Platform Documentation

- [ReConfirm External Attack Surface Documentation](#)
- [Secure Software Development Lifecycle (SSDL) Statement](#)

ReConfirm External Attack Surface Documentation

Introduction and Overview

About the ReConfirm External Attack Surface Management platform

ReConfirm does:

- Comprehensive scanning of domain and network registration databases.
- Analysis of Internet DNS IP to hostname resolution logs.
- Passive browsing of websites.
- Scanning for Email security
- Analytics of publicly accessible code, content, and configurations.
- Monitoring the dark web for potential data breaches.
- Find all related URLs.
- Finds real vulnerabilities.
- Analyzing Internet port scan data.
- Gives you insight in your External Attack Surface before hackers do.

ReConfirm does not:

- Tamper with parameters.
- Inject code.
- Try to bypass authentication.

Purpose

The "Introduction and Overview" section of our External Attack Surface Management platform documentation serves as the gateway to understanding the core purpose and functionality of our platform. Here, we aim to provide a clear and concise explanation of what our platform is designed to achieve.

Our primary goal is to empower organizations to proactively manage and secure their external attack surface. By offering comprehensive scanning, monitoring, and vulnerability management capabilities, our platform helps you identify and mitigate potential security risks before they can be exploited by malicious actors. Whether you're a security professional, IT administrator, or business owner, our platform equips you with the tools needed to safeguard your digital assets and protect your organization's reputation.

Audience

This documentation is intended for a diverse audience, catering to a wide range of roles and expertise levels:

1. **Security Professionals:** Security analysts, penetration testers, and cybersecurity experts who require in-depth knowledge of our platform's capabilities for conducting thorough assessments and maintaining strong security postures.
2. **IT Administrators:** Network administrators, system administrators, and IT managers responsible for configuring and managing the platform within their organization.
3. **Business Owners and Decision Makers:** Executives, business owners, and managers who want to gain a high-level understanding of how our platform enhances their organization's cybersecurity strategy.
4. **Technical Teams:** Developers and DevOps teams interested in integrating our platform into their existing toolsets or workflows to ensure the security of their applications and infrastructure.
5. **Anyone Concerned About Security:** Users who may not be technical experts but are concerned about the security of their organization's digital assets and want to learn how our platform can help mitigate threats.

No matter your role or background, this documentation will guide you through the essential features and functionalities of our platform, enabling you to make informed decisions and leverage our tools effectively to bolster your organization's security posture.

Getting Started and First Usage

Prerequisites

Before you begin, ensure you have the URL of your private ReConfirm dashboard.

In this section, we'll guide you through the essential steps to begin your journey with the ReConfirm External Attack Surface Management platform.

Here's what you can expect to find in this chapter:

1. Login and Account Security: Learn how to access the platform, manage your account and add additional security to your account.

2. Licensing: Explore how to add licenses to your platform to add the licensed domains to the platform.

3. Domain Verification: Perform domain validation, the mandatory process to confirm ownership of the licensed domains before initiating scans. We'll walk you through the steps to validate domains effectively.

Login and Account Security

Logging In:

- Navigate to your private dashboard URL.
- Log in using the provided account credentials.
- Upon successful login, you'll be directed to a password change screen.

Setting a Password:

- You have the option to let ReConfirm automatically generate a secure password for you.
- If you choose this option, simply copy and paste the generated password into the designated field.
- Click "Save" to confirm your password.
- Make sure you store the password in a safe place.

Linking a 2FA App:

- Navigate to "Account Settings". This can be accessed by clicking on the down-arrow on the right side of your Name in the left menubar to expand the Account Settings menu.
- Click on "Add App".

- You'll be presented with a QR Code. You can:
  - Scan this QR Code using your preferred 2FA application, or
  - Manually enter the provided connection code into your 2FA app.
- After adding the code, click "Next".

Verification:

- Your 2FA app will generate a One Time Pass (OTP) code.
- Enter the OTP code into the designated field.
- Click "Verify".

Completion:

- With the verification successful, your setup is complete. You've successfully linked your 2FA app to ReConfirm.

Licenses are a fundamental component of our External Attack Surface Management platform, allowing you to scan and assess domains that fall under your licensed agreement. In this section, we'll walk you through the process of managing licenses, highlighting the key details and information you can expect to find.

Licensing

Please note that access to the License section is exclusively reserved for administrators. Administrators have the privilege and responsibility of overseeing license management on the platform. Here's how you can access the License section:

1. **Administrator Login:** Log in to your account with administrative privileges using your unique credentials.
2. **Navigate to Licenses:** Once you're logged in, navigate to the "Licenses" section within the platform. This section is specifically designed for administrators.

Adding a License

Adding a license to your platform is a straightforward process. Follow these steps to get started:

1. **Click "Add License":** Within the License section, locate and click the "Add License" option. This initiates the process of adding a new license key to your account.
2. **Enter the License Key:** You will be prompted to enter the license key provided to you by your sales representative. Accuracy is paramount, as the license key serves as the authorization for domain scanning.
3. **License Details:** Upon successful entry of the license key, the page will display vital license details, including:
   - **License Owner Contact Details:** Information about the license owner, which is essential for communication and verification.

- **License Sales Representative:** Contact information for your sales representative, ensuring you have a direct point of contact for any inquiries or support regarding the license.
- **Licensed Domains:** A list of domains covered by the license agreement, specifying which domains are eligible for scanning.
- **License Expiration Date:** The date when the license is set to expire, prompting you to renew or extend your licensing agreement as needed.

