# AI-Driven Threat Detection in AWS Environments

With cyberattacks growing more sophisticated and the adoption of cloud services expanding, traditional security methods alone are no longer enough. AWS offers several AI-powered tools designed to enhance security and stay ahead of potential threats.

Amazon GuardDuty is like the security man to your apartment that continuously monitors your AWS environment for suspicious activity. It uses machine learning (ML) to detect unusual patterns, like unauthorized access attempts or unexpected data transfers, and sends alerts in real time.

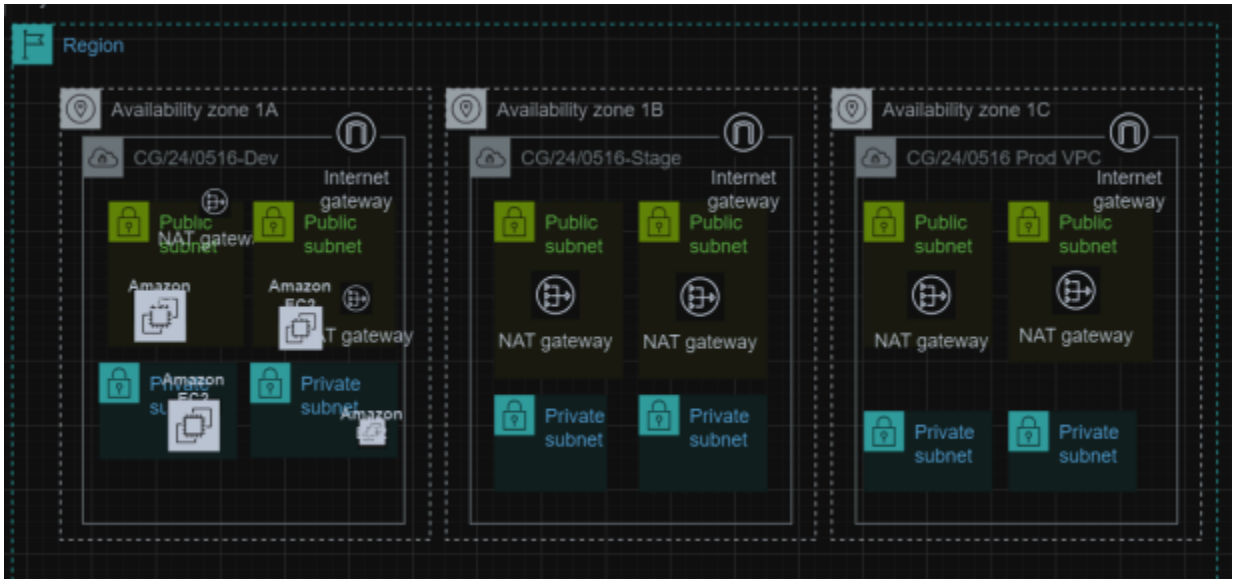
To help you investigate these alerts, Amazon Detective dives deeper by analyzing logs and visualizing security issues. This allows security teams to quickly find the root cause of incidents and take appropriate action.

For data protection, Amazon Macie is a key tool. It uses AI to identify and monitor sensitive data, like personal information, making sure your data stays secure and compliant with privacy regulations such as GDPR.

On the visual side, Amazon Rekognition can analyze images and videos such as CCTV footage to detect things like inappropriate content or faces, adding another layer of security in media-heavy environments.

