# Student Version

| Section C – Instructions to students |
| --- |
| **Task instructions:** |
| This assessment is comprised of three parts: Part 1: Flow Charts Part 2: Knowledge Questions Part 3: Splunk Comprehensive Lab  Part 1 Flow Charts: â€¢ Please refer the Supporting Documents for more information on this part of the assessment. In this part of the assessment you are required to answer a range of knowledge questions related to this subject. Some of these questions are more technical and ask you to discuss or explain particular technologies or terminologies while other questions are more holistic or bigger picture focused.   You will also need to answer questions about your incident response process and how you have developed your flowchart. You must answer each question in your own words.   Where you have used images or content from another creator you must make reference to this in the answer space provided. â€¢ You are required to attempt ALL questions and tasks individually  â€¢ Your answers are to be written in your own words. Copy and paste from a research link will not be accepted.  Part B Knowledge Questions: In this assessment you are required to answer a range of knowledge questions related to this subject. Some of these questions are more technical and ask learners to discuss or explain particular technologies or terminologies while other questions are more holistic or bigger picture focused.  â€¢ You are required to attempt ALL questions and tasks individually  â€¢ Your answers are to be written in your own words. Copy and paste from a research link will not be accepted. â€¢ You are required to list all references consulted in the reference box at the end of the assessment. Knowledge   Part 3: Splunk Comprehensive Lab â€¢ Please refer the Supporting Documents for more information on this part of the assessment. For this part of the assessment, you will use Splunk enterprise software to import and analyse â€œBig Dataâ€ for trends and discrepancies. The assessment must be completed individually. On the following pages there are questions for you to answer spilt into three sections. You must complete all sections of the do |

| Section D – Conditions for assessment | |
| --- | --- |
| **Conditions:**  Student to complete and attach Assessment Submission Cover Sheet to the completed Assessment Task. | |
| Conditions:  - This assessment is to be completed individually. - You must meet all criteria listed in the marking guide to be satisfactory in this task. - You may resubmit this task if not successful within the enrolment period as per Holmesglen conducting  assessment procedure. - It is expected all documents will be completed and submitted electronically but if this is not possible, make alternative arrangements for submitting the documents with your assessor. - You will have the opportunity to resubmit if any part of the assessment is deemed unsatisfactory (one resubmit allowed per task). - You can appeal an assessment decision according to the Holmesglen Assessment Complaints and Appeals Procedure. - If you feel you require special allowance or adjustment to this task, please decide with your assessor within one week of commencing this assessment, - The learner may use the internet research answers for this assessment. | |
| **Equipment/resources students must supply:** | **Equipment/resources to be provided by the RTO:** |
| Laptop Computer or Desktop computer or Tablet Writing Materials Active Email External HDD storage / Flash Drive to save a backup copy of your work Internet Access | Desktop Computer Internet Access  Access to BrightSpace |

