

HELIOS / AI TRUST & PDP SECURITY PARTNER BOOTCAMP 2026

FGD Workbook

Secure AI. Protect Data. Build Digital Trust.

Six Indonesia-focused scenarios for mapping customer risks to the Helios security portfolio. PDP means personal data protection.

FGD MISSION

Build one customer story that connects a business or personal-data risk to a practical security design and a clear next step. Start with discovery. Show where each control fits and what evidence will prove it works.

ONE ACCOUNT TEAM, ONE CUSTOMER STORY

SALES / lead the business conversation - Define the trigger and business impact. - Ask discovery questions and map decision makers. - Connect the risk to a commercial opportunity. - Close with a specific customer decision.	PRESALES / make the controls credible - Map data, systems, access paths, and trust boundaries. - Place controls at the relevant points. - State integrations, dependencies, and assumptions. - Design the pilot and success criteria.
---	--

FORMAT AND PRIZE

PREP	PITCH	PANEL Q&A	TEAM RULE
45 minutes	8 minutes	2 minutes	Every member speaks

Each group has a 10-minute slot. The group with the highest score wins the prize.

WHAT EVERY GROUP SHOULD PRESENT

- The customer problem, discovery insights, stakeholders, and cost of doing nothing.
- A simple view of data, applications, vendors, users, and control points.
- A recommendation in no more than three moves, led by the most relevant portfolio roles.
- A realistic workshop, assessment, or pilot with proposed measures and a commercial next step.

THE SIX SOLUTION ROLES

GOVERN	ASSESS	CONTROL	PROTECT	DETECT	TRUST
OneTrust	SecurityScorecard	Cloudflare	Sangfor	Darktrace	Utimaco

The companies and scenarios are fictional. Public incidents are comparison points, not Helios customers or proof of a similar incident at an Indonesian company. Product capabilities below follow the supplied bootcamp brief. Legal interpretations, product scope, licensing, and implementation details should be validated with the customer and principal.

JUDGING / 100 POINTS

How the pitch will be scored

The panel plays the customer. Strong teams understand the situation, choose a sound control path, explain value, and answer questions clearly.

CRITERION	WHAT THE PANEL IS LOOKING FOR	POINTS
Discovery & Business Framing	The team understands the customer, trigger, data or service at risk, stakeholders, and cost of inaction. It asks before recommending.	20
Solution Fit & Technical Accuracy	The architecture fits the scenario. The team maps the six Helios roles accurately, places controls at the right point, and avoids overclaiming.	25
Value Articulation & Commercial Outcome	The team explains a customer outcome, proposes a measure, and gives a credible commercial next step with a clear partner role.	20
Objection Handling & Differentiation	The team acknowledges pushback, answers with relevant evidence or a validation plan, and differentiates without dismissing existing controls.	20
Delivery & Structure	The pitch has a clear opening, logical flow, useful handoffs, and a specific close. Everyone speaks and the pitch finishes within 8 minutes.	15
TOTAL AVAILABLE	8-minute pitch + 2-minute panel Q&A = 10 minutes per group.	100

PANEL SCORE SHEET

DISCOVERY	SOLUTION FIT	VALUE	OBJECTIONS	DELIVERY	TOTAL
____ / 20	____ / 25	____ / 20	____ / 20	____ / 15	____ / 100

JUDGING NOTE

Score the team's decisions, not the number of products named. Give credit for a clear control boundary, a realistic sequence, stated assumptions, and an honest plan to verify unknowns.

USE CASE 01 / PDP + CRYPTOGRAPHIC TRUST

Retiring old systems without leaving customer records behind

SECTOR Banking & multifinance LEVEL CORE LEAD WITH OneTrust + Utimaco

REAL-WORLD REFERENCE

In 2022, the U.S. SEC said Morgan Stanley Smith Barney failed to safeguard customer information during hardware decommissioning. Thousands of devices were sold to a third party; some recovered devices held unencrypted customer data. The SEC also said the firm failed to monitor the disposal vendor's work. [Read the public source](#)

CUSTOMER

PT DanaRoda Finance (fictional) has 60 branches, a hybrid cloud, loan and collections systems, and a planned server refresh. Drives from branches and a small data center will be handled by an external disposal provider. The data protection officer asks what borrower data remains on the devices and what proof will be retained.