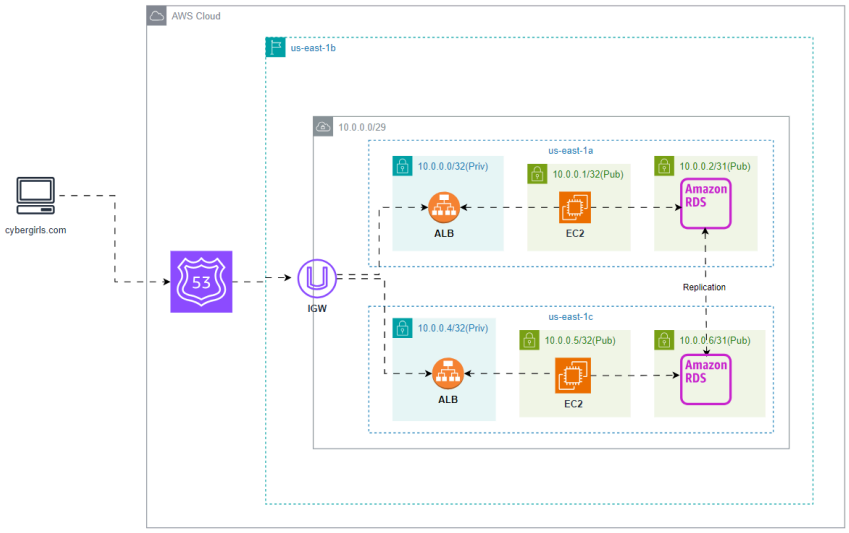
Together, these AWS tools offer a comprehensive, AI-driven approach to cloud security, helping businesses detect and respond to threats faster and more effectively.

See AWS Architecture Diagram Below



# Section B (AWS)

Q1:




| sn | Security Concerns | Recommendations |
|---|---|---|
| 1 | The EC2 instances (10.0.0.1/32 in us-east-1a, and 10.0.0.5/32 us-east-1c) are placed within public subnets.This exposes critical resources directly to the internet, increasing attack surface area. | EC2 instances handling frontend tasks can be in public subnets. While access to the backend should be restricted only through a bastion host. ALBs serving public traffic should be properly secured with SSL/TLS, enforcing HTTPS for all connections. |
| 2 | Amazon RDS instances appear to have public IPs (10.0.0.2/31, 10.0.0.6/31) and are **placed in public subnets**. | Public access to the RDS should be disabled via security group configurations. They should only be accessed over a VPN, Direct Connect, or through a bastion host in a private subnet. |
| 3 | There is no clear indication of inbound/outbound rules and Network ACLs (NACLs) | Use least-privilege rules in security groups to restrict access. EC2 instances should only allow necessary traffic such as port 80/443 for web servers and RDS should only allow connections from specific EC2 instances |
| 4 | The diagram does not include any logging or monitoring mechanism, which is essential for auditing and detecting malicious activity. | Enable VPC Flow Logs to capture information about the IP traffic going to and from network interfaces in the VPC.Consider using AWS GuardDuty and |

| | | |
|---|---|---|
| | | AWS CloudTrail for enhanced threat detection and monitoring. |

Q2.

To secure Como's cloud migration, I'd prioritize **data protection** by encrypting data at rest with *AWS KMS* or *Azure Key Vault* and using TLS/SSL for data in transit. I'd implement **DLP** tools like *AWS Macie* to monitor and prevent data leakage, ensuring backups are encrypted and access is controlled. For **network security**, I'd segment resources into public and private subnets with *VPCs*, using *security groups, NACLs,* and *Zero Trust using the Principle of Least Privledge* to manage access. I'd implement *WAF* and real-time threat detection with *GuardDuty* while securing remote access with VPNs and bastion hosts.

To handle **legacy applications**, I'd use the 6Rs of Cloud Migration, starting with rehosting in secure environments then refactor or containerizing apps using AWS ECS/EKS. Integrating security through DevSecOps and running regular vulnerability scans with AWS Inspector would ensure legacy systems are safe. For **regulatory compliance**, I'd use tools like AWS Security Hub to monitor standards like NDPR. IAM would enforce access control, and CloudTrail would ensure logging for auditability, with SIEM tools providing continuous security insights.

