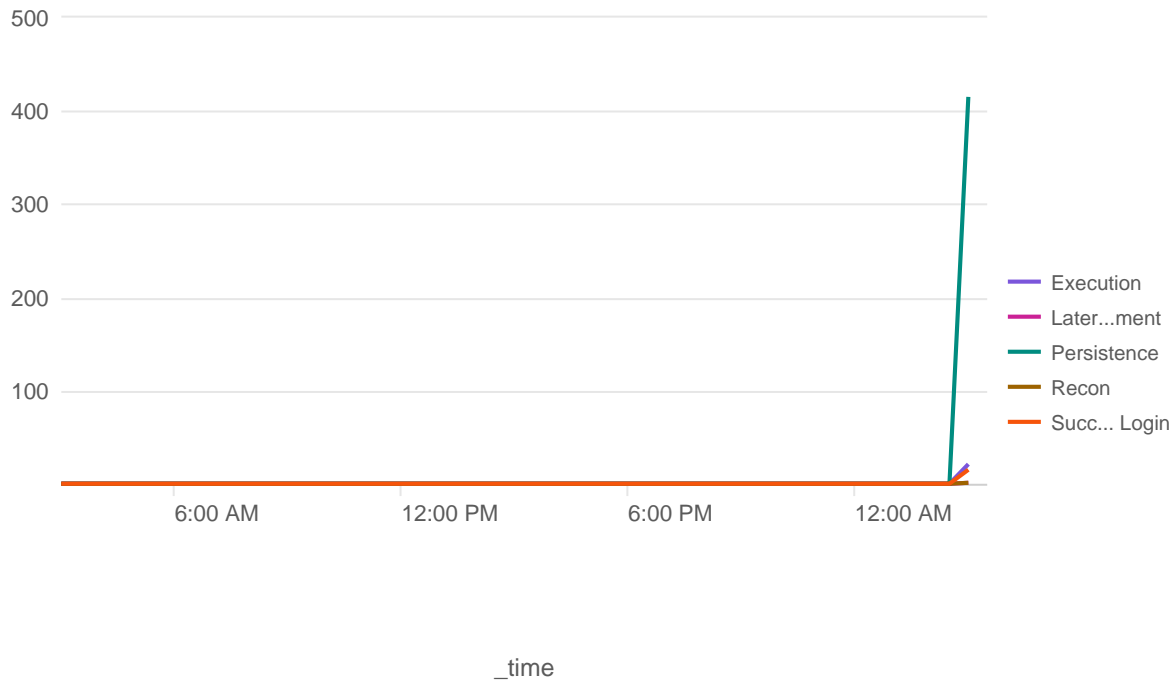
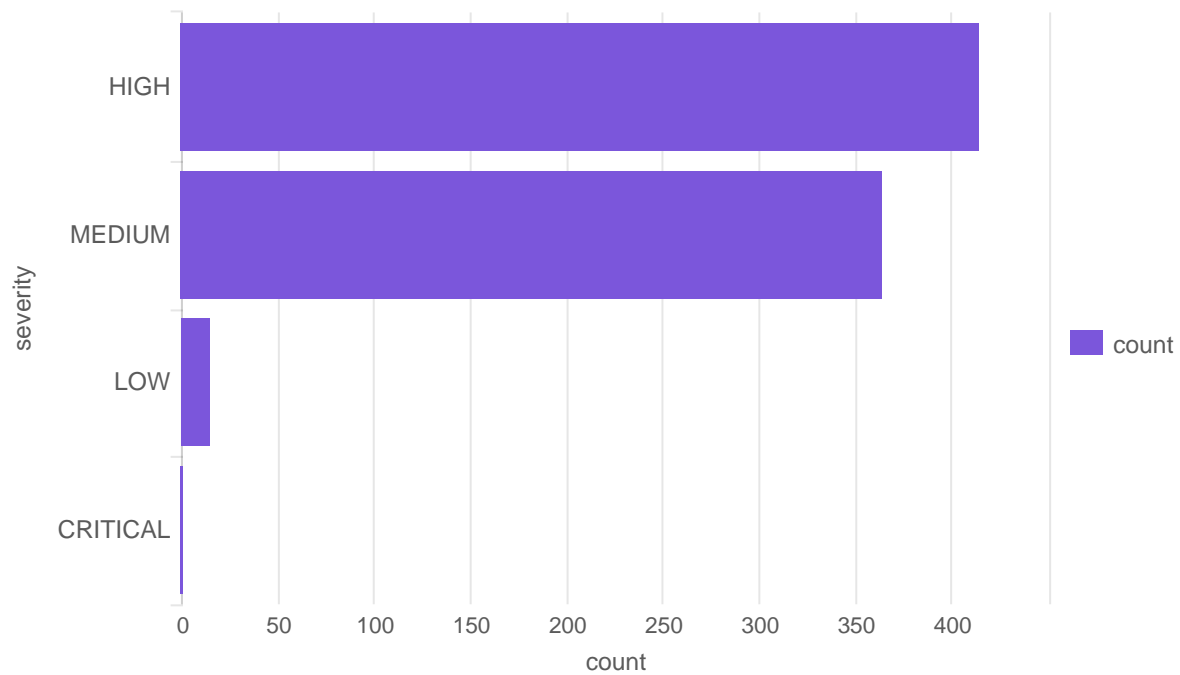


