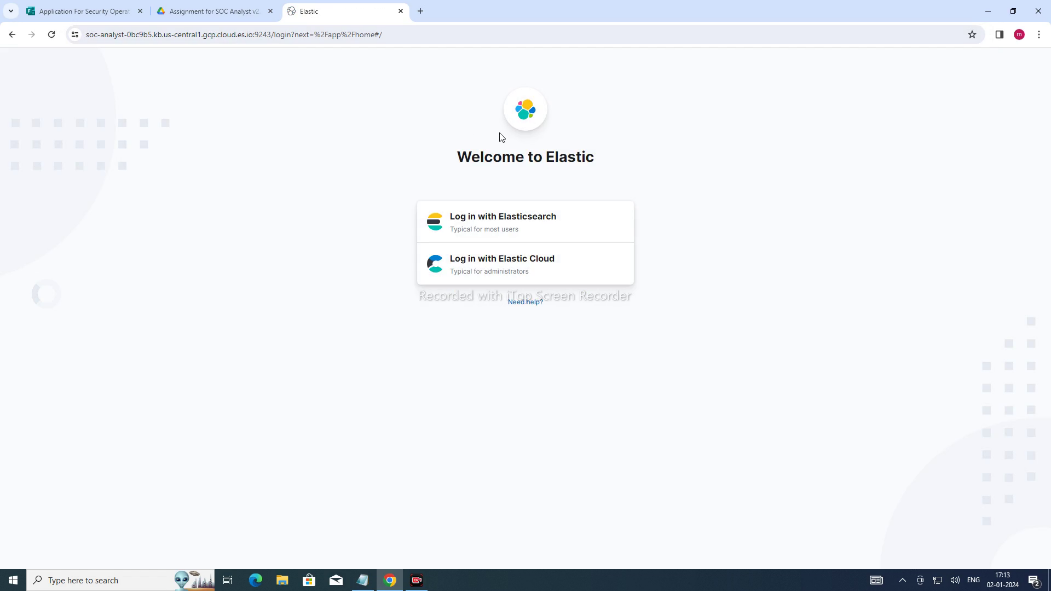
# Kibana-SIEM

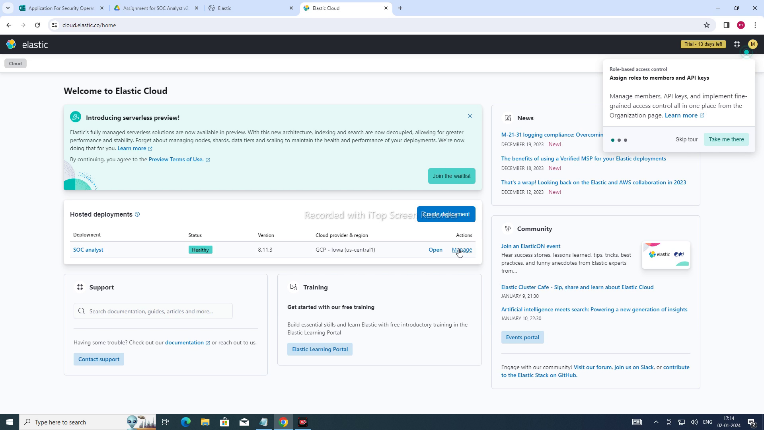
Integrating Windows Logs with Kibana for Enhanced Visibility

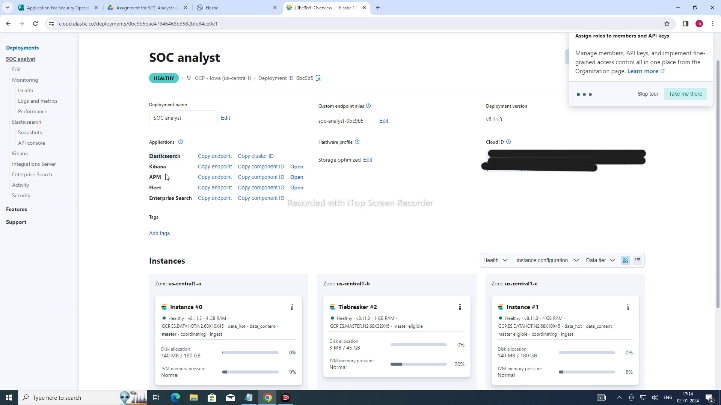
This tutorial demonstrates how to effectively integrate Windows logs with Kibana to gain valuable insights into your system's activity. By following these steps, you'll be able to create informative visualizations that help you monitor and troubleshoot your Windows environment.

