Qwen

Architecting a CTF & Conference Tracker MVP: An Engineering Blueprint for Automated Event Aggregation and Personalized Notifications

Data Sourcing and Ethical Ingestion Pipeline

The foundational pillar of the CTF & Conference Tracker is its ability to reliably ingest and normalize event data from a diverse array of sources. The strategy must prioritize ethical and efficient methods, adhering to the directive to favor official Application Programming Interfaces (APIs) and standardized feeds (RSS/ICS) over web scraping [96] [97]. This tiered approach not only respects the terms of service of source websites but also ensures higher data quality and reduces maintenance overhead. The primary sources can be categorized into official event aggregators, major conference organizers, and community-driven repositories.

The central hub for Capture The Flag (CTF) events is CTFtime, a platform indispensable for the tracker's core functionality [8] [70]. Its value lies in its aggregation of global CTF competitions, providing a single point of contact for a vast volume of events. While the specific terms of use and rate limits for the CTFtime API were not detailed in the provided context, such platforms typically offer public APIs for programmatic access to their curated data. The data fields available through such an API would logically include essential metadata like event name, start and end timestamps, duration, competition format (e.g., Jeopardy, Attack-Defense), platform link for registration, geographical location, and tags corresponding to challenge categories like Web, Crypto, Pwn, Forensics, and Reverse Engineering [7] [12]. Leveraging the CTFtime API represents the highest-priority ingestion path due to its comprehensiveness and reliability. For conferences, the sourcing strategy is more fragmented. Major events like Black Hat, DEF CON, and RSA often provide official schedules and call-for-proposal (CFP) pages on their websites [85] [86]. Some may offer official ICS or RSS feeds for their calendars, which would be the ideal target for automated subscription [20]. However, many conference sites rely on static HTML tables or dynamic JavaScript-rendered lists, necessitating a fallback to targeted scraping. Community events, particularly those organized under the BSides

banner, may maintain their own public calendars or use aggregators, representing a secondary tier of sources that require careful validation [5].

When official APIs and feeds are unavailable, ethical web scraping becomes a necessary component of the data ingestion pipeline. This process must be conducted with strict adherence to best practices to avoid overwhelming servers and to comply with website policies. The first step is to consult the `robots.txt` file of any target domain to identify prohibited crawling paths [96]. The scraper should implement a polite delay between requests, potentially using an exponential backoff strategy to increase wait times after encountering errors or rate limits. Identifying the bot with a custom, descriptive User-Agent string is a standard courtesy that facilitates communication with site administrators if issues arise. To prevent redundant network traffic and reduce server load, all fetched HTML should be cached locally, with re-fetching only occurring after a configurable time-to-live or when a cache-busting mechanism is triggered. Resilience against changes in website structure—often referred to as "anti-break" strategies—is critical for long-term maintenance. This involves relying on stable DOM selectors (e.g., semantic class names or IDs rather than fragile positional indices) and implementing robust error handling. Furthermore, all scraped content intended for display on the platform must undergo sanitization to mitigate risks of Cross-Site Scripting (XSS) and other injection attacks [60].

The following table summarizes the identified data sources, outlining their type, coverage, and operational characteristics. This serves as a strategic guide for developing the ETL pipeline.

Source	Type	Coverage	Update Frequency	Auth Needed	Rate Limit	Legal / Terms of Use Notes
CTFtime	API	Global CTF Events	Real-time / Near-real-time	No (for public data)	Unknown	Requires attribution; TOS must be reviewed for commercial use. Primary source for CTF data [8] [70].
Black Hat Official Site	HTML / API (if any)	Black Hat Conferences	Annually / Quarterly	No	Unknown	High-quality, authoritative data. Scraping requires respecting `robots.txt` and implementing polite delays [86].
DEF CON Official Site	HTML / API (if any)	DEF CON Conference	Annually / Quarterly	No	Unknown	Similar to Black Hat; data is authoritative but may require scraping [86].
RSA Conference Official Site	HTML / API (if any)	RSA Conference	Annually / Quarterly	No	Unknown	Authoritative source for one of the largest security conferences [2].
BSides Chapters (e.g., London)	HTML / ICS Feed	Local, regional events	Varies by chapter	No	Unknown	Excellent for niche events. ICS feeds, if available, are preferred over scraping [5] [85].
GitHub	API / HTML	CTF Write-ups, Conference Slides	Real-time (commits/ pushes)	No (public repos)	900 REST API points/min [40]	Goldmine for archive content. API allows programmatic discovery of relevant repositories [16] [37].
YouTube	API / HTML	Conference Talks, Recordings	Real-time (uploads)	Recommended (OAuth for full access)	900 points/min for unauthenticated calls [102]	Essential for video archives. API is preferred for structured data on talks and playlists [81].
Eventbrite / Meetup	API	Smaller meetups, informal CTFs	Real-time	Yes (API Key)	Varies by platform	Useful for discovering grassroots events, but data quality can be inconsistent [38].

