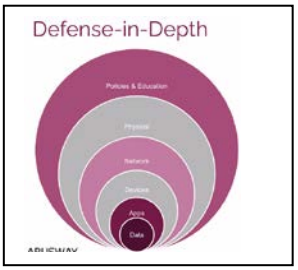
AWS Security (WAF)

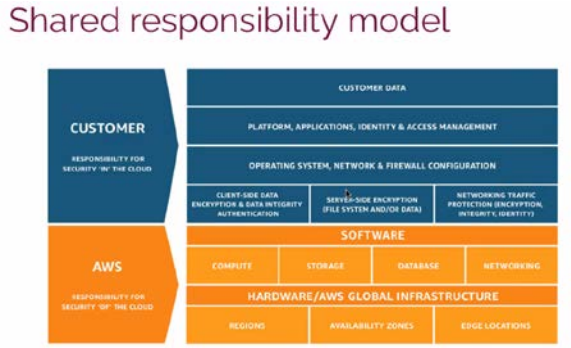
- Genel olarak siber güvenlik derinlemesine koruma (**defense-in-depth**) olarak bilinmektedir.
- DevOps (development operations) ilave olarak siber güvenlik dahil edildiği zaman DevSecOps (development security operations) olarak güvenlik kontrolleri de dahil edilmiştir.
- **CIA Prensibi** (Confidentiality *(Gizlilik esastır)*,Integrity *(Korunan bir datanın değişmediği ve müdahale edilmediği)*,Availability *(Güvenilir olarak zamanında erişebilmek)*)
- **Defense-in-depth (derinlemesine savunma),** bilginin korunması için en çok kullanılan bir yöntemdir. Katmanlı bir şekilde bilgi korunmaktadır. Her bir katmanda o katmanın güvenlik özelliğini devreye sokarak sistemin veya verinin korunmasıdır. **Katmanlar;**
    1. Policies & Education
    2. Physical
    3. Network
    4. Devices
    5. Apps
    6. Data



- **Detective:** Tehditin tanımlanması ve ortaya konulmasıdır.
- **Preventative:** İşlemin otomatik olarak yapılmasının engellenmesi durumudur.
- Sektörler çalışma alanlarına göre uymaları gereken belli başlı standartları vardır: NIST, HIPAA, PCI, FedRAMP, FISMA vb. gibidir.
- **Security Solutions:**
    1. **Encryption:** Verinin şifrelenmesi, verinin anlamsız hale getirilerek iletilmesidir.
    2. **Firewall:** Inbound ve outbound kontrolleri yapmaktadır. Yazılım veya donanım üzerinde kurulabilmektedir.
    3. **Web Application Firewall (WAF):** Bir web uygulamasına giden ve uygulamadan gelen tüm HTTP trafiğini filtreler, inceler ve bloklar. WAF, web uygulamasını veya web sitesini barındıran sunucu ile istemci istekleri arasında gelir. Herhangi bir tehdit varsa, istemci istekleri web sunucusuna iletilmeden önce WAF tarafından ele alınır. OSI modelinde Layer 7 ye hizmet vermektedir.
        - **(i) Cross Site Forgery :** Web uygulamasını kullanmakta olan kullanıcıların istekleri dışında işlemler yürütülmesidir.
        - **(ii) Cross Site Scripting (XSS):** Genellikle web uygulamalarında bulunan bir tür bilgisayar güvenlik açıklığıdır. XSS, diğer kullanıcılar tarafından görüntülenen web sayfalarına istemci taraflı kodun enjekte edilmesine imkân verir.
        - **(iii) SQL Injection:** Bir güvenlik açığıdır. Burada web uygulamasında yapılan SQL sorgusuna müdahale edilir ve veri tabanında bulunan verilere yetki dışı erişim sağlanır. Admin yetkilerini almak için ekstra sorgu atılmaktadır.
        - **(iv) DDOS Attack:** Bu tür saldırılar, bir şirketin web sitesini sağlayan altyapı gibi, herhangi bir ağ kaynağı için geçerli olan belirli kapasite sınırlarından faydalanır.
    4. **Host-Based Firewall:** Server'ı korumak amacıyla kullanılan güvenlik duvarı çeşididir. IP, port ve protocol üzerinden OSI model Layer 3 ve 4'te çalışmaktadır.
    5. **IDS (Intrusion Detection And Prevention):** Bu güvenlik sistemlerinin amacı zararlı hareketi tanımlama ve loglama yapmaktır. IPS ise ağ trafiğiniz içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti ile önlenmesi için kullanılan güvenlik sistemleridir. IDS (Intrusion Detection System) saldırıları tespit etmeyi amaçlarken IPS (Intrusion Prevention System) sistemleri saldırıyı durdurma, önleme üzerine kurgulanmıştır. 4 tip algoritmaya göre çalışmaktadır:
        a. Signature-based detection
        b. Anomaly-based detection
        c. Stateful protocol analysis
        d. Reputation analysis

6. **Security Information and Event Management System(SIEM):** Gelen log'ları inceleyerek bir sonuç çıkararak bir karar verilmesidir. SIEM, ağ ortamından çok büyük miktarda veri toplar(log), bu verileri birleştirir ve insanlar tarafından erişilebilir hale getirir.
7. **Vulnerability Scanners:** Bilgisayarları, ağları veya uygulamaları bilinen zayıflıklar açısından değerlendirmek için tasarlanmış bir bilgisayar programıdır. Bu tarayıcılar, belirli bir sistemin zayıf yönlerini keşfetmek için kullanılır. Güvenlik duvarı, yönlendirici, web sunucusu, uygulama sunucusu vb. gibidir.

