ChatGPT

Dinis Cruz’s Multi-Startup Strategy: Open-Source Innovation Across Four Synergistic Ventures

Introduction

Dinis Cruz is pursuing an innovative strategy by concurrently building four complementary startups in the cybersecurity and AI domain. Each venture addresses a different problem niche, but all share a common foundation: an open-source core technology and a lean, serverless infrastructure that keeps costs minimal. This approach allows each product to leverage and reinforce the others, creating a symbiotic ecosystem greater than the sum of its parts. The ultimate goal is to **deliver useful, scalable solutions with recurring revenue streams** by engaging early users, refining MVPs, and then scaling up with the help of first-round investments. Crucially, **open-source development is the cornerstone and force multiplier** of this strategy – it accelerates innovation, encourages collaboration, and enables the reuse of key technological building blocks across all four startups [1]. As a result, improvements in one product can directly benefit the others, speeding up execution and magnifying the impact of each investment.

In this briefing, we provide an overview of Dinis Cruz’s four startups, their individual focus areas, and how they interconnect through shared technology. We also outline the vision and execution plan (emphasizing why open source is a superpower in this context), current MVP status and early traction for each venture, and the opportunity for angel and early-stage investors to get involved. **Each startup is currently at MVP stage with initial users, and each is seeking its first round of investment to accelerate growth and customer acquisition.** Importantly, while each venture maintains a narrow and distinct focus (avoiding any internal competition or overlap), together they form a cohesive suite of solutions that reinforce one another’s value. The sections below detail each startup and the common framework underpinning them, followed by the investment proposition and next steps.

Four Startups at a Glance

The table below summarizes the four startups, their target problem, and the core technology/workflow each is building (which also benefits the others):

Startup	Focus & Problem Solved	Core Solution/Tech (Shared Workflow)	Status (MVP & Next)
The Cyber Boardroom (Cybersecurity Governance)	Bridging the communication gap between cybersecurity teams and executive boards/stakeholders. Boards need to understand technical cyber risks in business terms, and security leaders need feedback from boards.	GenAI-driven persona-based communication engine (LLM translator that converts technical jargon into board-level language and vice versa). Simulates stakeholder personas to refine messaging [2]. Leverages a **persona modeling** framework and two-way translation workflow.	**MVP complete** – Functional prototype with initial CISOs testing. Business plan developed; seeking seed investment to onboard pilot customers and refine features.
MyFeeds.ai (Personalized Info Feeds)	Cutting through information overload by delivering highly personalized news/intel feeds. Professionals (e.g. CISOs, CTOs) need relevant, up-to-date content without manual filtering.	**Semantic knowledge graph pipeline** that ingests RSS/news sources and transforms them via LLM into linked semantic graphs. Generates custom feeds by matching content graphs to user persona graphs. Implements a "LETS" workflow (Load, Extract, Transform, Save) for data processing. Emphasis on **content provenance** and explainability in recommendations.	**MVP live** – Demo newsletters (e.g. CEO, CISO daily briefs) generated. Early interest from industry users (one CISO piloting multiple tailored feeds). Raising first funding to integrate more data sources, harden the platform, and expand user trials.
Semantic Content Filter (AI Web Filtering)	Real-time filtering and customization of web content. Need for intelligent content controls (e.g. remove malicious or inappropriate content, enforce compliance) beyond simple keyword blocking.	**AI-powered filtering proxy** that intercepts web page requests and analyzes content on the fly using LLMs. Builds a semantic knowledge graph of each page's content, then applies user-defined rules or policies to modify or block content. Relies on high-performance caching, serverless functions, and the shared graph/LLM pipeline to operate in near real-time.	**Prototype in development** – Co-founded with industry partners; core engine under construction. Focused on scaling (high throughput analysis, caching). Exploring use-case pilots (enterprise security, parental control, etc.). Seeking seed investment to accelerate development and run controlled deployments for feedback.

Startup	Focus & Problem Solved	Core Solution/Tech (Shared Workflow)	Status (MVP & Next)
Interactive Report Assistant (AI Document Generation)	Streamlining the creation of complex reports (e.g. GDPR compliance assessments) via conversational AI. Traditional report generation is labor-intensive and prone to missing knowledge capture.	**Interactive LLM-driven workflow** that engages the user in a Q&A dialogue. Extracts facts, hypotheses, questions, and evidence from each interaction. Uses a feedback loop: user validates or corrects AI-generated facts in real-time. Accumulates a knowledge base specific to the report and then auto-generates a structured report (with templates) from the confirmed information. Emphasizes **provenance** (traceability of facts) to minimize hallucinations.	**MVP under testing** – Developed in collaboration with a consulting firm (for GDPR use case). Early version generates draft reports from chat transcripts. In beta with domain experts providing feedback. Seeking initial investment to expand to more domains (other compliance or audit reports) and refine the UX for broader use.

Table: Overview of Dinis Cruz's four startups, each tackling a distinct challenge with a shared foundation of open-source, AI-driven technology.

