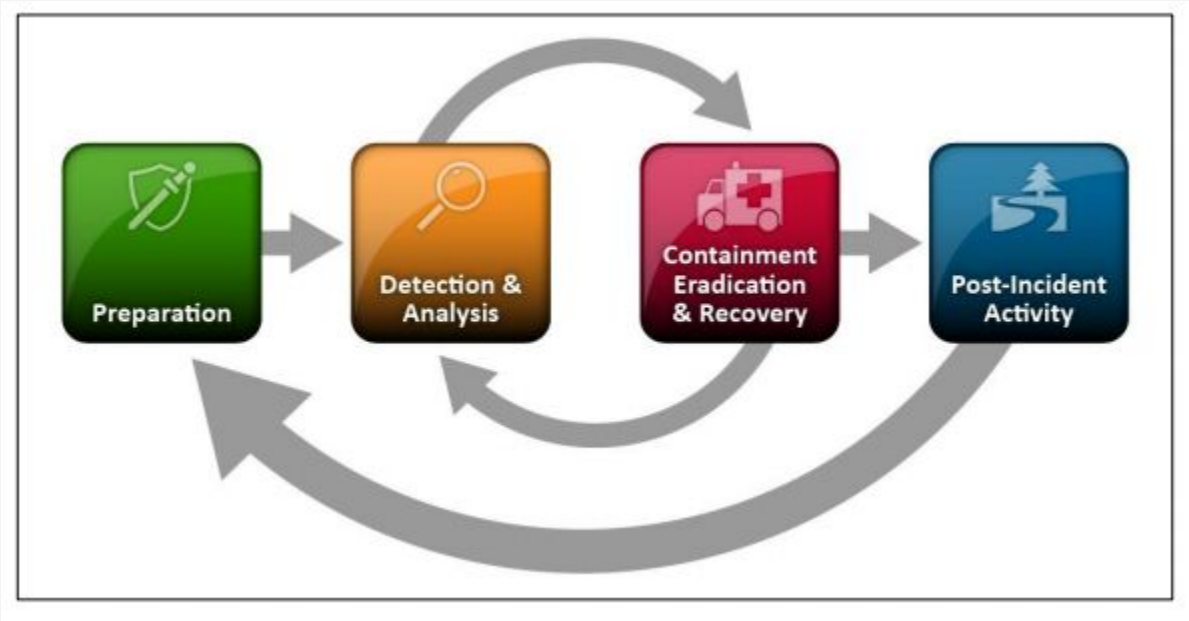
Build an Incident Response Program from Scratch

Richard Julian

What is Incident Response Exactly?



AWS Tooling for Incident Response - Metrics/Collection

CloudWatch | Eventbridge | Macie | GuardDuty



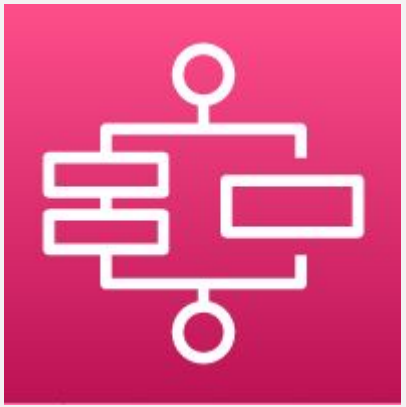

AWS Tooling for Incident Response - Notification

Simple Notification Service | Incident Manager

AWS Tooling for Incident Response - Containment

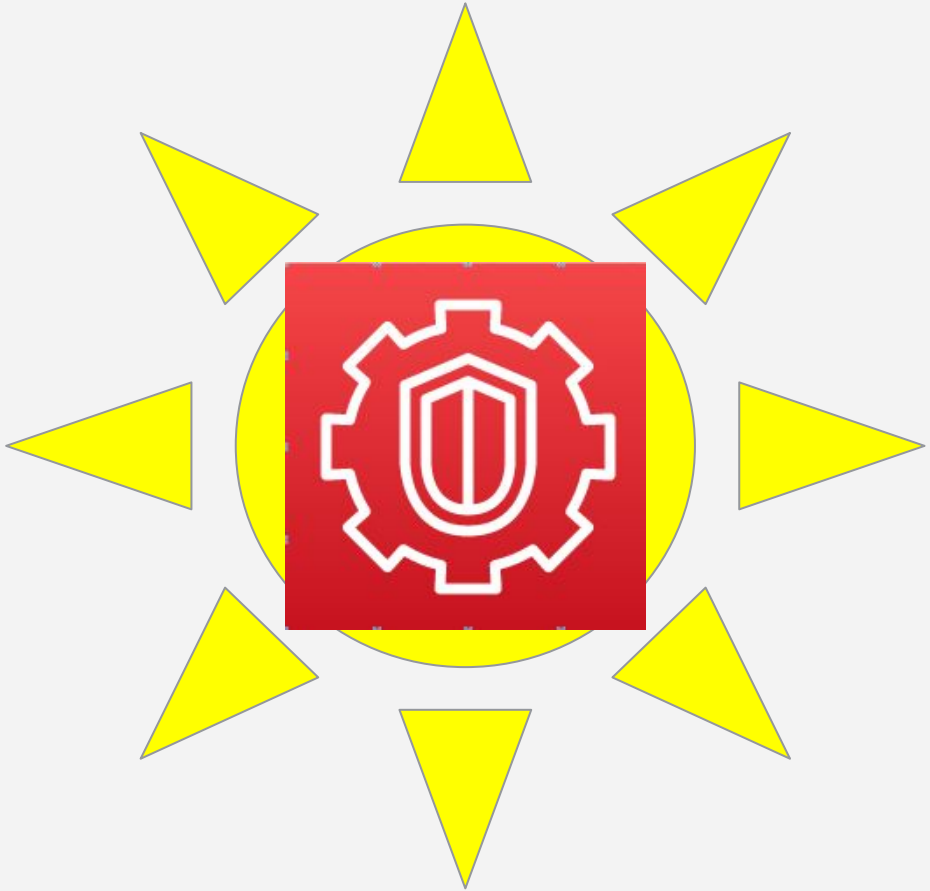
Incident Manager | Lambda | Step Functions | Security Hub



