# AWS Security

Tuesday, September 10, 2024 9:52 PM

## Today's Topics

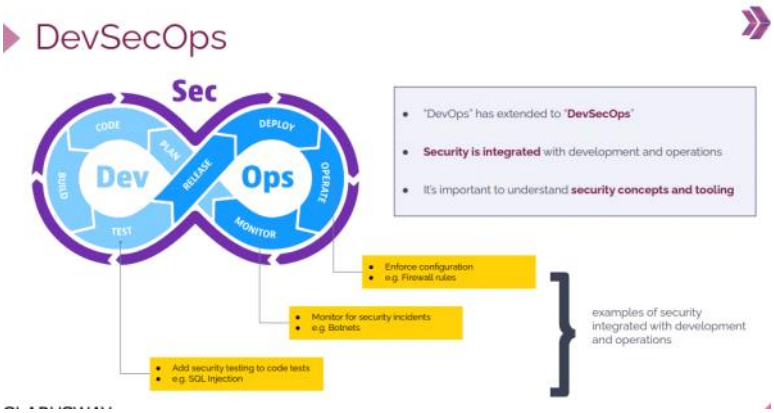
- General Cyber Security Concepts
- Cyber Security Tools & Technology
- AWS Security Tools & Technology

## Outcomes

By the end of the class, you should be able to ...

- **Explain defense-in-depth**
- **Describe various security tools and what purpose they serve**
- **Explain AWS security tooling and how it supports defense-in-depth**

## 1 General Cyber Security Concepts

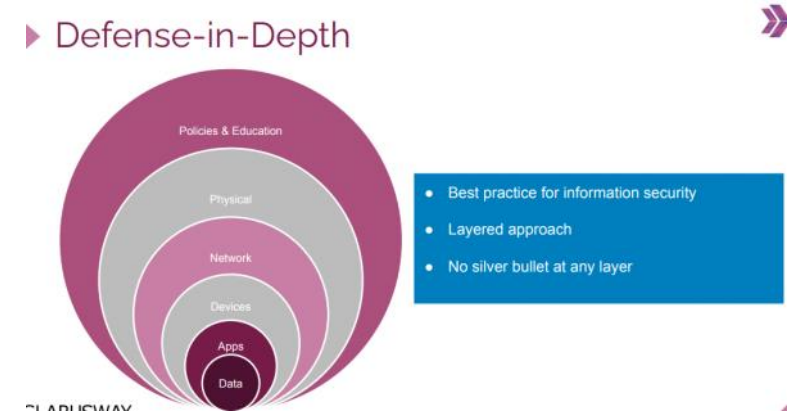



Devops cyclein icine bir de son zamanlarda DevSecOps diye birsey girdi.
Olay bu safhaya gelene kadar security kismi artmaya basldi. Mesela test yaparken testlerin icine SQL injectionlarla guvenli hale getirelim vs gibi ekstra guvenlik onlemleri alinmaya baslandi.
Securtiy kismiyla biz ilgilenmiyoruz ama bu sahne bize ait o yuzden bu konulari da bilmeliyiz.
Mesela kod yzan adamin maksimum duzeyde guvenligi dikkate alark yazip yazmadigini kontrol etmedigini kontrol etmen gerekebiliyor. Ve bunun uzerinden not veriyorsun. Geri donut olarak su kadar daha test guvenligini arttir vs gibi yorumlar yapabiliyorsun.
Bir saldiri var mi yok mu bunlari kontrol ediyorsun. Olay artik tum devops cycleina da sarmis bulunuyor.
SAST ve DAST diye iki kavram var devops kisminda sikca duyabiliriz.

While SAST examines code at rest to identify security flaws before deployment, DAST simulates attacks on live applications to find vulnerabilities that are only visible during execution. Together, SAST and DAST provide a comprehensive approach to security testing, covering both pre-deployment code analysis and post-deployment vulnerability assessment.

Yani kod deploy edilmeden butun guvenlik testlerin yapilm samasi SAST.
Deploy sonrasi gercek bir site uzerine ataklar yaparak guvenligini kontrol ettikleri sistem ise DAST.


Cyber securityde CIA diye bir prensip var. yani eger siber guvenlik ile ilgili birsey yapacaksan burada 3 sc ayagi var yani senin yaptigin hamlenin bu uc sac ayagindan birine uyuyor olmasi lazim:
-Confidentiality: bir onlem aliyosun mesela. Bunun yetkisi olmayan kisilerin erisimine kapatilmasi gerek.
-Integrity: yaptigin seyin bu dosyanin tumunu koruyor olmasi lazim. Yani dataya herhangi bir zeval gelmiyor olmasi lazim.
-Avalilability: butun bunlari da yaparken ayni zamanda istenilen datayi istenen zamanda guvenli bir sekilde ulastirabilmen de lazim. Yani datayi kotruyacgim derken onu elde edememenin bir manasi yok.