Open-Source Foundation and Shared Technology

A unifying thread across all four ventures is the **open-source technology stack** and a common set of innovative workflows. Dinis Cruz, a long-standing open-source advocate [3], has deliberately made each project's core code open source. This yields several advantages:

- **Faster Innovation and Collaboration:** Open sourcing invites contributions and feedback from the community and other developers. It also means solutions to technical challenges can be shared, reviewed, and improved in the open. This has been a *force multiplier* for development speed and quality across the projects. For example, a library created for semantic graph handling or a deployment script in one startup can be reused and enhanced by others immediately.
- **Reusable Building Blocks:** All startups leverage common building blocks that Dinis has developed. Key components include:
- **Unified CI/CD and Serverless Deployment Pipeline:** A deployment framework that packages applications to run on any environment (serverless functions, containers, on-premises) with minimal overhead. This was first built to ship The Cyber Boardroom everywhere and is now used by all projects to ensure low running costs (only paying for what users consume) and easy scalability.
- **MemoryFS & GraphFS (In-Memory and Graph Filesystems):** Custom storage abstractions that allow data (like RSS feeds, articles, user data) to be stored uniformly and represented as graphs. This enables seamless saving, querying, and visualizing of complex interconnected data (e.g., relationships between a user's interests and an article's topics).
- **LETS Pipeline (Load, Extract, Transform, Save):** A stepwise data processing workflow (inspired by traditional ETL) that ensures each piece of data goes through a controlled process. For instance, MyFeeds.ai uses LETS to fetch raw RSS feeds (Load), parse and clean them (Extract),

generate semantic metadata (Transform), and store results in both raw and processed form (Save). This structured pipeline improves transparency and tweakability – critical for debugging AI decisions and maintaining provenance.

- **LLM Integration & Persona Modeling:** All products rely on large language models for understanding and generation of text. A common approach is modeling "personas" – representing user roles or preferences in a way the LLM can use to tailor outputs. The Cyber Boardroom, for example, translates cybersecurity jargon to a *Board persona* perspective. MyFeeds represents the information interests of different personas as graphs. The Report Assistant builds a persona of the document's audience (e.g., a compliance officer) to shape how information is presented. Dinis's framework for defining and refining personas (including factors like role, expertise, cultural context, and goals) is employed across the board to enhance relevance and accuracy of AI outputs.

- **Semantic Knowledge Graphs:** Converting unstructured text into structured knowledge graphs is a core workflow shared by MyFeeds, the Content Filter, and to an extent the Report Assistant. By representing entities, topics, and their relationships in graph form, the AI solutions can reason about content more transparently. This enables explainable recommendations (why a certain news article was shown to a user), granular content filtering rules (e.g., detect relationships indicating a phishing attack on a web page), and traceable report facts (linking report statements back to source evidence nodes). All graphs are stored in standardized formats so that insights can be passed between systems (for example, an interesting threat topic identified in MyFeeds could be fed into Cyber Boardroom's knowledge base for boards).

- **Minimal Costs and Scalability:** The combination of serverless architecture and open-source software means each startup can run with extremely low fixed costs. There is no expensive proprietary license or heavy infrastructure burden. Compute and storage scale with usage, and costs can be directly tied to customer consumption (and thus easily covered by revenue). This **capital efficiency** is attractive for early-stage investment – more funds can go into feature development and user acquisition rather than infrastructure. It also lowers risk: each MVP is already running on cheap cloud functions or containers, so supporting initial users is financially sustainable.

- **Community Trust and Adoption:** Especially in cybersecurity, open-source tools are often preferred because they can be inspected and vetted by anyone. By open-sourcing the core, Dinis establishes credibility and trust with enterprise customers who can verify the security and integrity of the code. It also eases integration – other developers or companies can build on these tools, potentially leading to partnerships or ecosystem adoption. In the long run, this strategy can drive adoption **faster than a closed-source approach**, creating a wider user base that can be monetized via value-added services, support, or cloud-hosted offerings.

By weaving open-source principles into each startup's DNA, Dinis effectively **amplifies the impact of every line of code**. Progress in one domain (say, a breakthrough in semantic parsing for the Content Filter) can quickly propagate to improve the others. This shared technology strategy not only accelerates execution but also ensures that the four products remain **interoperable and mutually reinforcing** by design. It's a deliberate approach to **"building GenAI-powered environments where engineering and security act as business accelerators"** [4], aligning technical innovation directly with business value across all projects.

Startup 1: *The Cyber Boardroom* – AI for Cybersecurity Governance

Focus: The Cyber Boardroom is addressing a critical gap in organizations: the communication barrier between technical cybersecurity teams and non-technical executive stakeholders (board members, CEOs, business unit leaders). Security leaders often struggle to convey cyber risks, needs, or achievements in terms that boards understand, while board members have difficulty feeding their strategic priorities and concerns back to the security team in actionable form. This misalignment can lead to underinvestment in security, unclear risk appetite, or misinformed strategy. The Cyber Boardroom aims to solve this by acting as an intelligent translation layer in both directions.

Solution Approach: This startup uses a Generative AI engine (Large Language Model) to translate and **"interpret" between the language of cybersecurity and the language of business**. Think of it as an AI-powered facilitator that sits in the middle of the CISO-board relationship:

- On one side, a CISO or security manager can input a technical report, a risk assessment, or a budget request. The Cyber Boardroom will generate a polished executive summary or briefing tailored to the understanding of a board member – emphasizing business impact, using layman analogies if needed, and focusing on strategic priorities rather than low-level tech details. It ensures key messages land effectively.
- On the other side, a board member or CEO can ask questions or express concerns (e.g. "How are we protected against ransomware?" or "Why do we need to invest $X in cybersecurity next quarter?"). The system will translate these into specific queries or action items for the security team, or even answer directly in a way that bridges knowledge gaps (for instance, by pulling from security data but framing the answer in business terms).

A distinguishing feature of The Cyber Boardroom is its use of **persona simulation**. The platform can model the perspective of different stakeholders – for example, how a CFO versus a CTO versus an external board director might perceive a given cybersecurity message. The user can *simulate a boardroom conversation*: you input your message to the board, and the AI, assuming the persona of a skeptical CFO (as an example), will simulate a response: "If presented this way, the CFO might worry about X or misunderstand Y." This allows proactive refinement of communications. It's essentially a training and validation tool for cyber executives to improve their messaging strategy. Over time, this can significantly improve mutual understanding and trust between tech and business leadership [4].

