollback and records the result before pilot approval.

Customer acceptance scenarios

- A legitimate BookEasy login request is allowed.

2. A legitimate booking request is allowed. 3. A simulated malicious request is blocked in the test environment. 4. An admin can see which rule caused the block. 5. An admin can add an approved exception for a legitimate booking. 6. A viewer can review events but cannot change rules. 7. Operations can see service health and a simulated delivery failure.

Open items before baseline approval

- Confirm the exact security engine and license terms.
- Confirm which request fields can be stored and displayed.
- Confirm the performance target for the pilot environment.
- Confirm the exception approval and expiration process.
- Confirm whether the SIEM event feed is in the first pilot or a later increment.

Key terms

Requirement: A condition the product must meet.

Acceptance: The evidence that shows a requirement was met.

Rule: A condition that tells the service what to do with a request.

Exception: An approved case where a request should not follow the normal block rule.

Viewer: A role that can review information but cannot change protection settings.

Document 07 - Stakeholder Register and Communication Plan

Project: AegisShield Firewall Stage: Product definition Status: Draft for kickoff confirmation

Stakeholder register

Stakeholder	Interest	Role in the case
CTO / Sponsor	Investment, risk, and product direction	Approves stage boundaries, budget assumptions, and decision gates.
Project Manager	Coordination and visibility	Maintains the plan, risks, decisions, and communication.
Product Lead	Customer value and priorities	Owns the product hypothesis, scope, and customer scenarios.
Engineering Lead	Feasibility and delivery effort	Assesses the engine, integration, architecture, and estimates.
Security Lead	Safe protection and data handling	Reviews rules, access, logging, privacy, and false-positive controls.
Product Designer	Usable administration experience	Designs the setup, event review, rule, and exception journeys.
Operations Lead	Service health and support	Defines monitoring, on-call, recovery, and handover needs.
QA Lead	Evidence and customer validation	Plans tests and records acceptance evidence.
Customer Success	Customer coordination	Prepares BookEasy communication and pilot readiness.
BookEasy representative	Practical customer needs	Reviews scenarios and accepts or rejects the pilot results.
Support	Customer questions and escalation	Confirms how incorrect blocks are reported and handled.

Communication plan

Audience	What they need	Channel	Frequency	Owner
Sponsor	Progress, risks, decisions, cost and schedule changes	Written status summary	Weekly and at gates	Project Manager
Core team	Work, blockers, dependencies, and next actions	Working meeting	Twice weekly	Project Manager
BookEasy and Customer Success	Scenarios, test windows, expected impact, and results	Review call and email	Weekly during pilot preparation	Product / PM
Security and Operations	Controls, test evidence, alerts, and recovery	Review session	At design and release gates	Security / Operations
Support	Known limits, customer message, and escalation path	Handover session	Before pilot and handover	Customer Success

Escalation rules

- The Project Manager escalates a material scope, schedule, cost, or customer-impact risk to the sponsor.
- Security escalates unsafe data handling, access, or rule behavior immediately.
- Operations escalates service-health or recovery concerns before a pilot or release gate.
- Customer Success escalates a customer concern that could affect participation or acceptance.

Key terms

Stakeholder: A person or group affected by the project or able to influence it.

Communication plan: The agreement for what information is shared, with whom, when, and how.

Escalation: Raising a problem to someone with the authority to decide or help.

Decision gate: A scheduled review where evidence is used to make a decision.

Document 08 - Kickoff Meeting Notes

Project: AegisShield Firewall Meeting: Product definition kickoff Date: April 8, 2026 (simulated) Status: Simulated meeting record

Participants

Role	Attendance
CTO / Sponsor	Present
Project Manager	Present; facilitator and note-taker
Product Lead	Present
Engineering Lead	Present
Security Lead	Present
Product Designer	Present
Operations Lead	Present
QA Lead	Present
Customer Success	Present
BookEasy representative	Invited; attendance to be confirmed for the next customer review

Discussion and agreements

Topic	Agreement
Project purpose	Define and validate a limited AegisShield Firewall first version before approving a pilot build.
Customer boundary	The first scope is one BookEasy web application in a controlled test environment.
Product direction	Evaluate an established security engine before considering any proprietary engine.
Methodology	Use planned controls for gates and decisions, with short discovery and design loops.
Safety	Legitimate login and booking requests must remain available during testing.
Communication	Use the Communication Plan for updates and escalate material customer, security, cost, or schedule risks.
Approval authority	The CTO decides whether the work can move from validation to pilot build.

Open questions

Question	Owner	Due
Which security engines meet the first-release needs and license limits?	Engineering / Security	Week 3
Which request fields may be stored or shown to administrators?	Security / Product	Week 3

Question	Owner	Due
Which BookEasy flows must pass before pilot acceptance?	Product / Customer Success	Week 3
What performance level is acceptable for the pilot environment?	Engineering / Operations	Week 4
How will exceptions expire and be reviewed?	Product / Security	Week 4

Actions

Action	Owner	Due	Status
Finalize the first-release requirements and acceptance scenarios.	Product / QA	April 15, 2026	Pending
Compare engine options, licensing, and technical limits.	Engineering / Security	April 17, 2026	Pending
Create the administrator journey and first prototype screens.	Product Designer	April 17, 2026	Pending
Prepare the initial risk, cost, and capacity assumptions.	Project Manager / Operations	April 20, 2026	Pending
Confirm BookEasy participants and pilot constraints.	Customer Success	April 20, 2026	Pending

Next step

Complete the product requirements, prototype, technical option review, and first risk register before the next sponsor gate.

Key terms

Kickoff: The first team meeting where the work, roles, boundaries, and next actions are aligned.

Action owner: The person responsible for completing a follow-up task.

Open question: Information that must be answered before a decision or approval.

Document 09 - Product Experience and Prototype

Project: AegisShield Firewall Stage: Product design Status: Prototype for review

> *This is a visual prototype for a fictional product. It does not inspect traffic, block requests, or provide real security protection.*

Design goal

Make it easy for an administrator to understand what AegisShield Firewall is doing, see why a request was blocked, and correct a safe false positive without guessing.

Administrator journey

- Open AegisShield Firewall and check service health.

2. Register or select the BookEasy application. 3. Review the current protection mode and rules. 4. Open a request event and understand the matched rule. 5. Decide whether the block looks correct or may be a false positive. 6. Create an approved exception for a legitimate booking request. 7. Test the change in a safe mode. 8. Review the audit record and share the result with Support or Security.

Main screens

Screen	User goal	Main content
Overview	Know if the service is healthy	Application status, requests, blocks, possible false positives, and alerts
Applications	Select the application to manage	BookEasy app, environment, owner, protection mode, and last change
Rules	Understand and manage rules	Rule name, reason, mode, status, last change, and owner
Event detail	Understand a block	Request time, action, matched rule, safe request details, and next step
Exception review	Correct a false positive	Proposed exception, reason, expiry, approver, and test result
Audit and access	See who changed what	User, action, time, result, and permission level

Important product choices

- Start in monitor mode before enabling a block in the pilot.
- Show the matched rule before asking a user to change it.
- Require a reason and expiration for an exception.
- Keep a record of rule and exception changes.
- Separate viewer access from admin access.
- Keep request details masked when they could contain sensitive information.

