AccessModeler

Introducing AccessModeler™

Cloud environments are complex structures. Identity and access management (IAM) is complicated by the identities, roles, groups and policies setup within the cloud. Understanding access requires a deep dive into the infrastructure to uncover all the privileges an identity has. Failure to control access properly can result in hundreds of thousands of dollars in fines.

Insider threats are on the rise, both in frequency and impact.

AccessModeler assesses your configurations and activity logs to reveal what access someone and/or something has and what they have been using.

Privilege Escalation

- Privilege aggregation through a cascade of roles, groups and policies can lead to elevated access up to and including admin level
- Tracking which roles and groups an entity is associated with and the policies assigned to each is a daunting task

27% of users had more access to data than needed

Insider threats are increasing by almost 50% every year[1]

Over Privilege

- Privilege escalation leads to an over privileged condition
- Toxic combinations occur when a user is assigned to multiple roles, each role having access to different tasks in a business process resulting in an unacceptable fraud risk
- Access creep occurs through cloud infrastructure

58% of companies found over 1,000 folders that had inconsistent permissions

Data Privacy

- Penalties for non-compliance with privacy protection laws and regulations have become exorbitantly expensive
- Visualization of access rights in context to the data types and protections required has become a top priority for companies worldwide
- An entity can have more access than it should causing a privacy breach

53% of companies found over 1,000 sensitive files exposed to ALL employees

Average costs of insider threats is over $11 million yearly[2]

Data Exfiltration

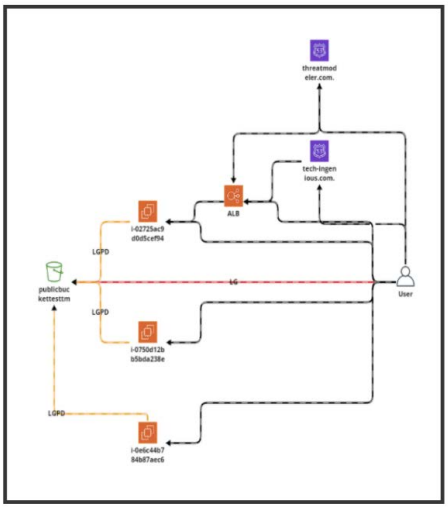
- Tracking data movement is exceeding difficult in a cloud environment
- Data exfiltration is made possible by excessive and/or aggregated access rights and privileges

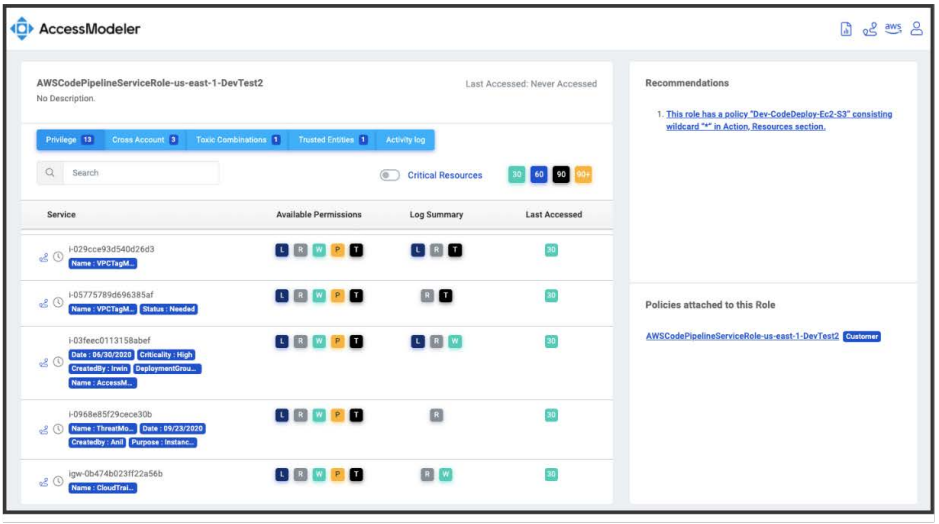
On average, every employee has access to over 17 million files

AccessModeler Solution

AccessModeler aligns AWS best practices with a deep dive into the policy configurations of your enterprise cloud setup. This visibility uncovers identity and access management issues so that your corporation can take action to defend from privacy and exfiltration concerns.

- **AccessModeler helps you to visualize existing granted permissions**
- **AccessModeler helps you to follow the map of who can access your crown jewels**
- **AccessModeler helps you to follow how data can be exfiltrated**





Discover
Human and machine identities, resources and access entitlements

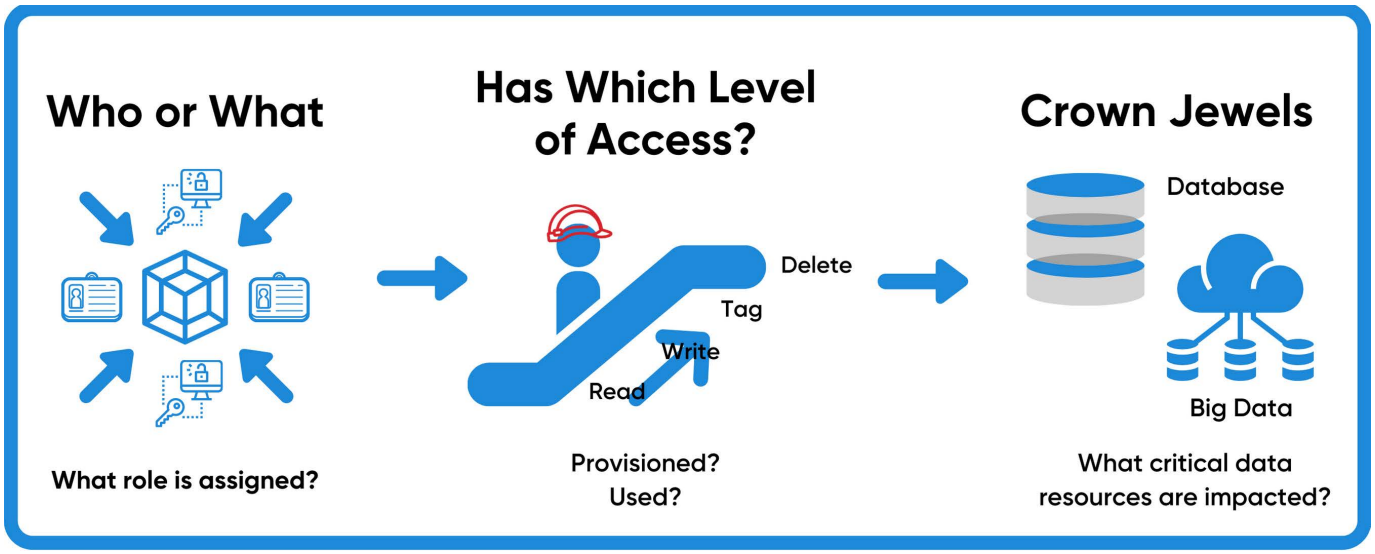
Identify
Toxic combinations that are high risk

Detect
Least privilege violations by comparing access granted versus access used

Analyze
Cascading cross account access between trusted and trusting accounts

Track
Critical assets and provide actionable access recommendations

Respond
By visualizing attack vectors and simulate policies before deployment



Increased visibility and contextual awareness of user and machine access

1 - https://www.observeit.com/cost-of-insider-threats/
2 - https://www.observeit.com/2020costofinsiderthreat/