ChatGPT

ColleaiQ – Proactive AI Cybersecurity Website Plan

Animated Graph Background (Visual Feature)

Concept mock-up of ColleaiQ's hero section with a network graph motif in the top-left.
A signature visual element is a **subtle animated graph network** anchored at the top-left of the viewport. This network consists of **larger nodes** and **clearly visible connecting lines** forming an abstract “cyber mesh” backdrop. The graph softly animates – nodes might **pulse or slowly drift** and connecting lines gently morph – to convey a living network without distracting from content. For example, nodes could very slowly orbit or pulse at ~0.5 Hz, creating a calm motion. The animation can also **react subtly to user input** (e.g. a slight ripple when the user scrolls or moves the cursor near the graph) to give a feeling of interactivity. This design is more pronounced than a typical faint background pattern, ensuring the motif is noticeable and on-brand.

To implement this efficiently, we will utilize an HTML5 **Canvas** or **SVG/WebGL** approach rather than animating numerous DOM elements. A proven option is the lightweight **particles.js** library (or a modern equivalent), which is designed for animated node/line backgrounds [1]. This approach can maintain high frame rates and GPU acceleration for smooth performance. Unlike heavy CSS animations on many elements, a canvas/WebGL solution can handle dozens of moving nodes with minimal CPU load [2]. We will configure the graph with a **limited number of nodes** and **modest velocities** to keep motion subtle and performance overhead low. As a progressive enhancement, if the canvas or animation is unsupported or if the user prefers reduced motion, the site will gracefully fall back to a static background image of the graph.

Dark Mode Inversion: The site supports light/dark themes, and the graph’s colors invert to preserve contrast and ambiance. In light mode, the background is a warm cream and the graph lines/nodes may appear in a soft sepia or muted gray. In dark mode, the backdrop switches to a deep graphite color, while the graph’s nodes and lines glow in a warm beige/sepia tone for contrast. This inverted scheme maintains the visual motif while meeting accessibility in both themes. For example, a pale beige node on a nearly-black background stands out clearly without harshness. We will ensure the animation and colors are synced with theme toggling – e.g. by updating the canvas drawing colors on theme change. The result is a consistent, tech-inspired aesthetic: an ever-present network **connecting across the layout**, reinforcing ColleaiQ’s focus on interconnectivity and proactive monitoring.

Persistent Preview Disclaimer (UX & Transparency)

Across all pages, we will display a **persistent disclaimer banner** at the very top to ensure transparency. The banner text (in a clear sans-serif font) will read: *“This is a preview website for ColleaiQ. The product is under active development and does not yet match all specifications shown. If you’re interested, contact us — we’d love to talk.”* This notice is immediately visible on entry (aligning with UX best practices that emphasize **visibility and accessibility** of important disclaimers [3]). The banner will have a distinct but not overbearing style: for the light theme, a **muted red** background (a desaturated, warm red that catches attention without glaring) with white or dark text; for the dark theme, a **dark sepia/brown** background with light text. These color choices convey an “alert” feel (red tones suggest caution/preliminary status) while blending with the site’s warm color palette.

The disclaimer bar will be relatively compact in height and can be designed as a dismissible alert. On the right side, a small “✕” close button allows users to hide the banner if desired. If dismissed, we’ll use a cookie or session storage to keep it hidden for that session, so returning visitors see it anew (ensuring first-time visitors always get the message). The banner’s text includes a call-to-action (“contact us”) which will be a hyperlink to the **Contact** page or email, making it easy for interested parties to reach out. By maintaining this notice site-wide, we set correct expectations about the beta nature of the product. The tone remains professional and inviting — acknowledging that not all features are finalized, while encouraging engagement. Visually, the banner will use high-contrast text for readability (meeting AA contrast standards) and will not obscure other content (it will push the page content below it). This approach balances transparency and user experience: the banner is prominent but can be dismissed once read.