Key Steps:

Sign Up for Elastic Cloud: 

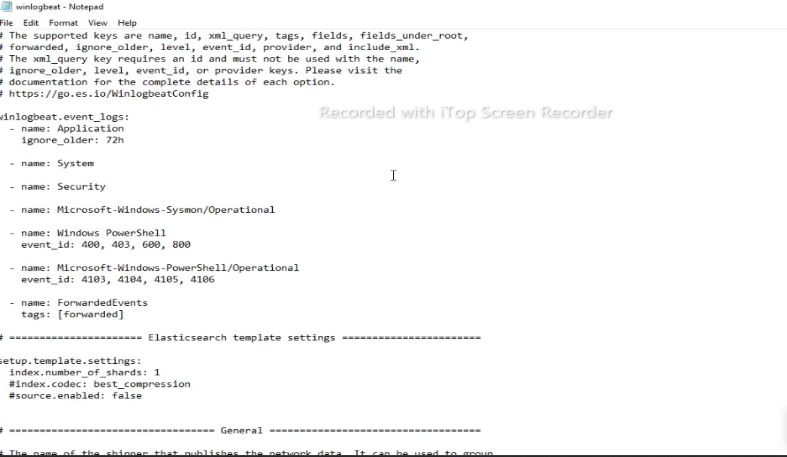
Create a free account on Elastic Cloud.

Set up a new deployment and note down the provided credentials.



Download and Configure Winlogbeat:

Download Winlogbeat from the Elastic website.

Extract the files and configure the YAML file with your Elastic Cloud credentials.

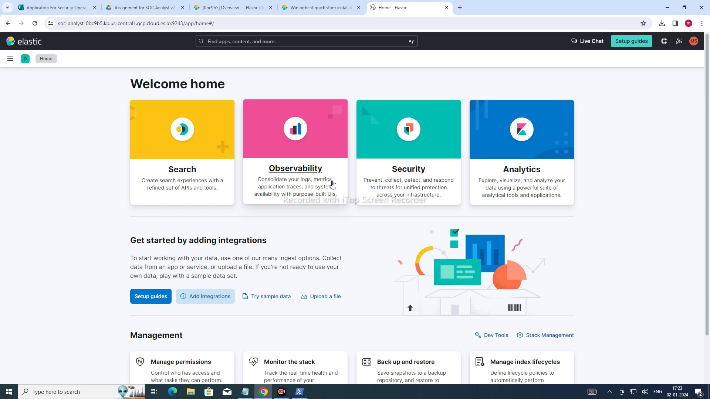
Install and start the Winlogbeat service.

https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation-configuration.html

Verify Configuration and Send Logs:

Use PowerShell commands to test the configuration and start sending logs to Elastic Cloud.

Create a Kibana Dashboard:



Access Kibana using the provided URL.

Explore the collected logs in the Discover section.