False-positive scenario

The prototype includes a fictional blocked booking request. The administrator can see that a rule matched a request pattern, review the safe details, and create a short-lived exception for the BookEasy booking path. The exception must be tested and reviewed before it is treated as ready.

Prototype review questions

- Can a new administrator tell which application they are managing?
- Is it clear whether the service is monitoring or blocking?
- Can the user understand why a request was blocked?
- Is the safe path for a false positive easy to find?
- Does the design show who approved an exception and when it expires?
- Are sensitive request details hidden by default?

Key terms

Monitor mode: The service observes and records requests but does not block them.

Block mode: The service stops a request that matches an active rule.

False positive: A safe request that the system treats as a threat.

Exception: A limited, approved change that allows a known safe request.

Audit record: A history of who made a change, what changed, and when.

Document 10 - Technical Approach and Delivery Plan

Project: AegisShield Firewall Stage: Technical validation and delivery planning Status: Proposed approach for review

Approach

Use an established security engine as the protection layer and build a small AegisShield control service around it. The control service manages applications, rules, events, exceptions, roles, audit records, and operational status.

The engine choice is not final. Engineering and Security must confirm licensing, supported deployment, rule behavior, performance, data handling, and recovery before a pilot build is approved.

Simple service flow

BookEasy request -> AegisShield Firewall control point -> security engine -> allow, monitor, or block -> event record -> AegisShield Firewall console -> optional SIEM event feed.

The pilot must start in monitor mode. Block tests use known simulated requests and must not affect real BookEasy users.

Main technical areas

Area	Proposed direction	Owner
Security engine	Compare established engines and choose one only after technical and license review.	Engineering / Security
Control service	Store application, rule, exception, role, and audit information.	Engineering
Event view	Show safe request details, action, matched rule, and time.	Engineering / Design
Exception flow	Require reason, owner, expiry, test result, and approval.	Product / Security
Permissions	Separate admin and viewer access.	Security / Engineering
Operations	Monitor service health, event delivery, and failed changes.	Operations
SIEM integration	Assess an event feed as an optional first increment.	Engineering / SIEM team

Delivery sequence

- Confirm the first-release requirements and customer scenarios.

2. Compare engine options and record licensing and technical limits. 3. Design the administrator experience and review it with Product and BookEasy. 4. Build or configure a non-production proof of the control flow. 5. Test allow, monitor, block, event review, permissions, exception, and recovery behavior. 6. Review cost, support, data protection, and pilot readiness. 7. Present evidence to the sponsor for the pilot-build decision.

Guardrails

- Monitor mode comes before block mode.
- No production traffic is connected during discovery or validation.
- Rules and exceptions have owners, reasons, and audit records.
- Sensitive request values are masked or excluded.
- A safe configuration can be restored before any pilot test.
- Engineering owns detailed design; the PM coordinates decisions and evidence.

Methodology

The team uses a hybrid model. The plan sets scope, decision gates, risks, budget assumptions, and milestones. Short delivery loops are used for the prototype, engine assessment, technical proof, and test corrections.

Key terms

Security engine: The component that evaluates a request against protection rules.

Control service: The AegisShield layer that manages applications, rules, events, users, and exceptions.

Monitor mode: Observe and record without blocking.

Block mode: Stop a request that matches an active rule.

Guardrail: A rule that keeps the work safe and within its approved limits.

Document 11 - Work Breakdown Structure

Project: AegisShield Firewall Stage: Delivery planning Status: Draft baseline

WBS hierarchy

```
AegisShield Firewall
■■■ 1.0 Product definition
■   ■■■ 1.1 Approved brief and charter
■   ■■■ 1.2 Customer discovery and decision record
■   ■■■ 1.3 Product scope and acceptance checklist
■■■ 2.0 Experience and prototype
■   ■■■ 2.1 Administrator journey
■   ■■■ 2.2 Visual prototype
■   ■■■ 2.3 Prototype review and updates
■■■ 3.0 Technical validation
■   ■■■ 3.1 Security engine comparison
■   ■■■ 3.2 Control service and data-flow option
■   ■■■ 3.3 Licensing, performance, and operating-cost assessment
■■■ 4.0 Pilot planning
■   ■■■ 4.1 Requirements and test scenarios
■   ■■■ 4.2 Risk, data, and recovery controls
■   ■■■ 4.3 Pilot-readiness recommendation
■■■ 5.0 Sponsor decision
■   ■■■ 5.1 Evidence package
■   ■■■ 5.2 Go / no-go decision
■   ■■■ 5.3 Decision actions and communication
■■■ 6.0 Project management
    ■■■ 6.1 Schedule, backlog, and status
    ■■■ 6.2 Stakeholder communication and decisions
    ■■■ 6.3 Closure and lessons learned
```

Completion evidence

WBS	Work package	Evidence
1.1	Approved brief and charter	Sponsor-approved boundary and authority
1.3	Product scope and acceptance checklist	Requirements linked to customer scenarios
2.2	Visual prototype	Reviewable screens using simulated data
3.1	Security engine comparison	Option matrix and license questions
3.3	Cost and operating assessment	Simulated estimate with assumptions
4.2	Risk and recovery controls	Risk register and test plan
4.3	Pilot-readiness recommendation	Evidence summary and open conditions
5.2	Sponsor decision	Recorded approval, rejection, or deferral
6.3	Closure	Results, pending items, and lessons learned

Scope check

The WBS covers product definition, experience, technical validation, pilot planning, sponsor approval, and project management. It does not include a full production launch or a proprietary security engine.

Key terms

WBS: A breakdown of the work into clear deliverables and work packages.

Work package: A group of work with a clear result and completion evidence.

Deliverable: Something the project produces and can hand over or review.

Scope check: A review to confirm that the WBS includes the approved work and excludes the rest.

Document 12 - RACI and Team Responsibilities

Project: AegisShield Firewall Stage: Delivery planning Status: Draft for team confirmation

R = does the work. A = answers for the result or final decision. C = gives input. I = receives an update.

Work	PM	Sponsor	Product	Eng	Security	Design	Ops	QA	BookEasy
Approve brief and charter	R	A	C	C	C	I	C	I	I
Confirm customer problem	R	I	A	C	C	C	I	C	C
Approve first-release scope	R	A	R	C	C	C	C	C	C
Design administrator journey	C	I	A	C	C	R	C	C	C
Compare security engines	C	I	C	A/R	R	I	C	C	I
Review data and access controls	C	I	C	R	A/R	I	C	C	I
Prepare prototype review	R	I	A	C	C	R	I	C	C
Prepare test scenarios	C	I	A	R	R	C	C	R	C
Confirm operations and recovery	R	I	C	C	C	I	A/R	C	I
Recommend pilot build	R	A	R	R	R	C	R	R	C
Sponsor pilot decision	R	A	C	C	C	I	C	C	I
Close and share lessons	A/R	C	C	C	C	C	C	C	I

Responsibility notes

- The PM coordinates the work but does not replace technical or security ownership.
- The Sponsor makes the investment and stage decisions.
- Product owns customer value and scope priorities.
- Engineering owns the technical assessment and delivery estimate.
- Security owns safe rule behavior, data protection, access, and audit review.
- Operations owns monitoring, support, recovery, and handover readiness.