WHAT IS GOING WRONG

- The asset list identifies servers but does not show which personal data each one may hold.
- The disposal provider uses subcontractors; access, custody, and destruction evidence are not gathered in one place.
- Some systems support encryption, but the customer has not confirmed where it is enabled or who controls the keys.
- Risk, IT, procurement, and the data protection officer are preparing separate answers.

WHAT THEY ARE TRYING TO ACHIEVE

Build a defensible view of the data and vendor relationship, confirm where encryption and key control apply, and establish an evidence-based retirement process. The process itself still needs operational controls for wiping or destruction.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
GOVERN / OneTrust	Data inventory, privacy governance, risk and assessment.	Map affected systems, data categories, processing purpose, and owners. It does not wipe or certify a disk.
ASSESS / SecurityScorecard	External posture and third-party or supply-chain risk.	Use as one input to vendor review. It does not prove secure media handling or replace contract evidence.
TRUST / Utimaco	HSM, KMS, cryptographic trust, and key lifecycle.	Assess key custody for encrypted systems. Key management does not destroy retired media.

SUGGESTED TALK TRACK ANGLE

Start with the decommissioning event and the data at risk. Recommend three moves: map data and systems, review the vendor and chain of custody, then confirm encryption and key responsibilities where applicable. Ask the customer to agree on the evidence required for each retired asset.

OBJECTIONS TO EXPECT FROM THE PANEL

- "Our disposal vendor already gives us a certificate."
- "Those drives are old. They probably contain no live customer data."
- "Encryption is enabled, so we are covered."

USE CASE 02 / RANSOMWARE + PDP RESPONSE

A ransomware incident disrupts clinical services and patient records

SECTOR Healthcare LEVEL CORE LEAD WITH Sangfor + Darktrace

REAL-WORLD REFERENCE

The Irish Health Service Executive’s post-incident report says the 2021 Conti ransomware attack led it to shut down IT systems and disconnect networks, causing significant disruption to healthcare. The report also describes data exfiltration before ransomware detonation. [Read the public source](#)

CUSTOMER

Bina Sehat Hospital Group (fictional) operates nine hospitals and 30 clinics in three provinces. A suspicious account has accessed a shared file service. Some endpoints show encryption activity, while the clinical team needs patient records, laboratory results, and appointment systems to keep care moving.

WHAT IS GOING WRONG

- The security team must distinguish affected user devices, shared services, and clinical systems quickly.
- IT, SOC, and hospital operations do not share one incident picture or agreed escalation path.
- The data protection officer needs to identify which patient and employee data may be involved.
- A vendor supports part of the hospital environment, but its role and access during containment are unclear.

WHAT THEY ARE TRYING TO ACHIEVE

Contain and investigate the activity, preserve clinical continuity, identify potentially affected data and vendors, and prepare a recovery and communications plan owned by the right teams.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
PROTECT / Sangfor	Endpoint, NGFW, NDR, workload and network cyber defense.	Map defenses to user devices, servers, and network paths. Product coverage does not replace an incident-response and recovery plan.
DETECT / Darktrace	Behavioral detection, investigation, and response.	Use available telemetry to investigate unusual accounts, traffic, or data movement. Confirm integrations and response authority.
GOVERN / OneTrust	Privacy, data inventory, risk and assessment.	Help map affected data and processing context. It is not the tool that detects or contains ransomware.
ASSESS / SecurityScorecard	External vendor and supply-chain posture.	Use as a vendor-risk input; it does not establish the incident’s cause.

SUGGESTED TALK TRACK ANGLE

Open with the patient-service impact. Agree on the decision path for containment, investigation, and clinical workarounds. Map the security controls to endpoints, network traffic, and workloads, then use a tabletop or scoped assessment to test escalation and recovery assumptions.

OBJECTIONS TO EXPECT FROM THE PANEL

- “We cannot disconnect clinical systems.”
- “We already have backups. Why add more controls?”
- “Can the platform confirm exactly which patient records were taken?”

