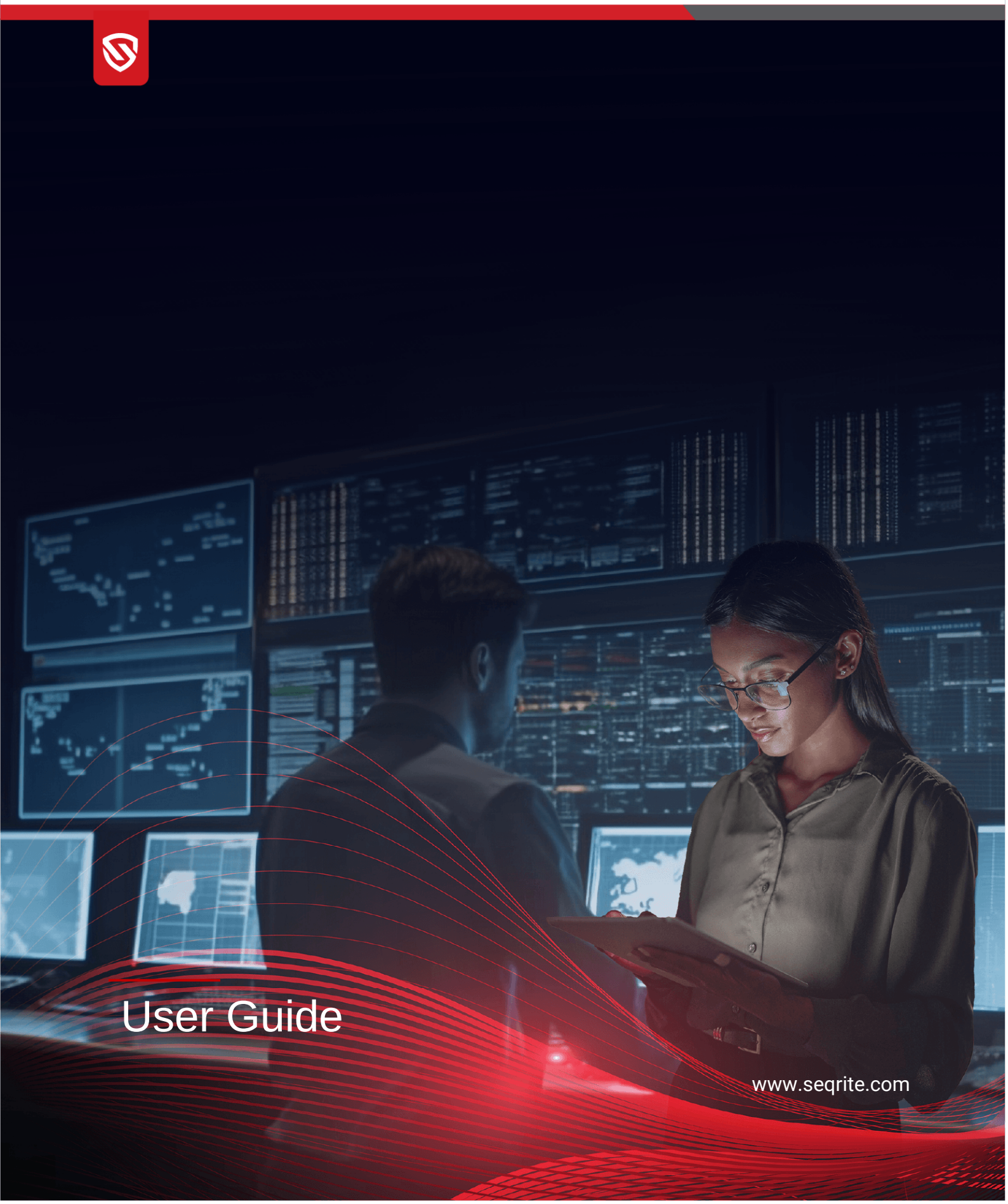
Seqrite Digital Risk Protection Services (DRPS)

SEQRITE



User Guide

www.seqrite.com

Copyright and License Information

Trademarks

Seqrite Digital Risk Protection Services is a trademark of Quick Heal Technologies Limited and its licensors, if any.

License Terms

Access to and use of Seqrite Threat Intel is subject to end-user's acceptance of the Seqrite Master End-User License Agreement. The license terms can be found at www.seqrite.com/eula.

Contents

Introduction

Seqrite DRPS is a brand protection platform developed by Seqrite to help businesses defend themselves against a wide range of online threats, safeguard their reputation, and protect critical digital assets. Seqrite DRPS combines cutting-edge technology, comprehensive threat intelligence, expert legal support, and proven crisis management methods into a single, unified solution for modern brand safety and security.

In today's fast-moving digital environment, where cyber threats, brand impersonation, and intellectual property violations are increasingly common, Seqrite DRPS empowers organizations with a robust and proactive way to maintain customer trust, avoid financial losses, and ensure regulatory compliance. With continuous digital monitoring, real-time alerts, and rapid incident response capabilities, Seqrite DRPS enables brands of all sizes to manage reputational risk and protect their digital presence more effectively than ever before.

On-Boarding Process

The user onboarding process for Seqrite DRPS is formally initiated upon receipt of a valid Purchase Order (PO) from the client. This PO serves as the contractual agreement to activate Seqrite DRPS services in accordance with the selected subscription plan and any associated add-ons.

- PO Validation: The received Purchase Order is carefully verified against the approved proposal and contractual terms to ensure alignment and accuracy.
- Acknowledgment: An official confirmation email is promptly sent to the client, clearly outlining the next steps, critical timelines, and expectations during the onboarding journey.
- Plan Allocation: The client's subscribed plan whether Essential, Professional, Enterprise, and any additional service packs or credits are confirmed and prepared for activation.
- License Preparation: License entitlements are provisioned according to the number of covered assets, premium features, and monitoring modules specified in the client's plan.
- Internal Kick-off: A coordinated alignment of Seqrite DRPS delivery resources is performed, involving the Customer Success Manager (CSM), Threat Analyst, and where applicable, the War Team and Legal Team representatives to ensure seamless execution.

