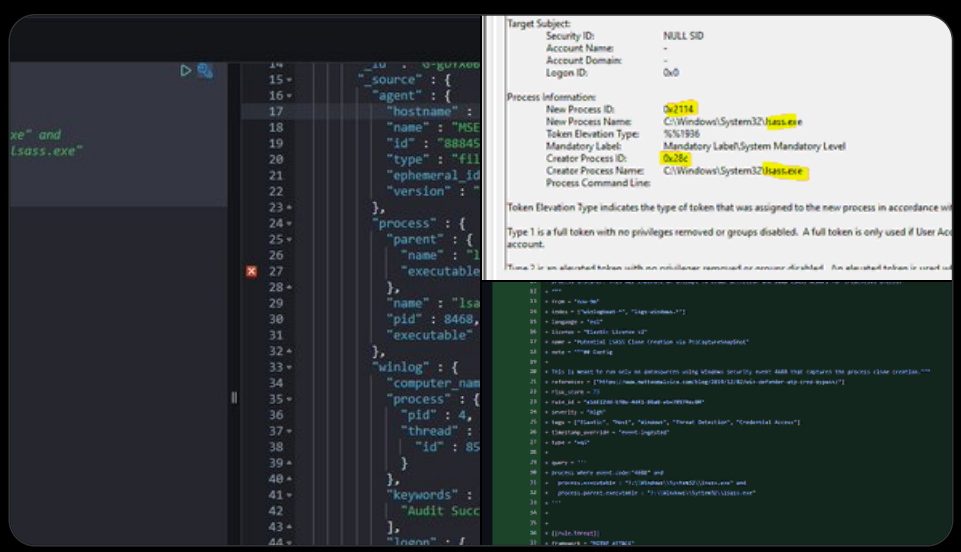
Post

Samir
@SBousseaden

just added a detection for creating an LSASS clone to dump memory or alike using event 4688, more details in the PR:

github.com/elastic/detect...



> **Adam** @Hexacorn · Jul 27, 2021
> Replying to @BlackMatter23 @binaryz0ne and 2 others
> I guess it's PspInsertProcess -> SeAuditProcessCreation ... -> 4688 and... PspInsertProcess is called before PspInsertThread inside NtCreateUserProcess

1:08 PM · Nov 27, 2021

45 Reposts **1** Quote **180** Likes **35** Bookmarks

35