USE CASE 03 / THIRD-PARTY ACCESS

A supplier account becomes a path into the distribution network

SECTOR Retail & distribution LEVEL CORE LEAD WITH SecurityScorecard + Cloudflare

REAL-WORLD REFERENCE

A U.S. Senate Commerce Committee staff report on the 2013 Target breach described third-party HVAC access, missed warnings, and movement into more sensitive systems. Use it as a vendor-access and control-boundary reference. [Read the public source](#)

CUSTOMER

PT PasarLintas Nusantara (fictional) runs 180 supermarkets and regional distribution centers. Refrigeration, point-of-sale, and warehouse systems are supported by several vendors. One supplier needs remote access for urgent maintenance, and customer loyalty data moves between stores and the central platform.

WHAT IS GOING WRONG

- Vendor accounts are shared across shifts and are not reviewed consistently after maintenance windows.
- The company has limited visibility into the supplier’s external cyber posture and subcontractor relationships.
- The route from a vendor connection to business applications is not clearly documented.
- Security alerts show unusual access, but analysts lack an agreed owner and response process.

WHAT THEY ARE TRYING TO ACHIEVE

Prioritize the suppliers that can affect critical operations or personal data, clarify each access path, and test controls on one vendor and one application before expanding.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
ASSESS / SecurityScorecard	External posture and supplier or supply-chain risk.	Prioritize vendor review. This is a risk signal, not a guarantee that a supplier is secure.
CONTROL / Cloudflare	SSE, application controls, and relevant access or data policies.	Identify which in-scope app or traffic path can be governed. Confirm the deployed service and policy coverage.
PROTECT / Sangfor	Endpoint, NGFW, NDR, workload and network defense.	Map protections to the assets in the vendor path. Do not assume segmentation exists without design evidence.
DETECT / Darktrace	Behavioral analytics, anomaly detection, investigation and response.	Test what relevant telemetry is available and who can act on an alert.

SUGGESTED TALK TRACK ANGLE

Lead with vendor access to stores and distribution, not with a score or product. Map the account, device, application, data, and owner. Pilot a narrower access path with one vendor, then test alert routing and offboarding evidence.

OBJECTIONS TO EXPECT FROM THE PANEL

- “Our vendor needs broad access to fix urgent problems.”
- “The vendor has a security certification.”
- “We already have a firewall between the vendor and our systems.”

USE CASE 04 / APPLICATION + API SECURITY

A customer portal exposes records through a misconfigured path

SECTOR Digital finance LEVEL ADVANCED LEAD WITH Cloudflare + Darktrace

REAL-WORLD REFERENCE

U.S. Department of Justice case materials on the Capital One incident describe a misconfigured web application firewall that enabled access to stored data. Use it to discuss app configuration and access paths; it is not an AI incident. [Read the public source](#)

CUSTOMER

PT KreditMaju Digital (fictional) serves customers through a mobile app and partner APIs. A planned promotion increases traffic. The CISO is asked whether customer records can be retrieved through application paths that were not part of the latest test.

WHAT IS GOING WRONG

- The application and API inventory is split across product teams and a cloud service provider.
- A firewall is in place, but ownership of rule changes, exceptions, and origin exposure is not clear.
- Application logs and SOC alerts are reviewed in separate tools, slowing investigation.
- Teams cannot quickly map an exposed endpoint to the personal data and processing purpose involved.

WHAT THEY ARE TRYING TO ACHIEVE

Confirm the application and API paths, apply the right controls at the agreed enforcement point, and test detection and escalation without disrupting customer access.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
CONTROL / Cloudflare	SSE, DLP, AI access, AI Gateway, and application controls.	Map relevant application/API controls to the exposed public path. Validate policy, configuration, and origin assumptions.
DETECT / Darktrace	Behavioral detection, investigation, and response.	Test whether the available telemetry can surface unusual access or data movement and reach the responsible team.
PROTECT / Sangfor	Endpoint, NGFW, NDR, workload and network defense.	Consider protections for the in-scope workload and supporting network. It does not replace application testing.
GOVERN / OneTrust	Data inventory, privacy governance, risk and assessment.	Identify the personal data involved and help assess impact; it does not fix an application configuration.

SUGGESTED TALK TRACK ANGLE

Ask which endpoint or data path is in scope and who owns each change. Show the path from customer request to API, application, and stored data. Propose a time-boxed configuration and exposure review, then validate the control with an agreed test and business-safe rollback plan.

