Cyfax Administrators Guide

CYFAX

BEACON TECHNOLOGY

cyfax.ai

Contents

01. Introduction

Cyfax is a next-generation cybersecurity platform designed to provide unparalleled external threat intelligence, proactive alerting, and continuous monitoring. With Cyfax, administrators gain access to a comprehensive security solution that replaces traditional penetration testing, offering a cost-effective and scalable approach to managing an organization's external surface vulnerabilities and cyber risks. The platform leverages cutting-edge technology, including advanced bot automation, deception tactics, and hyperautomated penetration testing, to ensure that businesses are always ahead of emerging threats.

1. Replaces Traditional Penetration Testing

• **Comprehensive Coverage:** Cyfax fundamentally changes the way organizations manage their security posture. Unlike traditional human-led penetration tests, which are costly and often limited in scope, Cyfax offers a far-reaching, automated solution that continuously scans and assesses the entirety of your external attack surface. This eliminates the need for periodic, expensive penetration tests, providing an always-on approach to threat detection and remediation.
• **Cost Reduction:** Human penetration testing can cost tens of thousands of dollars and typically focuses on a limited set of potential vulnerabilities. Cyfax, on the other hand, offers a broad-spectrum analysis across all potential entry points to your organization, including dark web mentions, exposed credentials, subdomain analysis, and much more. The result is a significant reduction in testing and remediation costs.

2. Real-Time Intelligence

• **Always Know What the Enemy Has on You:** With Cyfax, you gain access to real-time, actionable intelligence about your organization's external vulnerabilities. This includes information about stolen credentials, compromised data, and potential security gaps that could be exploited by attackers. Cyfax continually scans the dark web, hacker channels, and other hidden digital marketplaces to uncover data leaks and threats to your business, ensuring you are always prepared to defend your assets.
• **Proactive Alerting:** The platform's built-in alerting system not only detects threats but also takes proactive steps in helping you contain and prevent breaches. Alerts are designed to notify administrators immediately of any risk, whether it's a credential leak, exposed service, or vulnerability. Cyfax's alerts are timely and actionable, offering specific guidance on how to mitigate the identified risks.

3. Advanced Threat Detection

• **Deception Technology and Bot Automation:** One of the key advantages of Cyfax over other platforms is its use of advanced bot technology combined with deception tactics. This allows the system to penetrate threat actor channels, forums, and dark web marketplaces in a way that traditional monitoring systems cannot. By employing deceptive techniques, Cyfax lures bad actors into revealing more information about their tactics, helping you stay one step ahead of potential threats.
• **Neutralizing Threats Before They Escalate:** Through the use of deception and automation, Cyfax identifies threats at their earliest stages. This early detection is critical in preventing a cyberattack from reaching a critical point. Whether it's detecting stolen data being sold on the dark web or an exposed vulnerability in your system, Cyfax neutralizes threats before they escalate into major breaches.

4. Holistic Security Integration

• **Complementing Internal Defenses:** While Cyfax provides comprehensive external threat monitoring, it doesn't work in isolation. When integrated with internal security solutions like Beacon and Vortex, it offers a 360-degree view of an organization's cybersecurity posture. This holistic approach ensures that all aspects of your security—both internal and external—are monitored and aligned to provide optimal protection.
• **Enhanced Visibility:** This integration empowers your security team with unparalleled visibility into both external and internal threat vectors, helping to detect and mitigate potential risks from all sides.

5. Superior Coverage

• **Extensive Threat Landscape:** Unlike competitors who may focus on just a few aspects of external security—such as leaked credentials—Cyfax provides a much broader scope. In addition to monitoring dark web mentions and stolen credentials, Cyfax also covers exposed ports, domain impersonation attempts, email security configurations, and even VIP monitoring. This gives you a comprehensive understanding of the vulnerabilities facing your organization.
• **In-Depth Monitoring: C**yfax monitors thousands of online channels, forums, and dark sites, giving you a unique advantage in terms of threat intelligence. The platform's bot-driven approach enables it to continuously scan and detect emerging threats, providing your organization with real-time updates and detailed reports on potential risks.

6. Cutting-Edge Technology

• **Machine Learning and Bots:** The advanced tools behind Cyfax—such as machine learning and automated bots—allow it to operate at a scale and speed previously unimaginable. These technologies are key to Cyfax's ability to continuously scan and identify vulnerabilities across a vast array of online platforms, ensuring your security posture is always up to date.
• **Efficiency and Accuracy:** The automation and machine learning components allow Cyfax to perform its scans efficiently, minimizing human error and maximizing the accuracy of the findings. This level of precision ensures that the information provided is reliable and actionable, empowering security teams to make quick, informed decisions.

7. Ease of Use

• **User-Friendly Interface:** Despite its advanced technology, Cyfax is designed with ease of use in mind. Administrators can quickly access the information they need through a simple, intuitive interface. Whether reviewing a snapshot report or setting up alerts, the platform is straightforward to navigate, ensuring minimal effort is required to get the maximum benefit from its capabilities.
• **Comprehensive Coverage with Minimal Effort:** Cyfax delivers full-spectrum coverage without the need for complex configurations or extensive manual intervention. Administrators can set up and run scans with just a few clicks, ensuring that external security is handled without requiring constant oversight.

8. Additional Security Areas

• **Perimeter Vulnerabilities:** Cyfax excels in identifying perimeter vulnerabilities, such as exposed ports and services, which are often the first point of entry for attackers. It continuously monitors your external infrastructure to uncover these weaknesses, allowing you to fix them before they are exploited.
• **Automated VIP Monitoring: I**n addition to its perimeter scanning capabilities, Cyfax offers automated VIP monitoring, ensuring that high-value targets within your organization are closely watched for any signs of attack. This feature significantly sets Cyfax apart from other platforms, providing an added layer of protection for critical assets and personnel.

9. The Most Effective Dark Web Monitoring System

• **Unmatched Penetration into Dark Web Channels:** Cyfax's dark web monitoring capabilities are

unparalleled. By using advanced bot technology and deception tactics, Cyfax gains a deeper level of penetration into dark web channels, hacker forums, and online marketplaces than traditional systems. This allows Cyfax to detect stolen data, compromised credentials, and potential threats targeting your organization much earlier than other systems.

• **Early Surveillance and Alerting:** Cyfax provides early surveillance alerts, allowing your organization to take immediate action when a bad actor is targeting you or transacting stolen digital assets related to your organization. This proactive approach ensures that threats are addressed before they can escalate.

10. 360-Degree View of External Cybersecurity

• **Continuous, Hyperautomated Penetration Testing:** By combining automated penetration testing with continuous monitoring and real-time intelligence, Cyfax provides a complete, 360-degree view of your external cybersecurity posture. This integration of various technologies, such as machine learning, bot automation, and deception tactics, makes Cyfax an indispensable tool in modern cybersecurity defense.

• **Comprehensive Security Posture:** With Cyfax, you have access to a dynamic and comprehensive security posture that spans across the entire external threat landscape. From stolen credentials to domain variations and exposed services, Cyfax ensures that no potential vulnerability goes unnoticed.

02. Getting Started

Cyfax is designed to simplify the setup and onboarding process, allowing you to start monitoring your external cybersecurity posture with minimal effort. As a Platform-as-a-Service (PaaS), Cyfax does not require software installations and provides automated continuous monitoring once your account is set up. The system's self-service model is easy to follow, with most tasks automated, letting administrators focus on taking action against detected threats.

How to Create an Account

Creating a Cyfax account is a straightforward process. Whether you are an individual or part of an organization, follow these steps to get started:

1. Visit the Cyfax Website: Navigate to the registration page on the Cyfax website.

2. Choose Your Account Type:

- o Individual Account: For those managing their own external cybersecurity posture.
- o Organization Account: For enterprises that need monitoring for multiple domains.

3. Select Add-ons: Depending on your security needs, select any relevant add-ons or premium features such as VIP monitoring or advanced integrations.

- o Essentials Tier: Purchase directly on the website for a basic, core functionality plan.
- o Advanced Tiers: Work with the Cyfax account team to provision higher-level accounts.

4. Register: Complete the registration process, and for non-"Essentials" tiers, Cyfax or a partner will handle the provisioning for you.

Initial Setup

Once your account is created and you've logged in, you will be presented with a seamless dashboard. Here's what you can expect:

1. Preloaded Authorized Domains: Upon first login, any domain authorized to you (whether you're an admin or a partner) will already be loaded into your account. You will automatically be directed to the main dashboard for the primary domain you have access to.

2. Re-scan Organization:

- o Action Step: To start your Cyfax journey, the first action is to click the “Re-scan Organization” button on the landing page. This process initiates a full, hyperautomated penetration test of your domain.
- o Re-scan Duration: The scanning process typically takes about 30 minutes to complete. During this time, Cyfax will conduct a thorough security assessment of your authorized domain, checking for vulnerabilities and potential exposures.
- o Report Delivery: Once the scan is complete, the domain’s vulnerability data will be updated. You will also receive a snapshot report sent to your email.

3. Why Re-scan? While Cyfax may already have Indicators of Compromise (IOCs) identified for the domain, executing a rescan ensures that the Cyfax report you begin with reflects the most up-to-date exposure findings. It also provides a baseline for your ongoing monitoring journey.

4. Automated Monitoring: Once a domain is assigned to a Client Admin, Cyfax will begin continuous monitoring of that domain. This includes regular scans and real-time alerts whenever new exposures or threats are detected, ensuring that you stay ahead of any changes to your domain’s security posture.

Logging in to the Admin Panel

After registering your account and completing the initial setup, logging into the Admin Panel is simple:

1. Login: Visit the Cyfax login page and enter your administrator credentials.
2. Automatic Domain Load: Upon login, the system will automatically load your authorized domain and direct you to the dashboard.
3. View Your Dashboard: From the dashboard, you can:

- o Review your security posture and findings.
- o Access the Alert Management section to configure notifications and monitoring.
- o Initiate a re-scan anytime you wish to refresh your domain’s security status.

