THREAT MODELING CONNECT

THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE

THREAT 20
MODCON 23

Continuous Threat Modelling in Cloud Environments

Agenda

- About me
- Rate of change data
- How can I be impacted?
- Is change good or bad?
- How to be aware
- How not to be overwhelmed
- Maintain velocity and improve security
- Example workflows
- Q&A

About me

CTO @ TrustOnCloud

Previously worked with security-related service teams at AWS

Rate of change data

- API's are the best* method of understanding the possibilities of what a customer can do in the cloud.

- AWS
  - 2022 23% additional / updated API's
- Azure
  - 2022 28% additional / updated APIs
- GCP
  - 2022 25% additional / updated APIs

How can I be impacted?

1. API’s
2. Permissions
   1. Do you use managed roles?
   2. Do you have a ‘*’s somewhere in your permission policies?
3. Portal / CLI defaults

THREAT MODCON 2023

Is change good or bad?

Good.. new, improved controls for your existing threats!

- Amazon S3 Block Public Access
- Azure Storage copy scope
- GCP Vertex AI additional logging options

Not so good, new features can be abused…

- AWS, new GetClusterSessionCredentials API for Amazon EMR
  Allows for retrieving login credentials to EMR
- Azure, new SFTP feature for Azure Storage
  Creates local (non federated) users
- GCP, new database extension
  Allows easier outbound access from the database

How to be aware

From the Cloud Providers:

AWS APIs: https://github.com/boto/boto3

AWS Permissions: https://docs.aws.amazon.com/service-authorization/latest/reference/reference.html

Azure APIs: https://github.com/Azure/azure-rest-api-specs

Azure Permissions: Get-AzProviderOperation or az provider operation list

Microsoft Graph changelog: https://developer.microsoft.com/en-us/graph/changelog

GCP APIs: https://discovery.googleapis.com/discovery/v1/apis (and some coding)

GCP Permissions: https://cloud.google.com/iam/docs/permissions-reference

3rd party tracking sites (some offer RSS):

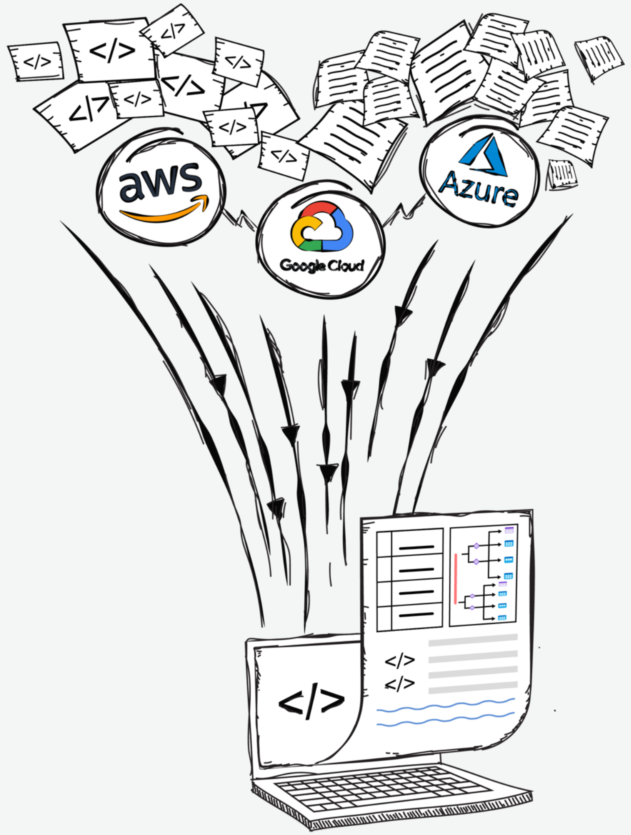
AWS APIs: https://awsapichanges.info/ , https://awsapichanges.com/

AWS Permissions: https://awsiamchanges.com/, https://github.com/iann0036/iam-dataset

Azure Permissions: https://www.azadvertizer.net/, https://azureiamchanges.com

GCP APIs: https://github.com/iann0036/iam-dataset, https://gcpapichanges.com/

GCP Permissions: https://github.com/iann0036/iam-dataset



How not to be overwhelmed

1. Know your environment and organizational structure
    1. Asset and configuration management
    2. Have clearly defined RACI’s
2. Reduce your impact
    1. Don’t use managed roles
    2. Maintenance windows
    3. Don’t rely on defaults
3. Consumable artifacts
    1. Your IaC of choice solution here, with known good artifacts shared through your organization
4. Principle of least privilege

