Aws: cloud trial

It service that enables, compliance , governance , operting audtiing and Risk auditing.
It start monitoring all the api activity in aws acount (console sdks , cli and other aws services)
Use cases:
1) **Compliance aid:**
It ensures compliances with internal policies and regulatory standard by providing a history of activity in your aws account.
[Log audit activity]
2)**Security Analysis:**
Perform security analysis and detect user behavior patterns.

Cloud trial is set up to log user activity.
⬇
Logs are sent to s3 buckets, and it can also stream to cloud watch logs
⬇
Log management and analytics solution retrieve the logs(siem)
⬇
User activity is analyzed for malicious behavior

Action is taken an identified security threat .
3) **Data exfiltration:**
It can detect data exfiltration with API events monitored by cloud watch events and aws lambda.

Data events logging is enabled in cloud trial for s3 bucket
⬇
cloud watch event rule is created to forward data event activity to a lambda function.
⬇
s3 activity hours
⬇
Unusual activity is detected by the lambda function based on preset rules and sns notification is sent to security team to review and take action.

4) **Operational Issues:**
Troubleshoot operational issues by leveraging the aws api call history produced by aws cloud trail.

An aws resource change causes an operational issue.
⬇
Api activity history is reviewed from the cloud trial console
⬇
Search results are filtered by impacted resource name
⬇
Capture details, including what changes was made and by whom are reviewed.
⬇
Corrective action is taken to resolve the issues.