Q3a. The misconfigured S3 bucket(**contoso-fin-team-creds**) publicly exposed an AWS access key ID and secret access key belonging to a member of Contoso's financial team.

| sn | Q | Answer |
|---|---|---|
| 1 | What is the access key ID? | AWS_ACCESS_KEY_ID="AKIAVPEYV7H4ALHQNAAV" |
| 2 | Who does the access key belong to i.e. name of the employee? | Cole |
| 3 | What permissions are associated with this access key? | AdministratorAccess |
| 4 | What is the status of the access key? | Inactive |
| 5 | Were these permissions necessary? | The AdministratorAccess permission level was excessive for a typical employee in a financial role. Remove AdministratorAccess from Cole and replace it with specific roles like AmazonS3ReadOnlyAccess that limit access to necessary resources. |

3b. After stealing the credentials, the attacker accessed a bucket and exfiltrated confidential data using those credentials. Attached is the log file to assist in your investigation
Logs - https://contoso-access-logs.s3.amazonaws.com/logs.json

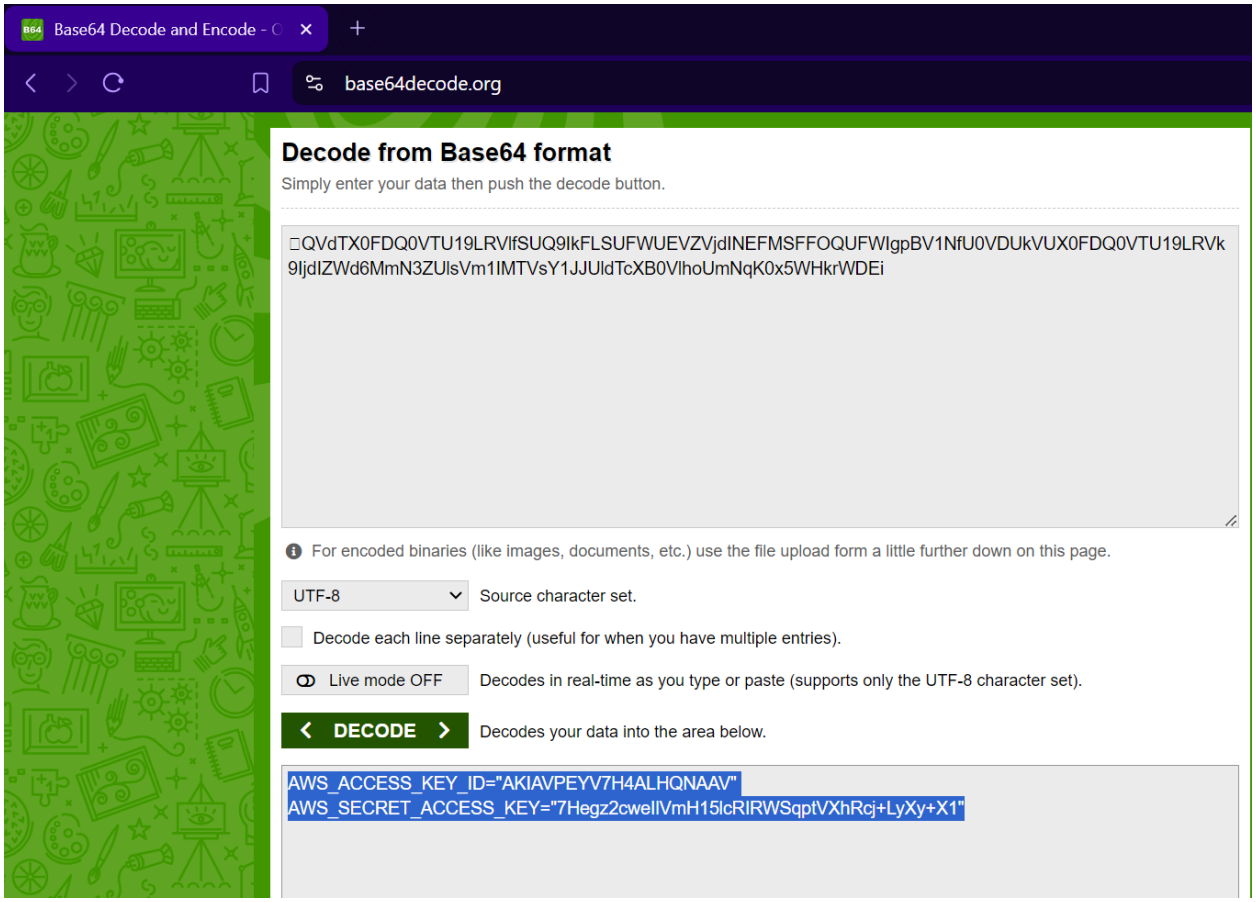
| sn | Q | Answer |
|---|---|---|
| i | What is the name of the bucket containing sensitive data? | contoso-private-data |
| ii | What country did the attack originate from? | The attack originated from multiple IP address 103.56.45.67 and 223.113.128.138 in **China** |
| iii | What is the IP address of the attacker? | The IP address 223.113.128.138 appears multiple times, notably with http_status: 200, confirming successful access to confidential data. |
| iv | When did the exfiltration occur? | 2024-10-16T09:54:10.925557Z |
| v | What are the names of the stolen files? | The stolen files include Employee-PII-records.xlsx, Employee-records.xlsx and Customer-PII.xlsx. |

