Policy Mapping Report

Policy Name	Policy ID	Cloud Type	Severity	Policy Type	Policy Subtype	Mapped Section	AI Rationale	In Baseline	Confidence	Remediation
'chpasswd' is used to set or remove passwords	0b7074cc-6374-48e1-af28-9d6c07de3fc9	ALL	medium	config	build	N/A	No confident mapping found due to low lexical similarity with any PDF policy section.	FALSE	0	Manual review needed to identify a potential mapping.
'public network access enabled' is not set to 'False' for mySQL servers	0224a383-4c7c-4dca-b52c-f6fab8014666	Azure	medium	config	build	N/A	No confident mapping found due to low lexical similarity with any PDF policy section.	FALSE	0	Manual review needed to identify a potential mapping.
2FA is not enforced in GitHub	af653e16-6742-4076-ada4-13c1d165e78e	ALL	high	config	build	N/A	No confident mapping found due to low lexical similarity with any PDF policy section.	FALSE	0	Manual review needed to identify a potential mapping.
A MySQL database instance allows anyone to connect with administrative privileges	d2a0c2ce-19b3-4894-89d5-b01e8dd0fb5d	Google Cloud Platform	low	config	build	N/A	No confident mapping found due to low lexical similarity with any PDF policy section.	FALSE	0	Manual review needed to identify a potential mapping.
A Policy is not Defined for KMS Key	23a308a5-49b3-4cb6-aab9-ef6b5e8b866f	AWS	medium	config	build	N/A	No confident mapping found due to low lexical similarity with any PDF policy section.	FALSE	0	Manual review needed to identify a potential mapping.
AWS account does not have a password policy	e63a3554-3507-4e0c-a3e9-012b6b858482	AWS	medium	config	build	4.7 Identity and Access Management	The policy name 'AWS account does not have a password policy' has a high lexical similarity with the PDF section 'Identity and Access Management'.	TRUE	75	Define and enforce a strong password policy for all IAM users in the AWS account.
AWS account is not configured with CloudTrail	b3b3b3b3-b3b3-b3b3-b3b3-b3b3b3b3b3b3	AWS	high	config	build	4.14 Logging	The policy name 'AWS account is not configured with CloudTrail' has a high lexical similarity with the PDF section 'Logging'.	TRUE	80	Enable CloudTrail in all regions to log all API activity.
AWS Config is not enabled in all regions	c4c4c4c4-c4c4-c4c4-c4c4-c4c4c4c4c4c4	AWS	medium	config	build	4.15 SIEM Integration	The policy name 'AWS Config is not enabled in all regions' has a moderate lexical similarity with the PDF section 'SIEM Integration' which discusses monitoring.	TRUE	65	

