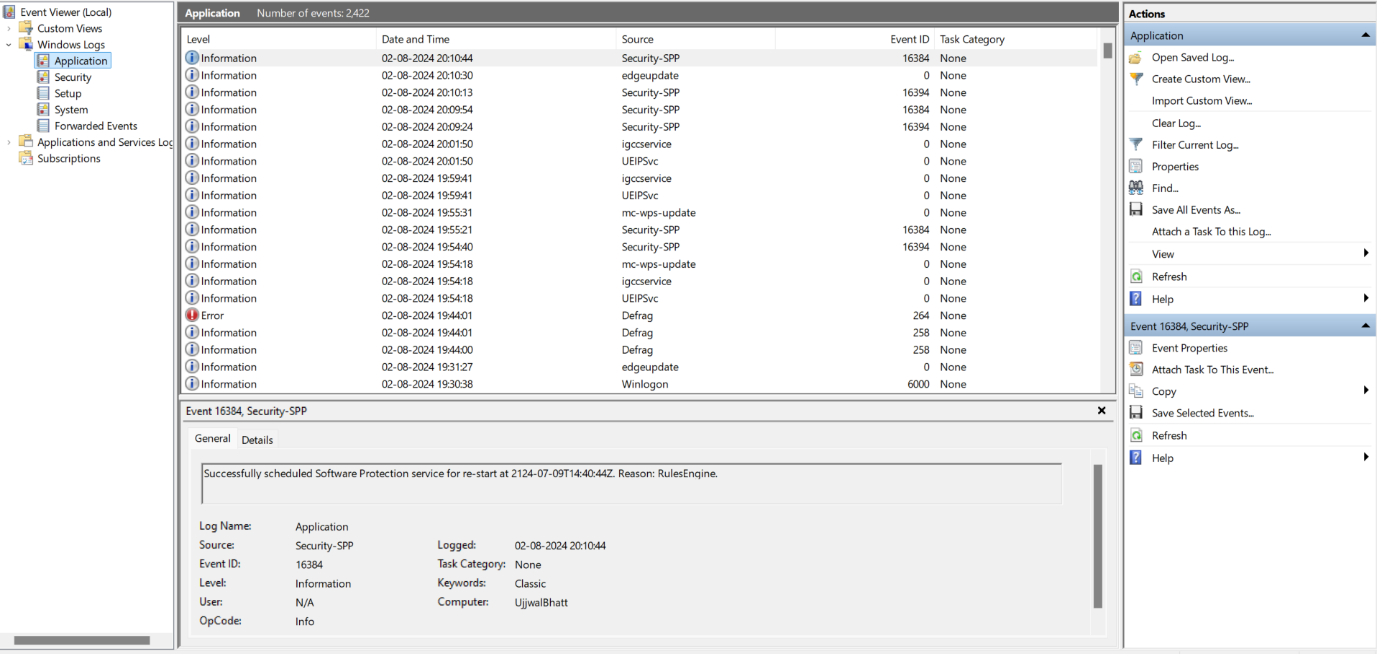
Cyber Threat Intelligence

Lab# 01: Analyse OS & Application Logs

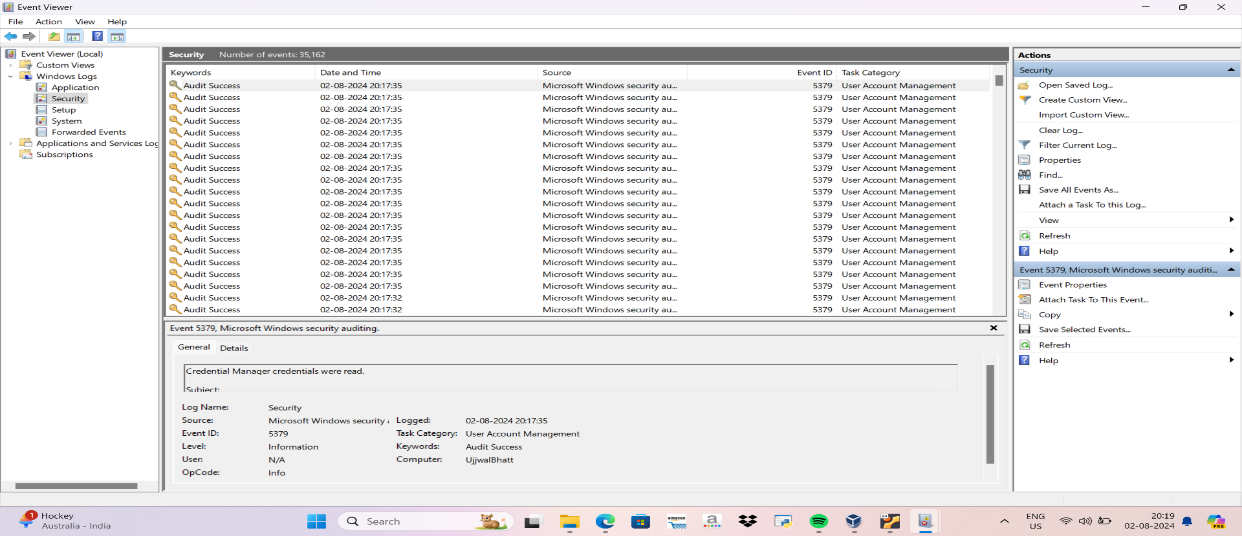
A log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server, or device

Windows OS Logs:

