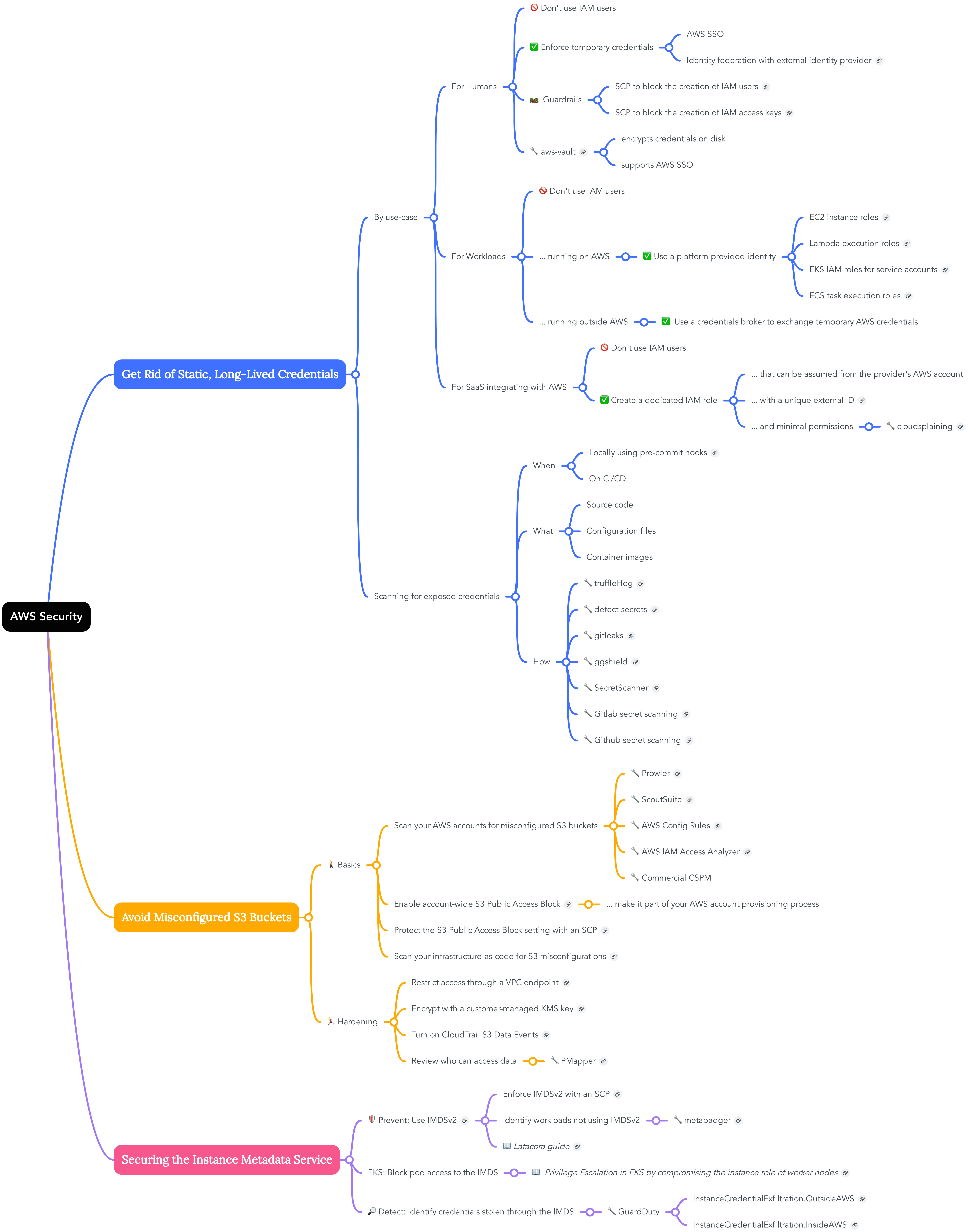

- AWS Security
  - Get Rid of Static, Long-Lived Credentials
    - By use-case
      - For Humans
        - 🚫 Don't use IAM users
        - ✅ Enforce temporary credentials
          - AWS SSO
          - Identity federation with external identity provider 🔗
        - 🚧 Guardrails
          - SCP to block the creation of IAM users 🔗
          - SCP to block the creation of IAM access keys 🔗
        - 🔧 aws-vault 🔗
          - encrypts credentials on disk
          - supports AWS SSO
      - For Workloads
        - 🚫 Don't use IAM users
        - ... running on AWS
          - ✅ Use a platform-provided identity
            - EC2 instance roles 🔗
            - Lambda execution roles 🔗
            - EKS IAM roles for service accounts 🔗
            - ECS task execution roles 🔗
        - ... running outside AWS
          - ✅ Use a credentials broker to exchange temporary AWS credentials
      - For SaaS integrating with AWS
        - 🚫 Don't use IAM users
        - ✅ Create a dedicated IAM role
          - ... that can be assumed from the provider's AWS account
          - ... with a unique external ID 🔗
          - ... and minimal permissions
            - 🔧 cloudsplaining 🔗
    - Scanning for exposed credentials
      - When
        - Locally using pre-commit hooks 🔗
        - On CI/CD
      - What
        - Source code
        - Configuration files
        - Container images
      - How
        - 🔧 truffleHog 🔗
        - 🔧 detect-secrets 🔗
        - 🔧 gitleaks 🔗
        - 🔧 ggshield 🔗
        - 🔧 SecretScanner 🔗
        - 🔧 Gitlab secret scanning 🔗
        - 🔧 Github secret scanning 🔗
  - Avoid Misconfigured S3 Buckets
    - 🚶 Basics
      - Scan your AWS accounts for misconfigured S3 buckets
        - 🔧 Prowler 🔗
        - 🔧 ScoutSuite 🔗
        - 🔧 AWS Config Rules 🔗
        - 🔧 AWS IAM Access Analyzer 🔗
        - 🔧 Commercial CSPM
      - Enable account-wide S3 Public Access Block 🔗
        - ... make it part of your AWS account provisioning process
      - Protect the S3 Public Access Block setting with an SCP 🔗
      - Scan your infrastructure-as-code for S3 misconfigurations 🔗
    - 🏃 Hardening