- BookEasy validates customer scenarios; it does not approve AegisShield internal design decisions.

Key terms

Responsible: The role that performs the work.

Accountable: The role that answers for the result or makes the final decision.

Consulted: A person whose input is needed before the work is completed.

Informed: A person who receives an update but does not approve the work.

Document 13 - Product Backlog and Estimates

Project: AegisShield Firewall Stage: Delivery planning Status: Initial planning backlog

Estimate unit: person-days. These are simulated planning assumptions, not actual time records.

ID	WBS	Work item	Owner	Priority	Estimate	Dependency	Acceptance evidence
AP-01	1.3	Confirm first-release scope and scenarios	Product / PM	High	2	Charter	Approved scope and scenario list
AP-02	2.1	Map administrator journey	Design / Product	High	3	AP-01	Journey reviewed by Product and BookEasy
AP-03	2.2	Build visual prototype	Design	High	5	AP-02	Setup, event, block, and exception screens reviewed
AP-04	3.1	Compare security engine options	Engineering / Security	High	5	AP-01	Option matrix and license questions
AP-05	3.2	Define control service and data flow	Engineering	High	4	AP-04	Data-flow note and feasibility review
AP-06	3.3	Estimate infrastructure and operating costs	Engineering / Ops	Medium	3	AP-04	Cost assumptions and open questions
AP-07	4.1	Write requirements and test scenarios	Product / QA	High	4	AP-01	Requirements linked to scenarios
AP-08	4.2	Define security, data, and recovery controls	Security / Ops	High	4	AP-05	Control checklist and recovery approach
AP-09	4.3	Prepare pilot-readiness recommendation	PM / QA	High	3	AP-03, AP-06, AP-07, AP-08	Evidence summary and open conditions
AP-10	5.1	Prepare sponsor evidence package	PM	High	2	AP-09	Decision pack ready
AP-11	5.2	Hold sponsor decision gate	Sponsor / PM	High	1	AP-10	Recorded go, no-go, or defer decision
AP-12	6.3	Record closure and lessons	PM	Medium	2	AP-11	Closure record and lessons

Prioritization

- High: required to make the sponsor decision or protect the pilot.
- Medium: needed for a complete planning view but can move slightly without blocking the decision.
- Low: useful follow-up work outside the first decision gate.

Estimate notes

The estimate reflects part-time work and review time. A five-day item may occupy more than one calendar week if the owner is available only part time or is waiting for input.

Backlog controls

The PM tracks status, owner, dependency, estimate, acceptance evidence, and changes. A change to scope or estimate is reviewed for impact before it is accepted into the baseline.

Key terms

Backlog: An ordered list of project work.

Estimate: A planning view of effort, not a promise of exact time.

Dependency: Work that must happen before another item can finish.

Acceptance evidence: Proof that the work meets the agreed result.

Document 14 - Budget and Capacity Plan

Project: AegisShield Firewall Stage: Delivery planning Status: Simulated planning estimate

> *All amounts and capacity figures are fictional assumptions for this portfolio case. They are not a quote or a real company budget.*

Capacity assumptions

Role	Availability	Main focus
Project Manager	50%	Plan, risks, decisions, status, and coordination
Product Lead	30%	Customer problem, scope, and value hypothesis
Engineering Lead	40%	Engine review, technical path, and estimates
Security Lead	20%	Rule safety, data, access, and audit controls
Product Designer	35%	Journey and prototype
Operations Lead	20%	Monitoring, support, recovery, and cost input
QA Lead	25%	Scenarios, evidence, and readiness review
Customer Success	15%	BookEasy participation and communication

Simulated budget estimate

Cost area	Planning assumption	Estimated amount
Product, PM, and design effort	120 person-hours at a blended planning rate	$12,000
Engineering and QA effort	160 person-hours at a blended planning rate	$20,000
Security and Operations effort	60 person-hours at a blended planning rate	$9,000
Prototype and test environment	Eight-week test environment and tooling assumption	$4,000
Security engine license or evaluation	Placeholder pending vendor review	$6,000
Contingency	15% planning reserve	$7,650
Total planning estimate	Simulated only	$58,650

Ongoing cost questions

- Engine license per application or request volume.
- Hosting and traffic costs.
- Monitoring and alerting costs.
- Rule maintenance and security review effort.
- Customer support and incident response coverage.
- Data retention and audit storage.

Capacity risks

- Engineering and Security may be needed for the same engine review.
- BookEasy availability may affect customer validation.
- Operations may not have enough time to review recovery and support needs.
- Licensing information may arrive after the technical comparison starts.

Budget decision boundary

The current estimate supports discovery and technical validation. It does not authorize production hosting, a full engineering build, or a customer rollout. The sponsor must approve a new funding boundary before the project moves into pilot build work.

Key terms

Capacity: The time a role can give to the project.

Blended rate: A planning rate used to estimate a group of roles without naming individual pay rates.

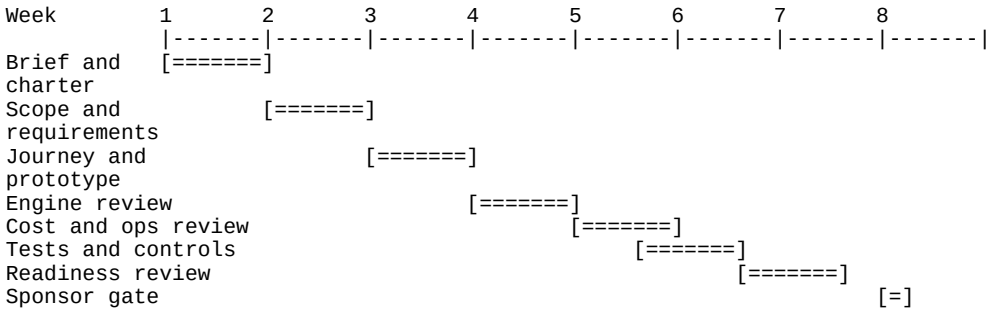
Contingency: A reserve for uncertainty.

Operating cost: A cost that continues after the product is running.