Under the hood, The Cyber Boardroom maintains a knowledge base of cybersecurity concepts and maps them to business outcomes. It factors in attributes like the stakeholder's role, their likely concerns (e.g., a CFO cares about financial impact, a General Counsel might focus on legal liability, etc.), and even their personal communication style if known. It also accounts for cultural context and corporate environment. All this context forms a "persona profile" used by the LLM to shape its translations. By leveraging a powerful world model from the LLM, the system can **"translate technical complexity into clear business value"** [4] – essentially speaking the language of the board.

Progress & Traction: The Cyber Boardroom concept was the first of the four to be developed, and it has a detailed business plan and a working MVP. Dinis published a full business plan outlining target customers, pricing models, and go-to-market strategy for this product early on, and the prototype has been iteratively improved with feedback from industry peers. A small group of CISOs have experimented with the tool to craft board presentations and found the persona simulation especially insightful. The MVP can already ingest things like RSS news about cyber incidents and produce a tailored briefing for a given persona (a feature developed in tandem with the MyFeeds.ai project). This startup has garnered attention in the cybersecurity community – for instance, it was highlighted as *"a pioneering cybersecurity startup using GenAI to revolutionize board-level decision-making"* [2]. With the core functionality proven, the next steps are to convert these early adopters into paying customers and expand features (such as richer two-way interactivity and integration with company-specific data).

Investment Opportunity: The Cyber Boardroom is seeking seed funding to move from a promising prototype to a scalable product. Investment will be used to **onboard early enterprise clients** (likely starting with design partners in sectors with high regulatory oversight, who have a strong need for board cybersecurity engagement), to enhance the UI/UX for seamless use in real board meetings, and to integrate further data sources (e.g., linking into a company's internal risk registers or threat intel feeds). Because the core technology is open source and serverless, the capital required is modest relative to traditional enterprise software startups – funds will primarily fuel continued R&D (refining the AI models for even better contextual understanding) and business development. Ultimately, this venture can drive value not just as a standalone product but as part of a **broader ecosystem** of AI tools for corporate governance. Success here also paves the way for cross-selling or up-selling the other solutions (e.g., an organization using Cyber Boardroom might also subscribe to MyFeeds.ai for curated intel, etc.). With Dinis's 20+ years of experience at the intersection of security and business [5] , The Cyber Boardroom is poised to become a trusted platform for elevating cybersecurity discussions to the strategic level.

Startup 2: *MyFeeds.ai* – Personalized News & Intelligence Feeds

Focus: MyFeeds.ai tackles the problem of **information overload in the cybersecurity and tech domains**. Professionals like CISOs, security analysts, CTOs, and even investors need to stay informed about a flood of news: emerging threats, vulnerabilities, industry trends, regulatory updates, etc. However, everyone's information needs are different – a CISO at a financial firm might care more about regulatory compliance news, whereas a CTO at a tech startup might be keen on the latest developer security tools. Most news platforms or aggregators do not adequately personalize content at this granular level, and raw RSS feeds or keyword alerts often produce too much noise. The result is that valuable information is missed or time is wasted sifting through irrelevant articles. MyFeeds.ai is designed to deliver **highly personalized, persona-specific news feeds** that surface the most relevant content for each user's role and interests, in a concise format (e.g., daily email briefings or dashboard).

Solution Approach: The core innovation of MyFeeds.ai is the use of **semantic knowledge graphs and AI to curate content**. Instead of treating articles as blobs of text and doing keyword matching, MyFeeds processes each piece of content through a pipeline that understands *meaning* and *context*:

1. **Ingestion of Multiple Sources:** The system aggregates data from many RSS feeds and news APIs across cybersecurity, tech, and business. Every few minutes or hours (configurable), it loads new articles or posts from these sources (for example, feeds from security news sites, tech blogs, threat intelligence reports, etc.).
2. **Content Parsing and Storage:** Each fetched item is parsed – the raw text, metadata (author, date, etc.), and even the HTML structure are saved in a cloud-based content store. This is where Dinis's custom **MemoryFS** abstraction comes into play, allowing the data to be stored uniformly and later accessed either as files or as graph nodes. The content is then **transformed into a JSON structure** for ease of processing (part of the "Extract" and "Transform" steps of the LETS pipeline).
3. **Semantic Graph Generation:** An LLM then analyzes the article to extract key **entities, topics, and relationships**, forming a semantic representation (a graph) of the article's content. For example, an article about a new ransomware might generate nodes like {Ransomware X, Healthcare Industry, Data Breach, Country Y, $$$ Impact} with relationships indicating that *Ransomware X caused a data breach in the healthcare sector in Country Y resulting in some impact*.

This graph is stored (via **GraphFS**) and essentially becomes a machine-interpretable summary of what the article is about.

4. **User Persona Graphs:** On the user side, MyFeeds creates a **profile graph** for each user (or each persona category). This graph represents what topics that user cares about. It can be built initially from explicit inputs (e.g., user says they are interested in "cloud security" and "EU cybersecurity regulations"), and over time it can evolve by learning which articles the user reads or flags as useful. The persona graph includes context like the user's role (e.g., CISO), industry, and even preferred content type (high-level summaries vs deep technical analysis).
5. **Matching and Curation:** With both content graphs and user graphs in a common semantic space, MyFeeds can algorithmically match articles to users. It finds intersections between the two graphs – effectively recommending an article if the semantic content overlaps significantly with the user's interests. Because this happens at a concept level (not just keyword), it's more precise: for instance, if a user's profile says "concerned about supply chain attacks in open-source software," the system can pick up an article about a new vulnerability in an NPM package as relevant, even if the article doesn't explicitly say "supply chain" – the knowledge graph can infer that an NPM library compromise is a type of supply chain issue.
6. **Explainability and Feedback:** A major benefit of this graph approach is explainability. MyFeeds can show *why* it recommended an article – e.g., *"this post was suggested because it discusses cloud security and zero-trust architecture, which are topics in your profile."* Users can give feedback (like thumbs up/down or adjust interest weights), and the system will update the persona graph accordingly. This fosters trust in the AI curation and continuously tunes the feed to the user's needs.

