Update for 2019

AD Federation w/ AWS (AD integrated)

* Twoway trust 양방향신뢰 ★
* [ADFS = trusted IdProvider ★
  AWS = trusted Relying Party]
  (user마다 consume 안해도됨)

ADFS : 마이크로소프트 SSO구현체
SAML 기반으로의 SSO 서비스

SAML structure진, (entity portal?)
ActiveDirectory 도구

① AD returns user info 8 group membership
② ADFS gives SAML token to AWS signin endpoint
③ AWS signin endpoint request STS AssumeRolewith SAML 호출
④ STS가 temp creds sign endpoint로전달
⑤ AWS signin endpoint → AWS mgmt console로 리다

security standards compliance
준수를 보여주는 것.

AWS artifact

Artifact inspection, Deep packet inspection

(가능) 규제사항준수 인증을 확인가능
규제사항요구에 충족하는 문서제공
ISO 27001, 8bc etc

Packet Inspection

Amazon 서비스에서는 불가
but 3rd party 를 이용하면가능 { WAF, HostIPS, WAF, VPC flow logs}
AWS 마켓플레이스에서
서드파티 3rd party 솔루션구매 or @market place

user defined parameter 저장서비스
├ Parameter store
[license, parameter-store 저장
  설정값, 암호화키값 저장)
  free.공짜 (대부분)
  AWS system manager 의 일부분임

Secret manager

DB계정을 안전하게 저장관리하는서비스
(at rest - kms / in transit encryption) 지원
∘ RDS creds (MySQL, PostgreSQL, Aurora)
∘ nonRDS DB creds
∘ key value pair~CSH, API keys)
∘ autoRFC built in Rotation ★
회전주기설정, 주기지나면 생성 secretmanager
암호화저장, 회전주기 오면 새로운키로 변경

Athena

interactive query source(w SQL standard
no need to deploy/provision
serverless 서버가 없다
★ 장, 단점 : 특정 데이터 analyze시 유용
비즈 / cost 2usage reports 등에 유용.
★암호화 S3에서 지원가능

Magic (Macie)

machine learning AI svc to find
Sensitive data (PII) 기밀정보 기밀정보를 찾는(AISVC)
reports .Dashboard 2cloudwatch events
데이터에 누가접근 accessed되는지 모니터링
PCI DSS 기준으로 규제준수
S3 D-cloudtrail에 기록된 permissions변경사항
사용자 로그인 시도 quantity of cloudtrail logs 등의
volume of DNS + VPC logs 등도
제공함 cloudwatch event로 DataRedcmp upstore (bydefault)
cloudwatch events로 후다 통보 알림등도
AWS service Role for Amazon(cloud) Duty

Guard Duty

Monitor cloudtrail, VPC, DNS logs
McAfee threadmicro외 feed update   (외부)
threat detect svc
위협감지, 외부위협, 외부위협탐지 탐지가능
샘플 sample finding report로
결과조회 가능.

SES

simple email service (SMTP)
기본적으로 TCP port 25를 이용. throttle by default
transmit 하려는경우 2587, 98 Port이용
all notification to SMTP endpoint
MUSTbe encrypted/암호화되어야함/w TLS