

AWS Security



Hello!

- **Mehmet Ayberk ANNADINÇ**
- App. Sec. Engineer @Intertech
- AWS Community Builder
- You can find me at [@mhmtayberk.](https://twitter.com/mhmtayberk)

AWS Community Builder Program

- Bilgi paylaşımı ve teknik toplulukla bağlantı kurma konusunda tutkulu olan AWS teknik meraklılarına ve gelişmekte olan düşünce liderlerine teknik kaynaklar, eğitim ve ağ oluşturma fırsatları sunar.

AWS CB Benefits

- AWS ürün ekiplerinden haber alın ve yeni hizmetler ve özellikler hakkında bilgi alın.
- Haftalık web seminerleri aracılığıyla çeşitli konularda AWS konu uzmanlarından bilgi edinin.
- İçerik oluşturmayı desteklemek için AWS Promosyon Kredileri ve diğer yardımcı kaynaklar.
- Benzer düşünen geliştiricilerle bağlantı kurma ve onlardan öğrenme fırsatları.

Roadmap

Bulut Bilişime Giriş /
Temel AWS Servisleri

1

AWS Güvenlik Servisleri

3

IaC Güvenliği

5

Saldırıgan Bakış Açısı

2

AWS Ortamlarında
Incident Response

4

Compliance & Best
Practices

6

LET'S MEET



Cloud Nedir?



“

There is no cloud
it's just someone else's computer

Cloud vs On-Premise

Cloud	On-Premise
İnternettedir	Local ortamdadır
Bakım işlemleri kolaydır	Bakım işlemleri zordur
Daha az yetkinlik gerektirir	Yüksek yetkinlik gerektirir
Maliyeti düşüktür	Maliyetlidir
Daha esnektir	Çok esnek değildir



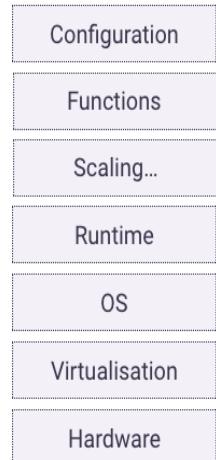
Cloud Types

- Public Cloud: İnternet üzerinden sağlanan ve kuruluşlar arasında paylaşılan bulut bilişimdir.
- Private Cloud: Yalnızca kuruluşunuza adanmış bulut bilişimdir. Dedicated.
- Hybrid Cloud = Private Cloud + Public Cloud





PIZZA AS A SERVICE



Homemade

Communal Kitchen

Bring Your Own

Takeaway

Restaurant

Party

Bulut Bilişim & AWS Temel Servisler

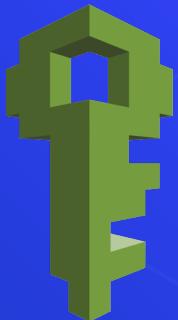
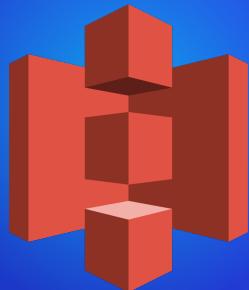


It's A

Service category ▾	Service type	Google Cloud product	Google Cloud product description	AWS offering	Azure offering
App Modernization	CI/CD	Cloud Build	Build, test, and deploy on Google Cloud serverless CI/CD platform	AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline	Azure DevOps, Github Enterprise
App Modernization	Execution Control	Cloud Tasks	Control and observe asynchronous service requests between independent applications using this zonal, execution-control service.	Amazon Simple Queue Service (SQS), Amazon Simple Notification Service (SNS)	Azure Service Bus, Azure Storage Queues
App Modernization	Multi-cloud	Anthos	Anthos is a managed application platform that extends Google Cloud services and engineering practices to your environments so you can modernize applications faster and establish operational consistency across them.	Amazon EKS Anywhere, Amazon ECS Anywhere	Azure Arc
App modernization	Multi-cloud	Anthos Clusters	Extend GKE to work in multiple environments, including attached clusters, AWS, Azure, bare metal, and VMWare.	Amazon EKS Anywhere	
App modernization	Multi-cloud	Anthos Config Management	Automate policy and security at scale for your hybrid and multi-cloud Kubernetes deployments.	Chef Automate, AWS OpsWorks	Azure App Configuration
App modernization	Multi-cloud	Config Connector	Manage Google Cloud resources through Kubernetes.	AWS Controllers for Kubernetes	Azure Service Operator
App modernization	Multi-cloud	Container-Optimized OS	Efficiently and securely run Docker containers on Compute Engine VMs.	AWS Bottlerocket	Azure Container Instances

“ 2021 yılı itibarı ile AWS üzerinde 305’ten fazla servis bulunmakta.





S3 (Simple Storage Service)

- Depolama servisidir.
- Tutulan veriler obje, verilerin tutulduğu yer ise Bucket olarak isimlendirilir.
- Ölçeklenebilir.
- Limitsizdir ancak tek dosya boyutu maksimum 5 TB olabilir.
- Statik web siteleri host edilebilir.



Block Based vs Object Based Storage

Block Based:

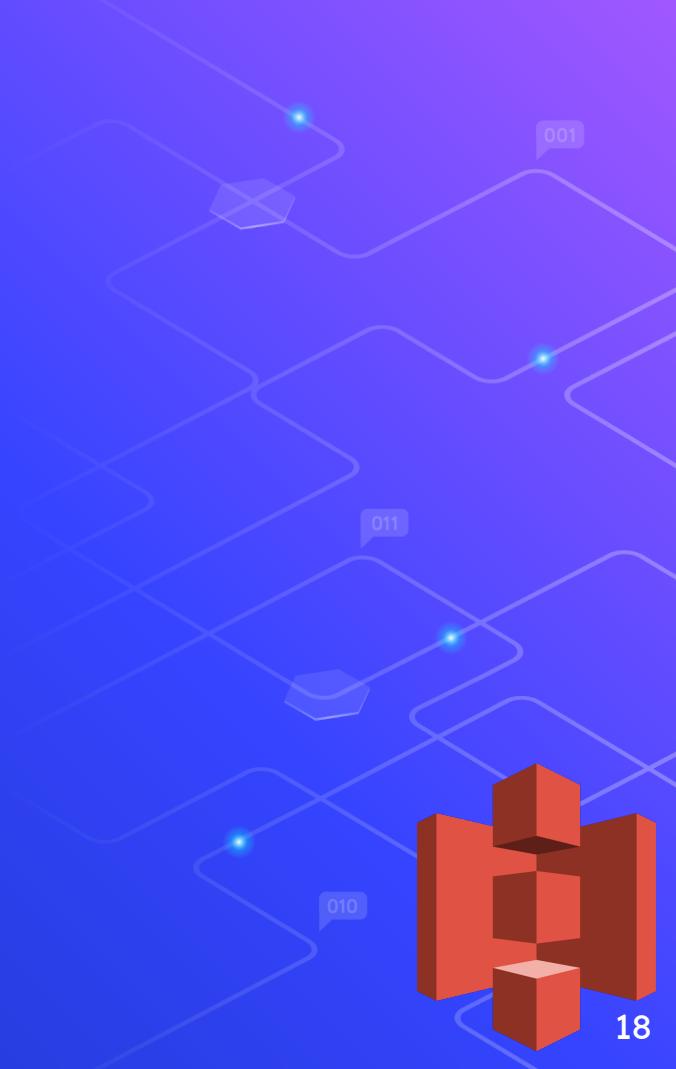
- Disk imajları şeklindedir.
- Örneğin EBS.
- Bir bilgisayara bağlanarak kurulum işlemleri yapılabilir.

Object Based:

- Objeler ve metadatalardan oluşur.
- Örneğin S3.
- Bir bilgisayara bağlanarak kurulum işlemleri yapılamaz.



```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AddCannedAcl",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": [  
                    "arn:aws:iam::111122223333:root",  
                    "arn:aws:iam::444455556666:root"  
                ]  
            },  
            "Action": [  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",  
            "Condition": {  
                "StringEquals": {  
                    "s3:x-amz-acl": [  
                        "public-read"  
                    ]  
                }  
            }  
        }  
    ]  
}
```



Edit Block public access (bucket settings)

Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through *new* public bucket or access point policies

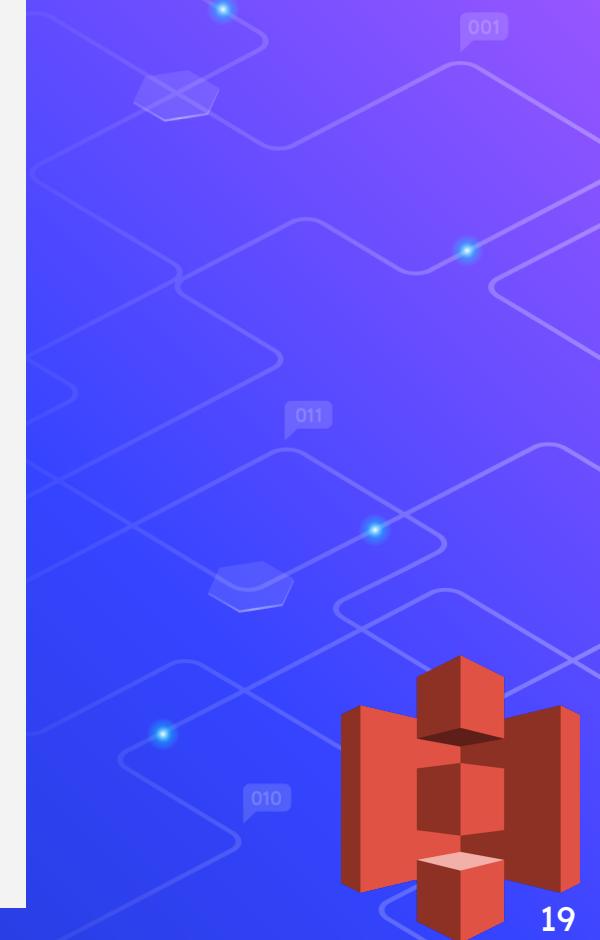
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

