ICTCYS407

Gather, analyse and interpret threat data

Assessment 5 of 5

Project

Assessor Guide

Version 1

Assessment Instructions

Task Overview

This Project assessment is divided into three (3) parts. Read the simulated environment setup and resource information in Part A and complete the associated tasks in Parts B to G. Project tasks include conducting practical tasks in analytic platforms, and completing simulated workplace documentation and/or templated written communication, such as emails.

Please provide all required screenshot evidence and written responses in the spaces provided.

Important: Before commencing your work, you must update your *Student name* and *Student number* in the footer from **page 2** onwards.

Additional Resources and Supporting Documents

ICTCYS407_05_Project_Scenario documents (compressed/zipped folder) - This folder contains the following scenario documents and templates required for completing the tasks in this assessment.

- WayneEnterprises_Email_template.docx
- WayneEnterprises_Threat Analysis Report_template.docx
- WayneEnterprises_Stakeholder Communication Policy.pdf

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the Learning Platform. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Part A: Simulated environment setup and resources

All tasks in this assessment refer to a simulated environment where conditions are typical of a work environment that is experienced in the cybersecurity threat analysis field of work.

Read the following details carefully before completing the tasks in Part B.

A1. Equipment and resources

To carry out the assigned job tasks in the cybersecurity threat analysis field of work, you must have access to:

- a computer installed with an operating system
- a reliable internet connection
- industry software packages such as:
  - Web browsing software (e.g. Microsoft Edge, Firefox, Chrome, Safari)
  - Microsoft Office software (e.g. WORD, Excel)
  - A PDF reader

A2. Analytical platform and applicable user instructions

To carry out cybersecurity threat analysis you must have access to:

- a Splunk user account
  Note: You can sign up for a Splunk account using your student email address.
- Splunk Enterprise – a popular and industry-accepted SIEM platform that allows you to gather, analyse and interpret threat data.
  - Refer to the applicable user instructions provided by Splunk to familiarise yourself with how to conduct searches and obtain results.
- the resources provided by the hands-on workshop 'Investigating Ransomware with Splunk'. Enrol to this workshop by logging into 'https://bots.splunk.com/' using your Splunk username and password at https://bots.splunk.com/workshop/6tyhaKn3uc7yAkUrMg2BVl.
  - Under the 'Resources' section of this workshop, you'll be provided with the link and credentials to access a cloud-hosted version of the 'Splunk Enterprise'.
  - The required datasets for this activity have already been ingested into the analytical platform. Using this dataset (botsv1), you are required to obtain and analyse results.
  - Go through the following sections of the workshop to understand the details of the scenario and the specifics of the dataset you will be investigating.
    - Introduction to Investigating
    - Getting started with the Companion App
    - Setting the Scene

A3. Organisational policies and procedures

Your role

You are hired as a **Cybersecurity Analyst** by Wayne Corporation to be part of a threat investigation project. You are responsible for gathering threat data from various sources, then analyse and interpret information for threats, inconsistencies and discrepancies.

You are provided with the following organisational policies, procedures and document templates required for your job tasks.

- **WayneEnterprises_Email_template.docx** - This template is referred to in the 'WayneEnterprises_Stakeholder communications policy.pdf' and must be used when drafting emails to Wayne Enterprises' stakeholders.
- **WayneEnterprises_Threat Analysis Report_template.docx** – This report template should be used when reporting on the analysis of identified threat data within the organisation's systems.
- **WayneEnterprises_Stakeholder communications policy.pdf** – includes organisational procedures, communication protocols and standards used when engaging with key stakeholders in the organisation and also includes records management, document access and sharing procedures.

Part B: Obtain and analyse threat data

For this part of the assessment, you must:

- read the scenario carefully
- access the required resources outlined in Part A of this assessment
- obtain and analyse results from the 'botsv1' dataset using the 'Splunk Enterprise' platform.

Scenario:

You are tasked with investigating a ransomware attack that occurred at Wayne Enterprises on the 24th of August 2016. Bob Smith's workstation (we8105desk) was the victim of this attack.

At the time of the incident, it was reported that the victim's workstation was connected to a file server.

Tasks:

Obtain results from the "botsv1" dataset to find out the following information relevant to the ransomware attack.

B1. The victim's workstation's IP address

B2. File server details (FQDN, hostname, IP address)

For the above information (B1 and B2), you must

- demonstrate that the results you have obtained are reliable and consistent. You can do this by using different search criteria and statistical analysis to check whether the results are the same.
- provide evidence of completing the task by including the following in 'Table 1':
  - 1-3 screenshots demonstrating how you performed this task using the analytical platform.
  - a description of your analysis of the results (Word count: 75-100 words) that may include:
    - the method(s) used to obtain results (i.e. search criterion used)
    - an interpretation of the results
    - any reasonable assumptions made during the analysis
    - comparison of mathematical data (number of events, IP addresses and other relevant metrics)
    - comments on how you ensured that the result is reliable and consistent.

Evidence of performing the task(s):

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

The students may use different wording in their responses. However, the provided details must reflect the characteristics described in the following benchmark answers.

The students may use a variety of search criteria and methods to obtain the following information:

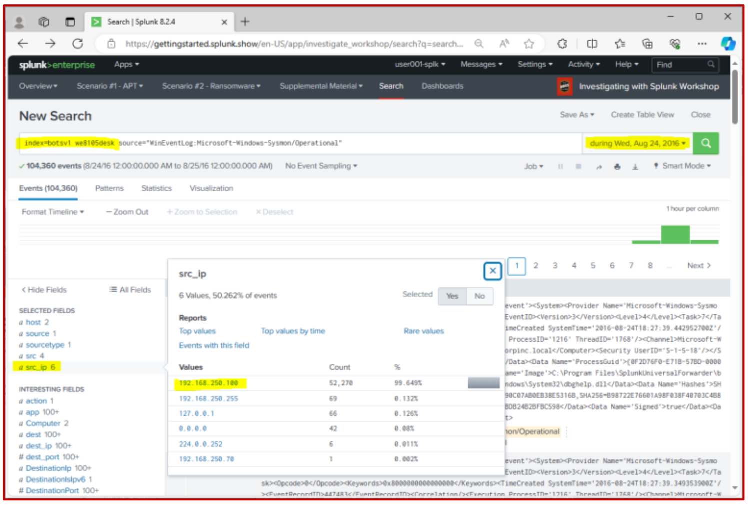
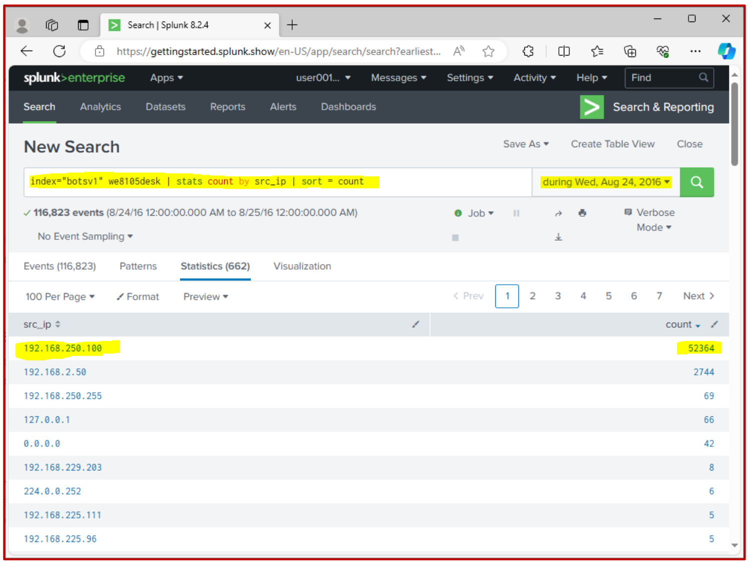
- The IP address of the victim's workstation: 192.168.250.100
- Details of the file server that Bob's workstation was connected to. (server name: WE9041SRV, IP Address: 192.168.250.20, FQDN: we9041srv.waynecorpinc.local)

To ensure that the results obtained are reliable and consistent, the student may:

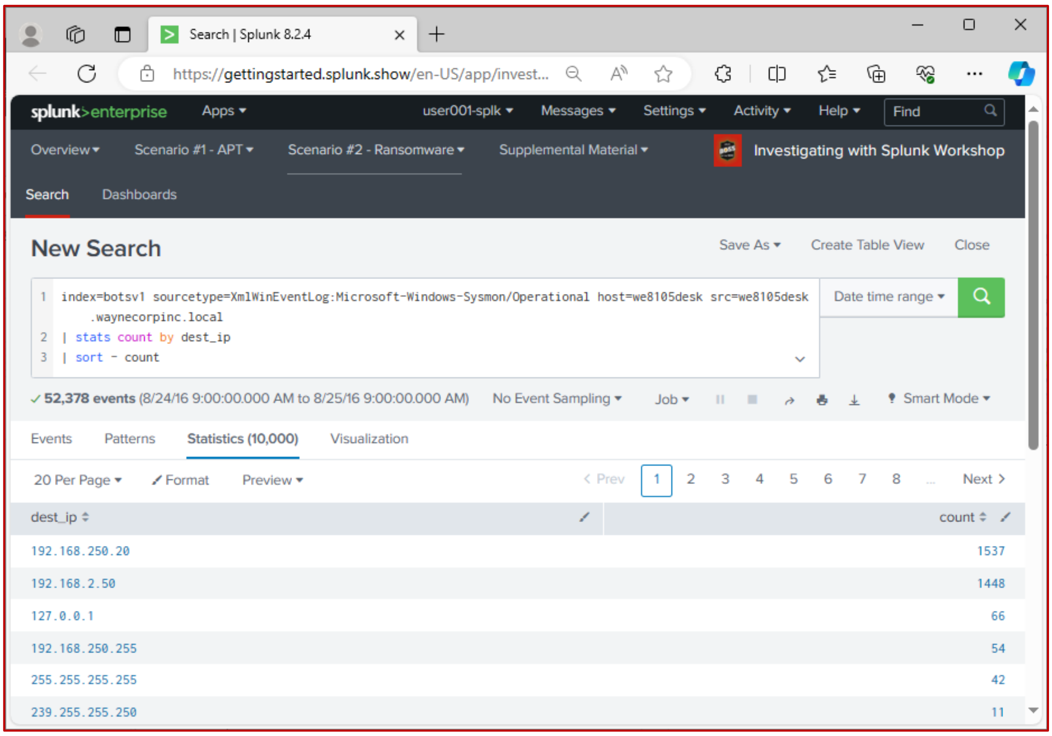
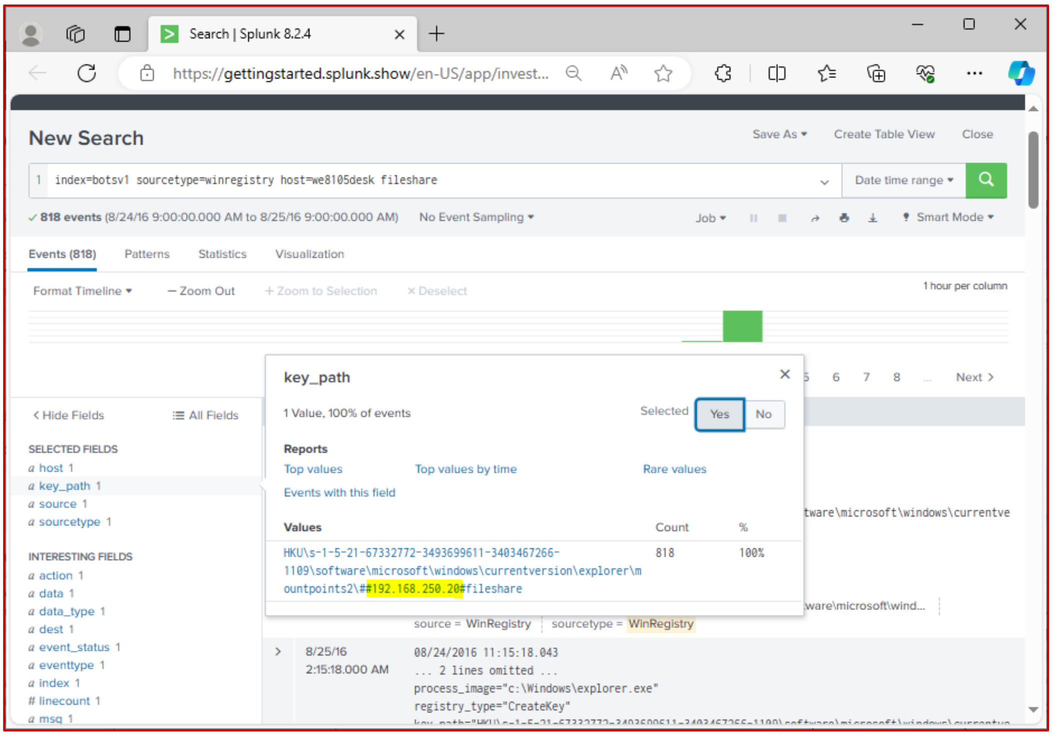
- present how they used different search criteria to obtain the same result
- find additional information for confirmation by performing a 'Google' search or by referring to technical articles or vulnerability databases.

A sample answer is provided below.

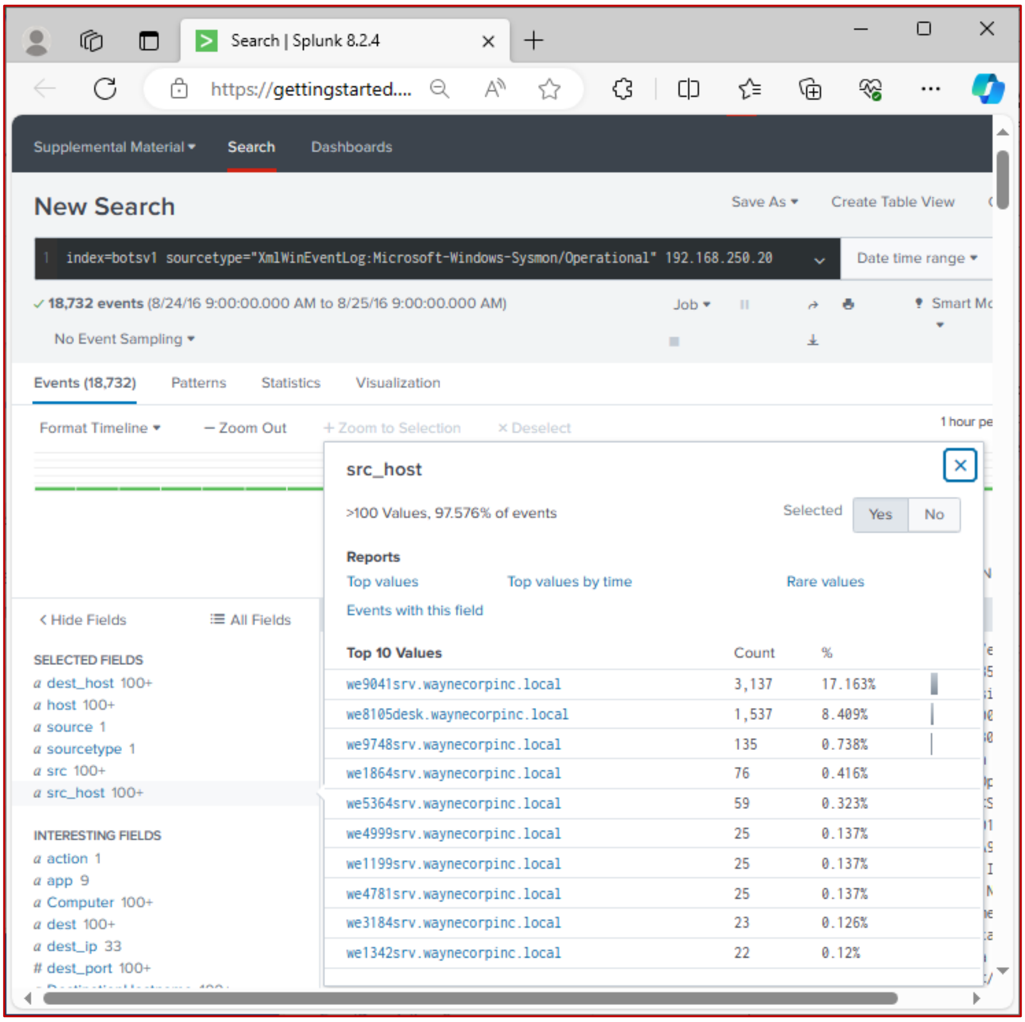
Table 1 - Part B answer table.