The ETL pipeline will be designed as a series of discrete stages to ensure modularity and resilience. The **Collector** stage will contain source-specific modules (e.g., `ctftime_collector.py`, `blackhat_scraper.py`) that interact with the respective APIs or scrape HTML. These modules will run on a schedule defined by a task queue manager like Celery with Redis. Collected data is then passed to the **Normalizer**, which transforms disparate data structures into a unified internal schema. This stage handles tasks like mapping CTFtime tags to a standard category list, parsing various date formats into ISO 8601, and normalizing geographic locations. Following normalization, the **Validator** stage performs integrity checks, ensuring all required fields are present and conform to expected formats. This prevents malformed data from corrupting the database. Validated data is then stored in the PostgreSQL database, which is well-suited

for this task due to its robustness and support for flexible JSONB fields for storing normalized metadata [80]. Finally, the **Notifier** module is triggered, cross-referencing new or updated events against user preferences to initiate the appropriate notifications. Failure modes, such as source unavailability or rate limit exhaustion, will be handled gracefully through retry logic, exponential backoff, and centralized logging to ensure the system remains stable and self-healing.

Platform Architecture and Technology Stack

Designing a Minimum Viable Product (MVP) for the CTF & Conference Tracker requires a pragmatic yet scalable architecture. The goal is to deliver core functionality quickly while laying a foundation that can accommodate future growth. The proposed architecture is a modular, decoupled system where distinct components handle specific responsibilities, communicating primarily through a message broker and a shared database. This design enhances maintainability, allows for independent scaling of components, and aligns with modern software engineering practices.

The high-level architecture consists of several key components. On the client side, a frontend application built with Next.js provides a modern, responsive user interface for managing preferences and viewing tracked events [80]. This UI communicates with a backend API server via standard HTTP(S) requests. The backend, preferably built with Python and the FastAPI framework, acts as the core business logic layer. FastAPI is an excellent choice for this MVP due to its high performance, automatic generation of OpenAPI documentation which simplifies frontend integration, and native support for asynchronous operations, which is beneficial for I/O-bound tasks like making external API calls during data ingestion [80]. All incoming requests from the frontend are processed by this API server.

The heart of the data processing system is the ETL pipeline, orchestrated by a task queue manager. Celery, paired with Redis as the message broker and result backend, is a robust and widely adopted solution for this purpose [80]. The collector modules (responsible for fetching data from CTFtime, conference websites, etc.) are configured as asynchronous Celery tasks. This decouples the data ingestion process from the main web application, preventing long-running scrapers from blocking API requests and degrading the user experience. When a collector task completes, it places the normalized event data onto a processing queue. A separate set of workers consumes these tasks, performing validation and storage operations before passing the final data to the notifier. This separation of

concerns ensures that failures in data collection do not impact the availability of the primary web service.

For data persistence, a relational database like PostgreSQL is recommended. It offers strong consistency and ACID compliance, which is crucial for maintaining the integrity of user preferences and event records. The use of PostgreSQL's JSONB data type is a key architectural decision for flexibility. Core, structured data such as user IDs, event titles, and timestamps can be stored in typed columns, while the highly variable and semi-structured data from different sources (e.g., raw API responses, extended descriptions) can be stored in a JSONB field. This allows the schema to evolve without requiring disruptive schema migrations, a significant advantage for a rapidly developing MVP [80]. Additionally, a lightweight caching layer using Redis is essential. It can store frequently accessed data, such as pre-computed iCal feed contents for popular filter combinations, and be used by the scraper to cache fetched web pages, reducing redundant network requests and improving overall system responsiveness.

The following table outlines the proposed technology stack, justifying each choice based on its suitability for the project's goals.

Component	Recommendation	Justification
Backend Framework	Python with FastAPI	High performance, automatic OpenAPI docs, async support, and a large ecosystem make it ideal for a rapid MVP [80].
Frontend Framework	Next.js	Enables server-side rendering for fast initial page loads, has a rich component ecosystem, and provides a modern developer experience [80].
Scraping Library	Requests + BeautifulSoup4 (BS4)	Simple, efficient for parsing static HTML, and easy to integrate with Celery for asynchronous tasks. Playwright can be used later for JavaScript-heavy sites [80].
Scheduler & Queue	Celery with Redis	Decouples data ingestion from the main app, manages task retries, and provides a robust system for running periodic ETL jobs reliably [80].
Database	PostgreSQL	Industry-standard relational DB offering strong consistency. JSONB support provides the flexibility needed for evolving event schemas [80].
Cache	Redis	Low-latency key-value store useful for caching scraped web pages and pre-computed results to reduce server load and latency [80].
Search	Meilisearch (Optional)	If advanced text search capabilities become necessary in the future, Meilisearch offers a simple, powerful, and fast search engine that can be integrated with the existing stack [80].
Push Notifications	Firebase Cloud Messaging (FCM)	Provides a free tier and robust SDKs for sending real-time push notifications to web and mobile browsers [109][120].
Email Notifications	SendGrid or Mailgun	Reliable transactional email services with APIs for programmatic sending and analytics on deliverability [120].

The database schema for the MVP should be minimal but effective. At a high level, it will consist of at least three core tables: `Users`, `Event`, and `Preference`. The `Users` table will store user account information. The `Preference` table will link a user to their specific filters (categories, regions, etc.). The `Event` table will store all ingested event data, with columns for standard fields and a `metadata` column of type JSONB to hold the normalized, source-specific data. This design supports the core requirement of personalization by allowing the system to efficiently query events based on a user's stored preferences. The API endpoints will be straightforward, focusing on CRUD operations for user preferences and serving the personalized iCal feed. For instance, an endpoint like `POST /api/v1/preferences` would allow a user to save their filters, while `GET /api/v1/feed/{user_id}` would generate the unique URL for their subscription.