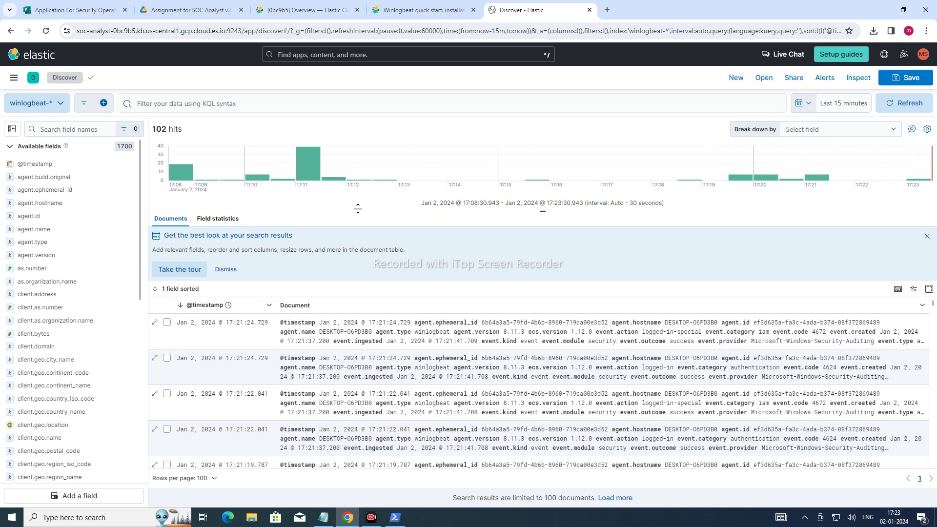
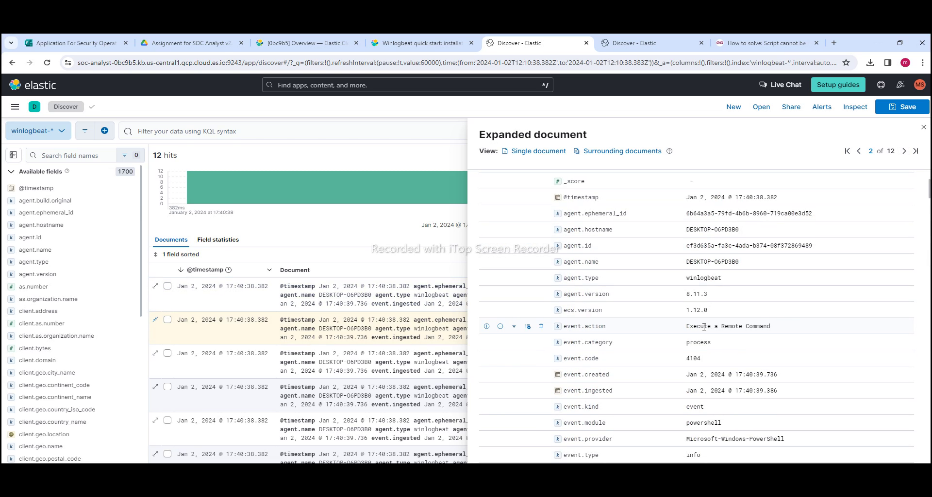
Create a new dashboard and add visualizations for:

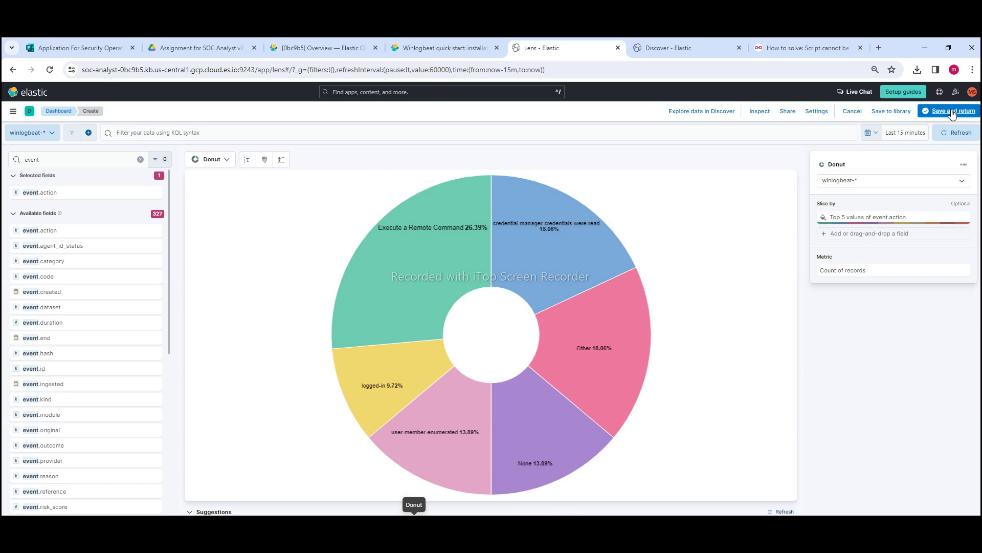
Number of hosts

Windows user event actions

Number of users

Operating system kernel and timestamp

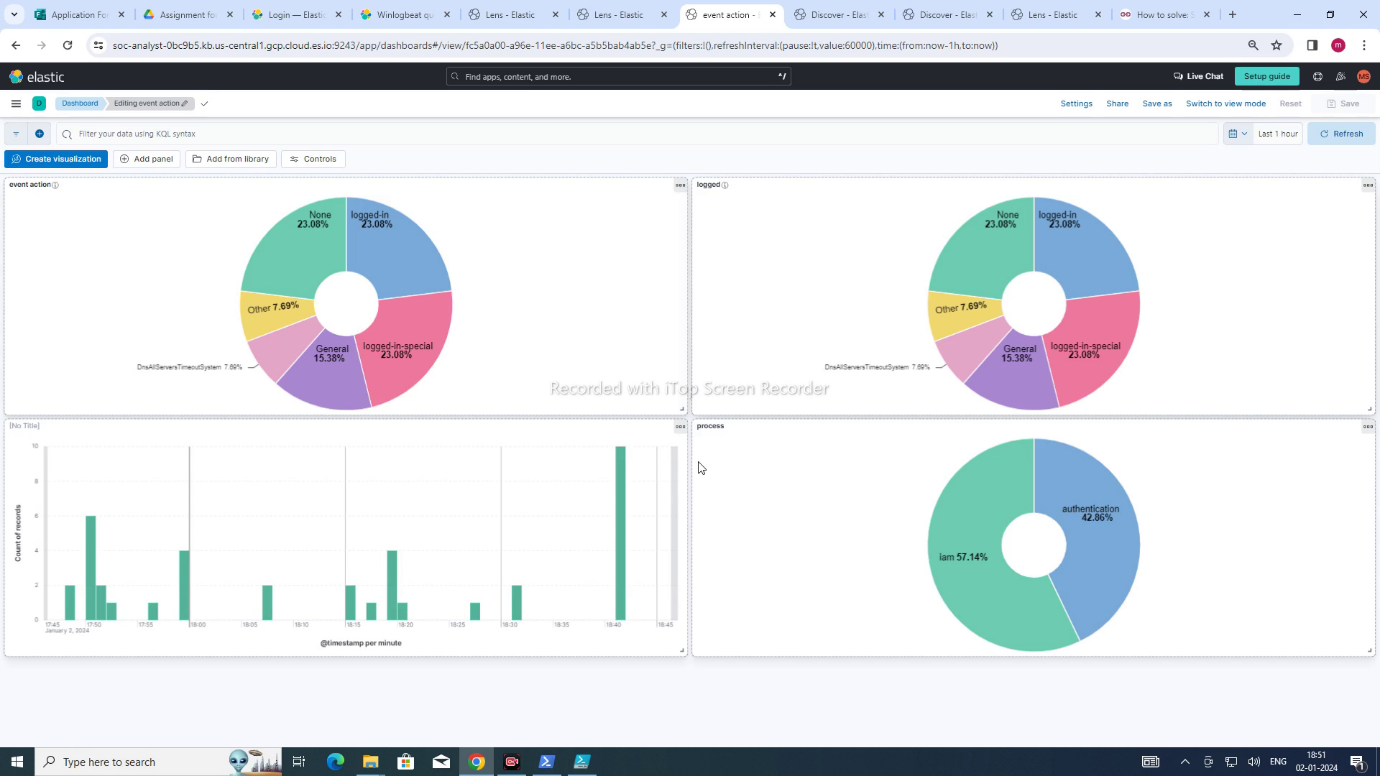
Customize the dashboard's layout and appearance. Filter and Analyze Data: 



Utilize Kibana's filtering capabilities to focus on specific time ranges or events.

Interact with the visualizations to gain deeper insights into your system's behavior.

Benefits of Integration:



Centralized Logging: Consolidate Windows logs in a single, searchable repository.

Visual Insights: Easily identify patterns, trends, and anomalies through customizable visualizations.

Improved Troubleshooting: Quickly pinpoint the root cause of issues and take corrective actions.

Enhanced Security: Monitor for potential threats and suspicious activity.

Streamlined Compliance: Facilitate adherence to regulatory requirements by maintaining comprehensive log records.