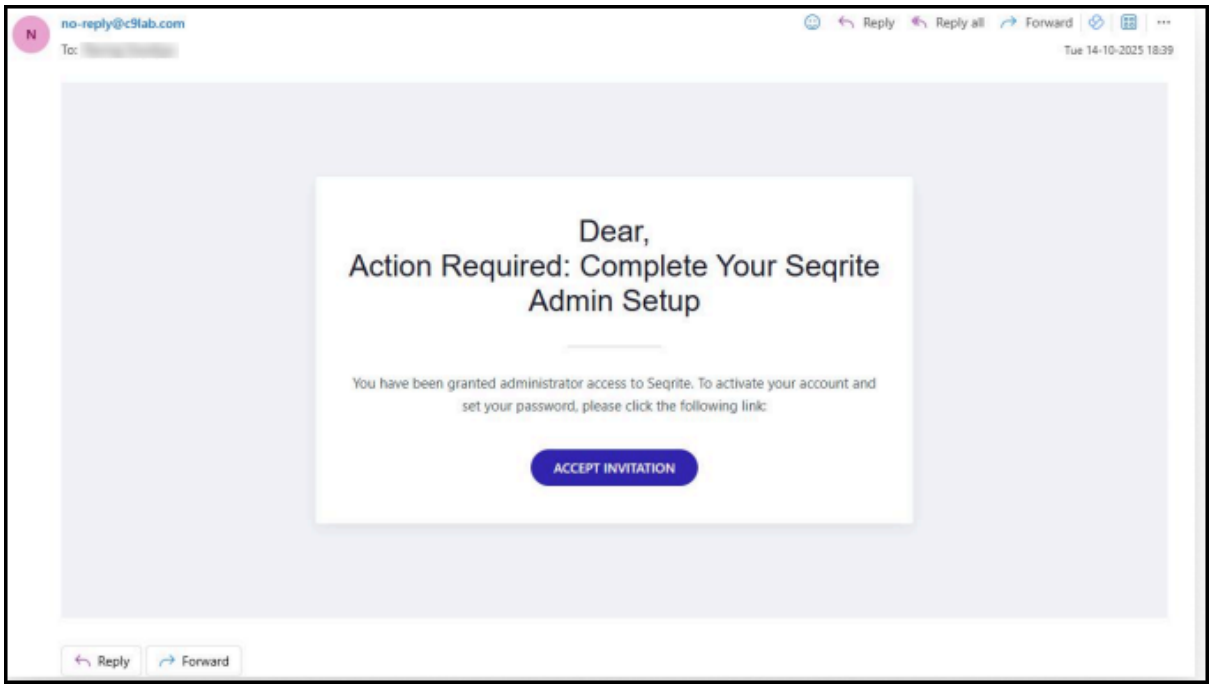
Account Creation and Authentication Process

The process of creating and authenticating an account involves three stages:

1. Receive and Accept Your Seqrite DRPS Admin Invitation
2. Setup Your New Password
3. Login to Your Seqrite Account

1. Receive and Accept Your Seqrite DRPS Admin Invitation

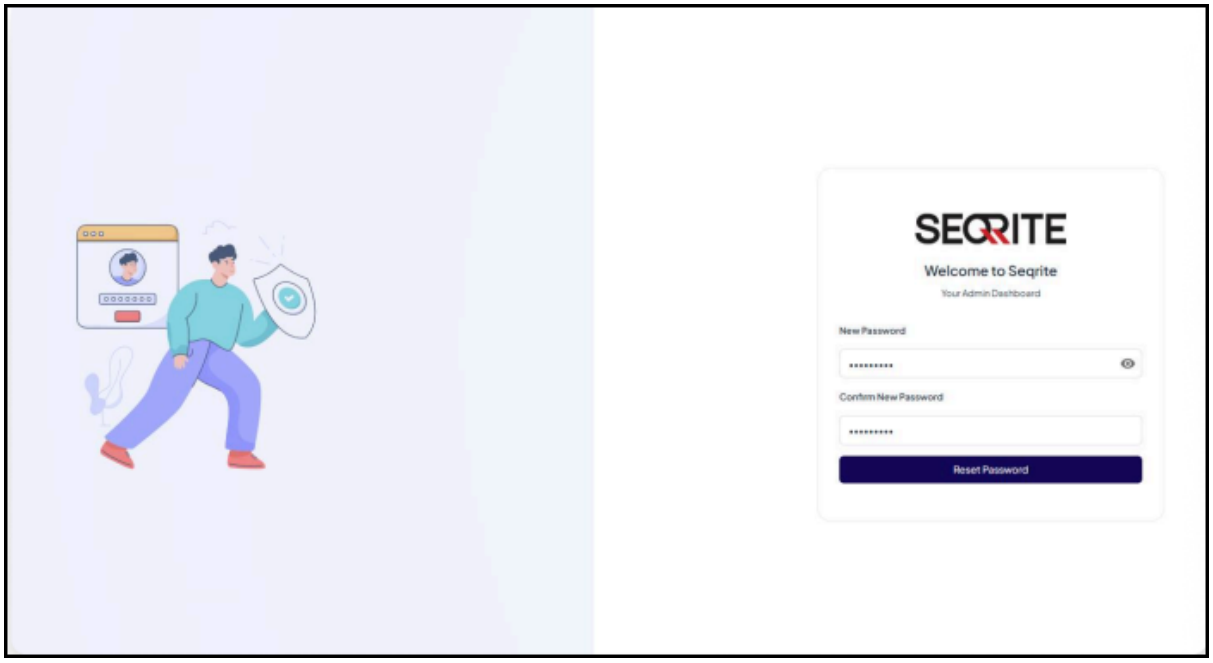
Once your onboarding process begins, you will receive an email title Action Required: Complete Your Seqrite Admin Setup. This email contains your administrative invitation, and next step is Account Activation.



- Click **Accept Invitation** in the email to start your account setup and proceed to create your password.

2. Setup Your New Password

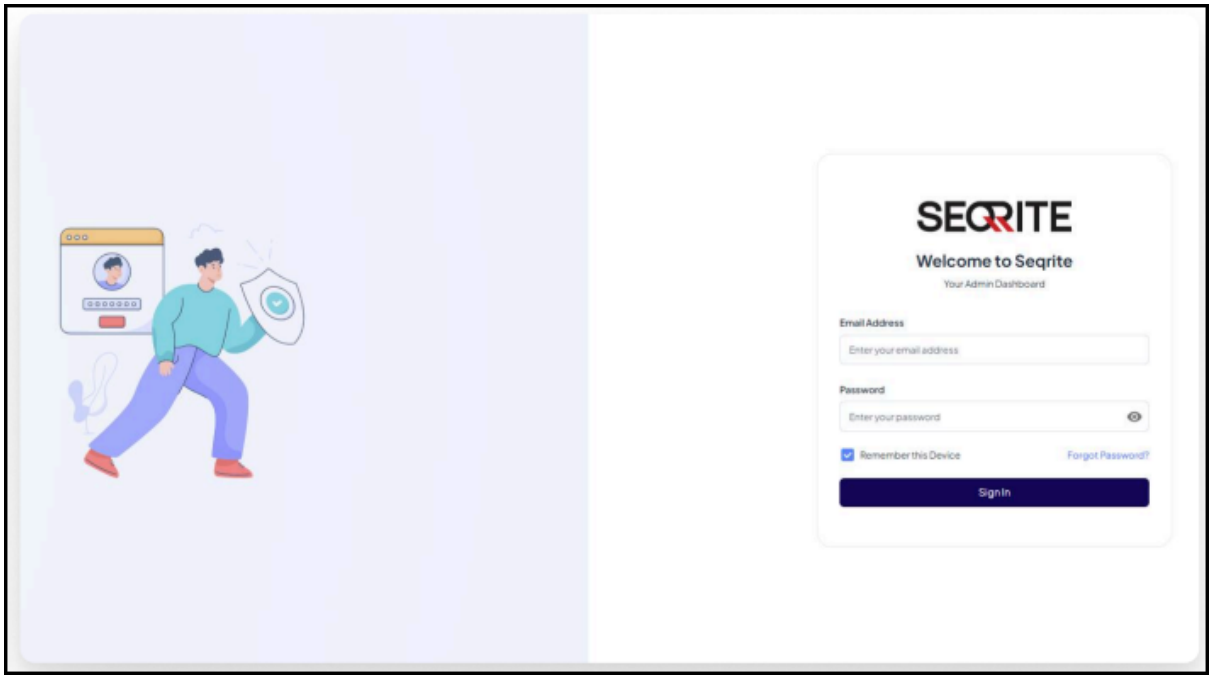
After clicking the invitation link, you will be redirected to the password creation page.