Defense-in-depth bu isin kalbi diyebilecegimiz bir concept. Derinlemesine yaklasim demek.
Bu bir surec isidir ve katmansal olarak iilerler. Yani bir katmana sizmis olsa mesela diger katmandaki guvenlik onun ilerlemsini engelliyor.
En onemli katman policies ve education katmani. Onemli cunku en zayif katman kisiler. Genelde en buyuk problemler kisilerin hatasi ya da egitimsizlik. Mesela sifreni siklikla degistir, su sitelere girme, su kamerayi kullanma vs gibi aciklmalar yapilir calisanlara. Cunku personelin bu konuda egitimli olmasi lazim.

Diger katman fiziksel katman. En amele katman gibi gorunuyor ama en klasik katmanlardan bi tanesidir. Bazi datalarin fiziksel ortamda tutulmasi gerektigi gibi bunlar birsekilde calinmya musait olabiliyor. O yuzden fiziksel olarak ortami korumak buyuk onem arz ediyor. Ki zaten bunu AWS bizim adimiza yapiyor.

Bizim en cok calistigimiz kisim network katmani. Artik olay burada donuyor daha cok. Genelde uraya agirlasiyoruz. Bu katmanda yeni firewallar var, yeni oneleme teknikleri vs var. ag trafigini yakindan inceliyor. Yeni nesil dedgimiz AI lari devreye aliyor. Loglarla bakiyor vs. network dedigimiz mode gibi dusunebiliriz.

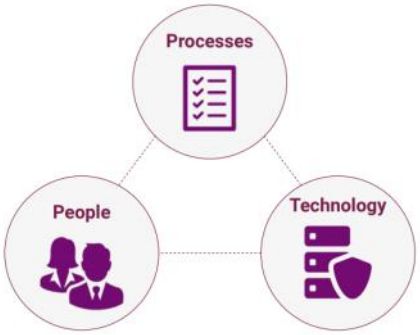
Devices dedigimiz ise bilgisarlari dusunebiliriz burada. Devce uzerinde patchingler var. yani guncellemeler vs. Mesela telefona gelen tum guncellemeler yuksek oranda security kaynaklidir. Ayni seyler burada sirketler icin gecerlidir. Hassas guncellemeler vardir yapilmasi gereken.

Appste ise aplikasyonda bir dengesizlik oldugunu varsayalim mesela slack. Bilgileri alacak kisi acaba buradan alabilirmiyim diye aplikasyonlari inceleyebilir. Bunu engellemek icin MFA ler gibi onlemler almayliyiz.

En dipte ne var DATA. Data bizim encrype ettigimiz bilgiler, secretlar vs. o yuzden encrypt etmek cok onemli. Ama bu katmaanda olay biraz da cost ekseninde donuyor. Ne kadar butcenizin oldugu ile alakali. Cunku bir de bunca datanin bilgisayari yavaslatma ihtimali var vs.

Bu kisim onemli. Cunku hangi kayerda neyin onemli oldugunu bilip ona gore bir yaklasim sergilemek cok onemli.

## Cyber Security: More Than Technology




- **Technology plays a part** in cyber security
- Must be **complemented with policies and procedures**
- **Educating** people is also key

Teknolojinin cok tesinde bir sey. Aslinda bizim buna yetisebilmemiz cokta mumkun degil.
Islem insan ve teknoloji arasinda devamli olarak evrilen, gelisen bir sistem.
Bu anlamda da education cok onemli bir faktor olarak karsimiza cikiyor.

## Preventative vs. Detective Controls

*A security control is a **safeguard** for an information system designed to **protect the confidentiality, integrity, and availability** of its information and to meet a set of defined **security requirements***

### Detective

- **Identifies** threats, **logs** events and sends **alerts**
- Requires **manual or automated remediation**

### Preventative

- Automatically **disallows** actions
- Can lead to **stopping legitimate** behavior

Burada iki yaklasimdan soz edebiliriz. Preventative (onlemek) ve detective (saptamak)
Detective modunda olanlar inceler, tespit eder ve rapor eder. Burada mudahaleler manuel mudahaleye tabi.
Preventativeler ise otomatik olarak bu actioni durdurur. Ama her zaman bu mudahalenin cok ustun oldugu anlamina gelmez.
Detective ya da preventative bir tercih meselesidir hangi mudahalayi yapmak isterlerse onu tercih ederek ilerlerler.
Mesela bir virus saptandi. Onu dosyayi en dogru nasil kurtaracaksak ona gore yol tercih edilir. Yani virus yok edilecek diye datayi patlatmamak gerek. Kontrollu ilerlemek istenir.