Key Features of Cyfax Setup

The primary setup tasks within Cyfax are automated, and once your account is configured, the

system runs independently, continuously monitoring your domain for vulnerabilities. However, there are a few key areas to focus on:

• **Understanding Posture:** After executing the “Re-scan Organization” process, you will have a clear understanding of the current security posture for your domain. Cyfax will automatically identify any leaked credentials, exposed services, or other threats that might compromise the security of your organization.
• **Continuous Monitoring:** As soon as a domain is assigned to a Client Admin, Cyfax begins its continuous monitoring. This ensures that your domain’s exposure is regularly assessed and alerts are sent to your team as soon as any new issues arise. This ongoing monitoring is automated, so you don’t need to worry about manually initiating scans—Cyfax takes care of that for you.
Summary

Getting started with Cyfax is easy:

• **Create an Account:** Register for Cyfax and choose the appropriate tier and add-ons.
• **Automatic Domain Setup:** After logging in, your authorized domains are already loaded, and you’re immediately directed to the dashboard.
• **Run the First “Re-scan Organization”:** Start your journey with Cyfax by executing the “Re-scan Organization” to get the most current cybersecurity posture for your domain.
• **Continuous Monitoring:** Once set up, Cyfax will automatically monitor your domains and send you real-time alerts on any potential threats or exposures.

Leaked Credentials:

Definition: Leaked credentials are sensitive user data, such as usernames and passwords, that have been exposed to unauthorized individuals or groups, typically through data breaches or cyberattacks.

How Cyfax Detects Them: Cyfax continuously monitors a range of online sources including dark web marketplaces, encrypted channels like Telegram, and hacker forums. When company credentials are discovered on these platforms, Cyfax flags them and provides a report on the exact nature of the exposure.

Example: If an employee's company email and password (e.g., john.doe@company.com, P@ssw0rd123) are found on a dark web marketplace such as Telegram, Cyfax will identify this exposure and notify administrators about the specific credentials, the platform where they were found, and the potential threat of unauthorized access.

Company Exposed Ports/Services:

Explanation: Exposed ports and services refer to open communication channels on the company's network that are accessible from the outside world, often leaving systems vulnerable to cyberattacks.

How Cyfax Scans and Reports Exposed Ports and Services: Cyfax uses automated scanning to detect open ports on company servers and other network assets. It identifies the services running on those ports and determines whether those services are secure or vulnerable to exploitation.

Example: Cyfax might detect that port 443 (used for HTTPS traffic) is open on the company's web server and is running an outdated SSL/TLS service that is vulnerable to attacks like "Heartbleed." Cyfax will report this as an exposed service, allowing administrators to take action, such as upgrading to a more secure version.

Sub-Domain Analysis:

Explanation: Sub-domain analysis refers to the process of identifying and evaluating sub-domains associated with the primary domain, such as blog.company.com or portal.company.com.

How Cyfax Performs Sub-Domain Analysis: Cyfax checks for sub-domains that are often overlooked or insecurely configured. It detects all sub-domains associated with the main domain and assesses whether they are properly secured or exposed to potential vulnerabilities.
Example: If Cyfax finds a sub-domain like ftp.company.com that is publicly accessible but should have restricted access, it flags this exposure as a potential risk. Administrators are advised to secure it to prevent unauthorized access.

Domain Variations:

Explanation: Domain variations occur when attackers register domain names that closely resemble the legitimate domain (e.g., disneyy.com instead of disney.com) to deceive users into visiting fraudulent websites.
How Cyfax Identifies Domain Variations: Cyfax uses advanced algorithms to detect domain names that are slightly altered to impersonate the company's legitimate site. It identifies variations such as those created through techniques like adding extra letters or using different top-level domains (TLDs).
Example: Cyfax might discover a domain variation like disneyy.com which looks similar to disney.com. This could be part of a phishing campaign. Cyfax alerts administrators to the potential impersonation and suggests steps to mitigate it.

Email Protection:

Overview: Email protection refers to the security measures put in place to prevent phishing, spoofing, and other email-based attacks that could compromise company data.
How Cyfax Scans for Email Protection: Cyfax scans email infrastructure to identify potential weaknesses, such as misconfigured DKIM, DMARC, or missing BIMI records. It also monitors for signs of phishing attempts and malicious email attachments that could pose a risk.
Example: If the company's email system does not have proper DKIM (DomainKeys Identified Mail) or DMARC (Domain-based Message Authentication, Reporting, and Conformance) policies configured, Cyfax will flag this as a vulnerability, allowing administrators to improve email authentication and prevent spoofing attacks.

Stealer Logs for Sale:

Explanation: Stealer logs are data records that contain information stolen from compromised devices. These logs often include sensitive information such as credentials, cookies, and session tokens.

How Cyfax Detects and Reports Stealer Logs for Sale: Cyfax monitors underground marketplaces and hacker forums for logs being sold, which could indicate that an organization's data has been compromised.
Example: Cyfax may find logs on a site like Russian Market, showing stolen login details from disney.com. These logs are flagged, and the administrators are alerted about the sale of sensitive information, allowing them to investigate and secure affected systems.

Stealer Logs From Infected Machine:

Explanation: These logs are generated from compromised machines where attackers steal sensitive data. The data might include credentials or other information, which is later sold or used for malicious purposes.
How Cyfax Identifies and Alerts Administrators: Cyfax identifies infected machines by tracking the logs generated and correlating them with known attacker behavior.
Example: If an employee's personal computer is infected with malware, Cyfax might identify logs from myid.disney.com or infinity.disney.com. The system will notify administrators, alerting them to a potential internal breach.

Dark Web Mentions:

Explanation: Dark web mentions refer to instances where the company's name, data, or other sensitive assets are mentioned on dark web forums or marketplaces.
Role of Cyfax in Dark Web Monitoring: Cyfax continuously scans multiple dark web platforms to find mentions of the company, including stolen credentials, exposed data, or discussions of potential attacks.
Example: Cyfax might detect a dark web mention like: "stolen credit card info for disneyplus.disney.com on sale now." This alert would help administrators take proactive steps to protect against any arising risks.

Hacker Channel Mentions:

Explanation: Hacker channel mentions are discussions or advertisements in online hacker groups or forums about the company, its assets, or its vulnerabilities.
How Cyfax Tracks Hacker Channel Activity: Cyfax monitors hacker channels such as Telegram or forums dedicated to discussing cybercriminal activities. It flags mentions of the company or its vulnerabilities as high-priority threats.

Example: Cyfax detects a message in a hacker forum saying: “Disney gift cards for sale here.” This would trigger an alert, notifying the security team of the potential threat and allowing them to respond swiftly.

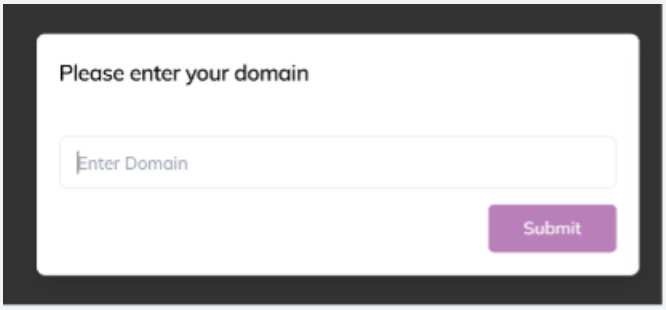
Sensitive Data:

Explanation: Sensitive data refers to any type of information that, if exposed, could harm the organization or its users. This includes API keys, access tokens, configuration files, and credentials.
How Cyfax Scans for Sensitive Data Exposure: Cyfax uses deep scanning techniques to detect sensitive data exposed in web pages, code repositories, or other publicly accessible areas. It identifies items like unmasked API keys or configuration files that contain confidential data.
Example: Cyfax might detect an exposed API key for Google services in a public GitHub repository. The system will alert administrators, allowing them to revoke the key and prevent unauthorized access.

04. Cyfax Dashboard Visualizations and Navigation Overview

The Cyfax Dashboard is the central hub for monitoring and managing your organization's external cybersecurity posture. Upon logging in, users will be greeted by this main dashboard. Depending on the user's role and the number of domains assigned, the dashboard view will vary:

• **For Partner or Client Admins with multiple domains:** Upon login, users will first see a domain selector pop-up as shown below, prompting them to choose the domain they want to manage. After selecting the domain, they will be directed to that specific domain's dashboard.



• **For users or Client Admins with a single domain assigned:** They will be automatically directed to their primary domain's dashboard.

The dashboard contains several key widgets, each designed to provide valuable insights into the security posture of your assigned domains. Here's what each graphic or widget on the dashboard represents:

1. Risk and Achievement Score

What It Means: The Risk and Achievement Score widget provides a visual representation of your organization's overall external cyber posture. The score is presented as a gradient color bar, with the score ranging from 0 to 100.

• **Risk Categories:**
  - o 0-40 (HIGH Risk): Critical exposure that requires immediate attention.
  - o 40-70 (MEDIUM Risk): Moderate risk level that requires proactive monitoring and action.
  - o 70-100 (LOW Risk): Clean or acceptable posture, with minimal to no vulnerabilities.

• **Markers:**

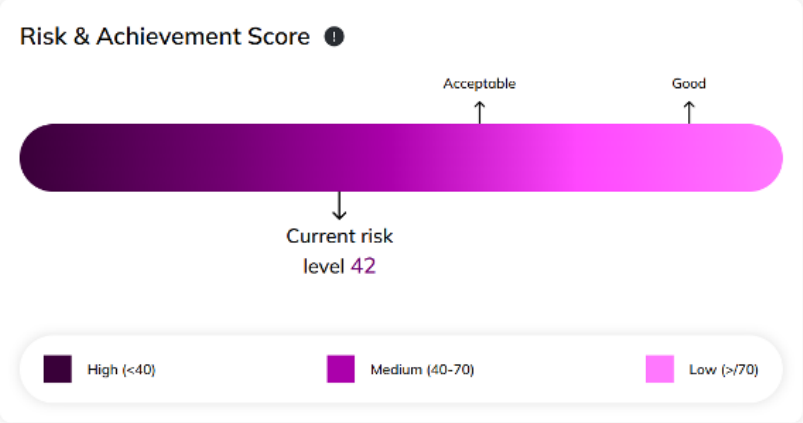
  o The acceptable score range is 70-90, which represents a balanced, manageable security posture.

  o A Good posture score of 90 or greater is considered optimal.

