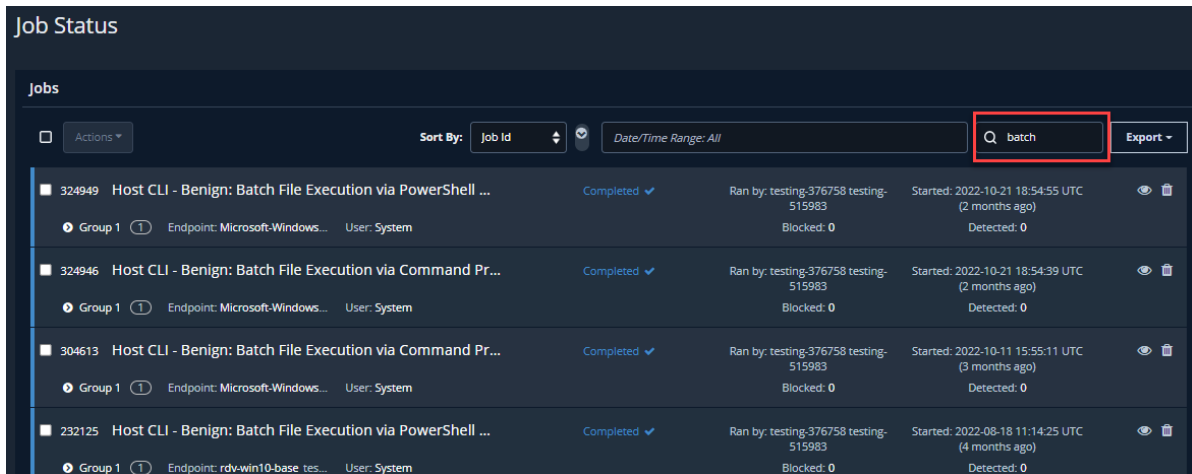


## FILTER JOBS

You can filter the Jobs by date or by completing a text-based search.

The text filter, highlighted in the image below, lets you search for matches in the Job ID, Job name, Monitor name, Sequence name, Evaluation Name, Job status, user first and last names, Action name, and VID.

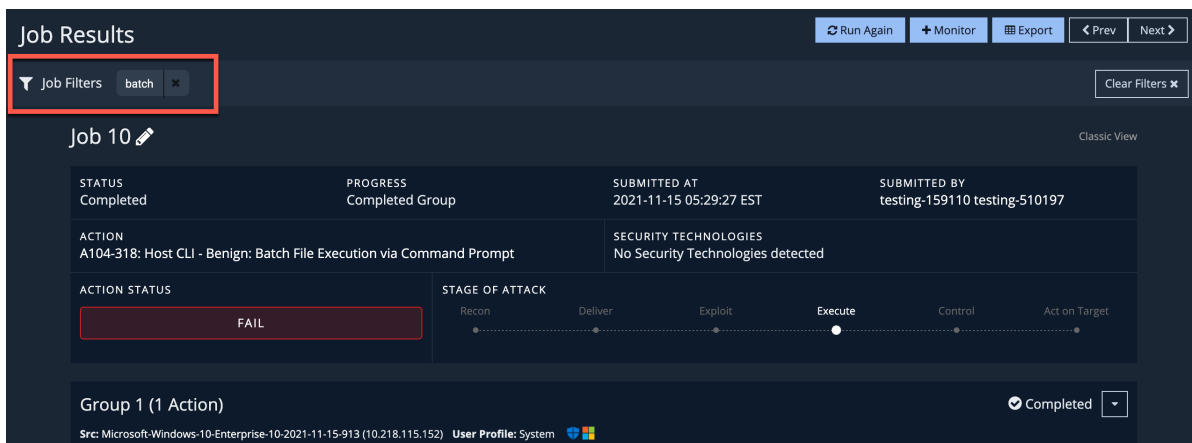


The screenshot shows the 'Job Status' page with a list of jobs. A search bar at the top right contains the text 'batch' and is highlighted with a red box. The list below shows four jobs, all with a status of 'Completed'.

Job ID	Job Name	Status	Ran by	Started
324949	Host CLI - Benign: Batch File Execution via PowerShell ...	Completed	testing-376758 testing-515983	2022-10-21 18:54:55 UTC (2 months ago)
324946	Host CLI - Benign: Batch File Execution via Command Pr...	Completed	testing-376758 testing-515983	2022-10-21 18:54:39 UTC (2 months ago)
304613	Host CLI - Benign: Batch File Execution via Command Pr...	Completed	testing-376758 testing-515983	2022-10-11 15:55:11 UTC (3 months ago)
232125	Host CLI - Benign: Batch File Execution via PowerShell ...	Completed	testing-376758 testing-515983	2022-08-18 11:14:25 UTC (4 months ago)

Job Status page

When you open a Job from the filtered Job list, the filter is maintained, as shown in the screenshot, allowing you to quickly scroll through the matching Jobs. You can remove the filter to scroll through all the Jobs, but if you want to apply a new filter, you must return to the Job Status page.



The screenshot shows the 'Job Results' page for 'Job 10'. The 'Job Filters' section at the top left contains the text 'batch' and is highlighted with a red box. The job details below show a status of 'Completed' and an action status of 'FAIL'.

STATUS	PROGRESS	SUBMITTED AT	SUBMITTED BY
Completed	Completed Group	2021-11-15 05:29:27 EST	testing-159110 testing-510197

**ACTION**  
A104-318: Host CLI - Benign: Batch File Execution via Command Prompt

**SECURITY TECHNOLOGIES**  
No Security Technologies detected

**ACTION STATUS**  
FAIL

**STAGE OF ATTACK**  
Recon → Deliver → Exploit → Execute → Control → Act on Target

Group 1 (1 Action) Completed

Src: Microsoft-Windows-10-Enterprise-10-2021-11-15-913 (10.218.115.152) User Profile: System

Filter on Jobs