OBJECTIONS TO EXPECT FROM THE PANEL

- "We already have a WAF."
- "The cloud provider owns the security configuration."
- "We cannot risk changing the portal before the promotion."

USE CASE 05 / MANUFACTURING RESILIENCE

A cyber incident interrupts production and supplier transactions

SECTOR Food manufacturing LEVEL ADVANCED LEAD WITH Sangfor + Darktrace

REAL-WORLD REFERENCE

JBS said its 2021 cyberattack affected some IT servers supporting North American and Australian systems and could delay customer and supplier transactions. The company said its backup servers were unaffected at the time. [Read the public source](#)

CUSTOMER

PT Mekar Pangan Nusantara (fictional) has six processing plants across Java and Sumatra, central ERP, plant-level systems, and a two-person security team. A cyber incident has taken several user devices and a shared business service offline during a high-volume production week.

WHAT IS GOING WRONG

- Plant teams, central IT, and the SOC have different views of the affected assets and business dependencies.
- The company needs to decide what can be isolated without creating a safety or production risk.
- External maintenance providers have access to some support systems, but the current inventory is incomplete.
- Backups exist, but restore ownership, priorities, and recovery evidence have not been exercised together.

WHAT THEY ARE TRYING TO ACHIEVE

Protect and investigate the affected environment while operations leaders decide safe workarounds and recovery priorities. Make vendor access and recovery dependencies visible before expanding controls.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
PROTECT / Sangfor	Endpoint, NGFW, NDR, workload and network defense.	Map coverage to user devices, shared services, and plant support systems. Validate any OT boundary with operations.
DETECT / Darktrace	Behavioral detection, investigation, and response.	Use available signals to investigate unusual behavior and agree who can contain or escalate. No detection tool guarantees discovery of every attack.
ASSESS / SecurityScorecard	External posture and supplier or supply-chain risk.	Prioritize review of critical service providers; validate access and continuity evidence separately.
TRUST / Utimaco	HSM, KMS, and cryptographic key lifecycle.	Include only where encrypted backup or application key custody is in scope. It does not provide backup or restore.

SUGGESTED TALK TRACK ANGLE

Open on production continuity and safe decision-making. Map business services to assets and suppliers. Recommend a limited control review and tabletop, with operations defining safety boundaries and a recovery owner for each critical service.

OBJECTIONS TO EXPECT FROM THE PANEL

- “Our plants cannot stop for a security exercise.”
- “We have backups, so recovery is already covered.”
- “The vendor manages that system for us.”

USE CASE 06 / AI + PDP

A claims team wants AI summaries without sharing raw personal data

SECTOR Insurance LEVEL CORE LEAD WITH OneTrust + Cloudflare

REAL-WORLD REFERENCE

In 2023, Italy's Data Protection Authority temporarily limited ChatGPT's processing of Italian users' data and raised concerns about personal-data collection and information provided to users. Use it as a privacy-governance reference, not as a corporate breach. [Read the public source](#)

CUSTOMER

PT AmanKita Asuransi (fictional) is piloting an AI assistant for claims and contact-center teams. Claims files may contain national ID numbers, health details, accident reports, bank information, and vendor correspondence. Business leaders want faster case handling; the data protection officer wants clear boundaries.

WHAT IS GOING WRONG

- Staff test public and vendor AI tools with real claim examples because there is no approved workflow.
- The company has not confirmed what prompt data and outputs the vendor retains or which subprocessors can access them.
- There is no agreed data-minimization rule for summaries or a clear owner for AI use-case approval.
- A blanket block may push users to personal devices and leave the business without visibility.

WHAT THEY ARE TRYING TO ACHIEVE

Inventory the AI use case and personal data, set an approved path, minimize what enters prompts, review the provider, and measure whether the workflow is useful without promising a compliance outcome.