By providing access to these license details, the platform equips administrators with the necessary information to manage and oversee licensing effectively. It ensures that you are well-informed about the scope of your license and the domains it encompasses.

Domain Verification

Domain Verification is a crucial step that customers must complete before initiating scans on their selected domains within our External Attack Surface Management platform. This process serves as a fundamental security measure to ensure that the customer has ownership and control over the specified domain. Once verified, the domain's status is changed to "validated," allowing scans to be executed. Below, we provide an overview of the Domain Verification process and its significance:

Why Domain Verification is Mandatory

Ownership Confirmation: Domain Verification acts as a verification mechanism to confirm that the customer is the legitimate owner of the specified domain. This is essential to prevent unauthorized scans and ensure the security of external attack surface assessments.

Preventing Unauthorized Removal: Once a domain has been successfully verified, it is crucial to note that it is not permissible to remove the HTML file or HTTP header used for verification. Doing so will result in the domain's status reverting to "unverified." Continual verification is essential to maintain the integrity and security of the scanning process.

Verification Methods

Domain Verification can be accomplished through one of the following methods:

1. HTML File Upload: Customers can upload a specific HTML file to the main domain's web server. The presence of this file on the web server indicates ownership and control of the domain to our system.

2. HTTP Header Configuration: Alternatively, customers can set a specific HTTP header on the main domain's website. The presence and correct configuration of this HTTP header serve as evidence of domain ownership.

Verification Process

When customers initiate the Domain Verification process, our system undertakes the following steps:

1. Verification Request: ReConfirm sends a verification request to the specified domain, either requesting the presence of the uploaded HTML file or validating the HTTP header configuration.

2. Successful Verification: If ReConfirm successfully locates the HTML file or validates the HTTP header, the domain's status is changed to "validated."

3. Ongoing Verification: Our system continues to periodically verify the domain to ensure ownership remains with the customer. This ongoing verification is essential to maintain the domain's "validated" status.

4. Verification Failure: In the event that verification fails at any point, the domain's status is automatically reverted to "unverified." Scans will no longer be executed on the domain until it is reverified.

Importance of Ongoing Verification

Ongoing verification is a critical aspect of domain security. It ensures that the customer maintains control and ownership of the domain throughout the scanning process. If, for any reason, the verification fails at any point, it serves as a proactive security measure to prevent unauthorized scans and maintain the integrity of the platform's assessments.

In summary, Domain Verification is a mandatory step in our platform that confirms domain ownership and control. It is essential to prevent unauthorized scans and maintain the security of external attack surface assessments. Customers are required to maintain the verification elements on their main domain to ensure continued validation and scanning.

Dashboard and User Interface

Dashboard Overview

Upon logging into our ReConfirm External Attack Surface Management platform, users land on the user-friendly and informative dashboard. The dashboard serves as a central hub for monitoring and managing the security of your organization's external attack surface. It provides a comprehensive view of key aggregated data, allowing you to quickly assess your security posture.

![ReConfirm_ScreenShot_000002](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000002.png)

Key Dashboard Metrics:

- **Vulnerabilities:** Get an overview of the total number of vulnerabilities detected across your scanned domains, with breakdowns by severity levels.
- **Open Ports:** Monitor the number of open ports discovered during scans, providing insights into potential attack vectors.
- **Assets:** Stay informed about the total count of assets.
- **DNS Records:** Keep track of your domain's DNS records and subdomains, helping you understand your digital footprint.

User Interface

Our user interface is designed with simplicity and efficiency in mind, ensuring that users can easily navigate and access the platform's features. The menu is structured to provide quick access to various sections based on user roles and permissions.

![ReConfirm_ScreenShot_000003](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000003.png)

User Details Section:

1. **Account Settings:** Manage your profile information, edit password and add or remove 2-Factor Authentication.
2. **Help Center:** Access our comprehensive help center for documentation, or request support by raising a ticket.
3. **Report a Bug:** Report any issues or bugs you encounter while using the platform to help us continually improve.
4. **Force reset:** Gives Administators and Security Engineers the possibility to reset the platform. For example when a scan needs to be stopped or when the platform is responding unexpected. This reset won't remove any data or settings in the platform.

User Interface Section:

1. **Dashboard:** Return to the dashboard to view all relevant data and security metrics.
2. **Calendar:** Manage all scheduled scans, review past scans
3. **Reports Archive** to access and download all previously generated reports.
4. **Domain Verification:** Add and verify new domains to the platform to expand your coverage.
5. **Activity:** Review an activity log that records all actions taken within the platform.

Administration Interface Section (for Administrators):

1. **License:** Manage licensing information and options for the platform.
2. **Organizations:** Create and manage multiple organization containers and assign domains for streamlined navigation.
3. **User Accounts:** Administer user accounts, permissions, and access levels.
4. **System Settings:** Configure platform-wide settings and preferences.

Scanning Section:

1. **Start a Scan:** Initiate new scans to assess the security of your external attack surface.
2. **Scan Profiles:** Configure and manage scan profiles for consistent scanning practices.
3. **Custom Checkups:** Create custom vulnerability checks for specific security assessments.

Scanned Domains Section:

For each scanned domain, access the following menu items:

- **Email Security:** Review email security findings and configurations.
- **Vulnerabilities:** Explore vulnerabilities detected on the domain.
- **Similar Domains:** Identify domains with similarities to the scanned domain.
- **Assets:** View and manage assets associated with the domain.
- **Data Leaks:** Monitor data leak findings specific to the domain.
- **Subdomains:** Explore subdomains discovered for the domain.
- **Subdomains - Inactive:** Review inactive subdomains.
- **SSL/TLS Information:** Assess SSL/TLS configurations and certificates.
- **Report/Data Download:** Generate and download comprehensive reports.
- **Compare Findings:** Compare security findings across different scans for the same domain.