      - Restrict access through a VPC endpoint 🔗
      - Encrypt with a customer-managed KMS key 🔗
      - Turn on CloudTrail S3 Data Events 🔗
      - Review who can access data
        - 🔧 PMapper 🔗
  - Securing the Instance Metadata Service
    - 🛡 Prevent: Use IMDSv2 🔗
      - Enforce IMDSv2 with an SCP 🔗
      - Identify workloads not using IMDSv2
        - 🔧 metabadger 🔗
      - 📖 *Latacora guide* 🔗
    - EKS: Block pod access to the IMDS
      - 📖 *Privilege Escalation in EKS by compromising the instance role of worker nodes* 🔗
    - 🔎 Detect: Identify credentials stolen through the IMDS
      - 🔧 GuardDuty
        - InstanceCredentialExfiltration.OutsideAWS 🔗
        - InstanceCredentialExfiltration.InsideAWS 🔗

AWS Security

1. Get Rid of Static, Long-Lived Credentials

1.1. By use-case

1.1.1. For Humans

1.1.1.1. :no_entry_sign: Don't use IAM users

1.1.1.2. :white_check_mark: Enforce temporary credentials

1.1.1.2.1. AWS SSO

1.1.1.2.2. Identity federation with external identity provider

Link: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

1.1.1.3. :railway_track: Guardrails

1.1.1.3.1. SCP to block the creation of IAM users

Link: https://asecure.cloud/a/scp_deny_iam_user_creation/

1.1.1.3.2. SCP to block the creation of IAM access keys

Link: https://asecure.cloud/a/scp_deny_iam_user_creation/

1.1.1.4. :wrench: aws-vault

Link: https://github.com/99designs/aws-vault

1.1.1.4.1. encrypts credentials on disk

1.1.1.4.2. supports AWS SSO

1.1.2. For Workloads

1.1.2.1. :no_entry_sign: Don't use IAM users

1.1.2.2. ... running on AWS

1.1.2.2.1. :white_check_mark: Use a platform-provided identity

1.1.2.2.1.1. EC2 instance roles

Link: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

1.1.2.2.1.2. Lambda execution roles

Link: https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html

1.1.2.2.1.3. EKS IAM roles for service accounts

Link: https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html

1.1.2.2.1.4. ECS task execution roles

Link: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task_execution_IAM_role.html

1.1.2.3. ... running outside AWS

1.1.2.3.1. :white_check_mark: Use a credentials broker to exchange temporary AWS credentials