Type of information	Screenshot evidence and description of analysis
B1. The victim's workstation's IP address	Screenshot 1 – Shows the criteria used to find the victim's workstation (we8105desk) IP address  `index=botsv1 we8105desk source="WinEventLog:Microsoft-Windows-Sysmon/Operational"` during Wed, Aug 24, 2016 ✓ 104,360 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) src_ip 6 Values, 50.262% of events Values / Count / % 192.168.250.100 / 52,270 / 99.649% 192.168.250.255 / 69 / 0.132% 127.0.0.1 / 66 / 0.126% 0.0.0.0 / 42 / 0.08% 224.0.0.252 / 6 / 0.011% 192.168.250.70 / 1 / 0.002% Screenshot 2 - Evidence of conducting statistical analysis to verify results  `index="botsv1" we8105desk | stats count by src_ip | sort = count` during Wed, Aug 24, 2016 ✓ 116,823 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) Statistics (662) src_ip / count 192.168.250.100 / 52364 192.168.2.50 / 2744 192.168.250.255 / 69 127.0.0.1 / 66 0.0.0.0 / 42 192.168.229.203 / 8 224.0.0.252 / 6 192.168.225.111 / 5 192.168.225.96 / 5

Type of information	Screenshot evidence and description of analysis
	Description of the analysis (Word count: 75-100 words) As shown in Screenshot 1 - Over 99% of the values for src_ip come from the IP address 192.168.250.100, Based on this information, a reasonable assumption can be made regarding the IP address of the victim's workstation to be 192.168.250.100. According to Screenshot 2, criteria had been used to provide statistical information regarding the source ip addresses for the date of the attack. This further confirms the IP address of the victim's workstation to be 192.168.250.100.

B2. File server details (FQDN, hostname, IP address)	Screenshot 1
	
	`index=botsv1 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational host=we8105desk src=we8105desk .waynecorpinc.local`
	`| stats count by dest_ip`
	`| sort - count`
	✓ 52,378 events (8/24/16 9:00:00.000 AM to 8/25/16 9:00:00.000 AM)
	Statistics (10,000)
	dest_ip — count
	192.168.250.20 — 1537
	192.168.2.50 — 1448
	127.0.0.1 — 66
	192.168.250.255 — 54
	255.255.255.255 — 42
	239.255.255.250 — 11
	Screenshot 2
	
	`index=botsv1 sourcetype=winregistry host=we8105desk fileshare`
	✓ 818 events (8/24/16 9:00:00.000 AM to 8/25/16 9:00:00.000 AM)
	key_path
	1 Value, 100% of events
	Values — Count — %
	HKU\s-1-5-21-67332772-3493699611-3403467266-1109\software\microsoft\windows\currentversion\explorer\mountpoints2\##192.168.250.20#fileshare — 818 — 100%
	source = WinRegistry sourcetype = WinRegistry
	8/25/16 2:15:18.000 AM
	08/24/2016 11:15:18.043
	... 2 lines omitted ...
	process_image="c:\Windows\explorer.exe"
	registry_type="CreateKey"

Type of information	Screenshot evidence and description of analysis
	Screenshot 3



New Search

```
index=botsv1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 192.168.250.20
```

✓ 18,732 events (8/24/16 9:00:00.000 AM to 8/25/16 9:00:00.000 AM)

No Event Sampling ▾

SELECTED FIELDS
- a dest_host 100+
- a host 100+
- a source 1
- a sourcetype 1
- a src 100+
- a src_host 100+

INTERESTING FIELDS
- a action 1
- a app 9
- a Computer 100+
- a dest 100+
- a dest_ip 33
- # dest_port 100+

src_host

>100 Values, 97.576% of events

Top 10 Values	Count	%
we9041srv.waynecorpinc.local	3,137	17.163%
we8105desk.waynecorpinc.local	1,537	8.409%
we9748srv.waynecorpinc.local	135	0.738%
we1864srv.waynecorpinc.local	76	0.416%
we5364srv.waynecorpinc.local	59	0.323%
we4999srv.waynecorpinc.local	25	0.137%
we1199srv.waynecorpinc.local	25	0.137%
we4781srv.waynecorpinc.local	25	0.137%
we3184srv.waynecorpinc.local	23	0.126%
we1342srv.waynecorpinc.local	22	0.12%

Description of the analysis (Word count: 75-10 words)

Screenshot 1 shows the search for registry data related to the victim's host we8105desk.

According to the search results, 192.168.250.20 and 192.168.2.50 both have a large number of logs associated with the victim's machine. Therefore another search was required to further clarify these findings.

From the result of 'Screenshot 2' looking at the 'key_path' values, the IP address can be identified as 192.168.250.20 all logs seem to have the same key_path value.

Screenshot 3 further shows the 'src_host' values where the Fully Qualified Domain Name (FQDN) of the file server can be identified as we904srv.waynecorpinc.local

Part C: Detect discrepancies and inconsistencies

For this part of the assessment, you must:

- read the scenario carefully
- access the required resources outlined in Part A sections A1 and A2 of this assessment
- obtain and analyse results from the 'botsv1' dataset using the 'Splunk Enterprise' platform.

Scenario:

'Wayne Enterprises' uses the Suricata IDS system. They have detected the 'Cerber' malware, which at its initial infection phase, had run a VB script and downloaded a file that contains the malware crypto code.

There is also a suspicion that Bob Smith may have visited a malicious website that would've caused the ransomware attack.

You are tasked with detecting any discrepancies and inconsistencies within the captured Suricata alerts within the dataset to find out information about the malicious domains, suspicious files and malware crypto codes.

Tasks:

Task C1

Identify the malicious website and domain(s) visited by Bob Smith on the day of the ransomware attack.

You must:

a. provide 1-3 screenshots demonstrating how you performed this task using the analytical platform.
b. provide a description of your analysis. (Word count: 100-135 words) that outlines:
    - the search criterion used to filter out irrelevant information
    - the reason(s) why the identified domain(s) is/are considered suspicious/malicious.

Evidence of performing the task 1:

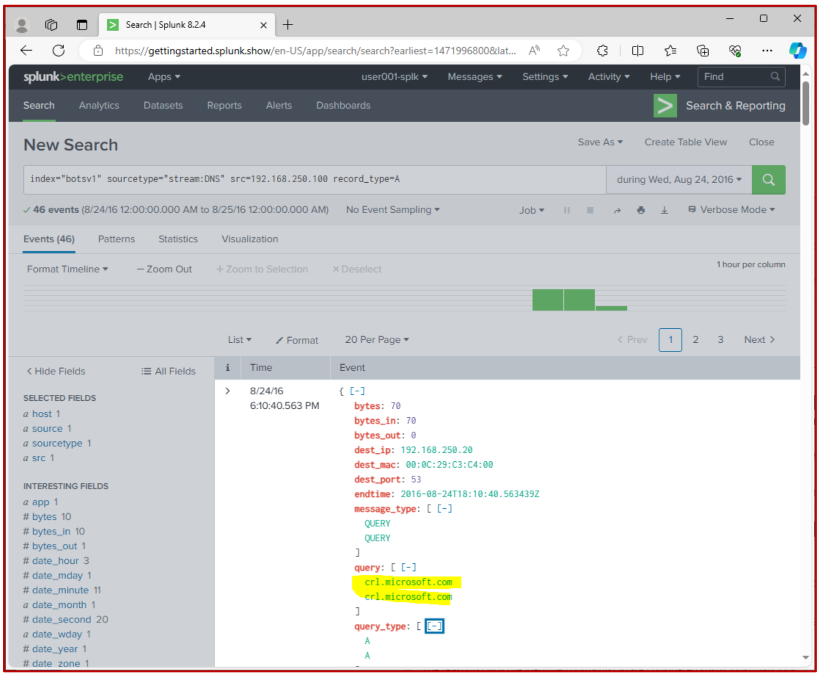
Provide evidence of performing the task along with screenshots and a brief explanation here.

Assessor instructions: Students must:

- identify inconsistencies and discrepancies within the data related to the suspicious domain.
- correctly interpret information from the analysis. The interpretation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
    - be within the specified word limit
    - reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Screenshot 1



```
index="botsv1" sourcetype="stream:DNS" src=192.168.250.100 record_type=A
```

during Wed, Aug 24, 2016

✓ 46 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM)

