

# Benutzerhandbuch

## ads-logs: Analyse von Audit Logs

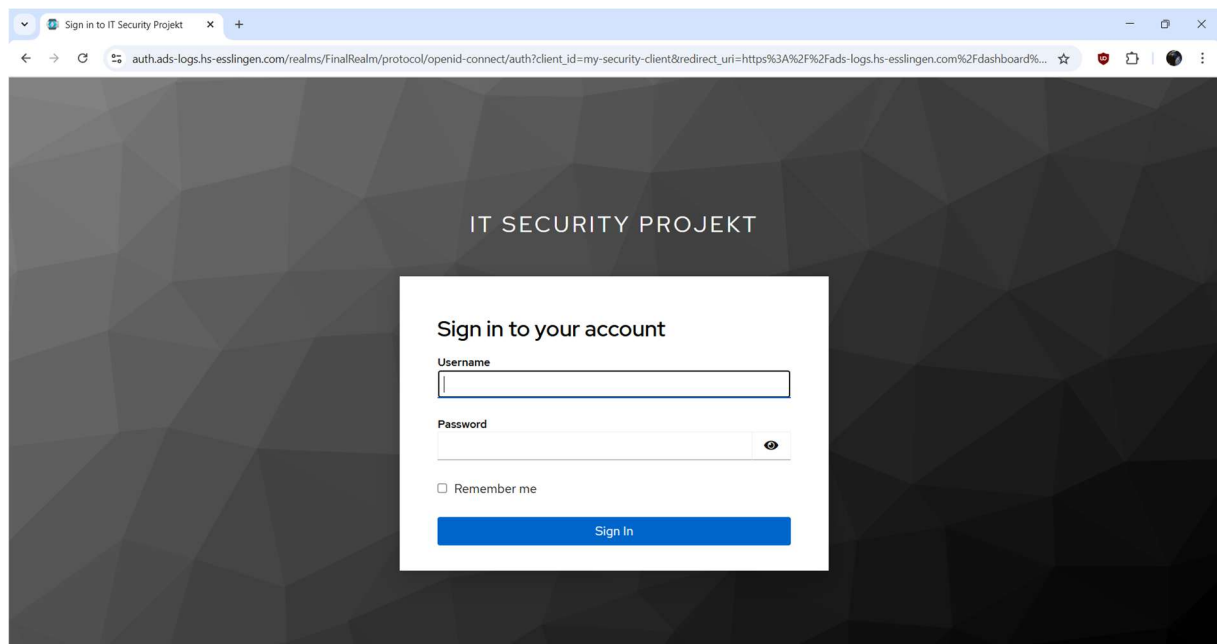
startup:

Führe die bashfile auf dem Server aus um das Programm auf dem Server zu starten

(standardmäßig deploy.sh)

Das Web-Dashboard ist nun unter der festgelegten Adresse erreichbar.

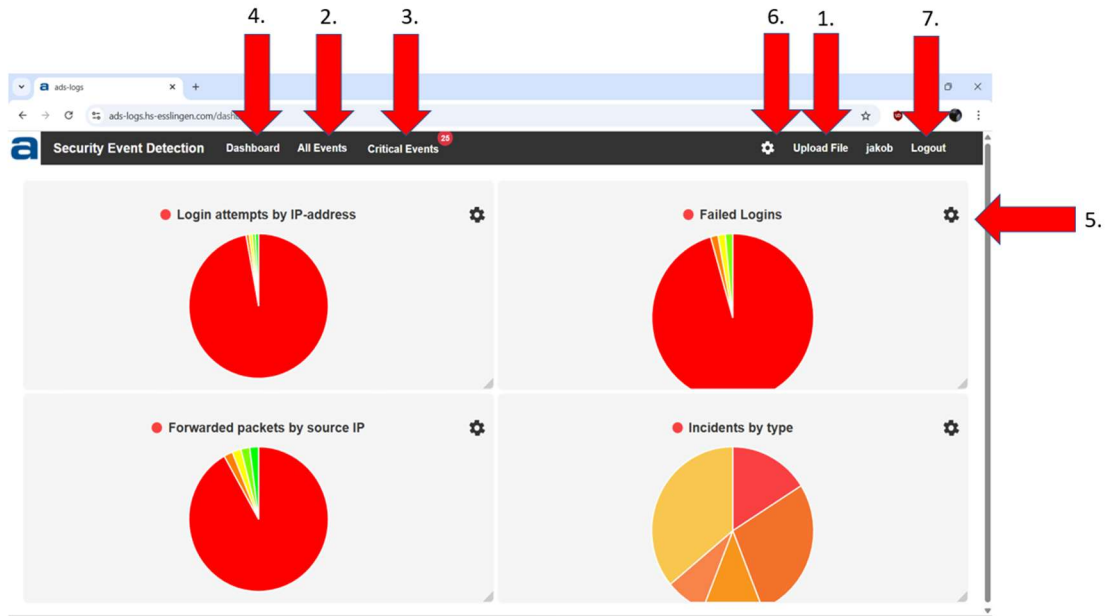
Du wirst auf die login-seite weitergeleitet



