



## 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](http://www.ixhsds.net)

File: download\_logs.csv

Query: index="demo" sourcetype="demo\_source"  
source="download\_logs.csv"

1/3/22  
11:01:33.000 AM

TASK\_LOGON\_SERVICE\_ACCOUNT,TASK\_RUNLEVEL\_HIGHEST,Microsoft Windows Verification PCA,Microsoft Windows,This task defragments the computers hard disk drives.,Microsoft Corporation,The file is signed and the signature was verified.,-c,%windir%\system32\defrag.exe,w0007FSX,ScheduledDefrag,true,true,Microsoft\Windows\Defrag\ScheduledDefrag

Event Actions ▾

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> hostname ▾	WW0007FSX	▾
	<input checked="" type="checkbox"/> name ▾	ScheduledDefrag	▾
	<input checked="" type="checkbox"/> source ▾	w32tasks.csv	▾
Event	<input type="checkbox"/> accountlogontype ▾	TASK_LOGON_SERVICE_ACCOUNT	▾
	<input type="checkbox"/> accountrunlevel ▾	TASK_RUNLEVEL_HIGHEST	▾
	<input type="checkbox"/> certificateissuer ▾	Microsoft Windows Verification PCA	▾
	<input type="checkbox"/> certificatesubject ▾	Microsoft Windows	▾
	<input type="checkbox"/> comment ▾	This task defragments the computers hard disk drives.	▾
	<input type="checkbox"/> creator ▾	Microsoft Corporation	▾
	<input type="checkbox"/> description ▾	The file is signed and the signature was verified.	▾
	<input type="checkbox"/> execarguments ▾	-c	▾
	<input type="checkbox"/> execprogrampath ▾	%windir%\system32\defrag.exe	▾
	<input type="checkbox"/> signatureexists ▾	true	▾
	<input type="checkbox"/> signatureverified ▾	true	▾
	<input type="checkbox"/> timestamp ▾	none	▾
	<input type="checkbox"/> virtualpath ▾	Microsoft\Windows\Defrag\ScheduledDefrag	▾

## 2. Artifact: Download of binary from

[www.ixhsds.net](http://www.ixhsds.net)

File: download\_logs.csv

Query: index="demo" sourcetype="demo\_source"  
source="download\_logs.csv"

1/3/22  
11:01:33.000 AM

TASK\_LOGON\_SERVICE\_ACCOUNT,TASK\_RUNLEVEL\_HIGHEST,Microsoft Windows Verification PCA,Microsoft Windows,This task defragments the computers hard disk drives.,Microsoft Corporation,The file is signed and the signature was verified.,-c,%windir%\system32\defrag.exe,W0007FSX,ScheduledDefrag,true,true,Microsoft\Windows\Defrag\ScheduledDefrag

Event Actions ▾

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> hostname ▾	WW0007FSX	▾
	<input checked="" type="checkbox"/> name ▾	ScheduledDefrag	▾
	<input checked="" type="checkbox"/> source ▾	w32tasks.csv	▾
Event	<input type="checkbox"/> accountlogontype ▾	TASK_LOGON_SERVICE_ACCOUNT	▾
	<input type="checkbox"/> accountrunlevel ▾	TASK_RUNLEVEL_HIGHEST	▾
	<input type="checkbox"/> certificateissuer ▾	Microsoft Windows Verification PCA	▾
	<input type="checkbox"/> certificatesubject ▾	Microsoft Windows	▾
	<input type="checkbox"/> comment ▾	This task defragments the computers hard disk drives.	▾
	<input type="checkbox"/> creator ▾	Microsoft Corporation	▾
	<input type="checkbox"/> description ▾	The file is signed and the signature was verified.	▾
	<input type="checkbox"/> execarguments ▾	-c	▾
	<input type="checkbox"/> execprogrampath ▾	%windir%\system32\defrag.exe	▾
	<input type="checkbox"/> signatureexists ▾	true	▾
	<input type="checkbox"/> signatureverified ▾	true	▾
	<input type="checkbox"/> timestamp ▾	none	▾
	<input type="checkbox"/> virtualpath ▾	Microsoft\Windows\Defrag\ScheduledDefrag	▾