Red-Team Card Visual Cleanup

It’s crucial that all UI components appear polished and free of glitches. One specific element is the **Red-Team Agent card**, which in earlier drafts showed some stray visual artifacts (e.g. unexpected lines or misaligned accents). We will refine the card’s design to ensure clean rendering. For example, if the Red-Team card uses a colored border or a decorative stripe to indicate its “red team” role, we’ll make sure that border is properly confined to the card edges with no breaks. In previous styling, a small misaligned pseudo-element caused a tiny red line to protrude from the card’s border. We will remove or correct such code so that only the intended borders are visible. Likewise, any icon or badge on the card (such as a red target icon or shield) will be positioned and scaled consistently, without clipping.

Example of a Red-Team Agent card before cleanup, where a blue dot/line appeared misaligned.

In the example above, a **blue dot** and partial line were unintentionally visible on the Red-Team card’s edge – likely a leftover from a connection graphic or a pseudo-element. To fix this, we will ensure that **decorative connectors or highlights are properly aligned** or removed. If the design calls for linking the Red-Team and Blue-Team cards (for instance, via a connecting line or arrow to show interaction), we’ll implement it in a deliberate way (e.g. an SVG line between card elements) rather than using overflow on the card itself. Every border, shadow, and icon will be tested at various screen sizes and pixel ratios to avoid rendering artifacts (e.g. no 1px lines appearing due to subpixel issues). By cleaning up these details, the Red-Team card will have a crisp appearance: perhaps a subtle red outline or header, a neatly placed team icon, and no unintended marks. This polish will apply across all similar components (Blue-Team cards, agent panels, etc.), yielding a consistent and professional UI. Any use of pseudo-elements for stylistic effects will be audited so they don’t introduce glitches, and we’ll stick to simple, robust CSS for borders and backgrounds. The result is a visually clean interface, with the Red-Team card’s styling clearly conveying its purpose (through color and icon) without any distracting flaws.

Theming and Visual Design Consistency

The site’s overall look and feel will follow the previously established **cream/beige color palette** with warm, professional tones. In light mode, backgrounds will predominantly be an off-white or light cream, paired with dark charcoal or espresso-colored text for high readability. Accents – like the network graph lines, icons, or section dividers – can use shades of sepia, brown, or muted red/blue (to correspond to red-team/

blue-team elements) that complement the warm palette. In dark mode, we invert to a **deep graphite** background (near black with a hint of warm tint) and use light text in beige or light gray. All interactive elements, logos, and graphics are designed to work on both backgrounds (for instance, the ColleaiQ logo and any illustrations will have versions or styling that swap colors in dark mode).

A **theme toggle** switch will be provided (likely in the site header) to let users seamlessly switch between light and dark modes. The toggle will be intuitive (e.g. a sun/moon icon) and accessible (with an aria-label like “Toggle dark mode”). On activation, the CSS variables or classes controlling colors will update, and elements like the animated graph background will redraw in the appropriate colors (warm lines on dark background, or vice versa, as discussed). We’ll ensure the theme toggle state persists (using localStorage) so that returning visitors see their preferred theme. Maintaining a consistent look in both modes is key – we will use the same base typography and layout, adjusting only colors and shadows as needed. For example, the muted red used in the disclaimer or error highlights in light mode might appear as a **darker brown/red** in dark mode for equivalent visibility. Every page will be reviewed in both themes to guarantee sufficient contrast (meeting accessibility guidelines) and aesthetic coherence.

Importantly, the **graph motif** will appear throughout the site in subtle ways beyond the hero background. This might include faint network-line patterns in section backgrounds or as part of images and icons, reinforcing the brand identity. For instance, section headers or the footer might have a very light watermark of connected nodes. These will be low-opacity and not interfere with text. By consistently using the network graph imagery, we create a visual thread tying all pages together. Yet we will **avoid overload** – the motif will be used judiciously so that it enhances the design without making pages feel busy. The end result is a cohesive visual design: warm, professional, and unmistakably themed around **networks and cybersecurity**.

