Cybersecurity

- Social media is a great way to connect to other security professionals in the industry ??????????????????????
- By staying informed about security trends, you can more effectively identify and develop remediation strategies to address a wide range of security challenges ????(??)????????????????????????????????????
- engaging with the security community through various security organizations and conferences is a great way to stay up-to-date on current security news ????????????????????????????????
- You don't have to know everything. You have teammates and other people that can help you with areas that you're weak in ????????????????????????????
- I take courses, try to get certificates if I can along the way ????????????????????????
- It's important to continue to learn in the field of cybersecurity because things change all the time ????????????????????????
- always remember not to click on unexpected links or attachments sent from unfamiliar users on social media. ????????????????????????????
- Be aware of social engineering ??????
- it’s also important to be mindful that hackers use social media to trick users into giving up private information ????????????????????????
- Are you interested in forensic security or data logging ??????????????????
- focus on reacting to security incidents or preventing them from happening ????????????????????
- Security is a constantly evolving industry. As professionals in security, we must evolve with it by seeking out new information. ???)??????????????????(??)????????????????????????????
- A few well-known security websites and blogs to get you started are ?????????? blog ?
- will help you stand out to hiring managers and could give you an extra edge over other candidates????????????????????????????????????
- What excites me about the security profession is??????????????????
- a few good resources for you to review periodically.??????????????????
- As the industry evolves, it's essential to stay up-to-date on the latest security trends and news????????????????????????????????
- As we approach the end of our program,???/???????????
- we'll share some ways to become involved with the security community.????????????????????
- we'll identify reliable security resources you can use to stay up-to-date on security news and trends.????????????????????????????????????
- how to engage with the security community, find jobs in the security field, create a resume, and navigate the interview process??????????????????
- other stakeholders will be more focused on how policies and procedures are working to prevent cyber attacks????????????????????????????????

- Juliana decides to put together a detailed document with timelines that clearly explain what happened??????????????????????????????
- Juliana’s manager has also been informed that???????...?
- Juliana's visual dashboard makes it easier for the high-level stakeholders to review incident #1 and determine a course of action?Juliana ????????????????????? #1?????????
- Her dashboard will use charts and graphs to relay important information??????????????????
- she used her company’s escalation policy to properly escalate the two incidents??????????????????
- escalation; escalate (??/???????/????)
- allow decision makers to determine how to address security issues that put the organization at risk?????????????????????????
- allow security team members to convey essential information to stakeholders??????????????????????
- Those stakeholders and the security team can then work together to determine how to address the issue?????????????????????????????/?????
- Based on this information,????
- wants to know how many employees are often clicking on phishing emails. The goal is to identify which five departments click on those emails most often. ??
- The audit gathered data showing how many phishing emails each department clicked over the last five months????????????????????????????????????
- Other times you might want to include a document attachment that further elaborates on a specific topic.????????????????????????????????
- Security is often a team effort.???????????????
- Visuals help provide these decision-makers with actionable information that can help them identify potential risks to the organization's security posture .??????????????????????????????????????
- An entry-level analyst might communicate directly or indirectly with these individuals.?????????????????????
- Create visual dashboards for impactful cybersecurity communications??????????????????
- If you don't receive a timely response from a stakeholder, following up shows initiative.?????????????????????????????
- It's important to stand out in the security profession, especially if you don't have previous experience in the industry.????????????????????????????????????
- It sounds simple, but a friendly call can often prevent a major issue from occurring ????????????????????????????????
- When appropriate, take the initiative to follow up with a stakeholder if they haven't responded to an email in a timely manner.????????????????????????????????
- Direct communication is often better than waiting days or weeks for an email response to an issue that requires immediate attention.??????????????????????????????????????
- that sometimes a simple instant message or call can help move a situation forward .?????????????????????????
- This means they may sometimes miss an email, or fail to respond in a timely manner .??????????????????????????????

