Amazon
EC2

Port change is made to EC2
security group

Cloud Trail

Logs are sent to Cloud Trail

CloudWatch

Cloud Watch Event Rule

Lambda

Lambda Function parses log
data from event and sends
alert message via web hook

Alert received

S3

Cloud Trail Logs Stored in S3
bucket

CloudWatch Rule Triggers
Lambda

Severity colors in Slack based on AWS Trusted Advisor metrics