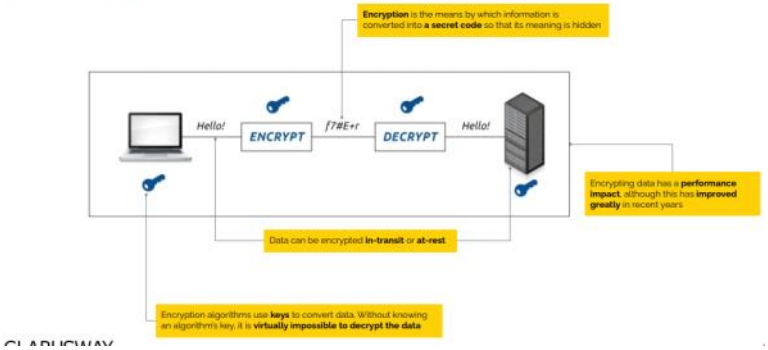
## Compliance Regulations


- Cyber security and data protection regulations are defined sets of **policies, procedures and controls**
- They can be **industry specific** or more **generic**
- Organizations must undergo **audits** to prove compliance

Az onceki bahsettiklerimiz senin kendi dusuncen sonucu aldigin onlemler.
Ama bir de zorunlu oldugun noktalar var.
Mesela bir ihaleye dahil oldun. Diyorlar ki savunma bakalnliginda olacaksan eger FedRAMPe dahil olmak zorundasin, bu degerlere gre sen kendimni ayarladin mi diye kontrol ediyor mesela.
Mesela online odeme yaptiriyorsa o zaman ode izinlerinin olmasi lazim PCI tarafindan. O databasede tutulan kart bilgilerinin bir sarti var. bunlarin izlenebilir ve takip edilebilir olmasi lazim.

# 2 Security Solutions

# Encryption

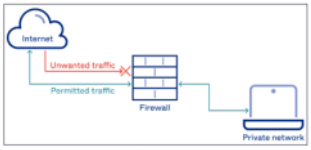



Az once bahsettigmiz durumlar icin onlem olarak neler yapildigini inceleyecegiz.
Ilk olarak ecryption.
Istenilen bir dosya var. elimde bir tane kripto anahtari var. Bu kripto anahtari bunun uzerine isliyorum ve bunu decrypt etmis oluyorum . Yani okunmaz anlasilmaz hale getiriyorum. Ama bu decrption anahtarinin aynisinin karsi serverda oldugu icin onu kullanarak bu dosyaya erisiyor. Dolayisiyla bu anahtari kaybettigin zaman olay bombalasiyor.
3 kriptolama var.
At-rest sadece depolanirken kriptoloma yapilir.
Encrypt in transition yolculuk esnasinda encrypt edebiliyorsun.
Client side encryption var. data bastan sona ulasana kadar full encrypt ediliyor.

Dezanataji sifrelemeyi bilgisayar okuyana kadar zaman aldigi icin yavaslatiyor.

Bu solutions DATA kisminda geciyor az once bahsettigimiz defense in depth konusunda.

# Firewall (Network Firewall)



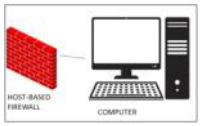

- **Network device** that controls inbound and outbound network traffic based on a set of security rules
- Typically control which traffic can ingress to or egress from an **internal network to an external network** (e.g. Internet)
- Can be an **appliance** (HW+SW) or just SW
- Today's firewalls are quite sophisticated and control traffic based on many factors:
  - **IP, port and protocol**
  - **Packet inspection**
  - **Anti-virus modules**
  - **Known bad IPs and domains**

Bu kisim da network safhasinda gerceklesiyor. Bizim en cok muhatap lacagimiz kisim.
Modemin onundeki koruma gibi. Internet providerlarda oluyor. Bu firewall software da olabilir hardware da olabilir.
Internet uzerinde bazi Iplerin, portlarin, protokollerin ve paketleirn englelemsini sagliyor virusu vs varsa mesela. Okullardaki internete baglananlarin instagrama, youtube vs girememesi gibi. Oradaki modemin onunde firewallar var ve bu sebepten o sitelere giris yapilamiyor.
Cocuk guvenligi saglamak icin yapilan sey de mesela firewalldur. Girmesini istemedginiz sitelere firewall koyarsiniz ve cocuk guvenligi saglanmis olur.


Aslinda tum yontemler OSA modelindeki bir hedef katmanda calisiyor.
Mesela network firewall dedigimiz IP port prtokoller uzerinde calsir yani 3. ve 4. layerdadir. Onun ilgi alani prasidir. Hedf alani orasi. Burada sadece aramalar ypiyor.

Bundan sonra gorecegimiz hemen hemen her solution ise yine kendini bir katmanda hedeflemis olarak gorecegiz.

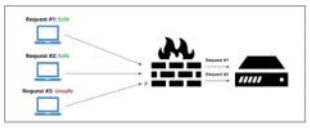
# Host-Based Firewall




- A **software-based** firewall **installed on a host** to monitor and control incoming and outgoing network traffic
- Operates at layers 3 & 4 of the OSI model
  - i.e. **IP, port and protocol**
- Examples:
  - **Windows Defender**
  - **IPTables**

Burada artik modemden bilgisayara geldik.
Host server demek. Bilgisayarimizi temsil eder.
Burada olay fiziksel aygit uzerinde oluyor olmasi.
Network firewall modemi asti ve ikinci bir koruma kalkani olarak bunu kuryoruz fiziksel aygitimiz uzerinden.
3-4 OSI modeli uzerinde calisiyor.
Amaci network uzerinden gelen saldirilari engellemek icin fiziksel aygita uygulamak.