The output to the end-user is a **personalized news feed or newsletter**. For example, a CISO might receive a morning briefing with the top 5 articles most relevant to *their* organization's context (perhaps "New Financial Sector Breach, Regulatory Update on Data Privacy, Critical Patch Advisory for a product they use, etc."). Each item might have a short AI-generated summary focusing on the aspects that matter to that user (again leveraging the persona model).

MyFeeds.ai essentially redefines how professionals consume industry news: instead of one-size-fits-all feeds, it delivers *contextual intelligence*. This not only saves time but also can uncover niche information that generic platforms would overlook.

Progress & Traction: The MyFeeds concept emerged from direct needs encountered during The Cyber Boardroom's development. Dinis realized that to demonstrate the board briefing AI, he needed a steady stream of **relevant content** to discuss (since many users were hesitant to input proprietary data initially). By creating personalized news feeds, he could simulate a flow of pertinent information for the board discussions. This quickly proved valuable on its own. An MVP of MyFeeds.ai was built, and Dinis even documented it publicly (the MVP is accessible at `mvp.myfeeds.ai`) and showcased example personalized newsletters (such as a "CEO Cybersecurity Brief" and an "Investor Tech Digest"). The results were well received – users remarked that the feeds were uncannily relevant. In one case, a CISO who tested MyFeeds asked if multiple distinct feeds could be generated: e.g., one for themselves, one simplified for their non-technical executives, and one for their technical team. The MVP was able to deliver on this request by simply creating different persona profiles. This validates that the same news content can be repackaged for different audiences automatically – a strong selling point for enterprise use (e.g., internal newsletters tailored to different departments).

On the supply side, MyFeeds also uncovered that many news providers have not modernized how their content is distributed or monetized. RSS feeds are often freely available but underutilized, and few have robust APIs or personalization. This presents an opportunity: MyFeeds could partner with or license from content providers to add value on top of their feeds, or even help them monetize corporate subscriptions to curated content. Dinis has explored potential business models (outlined in internal documents) where organizations pay for **premium personalized intelligence feeds** for their teams – effectively an AI research assistant scanning the news for them.

The current status is that MyFeeds.ai has a functional pipeline and a handful of pilot users. The heavy backend work (the graph processing and pipeline) is largely done and open-sourced. Next steps include improving the front-end user experience (making it easy for a user to set up their profile and view their feed), scaling up the number of sources (onboarding more RSS feeds, perhaps integrating Twitter/X or other relevant data streams), and hardening the system for production use (error handling, performance tuning). There's also interest in integrating MyFeeds with collaboration tools (imagine a Slack bot that posts personalized news to a team channel).

Investment Opportunity: MyFeeds.ai is seeking an early-stage investment (seed round) to accelerate these next steps. Funding would be used to **expand content coverage and refine the recommendation engine**, as well as to implement a subscription model and marketing to reach more users. Given the open-source core, development costs are efficient – a small team can maintain the platform. Revenue would come from SaaS subscriptions or enterprise licensing for organizations that want to deploy a private version (some companies might prefer to feed in their own internal data plus external news for an even more customized feed). For investors, MyFeeds offers a play in the burgeoning market of AI-driven personalization. It is a product that can appeal not only in cybersecurity but to any domain where professionals must keep up with fast-changing information. And importantly, it serves as the content "fuel" for other tools (like Cyber Boardroom or the Report Assistant), meaning success here could amplify the value of the entire portfolio of startups.

Startup 3: *Semantic Content Filter* – Real-Time AI Web Content Filtering

Focus: The Semantic Content Filter startup is focused on **real-time content filtering and modification of web content using AI**. In many scenarios, users or organizations want to control what content is accessible or visible – for safety, productivity, or compliance reasons. Traditional solutions (like web filters, parental control software, or corporate firewalls) usually rely on blocklists, simple keyword matching, or categorization of URLs into "allowed" and "disallowed" buckets. These methods are coarse and often fail to understand context. For example, a company might want to allow YouTube for educational videos but block certain topics, or a parent might wish to filter out only violent content on otherwise kid-friendly websites. Keyword filters can over-block or under-block because they lack semantic understanding (e.g., blocking "weapon" might block a news article about "weaponizing AI algorithms" which is not actually violent content). There is a need for smarter filtering that understands the *meaning* of content in real time. Additionally, emerging threats like phishing sites or scams could be detected by understanding page content and intent, rather than maintaining huge blacklists. The Semantic Content Filter aims to meet these needs by leveraging an AI that actually reads and comprehends web pages on the fly, then applies very granular, personalized filtering rules.

Solution Approach: The product is essentially an **AI-powered proxy server** that sits between the user's browser and the web. When a user requests a webpage through this proxy, the system performs a series of actions almost instantaneously:

1. **Intercept and Fetch:** The proxy receives the URL request, then goes and fetches the content of the page from the destination server. This includes HTML, text, images, scripts, etc. By design, this can be done in a streaming fashion or fully fetched, depending on optimization.