1.1.3. For SaaS integrating with AWS

1.1.3.1. :no_entry_sign: Don't use IAM users

1.1.3.2. :white_check_mark: Create a dedicated IAM role

1.1.3.2.1. ... that can be assumed from the provider's AWS account

1.1.3.2.2. ... with a unique external ID

Link: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

1.1.3.2.3. ... and minimal permissions

1.1.3.2.3.1. :wrench: cloudsplaining

Link: https://github.com/salesforce/cloudsplaining

1.2. Scanning for exposed credentials

1.2.1. When

1.2.1.1. Locally using pre-commit hooks

Link: https://pre-commit.com/

1.2.1.2. On CI/CD

1.2.2. What

1.2.2.1. Source code

1.2.2.2. Configuration files

1.2.2.3. Container images

1.2.3. How

1.2.3.1. :wrench: truffleHog

Link: https://github.com/trufflesecurity/truffleHog

1.2.3.2. :wrench: detect-secrets

Link: https://github.com/ibm/detect-secrets

1.2.3.3. :wrench: gitleaks

Link: https://github.com/zricethezav/gitleaks

1.2.3.4. :wrench: ggshield

Link: https://github.com/GitGuardian/ggshield

1.2.3.5. :wrench: SecretScanner

Link: https://github.com/deepfence/SecretScanner

1.2.3.6. :wrench: Gitlab secret scanning

Link: https://docs.gitlab.com/ee/user/application_security/secret_detection/

1.2.3.7. :wrench: Github secret scanning

Link: https://docs.github.com/en/code-security/secret-scanning/about-secret-scanning

2. Avoid Misconfigured S3 Buckets

2.1. :walking: Basics

2.1.1. Scan your AWS accounts for misconfigured S3 buckets

2.1.1.1. :wrench: Prowler

Link: https://github.com/prowler-cloud/prowler

2.1.1.2. :wrench: ScoutSuite

Link: https://github.com/nccgroup/ScoutSuite

2.1.1.3. :wrench: AWS Config Rules

Link: https://docs.aws.amazon.com/config/latest/developerguide/s3-bucket-public-read-prohibited.html

2.1.1.4. :wrench: AWS IAM Access Analyzer

Link: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html

2.1.1.5. :wrench: Commercial CSPM

2.1.2. Protect the S3 Public Access Block setting with an SCP

Link: https://asecure.cloud/a/scp_s3_block_public_access/

2.1.3. Enable account-wide S3 Public Access Block

Link: https://docs.aws.amazon.com/AmazonS3/latest/userguide/configuring-block-public-access-account.html

2.1.3.1. ... make it part of your AWS account provisioning process

2.1.4. Scan your infrastructure-as-code for S3 misconfigurations

Link: https://blog.christophetd.fr/shifting-cloud-security-left-scanning-infrastructure-as-code-for-security-issues/

2.2. :runner: Hardening

2.2.1. Restrict access through a VPC endpoint

Link: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html

2.2.2. Encrypt with a customer-managed KMS key

Link: https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-access-default-encryption/

2.2.3. Turn on CloudTrail S3 Data Events

Link: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html

2.2.4. Review who can access data

2.2.4.1. :wrench: PMapper

Link: https://github.com/nccgroup/PMapper

3. Securing the Instance Metadata Service

3.1. :shield: Prevent: Use IMDSv2

Link: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

3.1.1. Enforce IMDSv2 with an SCP

Link: https://github.com/nccgroup/PMapper

3.1.2. Identify workloads not using IMDSv2

3.1.2.1. :wrench: metabadger

Link: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

3.1.3. :book: Latacora guide

Link: https://docs.google.com/document/d/1X737xoQviufdxZk_l33bnpp6noOmNIYvMilQCdhtwoY/edit

3.2. EKS: Block pod access to the IMDS

3.2.1. :book: Privilege Escalation in EKS by compromising the instance role of worker nodes

Link: https://blog.christophetd.fr/privilege-escalation-in-aws-elastic-kubernetes-service-eks-by-compromising-the-instance-role-of-worker-nodes/

3.3. :mag_right: Detect: Identify credentials stolen through the IMDS

3.3.1. :wrench: GuardDuty

3.3.1.1. InstanceCredentialExfiltration.OutsideAWS

Link: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-iam.html#unauthorizedaccess-iam-instancecredentialexfiltrationoutsideaws

3.3.1.2. InstanceCredentialExfiltration.InsideAWS

Link: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-iam.html#unauthorizedaccess-iam-instancecredentialexfiltrationinsideaws