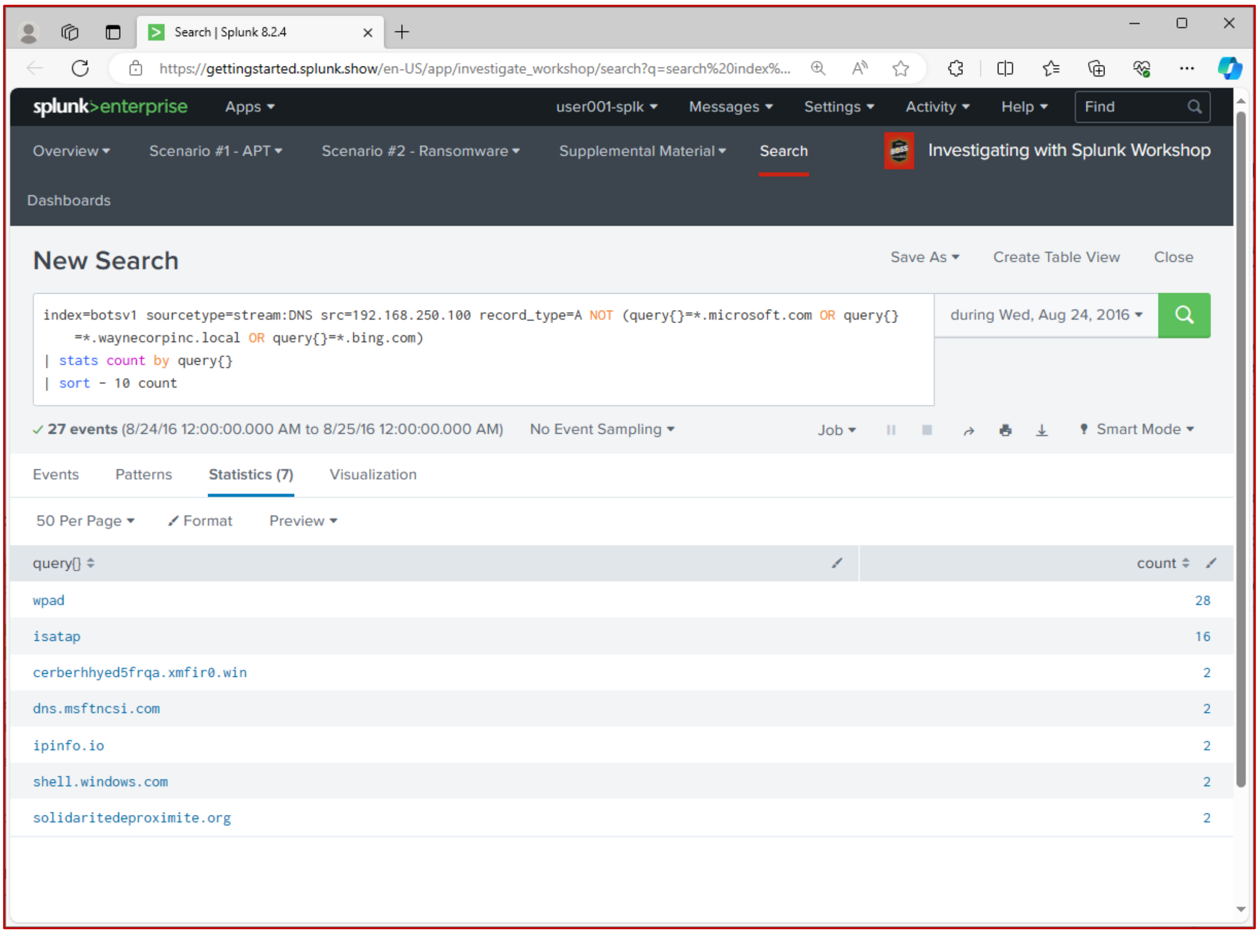
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a src 1

INTERESTING FIELDS
a app 1
# bytes 10
# bytes_in 10
# bytes_out 1
# date_hour 3
# date_mday 1
# date_minute 11
a date_month 1
# date_second 20
a date_wday 1
# date_year 1
# date_zone 1

8/24/16 6:10:40.563 PM

```
{ [-]
   bytes: 70
   bytes_in: 70
   bytes_out: 0
   dest_ip: 192.168.250.20
   dest_mac: 00:0C:29:C3:C4:00
   dest_port: 53
   endtime: 2016-08-24T18:10:40.563439Z
   message_type: [ [-]
     QUERY
     QUERY
   ]
   query: [ [-]
     crl.microsoft.com
     crl.microsoft.com
   ]
   query_type: [ [-]
     A
     A
```

Screenshot 2

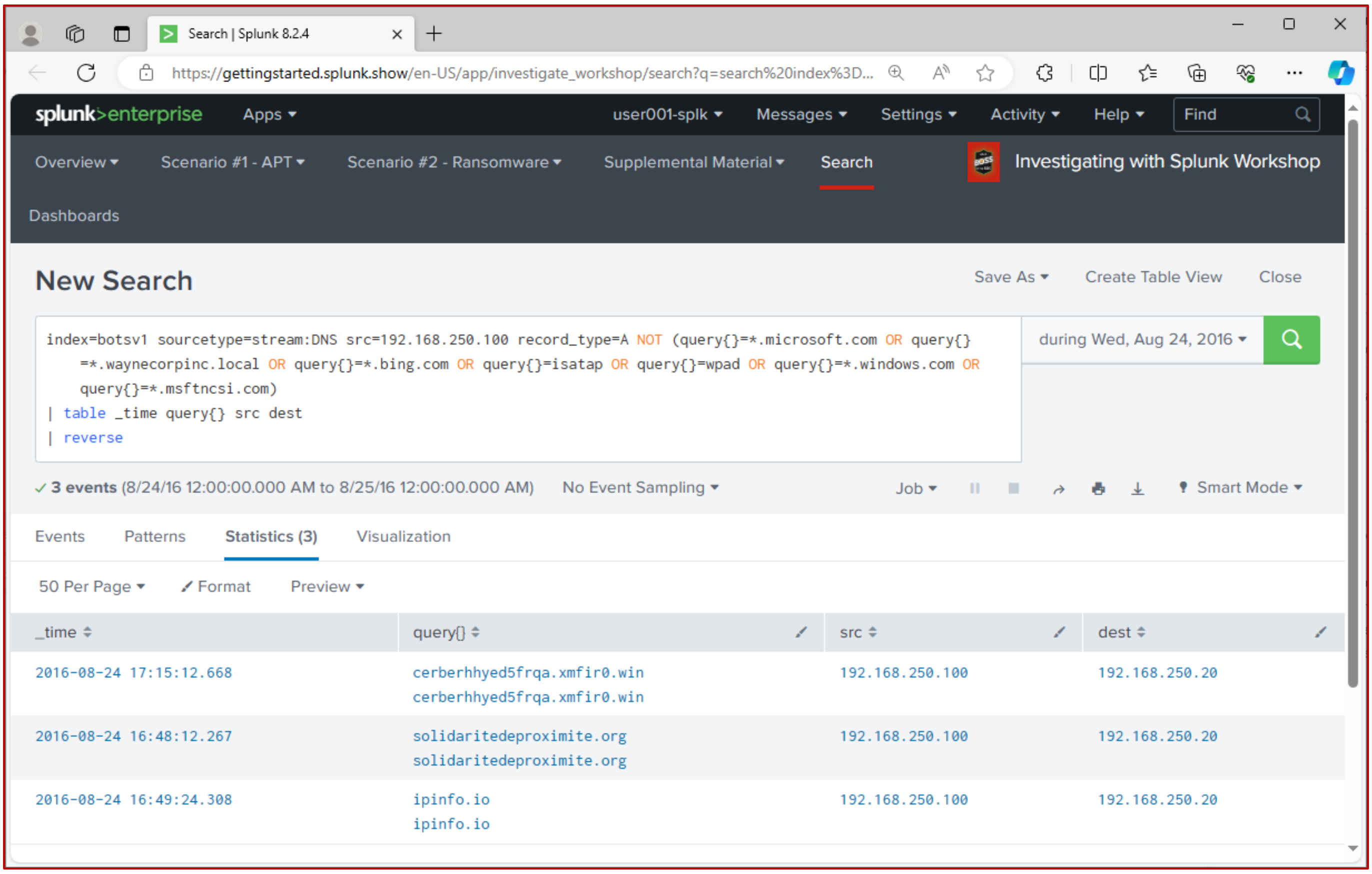


```
index=botsv1 sourcetype=stream:DNS src=192.168.250.100 record_type=A NOT (query{}=*.microsoft.com OR query{}
    =*.waynecorpinc.local OR query{}=*.bing.com)
| stats count by query{}
| sort - 10 count
```

✓ 27 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM)

query{}	count
wpad	28
isatap	16
cerberhhyed5frqa.xmfir0.win	2
dns.msftncsi.com	2
ipinfo.io	2
shell.windows.com	2
solidaritedeproximite.org	2

Screenshot 3



```
index=botsv1 sourcetype=stream:DNS src=192.168.250.100 record_type=A NOT (query{}=*.microsoft.com OR query{}
    =*.waynecorpinc.local OR query{}=*.bing.com OR query{}=isatap OR query{}=wpad OR query{}=*.windows.com OR
    query{}=*.msftncsi.com)
| table _time query{} src dest
| reverse
```

✓ 3 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM)

_time	query{}	src	dest
2016-08-24 17:15:12.668	cerberhhyed5frqa.xmfir0.win cerberhhyed5frqa.xmfir0.win	192.168.250.100	192.168.250.20
2016-08-24 16:48:12.267	solidaritedeproximite.org solidaritedeproximite.org	192.168.250.100	192.168.250.20
2016-08-24 16:49:24.308	ipinfo.io ipinfo.io	192.168.250.100	192.168.250.20

Description of the analysis (Word count: 100-135 words)

In screenshot 1, the search for domain name is refined further to result in DNS records of type 'A' we can see DNS queries going out to different sites.