Identifying Application crash

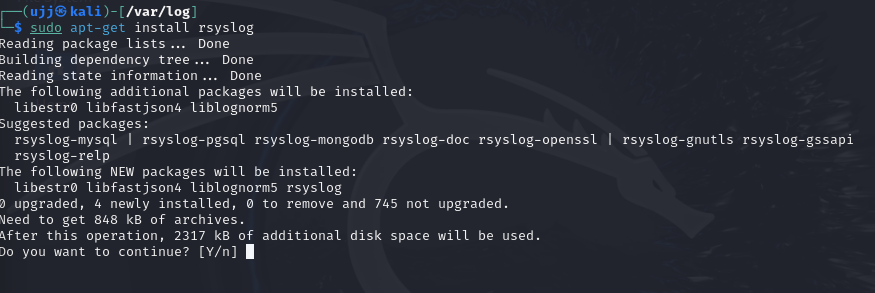


Monitoring Security Events

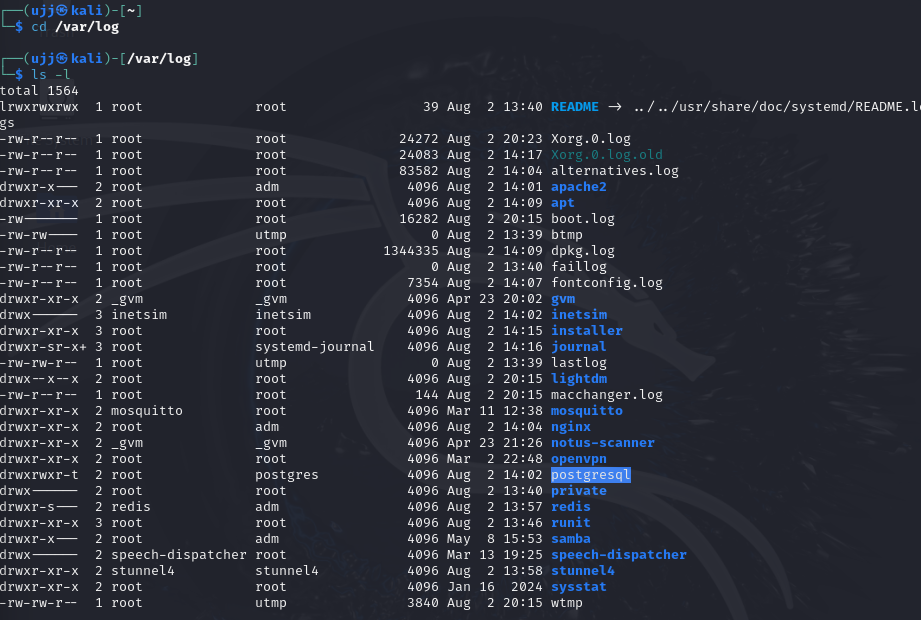


b.) Linux OS Logs

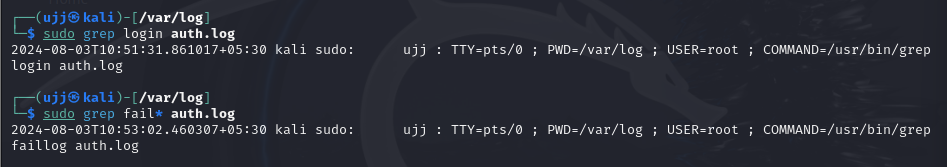
Linux logs can be found in /var/log folder. In case logs are not visible, install ‘rsyslog’



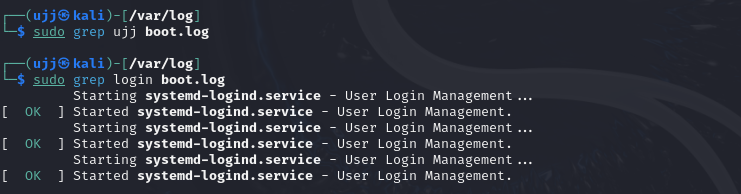
Open a terminal window go to /var/log folder and view the files and folders.