How It Works: This composite score is calculated from multiple risk vectors, including critical aspects such as Compromised Credentials and Exploitable Vulnerabilities. Other factors like subdomain risks, perimeter vulnerabilities, and more also contribute to the score.

Example:

If your organization has exposed credentials and several critical vulnerabilities on your web server, the score will likely be in the 40-70 (Medium Risk) range. You can check the vectors contributing to this score to better understand the areas needing immediate attention.



2. Security Findings

What It Means: This donut graph provides a breakdown of the different security threats facing your domain, represented by percentages. It displays the key security findings categorized into different threat vectors (e.g., compromised credentials, vulnerabilities, exposure).

How It Works:

• The center of the donut shows the total number of findings.

• The outer ring is segmented to show the percentage distribution of various security issues, such as Compromised Credentials, Exposed Services, Vulnerabilities, etc.

Example:

If the graph shows 40% of issues related to credentials, and 30% related to exploitable vulnerabilities, the chart helps prioritize remediation efforts in areas with the highest exposure.

3. Vulnerabilities vs Exploitable Services Over Time

What It Means: This line graph illustrates the trend of vulnerabilities in your organization's domain over time, with an additional line showing the exploitable services that are associated with those vulnerabilities.

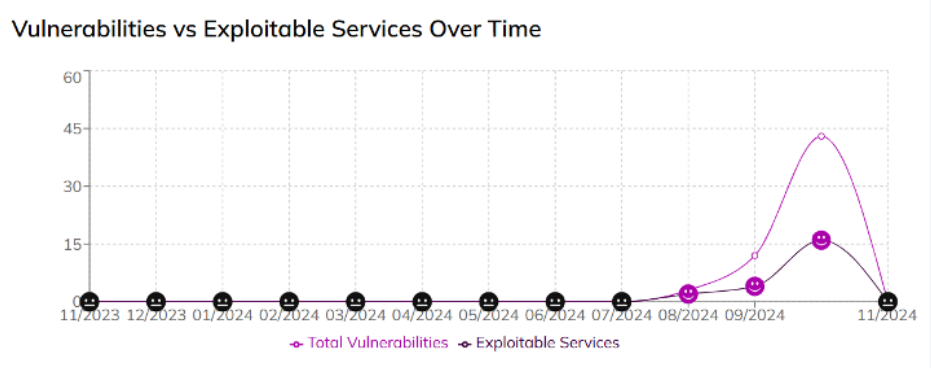
How It Works:

• One line shows the total number of vulnerabilities, while a second line tracks how many of those vulnerabilities are actively exploitable.

• The graph helps identify trends in increasing vulnerability and how many of those vulnerabilities are being targeted by attackers.

Example:

If your domain shows an upward trend in vulnerabilities but a stable or slightly decreasing line for exploitable vulnerabilities, you can prioritize patching or mitigating those that are vulnerable but not actively being exploited yet.



4. Leaked Passwords Over Time

What It Means: This graphic displays the leaked credentials over time and indicates their useful value in dark markets. The color gradient follows the same scheme as other dashboard widgets, ranging from dark plum (critical) to light pink (low risk).

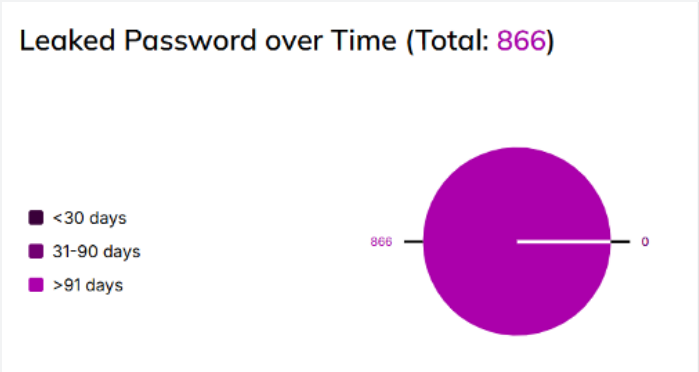
How It Works:

• This widget helps administrators track the shelf life of compromised credentials.

• Credentials are most dangerous within the first 30 days of exposure and become less valuable in the dark market as time passes.

Example:

If you see that a large number of compromised passwords were leaked last month, and they are still being actively traded, this will trigger a high-priority alert. The color of the bar will indicate the level of risk, such as dark plum for very critical exposures.



5. Attack Surface

What It Means: This widget provides a snapshot of your organization's external attack surface, focusing on key areas that might be vulnerable. These areas include computers, networks, and data that can be targeted by threat actors.

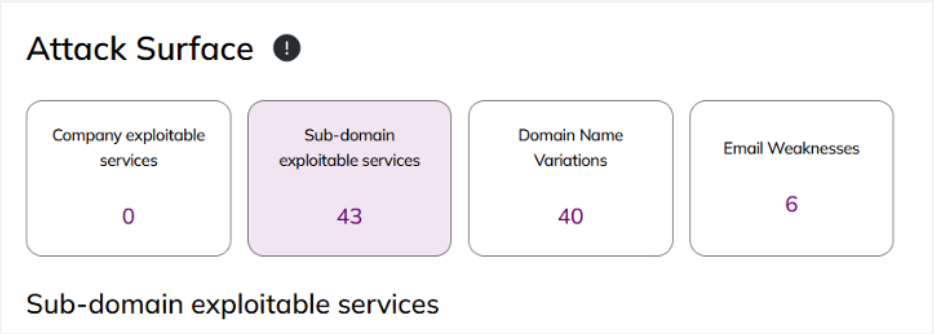
How It Works:

• The widget shows four key security areas, and when clicked, provides a summary of the most critical exposures for that vector.

• Clicking on any of these areas will provide additional details and insights into vulnerabilities or threats for that specific vector.

Example:

You might see that exposed ports are flagged in one of the four boxes. Clicking it reveals a list of ports open to external access, showing that port 8080 has an outdated service running. This would be flagged for immediate attention.



6. Rescan Organization Button

What It Means: The Rescan Organization button triggers a hyper-automated penetration test against the selected domain. This test checks for vulnerabilities and exposure in real-time.

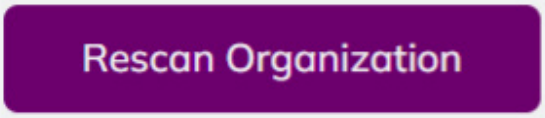
How It Works:

• Clicking the button will initiate a thorough security scan of the domain, which typically takes about 30 minutes to complete.

• Monthly hygiene: Though continuous monitoring is in place; it is recommended to run this test at least once a month to have trending analytics and updates on the organization's overall security posture.

• Frequency Limit: To prevent unnecessary strain on the system and to allow time for proper analysis, users can only perform the next scan at least 3 days after the last scan.

Example: You notice your domain's score is in the medium-risk range. Clicking Rescan Organization will allow Cyfax to perform a fresh scan, helping to confirm if there are any new vulnerabilities or exposures that need to be addressed.



7. Cyber Threat Assessment Download Options

What It Means: This area offers the option to download a cyber threat assessment report. Depending on the subscription plan, users can choose from a snapshot report for an executive summary or a detailed report that lists all vulnerabilities.

How It Works:

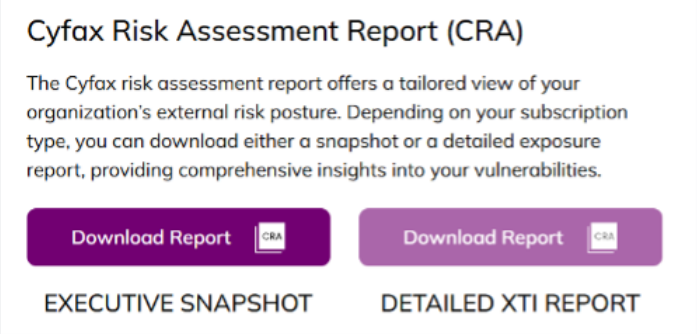
• Snapshot Report: Provides a high-level view of the external cybersecurity posture.

• Detailed Report: Lists all the vulnerabilities, findings, and recommendations for remediation, exported as a PDF file.

Example:

• A Snapshot Report is useful for executives who need a quick, easy-to-digest overview of the domain's risk.

• A Detailed Report is ideal for security practitioners who need a granular breakdown of every vulnerability and recommended remediation steps.



8. Navigation Bar Overview

What It Means: The Navigation Bar is where administrators can access all sections of the Cyfax platform. It provides quick links to each area for deeper analysis and management.

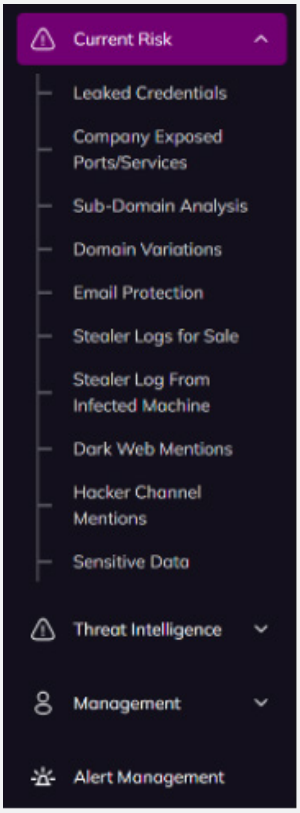
How It Works:

• Key sections include Current Risk, Threat Intelligence, Management, and Alert Management.

• Click on any section to access more detailed information related to that area.

Example:

You can click on Threat Intelligence to get a detailed look at dark web mentions, data leaks, and other external intelligence that might impact your organization.



05. Creating and Managing Organizations in Cyfax

The first step to setting up your account and managing external cyber posture in Cyfax is the creation of an Organization. This process establishes the foundation for all subsequent user, domain, and asset management in the system. Below is a step-by-step guide on how to create an organization in Cyfax, tailored for Partner Admins and Super Admins. Client Admins do not need to create organizations, as they are already assigned to a specific organization.