Personalization Engine and Notification System

The core value proposition of the CTF & Conference Tracker lies in its ability to move beyond simple data aggregation and deliver hyper-relevant, timely information directly to the user. This is achieved through a sophisticated personalization engine and a carefully managed notification system. The engine's primary function is to interpret user-defined interests and translate them into actionable intelligence, while the notification system ensures that critical updates are delivered without causing user fatigue or violating spam regulations.

The user preference model must be granular enough to cater to the specific needs of individual players and small teams. The MVP should support a multi-select filter system encompassing several key dimensions. First, challenge/event **Categories** are fundamental, allowing users to select their areas of interest, such as Web, Cryptography, Pwn, Forensics, Reverse Engineering, and others common in CTFs [7]. Second, **Formats** should be supported, distinguishing between common competition styles like Jeopardy and Attack-Defense [12]. Third, **Location and Accessibility** filters are crucial. Users should be able to specify a **Region** (e.g., North America, Europe, Asia-Pacific) and select their preferred **Location Type** (Online, Onsite, or both). This helps users find events that fit their logistical constraints. Finally, temporal and demographic filters like a customizable **Date Range** and preferred **Team Size** (e.g., Individual, 2-4 people) complete the preference profile. Storing these preferences in a dedicated `Preference` table linked to the `User` table allows for efficient querying and dynamic feed generation [80].

With the preference model established, the notification system must decide *what* to notify the user about, *when* to send the notification, and *how*. The choice of notification channel depends heavily on urgency. High-priority alerts, such as an imminent CTF starting in a few hours or a last-minute call for proposals, are best suited for immediate delivery via push notifications to a web browser or mobile app. Services like Firebase Cloud Messaging (FCM) or OneSignal are excellent choices, offering reliable delivery and free tiers for development [109][110]. For less urgent but still important information, such as a weekly digest of all new events added to the tracker, email is the appropriate channel. Email allows users to consume information at their own pace without the interruption of a push alert [105].

A critical aspect of the notification system is its anti-spam implementation. Overwhelming users with notifications is a primary reason for app uninstallation and poor reputation. Therefore, a multi-layered anti-spam strategy is non-negotiable. First, **frequency caps** must be enforced. For example, a user should not receive more than one push notification per hour for CTF start alerts, regardless of how many events meet the criteria. Second, a **priority scoring** mechanism should be employed to triage notifications. Not all events are equally important. A scoring formula could weigh factors like proximity to the event's start time (a penalty for events far in the future), alignment with the user's top-preference categories, and the event's exclusivity or prestige. Only events that surpass a certain score threshold would trigger an immediate, high-priority push notification. Third, offering a **digest mode** gives users control. They can opt to receive a single daily or weekly summary email instead of real-time alerts, catering to users who prefer batch processing of information over constant interruptions.

An illustrative scoring formula for determining notification urgency could be:

$$\text{NotificationScore} = (\text{StartTimePenalty} \times W_1) + (\text{CategoryRelevanceScore} \times W_2) + (\text{LocationPreferenceBo}$$

In this formula:

- **StartTimePenalty** decreases as the event start time approaches (e.g., -10 points for events > 7 days away, -5 for 3-7 days, 0 for < 3 days).
- **CategoryRelevanceScore** increases based on how closely the event's categories match the user's selected interests (e.g., $+10$ for a perfect match, $+5$ for a partial match).
- **LocationPreferenceBonus** adds a bonus point if the event matches the user's online/onsite preference ($+5$ for a match).

The weights (W_1, W_2, W_3) can be tuned based on user feedback and usage patterns. For instance, if users complain about missing online-only events, the weight for `LocationPreferenceBonus` could be increased. This dynamic, rule-based system ensures that the notification engine is both intelligent and adaptable, delivering maximum value while minimizing annoyance. The entire system—from preference storage to scoring calculation and channel selection—must be designed to be efficient and resilient, capable of handling thousands of concurrent users and millions of events without degradation in performance.

Archive Component and Content Strategy

The archive component of the CTF & Conference Tracker elevates the platform from a mere event calendar to a valuable resource repository. By automating the ingestion of write-ups, slides, and videos, the tracker provides a centralized hub for post-event learning and research, a feature highly valued by the target audience of players and small teams [29]. The strategy for this component focuses on automated acquisition from reputable, public sources, coupled with a meticulous metadata model and a strong commitment to ethical copyright practices.

The acquisition plan for archive materials must be systematic and automated. For CTF write-ups, the primary source is GitHub. Numerous repositories are dedicated to collecting and sharing solutions for past CTF challenges, often organized by event name or challenge category [11] [16]. The tracker's backend can leverage the GitHub API to monitor curated lists of these repositories for new commits or pull requests, triggering the ingestion process automatically [37]. This approach avoids the need for manual curation and ensures near real-time addition of new write-ups. Similarly, for conference materials, the YouTube Data API is an invaluable tool. Many conferences upload recordings of their sessions to official channels [81]. The tracker can be programmed to search for videos by combining keywords like the conference name (e.g., "Black Hat," "DEF CON"), the year, and speaker names. This allows for the automated discovery and cataloging of talks. Official conference proceedings, when available as PDFs, can also be sourced from their websites, though this may require more targeted scraping.