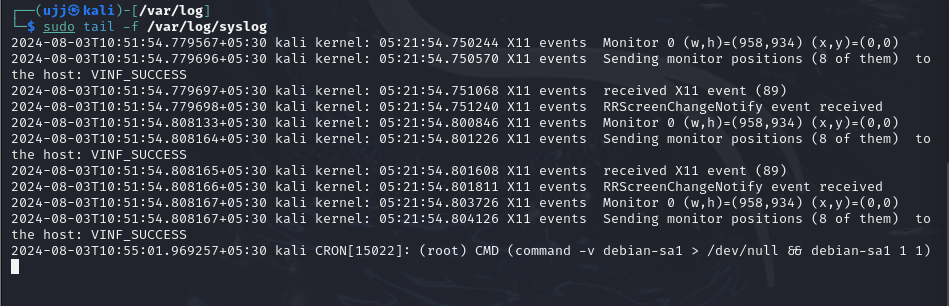
Identify Login Attempts



Check User Login Management

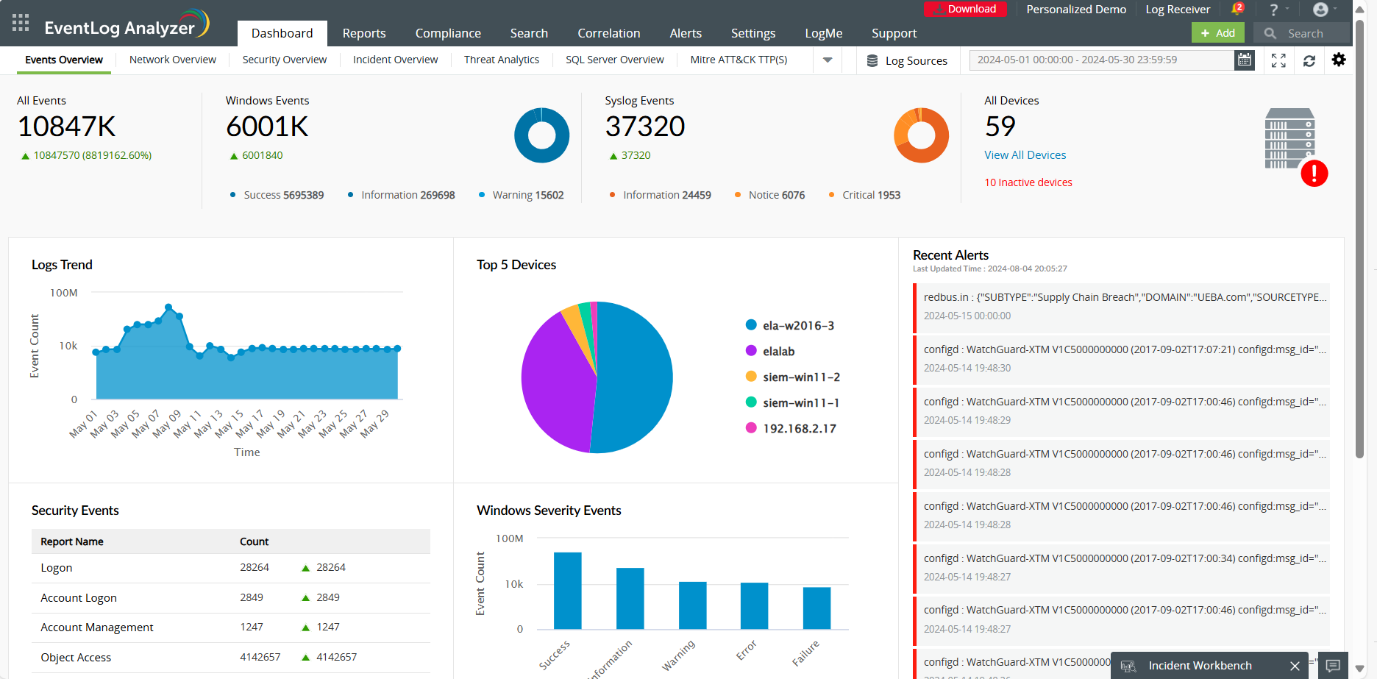


Monitor System Activity (using `tail` and `/var/log/syslog`)