2. **Content Analysis (Semantic Graph Creation):** The raw HTML is parsed and the text content is extracted. (Media like images or video might be handled separately, possibly via metadata or AI image recognition if needed in future extensions.) The extracted text and structural context of the page are then fed to an LLM (or a smaller distilled AI model for speed) to analyze. The AI generates a **semantic profile of the page** – essentially similar to MyFeeds's process: identifying the main topics, sentiments, possibly the presence of certain categories of content (like "this page contains graphic violence" or "this page is attempting to collect login credentials"). The result is a knowledge graph or a metadata profile for the page. Importantly, this analysis can also include **classification against user-defined policies**. For instance, if a parent user has a rule "Block content that has explicit language or violence," the AI classifier will flag if those are present. Or a corporate policy might be "Allow tech news sites but strip out comment sections and advertisements." The LLM can tag parts of the page content that match these criteria.
3. **Content Transformation (Filtering/Modification):** Based on the analysis, the proxy then transforms the page before delivering it to the user. This could mean **blocking the page entirely** with a notice ("This site is blocked by your policy"), or more subtly, **dynamically editing the content**. For example, it might remove a paragraph of text that is deemed inappropriate, or redact certain words, or remove images that are disallowed. In a less strict scenario, it might just insert warnings ("This section of the article contains unverified information") or highlight certain content (for example, highlight known malicious script elements in red for an administrator to notice). Essentially, the web page is rebuilt on the fly in a way that adheres to the user's or organization's rules, but as seamlessly as possible. The user still sees a coherent page – just tailored.
4. **Learning and Caching:** The system caches the processed results for efficiency. If multiple users request the same page and have similar policies, it can serve the results faster the second time. Also, by collecting data on what gets filtered or allowed, it can improve its filtering rules (e.g., if users consistently override a block on a certain type of content, the system learns that perhaps that content shouldn't be classified as disallowed under that policy).

This solution is powerful because it operates at a semantic level. It can, for instance, allow a news website but remove only the political news section for a user who doesn't want to see politics, while showing it for another user. Or it could neutralize phishing by detecting when a login form on a non-official domain is asking for credentials and blocking just that form. The **granularity and intelligence** is the differentiator – and that comes from the LLM's ability to parse context, not just static rules.

Technical Synergy: Developing the Semantic Content Filter has pushed the envelope on performance and scale in Dinis's toolkit. Unlike the other projects, which can operate asynchronously (e.g., generating a feed over minutes or crafting a report interactively), the web filtering proxy needs to work in near real-time to not noticeably delay page loads. This led to optimizing the **caching mechanisms** and the efficiency of the graph generation. It also leverages the serverless deployment approach heavily – instances of the function can scale out to handle bursts of traffic, and scale to zero when idle (keeping costs low for a few users, but able to handle enterprise loads on demand). The knowledge graph techniques from MyFeeds are reused here, but streamlined. Additionally, the filtering rules and transformation engine developed here could loop back into other products (for example, the ability to highlight or redact content based on AI understanding could enhance how reports are generated in Startup 4, or how summaries are presented in Cyber Boardroom). This cross-pollination is already happening at the code level.

Progress & Next Steps: The Semantic Content Filter is currently in the prototype phase, co-founded by Dinis and two other collaborators who have expertise in content security. A basic version of the proxy exists: it can handle simple pages, create a semantic representation, and apply rudimentary filters (like remove all profanity or block known phishing keywords). One challenge being tackled now is *defining* *the right product-market fit*. The technology itself has numerous applications: parental controls, enterprise compliance (blocking data exfiltration or toxic content), even individual user preferences (like a browser extension to clean up your social media feed). The team is exploring which initial market to focus on. They have early ideas such as offering it to schools (to protect students with smarter web filters) or bundling it with security products as an advanced safe-browsing feature.

On the technical side, the MVP needs further development to handle complex, dynamic web content (think single-page applications, or heavy JavaScript-driven sites). There's also ongoing work to compress the AI models or use clever heuristics so that 95% of pages can be filtered quickly without full LLM analysis, while still calling the LLM for the tricky cases – this hybrid approach will be key to keeping costs and latency low. Fortunately, the incremental improvements here (efficient graph processing, model distillation) benefit all the other startups as well, making the whole ecosystem more performant.

Investment Opportunity: As this startup is still in stealth mode (relative to the others) and building its MVP, it is seeking seed investment primarily to **accelerate product development and market experimentation**. Funds would be used to hire a few additional developers with AI and networking expertise, and to run pilot programs with select customers to gather real-world data. The investors coming on board now have the chance to help shape the go-to-market strategy – deciding which niche to target first for maximum traction. There is also potential IP being created (combining LLMs with proxy filtering in novel ways) that could be protected or patented, adding value. In terms of revenue, possible models include per-user or per-seat licensing (for enterprise deployments) or subscription fees (for consumer or SMB versions). In the bigger picture, success for the Semantic Content Filter would enhance the overall value proposition of Dinis's portfolio: it could feed curated safe content into MyFeeds, or be offered as an add-on to Cyber Boardroom (e.g., a board member safe-browser). It's a high-potential, high-impact play in an area (AI-driven content control) that few others are tackling with this level of semantic sophistication.

Startup 4: *Interactive Report Assistant* – AI-Guided Reporting and Knowledge Management

Focus: The Interactive Report Assistant addresses the **pain of producing comprehensive, accurate reports through a guided AI conversation**. Many industries (cybersecurity, compliance, consulting, auditing) require experts to gather information and compile detailed reports – think of a GDPR compliance assessment report, a security audit report, or even an internal risk analysis. Creating these documents is time-consuming: it involves asking stakeholders many questions, collecting evidence, noting down facts, formulating recommendations, and organizing everything into a formal structure. Often, important details can be overlooked or mis-communicated, and the narrative might not be tight because information is gathered in an ad-hoc way. The goal of this startup is to streamline that process by using an AI assistant that collaborates with the human expert, ensuring **no detail falls through the cracks and the final output is well-structured**.