To make this aggregated content discoverable and useful, a rich and interconnected metadata model is essential. The data model should be designed to represent the relationships between different entities. A potential schema would include several key tables: `ArchiveResource`, `Event`, `Talk`, and `Speaker`. The `Event` table would store

basic information about a CTF or conference. The `Talk` table would link to an `Event` and contain details about a specific session, such as the title, abstract, and duration. The `Speaker` table would store information about the presenter. The `ArchiveResource` table would serve as a junction table, linking a `Talk` or `Event` to a physical resource like a slide deck (PDF), a video recording (link to YouTube), or a supplementary write-up link. This creates a powerful graph of information where a user can navigate from a conference page down to a specific talk, see the speaker's details, and click through to all associated resources. This structure mirrors how users naturally explore content and provides immense value beyond the event schedule itself [79].

Copyright and intellectual property are paramount considerations. The tracker must operate as a directory or index, not a host of copyrighted material. To comply with fair use principles and respect creators' rights, the platform should never store large files like PDF slides or MP4 videos on its own servers. Instead, it should store only the metadata (title, description, author) and the URL pointing to the original content hosted on GitHub, SpeakerDeck, or YouTube. Every piece of content displayed must prominently feature a link back to its source. Furthermore, the platform should have a clear and easily accessible policy for content removal requests. Any creator or organization who wishes to have their work removed should be able to do so with a single request, demonstrating the platform's commitment to ethical operation [48]. By acting as a responsible aggregator that provides attribution and facilitates access without redistribution, the archive component can become a trusted and indispensable part of the cybersecurity community.

Security, Threat Modeling, and SecOps Implementation

As a platform operating within the cybersecurity domain, the CTF & Conference Tracker must embody the highest standards of security. A proactive approach to security, known as security by design, is not an optional add-on but a core requirement. This involves creating a comprehensive threat model to identify potential attack vectors and implementing a robust SecOps (Security Operations) plan to mitigate those risks. The platform's reliance on automated data collection introduces unique vulnerabilities that must be addressed specifically.

The threat model for this system should consider risks across its entire lifecycle. A primary concern is the **abuse of the scraping infrastructure**. If an attacker gains control of the IP addresses used by the scrapers, they could be repurposed for malicious activities like DDoS attacks or credential stuffing, leading to the IPs being blacklisted and crippling

the platform's data-gathering capabilities. Mitigations include rotating user-agents and, for more aggressive targets, using a pool of residential or datacenter proxies. Another significant threat is **injection attacks via scraped content**. Untrusted data from websites, such as a CTF challenge description containing malicious JavaScript, could be reflected on the tracker's pages if not properly sanitized. This could lead to Cross-Site Scripting (XSS) and compromise the accounts of other users. The defense here is rigorous output encoding and sanitization for all user-facing content rendered in the browser. **Supply chain risk** is another critical vector. The third-party libraries and dependencies used in the tech stack (e.g., FastAPI, Celery, Requests) may contain undiscovered vulnerabilities. Regular scanning with tools like Dependabot and adherence to secure coding practices are essential defenses. The accidental **exposure of API keys** is a common and severe vulnerability. Keys for services like Google Maps, SendGrid, or the YouTube API, if committed to version control, can be discovered by attackers and used to deplete funds or gain unauthorized access [48]. Strict secrets management practices, such as using environment variables and dedicated secrets management services like HashiCorp Vault or AWS Secrets Manager, are mandatory. Finally, the platform is susceptible to **Account Takeover (ATO)** through weak passwords, phishing, or vulnerabilities in the authentication flow. Implementing strong password policies, supporting two-factor authentication (2FA), and monitoring login logs for suspicious activity are necessary controls to protect user accounts [114].

Based on this threat model, a comprehensive SecOps checklist should be developed and implemented. This checklist forms the basis of the platform's operational security posture.

Control Area	SecOps Checklist Item	Rationale
Secrets Management	Store all secrets (API keys, DB credentials) in environment variables or a dedicated secrets manager. Never commit them to code repositories.	Prevents accidental exposure of sensitive credentials, a common cause of breaches [48].
Web Application Firewall (WAF)	Deploy a WAF in front of the application to filter and monitor HTTP traffic, blocking common attacks like SQL Injection and XSS.	Acts as a first line of defense against prevalent web-based exploits [51].
Rate Limiting	Enforce strict rate limits on all public-facing endpoints (API and web interface) to prevent brute-force attacks and DoS.	Limits the damage from automated attacks and protects system availability [72].
Logging and Monitoring	Implement centralized logging and monitor logs for anomalies like failed login attempts, unusual request patterns, or errors from the ETL pipeline.	Enables rapid detection and response to security incidents and operational failures [114].
Input Validation & Sanitization	Validate and sanitize all input from users and scraped sources. Escape all output rendered in the browser to prevent XSS.	Mitigates injection attacks and protects user data and session integrity [60].
Dependency Scanning	Regularly scan all third-party dependencies for known vulnerabilities using automated tools.	Reduces supply chain risk by identifying and patching vulnerable libraries [49].
Authentication Security	Enforce strong password policies and offer optional two-factor authentication (2FA) for user accounts.	Significantly raises the barrier to Account Takeover (ATO) [114].
Regular Audits & Penetration Testing	Conduct periodic security audits and simulated penetration tests to proactively identify and remediate vulnerabilities.	Provides an objective assessment of the platform's security posture and uncovers hidden flaws [74].
Abuse Prevention	Monitor the scraping infrastructure for signs of abuse (e.g., IPs being flagged by target sites). Implement proxy rotation or IP rotation.	Ensures the long-term viability of the data ingestion pipeline by avoiding blacklisting [75].