Interactive and Real-Time Features

To engage our target audience of cybersecurity specialists, the site will incorporate **real-time interactive components** that demonstrate ColleaiQ’s capabilities. One highlight is a **multi-agent simulation visual** on the **Simulation** page (or embedded in the landing page). This could take the form of an animated diagram showing red-team and blue-team AI agents in action. For example, we might display a small network of devices or services (nodes) being probed by a Red-Team agent, with the Blue-Team agent monitoring and responding. As the simulation runs, viewers can see an “attack” being attempted and then caught. This might be represented with icons (a red agent spider or virus icon moving toward a server icon, and a blue shield icon intercepting it), along with brief text or tooltips explaining each step. The animation can loop through a scenario: **Red agent** launches a test exploit, **Blue agent** detects it, and the system produces a report or fix suggestion. We will design this in a lightweight way – possibly using CSS animations or a small JavaScript animation (e.g. D3.js or GSAP for orchestrating SVG elements) – so that it doesn’t require heavy computation but still gives a dynamic **“live demo”** feel.

Another interactive element will be an **Attack Timeline** component. This could be a timeline UI that highlights the sequence of events during a cyberattack simulation. Each milestone (attack detected, system isolated, patch deployed, etc.) can appear as a point on a horizontal timeline that animates in as you scroll to it. Visitors could scrub through or click steps to see details. For instance, a timeline might illustrate the response to a new vulnerability: at *T0* a vulnerability is disclosed, at *T1* ColleaiQ’s red agent automatically attempts an exploit in a sandbox, at *T2* the blue agent identifies the attempt in logs, at *T3* a recommendation is generated, and so on – finally an analyst approval at *T4*. This narrative mirrors a real incident response, showcasing how ColleaiQ **works faster than a traditional reactive approach**. We will ensure this is interactive (hovering or clicking a step could pop up a short description) to invite exploration. Such visual storytelling will help specialists understand the workflow and the value of proactive defense.

We also plan to include **interactive diagrams** under the **Solution** section to explain technical concepts like the multi-agent architecture. For example, a diagram of the system architecture could respond to user input: hovering over “Red Team Agent” might highlight that part of the diagram and display a summary of its role, while hovering “Blue Team Agent” shows its role. Similarly, an interactive network graph could illustrate how agents communicate – perhaps animating lines between Red and Blue agents indicating data sharing or cooperative decision-making. By directly engaging the user with these visuals, we make the complex technology more tangible. However, we will keep these interactions **optional and intuitive** – the content will also be explained in text, so a user who doesn’t interact still gets the information. All interactive elements will be tested for performance (e.g. pausing animations if off-screen or after one loop) to avoid hogging resources.

Content Structure and Pages

The website will be organized into clear sections/pages to cover all the key information, with a navigation menu linking to: **Landing**, **Mission**, **Solution**, **Simulation**, **Compliance**, **Blog**, **Contact**, **Careers**, and **Community**. Each section will be crafted with cybersecurity professionals in mind, maintaining a **professional and explainable tone** – i.e., authoritative but avoiding unnecessary jargon, and explaining any technical terms or acronyms.

- **Landing Page:** This is the introduction and overview. It will feature a strong headline, e.g. *“Proactive, Explainable Cyber Defense Powered by Multi-Agent AI”*, encapsulating ColleaiQ’s value proposition. A subheading or brief paragraph will clarify that ColleaiQ continuously simulates attacks and fortifies defenses so organizations “don’t have to wait for the next incident” [4]. The animated graph background is prominent here, and possibly a call-to-action (“Learn More” or “Get in Touch for a Demo”) is included. We might also place a concise **tagline or mission statement** here for quick impact. For example: *“ColleaiQ is building proactive cybersecurity using specialized AI agents that continuously hunt threats, explain their findings, and help your team stay ahead of attackers.”* The landing can also showcase an eye-catching visualization – perhaps a snippet of the simulation or a rotating set of key benefits (Proactive Protection, Continuous Learning, Compliance-Ready, etc.). Overall it should immediately communicate **what ColleaiQ does and why it’s different**, in a polished, visually engaging manner.