Document 15 - Project Schedule

Project: AegisShield Firewall Stage: Delivery planning Status: Initial baseline for sponsor review

Eight-week schedule



Planned work

Work	Start	Finish	Owner	Dependency
Brief and charter	Week 1	Week 2	PM / Sponsor	Sponsor handoff
Scope and requirements	Week 2	Week 3	Product / QA	Charter
Journey and prototype	Week 3	Week 4	Design / Product	Scope
Engine and technical review	Week 3	Week 5	Engineering / Security	Requirements
Cost and operations review	Week 5	Week 6	Operations / PM	Technical options
Tests and safety controls	Week 5	Week 7	QA / Security / Operations	Requirements and technical path
Pilot-readiness review	Week 7	Week 8	PM / Product / QA	Evidence from prior work
Sponsor decision gate	Week 8	Week 8	CTO / Sponsor	Evidence package

Milestones

Milestone	Target	Evidence
Charter and scope approved	End of week 2	Approved boundary and requirements plan
Prototype reviewed	End of week 4	Screen review and notes
Technical option selected for validation	End of week 5	Option matrix and conditions
Pilot controls ready	End of week 7	Test, risk, data, and recovery evidence
Sponsor decision recorded	End of week 8	Go, no-go, or defer decision

Conditions to advance

- Scope must be clear before the prototype is treated as evidence.
- A technical option must be reviewed before cost and recovery estimates are final.

- Test and data controls must be ready before pilot-readiness review.
- The sponsor decision must be recorded before any pilot build or production work.

Capacity view

The schedule assumes the part-time capacity in Document 14. Work can move inside a week when the next gate is not affected. The likely critical path is scope -> technical option -> tests and controls -> readiness evidence -> sponsor gate.

Baseline control

The sponsor approves the initial eight-week baseline at the end of week 2. A change to scope, decision date, budget boundary, or pilot conditions must be recorded with its reason and impact before the baseline is changed.

Key terms

Baseline: The approved plan used to track progress.

Milestone: A meaningful point or result in the plan.

Critical path: The chain of work that controls the final decision date.

Change control: The process for reviewing and approving a change to the plan.

Document 16 - Test and Validation Plan

Project: AegisShield Firewall Stage: Pilot planning Status: Draft for Product, Security, QA, Operations, and BookEasy review

Test purpose

Show that AegisShield Firewall can protect the agreed BookEasy test application without blocking legitimate login and booking requests, exposing unsafe data, or making the service impossible to support.

Test environment and data

- Non-production environment only.
- Synthetic requests and approved masked BookEasy examples.
- No production credentials, payment data, or unmasked customer content.
- Test users for admin and viewer roles.
- Known safe booking requests and known simulated malicious requests.
- A recorded configuration snapshot before each major test.

Test scenarios

ID	Scenario	Expected result	Owner
T-01	Legitimate login	Request is allowed and the event is recorded without sensitive values.	QA / BookEasy
T-02	Legitimate booking	Booking request is allowed and the expected event is visible.	QA / BookEasy
T-03	Simulated malicious request	Request is flagged or blocked according to the test rule.	Security / QA
T-04	Block explanation	Admin can see the matched rule and safe request details.	Product / QA
T-05	False-positive correction	Admin creates a short-lived exception and the safe booking passes after the change.	Product / Security / QA
T-06	Viewer permissions	Viewer can read approved events but cannot edit rules or exceptions.	Security / QA
T-07	Audit record	Rule and exception changes show user, time, reason, and result.	Security / QA
T-08	Service health	Operations can see healthy, warning, and failed states.	Operations / QA
T-09	Event delivery	A simulated delivery failure creates an actionable alert.	Engineering / Operations
T-10	Recovery	The team restores the last safe configuration and confirms service behavior.	Engineering / Operations
T-11	Performance	The test result is compared with the agreed pilot performance target.	Engineering / QA

ID	Scenario	Expected result	Owner
T-12	Data protection	Logs and views do not expose credentials or unapproved sensitive data.	Security

Acceptance rules

- T-01 and T-02 must pass before any block-mode test.
- T-05 must pass before the pilot is recommended.
- T-06, T-07, and T-12 must pass before access is approved.
- T-08, T-09, and T-10 must pass before Operations accepts readiness.
- T-11 must meet the performance target agreed by Engineering, Operations, and BookEasy.
- Any critical issue must have a fix, accepted limitation, or sponsor decision before the gate.

Evidence to keep

- Test case and expected result.
- Test date, environment, and tester.
- Request or event identifier using simulated values.
- Screenshot or safe log excerpt.
- Pass, fail, blocked, or not run status.
- Defect link and retest result when needed.

Key terms

Test scenario: A situation the team uses to check the product.

False-positive test: A test that checks whether a safe request is incorrectly blocked.

Retest: Running a failed scenario again after a correction.

Test evidence: The record that shows what was tested and what happened.

Acceptance rule: A condition that must pass before the work can advance.

Document 17 - Risk Register

Project: AegisShield Firewall Stage: Pilot planning Status: Week 5 simulated baseline; review weekly

Scoring guide

- Low probability: Not expected under the current plan.
- Medium probability: A credible chance exists without more information or action.
- High probability: Likely unless the team takes action.
- Low impact: Small rework with no customer or gate effect.
- Medium impact: Material rework, cost, or schedule effect.
- High impact: Customer disruption, data exposure, unsafe protection, or a blocked decision.

Initial risks

ID	Risk and consequence	Probability / impact	Prevention	Trigger	Contingency	Owner	Status
R01	A selected engine cannot meet the pilot rules or license terms.	Medium / High	Compare options early and review license questions.	Required rule or license condition fails review.	Select another engine or recommend no-go.	Engineering / Security	Open
R02	A legitimate login or booking is blocked.	Medium / High	Start in monitor mode and test safe flows first.	T-01 or T-02 fails.	Disable the rule, restore safe config, investigate, and retest.	Security / QA	Open
R03	The product adds too much request delay.	Medium / High	Define a performance target and test before pilot approval.	Performance result misses the agreed target.	Reduce scope, adjust engine settings, or defer the pilot.	Engineering / Operations	Open
R04	Sensitive request information appears in logs or event views.	Medium / High	Mask fields, limit access, and review retention.	Security finds an unapproved value.	Stop the test, remove exposure, and review affected records.	Security	Open
R05	Exceptions remain active too long or are not reviewed.	Medium / Medium	Require owner, reason, expiry, and audit record.	Exception has no owner or expiry.	Disable it and review the affected flow.	Product / Security	Open
R06	BookEasy cannot provide the people or scenarios needed for the pilot.	Medium / Medium	Confirm availability and scenarios early.	Customer review is missed or scenarios are unclear.	Move the review within available float or recommend defer.	Customer Success	Open
R07	Operations cannot support the service after handover.	Medium / High	Define monitoring, recovery, and escalation before the gate.	Runbook or recovery test is incomplete.	Keep the work in validation and do not recommend pilot launch.	Operations	Open

ID	Risk and consequence	Probability / impact	Prevention	Trigger	Contingency	Owner	Status
R08	Ongoing license and support costs are higher than expected.	Medium / Medium	Use assumptions, request vendor input, and show sensitivity.	Cost estimate exceeds the sponsor boundary.	Reduce scope, negotiate, partner, or stop the initiative.	PM / Sponsor	Open

Review rule

The PM reviews risks weekly with the owners. If a risk happens, it becomes an issue with a date, impact, owner, actions, and evidence. The baseline should not describe a later issue as if it were already known.