By systematically addressing each item on this checklist, the development team can build a platform that is not only functional and user-friendly but also secure by design. This commitment to security will foster trust among the security-conscious user base and position the tracker as a reliable tool in the ecosystem.

MVP Roadmap and Synthesis

This research report has outlined the comprehensive design for a Minimum Viable Product (MVP) of a 'CTF & Conference Tracker'. The synthesis of the findings indicates that a focused, agile development approach is feasible within a 2-4 week timeframe, delivering significant value to the target user persona of individual players and small CTF teams. The success of this MVP hinges on a disciplined execution of the proposed architecture, data strategy, and user-centric features, all grounded in a robust security posture.

The core recommendation is to proceed with a read-only iCal (.ics) subscription model for calendar integration. This decision dramatically simplifies the MVP by avoiding the complex OAuth flows and conflict resolution logic inherent in bidirectional synchronization, thereby accelerating development and reducing technical debt [20] [21]. The platform's value is centered on its ability to act as a single source of truth for event data, curating it from multiple sources and presenting it in a personalized format that users can seamlessly integrate into their existing workflows. The personalization engine, driven by a well-defined user preference schema, is the key differentiator that transforms a simple aggregator into an indispensable utility.

The proposed technology stack—a combination of Python/FastAPI for the backend, Celery/Redis for the asynchronous ETL pipeline, PostgreSQL for flexible data storage, and Next.js for the frontend—provides a pragmatic yet powerful foundation [80]. This stack is well-suited for a student-led project, leveraging technologies with extensive documentation and community support, while also possessing the scalability to grow the platform beyond the MVP phase. The phased, week-by-week roadmap provides a clear and achievable path to launch, breaking down the complex task into manageable sprints focused on core functionalities.

The final synthesized recommendation is to embrace an iterative development cycle. The initial release of the MVP should focus exclusively on the core tracking and personalization features. Future iterations can then expand the platform's capabilities based on user feedback and engagement metrics. Potential enhancements include adding more data sources, introducing academic analytics for trend analysis, enabling community-driven submissions for write-ups and resources, and eventually exploring direct Google Calendar API integration or CalDAV support for power users. By launching a solid, secure, and highly useful MVP, the project can establish a loyal user base and create a sustainable platform for the global cybersecurity community.

Week-by-Week MVP Roadmap

Week	Focus Area	Key Milestones and Deliverables
Week 1	**Core Backend & Database Setup**	- Initialize FastAPI project and set up project structure. - Define and implement the core database models (`User`, `Preference`, `Event`, `Resource`) in PostgreSQL using SQLAlchemy ORM. - Develop and test basic CRUD API endpoints for managing user preferences.
Week 2	**ETL Pipeline Development**	- Build Collector modules for the primary data sources (CTFtime API and at least one major conference website). - Implement Normalizer and Validator logic to process raw data into the standardized internal schema. - Integrate Celery and Redis to orchestrate the ETL tasks and populate the database.
Week 3	**Frontend & Personalization Engine**	- Develop the frontend UI using Next.js for the preference filter settings. - Connect the frontend to the backend API to allow users to save their preferences. - Implement the core logic to query the database and generate a unique, signed URL for the personalized iCal feed.
Week 4	**Notifications, Polish, and Deployment**	- Integrate a push notification service (e.g., FCM) and an email service (e.g., SendGrid). - Implement the notification triggers and the anti-spam rules, including frequency caps and a basic priority scoring mechanism. - Conduct end-to-end testing of the entire system. - Deploy the MVP to a cloud hosting provider (e.g., Heroku, Vercel, AWS).

Reference

1. Varsalone Jesse, Haller Christopher - The Hack Is Back https://www.scribd.com/document/969971619/Varsalone-Jesse-Haller-Christopher-The-Hack-is-Back-2025
2. The top 9 US cybersecurity conferences to participate in 2026 https://www.cloudfest.com/blog/the-9-best-cybersecurity-conferences-to-attend-in-2026
3. The Best Security Conferences & Events 2026 https://www.splunk.com/en_us/blog/learn/cybersecurity-infosec-conferences-events.html
4. Cybersecurity Revolution: Conferences Leading the Way https://infosecwriteups.com/cybersecurity-revolution-conferences-leading-the-way-399659f5ae16
5. Side events list - SEORS - UNFCCC https://seors.unfccc.int/reports/events_list.html
6. Postal Terms - About USPS home https://about.usps.com/publications/pub32/pub32_terms.htm
7. CTF EVENTS - ENISA https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20CTF%20Events.pdf
8. Capture the Flag Challenge Success Strategy Guide - Trailhead https://trailhead.salesforce.com/content/learn/modules/capture-the-flag-activities/create-a-ctf-success-strategy