Domains from reputed sites like microsoft.com, google.com are not likely to be malicious domains. Therefore, any domains that are not of interest need to be filtered out.

Screenshot 2 shows how popular domains are filtered out of the search.

Used the Google search engine to find out more information on wpad and isatap. These can be eliminated from the result as they are not of a concern according to the Google search data.

The search is further refined by conducting a quick 'whois' check.

Screenshot 3 shows how the search is further refined to identify suspicious domain as solidaritedeproximite.org having the IP address: 92.222.104.182.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C2

Examine Suricata alerts to find the signatures that detected the Cerber malware. Check the results for false positives and identify which alert signatures were generated by the actual ransomware attack.

You must:

a. provide 1-3 screenshots demonstrating how you performed this task using the analytical platform.
b. provide a description of your analysis. (Word count: 55-85 words) that outlines:
    - the search criterion used to filter out irrelevant information
    - the process for checking the result for false positives
    - the reason(s) why the identified data/information is considered suspicious/malicious.

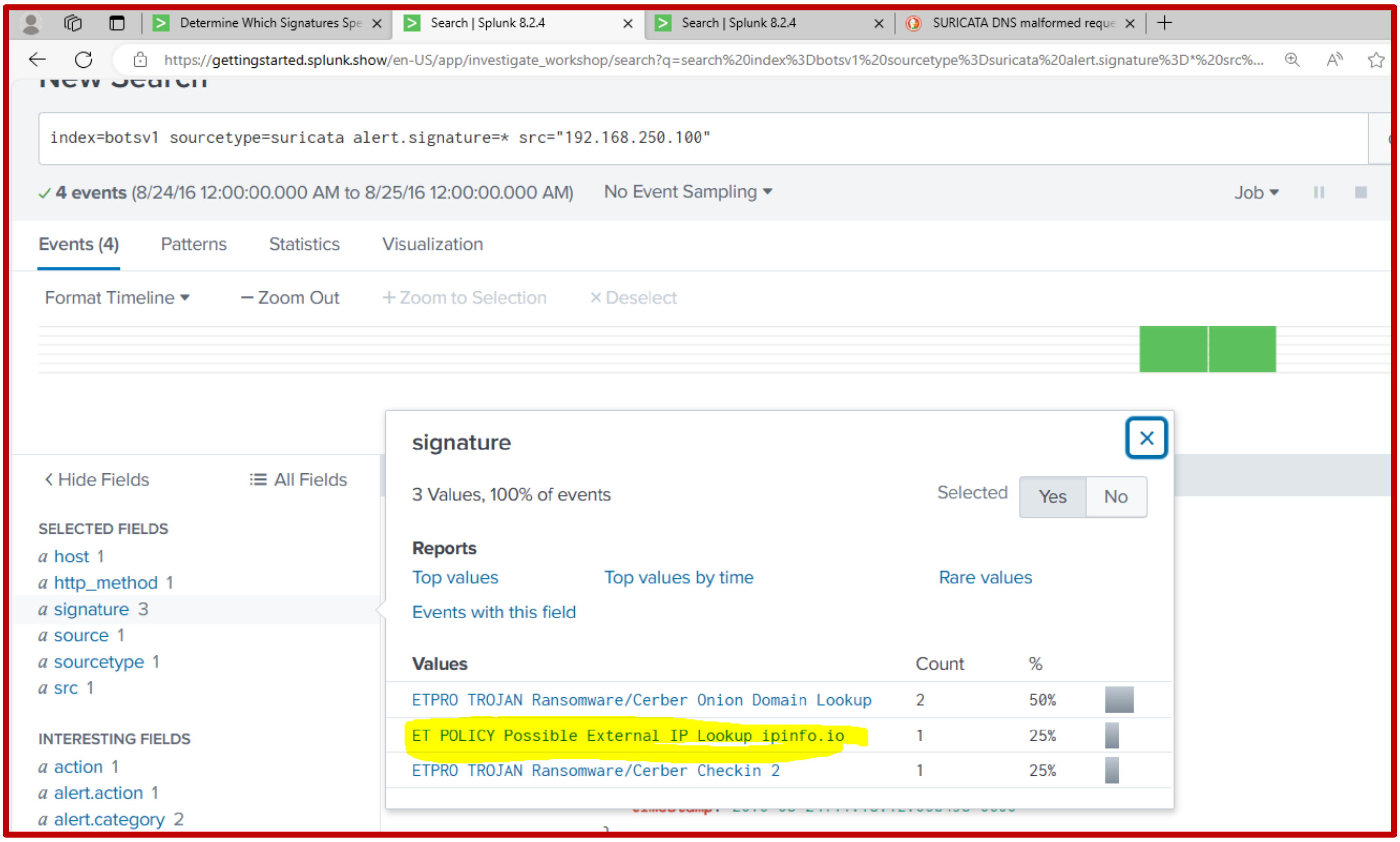
Evidence of performing the task 2:

Assessor instructions: Students must:

- check for false positive results
- identify inconsistencies and discrepancies within the data related to Suricata signature alerts.
- correctly interpret information from the analysis. The interpretation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
    - be within the specified word limit
    - reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Screenshot 1



```
index=botsv1 sourcetype=suricata alert.signature=* src="192.168.250.100"
```

✓ 4 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) No Event Sampling

signature

3 Values, 100% of events Selected: Yes No

Reports: Top values, Top values by time, Rare values, Events with this field

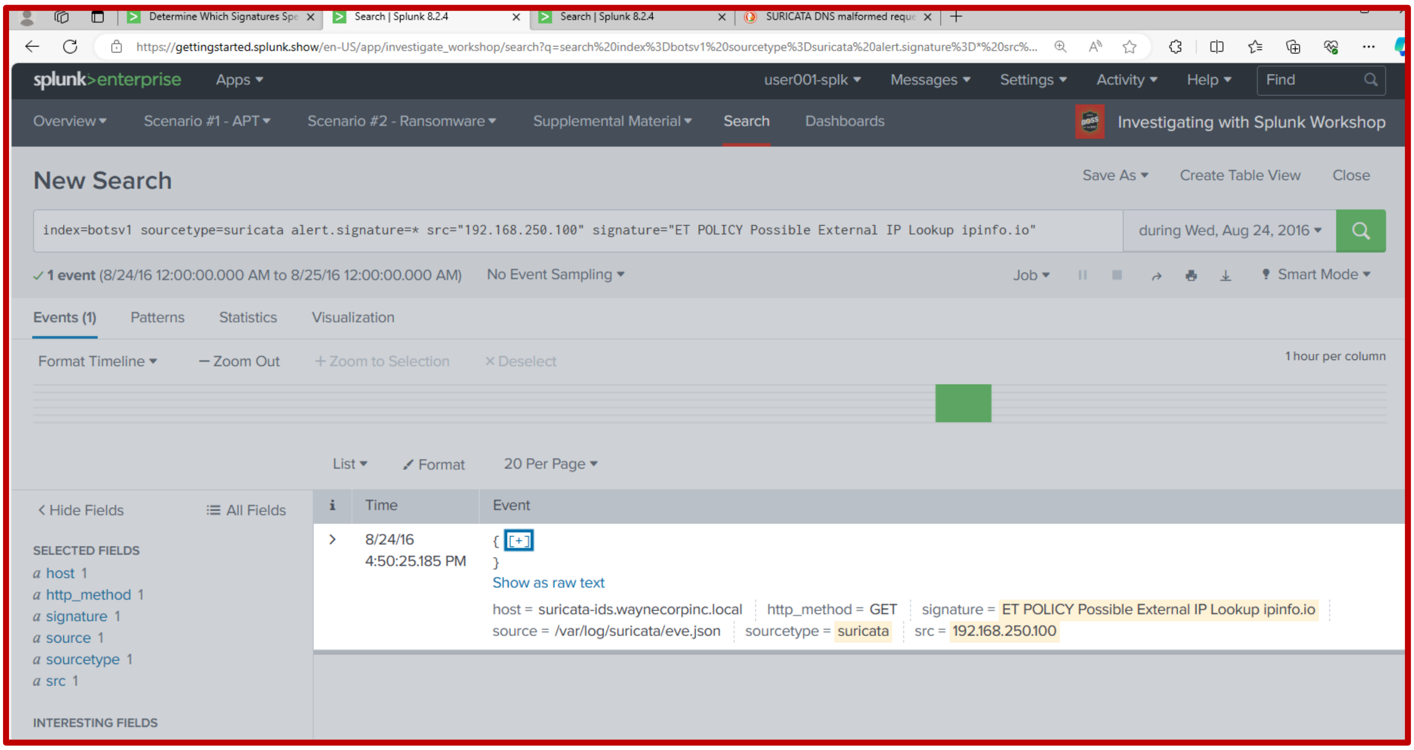
Values	Count	%
ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup	2	50%
ET POLICY Possible External IP Lookup ipinfo.io	1	25%
ETPRO TROJAN Ransomware/Cerber Checkin 2	1	25%