# Web Application Firewall (WAF)



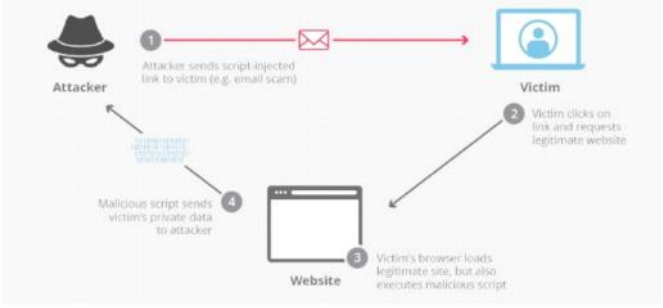
- Network device that operates specifically at protocol **layer 7** and monitors **HTTP traffic**
- Typically protects web applications against specific attacks:
  - **cross-site forgery**
  - **cross-site-scripting (XSS)**
  - **SQL injection**
  - **distributed-denial-of-service (DDOS)**
- Operates via a **set of rules** (policies)

Web application WAF diye gecer.
WAF 7. layerda calisir. Bu layerdaki tehditlere karsi koruma saglamak icin olusturulmus.
Burada 4 tip spesifik attacklar var.

## CROSS SİTE REQUEST FORGERY (CSRF)


Ilk attack sekli. Siteler arasi istek sahtekarligi diye cevirebilirz.
Her acitigimiz oturumun bir kullanim suresi var. bankacilikta mesela bir dakika bile ayril bsindan hemen sessioni kapatir. Sana bir kullanma hakki tanimlar. O kadar boyunca session acik kalir. Sahtekarlik ise suradan olur: mesela bir mail ile ayni bankadanmis gibi bir mail gelir. O yabanci sey senin banka sessionini alir. Sanki sen bankada birseye girmissin gibi baglanti kurar. E zaten banka senin orada oldugunu dusunuyor, sana bir session acmis. Hala sen kullaniyorsun saniyor. Ama o yabanci hesap senin adina trnsfer vs yapmaya basliyor mesela.
Bankaya gore o session dogrulandigi icin bunu farkedemeyebiliyor.
Bunlar layer 7 de gerceklesiyor.

## Cross Site Scripting (XSS)




Burada ise size bir mail, davetiye vs geliyor. Onu aciyorsunuz. Veya bir yonlendirme oluyor. Yonlendirdigi yer mesela gercekten bankanin sayfasi olabiliyor ya da onun gibi gercek siteler. Sen o arada o banka sitesine girerken senin arkana bir attacker takiyor ve o senin arkadan bilgilerini almaya calisiyro. Burada gercek bir sayfaya yonlendirilmis olmaktan sebep bir supheye dusmuyorsun.

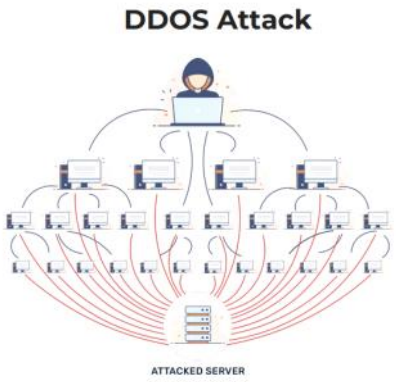
## SQL INJECTION


SELECT * FROM USERS WHERE username = 'osvaldo' and password = 'PI1234'

SELECT * FROM USERS WHERE username = 'administrator' –' and password = ''

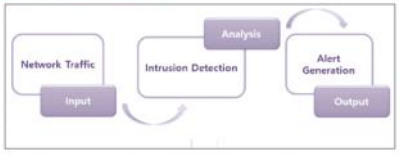
UNION SELECT username, password–

Burada da normalde bi \r yere mesela kayit yaptiginizda arkada donen python kodlarini dusunun onun yaptigi sorgulamanin icine ekstradan sizden bilgiler alcak kodlar enjekte edip sizin biligilerini almaya calisiyor.
Bu olayda layer 7 de gerceklesiyor.
Bunu da yine WAF onluyor.




Diger bir meshur olan attack ise DDOS attacklari.
Birbirine bagli bir suru bilgilsayar var. Tek kisi tarafindan bunlar elinin altina sokulmus vaziyette.
Farkinda bile olmuyorsunuz bunun.
Bir anda rakip server uzerinde bir basiyor sistem saldiriya geciyor. Sonra birden saniyede binlerce attack geliyor siteye. Boyle binlerce request gelince de server patliyor.
Bunlar kotu niyetten olan attacklar yani mesela requestleri gonderelim ve sistem patlasin.
Boylece insanlar alisveris yapamasin.
Amac kazanac elde etmek degil. Site cokertip karsidakini acizlestirmek.
Bu da yine 7. layerde gerceklesiyor.
WAF yine bunun icin de var.