Die Benutzerverwaltung erfolgt über das Keycloak Admin Dashboard

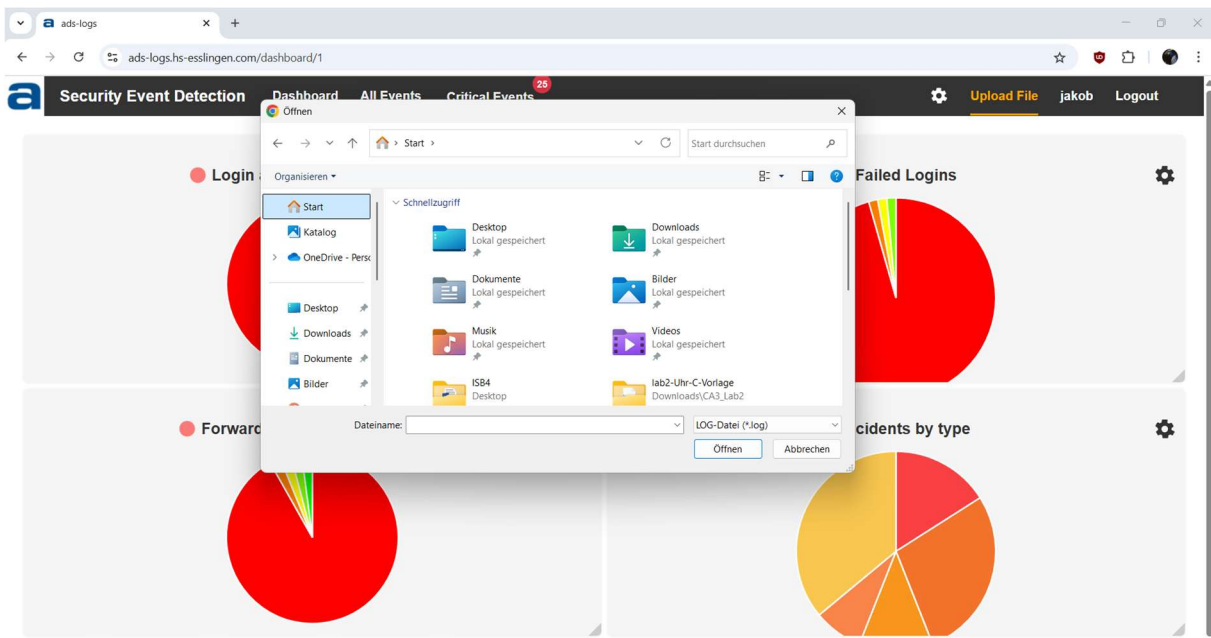
Solltest du dich das erste mal einloggen musst du eventuell Angaben zu deinem Benutzer ergänzen.

## Das Dashboard:



## Beschreibung der Buttons:

1. Fileupload: Hiermit kannst du deine Logfiles hochladen, der Button öffnet einen separaten Dialog zur Dateiauswahl



2. All Events: Der Button leitet dich auf eine Seite mit allen gefundenen Events, du kannst durch das Suchfeld und die Filter deine Ergebnisse einschränken.

Date	Event	Status	IPs	Description
05/24/2025 23:14:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 23:08:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 23:02:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:56:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:50:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:44:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:38:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:32:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:26:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:20:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:14:26	login	Warning	192.168.0.40	Status: fail
05/24/2025 22:08:26	login	Warning	192.168.0.40	Status: fail

3. Critical Events: Der Button leitet dich auf eine Seite mit allen Events die den Status kritisch haben, insbesondere generierte Incidents.

