Answer Sheet

Q1) Which of the following is an example of a log data type?

- Website requests per hour.
- Database tables.
- ✅ HTTP response records.

Explanation:-HTTP response records are examples of log data types.

- Percentage of CPU over time.

Q2) How are smart groups created?

- ✅ Automatically, using machine learning algorithms.
- Through the Azure CLI.
- Through a template deployment.

Q3) What query filter command would you use to get n rows in no particular order?1

- top
- ✅ take

Explanation:-Take is used on small datasets. It returns n rows from the result set in no particular order.

- sort by

Q4) Which one of the following is a valid prebuilt view that you can download and install in your Log Analytics workspace?

- Audit Events
- Azure AD Account Auditing Events
- ✅ Sign-ins Events

Explanation:-Sign-ins Events and Azure AD Account Provisioning Events are the two prebuilt views you can download and install in your Log Analytics workspace.

Q5) When you export reports, which one of the following is not a supported export type?

- Power BI
- ✅ PowerPoint

Explanation:-You can export your report data to either Excel or Power BI.

- Excel

Q6) What does the role of scribe do as part of incident response?

- ✅ documents the conversation around incident in as much detail as possible
- keeps track of the metrics in the monitoring system that are important
- creates a verbatim transcript for a call bridge
- writes up the post-incident review

Q7) Do you need all of the roles mentioned in this unit to do successful incident response?

- Correct
- ✅ Incorrect

Explanation:-especially in smaller organizations or during more minor incidents, not all roles will be needed.

Q8) What of these questions is not immediately useful to ask about an incident when you evaluate your incident tracking process?

- Who else is aware of the issue?
- ✅ How quickly can we reach a C-level executive about the problem?

Explanation:-though C-level executives are important, this does not help you evaluate your process.

- How bad is it?
- How did we find out about the problem?

Q9) When creating a conversation bridge to communicate about an incident, why is it important to carve out a unique channel for it?

- it lets us keep channels for engineers and management separate
- ✅ it will keep irrelevant discussion out of the channel making it easier to later use the data for post-incident review
- this process will make sure we are HIPAA-compliant

Q10) Which of the following is true?

- You should use only email to document discussions about the incident.
- ✅ You should keep information about an incident in a centralized place where it is accessible to everyone on the team

Explanation:-it is important that it is easy to find and access.

- You should keep information about incidents limited to only the primary and secondary responders until the incident has been resolved

Q11) Which tool can you use for codeless automation to automate your initial response?

- ✅ Logic Apps
- troubleshooting guides
- ChatOps

Q12) What is ChatOps?

- an informal get-together for operations professionals held in Boston each year
- a kind of bot that can help you with incident response
- ✅ a conversation-driven collaboration model

Q13) When communicating with stakeholders, which of these items are not part of the formula we suggested?

- This is what we're doing.
- ✅ This is who is staffing the incident response.

Explanation:-This answer is not information that stakeholders necessarily need to know (plus it may change as the incident progresses)

- This is what we know.
- We will get back to you in X amount of time

Q14) Why are workbooks and troubleshooting guides considered live documents in our description?

- they are automatically shared to the public as soon as they are written
- ✅ Kusto Query Language (KQL) queries can be embedded and will display their results when the document is read
- they can be edited at any time

Q15)

Suppose someone has inadvertently committed a sensitive API key stored in the .secrets folder.

What is the correct way to scrub that information from GitHub?1

- This is a trick question. Once you commit something to GitHub, it lives forever. That's why globally unique hashes are used to identify everything.
- Delete the sensitive file from GitHub. Then commit an empty file to the same location to overwrite it.
- ✅ Use git to remove the unwanted commit and update historical references. Then contact GitHub support to run garbage collection and invalidate the Git cache.

Explanation:-This approach is the correct process to remove the data moving forward. However, if you feel someone may have accessed the key while it was available, you should replace the key with a new one.

Q16) How does GitHub's top-level search bar differ from the search options available on repository tabs?

- Other than being located in different parts of the user interface, they are otherwise the same.
- They support different filter syntax options.
- ✅ The top-level search bar supports searching everything across all of GitHub, whereas the repository tab searches are scoped to cover specific types in the current repository.