SELECTED FIELDS: a host 1, a http_method 1, a signature 3, a source 1, a sourcetype 1, a src 1

INTERESTING FIELDS: a action 1, a alert.action 1, a alert.category 2

Determine Which Signatures Spe
Search | Splunk 8.2.4
Search | Splunk 8.2.4
SURICATA DNS malformed reque
https://gettingstarted.splunk.show/en-US/app/investigate_workshop/search?q=search%20index%3Dbotsv1%20sourcetype%3Dsuricata%20alert.signature%3D*%20src%...
Job
Events (4)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
‹ Hide Fields
☰ All Fields

Screenshot 2



New Search

```
index=botsv1 sourcetype=suricata alert.signature=* src="192.168.250.100" signature="ET POLICY Possible External IP Lookup ipinfo.io"
```

during Wed, Aug 24, 2016

✓ 1 event (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) No Event Sampling

i	Time	Event

›	8/24/16 4:50:25.185 PM	{ [+] }
		Show as raw text
		host = suricata-ids.waynecorpinc.local http_method = GET signature = ET POLICY Possible External IP Lookup ipinfo.io
		source = /var/log/suricata/eve.json sourcetype = suricata src = 192.168.250.100

SELECTED FIELDS: a host 1, a http_method 1, a signature 1, a source 1, a sourcetype 1, a src 1

INTERESTING FIELDS

Description of the analysis

Screenshot 1 shows the search results displaying 3 Suricata IDS alerts originating from the victim's IP address which is 192.168.250.100.

After looking into each Suricata alert, the specific alert details in Screenshot 2 shows that it is relevant to the local domain waynecorpinc.local. Evaluation of the source IP address further confirms that it is generated by local internal traffic, which poses no threat. So, it can be identified as a false positive.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C3

Examine the Suricata IDS system alerts to check for false negative results related to the suspicious domain visited by Bob Smith on the day of the attack.

You must:

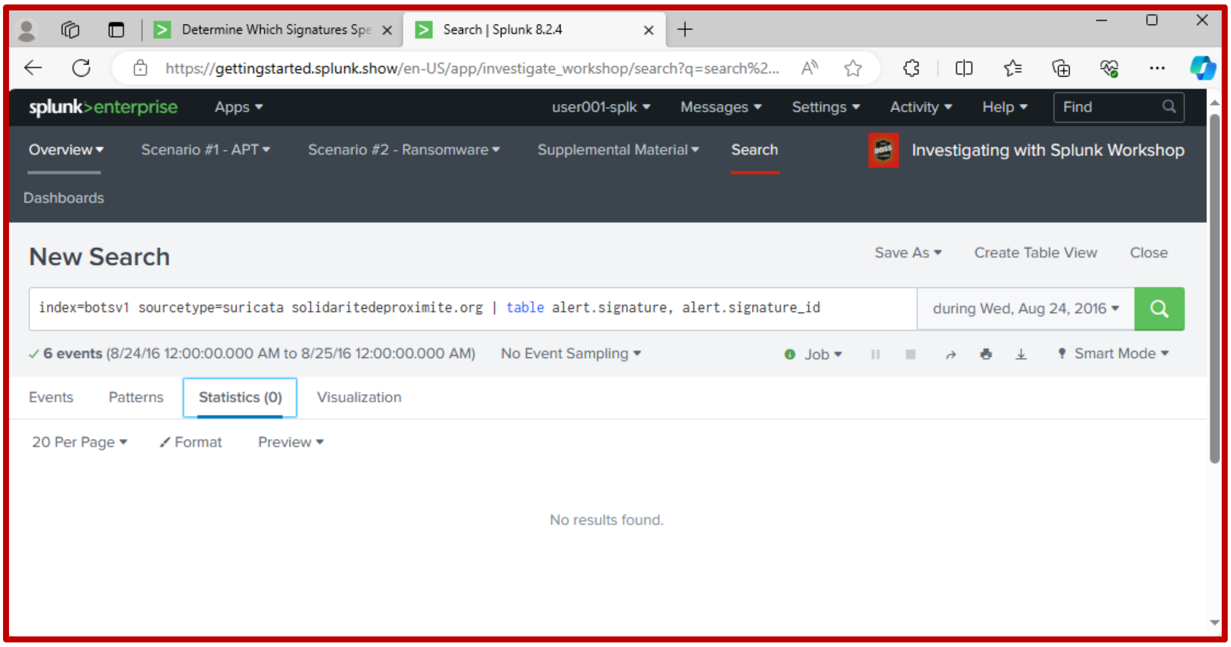
a. provide 1-3 screenshots demonstrating how you performed this task using the analytical platform.
b. provide a description of your analysis. (Word count: 40-75 words) that outlines:
   - the search criterion used to filter out irrelevant information
   - the reason(s) for identifying the result as a false negative.

Evidence of performing the task 3:

Assessor instructions: Students must:

- check for false negative results. If the student can identify an event that is related to the ransomware attack with IDS signatures that are not captured by an alert by the Suricata IDS system, then that is evidence of checking for false negatives.
- identify inconsistencies and discrepancies within the data related to Suricata signature alerts for the suspicious domain.
- correctly interpret information from the analysis. The interpretation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
   - be within the specified word limit
   - reflect the characteristics described in the exemplar answer.

A sample answer is provided below.



```
index=botsv1 sourcetype=suricata solidaritedeproximite.org | table alert.signature, alert.signature_id
```

✓ 6 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM)

No results found.

Description of the analysis

The malicious domain was previously identified as solidaritedeproximite.org.

As shown in the screenshot, the search criterion was used to find Suricata signature alerts, which contains information related to solidaritedeproximite.org

However, according to the search results, the Suricata IDS system did not generate any alerts related to the malicious domain solidaritedeproximite.org. Therefore, this can be identified as a false negative result.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Part D: Discuss and review threat data and results

To complete this part of the assessment, you are required to:

- refer to the organisational documentation and templates outlined in Part A, section A3 of this assessment
- refer to the threat data that you have gathered, analysed and interpreted in Parts B and C of this assessment
- discuss and review threat data results with required personnel in the organisation via email.

Scenario:

Wayne Corporation

After completing your initial analysis of the threat data results, you are now required to discuss and review the results of your analysis with the following key stakeholders of 'Wayne Enterprises'.

- Meryl Green– Chief Security Officer
- Steven Brown– Information Technology (IT) Manager

In your discussion with the key stakeholders, you will make suggestions for any lessons learnt, action steps, recommendations and risk mitigation strategies.

Tasks:

Do the following tasks in correspondence with Wayne Corporation's key stakeholders.

D1. Discuss and review threat data and results

D2. Discuss and assess identified threats, risk and their likelihood of occurrence and impacts of risks

D3. Suggest and confirm with required personnel:

a. lessons learnt
b. required action steps
c. recommendations
d. mitigation strategies.

As evidence of completing this task, you must:

- Email the information related to your discussion to the required personnel and obtain their responses for confirmation. You must specifically discuss the details of each task in the body of the Email using appropriate technical language (Word count: 150 – 200 words).

- Provide evidence of your discussion with the required personnel and confirmation obtained from them via Email correspondence using your student email. Provide screenshot(s) of the sent email as well as the responses received confirming the required information (Use Wayne Corporation's standard email template).

Evidence of performing the task(s):

Provide here screenshot(s) of the sent and received emails.

Assessor instructions: The student must:

- discuss and review threat results via email
- demonstrate learning skills for identifying and gathering information applicable to organisatioal procedures and threat data.
- demonstrate the use of problem-solving skills when interpreting the nature and impact of threat data.
- use organisational template for completing the task (Wayne Corporation Email template)

Students are likely to use different wording than the answer guidelines provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the answer guidelines

Answer guidelines are as follows:

D1: The student's discussion and review of threat data results should relate to the threat data and analysis findings from Parts B and C of this assessment by providing a summary of what they found. For example:

- Bob's workstation (we8105desk) IP address = 192.168.2.50
- File server hostname and IP address and FQDN: WE9041SRV, 192.168.250.100, we9041srv.waynecorpinc.local
- Malicious domain visited by the user: solidaritedeproximite.org
- Malware downloaded: Ransomware - 'Cerber'
- The analysis found that the incoming traffic from the malicious domain was not detected by the Suricata IDS system and therefore no alert was generated.