Date	Event	Status	IPs	Description
05/24/2025 21:38:54	incident	Critical	192.168.0.40	Type: bruteforce   Source IP: 192.168.0.40   Reason: 29 failed attempts in 2 minutes
05/14/2025 20:18:30	incident	Critical	172.16.0.2 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.2   Reason: 570 packets in 30 seconds
05/14/2025 20:15:30	incident	Critical	192.168.0.88	Type: ddos   Reason: 5 sources sent >= 10 packets in 30 seconds
05/14/2025 20:15:30	incident	Critical	172.16.0.2 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.2   Reason: 684 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	192.168.1.77	Type: ddos   Reason: 5 sources sent a total of 20 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.1.55	Type: ddos   Reason: 10 sources sent a total of 20 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	10.0.0.1 192.168.0.100	Type: DoS Attack   Source IP: 10.0.0.1   Reason: 24 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.1 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.1   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.3 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.3   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.4 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.4   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.5 192.168.0.88	Type: DoS Attack   Source IP: 172.16.0.5   Reason: 28 packets in 30 seconds
03/27/2025 11:50:35	incident	Critical	192.168.0.37	Type: concurrentLogin   Source IP: 192.168.0.37   Reason: user logged in again without previous logout

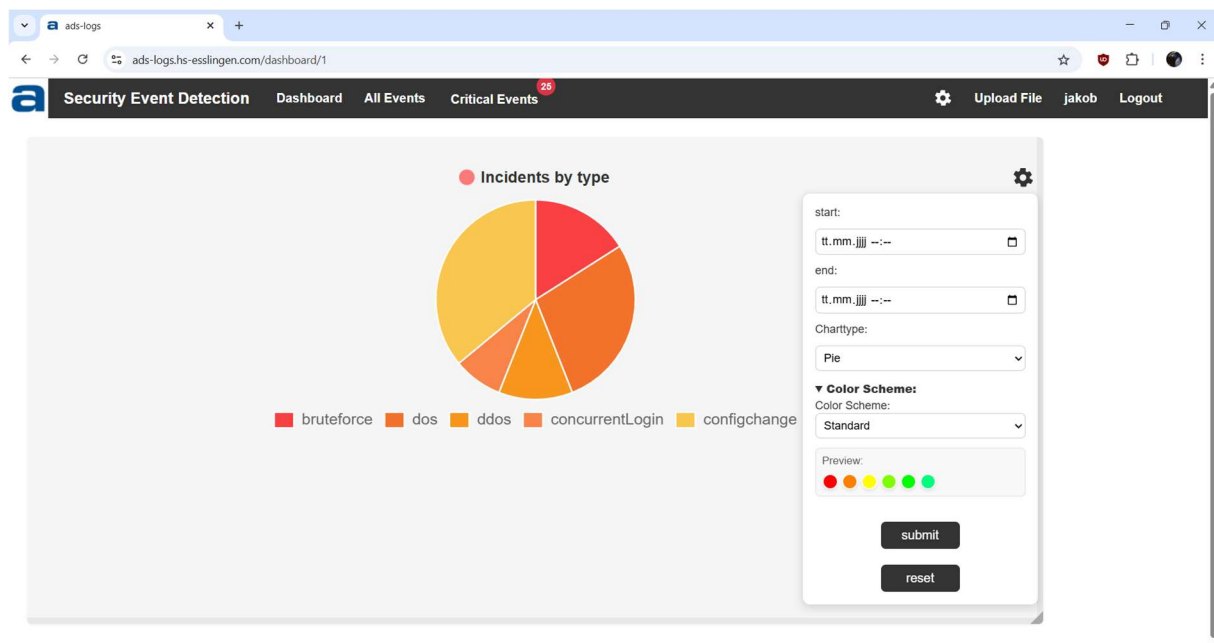
4. Der Dashboard-Button bringt dich immer wieder auf die Hauptseite zurück.

Wenn du über diesen Button hoverst erscheint ein Dropdownmenü, über das du deine Dashboards verwalten kannst, du kannst 3 Presets speichern und in jedem auswählen welche Diagramme angezeigt werden sollen