## Intrusion Detection and Prevention (Next Generation Firewall" (NGFW))

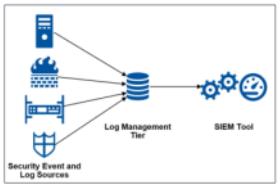



- Intrusion detection systems (**IDS**) **monitor and analyze** network traffic for for signs of imminent threats
- Intrusion prevention systems (**IPS**) go **one step further** and **block traffic** that pose such threats
- Together, IDS/IPS solutions are typically a module in a "**Next Generation Firewall**" (**NGFW**)
- Typically use 4 types of algorithms:
  - **signature-based** detection
  - **anomaly-based** detection
  - **stateful protocol** analysis
  - **reputation** analysis
- These are **dynamic rules** applied to network packets

Bu next generation firewall (NGFW) dye gecer.
OSI 3-4 layerda calisir.
Burada olay biraz daha yapay zeknin isin icinde oldugu bir durum.
Burada adam genis bir cercevede gelen frame ve Ipleri degerlendiriyor.
Gelen requestleri esit analizlere sokuyor.
2 tip yaklasimi var: DETECTION VE PREVENTION
4 tip algoritmasi var:

1. Signature-based: klasik networkte biz IP ve sietler giriyorum isimleri yani. DNSleri engelliyor. Burada ise yorum yapiyor. Tasinan paketlerin cinsine, alinan paketlere bir sablon uyguluyorsun. Su su su ozellikte birini gorursen bu tehlikelidir savun kendini diyorsun. O da o sablonun aksi olan bu seye karsi koruma sagliyor. Bu aslinda su demek. Elinde onceden tecrube ettigin bir suclu profili var. ona gore bir sablon belirlemis oluyorsun.
2. Anomaly-based: burada ise digerinin aksine normal profil resmi veriyorum. Diyorum ki mesel a gomlek giyen, pantolon giyen hirsiz degildir. Ama polis tisort giyeni gorunce mesela yakaliyor direkt. Bunun gibi. Verdigin profile uymayanlar anormal kabul ediliyor. Digerinde direkt suclu profili verilmisti siyah deri ceket elinde silah vs. bburada sistem zero day attack olarak gecer. Yani bugune kadar hic gorulmemis attack tipi var. yani bir killanma durumunda gosterilen bir tepki var.
3. Stateful protocol: burada ise sadece guvendigi yerlerden alisveris yapiyor.
4. Reputation analyses: bu da statefula benziyor bir yonden. Sikintili yerlerden requestleri direkt olarak reddediyor. Mesela kuzey koreden rusyadan bir request geldi onu direkt engelliyor.

## Security Information and Event Management (SIEM)




- A **SIEM** is a device that **ingests and aggregates logs**, including network log information
- Can perform analysis by cross-referencing various log information to **identify network-related threats**
- Unlike IDS/IPS, this type of **analysis is based on logs**, rather than traffic packets

Bu da loglarla calisiyor. Biraz daha tumdengelim methodu gibi dusunebiliriz.
Mesela bir kredi karti aldin. Mesaj geldi. Anytatikadan lahmacun siparisi vermissin. Bunun sacma oldugunu farkedip mesajin geldigi Ipyi direkt engelliyor mesel.
Burada vpc gibi farkli farkli loglri inceleniyor. Geriye donuk bir anormal problem tespit edilirse hemen ona mudahale ediliyor.

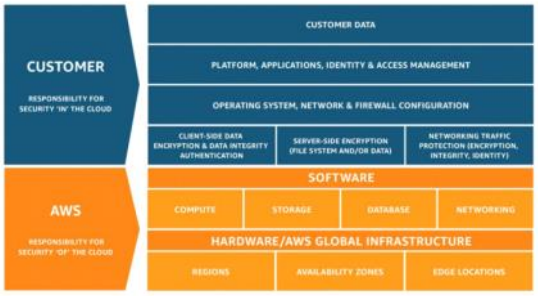
## Vulnerability Scanners

- After operating systems and software is released into the market, quite often **security vulnerabilities** are identified
- These vulnerabilities can be **exploited by hackers** in order to gain access to systems
- A publicly available **CVE ("common vulnerabilities and exposures") database** lists the vulnerabilities and remedies
- A vulnerability scanner **identifies unremediated exposures in hosts** within your environment

Vulnerability kirilganlik olcumu yani guvenlik acigi. Nerede hassasiyet varsa ya da bir acik olma ihtimali varsa ona yoneliyor.
Bunlar hackerlar tarafindan suistimal edilebilecek seyler. Public olarak bu listeler yayinlaniyor. Bu sikintilr liste halinde bircok programin kendi listesi halinde paylasiliyor. Bu da problem.
Mesela virus taramasi yaptirdin. Adam bu asamada zaten tum bilgisayari scanledi. Sonra virusleri oldurmek icin su kadar para verin diye istek cikartiyor.
Dolayisiyla guvenmediginiz yerlere virus taramasina vs girmeyin.

# 3 AWS Security Services

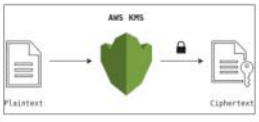
## Shared responsibility model




BU SINAVLARDA BIZIM KARISIMIZA CIKACAK!!!!!!!