- **AWS Security Services:** Bu servisin güvenli olabilmesi ve stabil çalışması için aşağıda belirtilen **"**Shared responsibility" modele göre sistem ayağa kaldırılmalıdır;



- **AWS Key Management Service (KMS):** Birçok **AWS** hizmetinde ve uygulamalarda şifreleme anahtarları oluşturup yönetilmesini ve bunların kullanımının denetlenmesini kolaylaştırır.

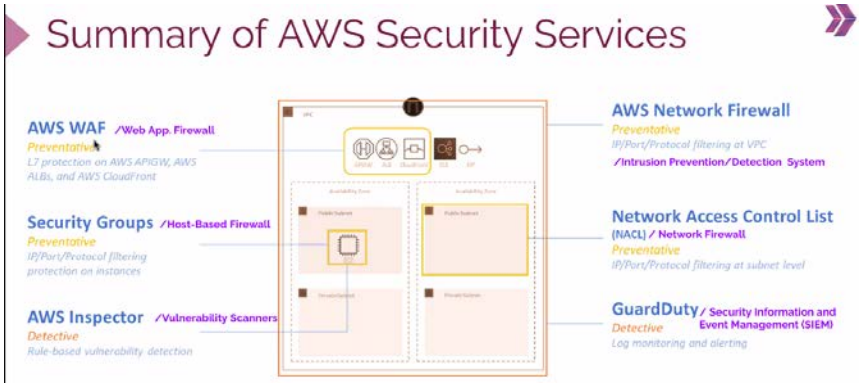
KMS Key Types

Type of KMS Key	Specific to Account?	Customer Manages?	Automatic Rotation	Key Policy Possible?
Customer Managed Key	Yes	Yes	Optional	Yes
AWS Managed Key	Yes	No	Every 3 yrs.	No
AWS Owned Key	No	No	AWS Dependent	No

- **Security Groups and NACLs :** Security grouplar host base ve Network Access Control List firewall olarak düşünülebilmektedir.

- **AWS WAF:** Web uygulamalarının veya API'lerin erişilebilirliği etkileyebilecek, güvenliği tehlikeye atabilecek veya aşırı kaynak kullanabilecek yaygın web açıklarına ve botlara karşı korunmaya yardımcı olan bir web uygulaması güvenlik duvarıdır. (create a policy, block&filter,monitor)

- **AWS Network Firewall:** Tüm VPC'ler için temel ağ korumalarını dağıtmayı kolaylaştıran yönetilen bir hizmettir. İzinsiz giriş önleme sistemi (IPS), imza tabanlı algılama kullanarak güvenlik açığından yararlanma durumlarını belirleyebilmek ve engelleyebilmek için etkin trafik akışı denetimi sağlar.
- **AWS Inspector:** AWS üzerinde dağıtılmış olan uygulamaların güvenlik ve mevzuat uyumluluğu seviyesini geliştirmeye yardımcı olan otomatik güvenlik değerlendirmesi hizmetidir. Amazon Inspector, uygulamaları güvenlik açıkları ve en iyi uygulamalardan sapma açısından otomatik olarak değerlendirir.
- **AWS Guard Duty:** AWS hesaplarını, iş yüklerini, Kubernetes kümelerini ve Amazon Simple Storage Service'ta (Amazon S3) depolanan verileri korumak için kötü amaçlı etkinlikleri veya anormal davranışları sürekli olarak izleyen bir tehdit algılama hizmetidir.
- **AWS Security Hub:** En iyi uygulama denetimleri gerçekleştiren, uyarıları toplayan ve otomatik düzeltme sağlayan bir bulut güvenliği durum yönetimi hizmetidir.
- **AWS Shield:** AWS üzerinde çalışan uygulamaları koruyan bir yönetilen *Dağıtılmış Hizmet Engelleme* (***DDoS(Denial-of-service attack)***) koruması hizmetidir. AWS Shield tarafından sunulan, uygulama kesinti ve gecikme süresini en aza indiren her zaman açık algılama ve otomatik satır içi risk azaltma özellikleri sayesinde DDoS korumasından yararlanmak için AWS Support ekibine ulaşmanıza gerek kalmaz.



Summary of AWS Security Services

AWS Security Service	Protects Against	Applies To	Similar To
Security Groups	Unauthorized access to VPC resources	Instance @ Layer 3, 4 (IP, Port, Protocol)	Host-based Firewall
Network Access Control List (NACL)	Unauthorized access to VPC resources	Subnet @ Layer 3, 4 (IP, Port, Protocol)	Network Firewall
AWS WAF	Web attacks e.g. SQL Injection, cross-site scripting	Layer 7 (HTTP)	WAF
AWS Network Firewall	Malicious network intrusion	Layer 3, 4, 7	IPS / IDS
Guard Duty	Malicious network traffic	Log analysis	SIEM
AWS Inspector	Exploitable vulnerabilities	EC2, ECR	Vulnerability scanner
SecurityHub	Provides single pane of glass view	Network, accounts	SIEM