Cybersecurity

- Make sure your browser is up to date with the latest version(???????????)
- it might be used to determine whether or not to lock an account. (??????)
- checks whether someone is allowed to access a particular file (??...; ??????)
- improve efficiency; allow it to work effectively (????; ????)
- use Python code to reduce the manual effort needed to manage an access control list(????;)
- Throughout this certificate you will use Qwiklabs and Jupyter Notebooks to complete hands-on activities???????????
- Security analysts can access Python through a variety of environments??????
- The fast.log file is used for basic logging and alerting and is considered a legacy file format???...????
- The Network-based IDS application inspects network traffic from different devices on the network???/???
- When suspicious or unusual network activity is detected??????????
- IDS (Intrusion Detection System) is an application that monitors activity and alerts on possible intrusions.??????????????
- Detection requires data, and this data can come from various data sources.?????
- It’s important to know how to read and interpret different log formats so that you can uncover the key details surrounding an event and identify unusual or malicious activity.??????????????
- logs provide key details about activities that occurred across an organization????
- logs record events that happen on a network, or system.????
- intrusion detection systems; intrusion prevent systems (IDS;IPS)
- investigating an alert involving a possible network intrusion??????
- When an outage occurs due to a security incident???????????
- Business Continuity Plan?BCP ???????
- the three letters in the CIA triad stand for confidentiality, integrity, and availability ??????????????????
- ensure that you complete a thorough analysis so that you have enough information to make an informed decision about your findings.???????????????
- you'll receive and assess the alert to determine if it's a false positive??????/???????
- which prioritizes incidents according to their level of importance or urgency .???????????
- Having previously investigated the file hash, it is confirmed to be a known malicious file.?????????????????????
- The email body and subject line contained grammatical errors.??????
- Tedious, error-prone, or time-consuming tasks can be automated, while analysts can prioritize their time with other tasks.??????????????...?
- It is an example of a non-automated playbook, which requires step-by-step actions performed by an analyst.????????
- This depicts the process for detecting a DDoS and begins with determining the indicators of compromise, like unknown incoming traffic.???????????

- Documentation must be regularly reviewed and updated to keep up with the evolving threat landscape. (??????????????????????)
- Incident response plans standardize an organization’s response process by outlining procedures in advance of an incident. (?????)
- If a malicious actor compromised a system, evidence must be available to determine their actions so that appropriate legal action can be taken. (?????????)
- You observe a known user successfully authenticate a new device using two-factor (???; ???)
- Security terms
  - malicious actors (?????)
  - malicious activity (????)
  - attackers (???)
  - security incidents (????;????)
  - security analysts (?????; ?????)
  - security professionals (????; ????)
  - the suspicious IP address (???)
  - unusual processes (????)
- IoCs may be the result of human error, system malfunctions, and other reasons not related to security. (????; ????)
- baselines help establish a standard of expected or normal behavior for systems, devices, and networks. (??)
- A baseline is a reference point that’s used for comparison. (baseline ?...)
- Once something unusual or suspicious is detected (?????????)
- How could the company prevent an incident like this from occurring again???????????????
- the stages of incident detection, investigation, analysis, and response???????????????
- analyze the contents of captured packets???????
- The app should be in compliance with PCI-DSS.???/???
- developers tend to focus on making their applications work correctly rather than protecting their products from injection.??????...?????????
- Malware??????
  - Virus????
  - Worm????
  - Trojan????
  - Ransomware??????
  - Spyware??????
- analyzing the suspicious message?????
- the group managed to gain access to the organization’s network and internal tools.????????...????
- Threat actors use many different tactics to carry out their attacks.?????????????
- unauthorized access to restricted systems.???????; ?????
- specific type of attacks that cybercriminals commonly use. (????)
- using fictitious emails to evaluate security awareness at the company. (????)
- Keeping software updated requires effort. (?????????????)
- Vulnerability scanners are meant to be non-intrusive. (??; ????)
- Examples of remediation steps might include things like enforcing (??)
- We'll explore this step in more details (????)

- An employee reports that they cannot log into the payroll system with their access credentials. (????; ????)
- Symmetric and asymmetric encryption (????????)
- keep private; keep safe (????; ????)
- you'll review the controls in place to prevent data leaks. (?????)
- Periodically auditing those accounts is a key part of keeping your company's systems secure.???; ??...???
- Score risks based on their severity (???)
- So much of the global marketplace has shifted to cloud-based services. (???)
- As the environment continues to transform, (?...??)
- Don't get discouraged now; Don't let anyone discourage you from cybersecurity. (????)
- Suppose you wanted to know what department the employee using ...????
- The principle of least privilege is the concept of granting only the minimal access and authorization required to complete a task or function. ????????
- we use u to represent the user, g to represent the group???; ???
- its output indicates that the working directory is logs ???; ???
- Although it took some practice and time to get used to, it has been one of the biggest tools ...??????????????
- you'll become much more familiar with????????
- it might happen because we don't have the appropriate permissions to perform a command. (???)
- I misspelled the command????
- the bash shell is the most commonly used shell in the ...???????
- You might examine different types of logs to identify what's going on in the system. (??; ??????????)
- Almost everyone learned on their own by experimenting (??????)
- These individuals will likely already have experience using GUIs (???; ??)
- security analysts commonly use a CLI in their everyday work (??; ?????)
- using a GUI is more like ordering food from a restaurant. (??)
- Using virtual machines can also be an efficient and convenient way to perform security tasks. (??????????????)
- One more aspect to consider is that (??????????)
- The OS is responsible for ensuring that each program is allocating and de-allocating resources. (??; ??)
- A variety of programs, tasks, and processes are ... (????)
- The OS handles resource and memory management to ensure the limited capacity of the computer system is used where it's needed most. (?????????; ??????)
- make sure all the resources of the computer are used efficiently. (???)
- Security analysts should be aware of vulnerabilities that affect operating systems. (?????; ??)
- They run multiple applications at once (??)
- will be an essential part of your job as a security analyst. (??????)
- The shared responsibility model states that the CSP must take responsibility for... (??)
- Brute force attacks are a trial-and-error process of guessing passwords. (????; ????)
- up-to-date; out-of-date (??; ??)
- security hardening involves minimizing the attack surface or potential vulnerabilities and keeping a network as secure as possible. (????; ??/??; ????; ????; ?????????

- refer to; referred to as (??...; ????...)
  - Software as a service, refers to software suites operated by the CSP that a company can use remotely without hosting the software.
  - it is referred to as a hybrid cloud environment.
- Open-source tools and proprietary tools (??/????)
- Analyst; Analysis; Analyze
  - As a security analyst
  - Splunk is a data analysis platform
  - Splunk Enterprise is a self-hosted tool used to retain, analyze and search the log data to provide security information and alert in real-time
- From there I managed to get myself into a security vendor and learn security (?????, ??????????????????)

Revision #75
Created 6 September 2024 14:03:56 by Admin
Updated 20 September 2024 13:10:23 by Admin