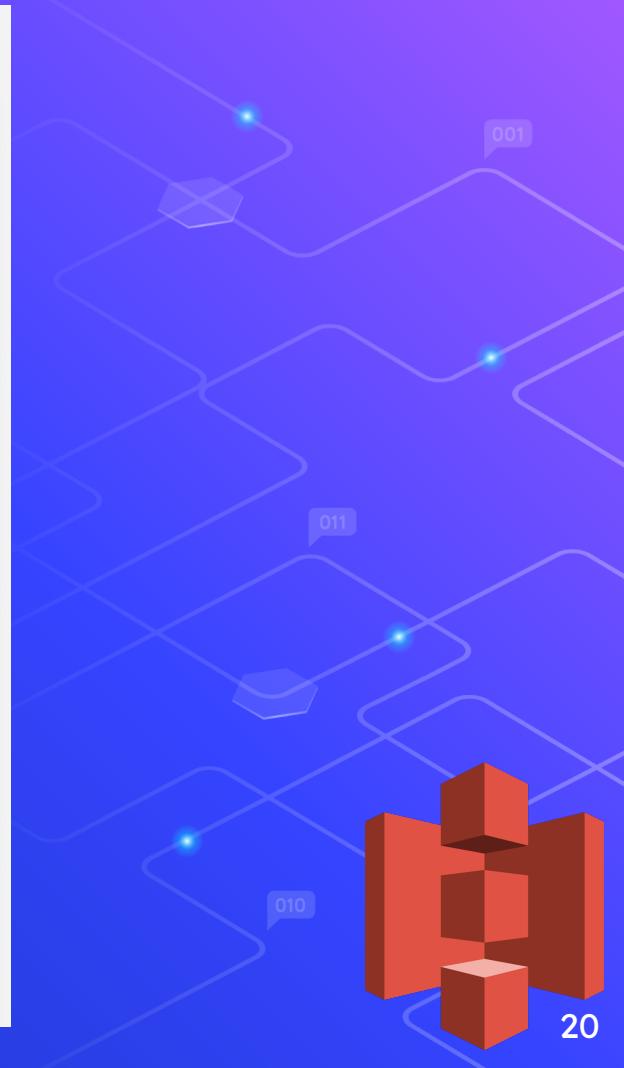


Edit access control list (ACL) Info

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Canonical ID: 83ad292974 e3f7119c07cbd2d33400d1d6b bb332ff0c18ca4a875649a92d4 d98		
Everyone (public access)	<input type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers		
S3 log delivery group	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
Group: http://acs.amazonaws.com/groups/s3/LogDelivery		



“

Statik web siteleri için BPA Public Access olduğuna göre nasıl güvenli hale getirilebilir?

S3 - Lab (Secure Site)



“

CLOSER LOOK

IAM (Identity and Access Management)

- Ayrıntılı erişim denetimi servisidir.
- Region bağımsızdır.
- Root user kullanılmamalıdır.
- Parola politikaları buradan ayarlanır.

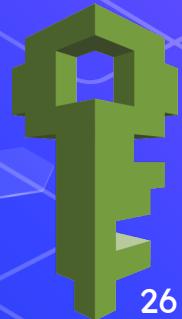


“

CLOSER LOOK

IAM - Lab (Root User Security)

- Root account için Dashboard'daki uyarıları yerine getirin.
- Root account için MFA'ı aktifleştirin.
- Güçlü bir parola politikası belirleyin.



EC2 (Elastic Compute Cloud)

- Bildiğimiz sanal makine (Instance).
- Farklı Instance tipleri vardır.
- Hazır sanal makineleri bulunur. (AMI)
- Varsayılan olarak dış dünyadan gelecek tüm trafiğe kapalıdır.



EC2 - Metadata

- AWS servisleri hakkında bilgi veren yapıdır.
- 169.254.169.254
- fd00:ec2::254



“

CLOSER LOOK

VPC (Virtual Private Cloud)

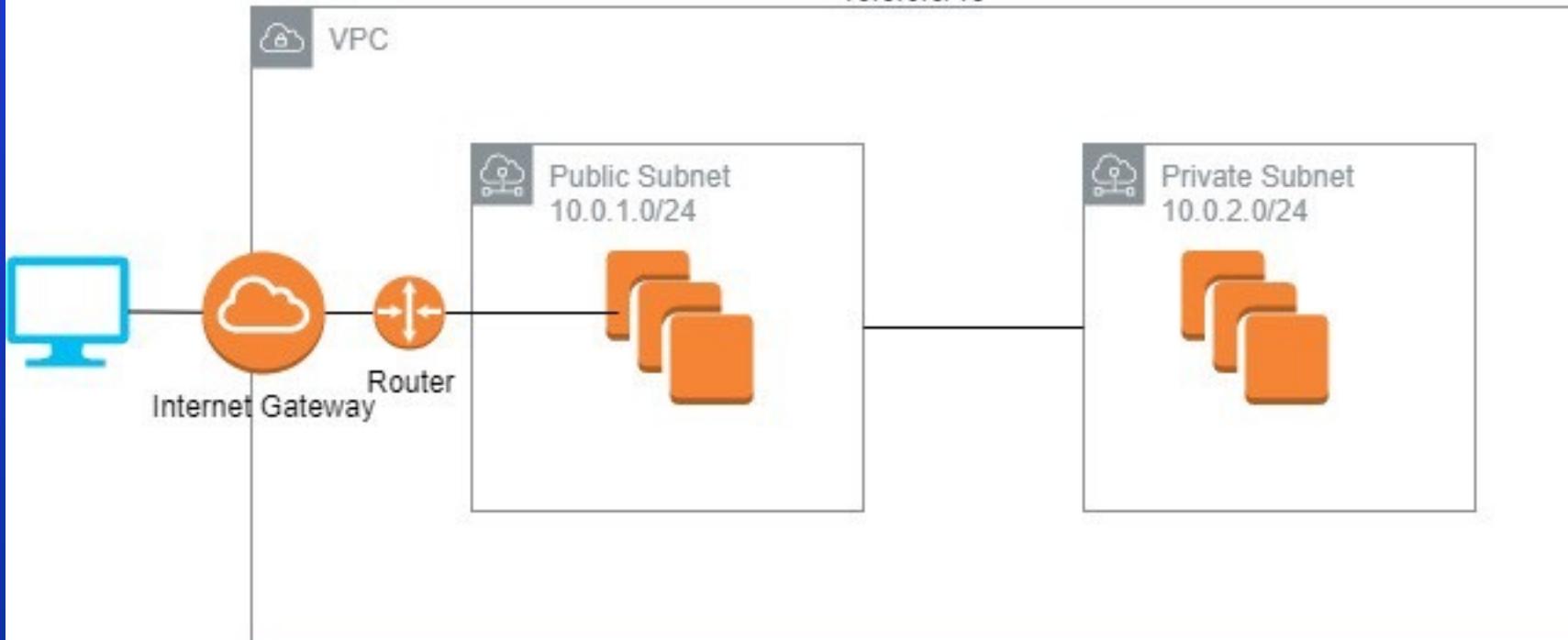
- Sanal ağlar oluşturabildiğimiz servistir.
- Public/Private Subetler ve gateway'ler oluşturulabilir.
- Route Table kuralları yazılabilir.
- AWS – On-prem arası Site-to-Site VPN bağlantısı yapılabilir.



