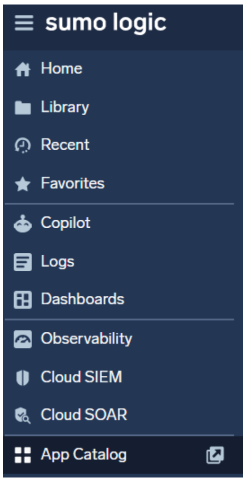
SIEM Dashboards

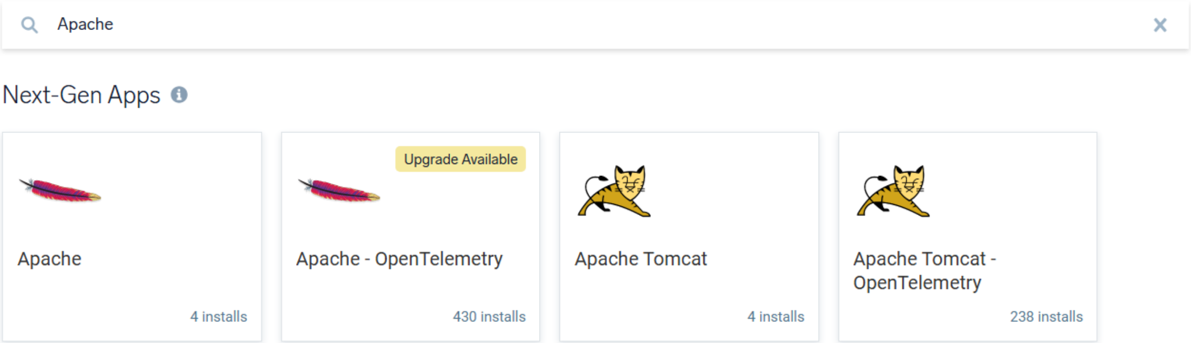
Dashboards in SIEM are software real-time interfaces that provide security teams with additional visibility of the company’s infrastructure in the form of graphs, charts, and tables. They provide actionable security insights into relevant data such as logs from cloud platforms, firewalls, endpoints, etc. An important feature of the dashboards is the possibility of modifying them to track certain performance or security indicators. Dashboards can focus on suspicious login geolocations, user behaviour that has not been seen before, or failed login attempts. They can also be used for compliance purposes, displaying adherence to certain frameworks like PCI DSS or ISO 27001.

Create the Dashboard

To create the dashboard in SUMO Logic, install the application first. In the left pane menu, choose the App Catalog option.

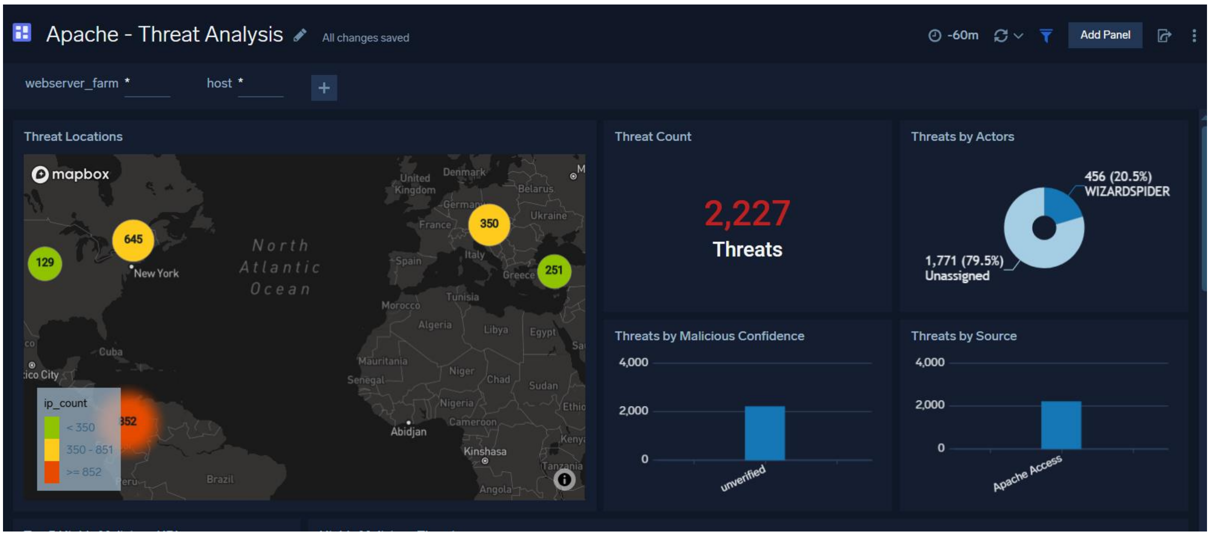


In the search field, type Apache, and choose the first available option.