Customize Your Experience

On every page of our platform, you'll find a settings wheel located in the middle right of the page. This settings wheel allows you to customize the theme, look, and feel of the platform according to your preferences. You can tailor the platform's appearance to create a personalized and comfortable user experience.

Our dashboard and user interface are designed to provide you with the tools and insights needed to proactively manage your external attack surface's security. Whether you're an administrator overseeing multiple organizations or an individual user focused on specific domains, our platform's intuitive interface ensures you can efficiently access and utilize the features that matter most to you.

System Settings

The "System Settings" page allows you to customize and configure various aspects of the ReConfirm platform to better align with your needs and preferences.

![ReConfirm_ScreenShot_000006](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000006.png)

- **Timezone Configuration**:
  - Ensure that all time-related settings, including scheduling, reflect your local timezone.
  - Properly configuring this ensures accurate scheduling and reporting times.
- **Slack Hook URL**:
  - Integrate with Slack to receive real-time updates about scan progress.
  - Simply input your Slack hook URL to enable this feature.
- **Custom Logo (White-labeling)**:
  - *Availability depends on your subscription package.*
  - Upload your company logo to personalize the reports.
  - Useful for businesses looking to maintain brand consistency in all communications.
- **Advanced Settings**:
  ReConfirm has created the SMTP email configuration so ReConfirm can align with your company's security policies.
  - SMTP Email Configuration:
    - Customize email settings for sending notifications and reports.
    - Ideal for companies with policies against using external email services.

Account Management

The Account Management interface is accessible exclusively to administrators and plays a pivotal role in overseeing user accounts within our External Attack Surface Management platform. This interface helps administrators to manage user accounts efficiently.

![ReConfirm_ScreenShot_000008](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000008.png)

User Accounts Overview:

- **User Listing:** Administrators can view a comprehensive list of all user accounts registered on the platform.
- **Search Functionality:** Utilize the search bar to quickly locate specific users based on their details or roles.
- **Recent Logins:** Stay informed about recent user logins to monitor platform activity.

User Details: For each user, administrators can access the following information:

- **Name and Last Name:** Identify users by their full name.
- **Username:** The unique email address serving as the user's login credential.
- **User Role:** Either Administrator, Security Engineer, or Auditor.
- **Last Login Date:** Track when a user last accessed the platform.
- **Password Expiration Date:** Monitor password expiration for each user.
- **2FA Status:** Indicate whether Two-Factor Authentication (2FA) is enabled.
- **Path Restrictions Status:** See if path restrictions are enabled or not.
- **Path Restriction Expression:** If enabled, view the regular expression defining path restrictions.
- **Notes:** Read notes or comments related to the user account.

User Management Actions: Administrators have the following actions at their disposal for each user account:

- **Create User:** Create a new user on the platform by entering First Name, Last Name, Email address and choosing the User role. Additionally path restrictions and notes can be configured too upon creation.
- **Edit User:** Modify user details, including name and last name.
- **Delete User:** Remove a user account when necessary.
- **Reset Credentials:** Trigger a credential reset process for the user.

User Role Permissions:

- **Administrator:** Grants full admin rights to manage the platform, users, licenses, domains, organizational containers, initiate scans, and perform various platform actions.
- **Security Engineer:** Provides permissions to perform scans, create scan profiles, conduct domain verification, create custom vulnerability checks, generate reports, and download data.
- **Auditor:** Allows viewing of scan data, results, and the dashboard but prohibits starting scans and other edits on the platform.

Path Restrictions:

The Path Restriction function enables administrators to control access to specific URLs for users. URLs can be defined using Regular Expressions. This feature is typically used when users are required to access specific pages or are restricted from certain areas of the platform.

ReConfirm_ScreenShot_000009
Image not found or type unknown

Notes: Administrators can create and maintain notes for each user account to record important information, special instructions, or reminders.

Reset Credentials:

- When administrators choose to reset a user's credentials, the platform removes the Two-Factor Authentication (2FA) configuration (if enabled).
- The system generates a secure temporary password for the user, which administrators must copy and send securely.
- This password is valid for 12 hours, and users must log in with it.
- Upon login, users are prompted to create a new password immediately.
- If a user does not log in within 12 hours, administrators can use the reset credentials function again to generate a new temporary password.

Account Management ensures that administrators have the necessary tools and controls to manage user accounts efficiently while maintaining the security and integrity of the platform.

SSO Enablement

ReConfirm allows you to configure Single Sign-On (SSO) for authentication, currently supporting Microsoft/Azure. To set it up, follow the steps below to create an app in Azure Active Directory and configure it within the ReConfirm platform.

1. **Create an App in Azure AD**:

   a. Navigate to the Azure Portal.
   b. Search for "App Registrations" if it is not visible on your dashboard.
   c. Click on **"New Registration"** and fill out the necessary details in the registration form.
   d. After creating the app, go to the **"Certificates & Secrets"** section and generate a new client secret. Copy this secret, as it will not be displayed again.

2. **Configure Redirect URIs**:

   a. In the Azure Portal, navigate to **"Authentication"** under your app's settings.
   b. Add the following URL to the **"Redirect URIs"** section:
   `https://yourprivateenvironment.reconfirm.nl/login/sso/success`
   Click the URL which is visible in your systemsettings after clicking the question mark to copy it to your clipboard.
   c. Ensure the URI is set as a **Web Redirect URI** by clicking **"Add URI"**.