Key terms

Risk: An uncertain event that could affect the project.

Issue: A current problem that has happened or needs action now.

Risk owner: The role that monitors and responds to the risk.

Trigger: A sign that the risk may be happening.

Mitigation: An action that reduces the chance or impact of a risk.

Contingency: The action used if the risk happens.

Document 18 - Data Protection and Operational Readiness

Project: AegisShield Firewall Stage: Pilot planning Status: Draft for Security and Operations review

Data protection controls

Control	Expected practice	Evidence
Access	Admin and viewer permissions are separate and reviewed.	Permission test and access list
Masking	Request values that could contain secrets or personal data are masked or excluded.	Security review and safe event sample
Logging	Logs show action and result without credentials or unapproved content.	Log review
Retention	The team defines how long pilot events and audit records are kept.	Retention decision
Changes	Rules and exceptions require an owner, reason, and audit record.	Change record
Environment	Tests use synthetic or approved masked data.	Test-data checklist

Monitoring and support

Operations should be able to see:

- Service health.
- Event delivery failures.
- Rule or exception changes.
- Unusual error volume.
- Failed recovery or configuration restore.

Support should know how to report an incorrect block. The escalation path is Support -> Customer Success -> Security or Engineering, with the PM informed when the issue could affect pilot acceptance or schedule.

Recovery approach

- Stop the affected rule or return the service to monitor mode.

2. Restore the last approved safe configuration. 3. Confirm legitimate login and booking scenarios. 4. Preserve the event and audit evidence needed for investigation. 5. Communicate the result and decide whether the rule needs a correction, removal, or new test.

Handover readiness

Operations must receive:

- Service and application ownership.

- Monitoring view and alert route.
- Rule and exception change process.
- Recovery steps and last safe configuration.
- Known limits and open items.
- Support and escalation contacts.

Readiness conditions

The service is not ready for pilot approval until the data controls, monitoring, recovery rehearsal, and support path have been reviewed by Security and Operations.

Key terms

Data masking: Hiding sensitive values while keeping enough detail for a test or investigation.

Retention: How long a record is kept.

Runbook: Step-by-step instructions for operating or recovering a service.

Handover: Moving service knowledge and support responsibility to Operations.

Document 19 - Execution Board and Snapshots

Project: AegisShield Firewall Stage: Fictional execution Status: Simulated board record

> *The project board is fictional evidence. The cards and dates are created to show how the work would be tracked; they are not records from a real customer project.*

Board workflow

Pending -> In progress -> In review -> In testing -> Blocked -> Done

The Project Manager keeps the board connected to the backlog, owner, dependency, acceptance evidence, and current status.

Snapshot 1 - Week 2: planning ready

What changed: The charter, scope, requirements, owners, and first schedule are ready.

Pending	In progress	Done
Engine comparison	Scope and acceptance checklist	Charter approved
Prototype review	Customer scenarios	Sponsor discovery decision
Test controls		Stakeholders assigned

Snapshot 2 - Week 6: issue found

What changed: During a safe booking test, the rule “Unexpected request pattern” blocked a legitimate booking. Pilot approval is blocked while the team investigates.

Pending	In progress	Blocked	Done
Pilot readiness review	Investigate APP-ISS-01	BookEasy pilot decision	Engine option review
Sponsor evidence pack	Reproduce safe booking flow	Block mode test	Prototype review
	Prepare rule correction		Test controls drafted

Snapshot 3 - Week 7: correction verified

What changed: The rule was changed to monitor mode, the safe booking passed, and the revised rule passed a controlled block test. The issue is closed for the pilot scope.

Pending	In review	Done
Sponsor decision	Pilot evidence	APP-ISS-01 closed
BookEasy acceptance	Security review	Legitimate booking passed
	Operations readiness	Exception audit passed

Snapshot 4 - Week 8: decision complete

What changed: BookEasy accepted the agreed pilot scenarios. The sponsor approved a controlled pilot build and did not approve production rollout.

Pending	In review	Done
Future production plan	Lessons learned	Pilot accepted
Product roadmap	Cost assumptions	Controlled pilot approved
		Handover plan ready

Key terms

Board snapshot: A saved view of work at a specific point in time.

Blocked: Work cannot continue until a condition or decision is resolved.

Issue card: A board item that records a current problem and its follow-up.

Status: The current position of a work item.

Document 20 - Issue Log

Project: AegisShield Firewall Issue: APP-ISS-01 Stage: Week 6 to week 7 simulated execution Status: Closed for pilot scope

Issue summary

Field	Record
Detected	Week 6 during a safe BookEasy booking test
Description	The rule “Unexpected request pattern” blocked a legitimate booking request.
Impact	The booking flow could not be treated as safe for pilot approval.
Priority	High
Owner	Security Lead with Engineering and QA support
Related requirement	APR-05 and APR-06
Current status	Closed in week 7
Customer impact	No production impact; the issue was found in the controlled test environment.

Investigation

The team reproduced the request with a known safe test user. The request matched a broad rule pattern. The rule was working as configured, but the rule scope was too broad for the agreed BookEasy booking path.

Options considered

Option	Result
Leave the rule active and continue the pilot	Rejected because the safe booking would remain blocked.
Disable the rule and stop all protection testing	Rejected because the team would lose the controlled block scenario.
Move the rule to monitor mode, narrow its scope, and retest	Selected because it protects the safe flow while keeping a controlled test path.
Create a permanent broad exception	Rejected because it could create an unsafe bypass.

Correction and retest

- Moved the rule to monitor mode.

2. Narrowed the rule to the intended test request pattern. 3. Added an approved, time-limited exception for the safe booking path. 4. Retested login, booking, block, event detail, exception, and audit behavior. 5. Removed the test exception after the scenario passed.

Closure evidence

- Legitimate login passed.

- Legitimate booking passed.
- Simulated malicious request was blocked in the controlled test.
- Event detail showed the matched rule and safe request identifier.
- Viewer could not change the rule.
- Exception had an owner, reason, expiry, and audit record.

Key terms

Issue: A current problem that needs action.

Root cause: The reason the problem happened.

False positive: A safe request incorrectly treated as a threat.

Retest: Repeating the failed scenario after the correction.

Closure evidence: Proof that the issue was resolved for the agreed scope.

Document 21 - Decision and Change Log

Project: AegisShield Firewall Stage: Fictional execution Status: Simulated decision record

Decision DEC-APP-01 - Safe response to APP-ISS-01

Field	Record
Requested by	Security Lead and Project Manager
Date	May 8, 2026 (simulated)
Problem	A legitimate booking was blocked by a broad test rule.
Decision	Move the rule to monitor mode, narrow the rule, use a time-limited exception, and retest.
Decision owner	Security Lead
Approver	Product Lead and Sponsor informed
Result	Approved for controlled test correction.

Schedule decision

No schedule change was approved. The correction used the testing buffer already included in weeks 6 and 7. The week-8 sponsor gate remained unchanged.