Step 1: Accessing the Organization Management Page

1. Login to Cyfax: Use your administrator credentials to log into the Cyfax portal.
2. Navigate to the Management Section: On the left sidebar, you will find a "Management" tab. Hover over or click on this tab to access the drop-down menu.
3. Select 'Org Management': From the drop-down menu, select 'Org Management'. This section allows you to manage organizational setups, including creating new organizations and linking them with the domains under your management.

Step 2: Creating a New Organization

1. Fill in Organization Details:

- o Organization Name: Enter the official name of the organization you are creating. This name will be used to identify the organization in the Cyfax portal.
  Example: Example Company
- o Authorized Administrator: Input the primary administrator's full name who will have management access to the organization. This user will be the main point of contact for the organization.
  Example: Joe Doe
- o Authorized Administrator Email: Enter the email address of the authorized administrator who will be responsible for managing the organization in Cyfax.
  Example: joe@example.com
- o Password: Create a strong password for the organization. This password will be used for secure login to the system. Make sure it follows your organization's password policy.
  Example: Zo2H#!

2. Confirm Password: Retype the password to ensure accuracy.
3. Authorized Organizational Domain: Enter the primary domain name associated with the organization. This is crucial because it will serve as the basis for scanning and monitoring.

- o Example: example.com

4. Permissions: Select the appropriate permissions for the organizational admin. Permissions define the scope of actions this administrator can perform within the organization.

- o Example: Select permissions such as:

Can view PDF reports with authorized group

Can view company exposure data with authorized group

Can perform manual scans with authorized group

5. Plan Name: Select the appropriate plan for the organization from the available options. The plans determine the level of access to various features in Cyfax, such as the number of domains to be monitored and the frequency of reports.

- o Available Plans:

Essential

Professional

Enterprise

6. Client or Partner: Indicate whether the organization is a Client or a Partner. This helps determine the level of functionality and access associated with this particular organization.

- o Example: Client

Step 3: Saving the Organization

Once all fields are filled out correctly, click the Save button to create the organization in Cyfax. Upon saving, the system will link this new organization to your administrator account, and you will be able to proceed to the next steps, including assigning users and configuring additional settings like domain monitoring and alert management.

Step 4: Verifying the Organization Creation

After creating the organization, you will be redirected to the organization's dashboard. If you are managing multiple domains or organizations, a Domain Selector will appear, allowing you to select the specific domain or organization to view. For those with only one domain, the dashboard will automatically display the associated domain's data.

Conclusion

Creating an organization in Cyfax is the first step in setting up your security posture monitoring. Once the organization is created, you can move forward with managing users, assigning roles, and configuring alert settings. This foundational process allows for efficient and seamless integration of the security management system and provides you with the necessary tools to manage and mitigate risks in real-time.

For further assistance or troubleshooting during this process, refer to the Cyfax Technical Support section, or contact support directly via the support channels provided in the portal.

06. Creating Users and Role Assignment

Once an organization has been created in Cyfax, the next step is to set up users within that organization. This is a critical step to ensure that the right individuals have the appropriate level of access to security data, alerts, and system management tools. This section outlines the process for creating and managing users, roles, and permissions within Cyfax, based on the organization structure you've set up.

Step 1: Accessing the User Management Page

1. Login to Cyfax: Use your administrator credentials to log into the Cyfax portal.
2. Navigate to the Management Section: On the left sidebar, you will find a "Management" tab. Hover over or click on this tab to access the drop-down menu.
3. Select 'User Management': From the drop-down menu, select 'User Management'. This section will allow you to view and manage all users assigned to your organization.

Step 2: Creating a New User

To create a new user, follow these steps:
1. Click 'Create User': At the top-right of the User Management page, click the 'Create User' button. This will open a user profile form where you can enter the necessary details.
2. Enter User Details:
- o Email: Enter the user's email address. This will be used for system notifications and login.
  Example: user@example.com
- o Full Name: Enter the full name of the user.
  Example: John Doe
- o Phone Number (Optional): Provide a phone number for the user if needed for communication.
  Example: +1234567890

3. Password:
- o Create a strong password for the user.
- o Ensure it follows your organization's password policy (e.g., minimum length, special characters).
  Example: CyfaxSecure!123

4. Confirm Password: Retype the password to ensure it matches.
5. Role Assignment:
- o Choose the Role for the user. The available roles are:

Partner User: A user with limited access, typically for those who need read-only access to client data.

Client User: A user who can view security data and alerts but has limited control over system settings.

Example: Client Admin for an administrator of a specific client domain.

Step 3: Assigning Permissions – Informational

Once the user's role has been selected, permissions define what actions the user can perform within their organization. These permissions should be tailored to the user's role and responsibilities.

Note: This is not an actionable step for users during the user creation process. It is informational and helps in understanding how to manage user roles and permissions. You will be assigning these permissions based on the user's role and responsibilities.

1. Permissions for Client Admins:

- o View and configure the organization's dashboard.
- o Set up alerts for vulnerabilities and threats.
- o Initiate domain rescans.
- o Monitor the security posture of their assigned domain.

2. Permissions for Partner Admins:

- o Create and manage users for client organizations.
- o View all client data under their management (but cannot make changes to client configurations unless explicitly authorized).
- o Assign or remove users from specific client groups.
- o Delete users within their partner organization or client groups.

3. Permissions for Client Users:

- o View security data and alerts.
- o Limited ability to interact with the system (read-only access).

Assign Permissions: Based on the role, you will assign appropriate permissions for each user. This ensures that each user has the necessary access to fulfill their role.

Step 4: Saving the User Profile

Once all details are filled in and permissions have been assigned, click the 'Save' button to create the user profile. The new user will receive an email with login instructions (if email notifications are enabled).

Step 5: Editing or Deleting Users

As an administrator, you can also edit or delete users as needed.

1. Editing a User:

- o In the User Management tab, locate the user in the list.
- o Click the Edit icon next to their profile.
- o Update any information, including their role or permissions.
- o Save the changes.

2. Deleting a User:

- o To delete a user, click the Delete icon next to their profile.
- o Confirm the deletion. Note that deleted users will no longer have access to the Cyfax system.

Step 6: Managing User Groups

For larger organizations or partners with multiple clients, user groups are a useful way to segment users based on their roles or access levels.

1. Creating User Groups:

- o A Partner Admin can create user groups for organizing users within their client organizations. This helps segment users who need similar permissions.
- o User groups can be assigned to specific domains or assets, ensuring that users have access only to the areas they are authorized to view.

2. Assigning Users to Groups:

- o After creating user groups, you can assign users to these groups to ensure they have access to the relevant data and functionalities within the system.

Conclusion

Managing users in Cyfax is an essential part of ensuring that your organization maintains a secure and efficient cybersecurity posture. By assigning appropriate roles, permissions, and user groups, you can ensure that the right individuals have the right access to the system's features and data. Proper user management helps in controlling who has the ability to view, modify, or manage critical security information.

For further assistance or troubleshooting related to user management, refer to the Cyfax Technical Support section, or contact Cyfax support directly via the support channels provided within the portal.

Partner Admin and Client Admin Permissions

Cyfax provides a range of user management permissions depending on the role assigned to the user. Partner Admin and Client Admin are key roles within the platform, with distinct permissions and responsibilities. Below, I'll break down what each role can and cannot do in terms of managing users.

1. Partner Admin Permissions

Partner Admin is an administrator within a Partner Org and is responsible for managing multiple client organizations (clients that the partner supports). Partner Admins are granted broader control over their Partner Org and the client organizations they are associated with.
What a Partner Admin Can Do:

- **Create Users:**
  - o Partner Users: A Partner Admin can create Partner Users within the Partner Org. Partner Users are members who have read-only access to the client data they are authorized to monitor. Partner Users can view but cannot edit or execute actions (like rescanning domains or setting up alerts).
  - o Client Admins: Partner Admins can create Client Admins for the client organizations they are authorized to manage. Client Admins have full permissions to manage their own organization's settings, including configuring alerts, managing domains, and setting up monitoring for their client's assets.
  - o Client Users: Partner Admins can also create Client Users for client organizations. Client Users are typically lower-level users who can view security data and alerts but do not have administrative privileges.
- **Manage User Groups:**
  - o A Partner Admin can create and manage user groups for each client organization they support. These user groups help segment users based on the type of access or functionality they require.
- **View Client Data:**
  - o Partner Admins have full visibility into the client data of all clients they manage. However, they cannot execute actions (like rescans or alert modifications) unless they have the relevant permissions or roles within a specific client organization.

- **User Deletion:**
  - o A Partner Admin can delete users from the groups within their Partner Org. The Partner Admin can either:
    Completely delete the user from the system, or
    Remove the user from the group without deleting their account entirely.
  - o If a Partner Admin wants to delete a user from a client domain, they can do so only if the user belongs to that client's group.

What a Partner Admin Cannot Do:

- **Cannot Manage Client Domains Directly:** Partner Admins cannot directly manage client domains. They can assign Client Admins to manage those domains.
- **Cannot Make Changes to Client Admin Settings:** While a Partner Admin can create Client Admins, they cannot make changes to settings that fall within the scope of the Client Admin's permissions.

2. Client Admin Permissions

A Client Admin is an administrator who has full control over the client's organization and domain(s) within the Cyfax platform. The Client Admin is responsible for managing the security posture of their domain, monitoring alerts, and configuring Cyfax settings specific to their organization.

What a Client Admin Can Do:

- **Manage Client Organization:**
  - o View and Configure the Organization's Dashboard: A Client Admin has full access to the organization's dashboard, where they can view current security data, vulnerabilities, and alerts. They can also configure the dashboard to focus on areas they deem most critical.
  - o Create and Manage Users: A Client Admin can create Client Users within their organization, as well as manage their roles and permissions. Client Users can view the security data but have limited access compared to Client Admins.
- **Set Up Alerts:**
  - o A Client Admin can configure alert management for their domain. They can select what types of threats or vulnerabilities they want to be alerted about (e.g., leaked credentials, exposed ports, dark web mentions) and define how they want to be notified (email, Slack, Teams).
- **Rescan Organization:**
  - o Client Admins have the ability to initiate a domain rescan to ensure the most current vulnerabilities and exposures are being tracked. This action is important for verifying the security posture and ensuring the domain is continuously monitored.