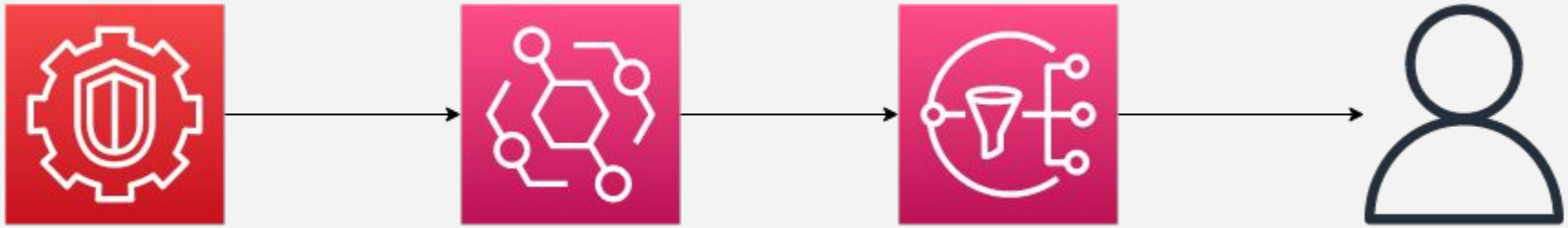



IR Level 0: No Incident Response

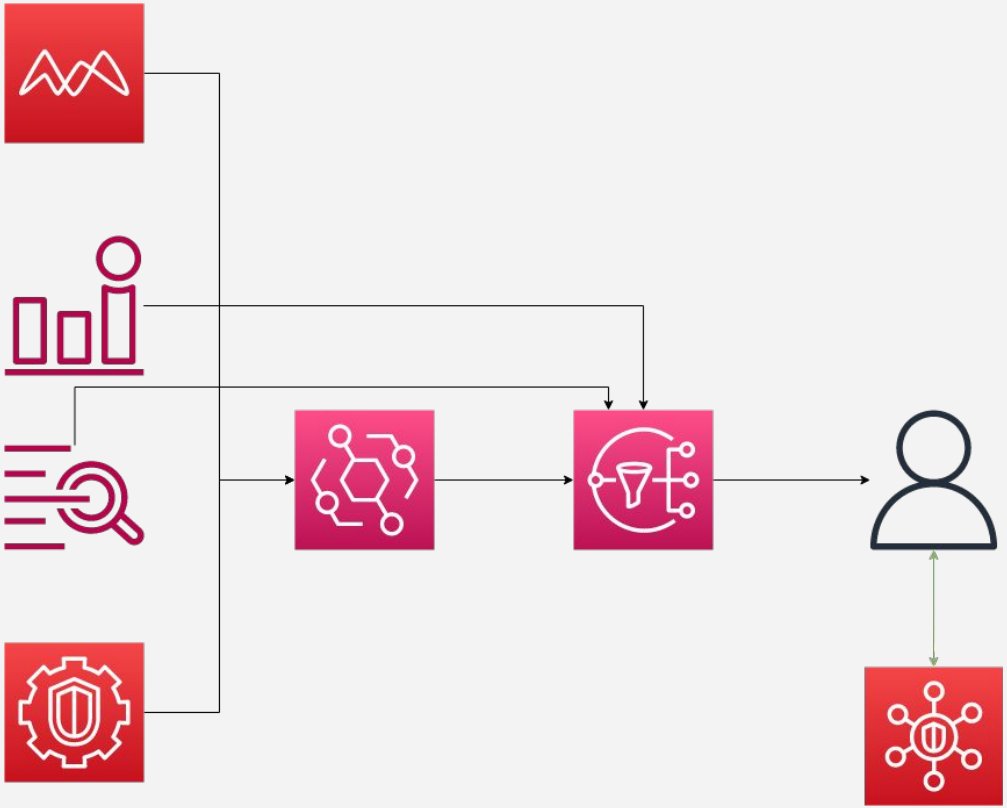
IR Level 20: Just a little more than absolutely nothing.