Maintain velocity and improve security

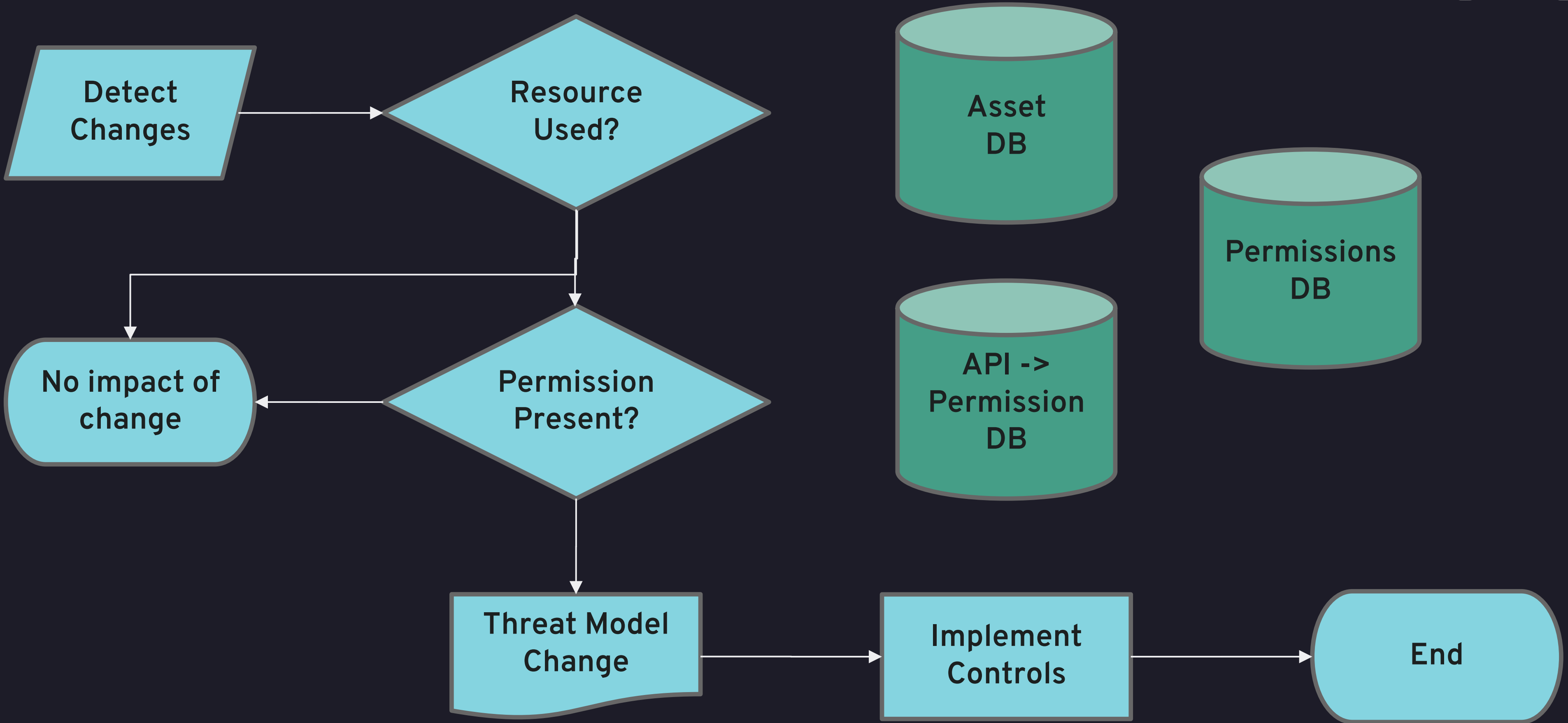
Triage the deluge

Ask yourself the following questions:

1. Is this impacting a type of resource that we are using?
2. If so does anyone/anything in my environment have the ability to execute this new feature?
3. If they can execute it, what would the threat be?
4. What's the sensitivity of the environments in which this threat can be executed?

Knowing your environment is key

Putting it tother, optimized workflow with components



Workflow challenges

1. Permission Inventory
    1. Knowing what is possible in your environment is difficult, automated reasoning is not trivial
2. API -> Permission Mapping
    1. Not all CSPs publish the permission(s) required to execute an API
3. CSP undocumented APIs / API changes

Q&A