AWS Foundational Security best practices standard is not enabled	d5d5d5d5-d5d5-d5d5-d5d5-d5d5d5d5d5d5	AWS	high	config	build	4.0 Requirements	The policy name 'AWS Foundational Security best practices standard is not enabled' aligns with the general 'Requirements' section of the security standard.	TRUE	85	Enable the AWS Foundational Security Best Practices standard in AWS Security Hub.
AWS Identity and Access Management (IAM) role is configured with full administrative privileges	f6f6f6f6-f6f6-f6f6-f6f6-f6f6f6f6f6f6	AWS	high	config	build	4.11 Privileged Identity Management	The policy name 'AWS Identity and Access Management (IAM) role is configured with full administrative privileges' directly relates to 'Privileged Identity Management'.	TRUE	95	Avoid using full administrative privileges. Apply the principle of least privilege and grant only the permissions required to perform a task.
AWS Key Management Service (KMS) key is not configured with a key rotation policy	a7a7a7a7-a7a7-a7a7-a7a7-a7a7a7a7a7a7	AWS	medium	config	build	4.19.3 Cryptography Requirements	The policy name 'AWS Key Management Service (KMS) key is not configured with a key rotation policy' is related to 'Cryptography Requirements'.	TRUE	70	Enable automatic key rotation for all KMS keys.
AWS Lambda function is configured with a role that has full administrative privileges	b8b8b8b8-b8b8-b8b8-b8b8-b8b8b8b8b8b8	AWS	high	config	build	4.11 Privileged Identity Management	The policy name 'AWS Lambda function is configured with a role that has full administrative privileges' is a specific instance of 'Privileged Identity Management' violation.	TRUE	90	Create a specific IAM role for the Lambda function with only the necessary permissions.
AWS Network Firewall is not configured to log firewall traffic	c9c9c9c9-c9c9-c9c9-c9c9-c9c9c9c9c9c9	AWS	medium	config	build	4.14 Logging	The policy name 'AWS Network Firewall is not configured to log firewall traffic' is directly related to the 'Logging' section.	TRUE	80	Configure AWS Network Firewall to log all traffic for auditing and security analysis.
AWS RDS instance is not encrypted	d0d0d0d0-d0d0-d0d0-d0d0-d0d0d0d0d0d0	AWS	high	config	build	4.19.7 Core Cloud IaaS offerings	The policy name 'AWS RDS instance is not encrypted' is related to the security of core IaaS offerings. The 'Database Security Standard' is mentioned within this section.	TRUE	85	Enable encryption at rest for all RDS instances.
AWS S3 bucket is publicly accessible	e1e1e1e1-e1e1-e1e1-e1e1-e1e1e1e1e1e1	AWS	high	config	build	4.10 Resource Access	The policy name 'AWS S3 bucket is publicly accessible' is a direct violation of proper 'Resource Access' control.	TRUE	95	Block all public access to the S3 bucket unless it is explicitly required for a specific business purpose
AWS Security Hub is not enabled	f2f2f2f2-f2f2-f2f2-f2f2-f2f2f2f2f2f2	AWS	high	config	build	4.15 SIEM Integration	The policy name 'AWS Security Hub is not enabled' is related to 'SIEM Integration' as Security Hub is a central place for security findings.	TRUE	85	Enable AWS Security Hub to get a comprehensive view of your security alerts and security posture across your AWS accounts.

Access to the Kubernetes API server is not restricted to specific IP addresses	a3a3a3a3-a3a3-a3a3-a3a3-a3a3a3a3a3a3	Kubernetes	high	config	build	4.18.1 External Connections	The policy name 'Access to the Kubernetes API server is not restricted to specific IP addresses' relates to securing 'External Connections'.	TRUE	80	Configure the Kubernetes API server to only allow access from authorized IP address ranges.
Administrative privileges are not restricted for containers	b4b4b4b4-b4b4-b4b4-b4b4-b4b4b4b4b4b4	Kubernetes	high	config	build	4.11 Privileged Identity Management	The policy name 'Administrative privileges are not restricted for containers' is a container-specific violation of 'Privileged Identity Management'.	TRUE	90	Do not run containers with root privileges. Use a non-root user or a user with the minimum required privileges.
Allow Privilege Escalation is not set to 'false' for containers	c5c5c5c5-c5c5-c5c5-c5c5-c5c5c5c5c5c5	Kubernetes	high	config	build	4.11 Privileged Identity Management	The policy name 'Allow Privilege Escalation is not set to 'false' for containers' is a critical setting related to 'Privileged Identity Management' in containers.	TRUE	95	Set 'allowPrivilegeEscalation' to 'false' in the security context of your container definitions.
Amazon Elastic Block Store (EBS) snapshots are not encrypted	d6d6d6d6-d6d6-d6d6-d6d6-d6d6d6d6d6d6	AWS	medium	config	build	4.19.7 Core Cloud IaaS offerings	The policy name 'Amazon Elastic Block Store (EBS) snapshots are not encrypted' is related to securing core IaaS offerings.	TRUE	75	Enable encryption by default for all new EBS snapshots.
Amazon Elastic Compute Cloud (EC2) instances are not configured with a security group that restricts traffic	e7e7e7e7-e7e7-e7e7-e7e7-e7e7e7e7e7e7	AWS	high	config	build	4.18.5.9 Security Groups and Network Access Control Lists	The policy name 'Amazon Elastic Compute Cloud (EC2) instances are not configured with a security group that restricts traffic' directly relates to 'Security Groups and Network Access Control Lists'.	TRUE	90	Configure security groups to only allow traffic from necessary sources and ports.