Explanation:-The top-level search allows the most flexibility, whereas the scoped tab searches provide popular filter dropdowns for easier refinement.

Q17) Which tool can help us retrieve a Teams conversation for the post-incident review?

- Azure Monitor
- Kusto Query Language
- ✅ Microsoft Graph API

Explanation:-we can query this API to retrieve Teams conversations.

Q18) Which of the following refers to telling a story about events that did not happen in order to explain what did happen?

- ✅ Counterfactual reasoning
- normative language
- mechanistic reasoning

Q19) Human error is a…

- diagnosis
- cause of problems
- ✅ label that causes you to quit investigating at precisely the moment when you're about to discover something interesting about your system

Q20) Which is a helpful practice for running a post-incident review meeting?

- It should be required for every incident to which the team responds
- It should last between two and four hours
- ✅ It should be run by a facilitator who was not involved in the incident

Q21) Which question could you ask that might lead to people skipping over valuable information in a post-incident review?

- what was the first thing you checked when you noticed the system was broken?
- how did you notice the system was broken?
- ✅ why did the system break?

Explanation:-questions like this can lead people to jump directly to a problem cause.

Q22) Which of the following is a goal for effective incident response?

- Be able to act with deliberation
- ✅ Be able to respond with urgency

Explanation:-we want to respond, not just react, with urgency.

- Be able to react with caution

Q23) How quickly can engineering teams that are classified as “elite or high performers” generally detect, respond, and remediate service disruptions?

- in less than 1 week or a month
- in less than 24 hours
- in less than 4 hours
- ✅ in less than 1 hour

Q24) Which of these can be considered the "pulse" of your system?

- ✅ incidents

Explanation:-incidents do provide a pulse for you.

- a service ticketing system.
- monitoring

Q25) Which of these is not a phase of an incident?

- Readiness
- Analysis
- Remediation
- ✅ Communication

Explanation:-communication is important but is not a phase of an incident.

- Response
- Detection

Q26) Which of these things is a pillar of incident response?

- ✅ All of these

Explanation:-They are all pillars of effective incident response.

- rotations
- roles
- rosters

Q27) What does git blame do?

- It reverts the effects of a git praise command.
- ✅ It displays the commit history of the file.

Explanation:-Despite the accusatory name, git blame is just a command to display commit history.

- It creates a bug assigned to the last person who committed changes to the specified file.

Q28)

Suppose a bug issue is reported on your project, and you know which pull request introduced the problem.

Which of the following options is not a cross-linking best practice?

- Add a comment to the bug report that links the pull request to it using the #ID syntax.
- Add a comment to the bug report that includes the pull request's author by using an @mention.
- ✅ Do not create cross-links when the root cause of the issue is already known.

Explanation:-It's a good practice to always add cross-links in case you or someone else needs the context later on.

Q29) Which of the following choices best describes the relationship between open source and InnerSource programs?

- ✅ InnerSource programs are fundamentally the same as open source programs, except that their access is limited to people within their organization.

Explanation:-InnerSource offers all of the benefits of traditional open source patterns, but to a limited audience in order to protect intellectual property.

- InnerSource programs are forked from open source programs by organizations that only use and maintain them privately moving forward.
- Anyone can offer a contribution to an open source program, whereas InnerSource programs only accept contributions from members of the team that owns the repository.

Q30)

Suppose your team has been receiving some low-quality bug reports without enough information to properly diagnose.

Which of the following choices is the best way to address the issue?

- Add a CONTRIBUTING.md file that clearly explains what's expected in bug reports, such as reproduction steps, system properties, and instructions for generating and including important logs.
- Use GitHub Script to add a workflow action that automatically rejects any issues with a description fewer than 200 characters long.
- ✅ Add an ISSUE_TEMPLATE.md file that includes fields for reproduction steps, system properties, and instructions for generating and including important logs.

Explanation:-This file will ensure that anyone filing a bug knows what's expected of them at the moment they're writing the report.

Q31)

Suppose your team has been tracking data of all kinds since your InnerSource program went live three months ago.

Which of the following metrics indicates your program is a great success?

- A steady decline in new issues.
- A growing rate of bug reports that are quickly closed because they cannot be reproduced.
- ✅ A dramatic rise in pull requests that address bugs in your software.