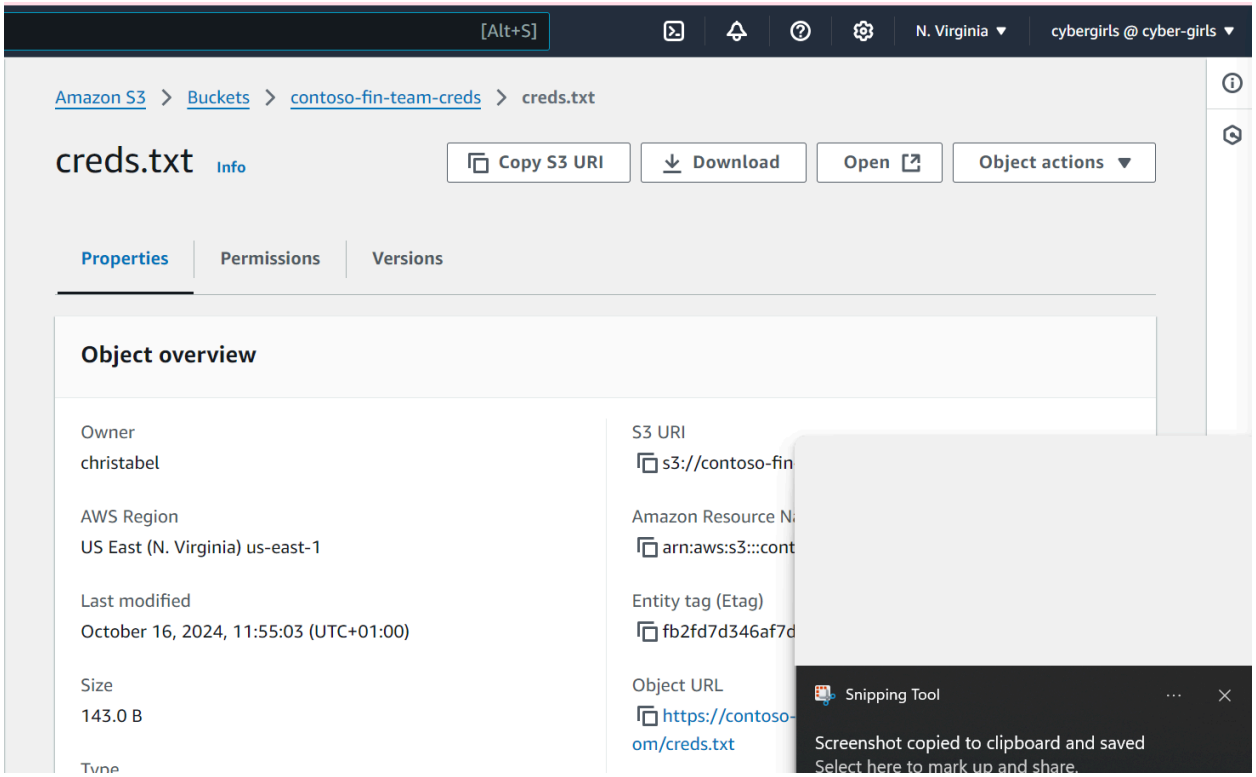
c. As a Security Consultant, what improvements would you recommend for Contoso's security monitoring practices using the recent breach as a point of reference?

