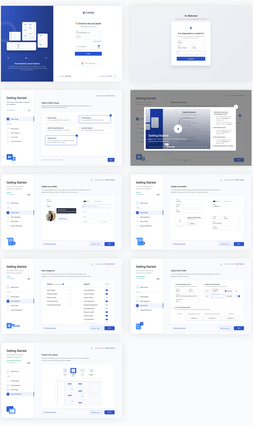
Cyware- CTIX 3.0 - Advanced Threat Intelligence Platform (B2B)

Agam Agarwal

User Onboarding

User onboarding is a critical phase in ensuring the successful adoption of our cybersecurity application. It is essential to provide a seamless and secure experience for new users. To achieve this, our onboarding process focuses on the following key aspects:

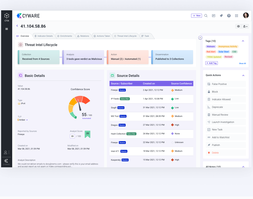
- **Registration:** Users can create an account with their email address or sign in using their existing credentials from popular identity providers like Google or Microsoft, ensuring ease of access.
- **Multi-Factor Authentication (MFA):** We encourage users to enable MFA during registration to enhance the security of their accounts and protect sensitive information.
- **Guided Setup:** A step-by-step setup guide helps users configure essential security settings and customize the application to their specific needs.
- **Educational Resources:** We provide educational content during onboarding to inform users about cybersecurity best practices and the importance of threat intelligence.



Threat Data- Details Page

Our Threat Data Details page is the heart of our application, providing users with in-depth information about potential security threats. Key features of this page include:

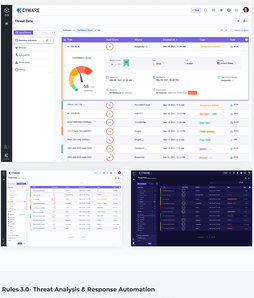
- **Comprehensive Threat Data:** Users can access detailed information about specific threats, including their origins, impact, and recommended actions for mitigation.
- **Interactive Visualizations:** Threat data is presented using interactive charts and graphs, making it easier for users to understand the threat landscape at a glance.
- **Historical Data:** Users can view historical data on threats, helping them identify patterns and trends in cybersecurity.
- **Actionable Intelligence:** We provide actionable recommendations on how to respond to threats, ensuring that users can take immediate steps to protect their systems.



Threat Data- Listing Page

The Threat Data Listing Page provides an overview of all detected threats, allowing users to quickly assess the current security landscape. Key features of this page include:

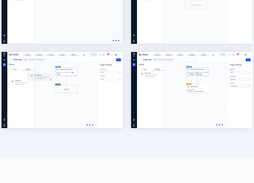
- **Filtering and Sorting:** Users can filter threats based on various criteria, such as severity, type, or date, and sort them for easy prioritization.
- **Alerts and Notifications:** Real-time alerts and notifications ensure that users are immediately informed of new threats or changes in threat status.
- **Integration with Third-Party Tools:** Our application seamlessly integrates with popular security tools, allowing users to take direct actions or investigations from this page.
- **Search Functionality:** A robust search feature enables users to find specific threats quickly, enhancing efficiency during incident response.



Rules 3.0- Threat Analysis & Response Automation

"Rules 3.0" module is a powerful tool for automated threat analysis and response. Key features include:

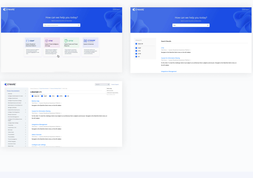
- **Customizable Rules:** Users can define conditions triggering automated responses.
- **Real-Time Monitoring:** Continuous threat monitoring with immediate action on rule matches.
- **Integration:** Seamless integration with other security tools for a unified defense.
- **Analytics:** Performance insights for rule optimization.
- **Incident Tracking:** Comprehensive incident logs and reporting.



Online Help Documentation

Our Online Help Documentation serves as a vitale resource for users seeking guidance on using our cybersecurity application effectively. Key aspects of our documentation include:

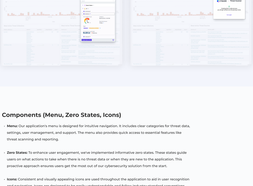
- **Comprehensive Guides:** We provide detailed guides and tutorials covering various aspects of the application, from setup to advanced threat analysis.
- **Frequently Asked Questions (FAQs):** Users can find answers to common queries in our FAQ section, saving them time and reducing the need for support requests.
- **Video Tutorials:** Visual learners can benefit from a library of video tutorials that walk them through key features and workflows.
- **Regular Updates:** Our documentation is continuously updated to reflect changes in the application, ensuring users always have access to accurate information.



Browser Extension

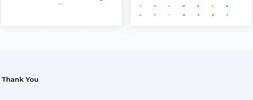
Our Browser Extension enhances the user's online security by seamlessly integrating with their web browser. Key features of this extension include:

- **Real-Time Threat Warnings:** The extension alerts users to potential threats while they browse, helping them avoid malicious websites or downloads.
- **Phishing Protection:** We offer phishing protection to prevent users from falling victim to phishing attacks by verifying website authenticity.
- **One-Click Reporting:** Users can report suspicious websites or content directly through the extension, contributing to our threat intelligence database.



Components (Menu, Zero States, Icons)

- **Menu:** Our application's menu is designed for intuitive navigation. It includes clear categories for threat data, settings, user management, and support. The menu also provides quick access to essential features like threat scanning and reporting.
- **Zero States:** To enhance user engagement, we've implemented informative zero states. These states guide users on what actions to take when there is no threat data or when they are new to the application. This proactive approach ensures users get the most out of our cybersecurity solution from the start.
- **Icons:** Consistent and visually appealing icons are used throughout the application to aid in user recognition and navigation. Icons are designed to be easily understandable and follow industry-standard conventions.



Thank You