AWS



10.0.0.0/16



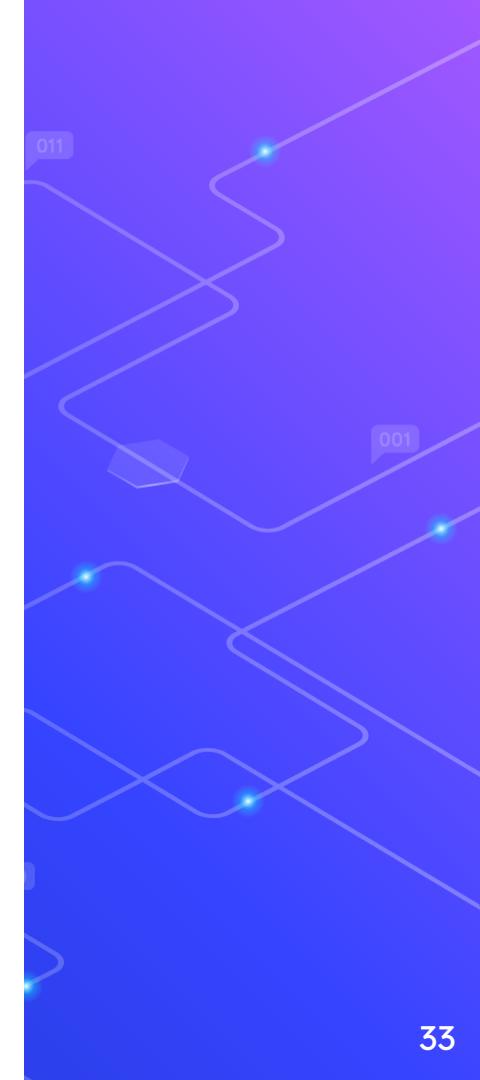
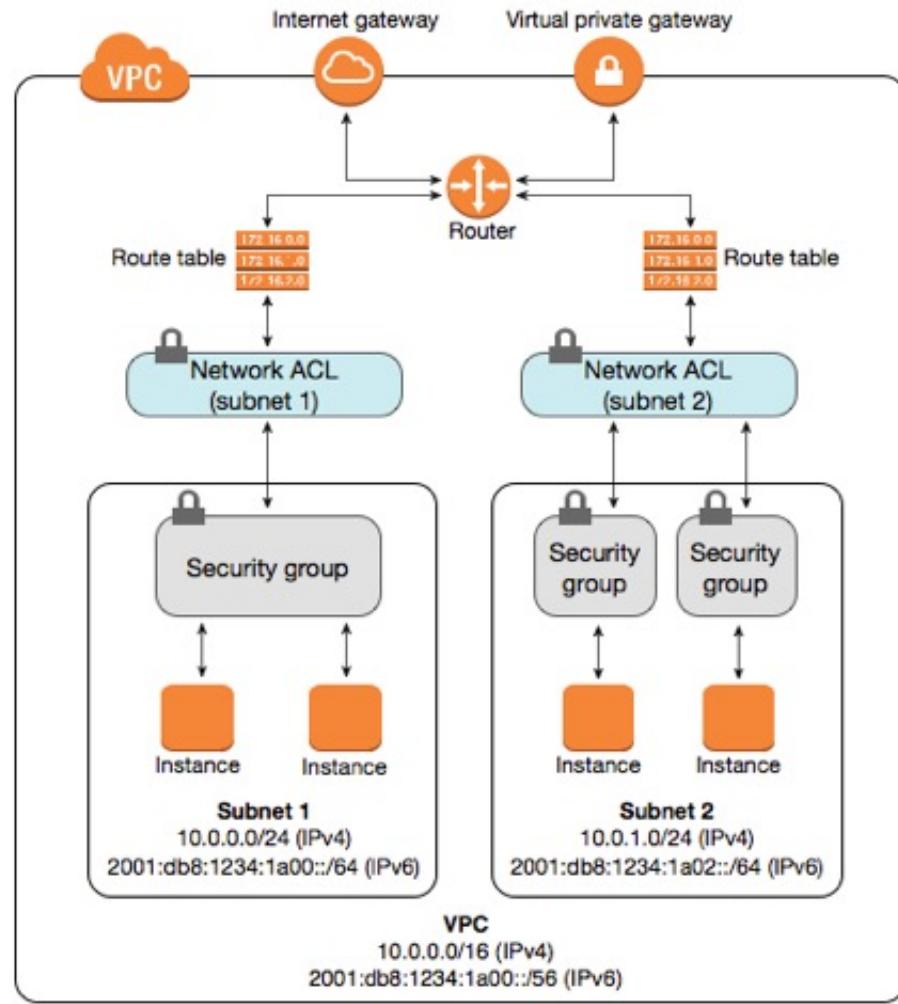
NACL vs Security Groups

NACL

- Allow ve Deny kuralları destekler.
- Subnet ile ilişkilidir.
- Kuralların Priority'si vardır.
- Her Subet bir NACL'a atanmak zorundadır.

Security Groups

- Sadece Allow kuralları destekler.
- EC2 ile ilişkilidir.
- Tüm kurallar aynı anda değerlendirilir.
- Her Subet bir SG'e atanmak zorunda değildir.



“

CLOSER LOOK

“

Bir Private sunucuya dış
dünyadan erişmek
istediğimizde bunu nasıl
yapacağız?

CloudWatch

- Monitoring servisidir.
- Raporlamalar ve metrikler sunar.
- CloudTrail, Route53 gibi farklı servisler ile entegre edilebilir.



States of Alarms

OK

Metrik, tanımlanan değer dahilindedir.

ALARM

Metrik ayarlanan sınırları aşmıştır.

INSUFFICIENT_DATA

Alarm yeni başladığında, ölçüm mevcut değil veya ölçümün alarm durumunu belirlemesi için yeterli veri yok.



“

Bir EC2 makinenin loglarını
(örneğin nginx access
logları) CloudWatch ile nasıl
izleriz?

“

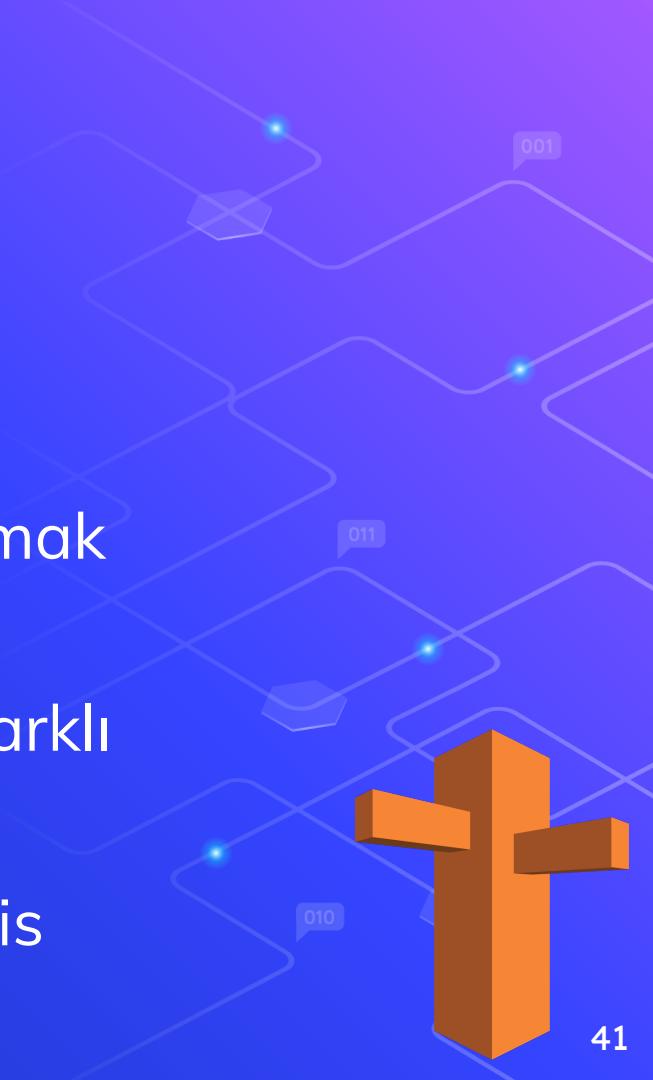
CLOSER LOOK

CloudWatch - Lab (Save Root Account)

- Root Account kullanıldığı takdirde bildirim alınabilmesi sağlanacaktır.
- Yeni bir Trail oluşturun.
- Log grubu gibi ayarları yapın.
- Yeni bir Metric Filter oluşturun.
- Filter olarak vereceğim Filter'ı ekleyin.
- Yeni bir Alarm oluşturun ve SNS Topic ayarlayın.
- Test edin.

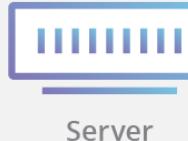
Route53

- DNS kayıtlarının yönetilebilmesini sağlayan servistir.
- Amazon üzerinden domain satın almak zorunda deňilsiniz.
- Geoproximity, Latency-Based gibi farklı Routing türlerini destekler.
- Domain Register hizmeti de bu servis ile yönetilir.



Complete DNS Lookup and Webpage Query

example.com



Server

1 8



DNS Resolver

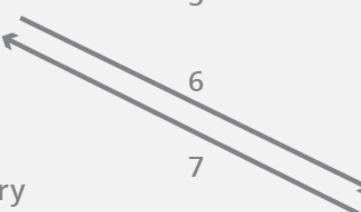


Root Server

4
5



TLD Server



example.com

— Recursive Query
→ Iterative Query

“

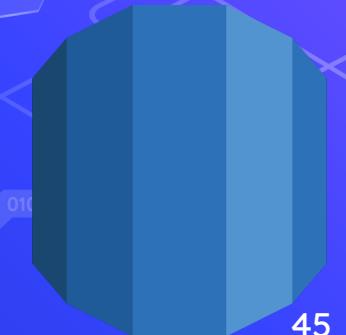
CLOSER LOOK

DynamoDB

- NoSQL veritabanı servisidir.
- Verileri partition'lara bölerek tutar.
- Attribute olarak maksimum 400KB veri tutulabilir.
- Global Table özelliği ile birden çok Region'da aynı anda çalışılabilir.

DynamoDB

- DB içerisindeki ögelere TTL değeri atanmasına olanak verir.
- 35 güne kadar otomatik yedekleme yapar. Manuel yedeklemeye de izin verir.



“

CLOSER LOOK

CloudFormation

- IaC (Infrastructure as Code) aracıdır.
- Template'ler ile aylık tahmini maliyet hesaplaması yapılabilir.
- YAML/JSON formatındadır.



Version	Description	Metadata	Parameters	Mapping	Conditions	Outputs	Resources
Template' e atanınan version numarasıdır. Templeate' in gelişimi takip edilebilir.	Template ile ilgili açıklama yapılmasına olanak	Template ile ilgili genel özellikler yer alır.	Oluşturulacak kaynakları ve özellikleri belirtilir.	Yaratılan kaynakların diğer kaynaklarla eşleşmesi sağlanır.	Condition olacaksa burada belirtilir.	Kaynaklar yaratıldıktan sonra kullanıcıya geri verilecek olan çıktıdır.	Must olan tek alandır. Hangi kaynakların yaratılacağı belirtilir.