- Be sure to follow the procedures outlined in your organization's playbooks???????????????
- Be mindful of the sensitive information contained in these types of communications. ??(??)?????????
- we'll focus on various communication strategies that can help you engage with and convey key ideas to stakeholders???????????????
- The ability to communicate threats, risks, vulnerabilities, or incidents and possible solutions is a valuable skill for security professionals.??????????????????????????????????????
- Senior-level stakeholders might be more interested in the underlying risks, such as the potential financial burden of a security incident—as opposed to the details around logs????????????
- How do I explain the situation in a nontechnical manner???????????????
- your immediate supervisor??????
- how it impacts the organization, and possible solutions to the issue.?????????
- It's essential that communications are specific and clear?...??...?
- Staying informed about security issues helps stakeholders do their jobs more effectively.?????..., ?????...?
- You don't want them to have to guess the reason for your email or why it matters to them.???????..., ??????
- keep those top-level stakeholders informed on the security measures??...????/??...?
- responsibilities; responsible for (??;?...??)
- there are certain stakeholders that the analyst will need to provide updates to (??????????????????)
- the security measures and protocols in place (???????????)
- A big part of what you'll do as a security analyst is report your findings to various security stakeholders. (????????????????????????????????????)
- the individuals who have a significant interest in those business operations: stakeholders. (?????????????????????)
- They're also tasked with creating security and business continuity plans. (??????????????????)
- CISOs are high-level executives responsible for developing an organization's (????)
- Another stakeholder with an interest in security is the Chief Information Security Officer, or CISO (???????; ???)
- They are concerned about security from a financial standpoint because of the potential costs of an incident to the business.(????/??)
- because the decisions made on a day-to-day basis by stakeholders will impact how you do your job (??/??;??????)
- on a daily basis?????
- the supervisor indicates that a data breach has occurred . This breach has impacted one of the manufacturing sites for the organization. ????????????????????????????????????
- the incident may be increased or decreased to a high or low criticality level.??????
- Suddenly, you notice there's been unusual log activity in an app that was recently banned from the organization.????????????????????????????????
- The internal compliance of an organization's data protection procedures. ??????
- Malware infections can cause a system's network to run an unusually low speeds .??????????????????????

- a few incident classification types to be aware of: malware infection, unauthorized access, and improper usage (??????????????????????????????)
- Security incident escalation is the process of identifying a potential security incident. (??????)
- you'll learn the importance of escalating security issues and the potential impact of failing to escalate an issue. (??????????;???????????)
- it has the potential to become a larger problem that costs the company money, exposes sensitive customer data, or damages the company's reputation. (??????????????????????????????????????)
- From the Chief Information Security Officer, also known as the CISO, to the engineering team, public relations team, and even the legal team, every member of the security team matters. (???;????;????;????)
- it's important that you know how to evaluate and escalate incidents to the right individual or team when necessary. (??????????????????????????????)
- I enabled debug logs in the service so I could observe what was going on (??/??)
- Penetration testing (pen test) (????)
- security mindset, security awareness (????; ????)
  - Your security mindset allows you to protect all levels of assets.
  - So having a security mindset helps analysts defend against the constant pressure from attackers.
  - Having a strong security mindset can help set you apart from other candidates as you prepare to enter the security profession. (????)
  - using fictitious emails to evaluate security awareness at the company.
- should be escalated to a supervisor. (?????)
- how to escalate incidents to protect an organization's assets and data (????)
- happen
  - after a security incident has taken place
  - in case a security incident does occur
- The role of a security professional is to ensure a company's data and assets are protected from threats, risks, and vulnerabilities. (??????????????????????????????????)
- business continuity and disaster recovery plans (???????????)
- Conduct training for the business continuity team (??...??)
- If you're not sure of the potential impact of an incident, it's always best to be cautious and report events to the appropriate team members. (???...; ??; ???????)
- When a security event results in a data breach, it is categorized as a security incident. (????; ????)
- if it was compromised (??????/??)
- Intellectual property (??)
- They can have a significantly negative impact on an organization if leaked publicly. (???????;????)
- Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data. (????;????;????)
- Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)
- This data classification type is important for an organization's ongoing business operations (????)
- Unauthorized access to sensitive data can cause significant damage to an organization's finances and reputation. (?????;????;??)

- personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI)
- Public data, Private data, Sensitive data, Confidential data
- If an individual gains unauthorized access to private data(??;??????)
- Private data is information that should be kept from the public. (????)
- threats, risks, and vulnerabilities that are posed by social engineering attacks, such as phishing (????????...)
- such as intellectual property, trade secrets, PII, and even financial information (????;????;????)
- helps you prepare for the worst-case scenario, even if it doesn't happen(?...????????)
- cybersecurity profession????????
- cybersecurity professionals????????
- cybersecurity field????????
- refine your understanding of key security concepts???/???
- Writing code that assigns security incident tickets to the appropriate cybersecurity team based on its priority level. (??????????????????????????)
- This results in DNS resolvers sending large responses to (??)
- which can lead to significant issues like unplanned downtime (??; ????; ????)
- can access restricted information (????)
- Security professionals are often tasked with reviewing log files(???/???/?????)
- Automate cybersecurity tasks with Python
- removing usernames that match specific criteria from an access list.??????
- 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?????; ?????
  - security profession??????
  - security field??????
  - 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; Analytic
  - like machine learning or data analytics
  - 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 #219
Created 6 September 2024 14:03:56 by Admin
Updated 2 November 2024 08:49:51 by Admin