9. Zephyr tracing with CTF format and TraceCompass https://stackoverflow.com/questions/78510623/zephyr-tracing-with-ctf-format-and-tracecompass-parsing-errors
10. Part 1: CTF 2022 Write Up – Marsha's PC https://cellebrite.com/en/part-1-ctf-2022-write-up-marshas-pc/
11. H1-702 CTF Writeups https://aadityapurani.com/2018/06/25/h1-702-ctf-writeups/
12. A Meta-Benchmark for Evaluating Cybersecurity AI Agents https://arxiv.org/html/2510.24317v1
13. (PDF) Towards Improving IDS Using CTF Events https://www.researchgate.net/publication/388231993_Towards_Improving_IDS_Using_CTF_Events
14. Policy measures to promote reuse and high-quality recycling ... https://publications.jrc.ec.europa.eu/repository/bitstream/JRC143206/JRC143206_01.pdf
15. Understanding Your ChemStation https://www.agilent.com/cs/library/usermanuals/public/G2070-91126_Understanding.pdf?srsltid=AfmBOooJxW3HiFlDP9tShsNW4zxRJKzA8w7YlMRd1qwy4cEz_-rjcCQ8
16. 平台和工具 - 架构师研究会 https://architect.pub/book/export/html/36
17. The Art of PHP – My CTF Journey and Untold Stories! https://www.ctfiot.com/257942.html
18. Iris: A Next Generation Digital Pathology Rendering Engine https://pmc.ncbi.nlm.nih.gov/articles/PMC11742306/
19. small modular reactors - Aris (iaea.org) https://aris.iaea.org/Publications/SMR_catalogue_2024.pdf
20. Can I stop iCal from caching my PHP-generated iCalendar ... https://stackoverflow.com/questions/9088126/can-i-stop-ical-from-caching-my-php-generated-icalendar-feed
21. What are the benefits and drawbacks of using ETag vs ... https://serverfault.com/questions/795129/what-are-the-benefits-and-drawbacks-of-using-etag-vs-lastmodified-as-a-cdn-cache
22. OpenF1 MCP 服务器 https://lobehub.com/zh/mcp/openf1-openf1-mcp-server
23. Rate limits https://docs.stripe.com/rate-limits
24. Rate limits for the REST API https://docs.github.com/enterprise-cloud@latest/rest/using-the-rest-api/rate-limits-for-the-rest-api
25. InfoSec Write-ups https://infosecwriteups.com/
26. Understanding Scroll To Text Fragment (STTF) Leak https://stackoverflow.com/questions/77132024/understanding-scroll-to-text-fragment-sttf-leak
27. CTF Field Guide | PDF | File Format https://www.scribd.com/document/890763400/CTF-Field-Guide

28. Software security in practice: knowledge and motivation https://academic.oup.com/cybersecurity/article/11/1/tyaf005/8071721
29. Cybersecurity Starter Kit: Essential Skills for Ethical Hacking https://www.linkedin.com/posts/a-ella-evivie_cybersecurity-ethicalhacking-techlearning-activity-7373093638391619584-LiiS
30. Availability, Reliability and Security - Springer Link https://link.springer.com/content/pdf/10.1007/978-3-032-00630-1.pdf
31. Cyber Security Management in Education Technologies https://www.scribd.com/document/975336365/Cyber-Security-Management-in-Education-Technologies
32. Sievers* M9/M9e - TOC Analyzers https://www.insatech.com/media/qyfbyaum/im_e_sievers-m9-manual_dlm_77020-02.pdf
33. BMW Group Report 2024 https://www.bmwgroup.com/en/report/2024/downloads/BMW-Group-Report-2024-en.pdf
34. P179952-c4bcdd8f-bda5-474b-88be-c92a8980ff3a.txt https://documents1.worldbank.org/curated/en/099110124145585959/txt/P179952-c4bcdd8f-bda5-474b-88be-c92a8980ff3a.txt
35. Observations of Highly Successful, Distributed Teams in a ... https://dl.acm.org/doi/10.1145/3769994.3770022
36. A Survey of Moving Target Defenses for Network Security https://ieeexplore.ieee.org/ielaam/9739/9173582/9047923-aam.pdf
37. Kunpeng/kunpengcompute https://gitee.com/kunpengcompute/kunpengcompute/blob/master/content.json
38. Management of Digital EcoSystems https://link.springer.com/content/pdf/10.1007/978-3-031-93598-5.pdf
39. [Dr. Martha Honey PhD] Ecotourism and Sustainable (b-ok. ... https://www.academia.edu/37796180/_Dr_Martha_Honey_PhD_Ecotourism_and_Sustainable_b_ok_cc_
40. Rate limits for the REST API - GitHub Enterprise Server ... https://docs.github.com/en/enterprise-server@3.17/rest/using-the-rest-api/rate-limits-for-the-rest-api
41. Rate limits - Cloudflare's API https://developers.cloudflare.com/fundamentals/api/reference/limits/
42. Pentesting, OSINT, Pentest tools, Network Security ... https://www.linkedin.com/pulse/pentesting-osint-pentest-tools-network-security-privilege-txus-p-c-
43. Advances in the Internet of Things: Challenges, Solutions ... https://www.researchgate.net/publication/392283047_Advances_in_the_Internet_of_Things_Challenges_Solutions_and_Emerging_Technologies_CRC_Press