“

CloudFormation Template'leri
kullanılırken güvenlik yaklaşımına
göre nelere dikkat edilmeliidir?

“

CLOSER LOOK

Lambda

- Sunucuları yönetmeden ve tedarik etmeden kod çalıştırmanıza olak tanır.
- Serverless.
- Java, Go, Powershell, Node.js, Python, C# ve Ruby'yi doğrudan destekler.



“

CLOSER LOOK

Big concept

The Red Team Perspective



Traditional Web vs. Modern Web

Attack Surface

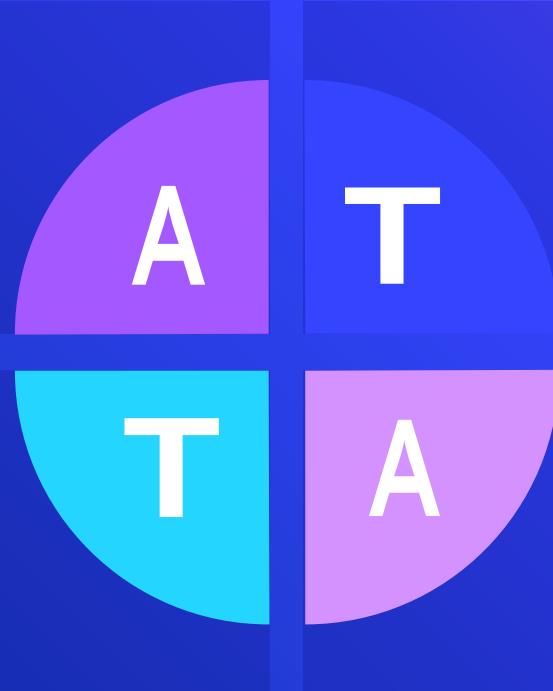
Modern web'te çok daha geniş bir atak yüzeyi bulunmaktadır.

Technologies

Modern web'te çok fazla çeşitli bir teknoloji ekosistemi var.

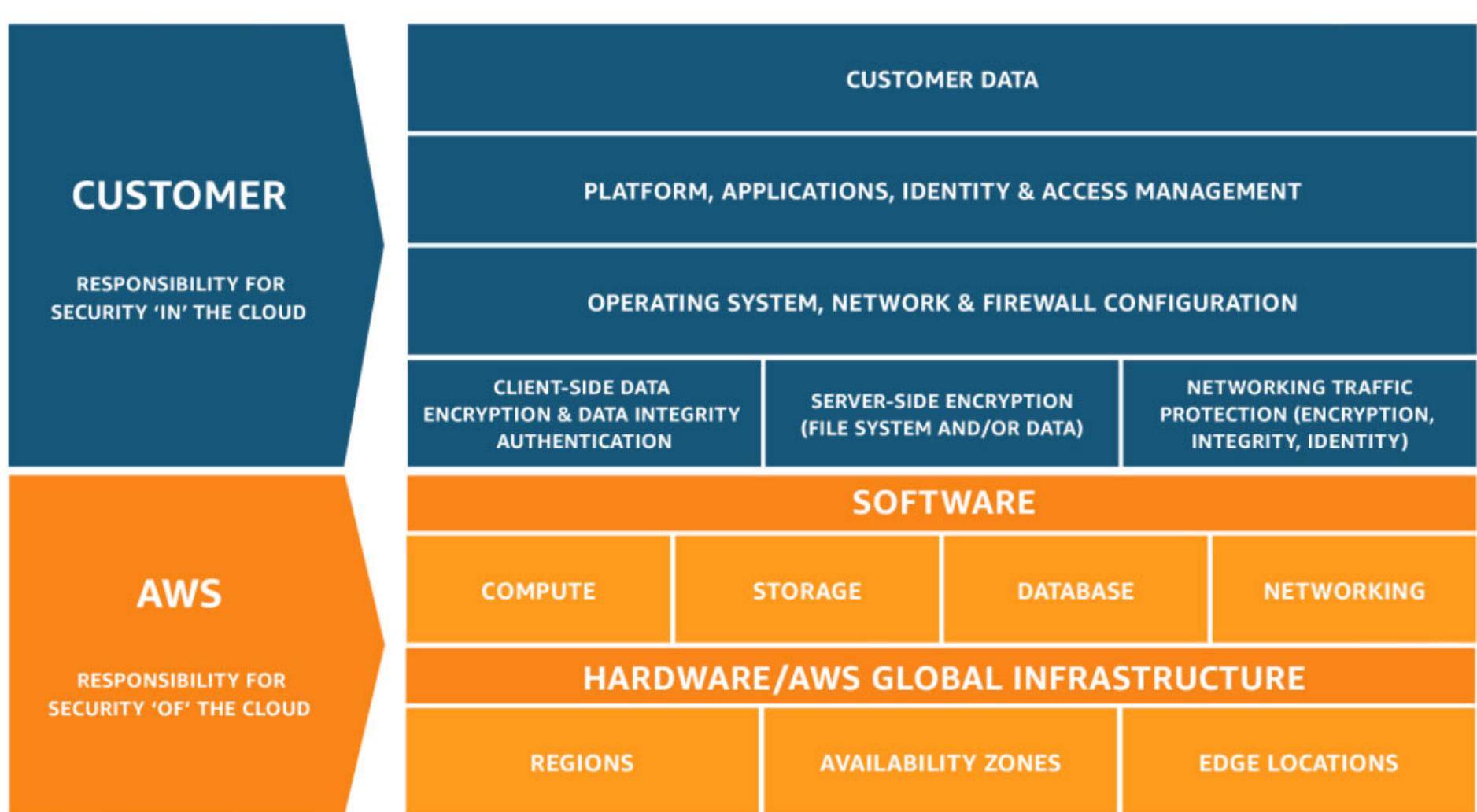
Modern web'te kullanılan araç seti çok daha çeşitli.

Tools



Modern web uygulamaları inşa edilirken çok daha farklı yaklaşımlar uygulanmaktadır.

Approaches



AWS's Pentest Policy

- AWS hizmetlerinin tamamı izin alınmadan test edilememektedir.
- AWS altyapısının kendisi ve altyapısı ile ilgili test yapılmasına izin verilmez.
- Simülasyon testleri için (DDoS, stres testi) ayrı politikaları mevcuttur.

AWS's Pentest Policy

İzin Verilen Servisler

- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateway'ler
- AWS Fargate
- AWS Lambda
- Amazon Ligthsail
- Amazon Elastic Beanstalk
- Amazon EC2

Yasak İşlemler

- Amazon Route 53 Barındırılan Alanları üzerinden DNS alan taraması
- DDoS, DoS

AWS Güvenlik Bülteni

- Güvenlik olaylarının müşterilere bildirildiği portaldır.
- AWS servislerinin güncel zayıflıklarla ilgili aldığı aksiyonlar da burada listelenir.



Bug Bounty & Abuse Reports

Vulnerabilities:

aws-security@amazon.com

Abuse:

<https://aws.amazon.com/tr/premiumsupport/knowledge-center/aws-abuse-report/>

HackerOne Reports

- EC2 SSRF
- S3 Public Buckets
- Cognito Account Takeover
- Subdomain Takeover
- SSM RCE





cujanovic submitted a report to **DuckDuckGo**.

Aug 15th (4 years ago)



Hello, I saw that SSRF on proxy.duckduckgo.com is out of scope but because of the severity I wanted to report this.

The payload is simple:

```
curl "https://proxy.duckduckgo.com/iur/?f=1&image_host=http://169.254.169.254/latest/meta-data/"
```

Response from the server:

Code 323 Bytes

Wrap lines Copy Download

```
1 ami-launch-index
2 ami-manifest-path
3 block-device-mapping/
4 hostname
5 instance-action
6 instance-id
7 instance-type
8 local-hostname
9 local-ipv4
10 mac
11 metrics/
12 network/
13 placement/
14 profile
15 public-hostname
16 public-ipv4
17 public-keys/
18 reservation-id
19 security-groups
20 services/```
21
```

001

n0x496n submitted a report to **Courier**.

Jun 22nd (2 years ago)

Hi I found open s3 bucket : backend-production-librarybucket-1izigk5lryla9

Step to reproduce :

- 1- Go to notification and click to create notification
- 2- Add new image (also allows svg & xss) then copy image location

https://s3.amazonaws.com/backend-production-librarybucket-1izigk5lryla9/85abcc94-a7db-4529-b0aa-826e3026c8c1/1592856757262_camion2.svg

Here is your bucket : backend-production-librarybucket-1izigk5lryla9

Configure your s3 command line tool..