**Part 1: Flow Charts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Provide your responses in the boxes below each question.** | | | |
| **Question 1:** | **List the SANS Six Steps of Incident Handling** | **Satisfactory response** | |
| Yes | No |
| **Answer: a. Preparation**  b. **Identification**  c. **Containment**  d. **Eradication**  e. **Recovery**  f. **Lessons Learned** | | Comment: | |
| **Question 2:** | **Describe each of the above steps.** | **Satisfactory response** | |
| Yes | No |
| **Answer: a. Preparation-** In this step you anthologize a list of all your wealth, rank them by standing of significance and monitor the cycles so you can produce conclusions to be used for comparisons subsequently. b. **Identification-** Accumulate everything you can on the incident, breakdown it then decide the entry point and the extent of the breach. c. **Containment-** At this step is where you fix the pitfall 's entry point d. **Eradication-** At this step the threat is removed e. **Recovery-** Tries to get the system functioning if it went down. f. **Lessons Learned-** This step provides the occasion to learn from your exploit so you can better react to coming security events. | | Comment: | |
| **Question 3:** | **From the perspective of a L1 SOC Analyst, what information do you have to work with for this scenario? (Refer the scenario given at the end of the document.)** | **Satisfactory response** | |
| Yes | No |
| **Answer:** Companies ticketing system logs The speed of the execution of new requests Unauthorized accounts | | Comment: | |
| **Question 4:** | **What further information do we need to collect to be able to implement the Incident response process? (Refer the scenario given at the end of the document.)** | **Satisfactory response** | |
| Yes | No |
| **Answer:** Contact name and information of the people reporting the Dos attack and phishing attack. Date and time the DOS and phishing incident was noticed. Type and circumstances under which the incidences takes place . The type of data, information, or accoutrements involved throughout the operation of the incident The locus of the Security or isolation Event, data or accoutrements affected; .Whether the Security or isolation Event puts any person or other data at hazard. Any associated ticket ciphering and log entries associated with the Security incidence | | Comment: | |
| **Question 5:** | **Provide both flow charts here.** | **Satisfactory response** | |
| Yes | No |
| **Answer:** | | Comment: | |
| **Question 6:** | **List and describe each of the subtasks for the process flowchart above:** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  **Suspected incident-The security team is notified of the security incident Identification- In this step we confirm the security incident situation, identify the affected devices and systems and estimate the potential damage. Assessment and classification- In this step the security incident is analysed and verified if it really occurred or if it’s a false alarm. Determine incident severity- We countify the disruption of the system from the security incident. If the incident is severity is high, contact the top security officials to inform them of the issue. Convene an incident response team- Assemble all the parties involved in security from human resource to all the personnel that can contain the issue. Incident Containment- Identify investigators, change security tokens and credentials and contain and isolate the network. Incident eradication- Preform forensic backup, remove cause of incident if possible, perform further vulnerabilities assessment and notify all the affected parties. System restoration- Restore the system from the backup. Apply patches and fixes. Well also perform vulnerability audit and verification. Finally, we monitor the system for backdoors. Follow-up activities- Here we record the lesson learned, create a full incident report and notify all parties of the containment of the security threat.** | | Comment: | |
| **Question 7:** | **Describe how you would implement the “Containment” subtasks for this scenario.** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  **I would disconnect any affected devices from the internet and also from the local area network to avoid the spread of the issue to other devices.** **IR team members will be notified to ensure proper timing. The next step is to wipe the data off al the affected machines and reinstall the operating system from the ground up. Block Ip address and domains that have been identified to be used by attackers to compromise the system.** | | Comment: | |
| **Question 8:** | **Do you think the implementation of the above process would be effective?** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  **Sure. The steps outlines follow the industry directives and should be enough to contain and eradicate any threats present.** | | Comment: | |
| **Question 9:** | **On further evaluation, what additional step or changes would you make to the above process given the scenario?** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  **Update the organisations threat intelligence and response and create** | | Comment: | |
| **Question 10:** | **What crucial step is to be implemented upon rectification of the incident?** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  Complete an Incident Report-It will help to enhance the incident response plan and escalate the security measures to avoid correspondent security incidents in the future. Monitor Post-Incident Closely cover for conditioning post-incident since imminence actors will re-appear again. Identify precautionary measures that affect new security ambition to prevent coming incidents. | | Comment: | |
| **Question 11:** | **Why is it important to document lessons learned and how will this useful in the future?** | **Satisfactory response** | |
| Yes | No |
| **Answer: I**t helps you to pinpoint holes in your organizational security practices and equip us with the knowledge of how to handle them in future. It aids you in understanding of not only why the incident happened, but also how effective your response was thus how to act the next time. The successful Basics of your response can help to inform robust coming security practices while agreeing and awarding positive hireling performance will set a standard and incentivize correspondent bearings in the coming | | Comment: | |
| **Question 12:** | **List all the resources you used in your assessment** | **Satisfactory response** | |
| Yes | No |
| **Answer:**  https://cybersheath.com/incident-response-learning-the-lesson-of-lessons-learned/ **https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide**  **https://www.icims.com/gc/incident-response-procedures/ https://digitalguardian.com/blog/five-steps-incident-response** | | Comment: | |

NB: Flow charting has the ability to take a large problem and ‘chunk’ it down into sub-tasks for easier processing.