Explanation:-This metric indicates that more people are motivated to improve the quality of your software and are making the investment themselves.

Q32) Which of the following Markdown snippets would produce this text: Hello, world!?

- ✅ *Hello, **world**!*

Explanation:-Remember that you can also use underscores (_) instead of asterisks if you prefer.

- **Hello, *world*!**
- *Hello, *world*!*

Q33) How do you print certain characters, like asterisks (*) and underscores (_), literally on your output?

- Unfortunately, this is not supported at this time.
- ✅ Escape them with a backslash, like * or _.

Explanation:-You can also escape other reserved characters, including { and #, using backslashes.

- Use three in a row, like *** or ___.

Q34)

Suppose there is an HTML snippet that you want to include on your GitHub Pages web site, but Markdown doesn't offer a way to render it.

What should you do?

- Open an issue that requests Markdown support for your very specialized scenario.
- Cut the content. If it's not supported in Markdown, then it's probably not worth including.
- ✅ Just add the HTML inline.

Explanation:-Markdown is not a complete replacement for HTML, so it's understood that you may need to add HTML in to get the final results you're looking for.

Q35) What is the best way to make sure you're integrating the most secure versions of your project dependencies?

- ✅ Enable Dependabot for your repository.

Explanation:-Dependabot will scan your repository's dependency manifests and notify you via pull request whenever a version you rely is marked as insecure.

- Configure your package files to always use the latest versions of dependencies.
- Check each project's security details closely before adding it to your dependencies by confirming its version status across multiple advisory sites.

Q36) Correct or Incorrect: You can download published audit reports and other compliance-related information related to Microsoft's cloud service from the Service Trust Portal

- Incorrect
- ✅ Correct

Explanation:-You can download published audit reports and other compliance-related information related to Microsoft's cloud service from the Service Trust Portal.

Q37) Which of these statements are not true about complex systems

- Catastrophe is always just around the corner
- ✅ Complex systems can run without human intervention.

Explanation:-this is not true. If anything, complex systems may need more human intervention to keep running.

- Complex systems run in degraded mode
- Complex systems contain changing mixtures of failure latent within them

Q38) What is the role of people in complex systems?

✅ they work within a system
Explanation:-Systems are socio-technical in nature, people are a part of them.
- they work with a system
- they work on the system

Q39) Which of these is the correct name for the process that helps us learn from failure?

- retrospective
✅ people have different names for the same thing, any of the above terms will work, it is the process that matters
Explanation:-There is no one correct name, it is the process that matters.
- postmortem
- post-incident learning review
- post-incident review

Q40)

Suppose one of your source projects relies on secrets kept in a folder called .secrets.

You would like to make sure that the files kept in this folder on development machines are not inadvertently committed to the repository.

Which of these files will best help enforce this policy?

- CONTRIBUTING.md
✅ .gitignore
Explanation:-.gitignore can be used to help enforce which files are included in commits by tools that respect it. However, note that this policy is enforced by the client and does not necessarily prevent users from committing files that violate policy.
- SECURITY.md

Q41)

Suppose someone has inadvertently committed a sensitive API key stored in the .secrets folder.

What is the correct way to scrub that information from GitHub?

- This is a trick question. Once you commit something to GitHub, it lives forever. That's why globally unique hashes are used to identify everything.
- Delete the sensitive file from GitHub. Then commit an empty file to the same location to overwrite it.
✅ Use git to remove the unwanted commit and update historical references. Then contact GitHub support to run garbage collection and invalidate the Git cache.
Explanation:-This approach is the correct process to remove the data moving forward. However, if you feel someone may have accessed the key while it was available, you should replace the key with a new one.

Q42) Which of the following scenarios is not a good candidate to be built as a GitHub App?

✅ An app that allows a user to approve a pull request from a custom tool.
Explanation:-This scenario wouldn't be a good candidate for a GitHub app because it would need to operate on behalf of a specific user.
- An app that checks the spelling of pull request titles after they're created.
- An app that requests a user to update the name of a pushed branch if they don't follow your team's user/feature branch naming convention.

Q43) When should you build an OAuth App instead of a GitHub App?