Solution Approach: The Interactive Report Assistant is essentially an AI co-pilot for analysts/consultants that operates in two modes: a conversational interview mode and a report generation mode. Here's how it works:

- **Conversational Data Gathering:** The user (e.g., a consultant) initiates a session by stating the context ("I'm doing a GDPR assessment for Client X" or "I need to create an incident report for Y breach"). The AI, powered by an LLM tuned for this domain, starts by asking high-level questions, much like a human consultant would. For instance: "What type of personal data does Client X process, and in which jurisdictions?" The user can answer from their knowledge or input data.

With each answer, the system **extracts key facts, figures, and any stated assumptions or uncertainties**. It might ask follow-up questions if something is unclear or if a critical piece of info is missing. This interactive Q&A continues, guided by a **dynamic script** that the AI adapts based on prior answers – effectively following investigative threads. If the user mentions a technical term or an entity, the AI can drill down ("You mentioned data is stored in AWS – do we know if encryption is enabled on those storage buckets?"). The conversation is thus a directed flow that covers all the necessary ground methodically.

- **Building a Knowledge Base in Real Time:** Behind the scenes, every piece of information from the conversation is being structured. The assistant creates entries for **facts** (e.g., "Client X stores customer emails and names in Database Y"), **hypotheses** or preliminary conclusions (e.g., "It appears Client X might be non-compliant with data retention policies"), **questions raised** (ones that might need external follow-up or data collection), and even **action items/evidence** (like "Need to verify if encryption is enabled on Database Y – pending evidence"). This is stored almost like a mini knowledge graph or a structured JSON document that grows as the interview progresses. The user can at any time view this growing "report outline" or knowledge base. Crucially, the user can correct the AI if it misinterprets something ("No, actually that's not correct, let me restate it…"), and the AI will update the facts accordingly. This **constant verification loop** minimizes hallucinations and errors – the AI is not making final claims on its own; it's capturing and organizing the human expert's input, with some inference but always subject to the user's confirmation.
- **Report Synthesis and Drafting:** Once the interactive Q&A has covered the necessary topics (or even at interim points), the user can prompt the system to generate a report draft. The assistant then uses the structured information it has collected to populate a report template. For a GDPR assessment example, it might have sections like Executive Summary, Data Processing Activities, Findings (with subsections like Data Storage, Data Transfer, Consent Mechanisms, etc.), Risks Identified, Recommendations, Conclusion. The content for each section is drawn from the facts and findings gathered. Because the data is structured and tagged, the AI can ensure that, for example, every recommendation is backed by some finding in the earlier text (and it could even cite where in the conversation that finding came from). The draft report is presented to the user, who can then edit or polish it, and if needed ask the AI further questions or provide more info to fill any gaps. The assistant can iterate – e.g., if the user says "Add a section on recent incidents," it can prompt for that info and then update the report.

The end result is a **well-organized, accurate report** produced in a fraction of the time. All the source facts are traceable (provenance is maintained: one could imagine clicking a statement in the report and seeing the conversation snippet that produced it). This not only speeds up the reporting task but also **improves quality** – it's less likely to forget to ask a crucial question or to omit a key detail, because the AI's world knowledge can remind the user of standard best practices or common issues. It's like having a second brain dedicated to organization and thoroughness.

Use Case and Synergy: The initial use case being tackled is GDPR compliance reporting, because Dinis partnered with a company active in that consulting space. However, the framework is general and could be applied to many domains: security incident reports, vendor risk assessments, even non-security fields like financial due diligence or medical case history taking. Essentially, any scenario where a guided questionnaire and resulting document are needed.

This startup's technology strongly complements The Cyber Boardroom (imagine using the Q&A approach to prepare for a board meeting – extracting key points to report) and MyFeeds (the ability to extract *facts* and *insights* from articles could feed into the news summaries, turning unstructured news into structured intel). It could also enhance the Content Filter by providing a mechanism to summarize or explain filtered content decisions. In Dinis's broader vision, these pieces eventually come together:

e.g., a security officer might use MyFeeds to stay informed, use Cyber Boardroom to communicate quarterly updates to the board, use the Report Assistant to compile a quarterly risk report, and maybe have the Content Filter protecting their team’s web browsing – all interlinked and sharing data where appropriate.

Progress & Traction: The Interactive Report Assistant is in the advanced prototype stage. The team has developed the conversation engine and a basic UI where the Q&A happens on one side of the screen and the “living report” outline builds on the other side. In trial runs with actual GDPR consultants, the feedback has been positive – it ensures a thoroughness that even experienced analysts found helpful (the AI would sometimes ask about a detail they might have overlooked). Another benefit noted was training junior staff: a junior consultant using this tool can perform at a higher level because the AI guides them on what to ask or look for. This suggests a strong value proposition for consulting firms (improve consistency and quality of deliverables, and get junior employees up to speed faster).

The MVP currently handles text-based input and some document imports (e.g. it can ingest a policy document and incorporate its content into the knowledge base if the user uploads it during the session). Further work is ongoing to refine the templates for report generation and to incorporate domain-specific regulations (e.g., know that GDPR has 99 articles and suggest checking compliance against relevant ones). This will continue to improve as the system learns from more sessions. Importantly, the entire framework is built with openness and extensibility in mind – new domains can be added by defining their ontology (set of facts/hypotheses relevant) and training the AI on domain knowledge, much of which can come from open data or prior reports (with permission, since the AI is open source, even the method of training can be transparent to clients concerned about data).