Then run :

```
$ aws s3 ls backend-production-librarybucket-1izigk5lryla9
```

Code	6.17 KiB	Wrap lines	Copy	Download
1	PRE 07d11869-8744-4a59-a871-cf44a833f95d/			
2	PRE 07dfd29d-7dee-4d7a-85b8-566d2d223799/			
3	PRE 07f4ed3f-3bac-4ca2-bc99-51a51f738d25/			
4	PRE 0a5c28b2-47e8-40df-9178-0603dba1c848/			
5	PRE 0c34571a-f774-4ad9-b1d3-3e426c3a4327/			
6	PRE 131f3727-3ef3-4470-9979-6868678c70a0/			
7	PRE 15a5ce40-e45d-4f31-aed1-812187826100/			
8	PRE 15cfccb49-fdd2-430c-99e2-cb4fa1ac5db7/			
9	PRE 15e77f43-b14a-48ee-9f76-234263e207a7/			
10	PRE 18bfd6aa-ae6e-4986-be70-f25fa17b0a3a/			
11	PRE 198c03a4-ec81-47e1-8437-dfa3cf2dff40/			
12	PRE 1ad057c7-64ea-4ae3-a901-fdbeee68f4c7/			
13	PRE 1c9dac1f-d101-4204-95d6-d00dbd293e03/			

001

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)

404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: happymondays.starbucks.com
- RequestId: 4EFBF81B2BD369BA
- HostId: rxEDBP8eQS4O1NZrNN9BMktQI7uaA6LSLfQz0AHp4tan+bTzz4Rv+0pVMOy7+crZEa1AdPjxM=

As happymondays.starbucks.com was free to register on AWS S3 service and DNS-setup is already correct set-up:

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)

```
; ANSWER SECTION
; happymondays.starbucks.com. 86399 IN CNAME happymondays.starbucks.com.s3-website-us-east-1.amazonaws.com.
; happymondays.starbucks.com.s3-website-us-east-1.amazonaws.com. 59 IN CNAME s3-website-us-east-1.amazonaws.com.
; s3-website-us-east-1.amazonaws.com. 4 IN A 52.216.1.82
```

I was able to claim the domain for PoC using the following set-up:

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)

Bucket: happymondays.starbucks.com
Region: US Standard
Creation Date: Tue Nov 29 23:52:02 GMT-500 2016
Owner: danil.grubkov

Permissions

Static Website Hosting

You can host your static website entirely on Amazon S3. Once you enable your bucket for static website hosting, all your content is accessible to web browsers via the Amazon S3 website endpoint for your bucket.

Endpoint: happymondays.starbucks.com.s3-website-us-east-1.amazonaws.com

Each bucket serves a website namespace (e.g. "www.example.com"). Requests for your host name (e.g. "example.com" or "www.example.com") can be routed to the contents in your bucket. You can also redirect requests to another host name (e.g. redirect "example.com" to "www.example.com"). See our walkthrough for how to set up an Amazon S3 static website with your host name.

Do not enable website hosting

Enable website hosting

Index Document: index.html

Error Document:

Edit Redirection Rules: You can set custom rules to automatically redirect web page

That's all Folks!

Don't Forget This

Bulut bilişim de aslında normal sunuculardan oluşur.

Enumeration – Without Creds.

- Github Leaks
- Gray Hat Warfare
- Google Dorks
- Censys
- S3 Direct Access
- Cognito Usage

Enumeration – With Creds.

- EBS Snapshots
- Lambda
- RDS Instances
- S3 Buckets
- IAM Enumerations
- And another many services...



Github Leaks

“flaws.cloud” API_key

“flaws.cloud” secret_key

“flaws.cloud” aws_key

“flaws.cloud” AWS_ACCESS_KEY_ID

“flaws.cloud” PROD_AWS_ACCESS_KEY_ID

“flaws.cloud” PROD_AWS_SECRET_ACCESS_KEY

“flaws.cloud” AWS_ROLE_TO_ASSUME

“flaws.cloud” AWS_ROLE_EXTERNAL_ID

“flaws.cloud” arn:aws:iam

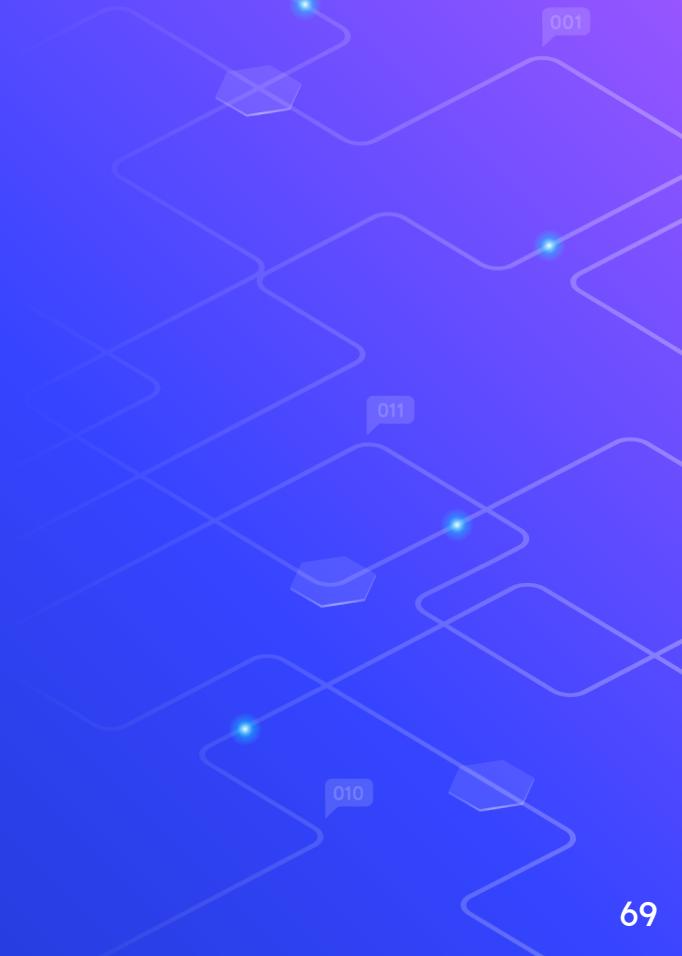


Github Leaks – Automated Tools

- GitLeaks
- TruffleHogs
- Any any other tools.

Gray Hat Warfare

- Public Bucket'ları listeleyen veritabanıdır.
- API'ı bulunmaktadır.
- Azure ve AWS için kullanılabilir.
- Ücretsiz/ücretli versiyonları vardır.



Google Dorks

site:s3.amazonaws.com example

site:s3.amazonaws.com example.com

site:s3.amazonaws.com example-com

site:s3.amazonaws.com com.example

site:s3.amazonaws.com com-example

site:s3.amazonaws.com filetype:xls password

site:http://s3.amazonaws.com intitle:index.of.bucket

site:http://amazonaws.com inurl:".s3.amazonaws.com/"

Censys

- API desteği mevcuttur.
- Ücretli/ücretsiz versiyonları vardır.
- Sertifikaları ve hostları arayabilirsiniz.
- Kullanımı kolaydır.

 Services: 2.0B

 IPv4 Hosts: 216.8M

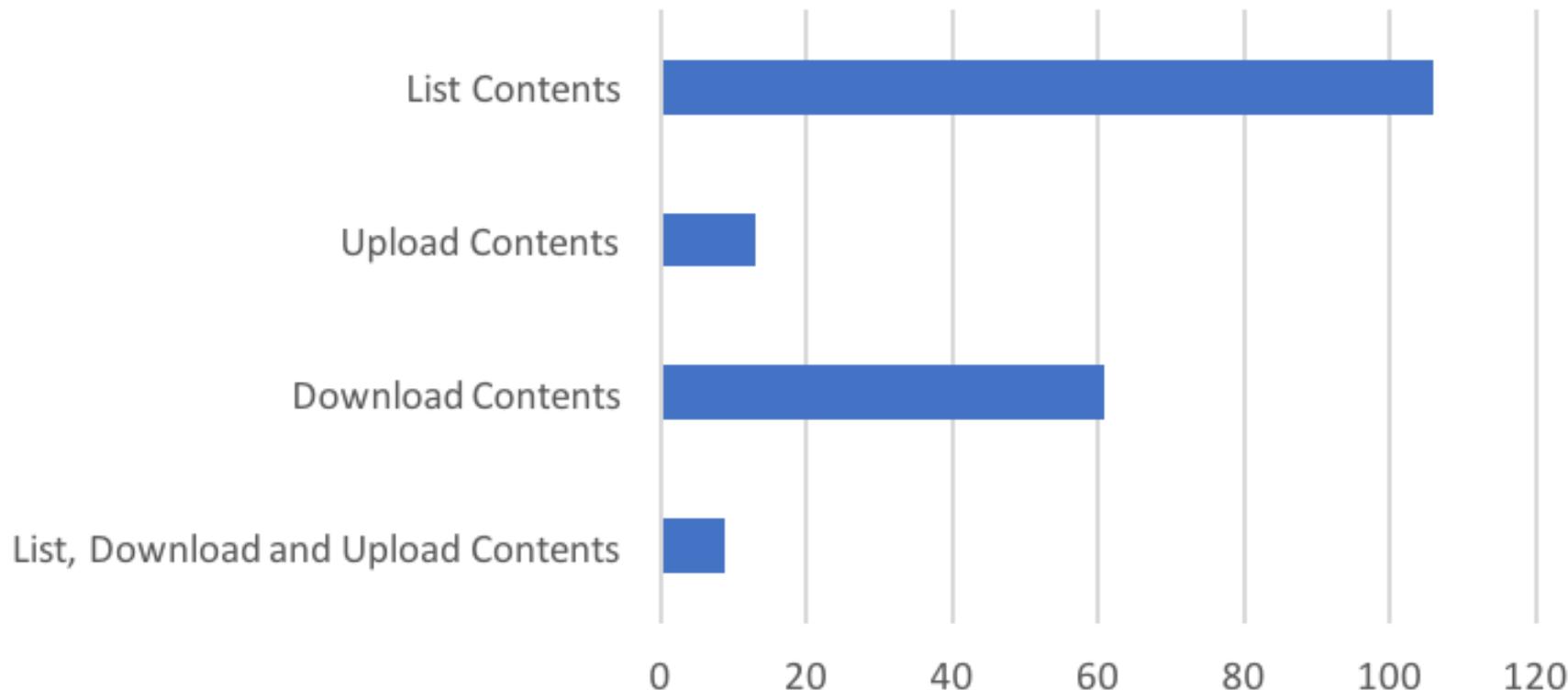
 IPv6 Hosts: 17.5M

 Virtual Hosts: 510.1M

S3 Direct Access

- Bucket yapısı:
 - [https://\[bucketname\].s3.amazonaws.com](https://[bucketname].s3.amazonaws.com)
 - [https://s3-\[region\].amazonaws.com/\[Org Name\]](https://s3-[region].amazonaws.com/[Org Name])
- dig domain.com
- nslookup IP
- Direct access from Browser or CLI usage.

