

QUESTION NUMBER 7

QUESTION 7

QUESTION 7A

How would you detect and respond to a malware infection on an endpoint?

ANSWER

1. DETECTION

Malware can be detected using automatic and manual method

Automatic method

- Endpoint Detection and Response (EDR) - EDR uses signature-based detection and behavioral monitoring
- SIEM monitoring - Security Information and Event Management is used to aggregate and analyze logs from various sources and to search for IoC
- Sysmon and Windows Event logs - Event viewer to monitor for suspicious activity.

Manual method

-Network traffic analysis and file integrity monitoring

2 CONTAINMENT

- Isolate the affected system :** Disconnect the infected system from the network to prevent the spread of malware.
- Compromised Accounts:** If the accounts of the user are compromised, the user accounts should be disabled

3. ERADICATION

- Malicious files should be deleted manually or use of anti virus to scan and remove malicious files

4.RECOVERY

- Apply security patches and update the software to close any vulnerabilities exploited by the malware and restore the system from a clean back up. Password for affected accounts should be changed

5. Post-Incident Review and Prevention

-Document the incident and the steps taken to recover so as to understand the root cause. Security awareness should be made compulsory for all workers.

QUESTION 7B

Set up a test environment with Sysmon installed on a Windows machine. Simulate a malware infection by executing a test malware file. Monitor the endpoint for unusual behavior (e.g., new processes, registry changes) and document your incident response steps to contain and remove the malware. □

Tools: Sysmon, Process Explorer (from Sysinternals Suite)

ANSWER

-First of all i downloaded sysmon v5.15 from microsoft website

The screenshot shows a web browser displaying the Microsoft Learn - Sysinternals page. The URL in the address bar is <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>. The page has a navigation bar with 'Learn' selected, along with 'Discover', 'Product documentation', 'Development languages', and 'Topics'. Below the navigation is a 'Sysinternals' menu with 'Downloads', 'Community', and 'Resources' options. A search bar with a 'Filter by title' button is present. The main content area features a large heading 'Sysmon v15.15' with a subtext 'Article • 07/23/2024 • 10 contributors'. To the left is a sidebar with a tree view of Sysinternals tools, where 'Sysmon' is currently selected. Other tools listed include Home, Downloads, File and Disk Utilities, Networking Utilities, Process Utilities, Security Utilities, System Information, Miscellaneous, and Sysinternals Suite. To the right of the article summary are sections for 'In this article' (Introduction, Overview of Sysmon Capabilities, Screenshots, Usage, Show 5 more), author information (By Mark Russinovich and Thomas Garnier), publication date (Published: July 23, 2024), and download links (Download Sysmon (4.6 MB) and Download Sysmon for Linux (GitHub)).

- I extracted the sysmon files

-I opened my powershell and run as the administrator, I moved to the Downloads directory on my powershell to see what I have downloaded

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> cd C:\Users\User\Downloads
PS C:\Users\User\Downloads> ls

Directory: C:\Users\User\Downloads
```

```
Administrator: Windows PowerShell
website.

specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.

>PS C:\Users\User\Downloads> sysmon -accepteula -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
by Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install:           Sysmon.exe -i [<configfile>]
Update configuration: Sysmon.exe -c [<configfile>]
Install event manifest: Sysmon.exe -m
Print schema:      Sysmon.exe -s
Uninstall:         Sysmon.exe -u [Force]
-c   Update configuration of an installed Sysmon driver or dump the
     current configuration if no other argument is provided. Optionally
     take a configuration file.
-i   Install service and driver. Optionally take a configuration file.
-m   Install the event manifest (done on service install as well)).
-s   Print configuration schema definition of the specified version.
     Specify 'all' to dump all schema versions (default is latest)).
-u   Uninstall service and driver. Adding force causes uninstall to proceed
     even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.