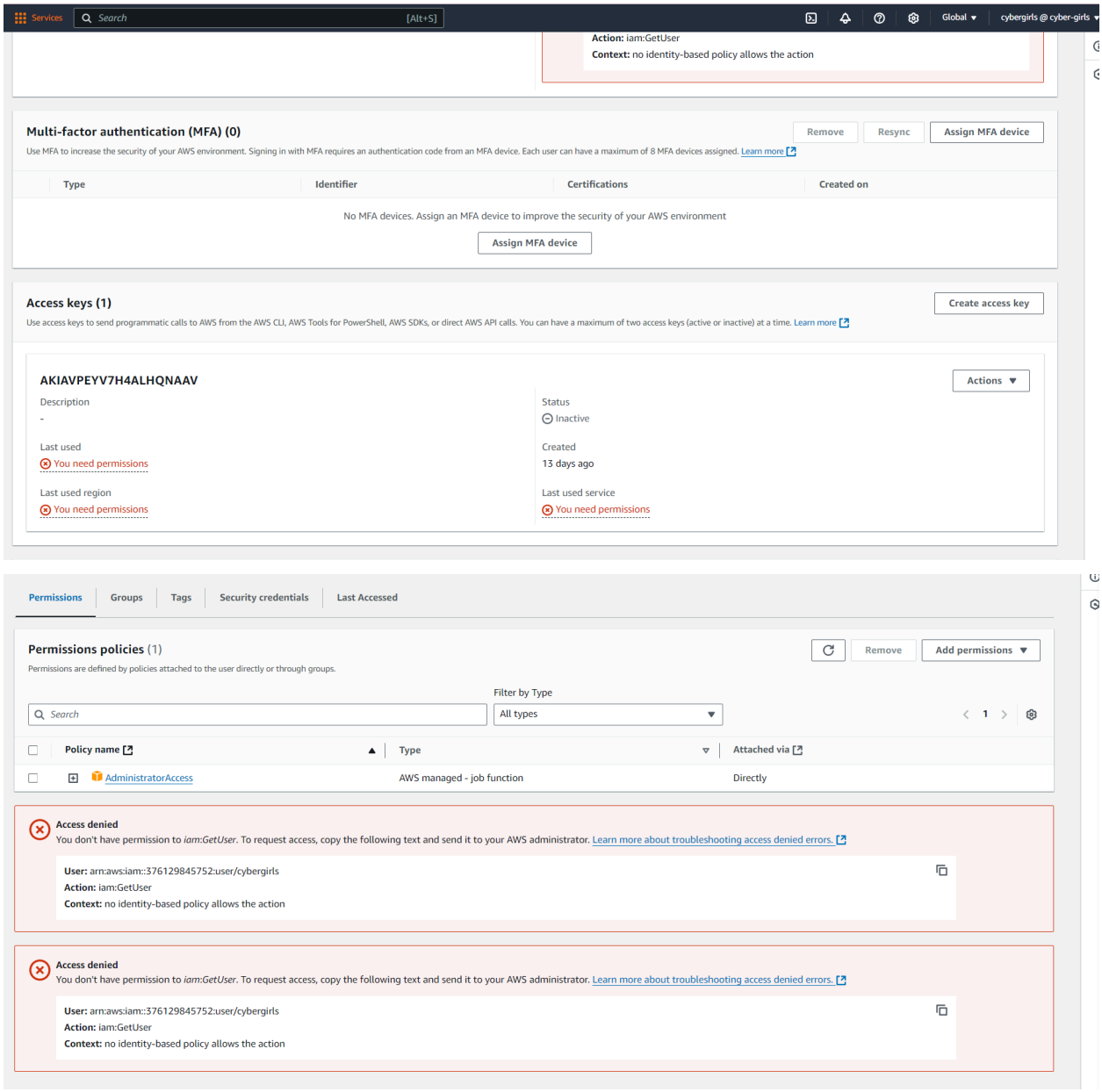
As a Security Consultant, I would recommend the following to Contoso:

- Ensure all sensitive data is encrypted both at rest and in transit, and implement strict IAM policies with MFA for accessing sensitive data.
- Use VPCs with proper subnetting, security groups, and NACLs, and implement continuous monitoring using AWS CloudTrail and AWS Config.
- Apply the principle of least privilege to all IAM users, regularly rotate access keys, and use IAM roles with temporary credentials.
- Enhance logging and monitoring to detect and respond to suspicious activities promptly, and conduct regular security audits and vulnerability assessments.

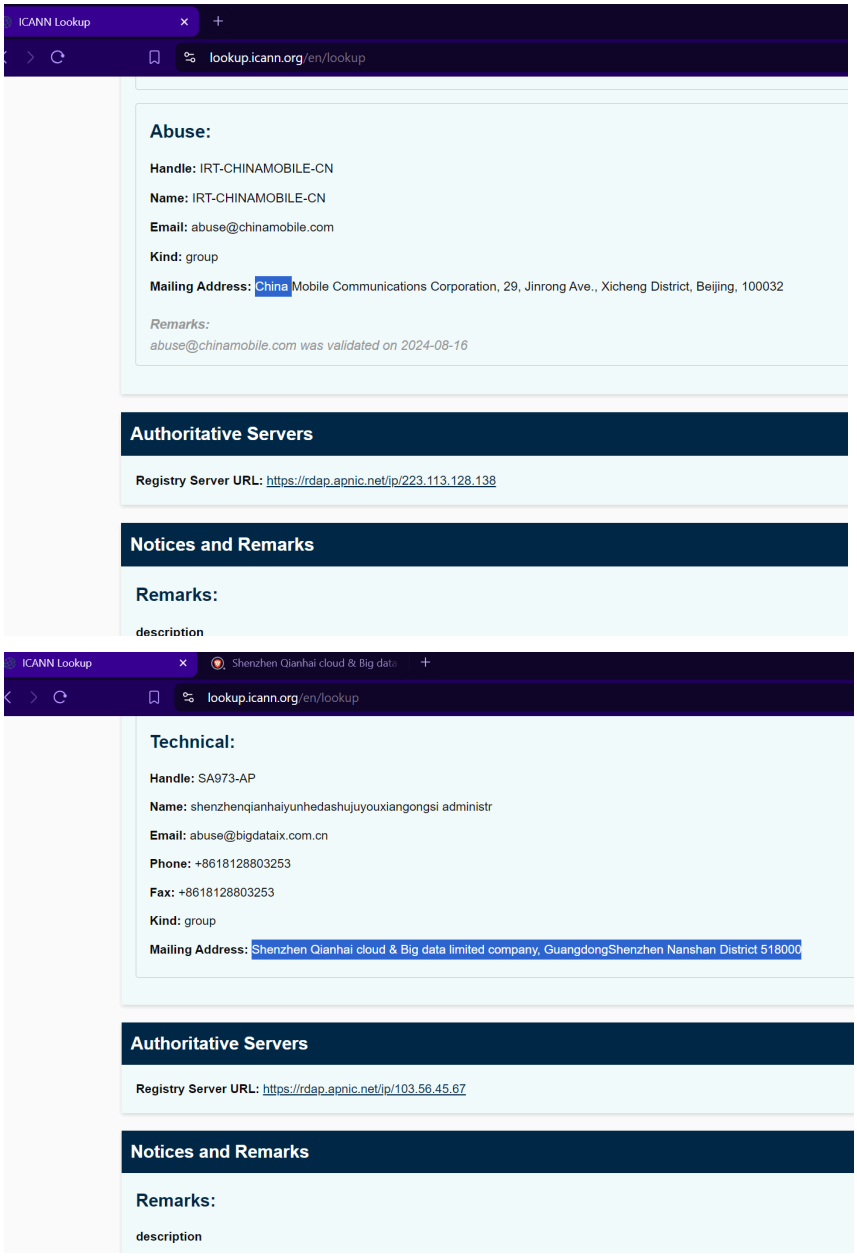
Pictures for Q3a (i-iv)