Why this option was selected

It protected the legitimate booking flow, kept the test safe, avoided a permanent bypass, and allowed the team to collect evidence before recommending a pilot build.

Follow-up actions

Action	Owner	Due	Status
Record the rule change and test result	Security / QA	Week 7	Done
Confirm the exception expiry and removal	Product / Security	Week 7	Done
Update pilot readiness evidence	PM	Week 7	Done
Tell BookEasy what changed and what was tested	Customer Success	Week 7	Done

Key terms

Decision log: A record of an important choice and why it was made.

Change: A change to a rule, scope, schedule, cost, or approved plan.

Buffer: Time or capacity held for expected uncertainty.

Permanent bypass: A broad exception with no clear end or review.

Document 22 - Project Status Report

Project: AegisShield Firewall Reporting period: Weeks 5-6 Issue date: May 8, 2026 (simulated) Status: Amber - recovery action in progress

Summary

The team completed the prototype, technical option review, and most test controls. During a safe booking test, a rule blocked a legitimate request. The issue is contained in the test environment, but pilot readiness cannot be approved until the rule is corrected and retested.

Status by area

Area	Status	Update
Scope	Green	First-release scope remains unchanged.
Product design	Green	Prototype review is complete.
Technical option	Green	Established engine path remains feasible pending final license confirmation.
Customer validation	Amber	BookEasy booking scenario is blocked until APP-ISS-01 closes.
Security and data	Amber	Rule correction and event-data review are in progress.
Schedule	Green	Week-8 sponsor gate remains forecast.
Budget	Green	No change to the simulated estimate.

Recommendation

Keep the baseline and complete the correction inside the existing testing buffer. Do not approve pilot readiness until the safe booking, controlled block, permissions, audit, and data-protection scenarios pass again.

Decision needed

The sponsor should confirm that the team may continue with the same scope and schedule while the issue is corrected. No production protection is requested.

Key terms

Status report: A short update on progress, risks, decisions, and next steps.

Amber: A concern needs action, but there is still a reasonable path to continue.

Forecast: The current expectation for a future result.

Baseline: The approved plan used for comparison.

Document 23 - Pilot Test Results and BookEasy Acceptance

Project: AegisShield Firewall Stage: Week 7 simulated pilot review Status: Accepted with conditions for a controlled pilot build

> *These results are simulated. They do not show real security performance or a real customer approval.*

Test results

Scenario	Result	Evidence
Legitimate login	Pass	Safe test request allowed and event recorded.
Legitimate booking	Pass after APP-ISS-01 correction	Booking request allowed after rule scope was narrowed.
Simulated malicious request	Pass	Controlled test request was blocked.
Block explanation	Pass	Event showed matched rule, action, time, and safe identifier.
Exception flow	Pass	Exception had owner, reason, expiry, and audit record.
Viewer permissions	Pass	Viewer could not edit rules or exceptions.
Data protection	Pass	No credentials or unapproved sensitive values were shown in test evidence.
Recovery	Pass for configuration restore	Last safe configuration was restored and safe booking was checked again.
Performance	Pending final target confirmation	Engineering and Operations must confirm the target before production use.

BookEasy review

The simulated BookEasy representative reviewed the agreed login, booking, block, event, and exception scenarios. BookEasy accepted the results for the controlled pilot scope with the following conditions:

- The pilot remains in a non-production environment.
- Production blocking is not approved by this record.
- Exceptions require an owner, expiry, and review.
- The performance target must be confirmed before any future production decision.
- Customer Success receives the support and escalation path.

Acceptance decision

Decision: Accepted with conditions for controlled pilot build planning. Accepted by: BookEasy representative, simulated. Date: May 15, 2026 (simulated). Next decision: Sponsor go/no-go for controlled pilot build.

Key terms

Pilot: A limited test with a defined customer, environment, and scope.

Acceptance: The customer confirms that the agreed scenarios met the expected result.

Condition: A requirement that must remain true for the acceptance to apply.

Production: The live environment used by real customers.

Document 24 - Go-No-Go and Release Record

Project: AegisShield Firewall Stage: Week 8 sponsor gate Status: Simulated decision record

Decision requested

Decide whether to authorize a controlled AegisShield Firewall pilot build using the established security engine path and the approved BookEasy test scope.

Evidence reviewed

- Approved brief, charter, scope, and requirements.
- Product prototype and BookEasy review.
- Engine comparison and license questions.
- Test results and APP-ISS-01 closure evidence.
- Data-protection, monitoring, and recovery controls.
- Simulated budget and capacity estimate.
- Open conditions and known limits.

Decision

GO: Authorize a controlled pilot build and pilot-readiness work for one BookEasy web application in a non-production environment.

NO-GO: Do not authorize production protection, customer rollout, or a proprietary engine.

Conditions

- Final engine license terms are confirmed.
- Performance target is agreed before any production discussion.
- Monitor mode remains the default until separate evidence supports block mode.
- BookEasy confirms the test window and participants.
- Security and Operations sign off on data, monitoring, recovery, and support controls.

Execution record

Field	Record
Decision date	May 22, 2026 (simulated)
Decision maker	CTO / Project Sponsor
Recommendation	GO for controlled pilot build; NO-GO for production
Scope version	AegisShield Firewall first version v1.0
Environment	Non-production BookEasy test environment

Field	Record
Rollback	Restore last approved safe configuration
Open items	License confirmation and performance target

Key terms

Go: Proceed under the stated conditions.

No-go: Do not proceed until the blocking conditions are resolved.

Release gate: A review that must pass before a product change moves forward.

Known limit: A boundary or condition the team has not solved or approved for broader use.

Document 25 - Stabilization and Operations Handover

Project: AegisShield Firewall Stage: Controlled pilot build close-out Status: Simulated handover record

Stabilization period

The team monitors the controlled pilot build for five business days. During this period, the default mode is monitor, the rule and exception audit is reviewed, and the support path is tested.

Handover checklist

Item	Receiving role	Result
Service overview and application ownership	Operations Lead	Accepted for controlled pilot support
Health view and alert route	Operations Lead	Reviewed and tested
Rule and exception process	Security Lead	Reviewed; expiry and approval required
Safe configuration restore	Engineering / Operations	Rehearsed successfully
Known limits	Product / Support	Recorded and shared
Customer support message	Customer Success / Support	Reviewed with BookEasy
Escalation path	Support / Security / Engineering	Confirmed

Known limitations

- The product is validated only for one BookEasy test application.
- Production performance is not proven by this case.
- The security engine and license terms require final confirmation.
- The prototype and simulated evidence do not prove real-world threat coverage.
- Block mode requires separate approval and more evidence.

Handover decision

Operations accepts the service for the limited controlled pilot scope. This acceptance does not approve production rollout or a broader customer launch.

Key terms

Stabilization: The period after a change when the team watches service health and resolves early issues.

Handover: Transfer of service knowledge and support responsibility to Operations.

Escalation path: The route for raising a problem to the right team.

Known limitation: A confirmed boundary that users must understand.