3. **Configure SSO in ReConfirm**:

   a. Log in to your ReConfirm platform.
   b. Go to **System Settings**.
   c. Paste the copied Application (client) ID and client secret from Azure into the corresponding fields within the ReConfirm SSO settings.

4. **Finalize and Save**:

   a. Click **"Save"** within ReConfirm to finalize the SSO setup.

Note: To allow a user to log in using SSO, ensure that the user already has a local account with the same email address. You can also configure whether to allow both password and SSO login methods or only allow SSO.

Organizational View

The Organizational View is a powerful feature within our External Attack Surface Management platform that empowers administrators to create a structured hierarchy of organizations and efficiently manage access to domains and scan results. This hierarchical view is particularly useful for large concerns that own multiple smaller companies or for organizations with complex structures.

Creating and Managing Organizations

Administrators can create and manage organizations within the platform to represent various entities, such as parent companies and subsidiaries. Here's how it works:

![ReConfirm_ScreenShot_000012](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000012.png)

![ReConfirm_ScreenShot_000013](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000013.png)

- **Organization Name:** Administrators can assign a unique name to each organization, reflecting the entity it represents.
- **Assigned Domains:** For each organization, administrators can assign one or more domains. These domains are associated with the organization and can be viewed by users with access to that organization.
- **Parent Organization (Optional):** Administrators can define a parent organization for each organization, creating a hierarchical structure. Sub-organizations are one level deep, and they cannot have sub-organizations themselves.

Accessing the Organizations Page: The Organizations page can be found within the Administrator Interface section of the menu, accessible only to administrators.

Organizational View for Users

The Organizational View feature enables users to streamline their view of scan results and domains based on their organizational needs. Here's how it works:

ReConfirm_ScreenShot_000011

- **Select View Option:** Users can access the Organizational View by clicking on the eye icon next to their username in the top-left menu.
- **Modal Interface:** Clicking the eye icon opens a modal interface with two tabs: Select Organizations and Select Domains.
  1. **Select Organizations Tab:** In this tab, users can select one or multiple organizations they want to have access to. This allows them to view scan results and domains associated with the selected organizations.
  2. **Select Domains Tab:** After selecting organizations in the Select Organizations tab, users can access the Select Domains tab. Here, they can further refine their view by selecting or deselecting specific domains within the chosen organizations.
- **Apply View:** After selecting the desired organizations and domains, users can click the "Apply View" button. The page will be reloaded with the selected view options, allowing users to focus on the scan results and domains relevant to their roles and responsibilities.

Maintaining the Organizational Structure

Administrators play a crucial role in maintaining the organization structure within the platform, especially when new domains are added. Here are the key steps:

1. **Assignment of New Domains:** When new domains are added to the platform, administrators should ensure they are appropriately connected to an organization. This may involve assigning the new domains to an existing organization or creating a new organization if needed.
2. **Hierarchy Management:** Administrators should review and manage the hierarchy of organizations, ensuring that parent and sub-organizations accurately reflect the organizational structure.

The Organizational View feature simplifies access to scan results and domains for users while allowing administrators to maintain a structured and organized platform that aligns with their organization's real-world structure.

Scanning and Monitoring

Initiating a Scan:

- Navigate to the dashboard.
- Click on the "Start a Scan" button.
- Fill in the required fields:
  - Assessment Title
  - Description
  - Domain
- If you wish to exclude a specific subdomain from the scan, enter it into the "Excluded Subdomains" field.

![ReConfirm_ScreenShot_000015](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000015.png)

Scheduling Your Scan:

You have two scheduling options:

![ReConfirm_ScreenShot_000016](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000016.png)

- **Specific Time**:
  - Select this option if you want to schedule a scan for a specific time in the future.
  - The scan will commence automatically at the chosen time.
- **Recurring Interval**:
  - Choose this option if you want the scan to recur at regular intervals.
  - Specify whether the scan should run daily, weekly, or monthly and at which specific time.

Configuring Your Scan:

- **Scan Profile**:
  - Options available:
    - Retag found subdomains with tags from previous scan findings (if the domain was scanned previously).
    - Enable Deep Search for Subdomains (Note: This option is slow).
    - Vulnerability Scan on Subdomains.

- SSL Scan on Subdomains.
  - Suffix Scan on Subdomains.
- **Suffix Configuration Thoroughness Level**:
  - Choose the depth:
    - Quick
    - Mildly Deep
    - Deep
    - Extremely Deep
- **Port Scanning Options**:
  - Ranges from the top 100 most commonly used ports to all ports.
  ![ReConfirm_ScreenShot_000018](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000018.png)

Custom Subdomain Sources

ReConfirm's default subdomain scanner can sometimes send numerous requests to DNS servers, potentially leading to additional charges from DNS providers. To address this, ReConfirm now supports custom subdomain sources, giving you more control over the subdomain discovery process.

Custom Sources:

A "source" is an API configuration for a DNS provider. You can add multiple sources, even for the same provider, using descriptive names for easy identification.

Supported Providers:

Currently supported are IBM NSone and TransIP.

How to implement:

1. **Go to your dashboard**
   Navigate to the dashboard as the first step.
2. **Navigate to System Settings**
   On the menu on the left, click on **System Settings**.
3. **Scroll to Custom Subdomain Sources**
   Scroll down to the "Custom Subdomain Sources" section.
4. **Add a New Source**
   Click on **"Add New Source"**.
5. **Name the Source**
   Give the source a descriptive name like **"NSone API"** or **"TransIP API"**.
6. **Generate an API Key**
   Generate an API key for the chosen resource (NSone or TransIP).
7. **Enter the API Key**
   Paste the API key into the corresponding field.