SECURITY SOLUTION MAP

HELIOS ROLE / PRINCIPAL	CAPABILITY FROM THE BRIEF	FIT IN THIS CASE / BOUNDARY
GOVERN / OneTrust	AI governance, privacy, data inventory, risk and assessment.	Register the use case, data, purpose, owner, and assessment actions. Legal and the data protection officer own legal interpretation.
CONTROL / Cloudflare	SSE, DLP, AI access, AI Gateway, and application controls.	Apply in-scope prompt and access policies on the agreed traffic path. Test policy coverage; it does not govern every unmanaged device automatically.
ASSESS / SecurityScorecard	External vendor and supply-chain posture.	Add external posture signals to vendor review alongside contract and data-handling evidence.
DETECT / Darktrace	Behavioral detection, investigation, and response.	Consider only if relevant telemetry is available; it does not automatically reveal every prompt sent to an external AI service.
TRUST / Utimaco	HSM, KMS, and cryptographic key lifecycle.	Assess key custody for sensitive backend data if required by the architecture.

SUGGESTED TALK TRACK ANGLE

Start with the claims workflow and the personal data it uses. Show three moves: govern the use case, control the approved prompt path, and test whether data minimization still gives useful summaries. Agree on a small pilot with the claims owner, data protection officer, Security, and the AI provider.

OBJECTIONS TO EXPECT FROM THE PANEL

- “The AI vendor says it does not train on our data.”
- “We already pay for an enterprise AI license.”
- “Can this make us compliant with PDP requirements?”

PITCH PREP TOOLKIT / 45 MINUTES

Build the customer argument

Use prep time to agree on the problem, sketch the control path, assign speaking parts, and rehearse the opening and close.

TIME	TEAM TASK	LEAD	OUTPUT
0–8 min	Choose the customer, trigger, and one main business or PDP risk. State assumptions.	Sales	Account hypothesis
8–15 min	Choose three discovery questions and map sponsor, user, owner, and blocker.	Sales	Stakeholder map
15–25 min	Draw the data, application, vendor, identity, and system paths. Mark trust boundaries.	Presales	Logical architecture
25–33 min	Choose up to three portfolio moves. Distinguish Govern, Assess, Control, Protect, Detect, and Trust.	Together	Control journey
33–40 min	Set the assessment or pilot scope, success measures, assumptions, owners, and next step.	Together	Pilot and ask
40–45 min	Rehearse the opening, handoffs, likely objections, and close.	Everyone	Pitch ready for 8 minutes

EVERY MEMBER HAS A PART

SALES	PRESALES	JOINT HANDOFF
Open with the customer context, business risk, stakeholders, value, and commercial ask.	Explain the path, control points, dependencies, pilot design, and success criteria.	Make the handoff clear: “Now we will show where the data or service is controlled.” Close with a specific decision request.

DISCOVERY QUESTIONS: CHOOSE TWO OR THREE

- What changed and made this a priority now?
- Which data, service, or business process is most exposed?
- Where does the personal or confidential data move, and who can access it?
- Which vendors or subcontractors can reach these systems or data?
- What security controls already exist, and where are the gaps or unclear boundaries?
- Who owns the operational decision if a system needs to be isolated?
- What would the customer measure to decide whether a pilot worked?

PITCH PREP TOOLKIT / 10 MINUTES PER GROUP

An 8-minute pitch, then 2 minutes of Q&A

The panel plays the customer. Keep the pitch focused on a customer decision, not a catalogue of features.

TIME	SECTION	WHAT TO COVER
0:00–0:45	Open in their world	Name the customer, business moment, and one-sentence problem.
0:45–2:00	Problem and cost	Choose two or three consequences: service disruption, data exposure, manual work, lost time, or vendor dependency. Explain the cost of doing nothing.
2:00–3:30	Recommendation in three moves	Say what comes first, second, and third, and why. Show judgment with a clear order.
3:30–5:15	How it works	Draw user/vendor > app or system > company data/service. Mark governance, app/API, SSE/DLP, endpoint/network, detection, third-party risk, and key controls where relevant.
5:15–6:15	Value and proof	Name a customer outcome and one baseline or measure to test. Do not invent a benchmark.
6:15–7:30	Commercial next step	Propose a workshop, assessment, or PoC with scope, duration, owners, dependencies, and agreed success criteria.
7:30–8:00	Close and ask	Restate the outcome and ask the panel for a specific decision.
8:00–10:00	Panel Q&A	Acknowledge the concern, connect it to a business risk, give one fact or validation, and propose a small next step.