**Part 2: Knowledge Questions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Provide your responses in the boxes below each question.** | | | |
| **Question 1:** | Big data concepts: Describe with 1 example each of the following:   * 1. Volume   2. Variety   3. Velocity   4. Veracity   5. Variability | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  **a. Volume-** It defines the quantities of data that reach almost incomprehensible proportions which requires distinct and different processing technologies. Example includes user account information b. Variety- refers to all the structured and unstructured data that can be generated either by humans or by machines in an organisation. example includes photos. c. Velocity- It refers to the speed at which data can be created in companies’ system from users and other computers. Example of high velocity data is the post that are being added to Instagram by all its users.  d. Veracity- It refers to the quality and usefulness of the data that is being analysed. Example of high veracity data include results from a science experiment. e. Variability- It defines the quality of the data that is being analysed. Example include incorrect user account details in the database | | Comment: | |
| **Question 2:** | Describe the 3 main types of databases and their typical use. Include in your answer the types of data that would be found in each database | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  **Text database-** Data is organized and stored in text file that contains rows and columns with each row representing an entry in the database. Examples includes bibliography data available in books  **Relational database-** It is structured such that it stores data in relation to another piece of data in the database and the data is organized into tables. Examples include SQL, Oracle  **Object-oriented databases-** It is a database that's grounded on object - oriented programming and the data is represented and stored in the form of objects. Examples include Smalltalk is used in GemStone, LISP is used in Gbase, and COP is used in Vbase | | Comment: | |
| **Question 3:** | Read the following scenario and then answer the accompanying questions.  You work in a db admin team Jo is your team leader. You work in a team of 4 others.  During a routine system test of an ACME Database, typical tests undertaken were domain name research, operating system fingerprinting and port scans. The results of the initial testing revealed no serious issues for the database. The next phase involved application-based testing which resulted in the confirmation of SSL – encrypted forms of authentication.  Whilst testing for injection attacks, the following command was inserted into the login credentials area of the web page – ‘\*’, and a list of user information was returned.  It has also been discovered that Jo, the .db administrator, has sole and full control of access roles on the database. Jo claims that his expertise is sufficient enough to retain this job function and that therefore there should not be any trust issues over having sole control.  It has been established that ACME has appropriate .db backups that are stored online within the physical location of the organization and the same network. There is no evidence of any offline facility.  *Use your knowledge of SQL .db and identify any vulnerabilities.* | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 4:** | There has been an incident reported of a .db breach and Jo is unavailable to take control. You are now tasked with identifying the threats and should note down the steps involved to rectify the incident. | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** Take affected database offline with the goal of stopping any ongoing conditioning by limiting communication to and from the impacted database but not commit any action which might abolish cues, befoul attestation or otherwise inadvertently prop the assaulter. Make sure that the db monitoring has been going on and is intact. However, if the db monitoring is switched off, switch it back on and restore it before doing anything else. Lock credentials to assure the arrest of said breach if it's ongoing. Figure out what happened here; what information was accessed, what systems were compromised, and which accounts may have been utilized. Determine the root cause of the breach weather it weak security policies human error that aided the breach.   Determine the corrective measures that should be carried out to remedy the effects of the data breach and then enact the solutions that you come up with. Inform all the internal personnel about the breach, how it occurred, what details were involved, and what has to be done. The public should also be notified and what has been done to get control of the situation. | | Comment: | |
| **Question 5:** | The use of automation for data collection is an ever-growing feature in recent technology. Explain a technique that has used automation for collecting data, and give a brief explanation of how this information gathered can be analyzed. | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  Optical Character Recognition- is the use of technology to distinguish issued or handwritten handbook characters inside digital images of physical documents, analogous as a checked paper document.  The core process of OCR involves examining the source text and paraphrasing the characters into canon that can be used for data processing.  OCR is sometimes also appertained to as handbook recognition. OCR systems are made up of a combination of accoutrements and software that's used to convert physical documents into machine - readable text Software can also take advantage of artificial intelligence (AI) to administer more advanced forms of intelligent character recognition (ICR), like associating languages or styles of handwriting. | | Comment: | |
| **Question 6:** | Describe the following data sources, making reference to the type of data collected.   1. Firewalls 2. Intrusion Detection System 3. Access Control Systems 4. Security & Event Management Systems | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  1.Firewalls- It captures network traffic data that's captured from the firewalls on a network. Firewalls can combine with other device functions and produce added data, for example proxies and network intrusion discovery data. 2. Intrusion Detection System- It monitors a network's traffic for conditioning that appear to be imminences and - or attempts at infiltrating  a network or system. When a threat is detected the IDS sends alarms to directors who can besides take action. Types of information collected includes internal system files such as operating systems and network traffic logs. 3 Access Control System - Access control is a method of validating and making sure that users are who they say they are and that they have the appropriate access to company data. Information collected include user credentials like username and password. 4. Security and event management systems- It's a software solution that combines and analyses conditioning from multiple different devices across the entire IT Infrastructure of a company. SIEM collects security data from network leaning, garçons, front controls. | | Comment: | |
| **Reference URL links:**  **https://www.varonis.com/blog/what-is-siem/**  **https://en.wikipedia.org/wiki/Security\_information\_and\_event\_management**  **https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html**  **https://smb.avast.com/answers/intrusion-detection-system-ids**  **https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7**  https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7 https://processflows.co.uk/direct/process-automation-components/data-capture/methods-of-data-capture/ https://www.sciencedirect.com/science/article/abs/pii/036083529190091J https://cybersheath.com/incident-response-learning-the-lesson-of-lessons-learned/ https://www.igi-global.com/gateway/article/249229#pnlRecommendationForm https://www.tutorialspoint.com/Types-of-databases https://www.techrepublic.com/article/8-steps-to-take-within-48-hours-of-a-data-breach/ | | | |