- **Mission:** The mission section/page delves into *why* ColleaiQ exists and the problem it addresses. We will describe the current cybersecurity landscape: escalating threats, new regulations, and talent shortages. For instance, we’ll note the rise of advanced attacks and the fact that many breaches are increasingly costly. (We can mention real examples like *“the NotPetya attack cost shipping giant Maersk up to $300M in damages* [5] *, and a 2025 ransomware incident disrupted major European airports’ operations* [6] *, underscoring the stakes.”*) We’ll highlight that traditional reactive security is no longer enough when faced with unknown *zero-day* exploits and AI-accelerated threats. Additionally, the mission can cite the **cybersecurity skills gap** – e.g., millions of cybersecurity roles are unfilled globally [7] – which is why intelligent automation is needed to augment human teams. This context builds the case for ColleaiQ. We then articulate ColleaiQ’s mission: *to empower organizations with an AI “colleague” that proactively strengthens their defenses*. We’ll emphasize values like **proactivity,**

explainability, and reliability. The tone will be passionate but credible, showing that ColleaiQ isn't just a product, but part of a larger mission to build resilience in an era of heightened cyber risk.

- **Solution:** The solution page is where we explain *how ColleaiQ works* and what features it offers. Here we introduce the concept of the **multi-agent system** – a team of AI agents with different roles working together (inspired by real Red Teams and Blue Teams). We'll break down the core components:

- **Red-Team Agents:** These AI agents simulate attackers. They continuously and safely attempt intrusions in controlled sandbox environments, mimicking tactics from known breaches and novel techniques. This proactive approach helps uncover vulnerabilities (even *zero-day* weaknesses) *before* real attackers do [8]. We'll note that by internally "red-teaming" your systems, ColleaiQ finds holes that would otherwise remain hidden.
- **Blue-Team Agents:** These agents act like defenders. They monitor system logs, network traffic, and the Red-Team's activities to detect suspicious patterns. Blue agents fuse signals from various sources and can recognize the Red-Team's simulated breaches, thereby validating that detection mechanisms work. They also watch for real external threats in live data, providing around-the-clock coverage.
- **Continuous Learning:** A key benefit is that both sets of agents learn and improve. When a Red-Team simulation finds a gap or a Blue-Team agent catches something, the platform **logs the outcome and adapts**. We'll highlight that every recommendation or alert ColleaiQ produces is accompanied by a clear explanation and evidence (fulfilling the explainability requirement). Every action by the AI is **traceable and auditable by design** [9] – unlike "black-box" tools, ColleaiQ shows the rationale behind its decisions. This traceability builds trust: analysts can review why an alert was triggered and see the chain of reasoning.
- **Human in the Loop:** We stress that ColleaiQ works **with** human analysts, not replacing them. For example, when ColleaiQ suggests a fix or flags an incident, it presents the information for a human to verify. The system *augments* the security team by handling repetitive scanning and first-line analysis, while letting humans make final decisions – combining the speed of AI with expert judgment. As our materials say, ColleaiQ is a "digital colleague" that **automates tedious work but keeps humans in control** [10].
- **Integration & Deployment:** We will mention that ColleaiQ is designed to integrate into existing security workflows. It's not a standalone black-box appliance; it provides APIs and supports data integration so it can plug into a company's SOC tools, ticketing systems, and cloud environments [11]. This means adoption can be incremental and it amplifies what organizations already have.

Visually, the Solution page may include diagrams or icons for each of these points (e.g. a pair of interconnected red and blue icons, a shield with a checkmark for explainability, etc.). The copy will focus on benefits (finding zero-days internally, reducing incident surprise, saving analysts' time, improving compliance readiness) backed by how the multi-agent approach achieves them. We will also differentiate from standard solutions: for instance, unlike purely anomaly-based AI products, our multi-agent coordination **actively probes for weaknesses** and **plans responses**, which single-agent or rule-based systems can't do [12] [13]. The competitive edge is that proactive simulation yields fewer surprises and a stronger security posture [14]. All these points will be written in an explanatory manner – complex enough to appeal to specialists, but clearly broken down.