D2: The student's discussion and assessment of threat results may include, but are not limited to the following:

- **identified threats:** For example, The Cerber malware was downloaded from a malicious website visited by the Bob Smith's workstation.
- **risk and their likelihood of occurrence:** For example, a basic risk matrix, listing the risks and their likelihood of occurrence
- **Impacts of risks** – For example, loss of data, revenue, and reputation.

D3: The student's suggestions and confirmation of analysis results may include, but are not limited to the following:

- **Lessons learnt** –This can include any discoveries or realisations that the organisation encountered during the threat data analysis and what can be implemented to prevent similar attacks from happening again.
- **Action steps** – For example, providing user awareness training and blocking access to harmful websites,

- **Recommendations** – For example, encrypting data, regular data backups, risk assessments and automatic vulnerability checks, prevention of data loss, user awareness training, update policies, disaster recovery planning.
- **Mitigation strategies** – For example, user awareness training, implementation of early detection systems to block malicious traffic, real-time monitoring of threats, analysis and regular reporting.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments: ☐ S ☐ NYS

Part E: Create a threat analysis report

To complete this part of the assessment, you are required to:

- refer to the relevant organisational documentation and templates outlined in Part A, section A3 of this assessment
- refer to the threat data that you have gathered, analysed and interpreted in Parts B and C of this assessment
- refer to the discussion, review, and suggestions on threat data results in Part D of this assessment
- prepare complex workplace documentation detailing research findings and recommendations and outcomes using the required structure, layout and technical language.

Scenario:

You have reviewed and discussed your analysis of the threat data with Wayne Corporation's key stakeholders. They have also confirmed the lessons learnt, required action steps, recommendations and risk mitigation strategies that you proposed to them previously via Email.

You are now tasked with documenting the results and findings in a formal report according to the organisation's reporting structure and layout.

Tasks:

Create a report of your threat data analysis using the organisation's report template. Your report must include the following:

- Threat data results and outcomes
- Findings (including details of identified threats, risks and their likelihood of occurrence and impacts of risks)
- Recommendations and outcomes (including any mitigation strategies for identified risks)

Use point form in your report where suitable (Word count: 175 – 250 words)

Evidence of performing the task(s):

IMPORTANT: You must upload a copy of your completed threat analysis report with this assessment document for marking.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments: ☐ S ☐ NYS

The student must demonstrate learning skills by identifying applicable organisational procedures for creating reports.

Students are likely to use different wording than the answer guidelines provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the answer guidelines
- use the organisation's report template.

Wayne Enterprises

Threat Analysis Report

Incident Details

Date of incident:	24 August 2016
Incident description:	Ransomware attack on the user (Bob Smith's) workstation (we8105desk)
Business impact: (i.e. relevant to CIA triad)	The ransomware attack had encrypted the data, which compromised the data integrity. This also resulted in impacting the availability of the data for the business.
Requirements:	Access to data logs from the Wayne Enterprises' network system Access to analytical platform.
Analyst:	<Student Name>
Key stakeholder(s):	Meryl Green– Chief Security Officer Steven Brown– Information Technology (IT) Manager

Threat Analysis Summary

Threat data results and outcomes	Specific information found during the analysis includes the following: - Bob's workstation (we8105desk) IP address = 192.168.2.50 - File server hostname: WE9041SRV - File server IP address: 192.168.250.100 - File server FQDN: we9041srv.waynecorpinc.local
Findings (i.e. details of threats, risks and their likelihood of occurrence and impacts of risks)	A malicious domain solidaritedeproximite.org was accessed by the user (Bob Smith), which downloaded the 'Cerber' malware. However, the incoming traffic from the malicious domain was not detected by the Suricata IDS system and therefore no alert was generated. ● Risks and their likelihood of occurance - (Assessor Instructions: Students should include provide here a basic risk matrix) ● Impacts of risks are loss of data, revenue and reputation as well as business downtime and having to pay the ransom.
Recommendations (i.e. mitigation	**Recommendations:** ○ User awareness training

strategies for identified risks]	○ Encrypt data ○ Backup data to onsite as well as offsite locations ○ Blocking access to suspicious domains ○ Tune the Suricata IDS system to generate alerts from suspicious domains ○ Restrict malicious file downloads and execution ○ Setup active monitoring tools, so that incidents can be detected faster and be prevented in a timely manner ○ Policy updates ○ Disaster recovery **Mitigation strategies:** • Review user training strategy and conduct user awareness training for all staff. • Ensure anti-malware tools, IDS and IPS systems are up to date and are properly tuned in order to notify, detect and prevent similar attacks.

Part F: Store documentation

To complete this part of the assessment, you are required to:

- refer to the relevant organisational policies and procedure documents outlined in Part A, section A3 of this assessment
- use the threat data analysis report you created in Part E of this assessment
- store threat data documentation to key stakeholders following organisational policy and procedure.

Scenario:

You have created a threat analysis report documenting the results and findings. Now you are tasked with storing the documentation according to the organisation's records management policy and procedures outlined in section 2 of the 'WayneEnterprises_Stakeholder communications policy.pdf'.

Tasks:

Rename and save the threat data analysis documents appropriately according to the organisation's records management procedure.

Note: Assume that your Student account's OneDrive is the organisation's cloud storage. Create a folder in your OneDrive called 'Wayne Enterprises' and demonstrate how you would store the threat analysis documentation within this folder. Provide a screenshot as evidence of storing the documentation under 'Evidence of performing the task(s)'.

Evidence of performing the task(s):

Provide here a screenshot(s) showing how threat analysis documentation is stored.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

The screenshot provided by the student should indicate a folder structure on the student's OneDrive cloud storage, similar to the following, to show that they have followed the organisation's policies and procedures for storing documents. Note: The version number (e.g. V1.0, V2.0) may differ depending on the document revisions the student would have worked on before the final version is created.

A sample answer is provided below.