- **Monitor Security Posture:**
    - o Client Admins can monitor the continuous security assessment of their domain. Cyfax will automatically track any changes or exposures to ensure that any drift in their security posture is detected and alerted to the admin.

What a Client Admin Cannot Do:

- **Cannot Create, Modify, or Delete Partner Users/Partner Admins:** A Client Admin does not have the permissions to create, modify, or delete Partner Users or Partner Admins. They can only manage users and settings within their own client organization.
- **Cannot Access or Manage Other Client Domains:** A Client Admin can only manage and view data for the domain(s) they have been explicitly assigned to by the Partner Admin. They cannot access or manage other clients' domains unless explicitly authorized.

3. User Deletion by Partner Admin

When a Partner Admin wants to delete users, they will be presented with two options:

- **Complete Deletion:** This action will remove the user from the system entirely, including any associated groups and permissions.
- **Remove from Group:** This action will remove the user from a specific group but keep their account active. The user can be re-added to the group or assigned to another group later.

The key here is that Partner Admins can only manage users within their Partner Org or the client organizations they are authorized to manage. A Partner Admin cannot delete users from other organizations unless they are assigned to the same domain or group.

Summary

- **Partner Admin:** Manages multiple client organizations, can create and manage Partner Users, Client Admins, and Client Users, and can view all client data. They have permissions to delete users but only within the groups they manage.
- **Client Admin:** Manages a specific client domain, can create Client Users, set up alerts, perform rescans, and monitor security posture for their domain. They cannot create or delete Partner Users, nor access data for other client organizations.

Cyfax Threat Intelligence Section

The Cyfax Threat Intelligence Section provides powerful tools for security practitioners to validate and review Indicators of Compromise (IOCs) and vulnerabilities using Beacon Technologies' proprietary Vortex Cyber Threat Intelligence platform. This section plays a crucial role in helping users reduce the workload associated with verifying malicious IOCs and gaining deeper insights into the latest vulnerabilities impacting their environment.

1. Indicator of Compromise (IOC) Lookup Using Vortex

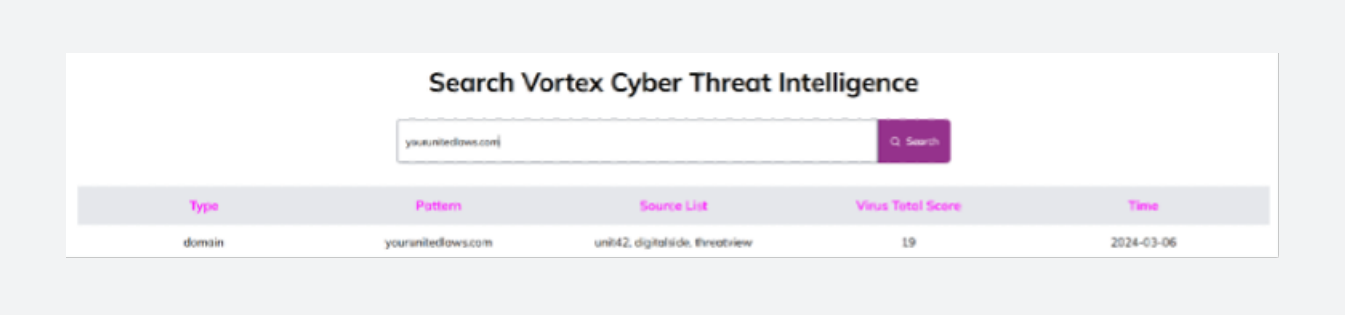
In this section, users can quickly check the status of any Indicator of Compromise (IOC) by entering details such as IPv4/IPv6, domain names, URLs, or hash values. Vortex will return the most up-to-date assessment regarding the maliciousness of the IOC, providing the user with critical insights about its potential risk. Additionally, Vortex will show the sources that have validated this IOC and other relevant data.

How It Works:

- **IOC Entry:** Users can enter IOCs like IP addresses, domains, URLs, or hash values into the Vortex IOC Lookup tool.
- **Vortex Validation Process:**
  - o Vortex employs a patented 3-step process to validate IOCs with high precision.
  - o It integrates data from over 70 reputable and premium sources worldwide, reducing the likelihood of false positives.
  - o For IOCs that are potentially patient zero (i.e., new IOCs that have not yet been widely tested), Vortex verifies these through a double-checking mechanism to confirm their malicious nature before issuing a verdict.
- **API Access:** For users who require bulk IOC lookups, API-metered access is available. Contact your Beacon representative to get started.

Example:

If a security analyst suspects that a domain is associated with a phishing attack, they can input the domain name into Vortex. Vortex will return a risk score, the validation sources, and any other relevant threat intelligence associated with that domain.



Benefits for Users:

• **No More Manual Validation:** Vortex removes the burden of manually cross-checking IOC data from multiple threat intelligence sources.
• **Increased Efficiency:** Vortex's automated validation process speeds up threat analysis for SOC analysts, reducing the need for time-consuming manual lookups.
• **Accurate, Actionable Insights:** With a focus on reducing false positives and checking new IOCs against various global sources, security teams can act with confidence.

2. Vulnerability Lookup Using Vortex

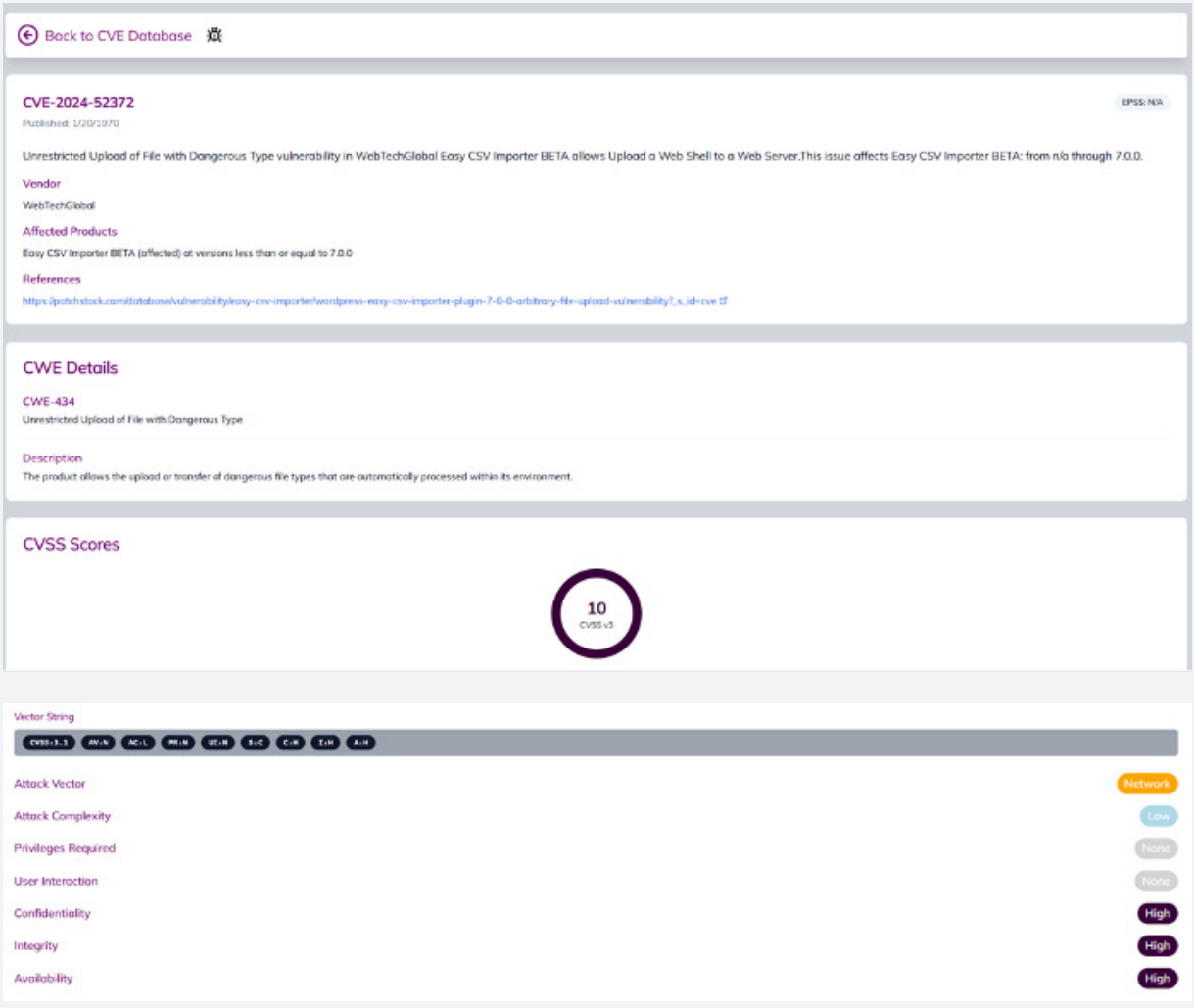
Cyfax's Threat Intelligence section also includes Vulnerability Lookups, powered by Vortex. This tool allows users to view the latest vulnerabilities, their exploitability, and other critical information.

How It Works:

• Users can explore the latest vulnerabilities (CVE) using a graphical interface that highlights which vulnerabilities are exploitable. Vulnerabilities that are exploitable are highlighted using key icons for easy identification.
• By clicking on any CVE listed, the user will gain access to detailed information about the vulnerability, including CVSS scores, affected products, and links to official references.
Example: When a user clicks on a CVE-2024-43625 entry, they are presented with a detailed view like this:
CVE-2024-43625
• **EPSS (Exploitability Probability Scoring System):** 0.000530000
• **Published:** 1/20/1970
• **Vendor:** Microsoft
• **Affected Products:**
  o Windows Server 2022
  o Windows 11 version 22H2 and above
• **CWE Details:**
  o CWE-416: Use After Free (Memory handling vulnerability)

• **CVSS Score:** 8.1 (High)
  o CVSS v3: Attack Vector: Local
  o Complexity: High
  o Privileges Required: None
  o User Interaction: None
  o Impact: High confidentiality, integrity, and availability impact.
• **References:**
  o Microsoft Security Response
• **Description:**

This vulnerability occurs when a product reuses or references memory after it has been freed, which could allow an attacker to execute arbitrary code.