- When your app needs to consume webhooks.
✅ When your app needs to operate on behalf of a specific user.
Explanation:-OAuth apps run as the user who authorized them. GitHub Apps run as themselves.
- When your app needs to access the GitHub API.

Q44) Which of the following choices is not a benefit of using webhooks over polling?

- Webhooks offer faster delivery of new data than polling.
- Webhooks use less bandwidth than polling.
✅ Webhooks have better network accessibility than polling.
Explanation:-Webhooks require the publisher to connect to the subscriber to push data, which may not be practical if the subscriber is behind a firewall. However, you can mitigate this scenario through relay services like smee.io.

Q45) What is GitHub Script?

- An automation syntax for GitHub Shell.
✅ A workflow action that enables GitHub API access from GitHub Actions.
Explanation:-It allows you to script any API usage that is available through the octokit/rest.js library.
- A programming language that compiles to JavaScript.

Q46) What is the difference between GitHub Script and GitHub Actions?

- GitHub Actions automates workflows that run inside GitHub. GitHub Script automates workflows that run outside of GitHub.
- ✅ GitHub Actions is a workflow engine that automates the execution of actions. GitHub Script is one of the actions available for use in a workflow.

Explanation:-GitHub Actions workflows may contain GitHub Script actions.

- GitHub Actions is for automating build and release pipelines. It was written in the GitHub Script programming language.

Q47) Why would someone use the following YAML in a GitHub Script action: if: contains(github.event.issue.labels.*.name, 'bug')?

- To automatically flag any commits containing code matching the github.event.issue.labels.*.name namespace pattern as a bug.
- To make sure that new issue names do not violate the bug reporting policy when created.
- ✅ To ensure that the script only runs when the target issue has been labeled as a bug.

Explanation:-This expression instructs the action to ignore issues that are not labeled as a bug.

Q48) Which of the following choices is not a good reason to protect a branch?

- ✅ The branch contains sensitive information that you don't want other repository participants to be able to see.

Explanation:-Protecting a branch doesn't hide its contents.

- You want to avoid accidental deletion after a pull request.
- You want to restrict who can push commits to it.

Q49)

Suppose your team repository contains several long-lived branches, including master, release-v1.0, and release-v2.0.

Which of the following Git commands best enables you to apply specific commits from master into release-v1.0 to apply hotfixes to the legacy version of the codebase?

- git rebase
- ✅ git cherry-pick

Explanation:-This command allows you to select specific commits to apply to a different branch.

- git merge

Q50)

Your project team has reached a major milestone and wants everyone to install the latest version of your app.

Which option is the best way to let interested users know?

- Merge the changes into master using a pull request.
- Create a Git tag.
- ✅ Create a release on GitHub.

Explanation:-This option will notify everyone who is watching your repository. It also gives you the opportunity to provide binaries for deployment and emphasize the importance of the release through release notes.

Q51) A post-incident review takes place during which phase of the incident lifecycle?

- Readiness
- ✅ Analysis
- Remediation
- Response
- Detection

Q52) Ideally, when should you do a post-incident review?

- at the beginning of the fiscal quarter
- after every incident
- once a month
- ✅ after every significant incident

Q53) What is the primary purpose of a post-incident review?

- ✅ to learn and improve
- to create a punch list of items to be repaired
- to pinpoint who is to blame for the failure

Q54) Is it possible to fire your way to reliability?

- ✅ Incorrect
- Correct

Q55) What should a post-incident review focus on?

- ✅ All of these

Explanation:-The focus needs to be on all of these items.

- hearing the different perspectives people have about the same incident

- better understanding of the system we work within
- deficits in process and technology

Q56) What is the first step to begin a post-review process?

- meet with the engineering manager associated with the service that had a problem
- schedule a meeting room for the discussion
- ✅ gather the data, including the conversation and context
- write down everything you can remember about the incident

Q57) Which Azure service allows you to configure fine-grained access management for Azure resources, enabling you to grant users only the rights they need to perform their jobs?

- Locks
- Policy
- Initiatives
- ✅ Role-based Access Control

Explanation:-Role-based access control (RBAC) provides fine-grained access management for Azure resources, enabling you to grant users only the rights they need to perform their jobs. RBAC is provided at no additional cost to all Azure subscriber.