1. Enter a secure, new password for your Seqrite DRPS account.
2. Re-enter the password to confirm and safeguard your credentials.
3. Click **Reset Password** to complete the setup.

3. Login to Your Seqrite Account

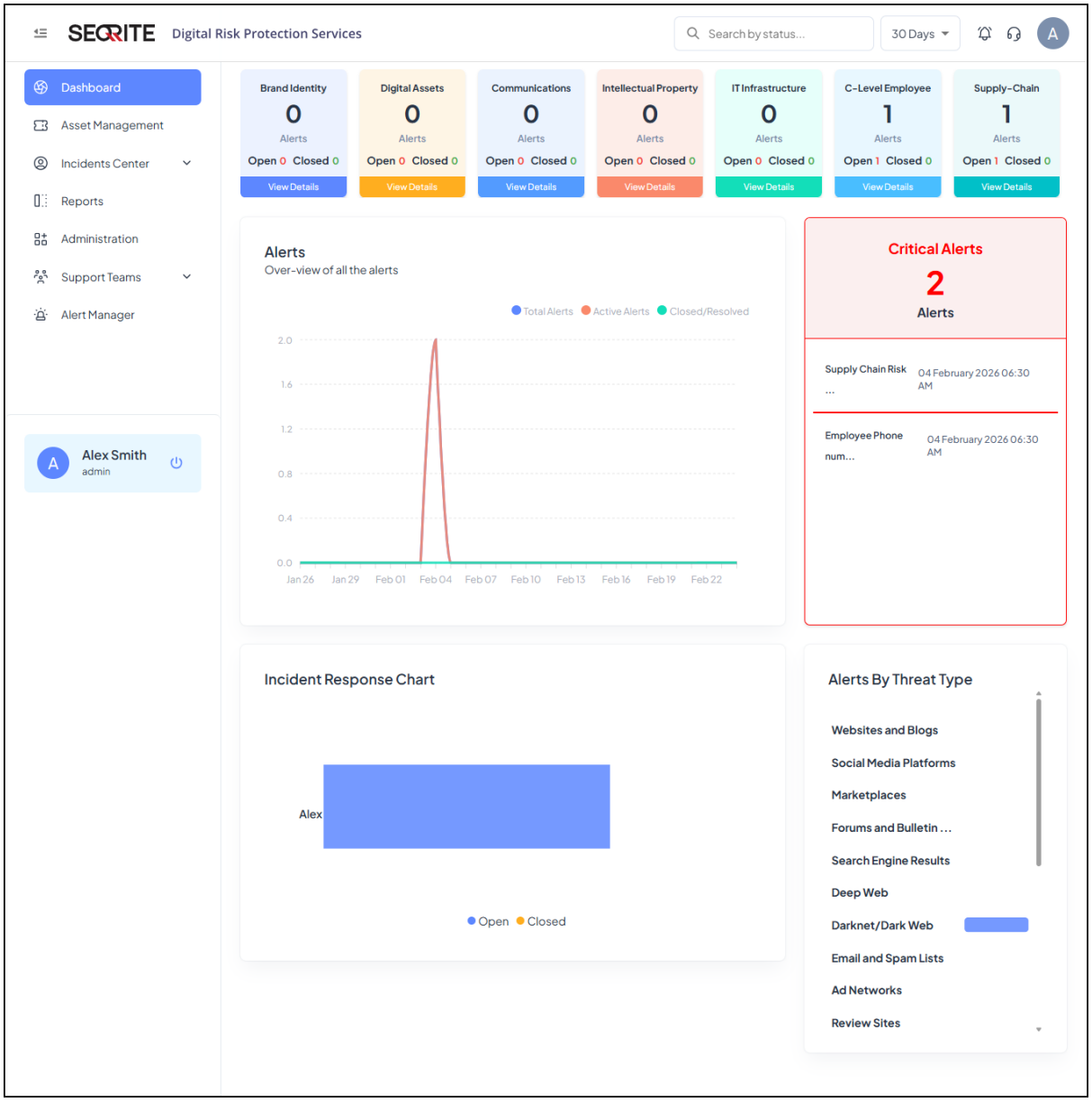
After setting your password, you will be directed to the Seqrite login screen.



1. Enter your registered email address and the new password you just created.
2. Click **Sign In** to access your Seqrite DRPS Admin Portal.

Dashboard

The Seqrite DRPS dashboard provides a unified overview of all monitored asset categories, displays real-time alert statistics and trends via interactive cards and graphs, and summarizes incident responses and alert sources for quick assessment of your organization's security posture.



Dashboard Metrics

Metric Name	Description
Alerts Count Widget	Alerts received from various verticals of DRPS, for example, Brand monitoring, Domain monitoring, Social Media

Metric Name	Description
	Monitoring (Communications), Intellectual property, EASM, Third Party Risks
Alerts	Trend of total alerts created vs closed and Open/active
Critical Alerts	Alerts with high severity for immediate attention and closure
Incidence Response Chart	Alert distribution across resources vs their closure
Alerts by Threat Type	Distribution of Alerts by Threat Type (For example, Dark web, EASM, Website and Blogs)

Global Search Bar

You can search the alert by status, alert name, alert name, alert name, alert name, alert ID, severity level, asset name, Email address, domain name, IP address, assignee name, and category along with the specified number of days.

Notifications

The upper-right section of the Seqrite DRPS console shows various types of notifications along with the following details:

- Description
- Incident Id
- Severity (Low, Medium, High, Critical)
- Incident details
- Source of alert
- Assigned to
- Alert status
- Evidence snapshot
- Affected assets

User Actions on Notifications

You can take required actions on notifications such as:

- **SOS** (Send urgent alerts for immediate assistance)
- **Take Down** (Request legal action to remove the threat)
- **Assign** (Assign alert to your team member)
- **General Support** (Ask our team for more details about this alert)

Change Notification/Alert Status

You can change the notification status to **Open** or **Report as false**.