- **Simulation:** This section highlights a concrete example of ColleaiQ in action. We will present a **sample attack simulation scenario**, walking the user through it step by step (potentially with the interactive timeline as discussed). For instance, the scenario: *"A new critical vulnerability (CVE-XXXX) is* _announced._ ColleaiQ's Red agents automatically generate an attack based on the CVE description and attempt it in a sandbox environment. The Blue agents detect the behavior as malicious (since they see abnormal changes in the sandbox's telemetry) and immediately flag it. The system determines whether the vulnerability could exist in the production environment by comparing configurations. It then outputs a **traceable fix recommendation** – for example, a patch or a configuration change – complete with an explanation of the impact and risk ⑮. A human analyst is notified with an alert and can **replay the simulation** or review logs to verify ColleaiQ's findings ⑯. Finally, the analyst approves and implements the recommended fix, and this feedback is fed into ColleaiQ, so the agents learn from the analyst's decision ⑰." _This narrative shows the full cycle from threat emergence to automated defense and human confirmation. We will format this story visually or as a short narrative on the page, reinforcing how proactive and iterative the system is. The Simulation page may also allow users to see multiple scenarios (e.g., a ransomware attempt vs. an insider threat simulation) to demonstrate versatility. The content here is meant to bring the technology to life and assure the user that ColleaiQ has been tested in realistic conditions_*. Any real metrics (if available, like "ColleaiQ discovered X unknown vulnerabilities in a pilot test") could be included as proof, although being a preview, we might focus on qualitative description.

- **Compliance:** This page will detail how ColleaiQ helps organizations meet frameworks like **NIS2, GDPR, ISO 27001** and other cybersecurity regulations. We will note that as of 2025, the EU's NIS2 directive imposes stringent cybersecurity requirements on thousands of companies, making practices like regular risk assessments, incident reporting, and _explainable AI decisions_ essential ⑱. ColleaiQ is built with compliance in mind: it generates **auditable logs** of all simulations and actions, which can be used as evidence for compliance audits. For example, if NIS2 requires demonstrating that you test your defenses and have response plans, ColleaiQ's continuous simulations fulfill that by design (each simulated attack and outcome is recorded). We'll also emphasize the **explainability** aspect here again – because regulators and standards (like NIS2 or future AI regulations) stress transparency, ColleaiQ's ability to show _why_ it flagged an issue or made a recommendation directly supports that need. Additionally, we could mention that ColleaiQ respects safe practices (it operates in isolated sandbox environments and under human oversight ⑲ ⑳) so it does not compromise the production systems or data privacy. Essentially, this page assures risk managers and compliance officers that adopting ColleaiQ will **strengthen their compliance posture rather than complicate it**. We might include specific mappings, e.g., "ColleaiQ can help satisfy requirements of NIS2 Article XYZ by providing continuous testing and incident logs." The tone will be straightforward and factual, aligning with the detail-oriented mindset of compliance professionals.

- **Blog:** The blog will serve as a knowledge hub and thought leadership platform. It will be designed with a clean, easy-to-read layout (large text, high contrast, and perhaps the option to filter by category like "AI Research", "Cyber Threats", "Company News"). We intend to publish articles relevant to cybersecurity specialists: e.g., insights into new attack techniques (and how AI can counter them), explainers on multi-agent AI, compliance tips for NIS2, and updates on ColleaiQ's development journey. By maintaining the subtle graph motif in the margins or header, the blog will still feel connected to the main site design. Each post will have social sharing, and possibly a comments or discussion integration (or a prompt to join the community forum, if we set one up). The blog content will reinforce ColleaiQ's credibility – showing that our team is up-to-date with the latest trends (for instance, a post might discuss how _GPT-4 was shown to autonomously exploit 87% of known vulnerabilities ㉑, and what that means for defenders_). This kind of content appeals to our target audience by acknowledging the evolving threat landscape and positioning ColleaiQ at the cutting edge of defense. We'll ensure the writing style remains professional and informative, which helps build trust with readers.

