Pre-Class Discovery Handout: Cybersecurity Business Models

Activity 1: Business Model Canvas Detective — Cyber Vendor Edition

Scenario: Pick ONE cybersecurity vendor whose product you have heard of — CrowdStrike, Recorded Future, BlueVoyant, Coalition, Onapsis, or any other in the same space. Fill in the Business Model Canvas below by investigating how the company actually works. Focus on the mechanics of value creation, not marketing language.

Canvas Element	Your Analysis
Value Proposition *What anxiety or compliance pressure does this vendor remove?*	
Customer Segments *Who signs the procurement contract — CISO, risk team, board?*	
Channels *How does the vendor reach buyers without retail distribution?*	
Revenue Streams *Type of income — subscription, retainer, premium (not amounts)?*	
Key Resources *What asset — telemetry, intel, licence — gives the vendor its edge?*	

Q1: What is the single most painful friction this vendor removes for the buyer?

Q2: How does the vendor reach new customers without traditional consumer marketing channels?

Q3: If this vendor disappeared tomorrow, what would clients lose that an in-house team could not easily replace?

Activity 2: Lifecycle Unbundling Map — Cybersecurity Edition

Scenario: Cyber-defence used to come in a single managed-services bundle from a Big-Four advisory firm. Specialist vendors have unbundled the bundle into separate lifecycle phases. Match each vendor to the lifecycle phase it primarily addresses, then answer the questions below.

Vendor		Defence Lifecycle Phase
CrowdStrike	____	Endpoint Protect and Detect
Recorded Future	____	Threat Intelligence (Identify and Detect)
BlueVoyant	____	Managed Detect and Respond
Coalition	____	Risk Transfer (Insurance)
Onapsis	____	ERP Identify and Protect

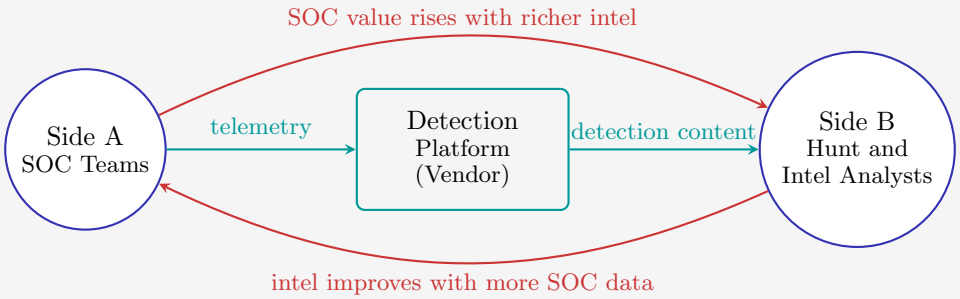
Q1: For each pair, describe in one sentence what specific friction the vendor removes for the SOC team.

Q2: Which of these vendors has begun adding services beyond its original lifecycle phase? What did it add?

Q3: Why might a single-phase vendor eventually want to bundle adjacent lifecycle phases into its offering?

Activity 3: The Defence Platform Puzzle

Scenario: An endpoint-detection vendor connects two sides of a market — enterprise SOC teams who consume detection content, and threat-intel analysts (internal hunt team plus external feeds) who produce detection content. Neither side finds the platform useful without the other.



Q1: Why does a detection platform with more SOC clients attract better hunt analysts (and vice versa)?

Q2: The "cold-start problem" in cyber-defence: which side should the platform attract first, and why?

Q3: Once the platform reaches critical mass, why is it hard for a competing vendor to displace it?

Solutions

Activity 1: Business Model Canvas Detective

A1: Model answer for CrowdStrike: The most painful friction removed is the impossibility of detecting novel intrusions across a sprawling endpoint estate using purely local rules. CrowdStrike pools telemetry from every client into a global detection graph that surfaces patterns no single firm could ever see alone, then deploys the resulting signatures back to every endpoint within minutes.

A2: CrowdStrike acquires customers primarily through procurement channels — enterprise sales, analyst-firm rankings, channel partners, and direct executive briefings — not through retail or app-store distribution. Industry analyst evaluations and public-incident response engagements act as proof points that reach the next CISO buyer.

A3: Clients would lose the cross-client detection graph, the validated content updates that ride on top of it, and the institutional knowledge embedded in the vendor's hunt team. A purely in-house SOC could rebuild the tooling but not the data network — and rebuilding the data network is the part that takes years and requires many willing peers.

Canvas elements (CrowdStrike):

- **Value Proposition:** Convert tail-risk breach loss into a predictable per-endpoint subscription, with global detection content that no single bank could assemble alone.
- **Customer Segments:** Primary — CISOs and SOC managers in regulated financial institutions and large enterprises; secondary — managed-security service providers reselling the platform.
- **Channels:** Direct enterprise sales, channel partners, analyst-firm rankings, public incident-response engagements as marketing.
- **Revenue Streams:** Per-endpoint subscription tiers, professional-services for onboarding and tuning, premium incident-response retainer.
- **Key Resources:** Cross-client telemetry pool, validated detection content library, in-house hunt team, brand reputation among CISOs.

Activity 2: Lifecycle Unbundling Map

A1: CrowdStrike → Endpoint Protect and Detect (removes the impossibility of pattern-matching novel intrusions across a sprawling endpoint estate without a shared telemetry pool). Recorded Future → Threat Intelligence (removes the firehose problem of collating open-source and dark-web indicators for a SOC team that lacks dedicated researchers). BlueVoyant → Managed Detect and Respond (removes the staffing impossibility of running a continuous SOC for a mid-sized financial institution). Coalition → Risk Transfer (removes the friction of buying cyber-insurance from a carrier that cannot price the risk because it lacks telemetry). Onapsis → ERP Identify and Protect (removes the blind spot in the ERP layer where most general-purpose security tools never look).

A2: CrowdStrike began with endpoint detection and added identity protection, cloud workload monitoring, log analytics and an LLM-assistant for SOC triage. Coalition began with cyber-insurance underwriting and added active monitoring, breach-coach services and even pre-claim mitigation tooling. Both illustrate **rebundling** — starting narrow, then cross-selling adjacent lifecycle phases once trust is established.

A3: A single-phase vendor faces high customer-acquisition costs and ceiling on contract value. Once a CISO trusts the vendor, the marginal cost of selling the next adjacent capability is low, while the marginal revenue is high. Rebundling raises annual contract value, deepens procurement lock-in through bundled licensing, and creates a competitive moat against narrower point-vendors.

Activity 3: The Defence Platform Puzzle

A1: This is a **cross-side network effect**. More SOC clients means more raw telemetry flowing into the platform, which means hunt analysts can identify patterns earlier and craft better detection content. Better detection content makes the platform more attractive to the next SOC client. Each side's growth reinforces the other's.

A2: Most successful detection platforms attract the **supply side** (intel analysts and detection content) first, often by operating an in-house hunt team and ingesting open-source intel before any client signs. The logic: if the platform already publishes high-quality content, SOC teams have an immediate reason to subscribe. Attracting SOC clients first is harder because they have no useful content yet. This is the cold-start problem applied to cyber.

A3: Once critical mass is reached, the platform enjoys a self-reinforcing loop that creates a **structural moat**. A new entrant would need to simultaneously attract both sides — each of which has little reason to join an empty platform. The incumbent's content quality grows with every additional SOC client, making the gap progressively wider. Competitors must find an underserved niche (ERP only, OT only, mid-market only) or offer dramatically different economics to pry either side away.