44. Analysis of Autonomous Penetration Testing Through ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11723266/
45. Mechanism of DNA capture by the MukBEF SMC complex and ... https://pmc.ncbi.nlm.nih.gov/articles/PMC7617805/
46. A helminth enzyme subverts macrophage-mediated ... https://www.science.org/doi/10.1126/sciimmunol.adl1467
47. Skill: Wireshark https://www.oreilly.com/search/skills/wireshark/
48. Joas A Santos' Post https://www.linkedin.com/posts/joas-antonio-dos-santos_capipen-redteam-cybersecurity-activity-7289871613259386881-9daA
49. Asset Discovery in Critical Infrastructures: An LLM-Based ... https://www.mdpi.com/2079-9292/14/16/3267
50. HoneyLite: A Lightweight Honeypot Security Solution for ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12390182/
51. Industrial Security 3.1 https://www.cisco.com/c/dam/en/us/td/docs/Technology/Industrial-Security-3-1-DG.pdf
52. State Fiscal Year 2025 Funding Guidelines Water Quality ... https://apps.ecology.wa.gov/publications/UIPages/documents/2310020.pdf
53. Customs Matters: Strengthening Customs Administration in a ... https://www.elibrary.imf.org/downloadpdf/display/book/9798400200120/9798400200120.pdf
54. Measuring and Augmenting Large Language Models for ... https://arxiv.org/pdf/2506.17644
55. A survey on large language model (LLM) security and privacy https://www.sciencedirect.com/science/article/pii/S266729522400014X
56. Suboptimal codon pairs trigger ribosome collisions and ... https://academic.oup.com/nar/article/53/22/gkaf1311/8402084
57. P-GW Administration Guide, StarOS Release 21.28 https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-28/pgw-admin/21-28-pgw-admin/m_gy.html
58. (PDF) Participative Web: User-created Content https://www.researchgate.net/publication/359204188_Participative_Web_User-created_Content
59. Cybersecurity Threats and Their Mitigation Approaches ... https://www.mdpi.com/2624-800X/2/3/27
60. Intelligent Techniques for Detecting Network Attacks https://pmc.ncbi.nlm.nih.gov/articles/PMC8587628/
61. FortiDeceptor 6.2.0 Administration Guide https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/2a1e05c4-9a5f-11f0-855d-6af4c3636dc7/FortiDeceptor-6.2.0-Administration_Guide.pdf

62. ENISA Threat Landscape Report 2018 https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.1.2.1%20-%20ENISA%20Threat%20Landscape%202018.pdf
63. CryoSift: an accessible and automated CNN-driven tool for ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12810319/
64. GitHub Repositories Ranking https://wangchujiang.com/github-rank/repos.html
65. Evaluating Frontier Models for Dangerous Capabilities https://arxiv.org/pdf/2403.13793
66. P-GW Administration Guide, StarOS Release 21.28 https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-28/pgw-admin/21-28-pgw-admin/m_pgwoview.html
67. Innovations in Cybersecurity and Data Science https://link.springer.com/content/pdf/10.1007/978-981-97-5791-6.pdf
68. Space Law in A Networked World - P.J. Blount, Mahulena ... https://www.scribd.com/document/894129639/Space-Law-in-a-Networked-World-P-J-Blount-Mahulena-Hofmann-Brill-Nijhoff-2023
69. Hybrid Intelligent Systems https://link.springer.com/content/pdf/10.1007/978-3-031-78928-1.pdf
70. Cyber-Zero: Training Cybersecurity Agents without Runtime https://openreview.net/pdf?id=D9kdB63vUJ
71. CTFUSION: A CTF-BASED BENCHMARK FOR LLM ... https://openreview.net/pdf/59353647d2dedfed20b8b6c2cca9f14ddff31e9e.pdf
72. Profile for MySQL Inc https://www.linknovate.com/affiliation/mysql-inc-6151778/all/?query=ports%20digital%20platform
73. NACE Rev. 2 - SFC Support Portal https://sfc.ec.europa.eu/system/files/documents/sfc2007/2022-10/nace-rev-2.pdf
74. ENISA THREAT LANDSCAPE 2023 https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
75. characterization, exploitation and forensic analysis https://theses.hal.science/tel-04155509v1/file/CNAM_LOPES-ESTEVES_2023.pdf
76. Daily Cyber News – October 7th, 2025 https://www.linkedin.com/pulse/daily-cyber-news-october-7th-2025-dr-jason-edwards-dm-cissp-crisc-pmvfc
77. Rate limits for the REST API https://docs.github.com/en/rest/using-the-rest-api/rate-limits-for-the-rest-api
78. Roadmap on data-centric materials science - IOPscience https://iopscience.iop.org/article/10.1088/1361-651X/ad4d0d
79. Cyber-Zero: TRAINING CYBERSECURITY AGENTS https://openreview.net/pdf/aa0861ae8b93c4a920e33877ae1fa85227323769.pdf

