Intro

This survey contains a list of pre-screening questions to gauge the participant's eligibility to participate in a study to measure the usefulness of analysis materials for threat validation. You will receive, in total, 20 questions based on GitHub and Kubernetes platforms.

Eligible candidates (attain at least 80% correct answers) will receive an invitation to participate in the paid study with a compensation of $90 (we estimate the duration of the full survey to be 1hr 45 minutes)

You can also get more information about the study by contacting k.tuma@vu.nl or w.mbaka@vu.nl
Click this link to access the full informed consent form.

By clicking next, you agree to participate in this pre-screening survey.

GitHub Questions

1. Which of the following measures is the most effective for protecting GitHub accounts from phishing attacks that steal two-factor authentication codes?

- ◯ Using time-based one-time password (TOTP) based two-factor authentication instead of single-factor login.
- ◯ Switching to hardware security keys or WebAuthn-based two-factor authentication.
- ◯ Relying on URL-shortening services to verify the authenticity of links.

2. What are the potential benefits and risks associated with enabling features such as core.autocrlf, core.whitespace, and receive.fsckObjects in a collaborative development environment that spans across different operating systems and repository sizes?

- ◯ Enabling core.autocrlf ensures consistent line endings across different platforms, but risks incorrect conversions on platforms like Linux; core.whitespace helps maintain clean code formatting, and receive.fsckObjects enhances security by checking data integrity but can slow down pushes for large repositories.
- ◯ Disabling core.autocrlf, core.whitespace, and receive.fsckObjects is recommended in all environments for maximum performance and minimum complexity.
- ◯ core.autocrlf is unnecessary for cross-platform work, core.whitespace only applies to Windows systems, and receive.fsckObjects is disabled by default to improve performance.

3. If you run git clone git://example.com/project.git, an attacker who controls e.g your router can modify the repo you just cloned, inserting malicious code into it. If you then compile/run the code you just cloned, you will execute the malicious code. True or False, provide a short justification for your choice.

- ◯ True
- ◯ False

4. Git can use four distinct protocols to transfer data: Local, HTTP, Secure Shell (SSH) and Git. Which protocol does not support authentication or encryption, making it potentially vulnerable to attacks?

- ◯ HTTPS
- ◯ SSH protocol
- ◯ Git

5. What happens if the *~/git-shell-commands* directory is present in a user's home directory?

- ◯ The user can execute any git server command

- ◯ The shell restricts all SSH commands except git receive-pack
- ◯ The shell can run interactively, allowing users to run custom commands

6. Which of the following is true about permissions in a GitHub repository owned by a personal account?

- ◯ Only collaborators can delete issues
- ◯ Teams can be used to manage permissions
- ◯ There are two permission levels: repo owner and collaborators

7. What does the *on* keyword define in a GitHub Actions workflow?

- ◯ The environment where the workflow will run
- ◯ The events that trigger the workflow
- ◯ The name of the workflow

8. Collaborators on a personal repository can pull (read) the contents of the repository and push (write) changes to the repository. What other actions can collaborators perform?

- ◯ Change the visibility of the repository
- ◯ Manage labels for issues and pull requests in the repository
- ◯ Merge a pull request on a protected branch

9. What is the default behavior of a branch protection rule regarding force pushes and branch deletion?

- ◯ Force pushes are allowed, but branches cannot be deleted
- ◯ Force pushes and branch deletion are both allowed
- ◯ Force pushes are blocked, and branches cannot be deleted

10. If you enable HTTPS for your GitHub Pages site but your site's HTML still references images, CSS, or JavaScript over HTTP, then your site is serving mixed content. Serving mixed content may make your site less secure and cause trouble loading assets. How can you resolve the problem of mixed content on GitHub

- ◯ Disable HTTPS for your GitHub Pages site
- ◯ Change the HTTP links to HTTPS in your HTML files
- ◯ Use a Content Delivery Network (CDN) to serve your assets

K8 Questions

1. Which of the following scenarios could enable an attacker to take over a Kubernetes cluster if cloud account credentials are compromised?

- ◯ Compromised cloud credentials give the attacker access to the Kubernetes control plane in the cloud provider's management layer.
- ◯ Cloud credentials with limited access (e.g., read-only permissions) allow an attacker to modify cluster resources.
- ◯ Running workloads in private clusters with restricted ingress/egress rules prevents all possible attacks from compromised cloud credentials.