**Part 3: Splunk Comprehensive Lab**

|  |  |  |  |
| --- | --- | --- | --- |
| **Provide your responses in the boxes below each question.** | | | |
| **Section 1: Splunk Setup** | | | |
| **Question 1:** | **What is Splunk and what does it do?** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  Splunk is a platform that enables one to search, analyse and visualize the machine-generated data that is gathered from various sources that make up the IT infrastructure of an organization | | Comment: | |
| **Question 2:** | **Which version of Splunk will you be using for this assessment task?** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
|  | | Comment: | |
| **Question 3:** | **Create two users for your Splunk setup. One user must have an administrator role and the other user have be a Power User role. Take a screenshot of your Users accounts page after you have added both users.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 4:** | **Describe one benefit of having different user roles and access levels** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:**  **It reduces the amount of work done by the IT staff- If different users have different roles and access levels, the administration can reduce the use of paper work and password changes when an employee is hired of acquires a new role, since you can simply add roles or switch roles.** | | Comment: | |
| **Section 2: Adding data to Splunk** | | | |
| **Question 1:** | **List and describe 3 different data source types you can use in Splunk.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** Files and directories- This is the data that comes from various folders and files. Network events- This data comes from any system logs of various processes. Examples include system log files and application logs.Windows sources- This is type of data that is unique to the windows operating system. Examples include windows event log data, windows registry data and performance monitoring data. | | Comment: | |
| **Question 2:** | **Import the “db\_audit\_30DAY.csv" data source into Splunk and rename the data source to “db\_audit – (YourName)”. Take a screenshot of the review page once completed.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 3:** | **Import the “linux\_s\_30DAY.log " data source into Splunk and rename the data source to “web\_server – (YourName)”. Take a screenshot of the review page once completed.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 4:** | **Import the “access\_30DAY " data source into Splunk and rename the data source to “Web\_application – (YourName)”.Take a screenshot of the review page once completed.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Section 3: Data Analysing** | | | |
| **Question 1:** | **Perform a basic search for errors and any type of failures in all data sources. Provide a screenshot of the entire page once completed.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 2:** | **Perform a new search for password and any type of failures on port 22 in all data sources. Provide a screenshot of the entire page once completed.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 3:** | **Do you see trends over time? If so, what was it?** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 4:** | **Use the output of your search to refine the results by adding a new field to the search** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Question 5:** | **Take a screenshot of your ‘Activity Jobs Menu’ detailing the current job saved with expiration date.** | **Satisfactory response** | |
| Yes ☐ | No ☐ |
| **Answer:** | | Comment: | |
| **Reference URL links:** | | | |

