Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending

Apply Now

Company: Emirates NBD Group

Location: united arab emirates

Category: other-general

The Cyber Security Cloud Operations Specialist role is responsible for effectively detecting, responding to, and mitigating threats targeting EmiratesNBD's cloud infrastructure and data. They will also act as standby resources for conducting the incident processes to ensure they are well drilled and effective. Maintain acceptable cyber hygiene levels and ensure the goals of the unit are met.

Continuously monitor cloud environments using security tools and services to detect potential intrusion attempts, data exfiltration, lateral movement, and unauthorized access. Utilize Security Information and Event Management (SIEM) tools to collect and analyze logs from various cloud services, identifying potential security incidents and abnormal patterns. Develop custom detection rules and queries to identify cloud-specific threats, such as API abuse, unauthorized resource provisioning, and data exfiltration.

Address cloud-specific attack vectors, such as identity and access management (IAM) issues, insecure API configurations, and data exposure due to misconfigured storage services. Implement container security monitoring solutions to ensure the integrity and security of containerized applications running in cloud environments. Utilize API security tools to monitor and protect cloud APIs from abuse, unauthorized access, and injection attacks. Deploy honeytokens and deception technology to lure and detect attackers attempting to exploit fake assets in the cloud.

Deploy machine learning-based anomaly detection to identify unusual user behaviors and potential account compromises within cloud environments.

Implement serverless security monitoring solutions to detect potential threats targeting serverless functions and ensure secure serverless application development.

Continuously review and enhance cloud security monitoring strategies, taking into account the evolving threat landscape and the cloud environment's changes.

Leverage CASB solutions to monitor and control data access and movement between cloud services and users, mitigating insider threats and unauthorized activities.

Conduct regular audits of Identity and Access Management (IAM) configurations, ensuring proper access controls and permissions across cloud resources.

Proactively search for signs of unauthorized activities, persistent threats, and advanced attack techniques within cloud environments using threat hunting methodologies.

Utilize threat intelligence sources and security data to detect cloud-specific threats such as misconfigurations, account compromises, and privilege escalation.

Use both manual and machine assisted techniques to find the Tactics, Techniques and Procedures of advanced adversaries.

Trace attacker paths and detect suspicious patterns of threat actors.

Research innovative methods for making Threat Hunting more efficient and effective.

Utilize digital forensics tools and techniques to perform in-depth analysis of compromised cloud instances, identifying attack vectors and post-incident indicators.

Develop acquisition and processing workflows to acquire and process cloud forensic artefacts.

Employ automated incident triage solutions to quickly assess the severity and impact of security alerts, prioritizing critical incidents for immediate response.

Execute incident response playbooks tailored to different cloud attack scenarios, ensuring the proper sequence of actions during each phase of incident handling.

Swiftly contain and isolate affected cloud resources to prevent further spread of the attack and conduct thorough investigations to identify the root cause of the incident.

Maintain clear and timely communication with stakeholders, providing updates on incident investigations, impact assessments, and recommended countermeasures.

Perform detailed post-incident analysis to understand attack vectors, tactics, techniques, and procedures (TTPs) employed by threat actors, enabling better defense against future attacks.

Help meet SLA's defined for Incident Management.

Prepare and provide relevant reports for identified incidents.

Ensure the relevant documentation is kept upto date at all times.

Proactively identify gaps and remediate them to keep observations from Auditors and Regulators to a minimum.

Help the CSIRT during security incidents.

#J-18808-Ljbffr

Apply Now

Cross References and Citations:

1. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Tradingjobs Jobs united arab emirates Tradingjobs ↗

2. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Barcelonajobs Jobs united arab emirates Barcelonajobs ↗

3. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Searchukjobs Jobs united arab emirates Searchukjobs ↗

4. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Fresherjobs Jobs united arab emirates Fresherjobs ↗

5. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Searcheuropeanjobs Jobs united arab emirates Searcheuropeanjobs ↗

6. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Topfishjobs Jobs united arab emirates Topfishjobs ↗

7. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Electricianjobs Jobs united arab emirates Electricianjobs ↗

8. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Ceojobs Jobs united arab emirates Ceojobs ↗

9. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on

11/21/2023 Trending Thecareerjobs Jobs united arab emirates Thecareerjobs ↗

10. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Statisticsjobs Jobs united arab emirates Statisticsjobs ↗

11. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Usajobscentral Jobs united arab emirates Usajobscentral ↗

12. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Clerkjobs Jobs united arab emirates Clerkjobs ↗

13. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Algeriajobs Jobs united arab emirates Algeriajobs ↗

14. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Oilandgasjobs Jobs united arab emirates Oilandgasjobs ↗

15. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Warehousejobsnearme Jobs united arab emirates Warehousejobsnearme ↗

16. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Executivejobsnearme Jobs united arab emirates Executivejobsnearme ↗

17. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Locumjobs Jobs united arab emirates Locumjobs ↗

18. Specialist Cyber Security Cloud Operations United Arab Emirates Posted on 11/21/2023 Trending Economicjobs Jobs united arab emirates Economicjobs ↗

19. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending Jobs United arab emirates ↗

20. AMP Version of Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending ↗

21. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending United arab emirates Jobs ↗

22. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending Jobs United arab emirates ↗

23. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending Job Search ↗

24. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending Search ↗

25. Specialist cyber security cloud operations united arab emirates posted on 11/21/2023 trending Find Jobs ↗