Mantik su: AWS hardware ve global infrstructure kurarim diyor. Networking database storage compute olayi bende diyor. Yani software hardware bende.
Ama encryption data guvenligi sende. Bu hizmeti sunuyor ama customerin tercihine bagli kalmis kullanip kullanmamak.
S3, efs vs mesela encryption customer kendi tercihine kalmis. Patlarsa customer sorumlulugunda.
Nacl, securty group vs ben sana sunarim. Alip almamak yine sende diyor.
Mavi kisim senin sorumlulugunda ben sana sunrim sen ister alirsin ister almazsin diyor.
Infrastucrerina hirsiz girdi diye suclayamam diyor mesela cunku o sorumluluk AWS te.

## AWS Key Management Service (KMS)



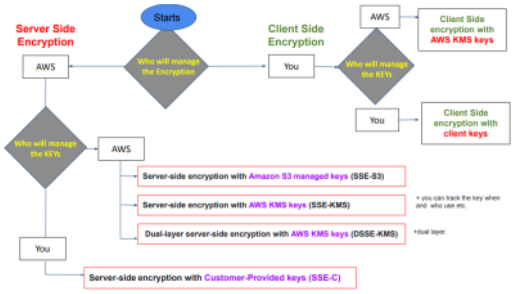

- Encrypts **data at rest**
  - EBS, S3, EFS, RDS, DynamoDB, more
- **Centralized management**
  - create, delete, view, set policies
  - Automatic **key rotation**
- Performance impact is **negligible**
- Permissions governed by **IAM and Key Policies**
- Must be cautious about **permissions and protecting keys from deletion**

Orularda mesela dicek ki kriptolamayi ben yonetmek istiyorum ama anahtari AWS versin derse iste buradaki gibi AWS KMS keys diyebiliriz. Bu tabloyu iyi anlamak onemli burdan mutlaka soru gelir!!!!

Encryption diyince bizim aklimiza ilk gelen KMS.
AWS in depolanirken datalarinin tutuldugu ve encrypt edildigi yer yani data at rest.
Burada simdi ilk suna karr verilecek:kriptolamayi kim yapacak? Ve anahtari kim saglayacak?
-----Aws tarafinda bu Is sadece server side encryption ile oluyor. Peki bu encryptionu AWS yapsin ama kim anahtari kim yonetsin kisminda ben yoneteyim dersen SSE-C denilen server side encryption with customer provided keys secmis oluyorsun. Ya da AWS yonetsin dersen 3 sekilde bunu yapiyor:
1.SSE with S3 manged keys (SSE-S3):Sadece s3 e has bir kriptolama yontemi

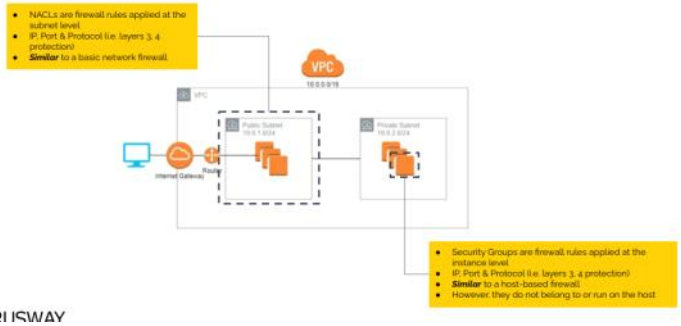
2. SSE-KMS : bu daha ust model. Burda keyleri kimler kullanmis vs izleyebiliyorsun ve bu izinleri rolelerle belirleyebiliyosun ve policylerle denetleyebiliyorsun. (BURADAN SORU GELIR!!!!!) Mesela instance ayaga kaldirirken kriptolu ve bana yetki verilmemis. Ben ec2 acarken problem yokmus gibi aciyorum. Ama acar acmaz kapatiyo. Bastan uyarmiyor ya da bir hata ver,iyor ama acilir acilmaz direkt shutting down.
3. 3.Dual layer SSE with AWS KMS keys(DSSE-KMS): bu da cift katmanli kriptolama

--------AWS degilde bu kriptolamayi ben yapmak istiyorum dedigimdepeki anahtaralri kim yonetecek sorusu cikiyor ortaya: Eger AWS yonetirse Client side encryption with AWS KMS keys ile yapiyor. Ama ben yonetirsem clietnt side encrytion with client keys ile yapiyorum.

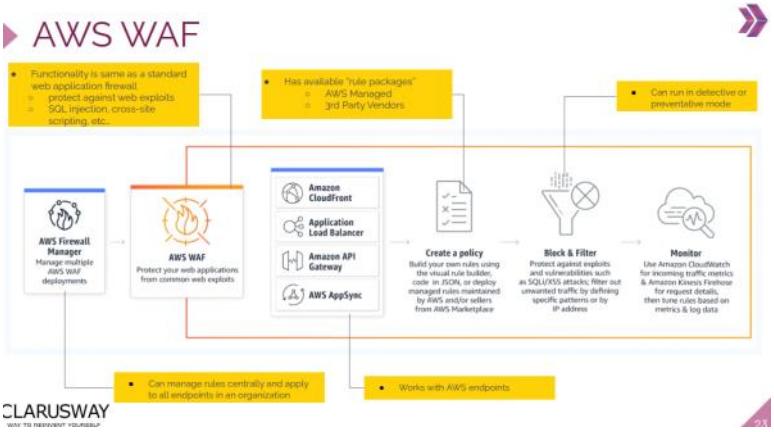



Yeni siklarda aws icin sorussa bu sadece server side encryoton.