Access Controls on S3 Buckets from Alexa Top 10,000



S3 Direct Access – Automated Tools

- S3Finder
- lazys3
- Mass3
- S3Scan
- Sublist3r
- Any any other tools.

Cognito Usage

Request:

- x-amz-target
- x-amz-user-agent
- Content-type:
application/x-amz-
json-1.1

Response:

- X-amzn-error-
message
- X-amzn-error-type
- x-amz-cognito-
request-id

```
1 HTTP/1.1 302 Found
2 Date: Sun, 14 Nov 2021 22:04:13 GMT
3 Content-Length: 0
4 Connection: close
5 x-amz-cognito-request-id: f733f3ae-a8b2-4e63-a991-edade83db8c4
6 X-Application-Context: application:prod:8443
7 Set-Cookie: cognito-f1=
    "W3sidGFyZ2V0UmVxdWVzdFBhdGgiOiIvbG9naW4iLCJtYXAiOnsibG9naW5FcnnJvck1lc3NhZ2UiO
    3QgdXNlcm5hbWUgb3IgcGFzc3dvcmQuIn19XQ=="; Version=1; Path=/; Secure; HttpOnly;
    SameSite=Lax
8 X-Content-Type-Options: nosniff
9 X-XSS-Protection: 1; mode=block
10 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
11 Pragma: no-cache
12 Expires: 0
13 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
14 X-Frame-Options: DENY
15 Server: Server
16 Location:
    https://ayberk.auth.us-east-2.amazoncognito.com/login?client_id=73fbim9p56ki26
    &response_type=code&scope=profile+aws.cognito.signin.user.admin+openid+phone+
    t_uri=http://localhost:8888/secure
17 Content-Language: en-US
18
19
```

“

```
{"payload":"{\"contextData\":{\"UserAgent\":\"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\", \"DeviceId\":\"k42hjublo4bvom18z6l7:1636927248305\", \"DeviceLanguage\":\"en-US\", \"DeviceFingerprint\":\"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0en-US\", \"DevicePlatform\":\"Win32\", \"ClientTimezone\":\"03:00\"}, \"username\":\"ayberk\", \"userPoolId\":\"\", \"timestamp\":\"1636927248305\"}","signature":"6QpDggY8w8VcwC5UVsn8whfhMM31FgBNlvdj6NC6Vio=","version":"JS20171115"}
```

Enumeration - With Creds.

- aws lambda list-functions
- aws rds describe-db-instances
- aws iam list-users
- aws iam list-roles
- aws s3api list-buckets
- aws ec2 describe-instances
- aws ec2 create-volume --snapshot-id snap-1337

Enumeration – With Creds. (Automation)

- weirdALL
- Pacu
- aws_pwn
- Scour
- ScoutSuite
- Barq
- Prowler
- CloudSploit



Public ECR

- Yazılım geliştiricilerin container görüntülerini ve yapıtlarını paylaşmasını ve dağıtmasını kolaylaştıran bir servistir.
- Elinizde key ikilisi varsa backdoor oluşturulabilir.



DoW (Denial of Wallet)

- DDoS'a çok benzer.
- Serverless yapılara özgü bir zafiyettir.
- Cloud yapılarda, sistemlerin ayakta kalabilmesi için Scalable yapılar bulunur. Saldırgan bu yapıyı hedef alır.

DoW - Lab (Protect Your Wallet)

- Billing Console altındaki Billing preferences'tan Receive Billing Alerts seçeneğini aktif edin.
- CloudWatch'dan yeni bir Alarm oluşturun ve Metric olarak Billing altındaki Total Estimated Charge seçin.
- Yeni bir SNS Topic oluşturun.
- Test edin.

Publicly Accessible S3 Bucket

- BPA ve Policy yapılandırma hatalarından kaynaklanır.
- İlgili S3 Bucket'ına yazılan verileri görüntülemenizi sağlar.
- Manuel ve otomatize araçlar ile sömürülebilir.

Publicly Writable S3 Bucket

- Yine BPA ve Policy yapılandırma hatalarından kaynaklanır.
- İlgili S3 Bucket'ına veri yazmanıza olanak sağlar.
- Manuel ve otomatize araçlar ile sömürülebilir.



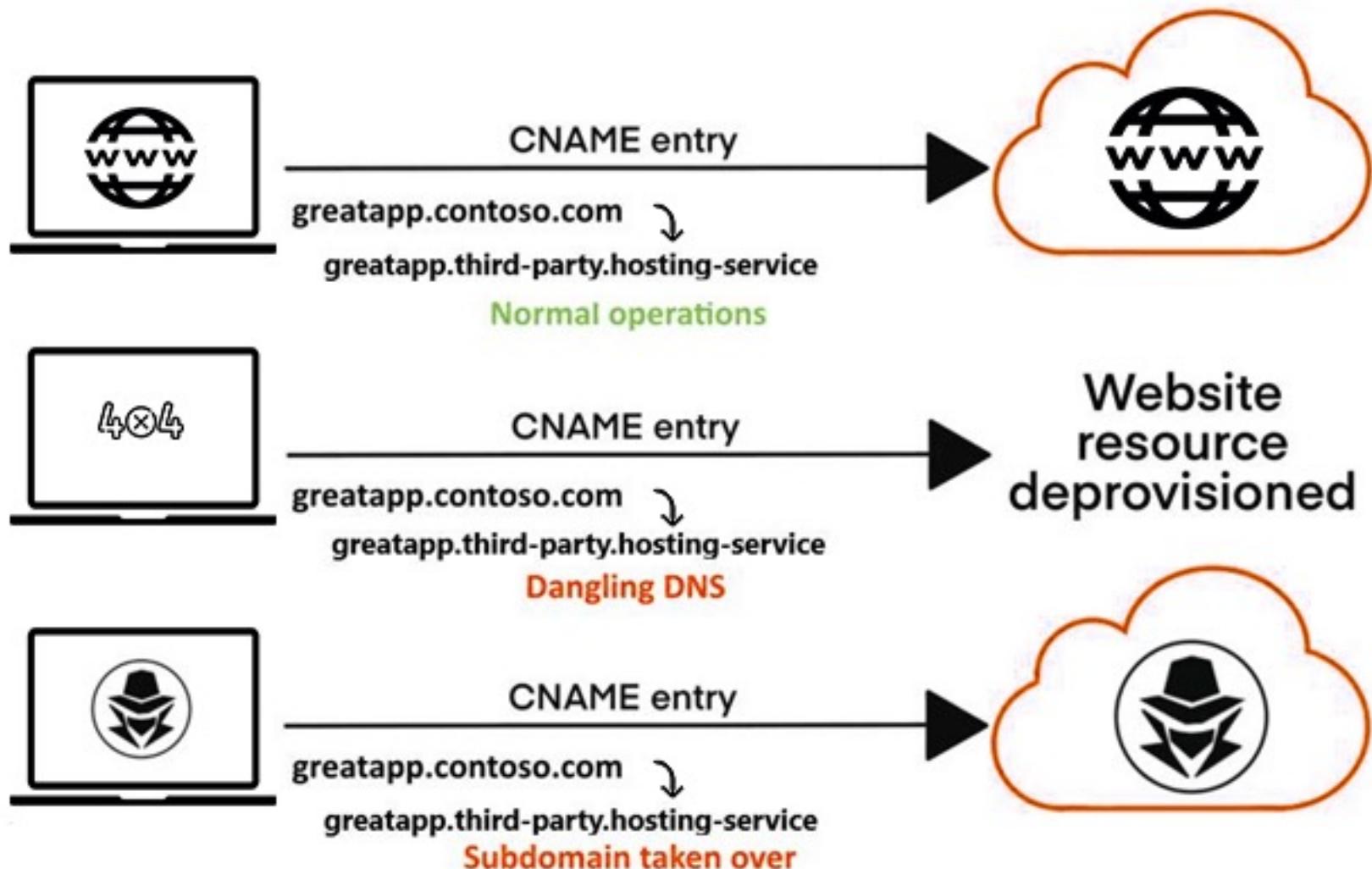
Subdomain Takeover

sub.domain.com IN CNAME anotherdomain.com.

Subdomain Takeover

- AWS'e özgü bir zafiyet değildir.
- Subdomain başka bir Domain'e CNAME kaydı ile yönlendirilmiştir.
- Yönlendirildiği Domain expire olmuştur.
- CNAME kaydı DNS Zone'dan silinmemiştir.





Takenover Proccess

- AWS konsol üzerinden S3 paneline erişim sağlayın.
- Yeni bir Bucket oluşturun.
- Bucket Name'i zafiyetli web adresi olarak belirtin. (Örn: takeover.ayberk.ninja)
- Bucket'ı bu ayarlar ile oluşturun.
- Upload sekmesine gelin.
- Buradan PoC dosyanızı Bucket'a yükleyin.
- Permission sekmesinden Grant public read access to this object(s) ayarını açın.
- Eğer yüklediğiniz dosya HTML dosyası ise yüklediğiniz dosyaya tıklayın ve More > Change Metadata menüsüne gelin.
- Add metadata diyerek Content-Type ayarını text/html olarak ayarlayın.

