worldskills India

Skill India
कौशल भारत - कुशल भारत

N·S·D·C
National Skill Development Corporation
Transforming the skill landscape

Module C

IndiaSkills National Competition

Cyber Security

NASSCOM®

Description

Let's go Threat Hunting.

The organization has multiple endpoints, the data of which has been made available to you. Along with that, you have also been provided with various other datapoints such as logged-on accounts on different endpoints, processes running, registry snapshots etc. All of these logs are also available on the Splunk instance provided to you.

The challenge is very simple. Find out all the affected endpoints, and the malicious actions performed on them. Please note that not all endpoints have had malicious actions performed on them. This Module is worth 30 Points. No granular marking would be provided. The artifacts that you find have points associated with it and would be awarded.

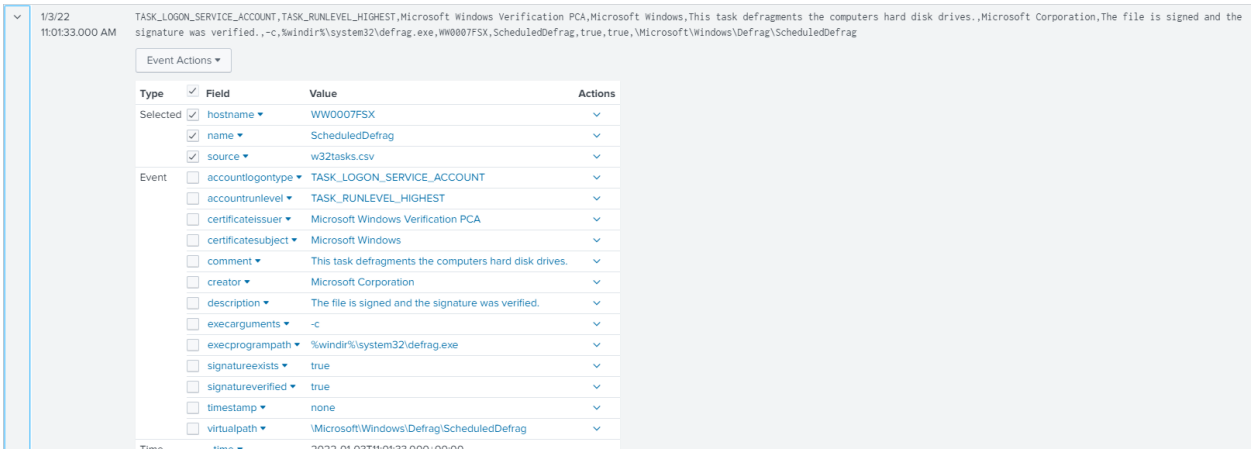
You need to make a report on Google Docs and submit it as a pdf on the provided Google Forms link. The filename of your report should be *YourState_YourName.pdf*

The next page shows how each page of your report should look. For each compromised hostname, mention the artifact you found, the file this artifact is present in and, the screenshot of the log indicating the artifact. If any artifact detail is not provided in the manner mentioned, it would not be considered and no points would be allocated for it.

Submission link -> https://forms.gle/YEwjYNoL9fLHqCKF6
Splunk URL -> http://127.0.0.1:8000/
Splunk Credentials -> splunk: splunk123

Hostname: Mike-PC

1. Artifact: Download of binary from www.ixhsds.net
   File: download_logs.csv
   Query: index="demo" sourcetype="demo_source" source="download_logs.csv"



2. Artifact: Download of binary from www.ixhsds.net
   File: download_logs.csv
   Query: index="demo" sourcetype="demo_source" source="download_logs.csv"