EXAMPLE CLOSE

"To understand where borrower data could remain after the server refresh, we suggest a short data and vendor review covering one data center and two branches. We will map the assets, confirm the evidence needed for disposal, and review key custody where encryption applies. Can we schedule a working session with IT, Procurement, and the data protection officer?"

A FOUR-STEP ANSWER TO AN OBJECTION

1 ACKNOWLEDGE	2 REFRAVE	3 EVIDENCE	4 ADVANCE
Repeat the concern in the customer's words.	Connect it to the business or data risk they care about.	Offer one relevant capability or test. Be specific about what it proves.	Propose a small step that will answer the concern.

PITCH PREP TOOLKIT / PORTFOLIO MAPPING

Match the problem to the principal

Use the brief's six roles to choose the smallest useful set. A product role should connect to a control point and a customer question.

ROLE / PRINCIPAL	CUSTOMER SIGNAL	CAPABILITIES IN THE EVENT BRIEF
GOVERN / OneTrust	"We do not know what personal data we process or which AI uses need review."	AI governance, privacy, data inventory, risk and assessment.
ASSESS / SecurityScorecard	"We rely on vendors, but we cannot prioritize their external cyber risk."	External posture and vendor or supply-chain risk. Use alongside customer evidence and contracts.
CONTROL / Cloudflare	"We need policy on user traffic, data movement, AI access, or application paths."	SSE, DLP, AI access, AI Gateway, and application controls. Confirm the specific traffic path and product scope.
PROTECT / Sangfor	"We need to defend endpoints, network, or workloads."	Endpoint, NGFW, NDR, workload and network cyber defense. Map coverage to the actual environment.
DETECT / Darktrace	"We need to spot unusual behavior and investigate it."	Behavioral detection, investigation, and response. Confirm available telemetry and response ownership.
TRUST / Utimaco	"We need clear custody and lifecycle for cryptographic keys."	HSM, KMS, and cryptographic key lifecycle. Key management does not replace application controls, backup, or media destruction.

COMMON OBJECTIONS AND A USEFUL RESPONSE

OBJECTION	RESPONSE DIRECTION
"We already have a firewall / endpoint product."	Recognize the existing control. Map the actual data or attack path, then check the gap and overlap.
"The vendor is certified."	Ask what the evidence covers. Pair external posture signals with the customer's contract, access, and data-handling review.
"Legal owns PDP."	Bring the data protection officer and Legal into purpose and obligation decisions; map the technical controls with IT and Security.
"Can this guarantee compliance or stop every attack?"	No product should be pitched as a guarantee. Agree on the specific control, test, evidence, and owner.

If a feature, integration, license, or control boundary is unknown, say what must be checked and who will confirm it.

PITCH PREP TOOLKIT / TEAM CANVAS

Fill this in before you present

Keep the architecture simple enough to draw on a whiteboard without slides.

1. CUSTOMER AND TRIGGER	Customer: _____ Business trigger: _____ Problem in one sentence: _____
2. DATA OR SERVICE AT RISK	Personal/confidential data: _____ Critical service/system: _____ Cost of doing nothing: _____
3. PATH AND BOUNDARY	User/vendor: _____ App/system: _____ Data destination: _____ Owner: _____ Trust boundary and control point: _____
4. RECOMMENDATION	Primary role and principal: _____ Supporting role(s): _____ Three moves in order: 1. _____ 2. _____ 3. _____
5. PILOT AND PROOF	Scope: _____ Duration: _____ Owner and dependencies: _____ Success measure and baseline: _____
6. COMMERCIAL ASK	Workshop, assessment, or PoC: _____ Decision requested from panel: _____ Who needs to join and when? _____

BEFORE YOU PRESENT

STORY AND TECHNICAL	PANEL AND TIMING
• Every member knows their section and handoff. • Opening and close have been rehearsed aloud. • The data or system path can be drawn without slides. • Product mapping follows the brief; assumptions are clear.	• Every member speaks in the 8-minute pitch. • One customer-relevant measure is proposed for testing. • The group leaves 2 minutes for panel Q&A. • The commercial ask is specific and has an owner.

COMMON SCORING TRAPS

Opening with product names; listing all six principals without a reason; claiming unverified results, certifications, or integrations; treating a posture score as assurance; assuming detection replaces response; or running out of time before making the ask.