8. **Test the Configuration**
   Click the **"Test"** button to ensure the configuration works correctly for the corresponding licensed domain.
9. **Finalize the Addition**
   If everything is working correctly, click **"Add New Source"** to finalize.

Using Custom Sources in Scans:

Once configured, you can select your new API connection for DNS in your scans. On the "Start a Scan" page, look for the **"Subdomain Discovery"** dropdown menu where your custom sources will be listed. Selecting one of these will use it to perform DNS import into your platform.

ReConfirm Pro Tip: Create a separate scan profile for these scans, so you don't have to fill out the forms each time you want to scan with these custom settings and DNS import.

Notification Settings:

- By default, ReConfirm will send an email notification upon scan completion.
- To add additional email addresses to the notification list:
  - Enter them into the designated field.
  - Note: Only email addresses associated with existing dashboard users will be accepted by ReConfirm.

Save and Start:

- For convenience, you can save this scanning profile for future use.
- Click on the start a scan button to commence the scan with your configuration.

Recommended Scanning Options:

For optimal and swift results, ReConfirm advises the following settings:

- Retag found subdomains (if scanned previously).
- Enable Deep Search for Subdomains (Slow).
- Vulnerability Scan on Subdomains.
- SSL Scan on Subdomains.
- Scan All ports (this might be a bit slower).

![ReConfirm_ScreenShot_000020](C:\Users\Hackdwerg\ReConfirm\Development - ReConfirm - Screenshots\ReConfirm_ScreenShot_000020.png)

Custom Checkups:

The Custom Checkups feature empowers Administrators and Security Engineers to tailor vulnerability scans specifically for in-house developed software.

Purpose:

- Detect vulnerabilities unique to custom applications.
- Enhance the accuracy of ReConfirm's vulnerability scans by considering proprietary software behaviors.

Creating Custom Checkups:

ReConfirm's intuitive interface makes it straightforward to define custom checkups:

ReConfirm_ScreenShot_000023

1. **Navigate** to the Custom Checkups section.
2. Click on the **'Create New Checkup'** button.
3. Fill in the form fields:
   - **Name**: Specify a name for the custom checkup, e.g., "SQLi in custom software."
   - **Reference**: Link to an internal or external document that provides context or further information about the checkup.
   - **Severity**: Define the level of risk, ranging from "Critical" to "Informational."
   - **Description**: Provide a concise description of the checkup.
   - **Request Path**: Indicate the targeted path, e.g., `{{RootURL}}/login.php?id=`.
   - **Request Method**: Specify the HTTP method: GET, POST, DELETE, PUT.
   - **Status Code**: Expected HTTP response status code, e.g., 200 or 300.
   - **Content Length**: Expected response content length from the server.
   - **Match Type**: Choose the format for the match: Plain Text or Regular Expression (ReGex).
   - **Match Text**: Specify the exact text or pattern to match against the response.
4. **Test the Checkup**: Before saving, test the checkup to ensure it functions as expected.
5. **Save** the checkup.

Implementation:

- Once saved, ReConfirm integrates this custom checkup into your private server.
- The checkup is automatically executed during every subsequent scan by ReConfirm.

Privacy Assurance:

- **Data Integrity**: Custom checkups, being proprietary to your operations, remain confidential. ReConfirm respects your privacy and ensures that these checkups are not shared externally and belong solely to the customer.

Scan Results

Scan Results within our External Attack Surface Management platform provide a comprehensive overview of the security posture and associated data for a given domain. Scan results are grouped by domain and cover various critical aspects of domain security. These topics include:

Email Security

The Email Security section presents the results of security checks on key email authentication protocols, including DMARC, SPF, MX, and DKIM. This information helps users assess the email security configuration of the scanned domain.

DKIM Selectors

ReConfirm checks a default list of DKIM Selectors. If you want to add a custom selector for your organization. Please click "Check Selectors" and add your selectors.

Vulnerabilities

In the Vulnerabilities page, users can explore all identified vulnerabilities for the selected domain. Key details for each vulnerability include:

- **URL or Host:** The location where the vulnerability was discovered.
- **Domain:** The domain associated with the vulnerability.
- **Severity:** Categorized as Critical, High, Medium, Low, or Informational.
- **Vulnerability Name:** The name or description of the vulnerability.
- **Tags:** Manually assigned tags for better organization.

Users can click "View" to access detailed information about each vulnerability, including the detailed result and, if available, mitigation advice. Additionally, users can mark vulnerabilities as "Resolved" if they believe the issue has been fixed. Resolved vulnerabilities are moved to a separate section for easy tracking. From that section users are able to put vulnerabilities back on the list again by clicking "Undo Resolved". If a resolved vulnerability is detected again in subsequent scans, the platform will automatically un-resolve it.

In the Vulnerabilities page, users have the following additional capabilities:

- **Add tags to selected vulnerabilities:** Select one or more vulnerabilities and add a custom tag to these to filter and group them in any way. Please note that tags may not contain special characters!
- **Email Vulnerabilities:** Select specific vulnerabilities and send them as attachments via email to designated recipients. This feature streamlines communication and collaboration among team members to address critical vulnerabilities promptly.