Investment Opportunity: The Interactive Report Assistant is seeking an initial round of investment to transition from a promising prototype to a market-ready product. The funds will go towards **expanding domain support** (beyond GDPR to other high-demand areas like ISO 27001 security audits or cloud security reviews), enhancing the user interface (making it more intuitive to navigate the Q&A and edit the report), and integrating with enterprise workflows (for example, allowing the export of the report to Word, or integration with ticketing systems to log follow-up tasks discovered during the assessment). Investors with interest in B2B SaaS and enterprise AI will appreciate the model: it’s a subscription per analyst or per report type, with a clear ROI for customers (time saved, quality improved). Moreover, because this solution builds structured knowledge bases, there is a potential moat: over time, it can accumulate industry-specific knowledge (e.g., common issues across all GDPR assessments in finance industry) which makes the AI smarter and the product more valuable. Being early to invest means being part of shaping a new category of “AI-assisted consulting”. And like the other ventures, its open-source core means it could become a de-facto platform for AI-guided documentation in many fields, driving widespread adoption. This broad applicability, combined with the immediate niche focus, makes it an exciting and scalable opportunity.

Vision, Execution, and Synergy

At a high level, all four startups form parts of a cohesive vision: **leveraging GenAI and semantic tech to solve complex information problems in cybersecurity and beyond, in an open and scalable way**. Dinis Cruz’s approach is akin to assembling a puzzle – each company addresses one piece, and together they address the broader challenge of understanding, communicating, and filtering the deluge of information in modern tech-driven organizations. The execution of running four startups in parallel is ambitious, but it’s grounded in a clear logic:

- **Symbiotic Development:** Each startup’s output serves as input or enhancement for another. This creates a feedback loop of improvement. For example, better persona communication models from The Cyber Boardroom can be reused in the Report Assistant’s dialogue system. Improvements in semantic parsing and graph databases from MyFeeds and the Content Filter make the board briefings more data-driven and the reports more evidence-based. This symbiosis means progress is non-linear – an advance in one propels all four forward, giving a small, focused team outsized productivity. It’s a deliberate strategy to maximize R&D efficiency by avoiding siloed efforts.
- **Distinct Focus, No Internal Competition:** Each venture has a clearly delineated focus area (governance communication, personalized intel, content filtering, report generation). By **keeping each scope narrow and unique**, the risk of overlapping or cannibalizing efforts is minimized. Instead, each team can become best-in-class at its specialty. This also simplifies the story for each individual startup when talking to customers: the Cyber Boardroom pitch is about board communication, and it doesn’t get muddled with, say, content filtering features – those are separate products. Dinis has consciously turned down opportunities to add other projects that did not offer a unique complementary angle, ensuring that the “first four” cover distinct bases with high synergy.
- **Unified Open-Source Ethos:** All four startups share not just code but a philosophy of openness. This cultural alignment makes it easier to manage them together – developers and contributors move fluidly between projects, and knowledge is shared freely. It also means the ecosystem can attract like-minded talent and partners. Open-source is the foundation that allows a small operation to have a **broad impact and reach**. Dinis is known for his leadership in open-source security tools [3] , and he’s using that experience to ensure these ventures punch above their weight by engaging the community. In practice, this might mean one GitHub organization where all the code repositories live, frequent technical blog posts or whitepapers (like the one that attracted interest via docs.diniscruz.ai), and a transparent development roadmap for each product. Investors can take comfort that this transparency also extends to development rigor and security – particularly important when dealing with enterprise software.

The **vision** driving all this is to create an integrated suite of AI assistants for the modern enterprise: from the boardroom to the back office, from daily news to official reports, and from filtering external threats to amplifying internal communication. Each product has a standalone market and revenue potential, but collectively they position Dinis Cruz’s portfolio at the forefront of AI adoption in cybersecurity and IT. It’s a bit reminiscent of how office productivity suites started as separate tools (word processor, spreadsheet, email) and later became a unified package – here we have separate “intelligent assistants” that together form a holistic toolkit for knowledge and security management.

Execution so far has been lean and rapid. In roughly a year’s time, four MVPs were built – an unheard-of pace in enterprise software – made possible by the open-source, serverless approach and by reusing components extensively. This showcases the execution capability of the team and the founder. Moving forward, execution will focus on **hardening each product and growing its user base** without losing the agility that the shared approach provides. Coordination among the four efforts will remain a priority to ensure they continue to complement rather than compete or diverge.

Traction and Next Steps for Each Startup

All four ventures are presently in the **MVP/early-user stage**, demonstrating the core functionality in real-world scenarios:

- **The Cyber Boardroom:** MVP is built and being used in a limited capacity by a few cybersecurity executives for testing. They have successfully generated board reports and refined their presentations using the AI. Next steps: formalize pilot programs with 2-3 organizations (likely mid-size companies with active security governance needs), iterate on features like integrating real corporate metrics, and prepare for a broader launch. The aim over the next 6-12 months is to go from prototype to a product that a CISO can subscribe to and use regularly with their board meetings. Key hires or partnerships (with say, a consulting firm that does virtual CISO work) might be pursued to reach initial customers.
- **MyFeeds.ai:** The personalized feeds service is live in MVP form, curating content for a small set of test users. It has shown tangible value by saving users time and alerting them to items they weren't aware of. The near-term plan is to enrich the content pipeline (adding more sources and perhaps including user's internal content, like an internal wiki, for an even more personalized feed) and improve personalization algorithms through user feedback. In parallel, MyFeeds will likely roll out a beta signup for cybersecurity professionals to grow a waiting list and gather more data on what content people are most interested in. This will validate pricing assumptions (e.g., who will pay and how much for curated intel).
- **Semantic Content Filter:** Prototype development is underway and expected to reach a demonstrable stage soon (for example, a browser extension or a local proxy app that early testers can install). Once a basic version is ready, the plan is to test it in specific scenarios – one identified path is a **"safe browsing" solution for kids and families**, which could be tested with a small user group of parents to fine-tune the filters. Another path is an **enterprise pilot focusing on phishing protection**, which might involve working with one company's IT/security team to deploy the proxy for a subset of employees and see how it catches malicious sites or content. The feedback from these tests will help decide which market to prioritize. On the technical front, a lot of next-step work involves optimizing response time and reducing operating cost per page scanned (to ensure it's commercially viable at scale).
- **Interactive Report Assistant:** The MVP is in use internally for GDPR report generation and possibly being trialed by a friendly consulting team. The concept has proven effective in guiding a less experienced user through an assessment. Next steps include automating more of the template customization (to easily switch between report types), and improving the AI's question set using domain experts' input (for example, making sure the AI asks all relevant GDPR questions by cross-referencing the regulation articles systematically). A controlled launch is anticipated, perhaps offering a limited beta to consulting firms or internal audit teams. That would yield insight into what features are most needed before a wider release (for example, some might want the ability to collaborate – multiple people working on a report – which could be a future addition).