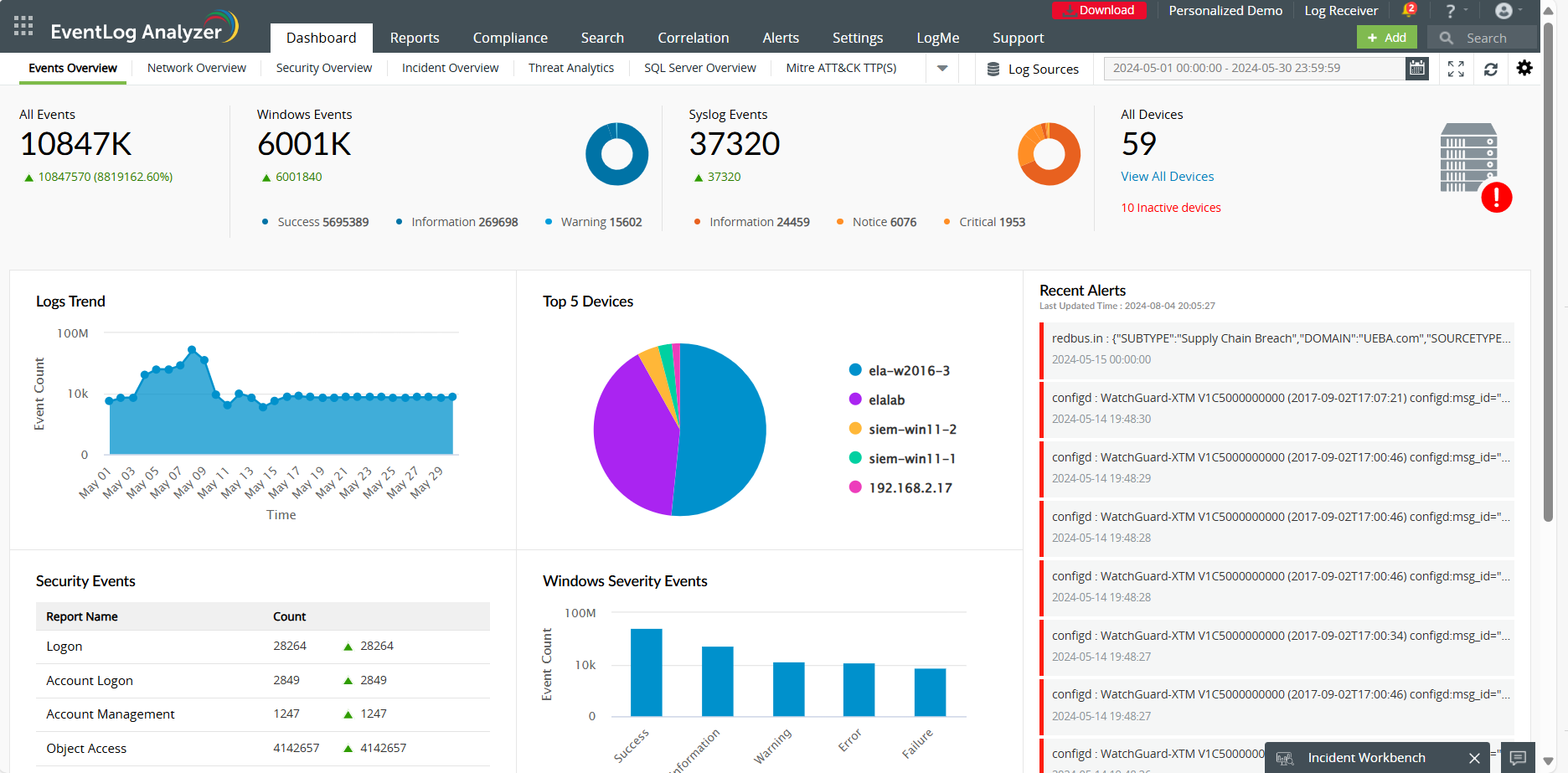


Demo Event Log Dashboard

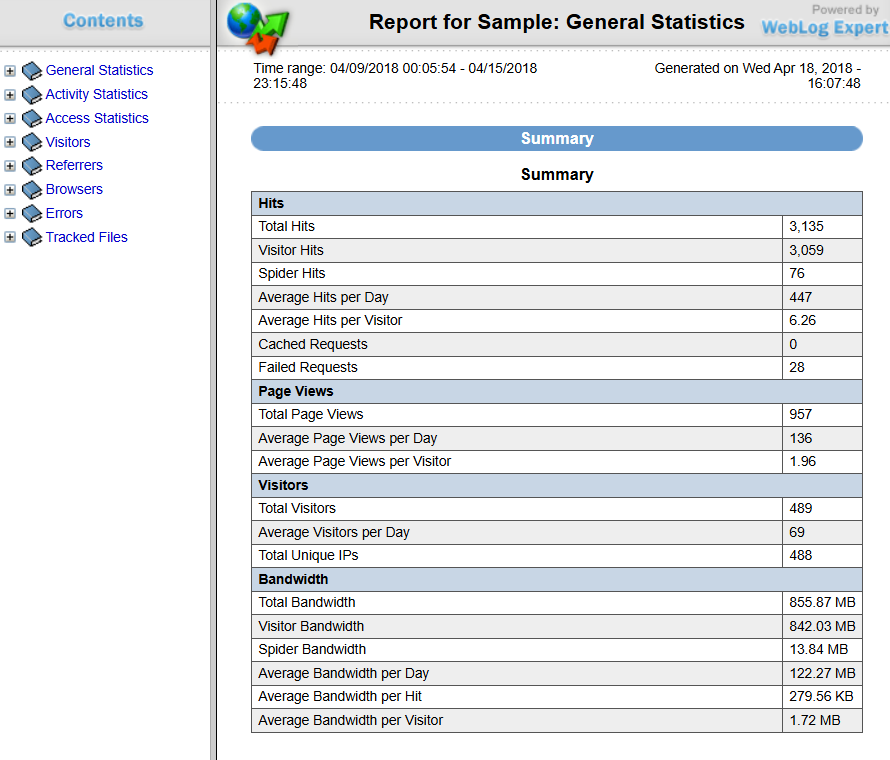
Access the demo dashboard for Manage Engine Event Log Analyzer



This displays the commercial dashboard for Events, Trends, Severity Alerts for app/device logs



Sample Web Log analysis



Web & Application Log Analysis

1. Apache Web Server