- **Export Vulnerabilities:** Choose vulnerabilities and export them in multiple formats, including TXT, CSV, or XML files. This functionality allows users to maintain records or share vulnerability data with relevant stakeholders.
- **Filter by (Sub)domain:** Users can filter vulnerabilities based on specific (sub)domains, allowing them to focus on vulnerabilities affecting particular areas of their external attack surface.
- **Severity Filtering:** Prioritize your response by filtering vulnerabilities based on their severity level, whether they are classified as Critical, High, Medium, Low, or Informational.
- **Text Search:** Utilize a powerful text search feature to search for specific result data, URL, or descriptions within the vulnerabilities. This capability streamlines the process of finding vulnerabilities related to specific keywords or phrases.

Similar Domains

The Similar Domains page lists domains that resemble or sound similar to the scanned domain. This information can be valuable for identifying potential look-alike domains that could be used for phishing or other malicious activities.

On the Similar Domains page, users can perform the following action:

- **Export Similar Domains:** Easily export the list of similar domains in a CSV file. This export feature simplifies data sharing and analysis for users working with domain similarity data.

Assets

The Assets page provides an overview of all IP addresses associated with the scanned domain. For each IP address, users can access details such as DNS records, open ports, and detected services, helping to identify potential entry points for attackers.

Data Leaks

In the Data Leaks section, the platform scans for occurrences of the scanned domain in multiple data breaches on the dark web or deep web. The results display leaked data and the quantity of leaks found in each applicable data breach, highlighting potential data exposure.

Subdomains

The Subdomains page presents a comprehensive list of detected DNS records within the scanned domain. For each subdomain, users can access details such as vulnerabilities, security headers (if scanned), assigned tags, SSL/TLS results, detected suffixes (if available), and, if provided, a screenshot of the webpage.

The Subdomains page offers several additional features for enhanced functionality:

- **Create and Add Tags:** Users can create custom tags and associate them with subdomains. Tags help organize and categorize subdomains for easier management and tracking.
- **Rescan Selected Subdomains:** Specific subdomains can be selected, and users can trigger a rescan of these selected subdomains directly from the interface. This feature allows users to verify and monitor the security status of specific subdomains proactively.
- **Manual Subdomain Entry:** In cases where a subdomain is not detected by our scanner, users can manually enter the missing subdomain by clicking the "Add Subdomains" option within the Subdomains page.
- **Export Subdomains:** Users can export the list of subdomains in a CSV file, facilitating data sharing and external analysis of subdomain information.

Subdomains - Inactive

This page displays DNS records that historically existed but could not be resolved during the scan. It also includes DNS records that were resolved but turned out to be unreachable due to a firewall or the IP address being offline.

On the Subdomains - Inactive page, users can export the inactive subdomains list in a CSV file for easy data sharing and further analysis.

SSL/TLS Information

The SSL/TLS Information page showcases the results of a security scan on the SSL/TLS protocol and certificates associated with the scanned domain. This information is crucial for assessing the domain's encryption and security configurations.

In the SSL/TLS Information page, users have the option to export SSL/TLS findings in a CSV file. This export capability simplifies data sharing and analysis related to SSL/TLS security configurations.

Compare Findings

The Compare Findings page is a valuable resource when at least two scans have been executed on a domain. It highlights the differences between scan results, enabling users to track progress in resolving findings and identify newly discovered vulnerabilities that require attention.

Scan Results provide users with detailed insights into the security status of their domains, enabling them to take proactive measures to enhance their external attack surface security.

Reporting

Once a scan is successfully completed, ReConfirm generates a comprehensive report, providing you with a detailed breakdown of the scan's findings.

- **Generating a Report**:
  - Click on the "Report/Data Download" button in the menu.
- **Report Features**:
  - **Detailed Descriptions**: Comprehensive breakdown of each dashboard section.
  - **Logical Order**: Findings are presented from critical to informative.
  - **Multiple Formats - Choose between:**
    - PDF: For offline reading and sharing.
    - HTML, or
    - Combined: Both PDF and HTML in a zip file.
- **Archived Reports**:
  - All reports are stored for future access.
  - Find them in the "Reports Archive" section.
  - For detailed instructions, see Chapter XXX.

Integrations

Webhook Integration

Our External Attack Surface Management platform offers a powerful webhook integration function that allows you to seamlessly connect our platform with your existing tools, workflows, and security processes. Webhooks provide a way to receive real-time notifications and data updates from our platform, enabling you to stay informed about changes and events that matter to your organization's security posture.

Key Benefits of Webhook Integration:

1. **Real-Time Alerts:** Receive instant notifications about new findings, scan results, and security events directly to your designated endpoints.
2. **Automation:** Integrate with your incident response, ticketing, or orchestration systems to automate responses and actions based on incoming webhook data.
3. **Customization:** Tailor the integration to fit your specific requirements and workflow by defining the data you want to receive.
4. **Enhanced Visibility:** Gain deeper insights into your external attack surface by integrating our data into your central security dashboards and reporting systems.

How to Set Up Webhook Integration:

Setting up webhook integration with our platform is straightforward:

1. **Access Webhook Settings:** Log in to your account and navigate to the "Integration" or "Webhook" section in your account settings.
2. **Create a Webhook:** Click on the "Create Webhook" or similar button to set up a new webhook integration.
3. **Configure Webhook Endpoint:** Provide the endpoint URL where you want our platform to send webhook payloads. You can also specify the HTTP method (e.g., POST) and any required authentication or headers.
4. **Select Events:** Choose the specific events or triggers you want to receive notifications for. These may include new vulnerabilities, scan completions, or other relevant events.
5. **Test and Save:** Test the webhook integration to ensure it's functioning correctly. Once validated, save the configuration.
6. **Customize Payload:** If necessary, customize the webhook payload format to align with your endpoint's requirements.
7. **Enable and Monitor:** Activate the webhook integration, and monitor incoming webhook data to ensure it aligns with your expectations.