How This Helps Security Practitioners:

• **Visual Insight into Exploitability:** The exploitability icons help users quickly gauge the risk of a vulnerability and prioritize remediation efforts.

• **In-Depth Information:** Each CVE entry includes vital details such as the affected versions, attack vector, CVSS score, and any available patches or mitigation steps.
• **Actionable Data:** By clicking on the CVE, users can drill down into the specifics and access vendor links to resolve or mitigate the vulnerability.

3. How Threat Intelligence Helps in Day-to-Day Operations

The Cyfax Threat Intelligence Section, powered by Vortex, equips administrators with essential tools for both short-term and long-term risk management:

• **Proactive Threat Detection:** By reviewing IOCs and CVEs regularly, users can take preemptive actions against known threats before they escalate.
• **Contextual Understanding:** Vortex provides not only the risk level but also context—whether a given IOC or CVE has been validated by global sources, helping to make decisions based on the broader security ecosystem.
• **Efficiency for Security Teams:** Automated threat analysis reduces the time and resources needed to investigate external threats, enabling security teams to focus on remediation efforts and strategic planning.

4. Summary of Vortex Threat Intelligence Benefits

1. Comprehensive IOC Lookups: Easily validate domains, IPs, URLs, or hashes against global threat intelligence sources.
2. Detailed Vulnerability Information: View CVE details, including exploitability, affected systems, remediation steps, and official vendor references.
3. Reduced False Positives: Thanks to the multi-source validation system in Vortex, false positives are minimized, allowing security teams to focus on actual threats.
4. API Access for Bulk Lookups: For organizations needing bulk IOC lookups, the API provides an efficient way to automate this process.
5. Visual Tools: Graphical representations of vulnerabilities and exploitable services over time, giving users actionable insights into security posture trends.

The Threat Intelligence Section of Cyfax provides a powerful suite of tools to keep your organization's cybersecurity posture ahead of emerging threats. With features like IOC lookups, vulnerability monitoring, and real-time updates from Vortex, administrators can confidently address both current risks and future vulnerabilities with precision and efficiency.

09. Alert Management Section

Cyfax's Alert Management system allows administrators to configure notifications to stay informed about critical security risks or vulnerabilities detected on their organization's perimeter. These alerts are essential for proactive risk mitigation, ensuring that your team can respond swiftly to emerging threats.

Accessing the Alert Management System

To configure alerts in Cyfax, administrators with Super Admin, Partner Admin, or Client Admin roles must follow these steps:

1. Login to Your Account: Use your administrator credentials to log into Cyfax.
2. Navigate to Alert Management: Click on the "Alert Management" option located in the "Management" section on the left sidebar.
3. Click "Create New Alert": In the Alert Management interface, click the "Create new alert" button to start setting up a new alert.

Creating a New Alert

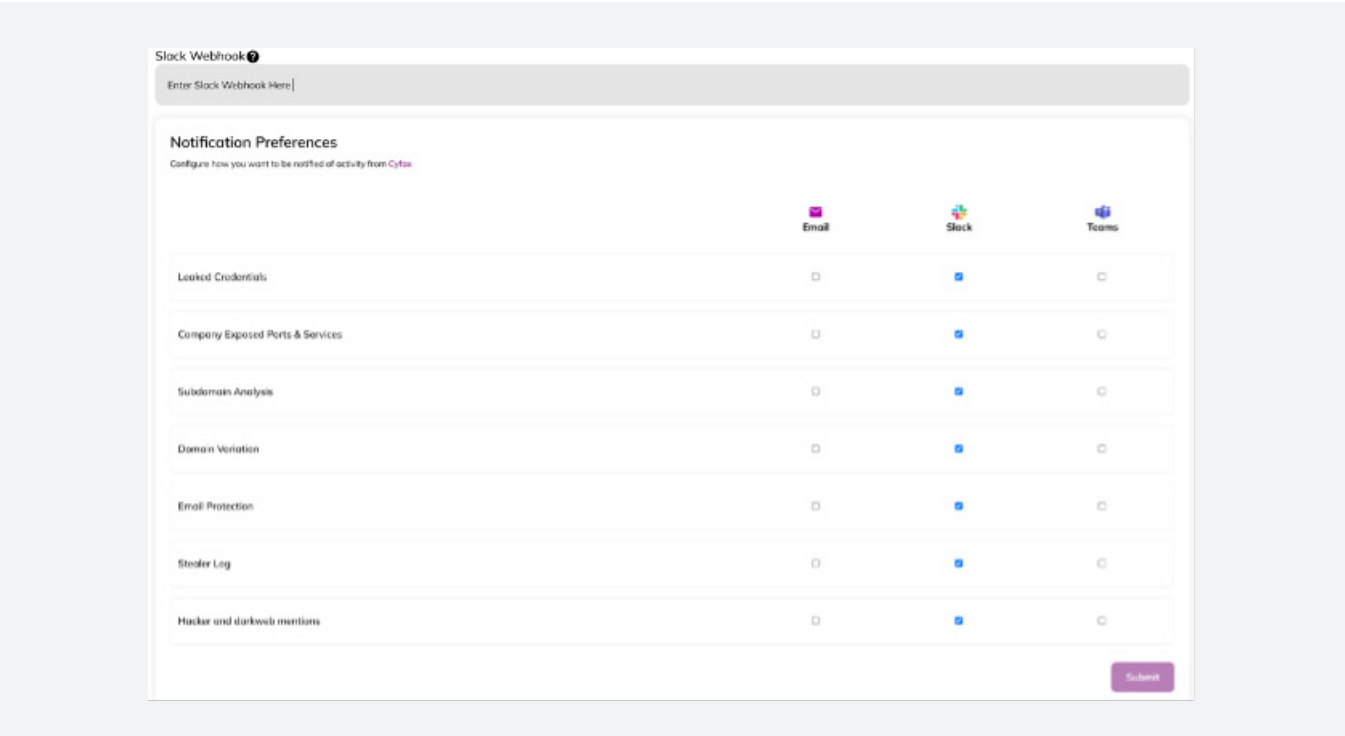
Once you are in the Alert Management section, follow these steps to create a new alert:

1. Select the Domain: Choose the domain for which you want to set up the alert. The domain must be tied to the organization you are managing.
2. Choose the Notification Method: There are multiple options for receiving alerts:
- o Email: Directly to your registered email address.
- o Teams Webhook: Integrate with Microsoft Teams to send notifications to a specific channel.
- o Slack Webhook: Integrate with Slack to send notifications to a particular channel.

3. Fill in the Required Fields: After choosing the notification method, fill in the necessary fields, such as the Owner Email (which will autofill) and select which alert types you wish to monitor (e.g., credential leaks, vulnerabilities, dark web mentions).

Note: If you select any checkbox in the **Email** column, the "Received Email" field is required. Similarly, if you select a checkbox in the **Slack** column, the "Slack Webhook" field is required. The same applies to the **Teams** column."

4. Click Submit: Once all fields are filled in, click “Submit” to save the alert.



Setting Up Slack Webhook for Alerts

To integrate Slack as your notification method for Cyfax alerts, follow these steps:

1. Create a Slack Workspace: If you don’t already have a Slack account, go to Slack’s get started page and follow the instructions to create a workspace.

2. Create a Slack Channel: After setting up the workspace, create a Channel where you want to receive the alerts.

3. Create a New Slack App:

- o Go to Slack API.
- o Choose “From scratch”, enter an application name, and select the workspace you created.
- o Press “Create App” to proceed.

4. Set Up Incoming Webhooks:

- o In the “Incoming Webhooks” section, press “Add New Webhook to Workspace”.
- o Choose the channel where you want the alerts to appear and press “Allow”.

5. Copy the Webhook URL: Once the webhook is created, copy the generated URL.

6. Paste Webhook URL into Cyfax:

- o Return to the Alert Management interface in Cyfax and paste the copied URL into the “Slack Webhook” section.

7. Submit the Alert: Click “Submit” to complete the process.

Once this is done, you’ll begin receiving Cyfax alerts in your selected Slack channel.

Setting Up Teams Webhook for Alerts

To integrate Microsoft Teams for alert notifications in Cyfax, follow these steps:

1. **Create a Microsoft Teams Account:** If you don't already have a Teams account, sign up at Microsoft Teams.
2. **Create a Channel in Teams:**
   - o After signing in, go to Teams, click the "+" button, and select "Create channel" to create a channel where you want to receive the alerts.
3. **Add Incoming Webhook:**
   - o Select More options (•••) next to the channel name, then click "Manage channel".
   - o Under Settings, click "Connectors", then choose "Edit".
   - o Search for "Incoming Webhook" and select Add, then follow the instructions to create the webhook.
4. **Copy the Webhook URL:** After setting up the webhook, copy the URL that's provided.
5. **Paste Webhook URL into Cyfax:**
   - o Go to the Alert Management section in Cyfax and paste the copied URL into the "Teams Webhook" field.
6. **Submit the Alert:** Click "Submit" to complete the integration.

Now, you will start receiving Cyfax alerts directly in your selected Microsoft Teams channel.

Modifying or Deleting Alerts

Once an alert is set up, you can modify or delete it based on your requirements:

- **Edit Alerts:** To change any details, navigate to the Alert Management section, locate the alert, and click on the Edit button. You can then adjust the domain, notification method, or alert settings as needed.
- **Delete Alerts:** If an alert is no longer necessary, you can delete it by selecting the Delete option next to the alert and confirming the action.

Best Practices for Alert Management

To ensure that your alert system is as effective as possible, consider the following best practices:

- **Fine-Tune Alert Sensitivity:** Set alerts to only trigger for high-priority or critical security issues, preventing alert fatigue from an overload of non-urgent notifications.
- **Use Multiple Notification Channels:** It is advisable to use more than one notification method (e.g., email and Slack/Teams) to ensure that alerts are seen promptly by the relevant team members.

• **Regularly Review Alerts:** Periodically check your alert configurations to ensure they reflect the current security posture and organizational priorities.
• **Prioritize Critical Alerts:** Set up alerts for the most critical vulnerabilities and security risks, such as high-severity CVEs or breaches involving sensitive data.