Base64 Decode and Encode - C
base64decode.org
Decode from Base64 format
Simply enter your data then push the decode button.
□QVdTX0FDQ0VTU19LRVlfSUQ9IkFLSUFWUEVZVjdINEFMSFFOQUFWIgpBV1NfU0VDUkVUX0FDQ0VTU19LRVk
9IjdIZWd6MmN3ZUlsVm1IMTVsY1JJUldTcXB0VlhoUmNqK0x5WHkrWDEi
For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Source character set.
Decode each line separately (useful for when you have multiple entries).
Live mode OFF
Decodes in real-time as you type or paste (supports only the UTF-8 character set).
DECODE
Decodes your data into the area below.
AWS_ACCESS_KEY_ID="AKIAVPEYV7H4ALHQNAAV"
AWS_SECRET_ACCESS_KEY="7Hegz2cwelIVmH15lcRlRWSqptVXhRcj+LyXy+X1"


[Alt+S]
N. Virginia
cybergirls @ cyber-girls
Amazon S3 > Buckets > contoso-fin-team-creds > creds.txt
creds.txt Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
christabel
AWS Region
US East (N. Virginia) us-east-1
Last modified
October 16, 2024, 11:55:03 (UTC+01:00)
Size
143.0 B
S3 URI
s3://contoso-fin
Amazon Resource Na
arn:aws:s3:::cont
Entity tag (Etag)
fb2fd7d346af7d
Object URL
https://contoso-
om/creds.txt
Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share.




Pictures for Q3b (iii)


ICANN Lookup
lookup.icann.org/en/lookup
Abuse:
Handle: IRT-CHINAMOBILE-CN
Name: IRT-CHINAMOBILE-CN
Email: abuse@chinamobile.com
Kind: group
Mailing Address: China Mobile Communications Corporation, 29, Jinrong Ave., Xicheng District, Beijing, 100032
Remarks:
abuse@chinamobile.com was validated on 2024-08-16
Authoritative Servers
Registry Server URL: https://rdap.apnic.net/ip/223.113.128.138
Notices and Remarks
Remarks:
description


ICANN Lookup
Shenzhen Qianhai cloud & Big data
lookup.icann.org/en/lookup
Technical:
Handle: SA973-AP
Name: shenzhenqianhaiyunhedashujuyouxiangongsi administr
Email: abuse@bigdataix.com.cn
Phone: +8618128803253
Fax: +8618128803253
Kind: group
Mailing Address: Shenzhen Qianhai cloud & Big data limited company, GuangdongShenzhen Nanshan District 518000
Authoritative Servers
Registry Server URL: https://rdap.apnic.net/ip/103.56.45.67
Notices and Remarks
Remarks:
description