Security Considerations:

When setting up webhook integrations, it's important to consider security best practices:

- Use secure and authenticated endpoints to protect data in transit.
- Implement proper access controls and authentication mechanisms to verify incoming webhook requests.
- Regularly review and update your webhook configurations to maintain their relevance and security.

Our webhook integration is designed to enhance your security operations by providing real-time insights and automating responses to potential threats. By connecting our platform with your existing tools and workflows, you can ensure a proactive and streamlined approach to managing your external attack surface.

If you have any questions or need assistance with setting up webhook integration, please refer to our detailed documentation or reach out to our support team for guidance.

Best Practices

ReConfirm's Recommended Scanning Options:

For optimal and swift results, ReConfirm advises the following settings:

- Retag found subdomains (if scanned previously).
- Enable Deep Search for Subdomains (Slow).
- Vulnerability Scan on Subdomains.
- SSL Scan on Subdomains.
- Limit to the top 100 ports.

FAQs and Troubleshooting

General Questions

Q1: What is the purpose of the External Attack Surface Management platform?

- *A1:* The platform is designed to help organizations monitor, assess, and manage the security of their external attack surface. It provides insights into vulnerabilities, email security, similar domains, assets, data leaks, and more to enhance overall security posture.

Q2: Who can use the platform?

- *A2:* The platform is accessible to both administrators and users with different roles, including administrators, security engineers, and auditors. Administrators have comprehensive control over platform settings, while other users have specific permissions based on their roles.

User Documentation

Q3: Is there user documentation available for the platform?

- *A3:* Yes, comprehensive user documentation is provided to guide users through platform functionalities, from navigation and scanning to accessing scan results and managing vulnerabilities.

Q4: How can I access the user documentation?

- *A4:* You can access the user documentation from within the platform. Simply refer to the "Help Center" in the User Details section of the menu for detailed guides and information.

User Interface and Navigation

Q5: How is the user interface structured?

- *A5:* The user interface is organized into sections, including User Details, User Interface, Administration Interface (for administrators), Scanning, and Scanned Domains, to provide easy access to relevant features.

Q6: Can I customize the platform's appearance?

- *A6:* Yes, users have the option to customize the theme and look of the platform using the settings wheel located on the middle right of each page.

Account Management

Q7: Who can perform account management tasks?

- *A7:* Account management functions are exclusive to administrators. They can manage user accounts, roles, permissions, and more.

Q8: What can administrators do in the Account Management interface?

- *A8:* Administrators can view all accounts, search for users, see recent logins, edit user details, delete users, reset user credentials, and manage user roles and permissions.

Q9: What are the user roles available on the platform?

- *A9:* User roles include Administrator (full admin rights), Security Engineer (permissions for scans and security tasks), and Auditor (view-only access).

Organizational View

Q10: What is the Organizational View feature?

- *A10:* Organizational View allows administrators to create and manage a structured hierarchy of organizations and assign domains to them, simplifying access and management.

Q11: How can users access the Organizational View?

- *A11:* Users can access the Organizational View by clicking on the eye icon next to their username and selecting organizations and domains to view.

Scan Results

Q12: What are Scan Results?

- *A12:* Scan Results provide detailed insights into the security status of scanned domains, including Email Security, Vulnerabilities, Similar Domains, Assets, Data Leaks, Subdomains, SSL/TLS Information, and the ability to Compare Findings.

Q13: Can vulnerabilities be filtered on the Vulnerabilities page?

- *A13:* Yes, vulnerabilities can be filtered based on (sub)domain, severity, text search, and user-defined tags, making it easier to manage and prioritize vulnerabilities.

Q14: How can I share vulnerability data with others?

- *A14:* You can email specific vulnerabilities as attachments or export vulnerabilities in TXT, CSV, or XML formats directly from the platform.

Q15: Can I export other types of data from the platform?

- *A15:* Yes, you can export Similar Domains, Subdomains, Subdomains - Inactive, and SSL/TLS findings in CSV files for data sharing and analysis.

Q16: Are there additional features available for Subdomains?

- *A16:* Yes, you can create and add custom tags to subdomains, rescan selected subdomains, manually enter subdomains, and export subdomains in CSV format.

Miscellaneous

Q17: What is Two-Factor Authentication (2FA) in account management?

- *A17:* 2FA adds an extra layer of security to user accounts. It can be configured and reset by administrators, providing an added level of protection.

Q18: How do I reset credentials for a user with 2FA enabled?

- *A18:* Administrators can reset credentials for users with 2FA. Upon resetting the 2FA configuration is removed. The system generates a temporary password, which must be sent securely to the user. The password is valid for 12 hours, and users are prompted to create a new password upon login. After logging in an user needs to reregister the 2FA.

Q19: Can I compare findings from different scans?

- *A19:* Yes, the Compare Findings page allows you to track progress and identify new findings or resolved issues between two or more scans.

Q20: Can I stop a running scan?

- A20: Yes, Administrators and Security Engineers can stop a running scan by initiating a Force Reset of the platform, which is available from the User Management menu.

Glossary of Terms

Dashboard: The main user interface of ReConfirm where users can manage and monitor their scans.

Subdomain: A subset of the main domain, representing a specific area or service, e.g., `blog.example.com` .

Excluded Subdomains: Specific subdomains that a user chooses not to scan.

