Report Information

Version: 5.4.2

Parameters used: aws

Date: 2025-03-28T17:15:03.267848

AWS Assessment Summary

AWS Account: 087307122278

AWS-CLI Profile: default

Audited Regions: All Regions

AWS Credentials

User Id: AIDARIU7I6ZTHBMYUVL4I

Caller Identity ARN: arn:aws:iam::087307122278:user/week2

Assessment Overview

Total Findings: 7066

Passed: 5216

Passed (Muted): 197

Failed: 1850

Failed (Muted): 128

Total Resources: 1176

Filters (4) Show 100 entries Search:

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	critical	ec2	us-west-2	ec2_instance_port_cassandra_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to Cassandra ports (TCP 7000, 7001, 7199, 9042, 9160).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Cassandra exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Cassandra is a distributed database management system designed to handle large amounts of data across many commodity servers, providing high availability with no single point of failure. Exposing Cassandra ports to the internet can lead to unauthorized access to the database, data exfiltration, and data loss.	Modify the security group to remove the rule that allows ingress from the internet to TCP ports 7000, 7001, 7199, 9042 or 9160.	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_elasticsearch_kibana_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to Elasticsearch and Kibana ports (TCP 9200, 9300, 5601).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Elasticsearch/Kibana exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Elasticsearch and Kibana are commonly used for log and data analysis. Allowing ingress from the internet to these ports can expose sensitive data to unauthorized users.	Modify the security group to remove the rule that allows ingress from the internet to TCP ports 9200, 9300, 5601.	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	critical	ec2	us-west-2	ec2_instance_port_memcached_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 11211 (Memcached).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Memcached exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Memcached is an open-source, high-performance, distributed memory object caching system. It is often used to speed up dynamic database-driven websites by caching data and objects in RAM to reduce the number of times an external data source must be read. Memcached is designed to be used in trusted environments and should not be exposed to the internet. If Memcached is exposed to the internet, it can be exploited by attackers to perform distributed denial-of-service (DDoS) attacks, data exfiltration, and other malicious activities.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 11211 (Memcached).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_cifs_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 139 or 445 (CIFS).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has CIFS exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	CIFS is a file sharing protocol that is used to access files and printers on remote systems. It is not recommended to expose CIFS to the internet.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 389 or 636 (LDAP).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •CIS-4.0.1: 5.1.2 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_sqlserver_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 1433 or 1434 (SQL Server).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has SQL Server exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	SQL Server is a database management system that is used to store and retrieve data. If an EC2 instance allows ingress from the internet to TCP port 1433 or 1434, it may be vulnerable to unauthorized access and data exfiltration.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 1433 or 1434 (SQL Server).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	critical	ec2	us-west-2	ec2_instance_port_oracle_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 1521, 2483 or 2484 (Oracle).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Oracle exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Oracle database servers are a high value target for attackers. Allowing internet access to these ports could lead to unauthorized access to the database.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 1521, 2483 or 2484.	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_ftp_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 20 or 21 (FTP)	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has FTP exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	FTP is an insecure protocol and should not be used. If FTP is required, it should be used over a secure channel such as FTPS or SFTP.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 20 or 21 (FTP).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.2, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.2, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_ssh_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has SSH exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	SSH is a common target for brute force attacks. If an EC2 instance allows ingress from the internet to TCP port 22, it is at risk of being compromised.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 22.	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.2, 2.6.6, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.2, 2.6.6, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_telnet_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 23 (Telnet).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Telnet exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Telnet is an insecure protocol that transmits data in plain text. Exposure of Telnet services to the internet can lead to unauthorized access to the EC2 instance.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 23.	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.2, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.2, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_mongodb_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 27017 or 27018 (MongoDB)	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has MongoDB exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	MongoDB is a popular NoSQL database that is often used in web applications. If an EC2 instance allows ingress from the internet to TCP port 27017 or 27018, it may be vulnerable to unauthorized access and data exfiltration.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 27017 or 27018 (MongoDB).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	critical	ec2	us-west-2	ec2_instance_port_mysql_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 3306 (MySQL).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has MySQL exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	MySQL is a popular open-source relational database management system that is widely used in web applications. Exposing MySQL to the internet can lead to unauthorized access and data exfiltration.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 3306 (MySQL).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_rdp_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 3389 (RDP)	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has RDP exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	RDP is a proprietary protocol developed by Microsoft for connecting to Windows systems. Exposing RDP to the internet can allow attackers to brute force the login credentials and gain unauthorized access to the EC2 instance.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 3389 (RDP).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.2, 2.6.6, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.2, 2.6.6, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_ldap_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 389 or 636 (LDAP).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has LDAP exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	LDAP is a protocol used for authentication and authorization. Exposing LDAP to the internet can lead to unauthorized access to the LDAP server and the data it contains.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 389 or 636 (LDAP).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1 •KISA-ISMS-P-2023: 2.6.1, 2.10.1
FAIL	critical	ec2	us-west-2	ec2_instance_port_postgresql_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 5432 (PostgreSQL)	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has PostgreSQL exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	PostgreSQL is a popular open-source relational database management system. Exposing the PostgreSQL port to the internet can lead to unauthorized access to the database, data exfiltration, and other security risks.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 5432 (PostgreSQL).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.10.1, 2.10.3

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	critical	ec2	us-west-2	ec2_instance_port_redis_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 6379 (Redis).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Redis exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Redis is an open-source, in-memory data structure store, used as a database, cache, and message broker. Redis is often used to store sensitive data, such as session tokens, user credentials, and other sensitive information. Allowing ingress from the internet to TCP port 6379 (Redis) can expose sensitive data to unauthorized users.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 6379 (Redis).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.6.4, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.6.4, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_kerberos_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 88, 464, 749 or 750 (Kerberos).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Kerberos exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Kerberos is a network authentication protocol that uses secret-key cryptography to authenticate clients and servers. It is typically used in environments where users need to authenticate to access network resources. If an EC2 instance allows ingress from the internet to TCP port 88 or 464, it may be vulnerable to unauthorized access.	Modify the security group to remove the rule that allows ingress from the internet to TCP port 88, 464, 749 or 750 (Kerberos).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.10.1, 2.10.3
FAIL	critical	ec2	us-west-2	ec2_instance_port_kafka_exposed_to_internet	Ensure no EC2 instances allow ingress from the internet to TCP port 9092 (Kafka).	arn:aws:ec2:us-west-2:087307122278:instance/i-0b3467aef4d20a6dc	•Name=defi-proxy-oregon3	Instance i-0b3467aef4d20a6dc has Kafka exposed to 0.0.0.0/0 on public IP address 34.221.61.64 in public subnet subnet-0549274d2fbcfdba7.	Kafka is a distributed streaming platform that is used to build real-time data pipelines and streaming applications. Exposing the Kafka port to the internet can lead to unauthorized access to the Kafka cluster, which can result in data leakage, data corruption, and data loss.	Modify the security group associated with the EC2 instance to remove the rule that allows ingress from the internet to TCP port 9092 (Kafka).	•ISO27001-2022: A.8.20, A.8.21, A.8.22 •KISA-ISMS-P-2023-korean: 2.6.1, 2.10.1, 2.10.3 •KISA-ISMS-P-2023: 2.6.1, 2.10.1, 2.10.3

Showing 1 to 17 of 17 entries (filtered from 7,073 total entries)

Previous 1 Next