EC2 SSRF

- Bildiğimiz SSRF.
- Metadata verileri elde edilebilir.
- Metadata sunucusuna ilgili Instance'tan gidilerek kritik bilgiler elde edilebilir.

EC2 SSRF - Important Paths

- http://instance-data
- http://169.254.169.254
- http://169.254.169.254/latest/user-data
- http://169.254.169.254/latest/user-data/iam/security-credentials/[ROLE NAME]
- http://169.254.169.254/latest/meta-data/
- http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]
- http://169.254.169.254/latest/meta-data/ami-id
- http://169.254.169.254/latest/meta-data/reservation-id
- http://169.254.169.254/latest/meta-data/hostname
- http://169.254.169.254/latest/meta-data/public-keys/
- http://169.254.169.254/latest/meta-data/public-keys/[ID]/openssh-key
- http://169.254.169.254/latest/meta-data/iam/security-credentials/
- http://169.254.169.254/latest/meta-data/iam/security-credentials/runCommand

EC2 SSRF – Prevention (IMDS v2)

- IMDS: Instance Metadata Service.
- IMDS, geçici, kimlik bilgilerine erişim sağlayarak ve hassas kimlik bilgilerini manuel veya programlı olarak örneklerde sabit kodlama veya dağıtmaya ihtiyacını ortadan kaldırarak bulut kullanıcıları için büyük bir güvenlik sorununu çözdü.

EC2 SSRF – Prevention (IMDS v2)

- Instance Metadata Service Version 1 (IMDSv1) – a request/response method
- Instance Metadata Service Version 2 (IMDSv2) – a session-oriented method

Cognito Account Takeover

- Cognito bir kimlik yönetimi servisidir.
- Yanlış yapılandırma sonucu yetki yükselme, sisteme kayıt olma ve Account Takeover zayıflıklarına sebebiyet verebilmektedir.

Cognito Self Registration

- Kullanıcıların arayüz üzerinden kayıt olmaları kapatılmış olabilir.
- Yanlış yapılandırma ile CLI üzerinden kayıt olunabilir.



Defend The Cloud

AWS Security Services



AWS Security Services

- IAM
- Config
- Inspector
- WAF & Shield & Firewall Manager
- CloudTrail
- Trusted Advisor
- GuardDuty



IAM

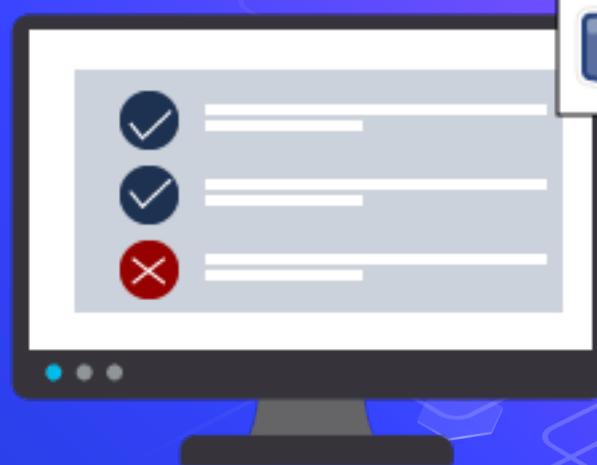
- Identity and Access Manager
- Adından da anlaşılabileceği gibi kimlik yönetimidir.
- Hangi kullanıcının ve servisin hangi servislere hangi yetkilerle erişebileceğini belirlediğiniz servistir.
- Parola politikası ayarlamaları da bu servis ile yapılır.

Authentication



Confirms users are who they say they are

Authorization



Gives users permission to access a resource

Least Privilege Access

- Best Practise olarak kullanıcılar en az yetkilere sahip olmalıdır. Sahip olmaları gerektikleri yetkiler haricinde herhangi bir yetkiye sahip olmamalıdır.
- Yetkiler düzenli olarak denetlenmelidir.
- Shadow Admin'lere dikkat edilmelidir.

User & Group

- Kullanıcılar, AWS'teki kaynaklarınızı belirli kurallar ile erişebilecek hesaplara verilen isimdir.
- Gruplar, birden fazla AWS kullanıcılarına tek seferde yetki atamayı sağlar. Ayrıca sınıflandırmayı kolaylaştırır.

Policy & Role

- Kimin, hangi kaynaklara ne şekilde ve ne kadarına erişebileceğini AWS'te Policy'ler ile belirliyoruz.
- Policy'ler JSON formatındadır.
- Role'ler ise AWS kaynaklarına diğer AWS kaynaklarının ne şekilde ve ne kadarına erişebileceğini belirler.
- Ayrıca Role'ler dış dünyadaki kimlik sağlayıcıları ile güven ilişkisi kurulmasını sağlar.

Find users by username or access key

Showing 14 results

	User name	Access key age	Password age	Access key ID
<input type="checkbox"/>	trob	! 546 days	334 days	AKIAFR2DYF3Z7ZIDWIIA (Active) AKIAFCM7OSGT2P6QHRDA (Active)
<input type="checkbox"/>	trent	✓ 48 days	48 days	AKIAFFHFSENEQ6ADI3BA (Active)
<input type="checkbox"/>	oscar	✓ Today	Today	AKIAECQ6ANN37OVMS7LQ (Active)
<input type="checkbox"/>	mallory	⚠ 199 days	Today	AKIAFA4VB7YDZSK7AUKQ (Active)
<input type="checkbox"/>	heidi	✓ Today	Today	AKIAFJ5BIBVXCEK4BFXQ (Active)
<input type="checkbox"/>	grace	✓ 42 days	Today	AKIAFXAKOKGROKFYXAUQ (Active)
<input type="checkbox"/>	frank	✓ Today	Today	AKIAFMB6S25SER5JIQVA (Active)
<input type="checkbox"/>	erin	✓ Today	Today	AKIAFEX6UG65HAYAAPOA (Active)

User Keys

Access Key ID

- 20 random alfanumerik büyük harften oluşur.



Secret Access Key ID

- 40 random alfanumerik ve alfanumerik olmayan, büyük ve küçük harften oluşur.



“

arn:aws:iam::123123123123:user/HackTrick
arn:partition:service:region:account-id:resource-type:resource-id

“

CLOSER LOOK

Users & Groups

Policy Structure

Version: Kullanılan Policy'nin versiyonunu belirtir.

Statement: Policy'nin ana koşulları belirtilir.

Condition: Policy'nin yerine gelmesi için gerekli koşulları belirtir.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "FirstStatement", ————— Unique identifier  
            "Effect": "Allow",  
            "Action": ["iam:ChangePassword"],  
            "Resource": "*"  
        },  
        {  
            "Sid": "SecondStatement",  
            "Effect": "Allow", ————— Allow or Deny  
            "Action": "s3>ListAllMyBuckets",  
            "Resource": "*"  
        },  
        {  
            "Sid": "ThirdStatement",  
            "Effect": "Allow",  
            "Action": [  
                "s3>List*", ————— Neler yapılacak?  
                "s3:Get*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::confidential-data",  
                "arn:aws:s3:::confidential-data/*"  
            ],  
            "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}  
        }  
    ]  
}
```

Hangi kaynaklar etkilenenecek?

Ways To Create A Policy

1. AWS tarafından yönetilen bir Policy’I kopyalayabilirsiniz.
2. Policy Generator’u kullanarak bir Policy oluşturabilirsiniz.
3. Tamamen manuel kendi Policy’nizi oluşturabilirsiniz.

“

CLOSER LOOK

Policy

Policy - Lab (Secure S3)

- Yeni bir S3 Bucket yaratın.
- Bu Bucket'a yalnızca belirli IP adresinden erişilmesine izin verilen Policy'yi hazırlayın.
- İlgili Policy'yi test edin.

The Problem – Rotating Keys



Key rotation



Key ID = 1234abcd-12ab-34cd-56ef-1234567890ab

Key ID = 1234abcd-12ab-34cd-56ef-1234567890ab

CloudTrail

- AWS hesabınızdaki tüm API call'larını kaydedip izleyen loglama servisidir.
- SDK, CLI, Management Console ve diğer AWS servislerinden yapılan tüm call'ları loglar.
- Otomatik aksiyon almaz fakat otomatize edilebilir.
- Tespit edilen aktiviteler Dashboard üzerindenfiltrelenebilir, arşivlenebilir, indirilebilir, analiz edilebilir ve aksiyon alınabilir.

CloudTrail vs CloudWatch

CloudTrail

- AWS'te kim ne yaptı?
- AWS'de gerçekleşen tüm eylemlerin günlüğüdür.
- Verileri 15 dakikada bir toplar.

CloudWatch

- AWS'te neler oluyor?
- Servislerin sağlık ve performansı hakkında bilgi verir.
- Verileri 5 dakikada bir toplar.



Process Flow



CloudTrail Permissions

AWSCloudTrail_FullAccess

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "sns:AddPermission",  
8                 "sns>CreateTopic",  
9                 "sns:SetTopicAttributes",  
10                "sns:GetTopicAttributes"  
11            ],  
12            "Resource": [  
13                "arn:aws:sns:*:*:aws-cloudtrail-logs"  
14            ]  
15        },  
16        {  
17            "Effect": "Allow",  
18            "Action": [  
19                "sns>ListTopics"  
20            ],  
21            "Resource": "*"  
22        },  
23        {  
24            "Effect": "Allow",  
25            "Action": [  
26                "s3>CreateBucket",  
27                "s3:PutObject",  
28                "s3:PutObjectAcl",  
29                "s3:ListBucket",  
30                "s3:ListBucketM  
31        ]  
32    ]  
33}
```