Help and Support

Redirects you to Seqrite Technical Support for any assistance.

User Profile

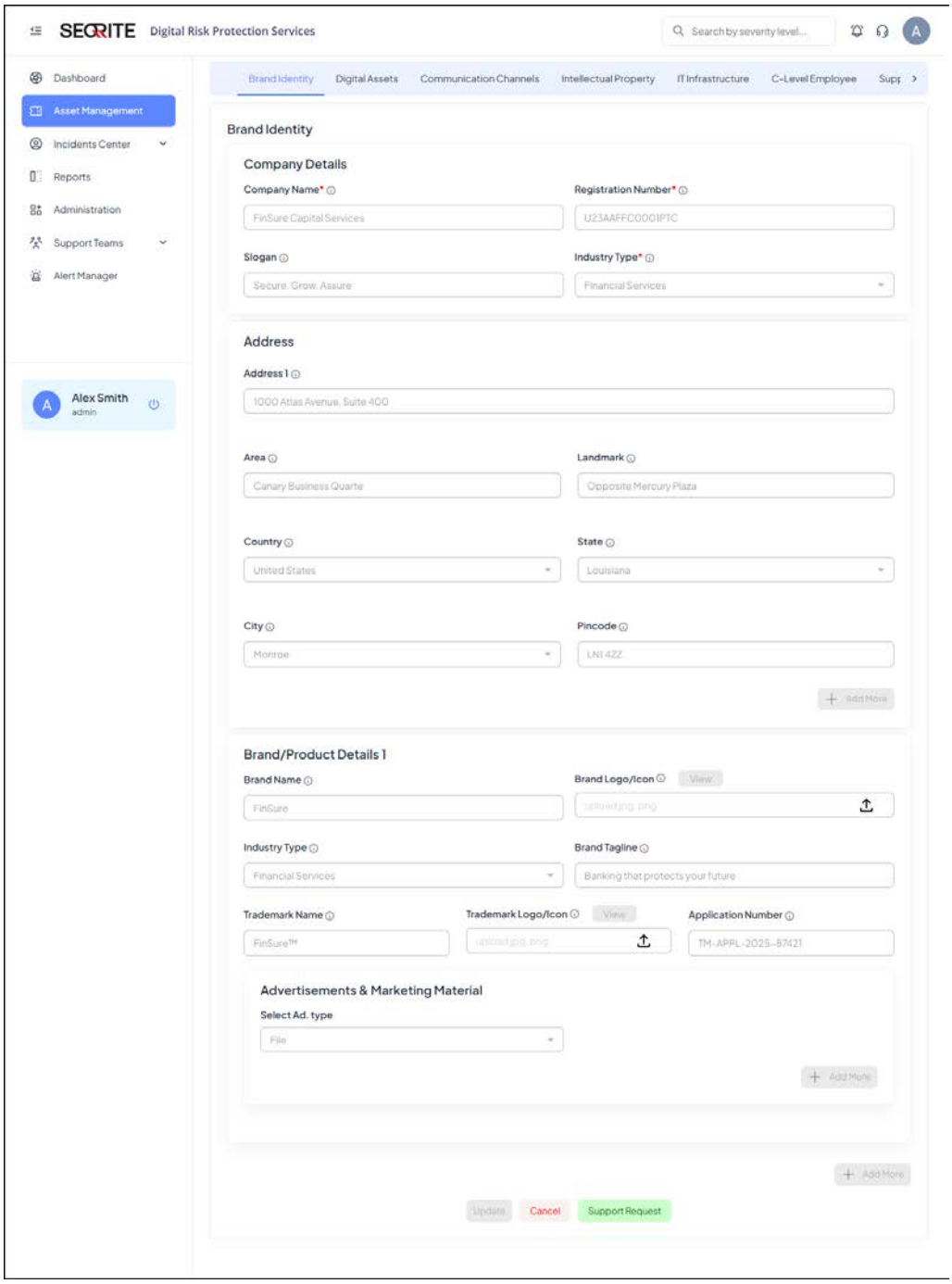
The User Profile section on the upper-right corner of the dashboard shows the name of the registered user.
When you click the logged-in username, the options are displayed:

- Role
- Email ID
- License Information: Shows your allocated license details such as, your plan type, covered assets, and feature activation status.
- Alert Normalize: This process will analyze and correlate alerts across all security categories using AI-powered normalization.
- Change Password
- Setup 2FA

Asset Management

In Asset Management, details of organization’s asset such as are domain name, URL,social media handles is captured.

Collecting detailed asset information ensures comprehensive monitoring for security and compliance. This process verifies that your organization legitimately owns or manages each asset, enabling proactive protection and risk mitigation.



Following asset details need to be collected from the organization to start monitoring:

1. **Brand Identity:** Includes company name, logos, trademarks, slogans, and marketing materials to protect brand reputation.

    - Organization Details such as Org Name, Registration number, Slogan, Industry they belong to, Address and other geo location details.
    - Additionally, we can add Brand / Product details, Logos of that product, Trademark details and Logo.

2. **Digital Assets:** Covers official websites, domains, subdomains, mobile apps, and digital media assets.

    - Organization main website URL, website colour scheme, website content
    - Application type, application URL
    - Owned brand domaim
    - Product/brand images, video URLs, application screenshot.

3. **Communication Channel:** Corporate emails, customer service numbers, SMS sender IDs, and social media accounts monitored for fraud or impersonation.

    - Official Email IDs
    - Phone numbers,
    - Sender IDs
    - Social Media Accounts
    - Chat Applications used within the organization like teams etc.

3. **Intellectual Property:** Patents, copyrights, trademarks, and trade secrets safeguarding your creative assets.

    - Patent Information
        - Patent Number
        - Brief summery of invention
    - Copyright Information
        - Title of Work
        - Registration Number
        - Short Description of Work

4. **IT Infrasructure**: Details about servers, operating systems, firewalls, firmware, and on-premises software crucial for cybersecurity.

    - Public facing server IP Information

    - Name
    - IP Address
    - Location

- Operating System
- Firewall and Firmware
- On Premises Software/Inventory
- Router and Switche

4. **C-Level Employee**: Records of top executives including contact details and photos to prevent impersonation attacks.

    - Full Name
    - Position/Title
    - Email
    - Phone Number
    - Location
    - Photo

5. **Supply Chain Management**: Information on vendors and partners, including their domains and contact details to detect third-party risks.