From an **investment perspective**, the immediate ask is funding to accelerate these next steps. Each startup is likely to use the infusion to hire key personnel (developers or domain experts), invest in product refinement, and kick off customer acquisition efforts (marketing, sales outreach, or channel partnerships as appropriate). Dinis envisions possibly raising separate seed rounds for each company (since they target different markets and could eventually spin out as standalone businesses), but there is also room for an investor who believes in the overall vision to take a stake across the portfolio – effectively backing the strategy as a whole. The flexibility is there; what matters is aligning with investors who support the open-source, multi-venture approach and who can add strategic value (for example, introductions to potential early customers, or experience in scaling enterprise SaaS businesses).

Why Invest: The Open-Source Advantage and Market Potential

Investing in Dinis Cruz's quartet of startups offers a unique value proposition:

- **Multiple Shots on Goal:** Rather than one idea, you're effectively backing four highly related ventures. This diversifies risk – if one idea encounters market headwinds, another might take off – while still maintaining a unifying theme. It's akin to a mini portfolio approach, but with the advantage that success in one directly lifts the others (through shared tech and cross-selling opportunities). The chances of overall success are amplified by this mutual reinforcement.
- **Open-Source as a Market Accelerator:** All four companies are built on open-source foundations, which can lead to faster adoption. Consider the numerous successful open-source-based companies in the past (Red Hat, Elastic, HashiCorp, etc.): they achieved widespread use quickly because developers could freely try and deploy their tech. Here, Dinis is applying that model to AI-powered enterprise tools. Anyone can experiment with the core technology, but monetization comes from managed services, advanced features, and integrations – a proven playbook. For an early-stage investor, this means these products could gain global userbases with relatively low marketing spend, as communities pick them up. Furthermore, open-source projects can attract top engineering talent attracted by the mission and transparency, which is a boon for a startup's growth. Dinis's reputation in cybersecurity (former OWASP board member and creator of open security tools [6]) lends credibility that will help in building those communities.
- **Founder's Vision and Execution Track Record:** Dinis Cruz has over two decades of experience straddling technology and business roles [5] . He has been a CISO and CTO, and has firsthand knowledge of the problems these startups are solving. His focus on "GenAI-powered environments where engineering and security act as business accelerators" [4] speaks to the core of what these products aim to do – use AI to unlock business value from technical processes. In a short time, he has executed on this vision by delivering four MVPs, demonstrating an impressive ability to drive projects forward. Investors can have confidence in his technical leadership and passion for open-source innovation (a domain in which he's recognized [3]). Moreover, his network in the cybersecurity and tech industry is a significant asset – it can be leveraged to form partnerships, get early customers, and recruit talent.
- **Market Timing and Demand:** The convergence of AI and cybersecurity (and generally AI in enterprise functions) is at a critical momentum. Companies are actively seeking ways to harness LLMs but in safe, domain-specific, value-generating manners. Each of these startups hits a timely need: Board communication about cyber risk is a hot topic (boards are more concerned than ever about security); personalized information feeds address the issue of alert fatigue and staying ahead of threats; intelligent content filtering responds to the demand for better online safety and compliance; and AI-assisted reporting taps into the massive trend of using AI co-pilots to boost knowledge work productivity. Early investors in such spaces stand to benefit not only financially but by being at the forefront of shaping how AI is adopted in these critical areas.

In summary, an investment now is an opportunity to support a **portfolio of cutting-edge solutions** led by a seasoned innovator in security and AI. The open-source, multi-startup strategy is a bold approach that is already bearing fruit in terms of rapid development and integrated capabilities. With the right funding and partnerships, these ventures are well-positioned to capture significant value. Whether taken individually or as a whole, they have the potential to become indispensable tools in their respective niches. The foundation has been laid – minimal viable products, core technology built, initial users showing excitement – and the next chapter involves scaling up and conquering the market. Early investors will play a key role in that journey, providing not just capital but guidance and connections to fully realize this vision.

Conclusion: Dinis Cruz's current strategy is to innovate fast, leverage open source, and address big problems through focused solutions that interlock. This briefing has outlined how each startup functions, their progress, and their potential. The strategy's strength lies in its coherence and the founder's deep understanding of the domain. For investors, it represents a chance to be part of a **transformative approach to enterprise AI adoption**, one that could yield multiple winners. The invitation is open to join this endeavor, contribute to its growth, and share in the success of bringing these pioneering technologies to market. Each of the four startups stands on its own merits, but together they signal something even more ambitious – a reimagining of how open-source AI solutions can be built and scaled in tandem to drive business value across the board.

---

[1] [2] [3] [4] [5] [6] Threat Mod Con
https://www.threatmodcon.com/speaker/dinis-cruz