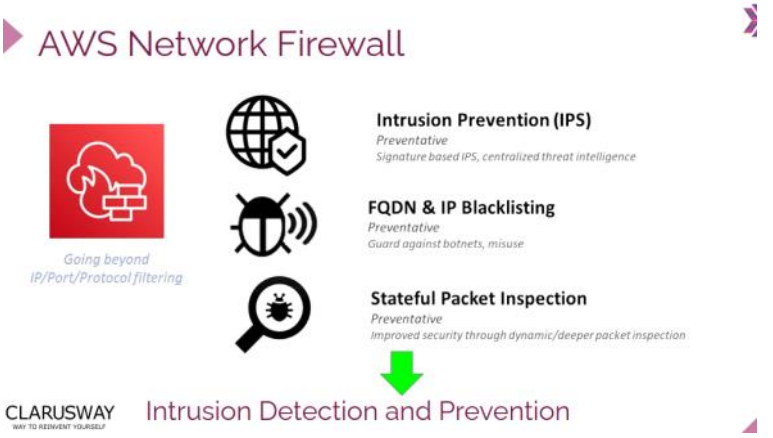
## Security Groups and NACLs



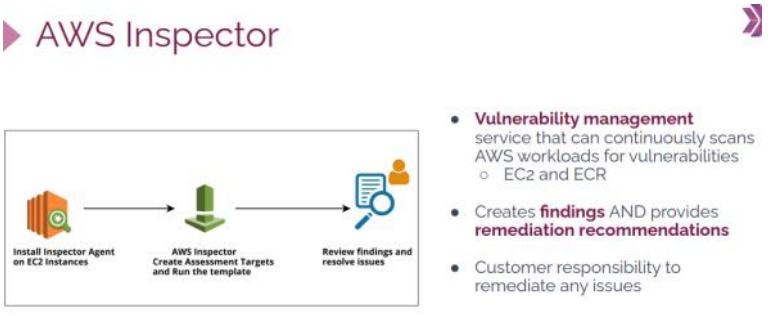

Network firewall dedigimiz AWS kisminda NACL, host-based firewall dedigimiz ise Security grouplar. Security gruplari ec2 uzerine kuruyoruz. Ec2 bir host. Yani host-based firewall olmus oluyor.
NACL ise subnetin onune ekleniyor. Yani networkun. Yani network firewallun AWS kismi bu olmus oluyor.



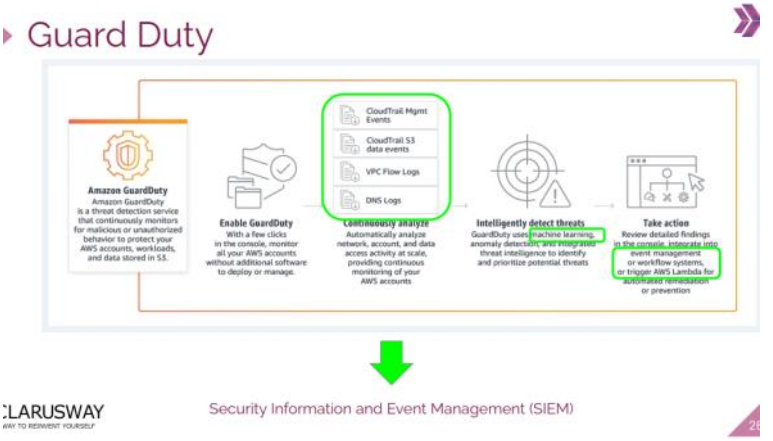

WAF ayni WAFin AWS versiyonu burada.
Bu da layer 7 de calisiyor. Bu da WAF gibi attacklara karsi mucadele ediyor. DDOS, cross sode attack vs gibi attacklar burada da gecerli.
Burada ise endpointler uzerinde kurulur WAFlar. Yani mesela cloudfront, ALB, Amazon API, AWS AppSync gibi. Cati servisler uzerine kurulur ki altinda baglanti kurulan servisler korunsun.
WAF bir bos alisveris sepeti gibidir. Icine ne ile ilgili bir madde atarsan WAF seni onunla iligli korur. Hangi paketi secmis ve parasini odemissen seni sadece ve sadece onlara karsi korur.




Hani suclulari protokollerine gore yakalayan prevention ve dedective model vardi. Onun gibi. Sablon var ve ona gore yorum yapip hirsiz yakalniyor gibi dusun burada da.
Bunun AWS teki karsiligi network firewall.
Burada intrusion prevention yapiyor yani sadece rapor etmiyor ayni zamanda onluyor. Direkt imha.
Layer 3-4 te calisir.




Bu bizim ec2larimizda ecr dedigimiz docker konteynirlarinda vs icerisine girip guvenlik acigi var mi filmini cekiyor.
Bu da aslinda vulnerability scannerin aynisi. Virus taramasi yapan gibi dusun.