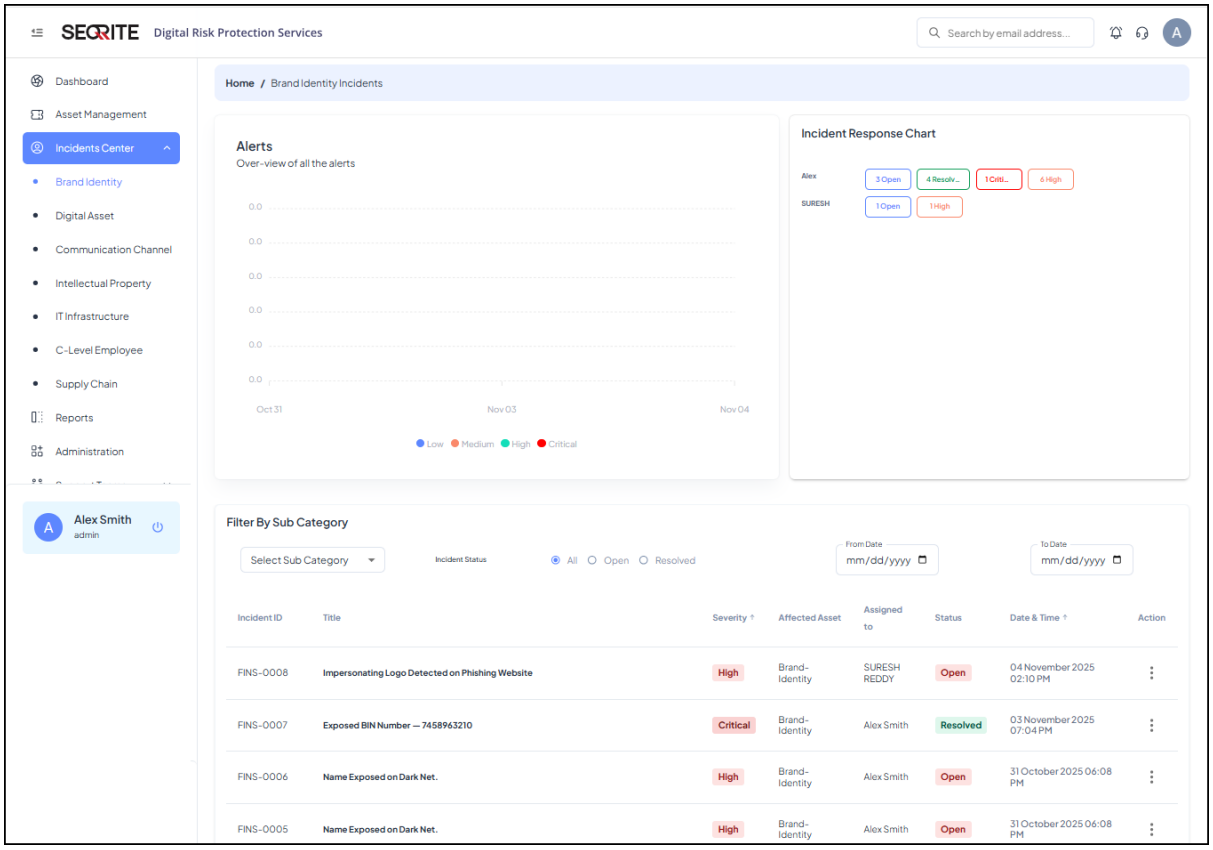
    - Vendor/Customer Name
    - Vendor's/Customer's Domain
    - Email
    - Phone Number

Note: After completing all asset information forms, allow up to 24 hours for the system to initialize monitoring and begin generating alerts. This initialization period ensures accurate threat detection and monitoring across all your registered assets.

Incident Center

The **Incident Center** is the central dashboard where detected digital threats are collected, organized, and managed.

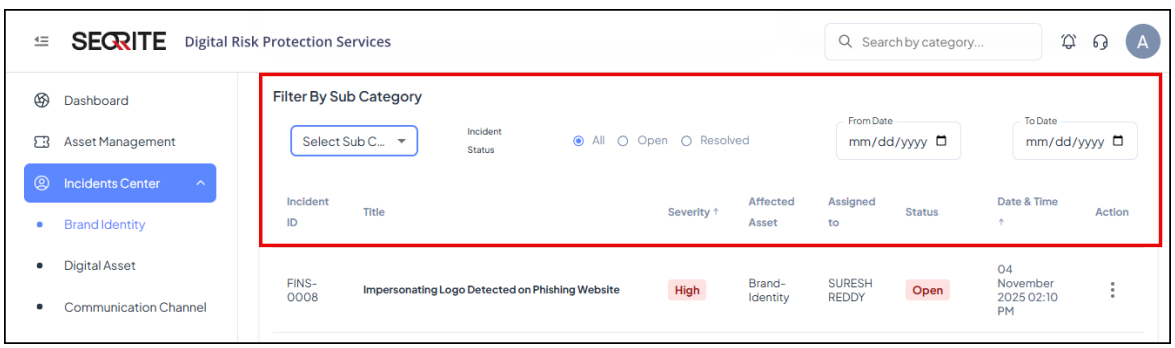
Incident Center gives a clear overview of all alerts in one place. It also includes an incident the Incident Response chart shows the number and severity of alerts assigned to each team member for efficient tracking and resolution.



It also gives a list of incidents along with details such as, incident ID, Title, Severity, Affected Asset, Assigned to, Status, and Date and Time.

Filtering Incident List

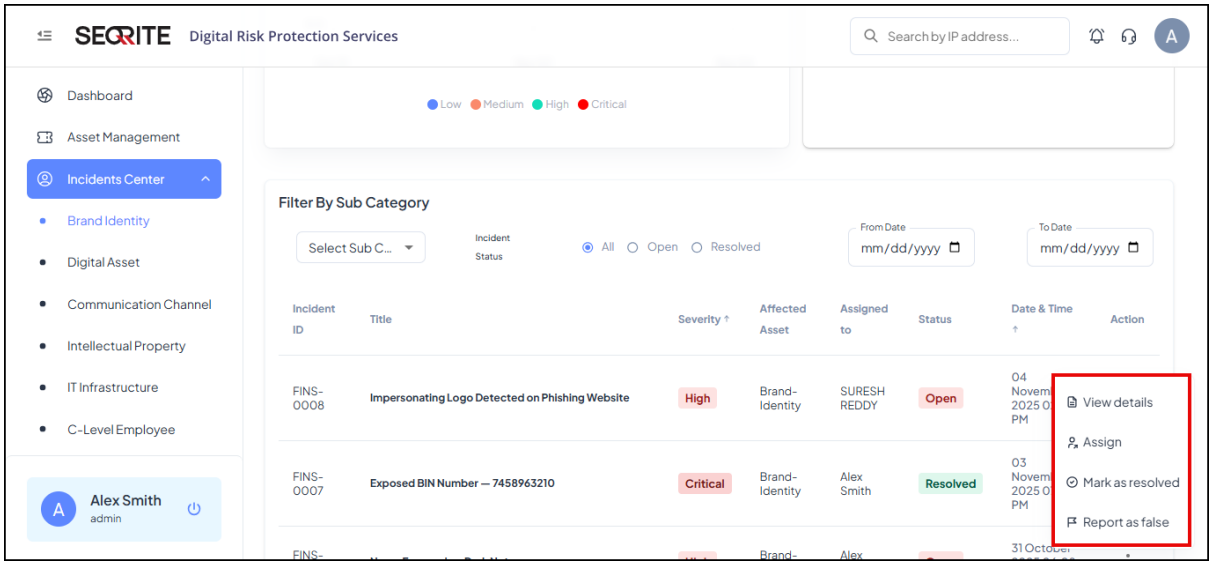
You can filter the incident list by category, subcategory such as Company, Address, Brand Details, Card Information, Incident Status (All, Open or Resolved), and by Date.