Deep Search for Subdomains: An extensive search method that tries to uncover more subdomains associated with the main domain. It's a more time-consuming method due to its thoroughness.

Vulnerability Scan: A type of scan focused on identifying security weaknesses in a domain or subdomain.

SSL Scan: A scan that inspects the Secure Socket Layer (SSL) configurations of a domain or subdomain for potential issues or vulnerabilities.

Suffix Scan: A scan focused on specific endpoints or paths within a domain or subdomain.

Suffix Configuration Thoroughness Level: Defines the depth and detail of the suffix scan. It ranges from "Quick" (most common vulnerabilities) to "Extremely Deep" (vast range of potential vulnerabilities).

Port: A communication endpoint in computer networking. Different services run on different port numbers.

Port Scanning: The process of checking a range of port numbers on a host to identify open ports and their associated services.

Endpoints: Specific URLs or paths within a domain or subdomain that can be accessed by users or services.

Webhook: A method used to provide real-time information to other applications.

Feedback and Suggestions

At ReConfirm, we value your feedback and actively encourage you to share your thoughts, ideas, and suggestions with us. We believe that your input is invaluable in helping us improve our External Attack Surface Management platform. Our commitment to providing you with the best possible experience means that we take your feedback seriously and use it to shape the future of our platform.

Why Your Feedback Matters:

1. **Continuous Improvement:** Your feedback fuels our ongoing efforts to enhance the platform's features, usability, and overall performance. We rely on your insights to identify areas for improvement and prioritize updates that align with your needs.
2. **Enhanced User Experience:** We strive to create a user-centric platform, and your feedback plays a pivotal role in making it more intuitive, efficient, and effective for all users.
3. **Tailored Solutions:** Your specific use cases and challenges are important to us. By sharing your feedback, you help us understand your unique requirements and develop tailored solutions that address your organization's security needs.

How to Provide Feedback:

We've made it easy for you to share your thoughts and suggestions with us:

1. **User Feedback Form:** You can use our user feedback form, know as the "Report a Bug" button, within the platform to submit your comments, ideas, or feature requests. Simply navigate to the "Report a Bug" section by clicking on your Username in the left sidebar to get started.

2. **Email:** Feel free to reach out to our support team at support@reconfirm.nl with your feedback or suggestions. We'll ensure your message is routed to the appropriate teams for consideration.
3. **Webinars and Events:** Stay tuned for webinars and events where you can interact with our team directly, ask questions, and provide feedback in real-time.

What to Include in Your Feedback:

When providing feedback, consider including the following details to help us better understand your perspective:

- **Description:** Clearly describe the issue or suggestion.
- **Use Case:** Explain how this impacts your workflow or security objectives.
- **Relevance:** Discuss why you believe this is important or beneficial.
- **Priority:** Indicate the urgency or importance of your feedback.

Remember, your feedback is anonymous by default, but you're welcome to provide contact information if you'd like a follow-up discussion.

We greatly appreciate your contribution to making our platform the best it can be. Together, we can continue to enhance security, streamline processes, and adapt to the evolving threat landscape.

Thank you for being a valued part of the ReConfirm community!

Secure Software Development Lifecycle (SSDL) Statement

At ReConfirm, we are committed to integrating security into every phase of our Software Development Lifecycle (SDLC). Our Secure Software Development Lifecycle (SSDL) approach is designed to identify, mitigate, and address security risks from the initial stages of design and development through to deployment and maintenance. The goal is to deliver secure, reliable, and compliant software that meets the highest security standards.

Key Principles of Our SSDL:

1. **Security by Design:** We embed security requirements from the outset by incorporating security-focused design principles and threat modeling in the architecture and design phases. Security requirements are treated as first-class citizens alongside functional requirements.
2. **Risk Assessment and Threat Modeling:** Before development begins, we conduct risk assessments and threat modeling exercises to identify potential vulnerabilities and attack vectors. This allows us to proactively address risks early in the lifecycle.
3. **Security Training and Awareness:** All developers, testers, and key stakeholders are provided with continuous security training to stay up to date with evolving threats, best practices, and secure coding standards.
4. **Secure Coding Practices:** Our development teams follow secure coding guidelines and industry standards such as OWASP and CWE. We ensure that code reviews include a focus on identifying and mitigating security vulnerabilities.
5. **Automated Security Testing:** Security testing is embedded in our CI/CD pipeline, incorporating static and dynamic analysis, dependency scanning, and automated security testing tools like SAST, DAST, and IAST to detect and fix vulnerabilities early.
6. **Vulnerability Management:** We maintain a robust vulnerability management process that includes regular scans, monitoring, and patching of software dependencies. We also integrate automated vulnerability detection tools into our testing workflows.
7. **Continuous Monitoring and Incident Response:** After deployment, we continuously monitor for potential security threats and vulnerabilities, ensuring rapid detection and response to any incidents. A dedicated security team manages this process, coordinating remediation efforts as needed.

8. **Compliance and Governance:** Our SSDL aligns with industry regulations, standards, and best practices such as ISO 27001, GDPR. We also conduct regular security audits and maintain documentation to ensure full compliance.
9. **Third-Party Security Assessments:** We regularly engage external security experts to perform penetration testing and code reviews to validate the security of our applications.
10. **Post-Release Review and Maintenance:** We ensure that security is maintained even after the release through continuous patching, updates, and security assessments. Any vulnerabilities discovered post-release are handled according to our incident response policies.

By adhering to the SSDL, we aim to continuously improve the security, reliability, and quality of our software solutions, protecting both our customers and stakeholders from potential security threats.