## Attack Phase Timeline



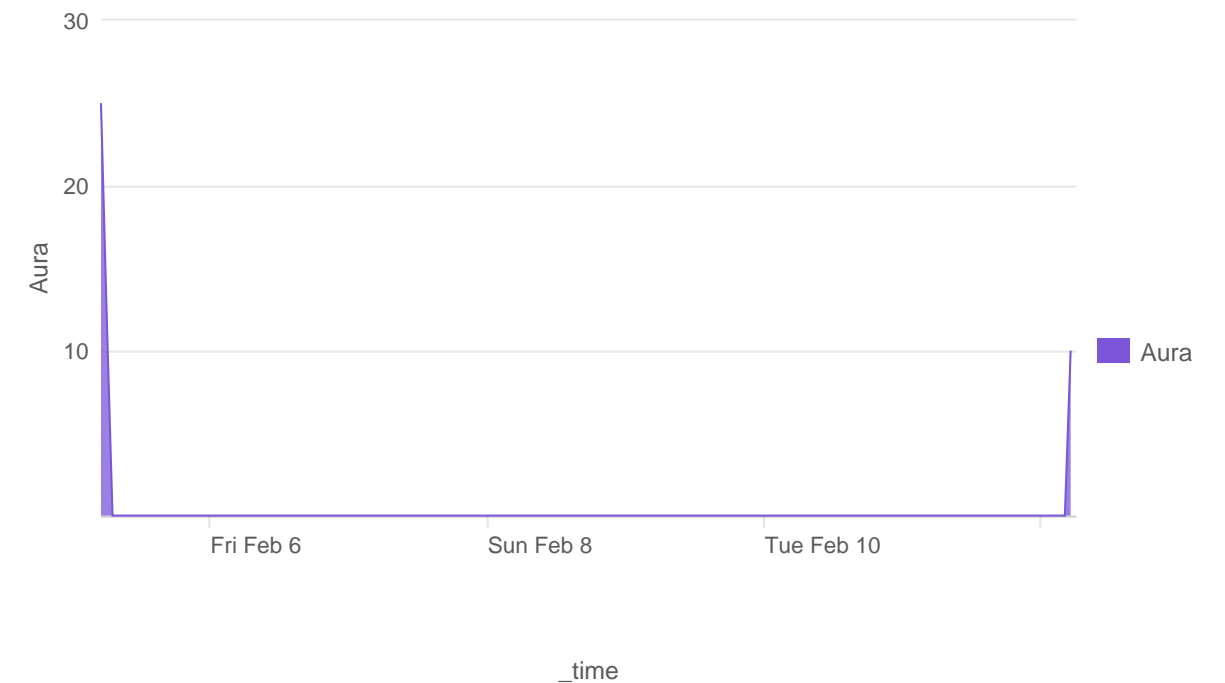
## Alert Severity Distribution



## Top 10 Processes by Event Count

Process	count
C:\Windows\System32\taskhostw.exe	14
C:\Windows\System32\svchost.exe	8
C:\Windows\System32\backgroundTaskHost.exe	4
C:\Windows\servicing\TrustedInstaller.exe	4
C:\Windows\System32\cmd.exe	3
C:\Windows\System32\rundll32.exe	3
C:\Windows\System32\sc.exe	3
C:\Program Files\RUXIM\RUXIMICS.exe	2
C:\Windows\System32\UsbClient.exe	2
C:\Windows\System32\WaaSMedicAgent.exe	2

## Failed Login Activity Over Time



# EDR — Defender Detections & Actions

Action	count
Detected	16
Quarantined	14