Viewing Incident Details

To view details of an incident, follow these steps:

1. After logging in to Seqrite DRPS, go to Incident Center.
2. Select the incident whose details you want to view and click ⋮ in **Action** column and then click **View details**.

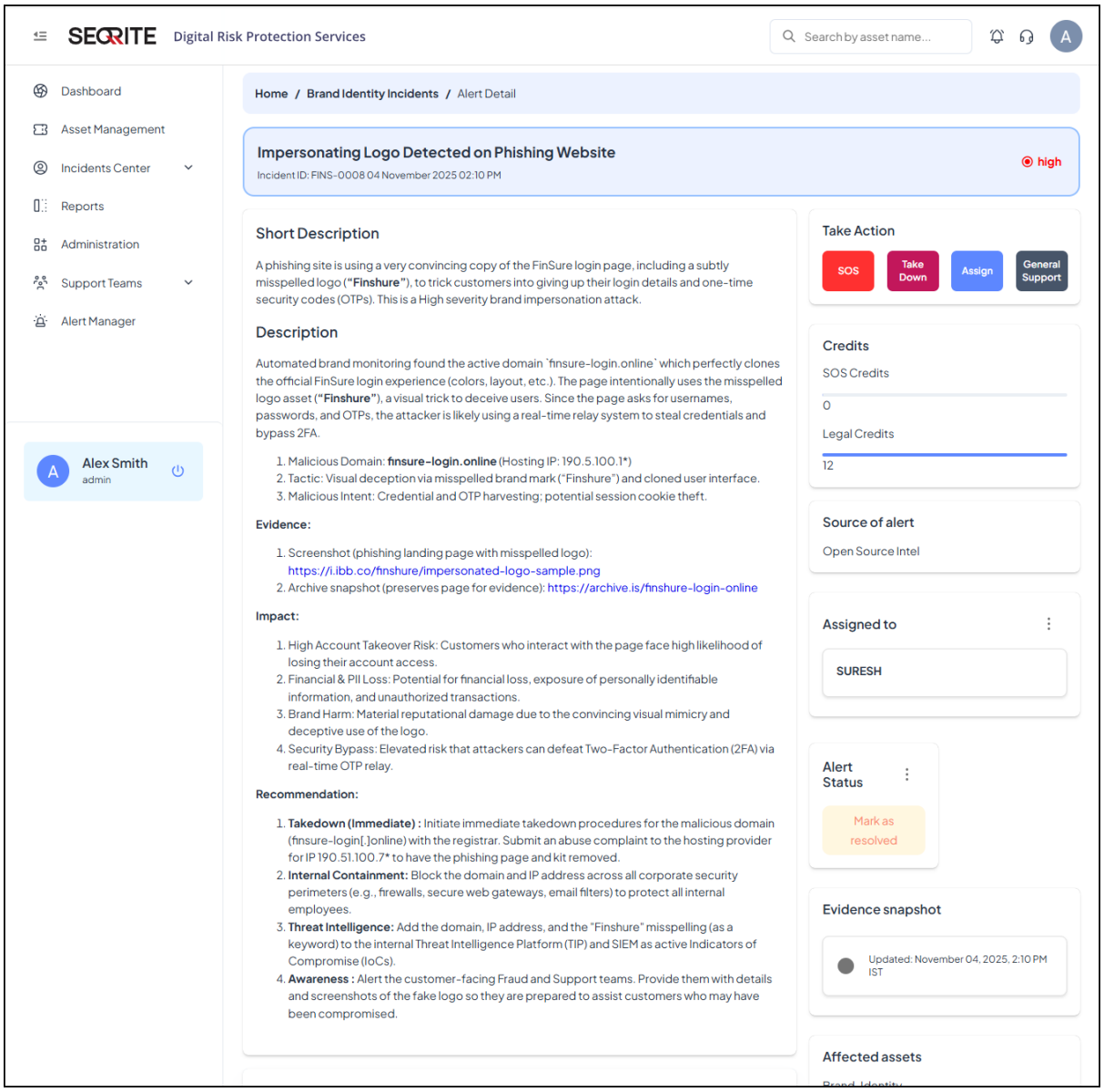


Incident detail page appears with following details:

- **Incident Description**: You can view full incident summary, impacted assets, and recommended actions.
- **Activity**: This section provides log of all incidents related actions including generation, assignments, status changes, team escalations. Gives track of from incident detection to resolution.
- **Take Action**: You can take actions such as:
    - **SOS**: For Immediate assistance and any kind of support required.
    - **Take Down**: To take down harmful and fraudulent content.
    - **Assign**: To assign alert to appropriate team members within the group to ensure prompt and efficient handling and resolution of incidents.
    - **General Support**: To ask more details about the incident to Seqrite team.
- **Credits**: SOS and Legal Credit show how many emergencies and legal actions are available.

  Note: Credit limits are defined based on the license type.
- **Source of Alert/Incident**: Shows where the incident originated.
- **Assigned To**: Shows incident is assigned to whom.
- **Alert Status**: Shows the status of alert that is, **Marked as resolved** or **Report as false.**
- **Evidence Snapshot**: Displays all the supporting images or documents collected for the incident.

- **Affected Assets**: Shows which company resource is being monitored or impacted by the incident.



