

AWS Services

RDS

CloudTrail

VPC Flow Logs

EKS

Network Firewall

WAF

Amazon CloudWatch

Servers & AD

AD: Winlogbeat

EC2: Filebeat / Auditbeat

Elastic Agent (AWS
Integrations)

Elasticsearch Cluster

SIEM UI

Elastalert