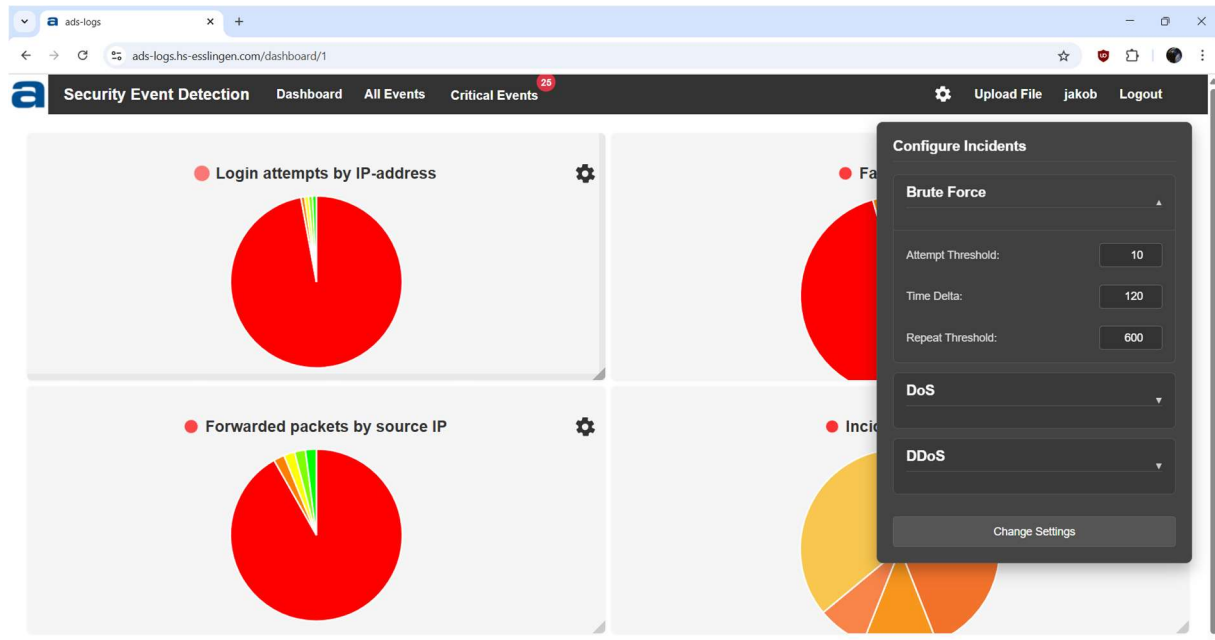
The screenshot shows the 'Security Event Detection' dashboard. The top navigation bar includes 'Dashboard', 'All Events', and 'Critical Events' (with a red badge showing 28 events). A search bar is on the left. A dropdown menu is open over the 'Dashboard' button, showing 'Dashboard 1', 'Dashboard 2', and 'Dashboard 3'. A second dropdown menu is open over the 'Dashboard 1' option, showing a list of event types with checkboxes: 'Attempted Logins', 'Failed Logins', 'Forwarded Packets', 'Incidents', 'DOS Packets', 'DDOS Packets', 'Configuration Changes (table)', and 'Configuration Changes'. The main table lists events with columns: Date, Event, Status, IPs, and Description. The events are all marked as 'Critical' and include details like source IP and reason.

Date	Event	Status	IPs	Description
05/24/2025 21:38:54	incident	Critical	192.168.0.37	Type: concurrentLogin   Source IP: 192.168.0.37   Reason: user loaded in again without previous logout
05/14/2025 20:18:30	incident	Critical	172.16.0.2	Type: DoS Attack   Source IP: 172.16.0.2   Reason: 570 packets in 30 seconds
05/14/2025 20:15:30	incident	Critical	192.168.0.1	Type: ddos   Reason: 5 sources sent >= 10 packets in 30 seconds
05/14/2025 20:15:30	incident	Critical	172.16.0.2	Type: DoS Attack   Source IP: 172.16.0.2   Reason: 684 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	192.168.0.1	Type: ddos   Reason: 5 sources sent a total of 20 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.1.55	Type: ddos   Reason: 10 sources sent a total of 20 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	10.0.0.1	Type: DoS Attack   Source IP: 10.0.0.1   Reason: 24 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.1	Type: DoS Attack   Source IP: 172.16.0.1   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.3	Type: DoS Attack   Source IP: 172.16.0.3   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.4	Type: DoS Attack   Source IP: 172.16.0.4   Reason: 28 packets in 30 seconds
05/14/2025 20:15:00	incident	Critical	172.16.0.5	Type: DoS Attack   Source IP: 172.16.0.5   Reason: 28 packets in 30 seconds

5. Zahnrad am Chart: Über diesen Button kannst du deine Charts konfigurieren, z.B. den Typ oder die Farbe ändern



6. Zahnrad im Header: Über diesen Button kannst du Parameter für die Verarbeitung der Log-Dateien setzen.



7. Logout: Über diesen Knopf loggst du dich wieder aus der Webapp aus