>PS C:\Users\User\Downloads> Sysmon.exe -i

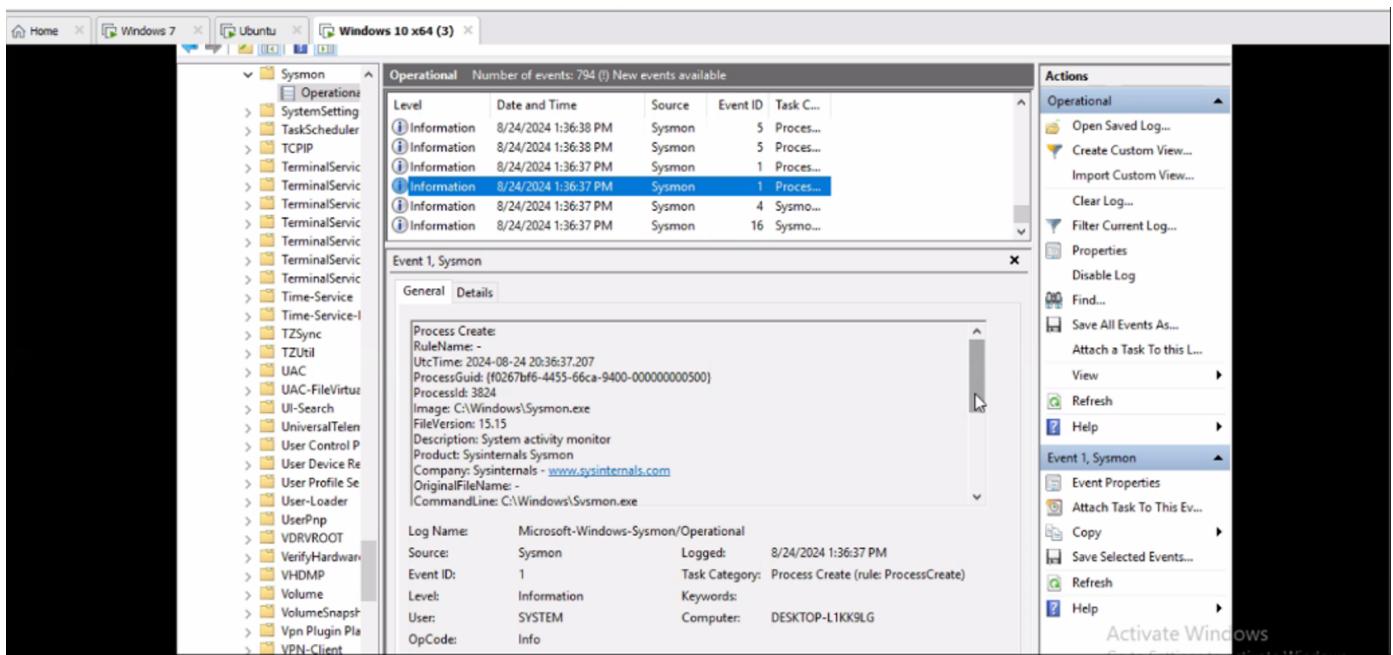
System Monitor v15.15 - System activity monitor
```

I installed sysmon.exe with the powershell

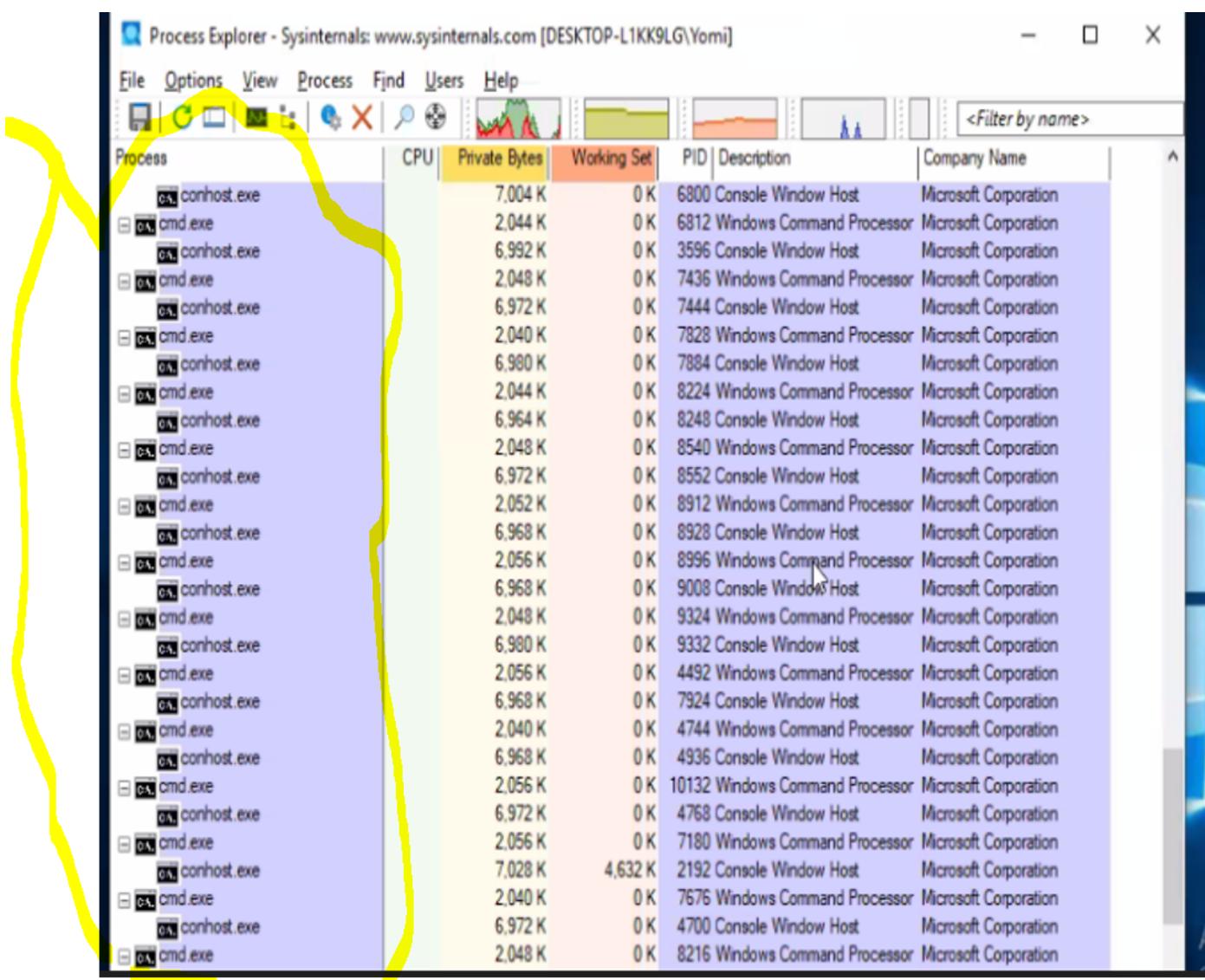