Document 26 - Project Closure and Lessons Learned

Project: AegisShield Firewall Stage: Closure Status: Simulated sponsor acceptance

Outcome

The project completed the approved product-definition and technical-validation stage in week 8. The team did not claim a production launch. It produced a clear first-release boundary, prototype, technical path, cost estimate, test evidence, issue resolution, pilot acceptance, and operations handover for the controlled pilot build.

Results against the approved boundary

Objective	Result
Define a limited first version	Completed for one BookEasy web application.
Test the customer problem	Simulated findings supported guided setup, clear event detail, and safe exception handling as the main value to test.
Confirm a technical direction	Established engine path recommended, subject to license and performance conditions.
Protect legitimate bookings	APP-ISS-01 was corrected and the agreed booking scenario passed.
Prepare a safe pilot decision	Completed with GO for controlled pilot build and NO-GO for production.
Prepare operations	Monitoring, recovery, support, and escalation were handed over for the limited scope.

Scope, schedule, and budget

- The approved eight-week planning baseline was met.
- The simulated budget estimate remained $58,650 for planning and validation.
- No production budget or customer rollout funding was approved.
- No schedule change was required because the false-positive correction used the planned testing buffer.

Lessons learned

Lesson	Owner for future use	Action
Test safe customer flows before block behavior.	Security / QA	Add login and booking scenarios before any block test.
Make exceptions temporary and auditable.	Product / Security	Require owner, reason, expiry, and review.
Treat engine licensing as an early dependency.	Engineering / Sponsor	Request license terms before final cost approval.
Keep the first product boundary small.	Product / PM	Use one application and a limited rule set before expanding.
Keep the prototype honest.	Design / PM	Label simulated screens and separate them from functional evidence.

Practices to repeat

- Use simple customer scenarios to guide requirements.
- Review monitor mode before block mode.
- Link issues to requirements and test evidence.
- Keep Operations involved before the launch decision.

Closure approval

Approved by: CTO / Project Sponsor, simulated. Date: May 29, 2026 (simulated). Closure result: Stage complete; controlled pilot build authorized under conditions.

Key terms

Closure: The formal end of the approved project stage.

Lesson learned: A useful insight to apply to future work.

Outstanding item: Work that remains open and needs an owner and date.

Resource release: Returning team capacity after the stage ends.

Document 27 - Portfolio Summary

Project: AegisShield Firewall Case type: Fictional product discovery and controlled pilot planning

The problem

AegisShield wanted to evaluate a new product that could protect customer web applications without making legitimate bookings fail. The case focused on BookEasy, an existing SIEM customer with an online scheduling application.

My role in the case

As Project Manager, I turned the sponsor request into a clear stage, coordinated Product, Engineering, Security, Design, Operations, QA, Customer Success, and BookEasy, and kept the work connected through scope, backlog, risks, decisions, tests, and handover.

Main decisions

- Keep the first version limited to one BookEasy web application.
- Evaluate an established security engine instead of assuming a proprietary engine.
- Start in monitor mode before testing blocks.
- Require safe exception handling, audit records, access control, and recovery evidence.
- Approve a controlled pilot build but not production rollout.

What happened in execution

A simulated rule blocked a legitimate booking in the test environment. The team moved the rule to monitor mode, narrowed the rule, created a time-limited exception, retested the flow, and closed the issue without changing the eight-week plan.

Outcome

The fictional case ended with a sponsor-approved controlled pilot build, BookEasy acceptance of the agreed scenarios, a clear set of known limitations, and an operations handover. It does not claim a real customer launch, working security protection, or real research results.

Evidence included

- Product discovery and sponsor decision.
- Project brief, charter, requirements, and stakeholder plan.
- Prototype and administrator journey.
- Technical approach, WBS, RACI, backlog, budget, capacity, and schedule.
- Test plan, risk register, data controls, issue log, and decision record.
- Pilot acceptance, release decision, handover, closure, and lessons learned.

Key terms

Portfolio case: A structured example used to show how work is planned and managed.

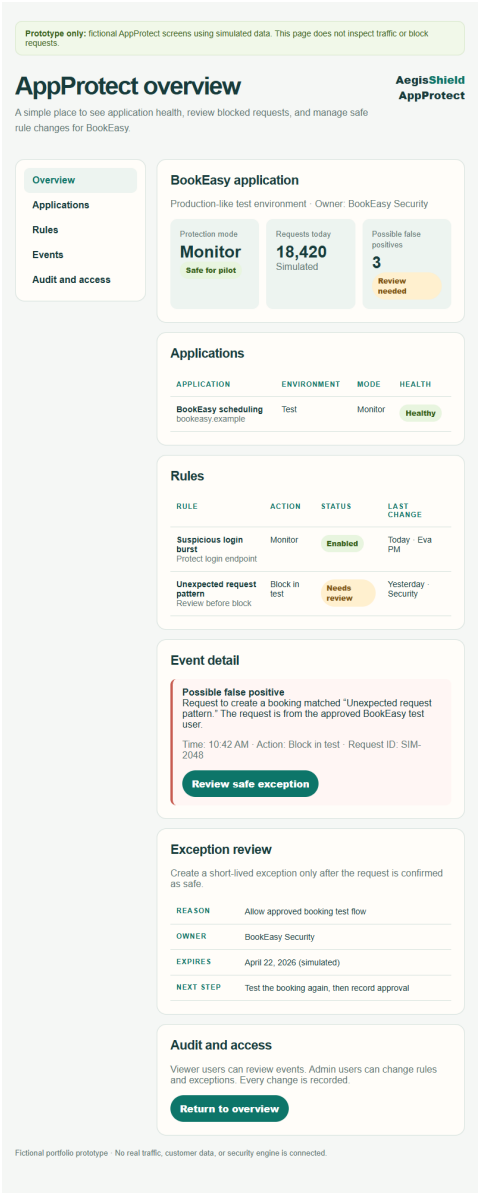
Simulated outcome: A fictional result created for learning and demonstration.

Evidence: A document, test result, decision, or visual record that supports a project claim.