- **Contact:** The contact page will provide all the necessary information for interested parties to reach us. This includes a **contact form** (with fields for name, email, company, and message) and a direct email link (such as contact@colleaiq.dk). We will also list any relevant phone number or physical office address if appropriate. Given the banner's invitation to contact, this page should be welcoming and encourage people to start a conversation – we might say *"Whether you have questions about our tech or want to explore a pilot project, we'd love to hear from you."* The design will be simple and clean, possibly with a smaller graph background element to keep the style. We will also include links to ColleaiQ's social media or LinkedIn if available, and perhaps a note about response time ("We typically respond within 1-2 business days"). Since the product is in development, a key goal is to **capture leads and potential collaborators**, so the contact page is important to get right (clear, easy, and reliable in sending messages).

- **Careers:** Even as a startup under development, we dedicate a section to careers to signal growth and attract talent. This page will outline the kind of team we are and possibly list open positions (if any) or expected roles in the near future. We might not have specific job postings yet, so the content could say *"We're always looking for passionate talent in AI, cybersecurity, and software engineering. If you're excited about our mission to build proactive cyber defense, get in touch!"* For transparency, we could mention our founding team (as per our pitch: AI engineers from DTU, etc.) and the areas we plan to expand (e.g., "In the coming months we'll be seeking experts in cybersecurity operations and business development to join us"). Even if no formal openings, a link to send an unsolicited application or an email is useful. Design-wise, we keep it consistent, perhaps including a group team photo or a graphic. The tone here is enthusiastic and inclusive, emphasizing the chance to work on cutting-edge tech for a meaningful purpose.

- **Community:** The community page will help build an ecosystem around ColleaiQ. Since our target users are specialists who often share knowledge, this page can point to resources and forums where people can engage. For instance, we might set up a **Discord/Slack group or a forum** for discussions about AI in cybersecurity. The community page would invite users to join these channels to discuss ideas, get updates, or even contribute feedback to ColleaiQ's development. Additionally, this section can highlight any events or partnerships: e.g., if ColleaiQ participates in cybersecurity conferences, hackathons, or academic collaborations (since we have ties to DTU), we can list those here. A newsletter sign-up could also appear here for those who want email updates. Overall, the community page fosters a sense that ColleaiQ is not just a product, but a collaborative effort with the broader cyber defense community. The content will encourage **knowledge exchange and feedback**, perhaps saying *"Join our community of cybersecurity professionals and researchers as we explore the future of proactive defense together."* By engaging the community, we also subtly validate our approach (crowdsourcing ideas, showing openness to red-teaming our own product, etc.). The style of this page will remain aligned with the rest (graph motifs, etc.), but with perhaps more informal language to be welcoming.

Throughout all pages, we maintain a **professional, clear tone**. We avoid hyperbole and instead back statements with reasoning or evidence (citing known stats or requirements). The language will be accessible – for example, we'll explain terms like "multi-agent system" or "NIS2 compliance" in brief if they appear, so even a non-specialist investor or executive reading the site can understand the gist. Yet, the content will not be dumbed down; cybersecurity professionals will find the level of detail and terminology appropriate. Any claims we make (like improving security or compliance) will be followed by an explanation of *how* (to stay credible).

Performance and Accessibility Considerations

Finally, we will ensure that all these features are delivered in a performant and accessible way. On the performance side, the site will employ best practices: minified assets, lazy-loading images and animations (e.g. the heavy simulations won't run until the user scrolls to them), and using CSS effects over JavaScript when possible for simpler animations. The background graph animation will be tuned to not consume excessive CPU/GPU – using requestAnimationFrame and throttling itself when the tab is inactive. We'll also offer a "Reduce Motion" mode: if a user has `prefers-reduced-motion` set or if we notice performance issues, we can disable non-essential animations (the graph might then become a static image) so that users prone to motion sensitivity or on slow devices still have a good experience.