80. Kalyan Cheerla - AI Engineer | Multimodal AI (Text, Voice ... https://www.linkedin.com/in/kalyancheerla
81. Cyb3rpanda - Hitch-Hacker's Guide To The Network (2023 ... https://www.scribd.com/document/806685750/Cyb3rpanda-Hitch-Hacker-s-Guide-to-the-Network-2023-Cyb3rpanda-Libgen-li
82. (PDF) Generative AI for cyber threat intelligence https://www.researchgate.net/publication/394790050_Generative_AI_for_cyber_threat_intelligence_applications_challenges_and_analysis_of_real-world_case_studies
83. A Survey on Encrypted Network Traffic Analysis ... https://dl.acm.org/doi/10.1145/3457904
84. Tracking on the Web, Mobile and the Internet-of-Things https://arxiv.org/pdf/2201.10831
85. What to expect from BSides, Black Hat, and DEF CON https://www.theregister.com/2025/08/05/bsides_blackhat_defcon_preview/
86. Black Hat 2025 & DEF CON 33: The Attendees' Guide https://www.splunk.com/en_us/blog/learn/blackhat-defcon-conference.html
87. Kaleidoscope Academic Conference Proceedings 2024 https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/PublishingImages/Pages/default/KALEIDOSCOPE%202024%20CONFERENCE%20PROCEEDINGS.pdf
88. Advanced Information Networking and Applications https://link.springer.com/content/pdf/10.1007/978-3-031-87784-1.pdf
89. IEEE Project Domains 2020 - 2021: We Can Help You To ... https://www.scribd.com/document/542296016/Ece-Project-Topics
90. REST API endpoints for repository security advisories https://docs.github.com/en/rest/security-advisories/repository-advisories
91. DPSCoach – 面向《王者与自由》的AI 驱动战斗日志分析器 https://lobehub.com/zh/mcp/stalcup-dev-tl-dps-mcp
92. Cyber-Zero: Training Cybersecurity Agents without Runtime https://www.arxiv.org/pdf/2508.00910v1
93. (PDF) Cybench: A Framework for Evaluating Cybersecurity ... https://www.researchgate.net/publication/383236134_Cybench_A_Framework_for_Evaluating_Cybersecurity_Capabilities_and_Risk_of_Language_Models
94. RENEWABLE ENERGY SOURCES CLIMATE CHANGE ... https://www.ipcc.ch/site/assets/uploads/2018/03/SRREN_FD_SPM_final-1.pdf

95. UNITED NATIONS 18 April 2024 ECONOMIC ... https://unece.org/sites/default/files/2024-04/2024_EC3_Guidance%20on%20the%20role%20of%20NSOs%20in%20achieving%20climate%20objectives.pdf
96. Operator Handbook Red Team Osint Blue Team Reference ... https://www.scribd.com/document/595501399/Operator-Handbook-Red-Team-Osint-Blue-Team-Reference-v10nbsped-9798605493952
97. Pentesting Checklist | PDF | Transport Layer Security https://www.scribd.com/document/895096579/Pentesting-Checklist
98. Learning Cloud with HTB Business CTF 2025 https://infosecwriteups.com/learning-cloud-with-htb-business-ctf-2025-a-complete-cloud-writeup-part-1-6188fa67219c
99. Dynamic Risk Assessments for Offensive Cybersecurity ... https://arxiv.org/pdf/2505.18384
100. Springer Software Engineering For Games | PDF | System https://www.scribd.com/document/724402721/Springer-Software-Engineering-for-Games
101. Rate limits and query limits for the GraphQL API https://docs.github.com/en/graphql/overview/rate-limits-and-query-limits-for-the-graphql-api
102. REST API endpoints for rate limits https://docs.github.com/en/rest/rate-limit/rate-limit
103. Planet Thunderbird https://planet.mozilla.org/thunderbird/
104. On Using Machine Learning for Network Intrusion Detection https://www.researchgate.net/publication/220713766_Outside_the_Closed_World_On_Using_Machine_Learning_for_Network_Intrusion_Detection
105. 2024 email spam compliance rules https://www.linkedin.com/top-content/technology/tech-compliance-standards-for-businesses/2024-email-spam-compliance-rules/
106. Internet Institute Repository | PDF | Cyberspace https://www.scribd.com/document/432994735/Internet-Institute-Repository
107. Privacy engineering in social networks https://core.ac.uk/download/pdf/20331417.pdf
108. Firebase vs OneSignal: which should you choose in 2026? https://ably.com/compare/firebase-vs-onesignal
109. Firebase Cloud Messaging VS OneSignal https://stackoverflow.com/beta/discussions/77193222/firebase-cloud-messaging-vs-onesignal
110. Firebase vs OneSignal: Which Push Notification Service is ... https://www.linkedin.com/posts/fahadislam2_mobiledevelopment-pushnotifications-techcomparison-activity-7335288441334591488-w-AS

111. Authenticate Outbound Email to Improve Deliverability https://techcommunity.microsoft.com/blog/exchange/authenticate-outbound-email-to-improve-deliverability/3947623

112. Cold Email Deliverability Guide | PDF | Spamming | Internet https://www.scribd.com/document/911015782/Cold-Email-Deliverability-Guide

113. IoT-Enabled Tokenization of Physical Assets https://www.sec.gov/files/ctf-written-input-daniel-bruno-corvelo-costa-092125.pdf

114. Security log events https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/security-log-events

115. What Is A Good Email Deliverability Rate In 2026? https://powerdmarc.com/email-deliverability-rate/

116. Mastering Email Deliverability: The Ultimate 2026 Guide https://www.mailmunch.com/blog/mastering-email-deliverability

117. Firebase Cloud Messaging vs OneSignal https://ably.com/compare/fcm-vs-onesignal

118. Email Deliverability 2024: Fix your DKIM, SPF and DMARC https://www.udemy.com/course/email-deliverability/?srsltid=AfmBOoqOHdJXnk0DMbgDUkoikLQ89uyUWGGp1_UIdy9E4RgOhZe5ehef

119. Email Deliverability 2024: Fix your DKIM, SPF and DMARC https://www.udemy.com/course/email-deliverability/?srsltid=AfmBOopE2JS3RGhqIoiNCRPzIh0ZVVnIxxdcwV0pIWZqbLYWGrUwAEAN

120. Free For Dev | PDF | Cloud Computing | World Wide Web https://www.scribd.com/document/605119537/free-for-dev