Exploring applications security services

Questions	Notes
Web application Firwall (WAF)	- WAF helps you protect your web applications against common web attacks - Protects apps against common attack patterns - Protects against SQL iinjection - Protects against cross-site scripting **In The Real world:** - Protect your web application from cross-site scripting attacks (XSS): you can deploy a web application directly to an EC2 instance and protect it from cross-site scripting attacks using [WAF.You](WAF.You) can even deploy WAF on Cloudfront as part of your CDN solution to block malicious traffic.
DDOS Attacks	A DDos attack causes a traffic jam on website or web application in an attempt to cause it to crash
Sheild	- Always-on detection - Sheild standard is free: provides free protection against common and frequently occuring attacks - sheild advanced is a paid service: provides enhanced protections and 24/7 access to aws experts for a fee - DDoS protection via Shield advanced is supported on several services: - CloudFront - route 53 - Elastic Load balancing - Aws global accelerator
Macie	- Macie helps you discover and protect sensitive data - uses machine learning - evaluate S3 environment - Uncovers personally identifiable information(PII)
things to remember to the EXAM	- WAF: protects against SQL injection and cross-site scripting attacks - Macie : Helps you find sensitive information - Sheild: provides DDOS protection and works with CloudFront , Route53 , Elastic load balancer , and aws global accelerator