Accessibility is a priority: all text will have sufficient contrast against backgrounds (the warm beige palette will be chosen with contrast in mind; for example, body text on cream will likely be a dark brown #2b2b2b which on a light beige still yields a contrast ratio above 7:1). We will add **alt text** to all images and ensure that any infographic or animated diagram has an accompanying description. Interactive elements will be keyboard-navigable (e.g., the timeline can be tabbed through, the theme toggle is a proper button). ARIA roles and labels will be used where appropriate, such as marking the disclaimer as a "status" or "alert" role so screen readers announce it. We'll also ensure the site works across browsers and devices – the layout will be responsive (the graph background might be hidden or simplified on mobile to save space and CPU, for instance).

By adhering to these performance and accessibility standards, we make sure the fancy visuals and dynamic content do not come at the expense of user experience. The outcome will be a **polished marketing website** that not only looks cutting-edge with its animated graph and rich content, but also feels smooth to use and instills confidence through its clarity and professionalism. Each element – from the disclaimer banner building trust, to the cleaned-up UI components, to the comprehensive content sections – contributes to a cohesive presentation of ColleaiQ as an innovative, reliable, and user-focused cybersecurity solution. With this website, cybersecurity specialists and other stakeholders will quickly grasp what ColleaiQ offers and be encouraged to learn more or get in touch, all while enjoying a visually engaging yet performant browsing experience.

Sources:

1. ColleaiQ Funding/Overview Document (2025) – Explanation of ColleaiQ's proactive multi-agent approach and compliance focus ㉒ ⑱ .
2. ColleaiQ Pitch Deck (2025) – Competitive advantages of explainable, proactive simulation and human-AI collaboration ㉓ ⑩ .
3. TechRepublic (2024) – Study finding that GPT-4 can autonomously exploit 87% of described vulnerabilities ㉑ .
4. Reuters (2025) – Report on cyberattack disrupting European airports in Sep 2025 ⑥ .
5. Digital Guardian (2017) – Report on NotPetya malware causing $200–300M losses at Maersk ⑤ .
6. National University Cybersecurity Stats (2024) – Projected 3.5M unfilled cybersecurity jobs by 2025 ⑦ .

7. Stack Overflow (2018) – Recommendation of particles.js for interactive node animations (network/dots background) ① .
8. GetGenAI Blog (2025) – Emphasis on making disclaimers highly visible and accessible to users ③ .

---

① html - How to create a website background full of moving 'nodes' that responds to mouse movements? - Stack Overflow
https://stackoverflow.com/questions/51619667/how-to-create-a-website-background-full-of-moving-nodes-that-responds-to-mouse

② Performance of moving image on web page via CSS vs HTML5 ...
https://stackoverflow.com/questions/4842872/performance-of-moving-image-on-web-page-via-css-vs-html5-canvas

③ Best Practices for Disclaimer Placement: Expert Tips for Compliance and Clarity
https://www.getgen.ai/post/best-practices-for-disclaimer-placement-expert-tips-for-compliance-and-clarity

④ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳ ㉒ ㉓ ColleaiQ.pdf
file://file-FSVNYqtooGspZAezrmt6xq

⑤ The Cost of a Malware Infection? For Maersk, $300 Million | Fortra's Digital Guardian
https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million

⑥ European airports snarled by cyberattack, disruption to stretch into Sunday | Reuters
https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/

⑦ 101 Cybersecurity Statistics and Trends for 2025 | NU
https://www.nu.edu/blog/cybersecurity-statistics/

⑧ ColleaiQ___Skylab_Funding-13.pdf
file://file-86MHhpHNy6N5z1wWYZw3DX

㉑ OpenAI's GPT-4 Can Autonomously Exploit 87% of One-Day Vulnerabilities
https://www.techrepublic.com/article/openai-gpt4-exploit-vulnerabilities/