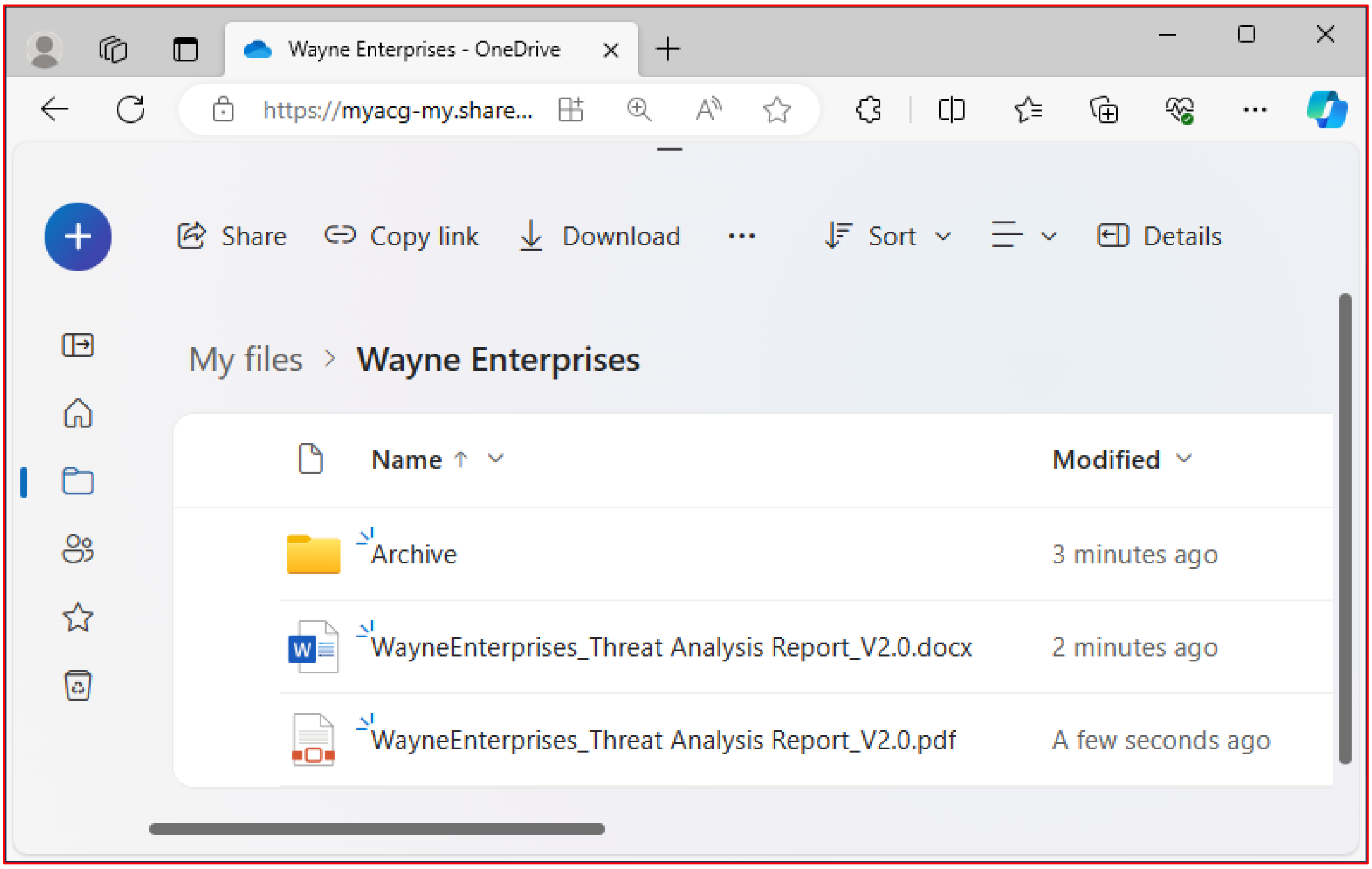
WayneEnterprises_Cyber Threat Analysis

Archive

- WayneEnterprises_Threat Analysis Report_V1.0.docx

WayneEnterprises_Cyber Threat Analysis Report_V2.0.docx

WayneEnterprises_Cyber Threat Analysis Report_V2.0.pdf


Wayne Enterprises - OneDrive
https://myacg-my.share...
Share
Copy link
Download
Sort
Details
My files > Wayne Enterprises

Name	Modified
Archive	3 minutes ago
WayneEnterprises_Threat Analysis Report_V2.0.docx	2 minutes ago
WayneEnterprises_Threat Analysis Report_V2.0.pdf	A few seconds ago

Part G: Distribute documentation

To complete this part of the assessment, you are required to:

- refer to the relevant organisational policies and procedure documents in Part A, section A3 of this assessment
- use the threat data analysis report you have stored in Part F of this assessment
- distribute threat data documentation to key stakeholders following organisational policy and procedure.

Scenario:

You have prepared a threat analysis report and have stored it in the cloud storage according to Wayne Enterprises' policies and procedures.

The key stakeholders Meryl Green (Chief Security Officer) and Steven Brown (Information Technology Manager) have requested you to send them a copy of the completed threat analysis report for reference.

To ensure the key stakeholders can access the distributed document, you will follow Wayne Enterprises' document access and sharing policy and procedures outlined in section 3 of the 'WayneEnterprises_Stakeholder communications policy.pdf'.

Tasks:

Distribute the threat data analysis report to the key stakeholders following organisational policy and procedures.

To demonstrate completion of this task, you must provide a screenshot showing the share settings of the document. The captured screenshot must provide evidence that you are:

- sharing the document with the key stakeholders
- granting only the required level of access to the key stakeholders
- including a brief message to provide context to the shared document (Word count: 25 – 35 words).

Evidence of performing the task(s):

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments: ☐ S ☐ NYS

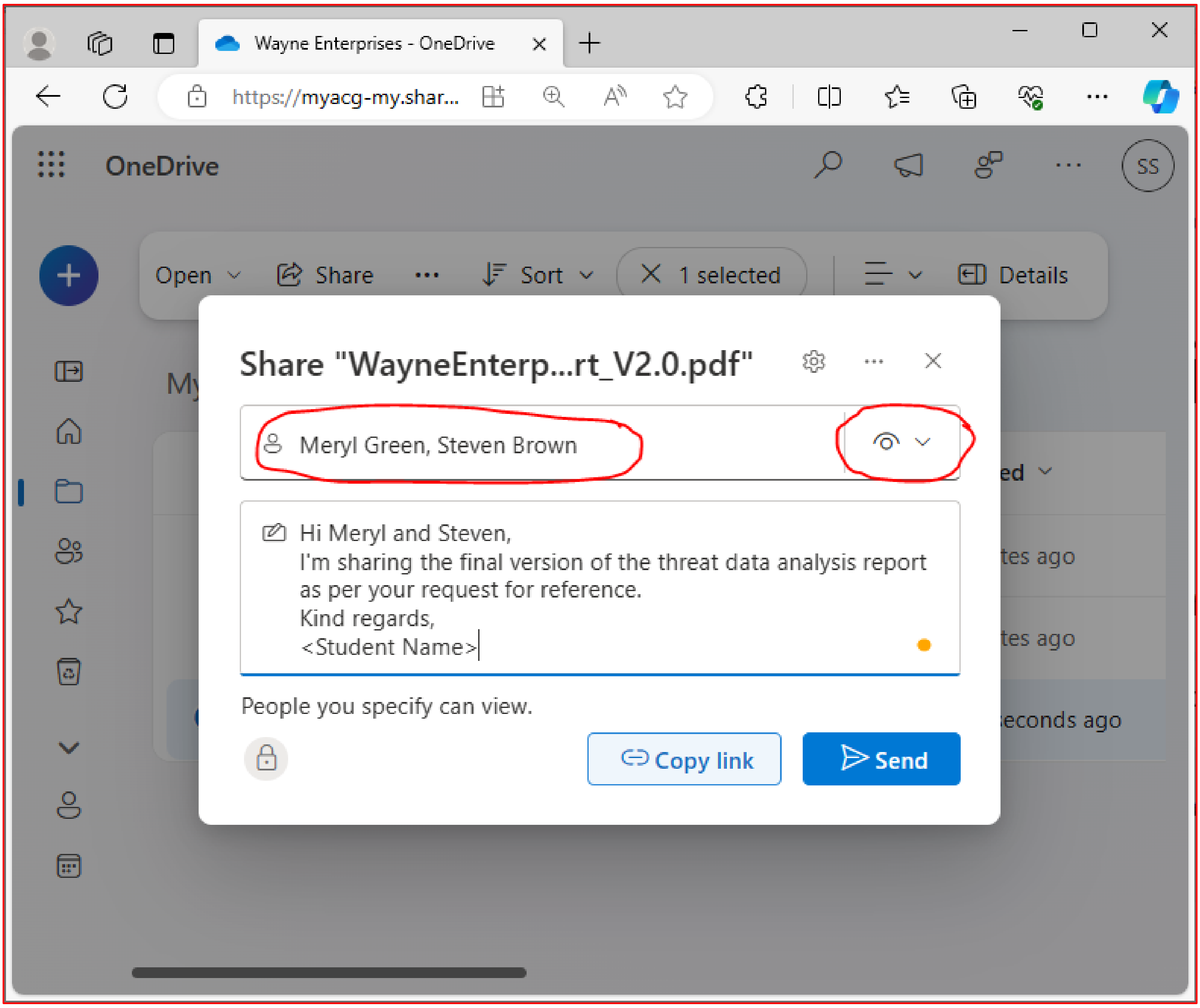
The student must demonstrate:

- learning skills by identifying applicable organisational procedures for distributing threat data documentation
- distributing the threat analysis report via cloud storage share settings
  - addressing the relevant personnel (Meryl Green and Steven Brown)
  - providing 'View' only access
  - including a clear short message indicating what the document is and why it is shared.

    Note: Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

    - be within the specified word limit
    - reflect the characteristics described in the benchmark answer

A sample answer is provided below.



Share "WayneEnterp...rt_V2.0.pdf"

Meryl Green, Steven Brown

Hi Meryl and Steven,
I'm sharing the final version of the threat data analysis report as per your request for reference.
Kind regards,
<Student Name>

People you specify can view.

Appendix 1: Assessment submission checklist

Submit a PDF version of this completed assessment document. Make sure you have also included each of the following files as evidence of your performance. Remember to create a compressed folder for each module before uploading them for submission

Part B: Obtain and analyse threat data		
B1	Key information #1: 1-3 screenshots + description of results	□
B2	Key information #2: 1-3 screenshots + description of results	□
Part C: Obtain and analyse results		
C1	1-3 screenshots + description of results	□
C2	1-3 screenshots + description of results	□
C3	-3 screenshots + description of results	□
Part D: Obtain and analyse results		
	Drafted email to required personnel to discuss requirements and strategy.	□

Part E: Create a threat analysis report		
	Submitted copy of the threat analysis report	□
Part F: Store documentation		
	One (1) screenshot of document storage	□
Part G: Distribute documentation		
	One (1) Screenshot of the share settings of the document in cloud storage.	□

Assessment feedback

Assessors are to indicate the assessment outcome as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

□ S □ NYS

Congratulations, you have reached the Assessment 5!