Custom API and SIEM Integrations

For enterprises requiring more advanced integration, Cyfax offers custom API and SIEM integrations. These integrations allow organizations to connect Cyfax's alerting system to their existing security infrastructure, providing a seamless flow of threat intelligence and security events. To explore these advanced integration options, please contact your account representative to discuss your organization's specific needs and how Cyfax can be customized to fit within your existing security ecosystem.

Troubleshooting Alert Setup Issues

If you encounter issues when setting up or managing alerts, consider these troubleshooting steps:

• **Ensure Permissions Are Correct:** Only users with Super Admin, Partner Admin, or Client Admin roles can access and configure alerts. Ensure that your role has the necessary permissions.
• **Check Webhook Configurations:** If you are using Teams or Slack webhooks for notifications, make sure that the webhook URL is entered correctly and that the appropriate permissions are granted for sending messages to the selected channel.
• **Verify Email Configuration:** Double-check that the correct email addresses are listed and ensure that your email system is configured to allow messages from Cyfax's servers.
• **Alert Duplication:** If you see duplicate alerts or unexpected behavior, try resetting your alert settings and reconfiguring them from scratch.

Conclusion

Cyfax's Alert Management system is a powerful tool for keeping your organization secure by notifying administrators of potential threats in real-time. By setting up alerts, you are taking a proactive approach to cyber defense, ensuring that you are notified promptly of any security risks and can take immediate action to mitigate them. With a simple setup process, the ability to fine-tune alerts, and integrations with popular communication tools, Cyfax makes it easier than ever to stay on top of your organization's cybersecurity posture.

By effectively utilizing Cyfax's alerting system, you ensure that your organization is always prepared to respond to threats, no matter when or where they arise.

10. Sensitive Data Scanning

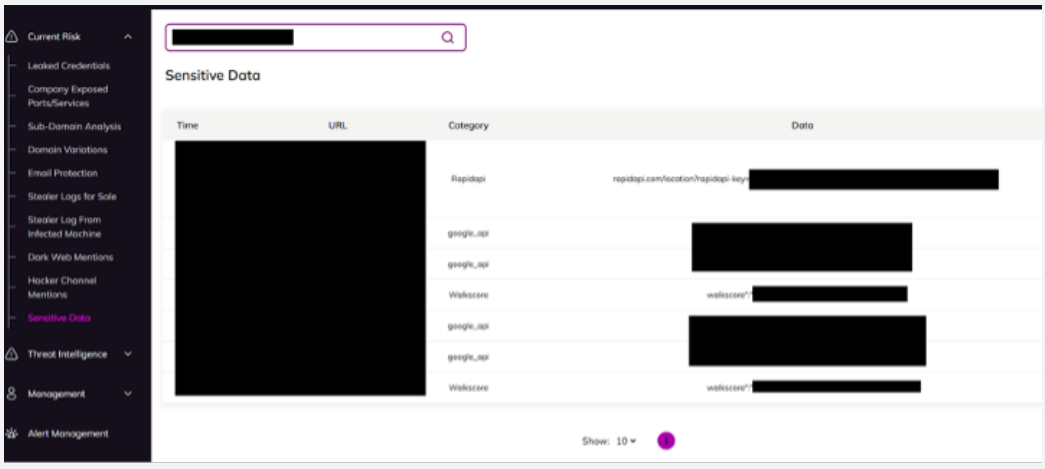
Sensitive data refers to any information that, if exposed or misused, could compromise the security, functionality, or reputation of an organization. Examples of sensitive data include:

- **API Keys:** These keys provide programmatic access to various services. If compromised, they can allow unauthorized users to perform actions or access resources.
- **Access Tokens:** Often used for authentication and session management, exposed tokens can lead to unauthorized access.
- **Encryption Keys:** Used to encrypt and decrypt sensitive information. Their exposure can compromise the confidentiality of data.
- **Configuration Files:** Files containing credentials, system settings, or sensitive code snippets that should not be publicly accessible.
- **Credentials:** Plaintext usernames and passwords embedded in code or configuration files.

Why Protect Sensitive Data?

The exposure of sensitive data can have significant consequences, including:

1. **Unauthorized Access:** Malicious actors can use compromised keys or tokens to gain unauthorized access to systems, services, or data.
2. **Service Disruption:** Attackers may abuse compromised API keys or tokens to exhaust quotas or disable critical services.
3. **Financial Loss:** Exposed credentials can lead to fraudulent activities or unexpected usage costs.
4. **Reputational Damage:** Public exposure of sensitive data can harm customer trust and brand reputation.



How Cyfax Scans for Sensitive Data

Cyfax leverages advanced scanning techniques to identify sensitive data exposure across an organization's external attack surface. Here is an overview of its capabilities:

Scanning Capabilities:

- **Deep Source Code Analysis:** Cyfax inspects publicly accessible code repositories, web applications, and libraries for embedded sensitive data such as API keys, tokens, and credentials.
- **Pattern Recognition:** Uses machine learning and predefined patterns to identify sequences matching known sensitive data formats (e.g., Google API keys, AWS tokens).
- **Contextual Analysis:** Evaluates the surrounding context of identified patterns to reduce false positives and pinpoint actual exposures.
- **Continuous Monitoring:** Cyfax provides ongoing scans to detect new exposures, ensuring real-time insights into potential risks.

Detection Methods:

1. **Static Webpage Scanning:** Analyzes the source code of public-facing websites and applications.
2. **File Inclusion Monitoring:** Identifies sensitive data embedded in linked JavaScript, CSS, or other resource files.
3. **Version Control Leaks:** Scans public repositories for leaked data in historical commits or configuration files.

Risk Mitigation

To address sensitive data exposure, Cyfax provides actionable insights and recommendations:
General Recommendations:

- **Immediate Rotation of Exposed Keys:** Upon identifying an exposed key or token, regenerate it and revoke the old key to prevent misuse.
- **Restrict API Key Usage:** Configure referrer restrictions in cloud platforms (e.g., Google Cloud, AWS) to ensure keys are only usable by specific domains or IP ranges.
- **Enable Least Privilege:** Assign minimal permissions to each API key or token to limit the potential impact of exposure.

Development Practices:

1. **Avoid Hardcoding Sensitive Data:** Use environment variables or secret management tools to store credentials securely.
2. **Secure Configuration Files:** Ensure that sensitive files are excluded from public repositories using .gitignore or equivalent mechanisms.

3. Encrypt Sensitive Data: Store sensitive information in encrypted formats wherever feasible.

Platform-Specific Guidance:

- **Google API Keys:** Enable billing alerts and API usage limits. Monitor logs for unusual activity.
- **AWS Access Keys:** Use IAM roles instead of long-lived access keys wherever possible.
- **Square Access Tokens:** Regularly review integrations and enforce two-factor authentication for associated accounts.

Continuous Monitoring:

Cyfax's continuous monitoring ensures:

- **Detection of Drift:** Identifies changes in the external attack surface that could expose new sensitive data.
- **Real-Time Alerts:** Sends notifications when new exposures are detected.
- **Comprehensive Reporting:** Provides detailed insights into the location and nature of sensitive data exposure to support remediation efforts.

Conclusion

Sensitive data exposure poses a significant risk to organizations, but with Cyfax's advanced scanning and monitoring capabilities, administrators can detect, address, and prevent such issues proactively. By implementing the recommended practices and leveraging Cyfax's continuous assessment features, organizations can maintain a robust and secure external attack surface.

11. Security and Best Practices

Security Configuration Guidelines:

• **Enforce Multi-Factor Authentication (MFA):** Always enable MFA across all user accounts, particularly for administrators. This adds an extra layer of protection by requiring something the user knows (password) and something the user has (MFA code or app), reducing the risk of unauthorized access.
• **Update and Patch Regularly:** Ensure all systems, including Cyfax integrations, are up to date with the latest security patches. Regular updates help protect against newly discovered vulnerabilities.
• **Change Passwords for Leaked Credentials:** Immediately change passwords for any compromised credentials detected within Cyfax. Leaked credentials are highly valuable to attackers, so swift action is critical. Enforce periodic password changes (e.g., quarterly) and ensure passwords are strong (use passphrases, complexity requirements, etc.).
• **Limit User Access (Least Privilege):** Assign users only the permissions necessary for their job roles. This minimizes the risk of malicious or accidental misuse of the platform. Regularly review user roles to ensure they still align with job responsibilities.
• **Enforce Strong Password Policies:** Beyond regular changes, enforce strong password policies such as minimum length, use of special characters, and disallowing common passwords. This reduces the likelihood of passwords being guessed or cracked.
• **Monitor Access Logs:** Regularly audit access logs to detect unusual or unauthorized access patterns. Set up alerts for high-risk actions, such as failed login attempts or privilege escalations, and investigate suspicious activity immediately.
• **Backups and Redundancy:** Ensure that critical data and configurations are backed up regularly, and test recovery procedures. Implement disaster recovery protocols to minimize downtime in the event of a security breach.

Managing User Roles and Permissions:

• **Role-Based Access Control (RBAC):** Leverage role-based access to assign permissions based on job function. Ensure that Partner Admins, Client Admins, and Users only have access to the data they need to perform their roles. This minimizes the potential for internal breaches.
• **Review Permissions Regularly:** Conduct periodic reviews of user access and permissions to ensure no over-privileged accounts exist. Users should only retain access to resources for as long as needed, with a documented process for when access is revoked or modified.

• **Separation of Duties:** For critical security actions, ensure that multiple levels of approval are required. For example, have one user responsible for initiating a password change and another for verifying or approving the change.
• **Use Groups for Organizational Structure:** Use Cyfax's group management capabilities to organize users according to departments or roles (e.g., marketing, IT, finance). This allows for easier management of permissions and ensures consistency across the organization.