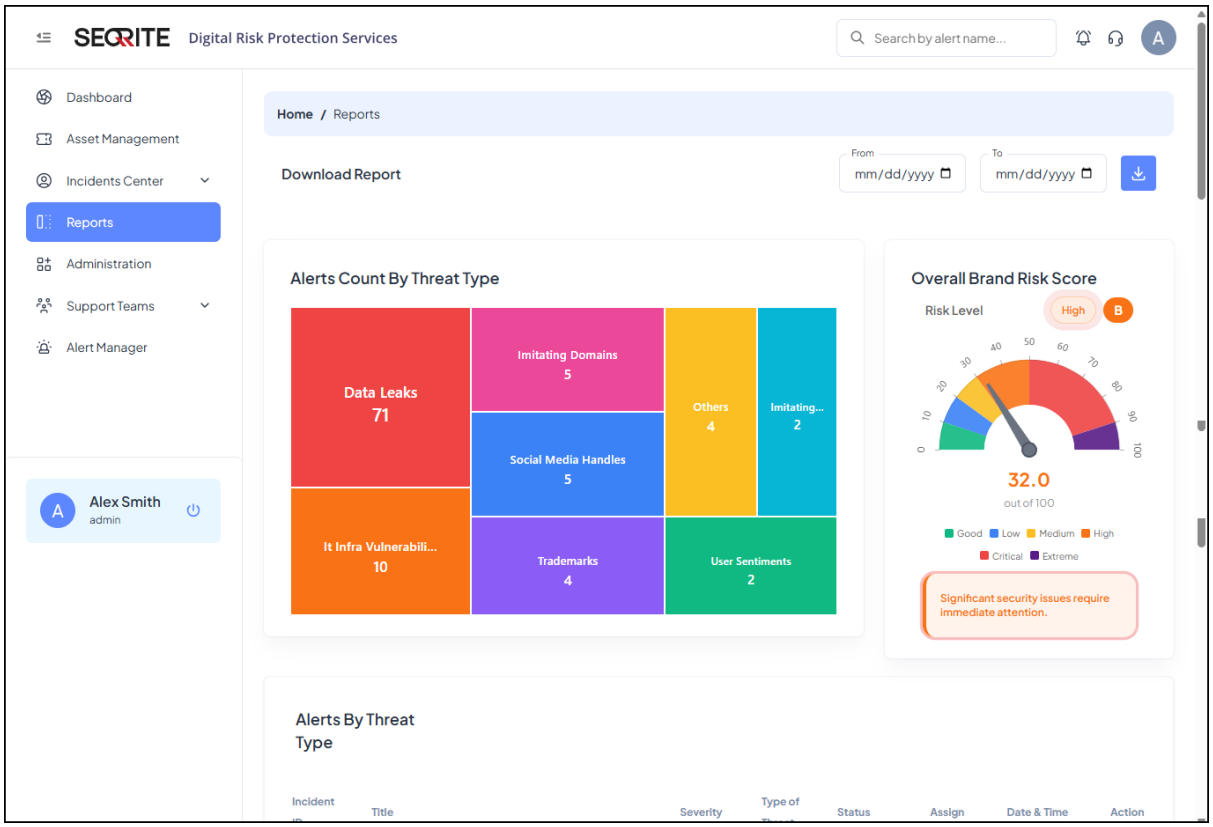
Alert Types Generated

Following DRPS alert types will be generated and shown on Portal:

Category	Use Case Description
Brand Identity	• Brand name misuse detection – Identifies unauthorized use of the brand name across the internet, including fake ads or promotions. • Trademark & Logo Infringement - Scans web, marketplaces, apps, and social platforms to detect unauthorized use of logos or brand visuals
Digital Assets (Domains, Web Presence)	• Domain abuse & lookalikes – Finds typo-squatted or impersonating domains designed to mislead users. • Domain expiry & SSL monitoring – Tracks certificate expiry and domain validity to avoid outages or security issues.
Communication Channels	• Monitoring of organizational emails & phone numbers – Alerts on exposure or misuse of official communication identifiers. • Fraudulent Support Number Detection – Searches all search engines for fake support numbers
Intellectual Property (IP Assets)	• Copyrighted content misuse – Detects illegal use of original content such as documents, images, software, or videos. • Patent Misuse Detection– Monitors patent metadata to identify unauthorized referencing or copying.
IT Infrastructure	• Server Misconfiguration Detection– Automatically identifies internet-facing servers and flags for any misconfigurations or Open Ports. • Vulnerability detection on exposed infra – Flags weaknesses such as open ports, outdated software, and misconfigurations.
C-Level Employee (VIP Monitoring)	• Credential leakage checks – Alerts when executive emails, passwords, or phone numbers appear in breaches.
Third-Party Risk Management	• Vendor reputation & exposure monitoring – Tracks cyber risks tied to key partners, suppliers, and outsourced teams.

Reports

Reports are assigned a unique score at the brand level, where a higher score indicates greater risk. You can retrieve a complete report for any given date, and the report will be delivered directly to your registered email address.



Download/Export Reports

To export reports, follow these steps:

1. After logging in to Seqrite DRPS, go to **Reports**.
2. Select a date range and click  .

The system downloads the report for the selected date range.

Administration

The **Administration** section displays a list of all sub-admins added to the system and allows you to manage them efficiently. Within this section, admin can add new sub-admins, edit their details, and control their status by activating or deactivating accounts.

Add Sub-Admin

To add sub admin, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Click **Add Sub-Admin.**
3. Enter first name, last name, and email.
4. Select **Read** and **Write** permission for each category and click **Add**.

Edit Sub-Admin

To edit the sub-admin details, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Select the sub-admin you want to edit and click **Edit**.
3. Edit the details and click **Submit**.

Activate/Deactivate the Sub-Admin

To activate or deactivate the Sub-Admin, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Select the sub-admin you want to activate/deactivate and click **Edit**.
3. Switch the **User Active or Inactive** toggle and click **Submit**.

Resend Invitation

If a sub-admin's application access invite has expired, the admin can resend the invite.
To resend the invitation, follow these steps:

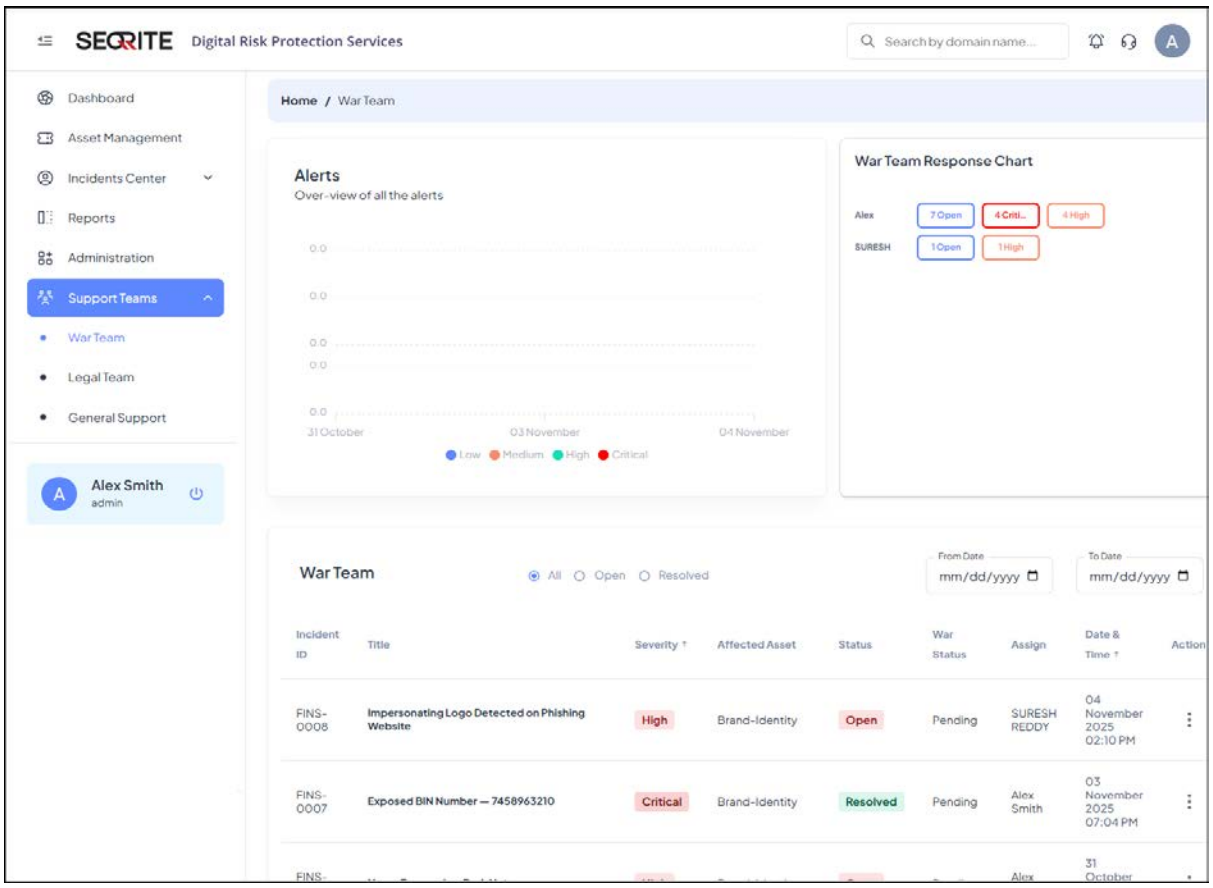
1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Select the sub-admin you want to resend the invitation and click **Resend Invitation**.
3. Switch the **User Active or Inactive** toggle and click **Submit**.

Support Team

The Support Team is divided into three groups—the War Team, the Legal Team, and General Support—each responsible for handling incidents in their own area. Each gives incident details such as, Incident IDs, title, severity, affected asset, status, assignee, date and time and incident response chart.

War Team

In the War Team, you can view all alerts assign for immediate action after an SOS is triggered, including critical communication and social media exposure, along with their status and available team response action.



Legal Team

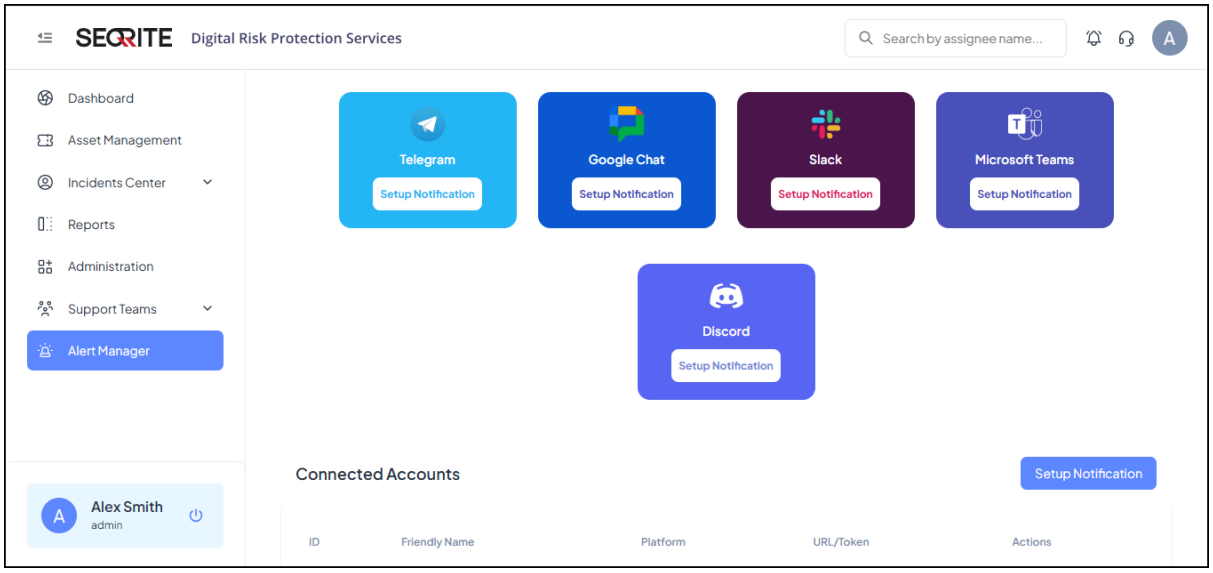
In the Legal Team, you can view and manage all alerts sent for takedown and legal review via the Take Down action. Track their legal status, access supporting documents, and monitor progress towards resolution.

General Support

Technical assistance provided by the team to address customer queries and issues.

Alert Manager

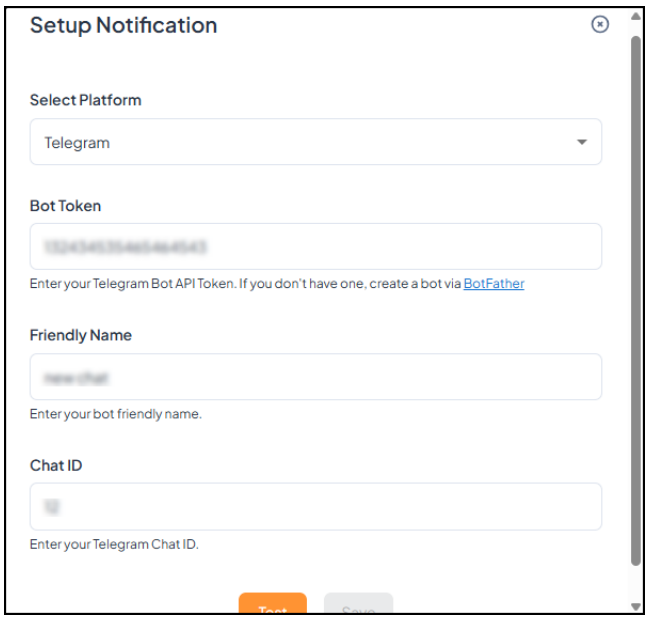
Seqrite DRPS also supports API integrations with chat applications like Microsoft Teams, Slack, Telegram, Google Chat, and Discord. You can set up custom notifications within these apps, allowing your teams to receive and respond to alerts directly in their preferred communication platform.



Setup Custom Notifications

To set up custom notifications with chat applications, follow these steps:

1. After logging in to Seqrite DRPS, go to **Alert Manager.**
2. Click the platform for which you want to set up custom notifications and click **Setup Notification**.
   The **Setup Notification** screen appears.



3. Select the platform, enter your BOT API token, enter name, chat ID.
4. Click **Test**, if successful, click **Save.**