2. Which of the following scenarios could enable an attacker to take over a Kubernetes cluster after obtaining compromised cloud credentials via a spoofing attack?

- ◯ Kubernetes Role-Based Access Control (RBAC) is misconfigured, allowing the attacker to escalate privileges within the cluster.
- ◯ The attacker leverages the compromised cloud credentials to bypass Kubernetes authentication mechanisms and directly access the API server.
- ◯ The cloud account credentials only allow access to a restricted IAM role that cannot modify cluster settings.

3. Which of the following configurations can contribute to resource exhaustion (e.g., due to cryptocurrency mining scripts) and potentially cause node instability or failure?

- ◯ Not setting CPU and memory resource limits for containers, allowing them to consume all available resources on the node
- ◯ Enforcing network policies to restrict pod-to-pod communication within the cluster.
- ◯ Setting CPU and memory resource limits for containers in the deployment specification.

4. Which of the following configurations can increase the risk of a container image supply chain attack?

- ◯ Restricting the use of root users in containers through Pod Security Policies (PSPs).
- ◯ Using image vulnerability scanning tools before deploying images to the cluster.
- ◯ Pulling images from public registries without validating their authenticity or integrity.

5. What are the risks associated with privileged containers that an attacker can leverage to get access to the host machine?

- ◯ Restricting the ability to run privileged containers through Kubernetes RBAC policies reduces the risk of host compromise.
- ◯ Privileged containers have the same capabilities as the host machine, allowing attackers to interact with the host's resources if they gain access to the container.
- ◯ Privileged containers are isolated from the host system and cannot access host resources, even if compromised.

6. Which of the following configurations can contribute to an attacker moving laterally between pods after compromising a container?

- ◯ The compromised container has been assigned a highly privileged service account that enables broad access to other pods.
- ◯ The cluster's CNI (Container Network Interface) plugin is configured to isolate traffic between namespaces by default.
- ◯ The attacker is able to retrieve environment variables within the compromised container, giving access to sensitive information about other pods.

7. Which of the following scenarios describes the implications of an attacker having access to a container image that contains sensitive information?

- ◯ The attacker can retrieve sensitive information embedded in the image layers, even if those layers are shared with other images
- ◯ If the sensitive information is stored in environment variables, the attacker can easily access them from the running container.
- ◯ Shared layers between images can prevent the attacker from accessing sensitive information in those layers if they do not have access to the other images

8. Which of the statements describes the potential risks associated with the use of the kubectl exec command?

- ◯ Legitimate OS images, such as Ubuntu, can be used by attackers as backdoor containers, enabling them to run malicious code remotely.
- ◯ Using role-based access control (RBAC) effectively mitigates the risk of unauthorized kubectl exec usage by limiting permissions to trusted users.

- ◯ The kubectl exec command can only be executed by cluster administrators, thereby reducing the risk of exploitation by regular users.

9. Which of the following configurations can potentially expose sensitive information to attackers probing the Kubernetes API server?

- ◯ Lack of defined admission controllers in the cluster.
- ◯ Cluster role bindings allow unauthenticated users to access resources within the cluster.
- ◯ RBAC (Role-Based Access Control) is properly configured to limit access to sensitive resources.

10. Which of the following statements regarding network plugins (Container Network Interface, or CNI) is true?

- ◯ CNI plugins are responsible for managing pod-to-pod communication across nodes in the cluster.
- ◯ Network plugins must be configured individually for each pod; they cannot be applied at the namespace or cluster level.
- ◯ All Kubernetes network plugins support network policy enforcement.

Invite to survey

Thank you for your participation. If you are eligible, we would like to invite you to participate in the paid survey. Kindly leave the link to your Upwork profile for ease of hiring.

Here is an example of the task to be expected during the actual study.

You will receive a scenario (two in total), and ten security threats to each scenario. Each threat contains a threat description, assumption(s), STRIDE threat type (that will be compromised if the threat is realistic), and affected data flow diagram components, as can be seen below. You will then be asked to assess the correctness of each threat. That is, mark each threat as either realistic (likely to occur) or bogus (unlikely to occur).

Scenario: updating a remote repository on GitHub

Threat description: Exploit a vulnerability in the code in the remote repository to attack the server running the code.

Assumptions: Remote repository and running server reachable by the attacker. The source code has security vulnerabilities.

STRIDE threat type: Information disclosure

Affected components: Victim’s server