Loglar uzerinden gider.
Yani SIEMin buradaki krsiligi. Tumdengelim var burada da. Yani antartikadaki harcamalar ornegi. Cloudtrail, VPC, DNS logs, machine learningte bunlari integre ediyor. Ve gelen tehlike karsisinda seni uyariyor ve trigger etmek sana kalmis.

# Security Hub

AWS Security Hub

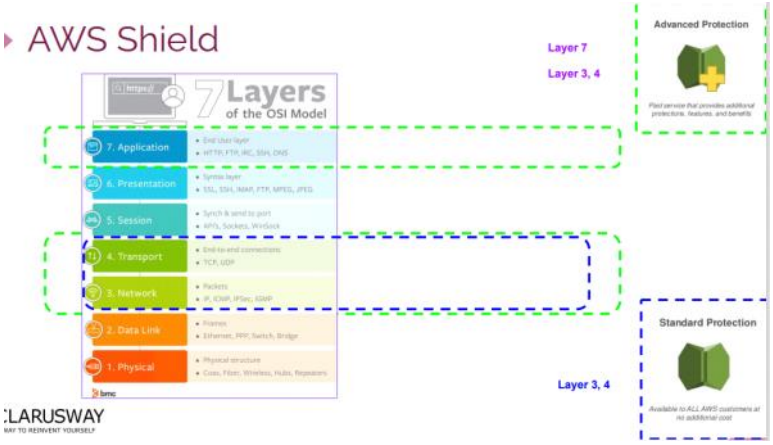
- **Integrates** with other AWS & 3rd party security services
  - Guard Duty
  - Inspector
  - Firewall manager
  - and more ..
- Provides a comprehensive view of security state
  - "**single pane of glass**"
- Also **creates alerts** based on security best practices

Bunun AWS disinda bir karsiligi yok.  CloudWatch gibi dusunebilirsiniz.
Butun herseyi tek bir merkezden yonetiyor. Alarm vs de kurabiliyorsunuz.
Securitynin karargahi gibi dusunebilirsiniz. Burada yazanlarin hepsini AWS uzerinden gozlemyebiliyorsunuz.

# Amazon Detective


SINAVLARDA CIKMAYA BASLADI!!!!!!!!
Security hub gibi ama onu da kapsayan DuardDutyi, Amazon Inspectoru heosini kapsayan ve hepsini inceleyen, bunun aciklarini hassasiyetlerini sana donduren servis.
Security hubta bir gozlemleme var sadece. Ama burada root cause of potensial diye gecer sinavlarda yanisorunun kaynaginin neresini oldugunu sana soyler sadece gozlem yapmaz.
Butuncul bir yaklasimla sizin butun hesabinizi inceler.

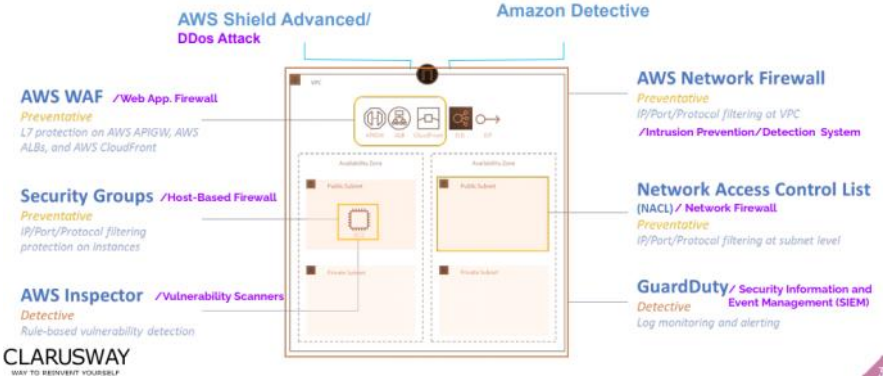
# AWS Shield




DDO ataklari icin gelistirilmis birsey.
WAF ta da engelleniyordu ama paketi satin alirsan engelleyebiliyordun yoksa yok. Ama shield tamamen DDO ttacklari uzerine dizayn edilmis bir servis.
AWS Shield bu isin uzmani DDOS hakkinda.
Bu tataklar 3-4-7. layerlardan gelir.
3-4 ten gelen attacklar icin standart protectioni korur ekstra bir ucret talep etmeden.
Layer 7den gelirse bu isi profesyonel olarak yapan Advanced protection var. belirli bir maliyeti var.  Ayni zamanda 3 ve 4 ten gelenlerden de korur.
Ya da WAF satin alabilirsin diyor. Oradan odeme yapar alirsin.

OZETLE SHIELD DDOS ATTACK UZMANI!

# Summary of AWS Security Services



# Summary of AWS Security Services

| AWS Security Service | Protects Against | Applies To | Similar To |
|---|---|---|---|
| Security Groups | Unauthorized access to VPC resources | İnstance @ 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 |
| AWS Shield | DDos Attack | Layer 3, 4 (Shield Standard)<br>Layer 7 (Shield Advanced) | WAF |