IR Level 40: The Basics

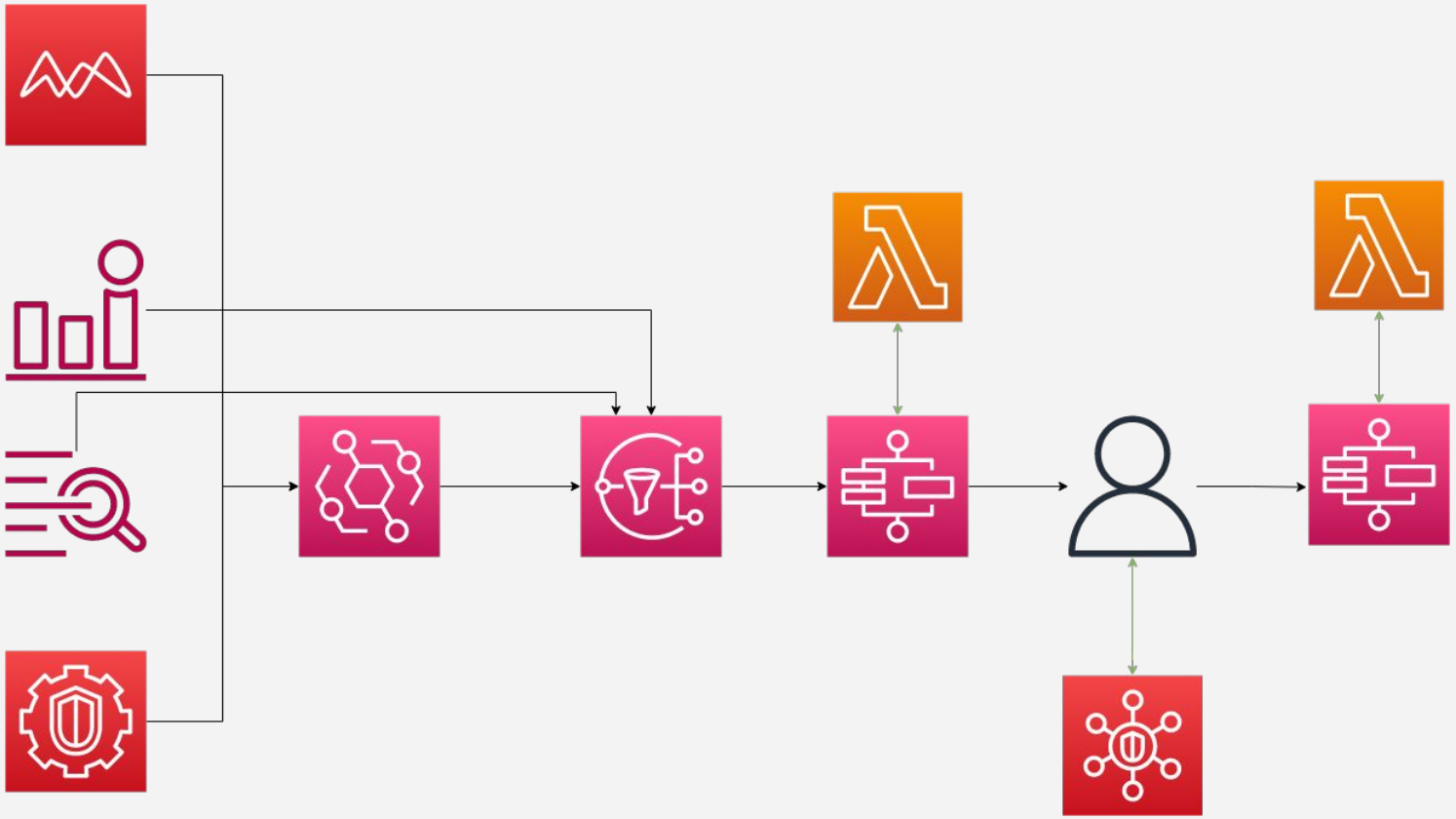


IR Level 60: Enhanced Inspection and Auditing



IR Level 80: Procedural Response

IR Level 100: Automation Automation Automation



Resources

- NIST Computer Incident Response Handling Guide (SP 800-61r2): https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- https://github.com/rjulian/aws-incident-response-bootstrap
- https://aws.amazon.com/products/security/