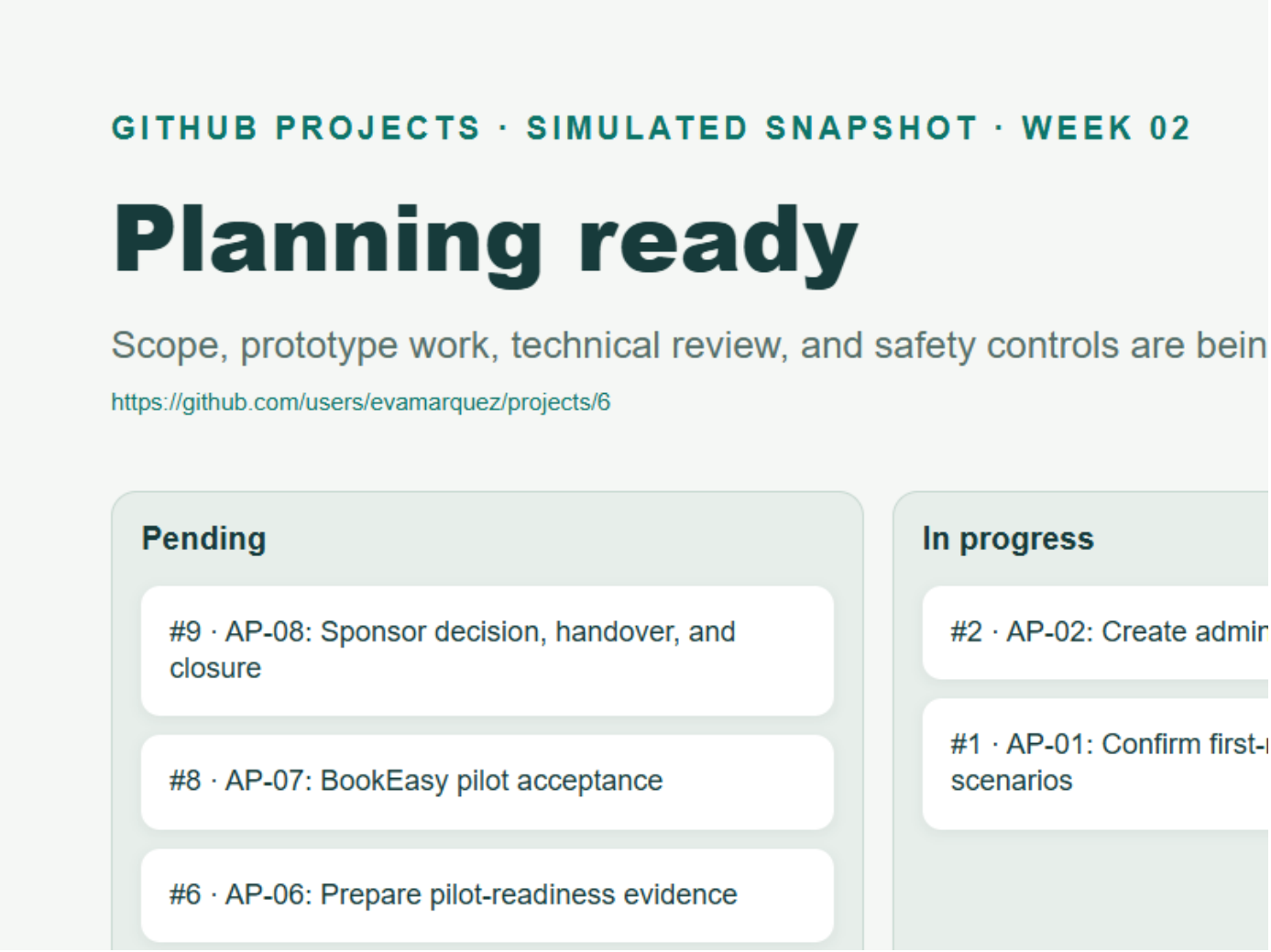
Evidence images

These images support the fictional case. The board captures are generated from the linked GitHub Projects data, and the prototype is a visual, non-functional concept.

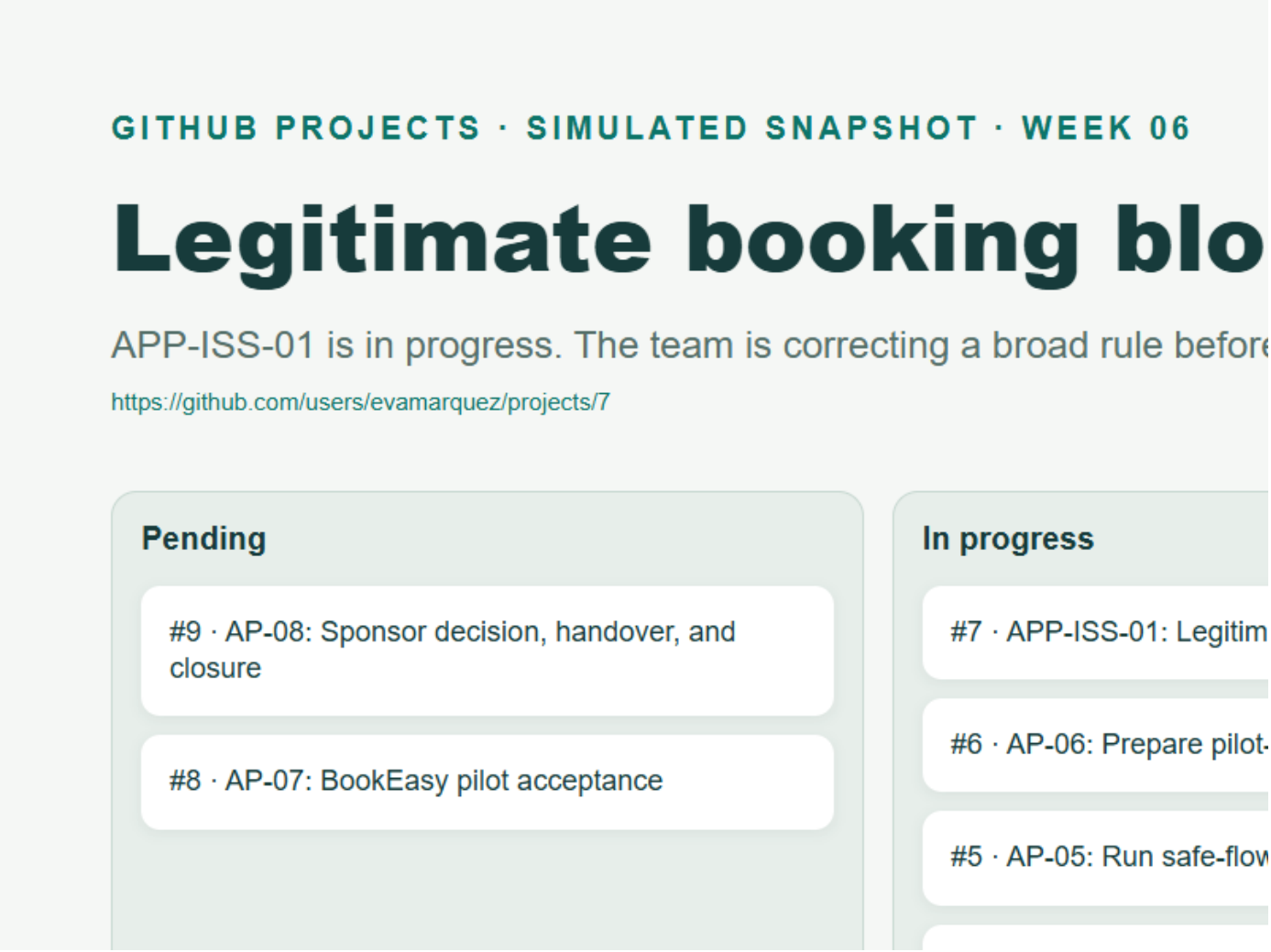
Appprotect Prototype



Github Board Week 02



Github Board Week 06



Github Board Week 08