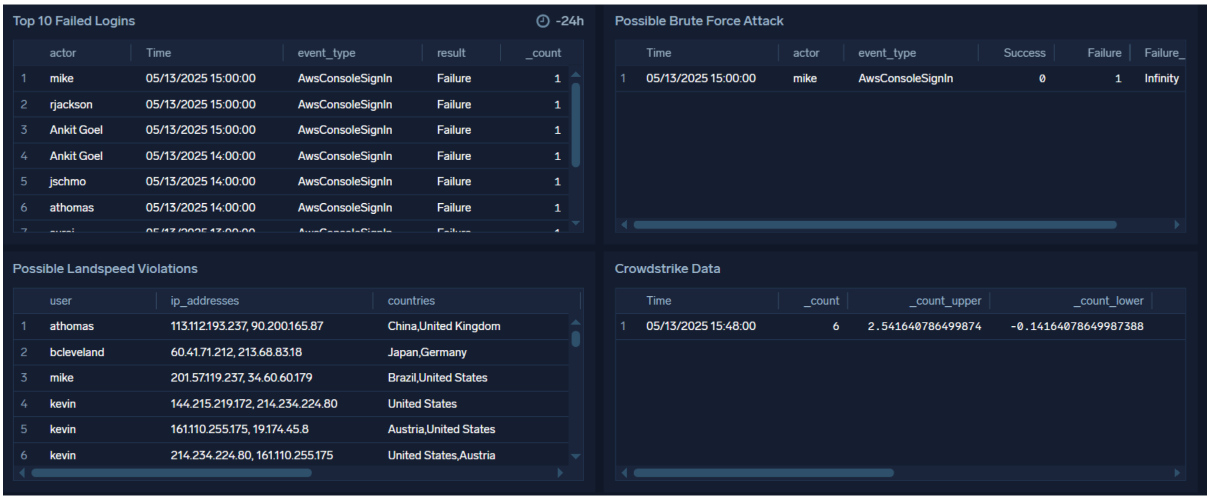


Continue to install the App. At the end of the process, you will be able to choose from many pre-built dashboards visualizing data from the installed Application.

Dashboard examples



In the first dashboard example, we can see how many threats the SIEM has identified within the last 60 minutes (time period can be changed). We can see the geolocation of the threats and identified actors. From the SOC Analyst's point of view, all those statistics are very important. Geolocation helps you detect access from unexpected countries, especially those known for cybercrime or APT activity. “Threats by actor” chart helps with identifying which threat actor is the most active, allowing analysts to prioritize proactive security measures, e.g., blocking the IP address.


Top 10 Failed Logins

-24h

	actor	Time	event_type	result	_count
1	mike	05/13/2025 15:00:00	AwsConsoleSignIn	Failure	1
2	rjackson	05/13/2025 15:00:00	AwsConsoleSignIn	Failure	1
3	Ankit Goel	05/13/2025 15:00:00	AwsConsoleSignIn	Failure	1
4	Ankit Goel	05/13/2025 14:00:00	AwsConsoleSignIn	Failure	1
5	jschmo	05/13/2025 14:00:00	AwsConsoleSignIn	Failure	1
6	athomas	05/13/2025 14:00:00	AwsConsoleSignIn	Failure	1

Possible Brute Force Attack

	Time	actor	event_type	Success	Failure	Failure_
1	05/13/2025 15:00:00	mike	AwsConsoleSignIn	0	1	Infinity

Possible Landspeed Violations

	user	ip_addresses	countries
1	athomas	113.112.193.237, 90.200.165.87	China,United Kingdom
2	bcleveland	60.41.71.212, 213.68.83.18	Japan,Germany
3	mike	201.57.119.237, 34.60.60.179	Brazil,United States
4	kevin	144.215.219.172, 214.234.224.80	United States
5	kevin	161.110.255.175, 19.174.45.8	Austria,United States
6	kevin	214.234.224.80, 161.110.255.175	United States,Austria

Crowdstrike Data

	Time	_count	_count_upper	_count_lower
1	05/13/2025 15:48:00	6	2.541640786499874	-0.14164078649987388

This dashboard provides us with 4 different measurements. First is the top 10 failed logins, which could tell the Analysts which actor had the most failed attempts to log in. This could indicate an unauthorized attempt to access the system. The second pane shows possible brute force attacks, which, again, can highlight the danger from the same point of view. 3rd pane shows the Possible Landspeed Violations, which are anomalies in user data access where the geographical distance between two places makes it impossible for the user to travel in a given time. The last pane shows Crowdstrike Data, where Sumo is checking the threats metadata against Crowdstrike’s database. Any results in this pane can point the analyst to a potential threat agent attack.