Maintaining Data Integrity and Privacy:

• **Encrypt Sensitive Data:** Always use encryption for sensitive data, both in transit and at rest. This ensures that even if data is intercepted or accessed by unauthorized parties, it remains unreadable.
• **Data Minimization:** Limit the collection and storage of sensitive data to only what is necessary for business operations. Regularly assess what data is stored and ensure it's justified.
• **Data Access Audits:** Regularly audit access to sensitive data, particularly personal and financial information. This can help identify unauthorized access and mitigate risks related to insider threats.
• **Third-Party Integration Security:** When integrating with third-party systems, ensure that they meet the same security standards as your internal systems. Use secure APIs and regularly monitor integration points for vulnerabilities.
• **Ensure Compliance with Data Protection Laws:** Cyfax is designed with compliance in mind, aligning with global data protection regulations such as GDPR, CCPA, HIPAA, and ISO/IEC 27001 standards. As part of the platform's commitment to safeguarding sensitive data, Cyfax adheres to strict data handling, retention, and deletion practices. These guidelines ensure that data is processed in accordance with the highest industry standards and regulatory requirements.

  o Data Processing and Retention: Cyfax follows data retention policies that specify how long data is kept based on its relevance and the organization's compliance requirements. Once data is no longer needed or after an explicit request for deletion, it is securely erased in compliance with the applicable regulations.

  o Data Deletion and Anonymization: Cyfax implements processes to ensure sensitive data is deleted securely when no longer required, and if stored temporarily, it is anonymized. This ensures compliance with GDPR's Right to Erasure and similar regulations.

  o ISO 27001 Certification: Cyfax follows the ISO/IEC 27001 framework for information security management. This provides assurance that data security measures are regularly audited and are effective in protecting sensitive information.

• **Data Integrity and Privacy Through Patented Techniques:** Cyfax ensures the integrity and privacy of sensitive data through advanced techniques such as one-way hashing. For discoveries sourced from criminal channels or forums, Cyfax employs one-way hashing to mask sensitive data during

the validation process. This ensures that malicious IOCs are flagged without storing the full details, thereby minimizing risk and further protecting organizational data.

• **Data Anonymization:** In cases where detailed information is not required, anonymize or pseudonymize data before storing or processing it. This reduces the impact of a data breach by ensuring that exposed data cannot be traced back to individuals.

Best Practices for Addressing Specific Findings in Cyfax:

• **Leaked Credentials:** Change the compromised passwords immediately. Use Cyfax alerts to identify and address any new leaks. Enforce regular password changes and ensure that passwords meet complexity requirements. Implement MFA to protect accounts even when passwords are compromised.

• **Exploitable Vulnerabilities:** Use Cyfax's findings to identify critical vulnerabilities in your external infrastructure. Patch these vulnerabilities immediately and prioritize them based on their potential exploitability. Review and follow NIST vulnerability management guidelines, and ensure that patched systems are re-scanned for confirmation.

• **Sensitive Data Exposure:** When sensitive data is exposed (e.g., API keys, access tokens), immediately revoke the exposed keys and rotate credentials. Implement access control and monitoring mechanisms to prevent unauthorized access to sensitive data.

• **Dark Web Monitoring Alerts:** Set up alerts to notify you of sensitive data or compromised credentials related to your organization being mentioned on the dark web. Act swiftly to mitigate any risks by updating passwords, enabling MFA, and securing affected accounts.

• **Hacker Channel Mentions:** If your organization is mentioned in hacker channels, assess the context of the mention and respond accordingly. Monitor the affected systems for signs of exploitation and strengthen defenses around critical assets.

By following these best practices, admins can maintain a robust cybersecurity posture, prevent unauthorized access, and ensure that sensitive data remains secure. Regular monitoring, timely responses, and adherence to security protocols help ensure that Cyfax delivers maximum protection for your organization.

12. Troubleshooting and Support

Common Issues and Solutions:

While Cyfax employs cutting-edge technology and automation to ensure the seamless operation of its systems, there are occasionally instances where things do not go as planned. The system is geo-redundant across the globe, allowing for quick data processing and faster discovery of vulnerabilities. However, due to the scale of the system's capabilities, certain issues can arise that require attention. Below are some of the most common issues users may encounter and suggested solutions:

1. Delayed Penetration Testing Reports:

- **Issue:** Occasionally, users may experience delays in receiving penetration testing reports, especially when the system is under significant load.
- **Cause:** This delay usually happens when Cyfax is processing millions of Indicators of Compromise (IOCs) from various sources worldwide. The system is working hard to validate and generate detailed reports, and high traffic may slow down processing time.
- **Solution:** In these cases, patience is key. Most delays are temporary and are resolved within a short period. A report should never take more than 3 hours to complete. If a report exceeds this timeframe, contact Cyfax support.

2. System Not Responding or Slow Performance:

- **Issue:** At times, users may experience slow performance or the system may fail to respond.
- **Cause:** This could be due to heavy traffic or large-scale processing tasks within the platform.
- **Solution:** Wait a few moments, as the system may be processing large volumes of data. If the issue persists, try logging out and logging back in. If the problem continues, contact support for assistance.

3. Inaccurate Data or Missing Information:

- **Issue:** Sometimes, users may notice discrepancies in the data or missing information in reports.
- **Cause:** These discrepancies can occur when the system has not completed a full scan or when there was an issue processing certain indicators.
- **Solution:** Perform a re-scan of the domain to ensure the latest data is gathered. If the problem continues, it may be a specific data processing error. Contact support for further troubleshooting.

4. Alerts Not Being Triggered or Delayed Alerts:

o Issue: Alerts that should be triggered in the event of a potential security issue may not appear, or they may be delayed.
o Cause: Alerts may be delayed due to high system load or misconfiguration of the alert settings.
o Solution: Review the alert settings to ensure they are configured correctly. If the problem persists, contact support to investigate any underlying issues in the alert system.

5. User Permissions or Access Issues:

o Issue: Users may experience issues with roles and permissions, such as not having the correct access to certain sections of the platform.
o Cause: This can be due to misconfigured roles or permission settings.
o Solution: Review user roles and permissions to ensure they are correctly assigned. If adjustments are needed, make the necessary changes. For assistance, contact support to help resolve access issues.

6. Problems with Report Download or Data Export:

o Issue: Users may encounter difficulties when attempting to download reports or export data.
o Cause: This issue may be related to network connectivity or temporary server issues.
o Solution: Ensure your network connection is stable and try the download again. If the issue persists, try downloading a different report or contact support for assistance.

Contacting Support:

If you encounter an issue that you cannot resolve on your own or require further technical assistance, Cyfax provides dedicated support to help address your concerns.

• **Email Support:**

For technical issues or questions about the system, please reach out to Cyfax's support team by sending an email to tac@cyfax.ai. Include a detailed description of the problem, including screenshots or error messages if possible. This will help the support team respond more efficiently.

• **Contact Us Forms:**

You can also access contact forms on the Cyfax website at cyfax.ai. These forms are available on various pages across the site and provide an easy way to submit inquiries or report issues directly to the support team.

• **Response Time:**

Our technical support team aims to respond as quickly as possible. Most issues are resolved within 24-48 hours, but please note that high-priority incidents may take precedence.

Cyfax is committed to providing fast, reliable support to ensure your experience is as seamless as possible. Our team is available to guide you through any issues or questions you may have and to ensure that the platform continues to meet your cybersecurity needs.

13. Appendices

Glossary of Terms

This section provides a list of key terms, acronyms, and their definitions to help users navigate and understand the content in the Cyfax Administrator's Guide more easily.

- **API (Application Programming Interface):** A set of protocols and tools that allow different software applications to communicate with each other. In Cyfax, the API allows users to perform bulk lookups of IOCs and integrate Cyfax data into their existing security systems.
- **CVE (Common Vulnerabilities and Exposures):** A publicly disclosed list of vulnerabilities and exposures in software or hardware. Each CVE has a unique identifier used to track and manage specific vulnerabilities.
- **CVSS (Common Vulnerability Scoring System):** A standard for measuring the severity of vulnerabilities. It provides a numeric score ranging from 0 to 10, with higher scores indicating greater severity.
- **IOC (Indicator of Compromise):** Artifacts or pieces of forensic data that can be used to identify potential malicious activity on a network or system, such as IP addresses, domains, file hashes, or URLs.
- **EPSS (Exploitability Probability Scoring System):** A scoring system used to assess the likelihood that a vulnerability will be exploited, based on several factors including exploitability and exposure.
- **Vortex:** Beacon Technology's proprietary Cyber Threat Intelligence platform that powers the IOC lookups and vulnerability validation within Cyfax.
- **SOC (Security Operations Center):** A team or facility responsible for monitoring and defending an organization's information systems and networks from cyber threats.
- **CWE (Common Weakness Enumeration):** A community-developed list of common software weaknesses that provides detailed information about how vulnerabilities are introduced into systems.
- **Patented 3-Step Process:** A process used by Vortex to validate IOCs, focusing on reducing false positives, verifying IOCs in the wild, and double-checking new IOCs to ensure they are accurate and actionable.
- **Exploitability:** Refers to the potential for a vulnerability to be used by attackers to exploit a system. The higher the exploitability, the more likely an attacker can use that vulnerability to compromise a system.
- **Vulnerability:** A weakness in a system, software, or hardware that can be exploited by a threat actor to compromise the system's security.
- **Threat Intelligence:** Information about potential or current threats to an organization's

cybersecurity, including data about IOCs, vulnerabilities, and ongoing cyberattacks.

- **Rescan:** The process of running a hyperautomated penetration test to check for new vulnerabilities or exposures in an organization's external cybersecurity posture.
- **Dark Web Monitoring:** The practice of monitoring dark web platforms and marketplaces for mentions of sensitive data, stolen credentials, or other malicious activities that could affect an organization.
- **Exploit Code Maturity:** A rating that describes the maturity level of an exploit, ranging from unproven (not yet used in the wild) to high (widely available and actively used).

References

This section includes external references used throughout the guide to provide further context or to offer additional resources for advanced users.

1. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations – A reference to cybersecurity and privacy controls in federal systems, useful for understanding risk management frameworks.

2. CVSS v3.1 Specifications: Common Vulnerability Scoring System (CVSS) – A resource to understand the methodology and scoring system used to evaluate vulnerabilities.

3. MITRE ATT&CK Framework – A knowledge base of adversary tactics, techniques, and procedures based on real-world observations.

4. Microsoft Security Response Center (MSRC): CVE-2024-43625 – An example link to a CVE detail page for understanding vulnerability specifics.

Cyfax Administrators Guide
detect.solutions