| **Criteria for assessment** | | **Satisfactory** | | **Comment** |
| --- | --- | --- | --- | --- |
| **Yes** | **No** |
| **The following has been submitted for assessment:** | | | | |
| **Section 1: Splunk Setup** | | ☐ | ☐ |  |
| **Section 2: Adding data to Splunk** | | ☐ | ☐ |  |
| **Section 3: Data Analysing** | | ☐ | ☐ |  |
| **Marking criteria for each product document/s supplied:** | | | | |
| 1. | Access to data in a database is demonstrated | ☐ | ☐ |  |
| 2. | Detecting discrepancies in data is described and performed | ☐ | ☐ |  |
| 3. | Pattern recognition is demonstrated | ☐ | ☐ |  |
| 4. | Detecting anomalies in data is identified | ☐ | ☐ |  |
| 5. | Software tools to support the detection of anomalies and discrepancies are demonstrated | ☐ | ☐ |  |
| 6. | Common software tools to identify data patterns are identified and demonstrated | ☐ | ☐ |  |
| 7. | Using data recognition software tools | ☐ | ☐ |  |
| 8. | Reading and comprehending documented material and procedures | ☐ | ☐ |  |
| 9. | Inputting data to a database | ☐ | ☐ |  |
| 10. | Accessing data from a database | ☐ | ☐ |  |
| 12. | Splunk as an example of software used in data analysis | ☐ | ☐ |  |

**Supporting document**

# Assessment Submission Cover Sheet (VET)

Student to complete relevant sections and attach this cover sheet to each assessment task for submission.

**Note:**

**Assessor to attach a photocopy of the completed Marking Guide (Section E) from the Student version of the Assessment Task.**

**Final result of the subject/unit will be entered on Banner by the teacher/assessor once all assessment tasks have been assessed.**

**Part 1: Flow Charts**

**Background Information:**

You are a Level 1 Security Analyst at Techno Intelligence Threat Systems SOC and are tasked with developing processes for the following incidents that were received by the company ticketing system. The incidents are:

* Suspected DDoS Attack
* Suspected Phishing Attack

Your Critical Incident Response Team (CIRT) have implemented the PICERL model to develop an incident response process for each of the incidents detected.

The process/response that you develop for BOTH incidents MUST BE submitted as a flowchart. Each step of your response should be reflected in your flow chart, and should include a brief description outlining any symptoms, reasons to support the process of decision-making.

**As a guide you may follow the SANS Six (6) Steps of Incident Handling in your flowchart You will need to research both incidents to the point where you have a basic understanding of each event and can then formulate a process of mitigation.**

**Your response must be in the form of a flow chart and answer the accompanied questions. Each step in your flowchart sequence MUST be represented with the correct symbol.**

**Your flowchart should cover the following steps:**

**• symptoms of the event/incident**

**• identification**

**• probable course of action**

**• containment strategies**

**• mitigation**

**• any other information you deem to be necessary**

**Answer the following questions about your incident response process and how you have developed your flowchart. You must answer each question in your own words. This is an individual assessment task.**

***Where you have used images or content from another creator you must make reference to this in the answer space provided.***

**Part 3: Splunk Comprehensive Lab**

For this assessment task, you will use Splunk enterprise software to import and analyse “Big Data” for trends and discrepancies. The assessment must be completed individually. On the following pages there are questions for you to answer spilt into three sections. You must complete all sections of the document satisfactorily.

**Section 1: Splunk Setup**

**Section 2: Adding data to Splunk**

**Section 3: Data Analysing**

**Section 1: Splunk Setup**

In this section, you will be assessed on how you setup and configure your Splunk environment ready for data sources. You will be required to setup two user accounts of different access levels.

• User 1 must be an administrator

• User 2 must have a power user role

**Section 2: Adding data to Splunk**

In this section, you will be assessed on your knowledge of Big data types and how they can be imported and configured inside of Splunk. You will setup data for a range of sources including web access log, Linux web server and database records.

**Section 3: Data Analysing**

In this section, you will be assessed on your ability to refine searches, detect abnormalities and view trend data in the given data sources.

For this assessment, you will be given three data source files to import and configure to answer the questions on the next pages. These files can be found on Brightspace under Week 4 Resources. If you are having trouble locating the files, please contact your instructor ASAP.