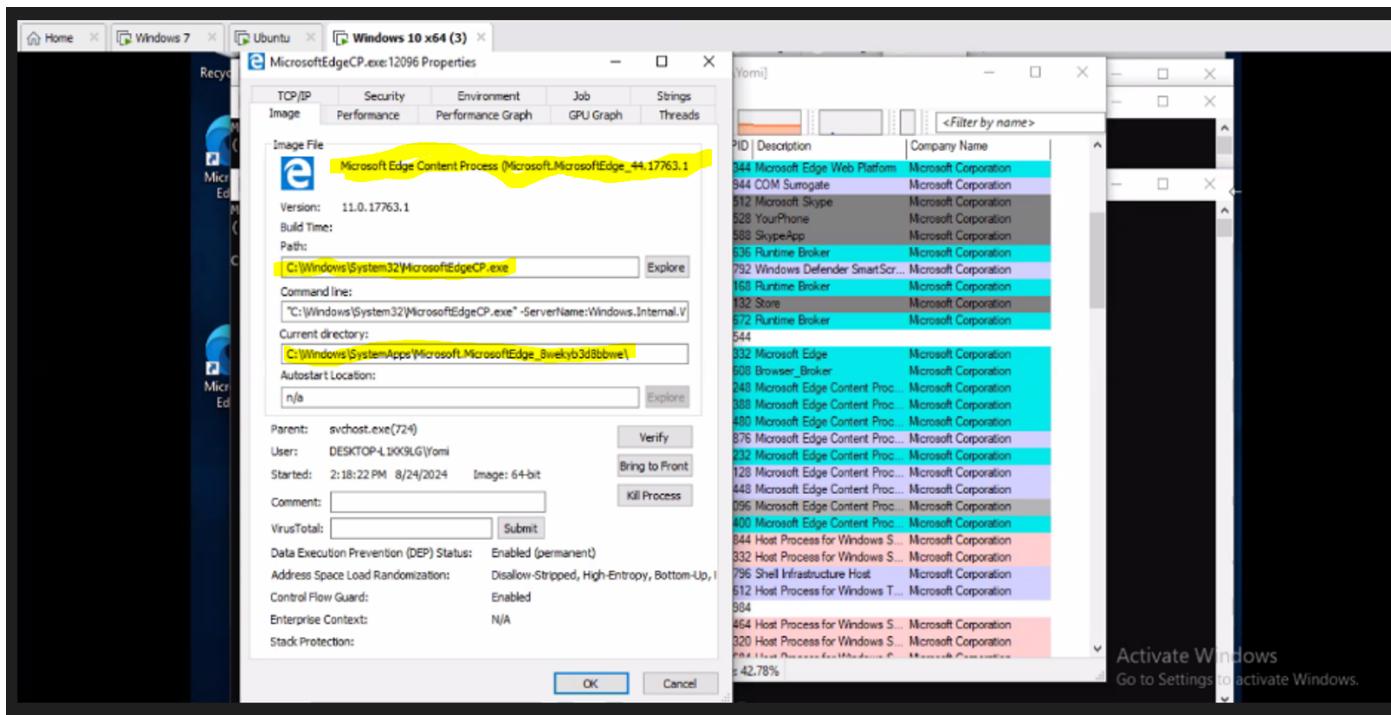
-I created a malicious file and executed on the windows system VM.

```
@echo off
:LoopStart
start
start www.nairaland.com
del c:\important\. /Q
goto :LoopStart||
```

-I monitored the Window endpoint for unusual activity by using the event viewer to check Sysmon logs



- The Process explorer was used to identify processes running from unusual directories and the image path on the process explorer was used to identify the location of the executable malicious file and the command line was used to identify how the file was launched.



The image above shows the process explorer.

--I noticed a Virus total property on the process explorer and i used it to check the virus total score.

The screenshot shows the Windows Task Manager with the title bar "SecOps Services Agree X". Below it is the Process Explorer window titled "Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-L1KK9LG\Yomi]". The menu bar has "File", "Options" (which is selected), "View", "Process", "Find", "Users", and "Help". A context menu is open over a process named "Check VirusTotal.com" (PID 5636). The menu items include "Run At Logon", "Verify Image Signatures", "VirusTotal.com" (selected), "Always On Top", "Replace Task Manager", "Hide When Minimized", "Allow Only One Instance", "Confirm Kill", "Tray Icons", "Configure Symbols...", "Configure Colors...", "Difference Highlight Duration...", "Font...", "Theme", and "taskhostw.exe" (selected). The main table lists processes with columns: Private Bytes, Working Set, PID, Description, and Company Name. Several Microsoft Edge processes are listed, along with various svchost.exe and host processes.

Private Bytes	Working Set	PID	Description	Company Name
149,872 K	0 K	5588	SkypeApp	Microsoft Corporation
6,172 K	212 K	5636	Runtime Broker	Microsoft Corporation
15,692 K	14,076 K	5792	Windows Defender SmartScr...	Microsoft Corporation
5,168 K	1,808 K	2168	Runtime Broker	Microsoft Corporation
16,020 K	0 K	6132	Store	Microsoft Corporation
1,524 K	160 K	4672	Runtime Broker	Microsoft Corporation
2,068 K	680 K	6544		
26,304 K	48,828 K	10012	Microsoft Edge	Microsoft Corporation
3,604 K	9,336 K	8560	Browser_Broker	Microsoft Corporation
124,036 K	80,480 K	12024	Microsoft Edge Content Proc...	Microsoft Corporation
6,040 K	23,436 K	10476	Microsoft Edge Content Proc...	Microsoft Corporation
135,796 K	162,148 K	8440	Microsoft Edge Content Proc...	Microsoft Corporation
6,024 K	24,120 K	564	Microsoft Edge Content Proc...	Microsoft Corporation
7,704 K	7,344 K	844	Host Process for Windows S...	Microsoft Corporation
40,840 K	13,444 K	332	Host Process for Windows S...	Microsoft Corporation
7,864 K	14,572 K	2796	Shell Infrastructure Host	Microsoft Corporation
8,928 K	7,520 K	612	Host Process for Windows T...	Microsoft Corporation
2,632 K	0 K	2984		
11,072 K	4,496 K	464	Host Process for Windows S...	Microsoft Corporation
12,356 K	5,152 K	320	Host Process for Windows S...	Microsoft Corporation
19,476 K	6,340 K	684	Host Process for Windows S...	Microsoft Corporation
6,808 K	5,640 K	644	Host Process for Windows S...	Microsoft Corporation
7,128 K	4,788 K	3176		
1,644 K	904 K	1228	Host Process for Windows S...	Microsoft Corporation
8,644 K	2,988 K	1288	Host Process for Windows S...	Microsoft Corporation

CONTAINMENT AND REMOVAL OF THE MALWARE

--- I used the kill process to kill the suspicious process. I disconnected the machine to prevent further spread of the malware

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-L1KK9LG\Yomi]

The screenshot shows the Windows Task Manager with a context menu open over a Microsoft Edge process. The menu options include: Window, Set Affinity..., Set Priority, Kill Process (highlighted with a yellow circle), Kill Process Tree, Shift+Del, Restart, Suspend, Create Dump, Check VirusTotal.com, and Properties... .

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
dlhost.exe	1.47	5,740 K	6,424 K	944	COM Surrogate	Microsoft Corporation	0/79
SkypeHelper.exe	Susp...	1,960 K	0 K	5512	Microsoft Skype	Microsoft Corporation	0/78
YourPhone.exe	Susp...	23,808 K	0 K	5528	YourPhone	Microsoft Corporation	0/79
Skype4Life.exe	Susp...	149,872 K	0 K	5588	SkypeApp	Microsoft Corporation	0/78
RuntimeBroker.exe		6,252 K	52 K	5636	Runtime Broker	Microsoft Corporation	0/78
smartscreen.exe		16,104 K	9,252 K	5792	Windows Defender SmartScr...	Microsoft Corporation	0/78
RuntimeBroker.exe		5,320 K	1,584 K	2168	Runtime Broker	Microsoft Corporation	0/78
WinStore.App.exe	Susp...	16,020 K	0 K	6132	Store	Microsoft Corporation	0/76
RuntimeBroker.exe		1,524 K	0 K	4672	Runtime Broker	Microsoft Corporation	0/78
MicrosoftEdge.exe	< 0.01	22,292 K	62,456 K	11448	Microsoft Edge	Microsoft Corporation	0/73
browser_broker.exe		1,840 K	7,348 K	10552	Browser_Broker	Microsoft Corporation	0/76
MicrosoftEdge				166,916 K	7592 Microsoft Edge Content Proc...	Microsoft Corporation	0/76
svchost.exe				7,296 K	844 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				14,016 K	332 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				13,836 K	2796 Shell Infrastructure Host	Microsoft Corporation	0/78
svchost.exe				7,304 K	612 Host Process for Windows T...	Microsoft Corporation	0/78
svchost.exe				0 K	2984	The sys...	
svchost.exe				3,320 K	464 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				5,008 K	320 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				5,224 K	684 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				2,792 K	644 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				6,088 K	3176	The sys...	
svchost.exe				0 K	1228 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				3,792 K	1288 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				0 K	1616 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				3,168 K	1668 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				0 K	1804 Host Process for Windows S...	Microsoft Corporation	0/79
svchost.exe				0 K	1812 Host Process for Windows S...	Microsoft Corporation	0/79

I deleted the malware file and the registry changes made by the malware were removed.