AWSCloudTrailReadOnlyAccess

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "s3:GetObject",  
8                 "s3:GetBucketLocation"  
9             ],  
10            "Resource": "*"  
11        },  
12        {  
13            "Effect": "Allow",  
14            "Action": [  
15                "cloudtrail:GetTrail",  
16                "cloudtrail:GetTrailStatus",  
17                "cloudtrail:DescribeTrails",  
18                "cloudtrail>ListTrails",  
19                "cloudtrail:LookupEvents",  
20                "cloudtrail>ListTags",  
21                "cloudtrail>ListPublicKeys",  
22                "cloudtrail:GetEventSelectors",  
23                "cloudtrail:GetInsightSelectors",  
24                "s3>ListAllMyBuckets",  
25                "kms>ListAliases",  
26                "lambda>ListFunctions"  
27            ],  
28            "Resource": "*"  
29        }  
30    ]  
31}
```

Trail

- CloudTrail'de loglamaya başlamak için ilk olarak Trail oluşturmanız gerekmektedir.
- Hangi API Call'larının loglanacağı, hangi S3 Bucket'ında tutulacağı, log validation yapılmış olup olmadığı gibi bilgiler Trail oluşturulurken ayarlanır.

CloudTrail Logs

- JSON formatındadır.
- Her API çağrıları için yeni bir olay yazılır.
- Her 5 dakikada bir yeni bir log dosyası oluşturulur.
- Log dosyaları 15 dakikada bir S3'e yazılır.
- AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat

```
{"Records": [{"eventVersion": "1.0", "userIdentity": {"type": "IAMUser", "principalId": "EX_PRINCIPAL_ID", "arn": "arn:aws:iam::123456789012:user/Alice", "accessKeyId": "EXAMPLE_KEY_ID", "accountId": "123456789012", "userName": "Alice"}, "eventTime": "2014-03-06T21:22:54Z", "eventSource": "ec2.amazonaws.com", "eventName": "StartInstances", "awsRegion": "us-east-2", "sourceIPAddress": "205.251.233.176", "userAgent": "ec2-api-tools 1.6.12.2", "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}}, "responseElements": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2", "currentState": {"code": 0, "name": "pending"}, "previousState": {"code": 80, "name": "stopped"}}]}]}]}]
```

“

CLOSER LOOK

Inspector

- EC2 Instance'ları ve ECR Container'ları üzerindeki zayıflıkları tespit eder.
- Agent ile çalışır.
- Linux-based, Windows-based ve Amazon Linux 2 AMI üzerine Agent kurulabilir.
- Ücretlendirmesi oldukça uygundur.
- Tespit edilen zayıflıklar opsiyonel olarak S3'te de depolanabilir. (Dashboard 30 gün tutar.)

Inspector - Agent Installation

For Linux:

- wget <https://inspector-agent.amazonaws.com/linux/latest/install>
- sudo bash install

For Windows:

- <https://inspector-agent.amazonaws.com/windows/installer/latest/ASAgentInstall.exe>

Inspector



CVE



CIS Benchmarks



Security Best Practises



Runtime Behavior Analysis

- hexagon Oluşturulduktan sonra düzenlenemez.
- hexagon Agent'ın taramayı nasıl yapacağını belirttiğimiz yerdir.
- hexagon SNS Topic başlama zamanı, bitiş zamanı, durum değişiklikleri ve tespit edilen bulgular hakkında bildirim yapabilir.

Assetment Template

Rules Packages

- CVE
- Best Practices

Duration

- 1 hour

SNS Topic

- Alert

Attributes for Findings

- Key: "Enviroment"
- Value: "Test"

HIGH

Hızlı bir şekilde aksiyon alınması gereken bulgulardır.

MEDIUM

Verilerinizin bütünlüğü, gizliliği ve kullanılabilirliği için risk oluşturur.

LOW

Aciliyeti olmayan fakat yine de aksiyon alınması gereken bulgulardır.

Finding Reports

- Taranan EC2 Instance'larının listesi.
- Kullanılan Rule paketleri.
- Tespit edilen bulguların detaylı listesi.

Full Report

- Finding Report'ta bulunan herşey.
- 
- Başarıyla geçen Rule paketlerinin de listesi.

Ücretsiz Deneme Ayrıntıları

Amazon Inspector'un ilk kullanımından sonraki 90 gün

İlk 250 sunucu değerlendirmesi

Sunucu Değerlendirmesi Başına Fiyat

0,00 USD

Fiyatlandırma Ayrıntıları

Belirli bir ayda

İlk 250 sunucu değerlendirmesi

Sunucu Değerlendirmesi Başına Fiyat

0,15 USD

Sonraki 750 sunucu değerlendirmesi

0,13 USD

Sonraki 4000 sunucu değerlendirmesi

0,10 USD

Sonraki 45.000 sunucu değerlendirmesi

0,07 USD

Diğer tüm değerlendirmeler

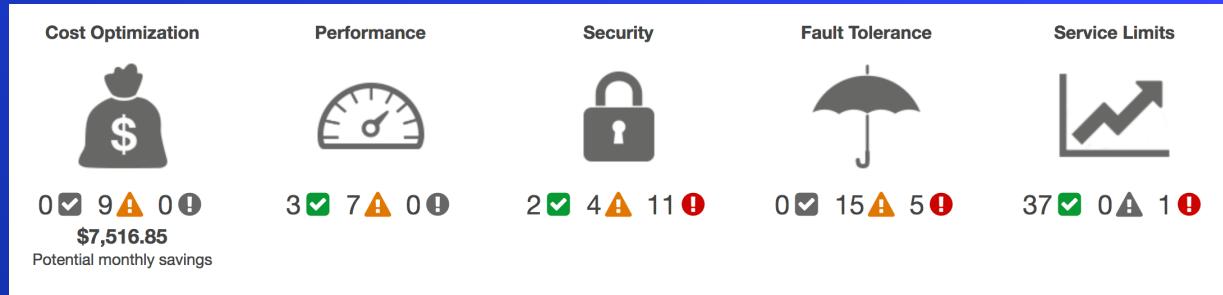
0,04 USD

“

CLOSER LOOK

Trusted Advisor

- Bir dizi önemli alanda altyapınızı optimize etmenize yardımcı olur.
- Yalnızca güvenlik değil; performans, servis limitleri gibi konularda da optimizasyon yapmanıza yardımcı olur.



	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
Cost Optimization	✗	✗	✓	✓
Performance	✗	✗	✓	✓
Security	6 core checks	6 core checks	✓	✓
Fault Tolerance	✗	✗	✓	✓
Service Limits	✓	✓	✓	✓

Basic Plan Checks

- S3 Bucket İzinleri
- EBS Public Snapshot'lar
- RDS Public Snapshot'lar
- IAM Kullanım Verileri
- Root Hesapta MFA Kullanımı
- Security Groups



Trusted Advisor Permissions

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy

Access for the AWS Trusted Advisor Service to help reduce cost, increase performance, and improve

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "autoscaling:DescribeAccountLimits",  
8         "autoscaling:DescribeAutoScalingGroups",  
9         "autoscaling:DescribeLaunchConfigurations",  
10        "cloudformation:DescribeAccountLimits",  
11        "cloudformation:DescribeStacks",  
12        "cloudformation>ListStacks",  
13        "cloudfront>ListDistributions",  
14        "cloudtrail:DescribeTrails",  
15        "cloudtrail:GetTrailStatus",  
16        "dynamodb:DescribeLimits",  
17        "dynamodb:DescribeTable",  
18        "dynamodb>ListTables",  
19        "ec2:DescribeAddresses",  
20        "ec2:DescribeReservedInstances",  
21        "ec2:DescribeInstances",  
22        "ec2:DescribeVpcs",  
23        "ec2:DescribeInternetGateways",  
24        "ec2:DescribeImages",  
25        "ec2:DescribeVolumes",  
26        "ec2:DescribeSecurityGroups",  
27      ]  
28    }  
29  ]  
30}
```

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy

Service Policy for Trusted Advisor Multi-account Reporting

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": [  
6         "organizations:DescribeOrganization",  
7         "organizations>ListAWSServiceAccessForOrganization",  
8         "organizations>ListAccounts",  
9         "organizations>ListAccountsForParent",  
10        "organizations>ListOrganizationalUnitsForParent",  
11        "organizations>ListChildren",  
12        "organizations>ListParents",  
13        "organizations:DescribeOrganizationalUnit",  
14        "organizations:DescribeAccount"  
15      ],  
16      "Effect": "Allow",  
17      "Resource": "*"  
18    }  
19  ]  
20 }
```

Basic Support Planı dahil

Developer

Hangisi büyüğse: 29,00 USD

- veya -

aylık AWS ücretlerinin %3'ü

Business

Hangisi büyüğse: 100,00 USD

- veya -

ilk 0-10.000 USD aralığındaki aylık AWS ücretlerinin %10'u

10.000-80.000 USD aralığındaki aylık AWS ücretlerinin %7'si

80.000-250.000 USD aralığındaki aylık AWS ücretlerinin %5'i

250.000 USD üzerindeki aylık AWS ücretlerinin %3'ü

Enterprise On-Ramp

Hangisi büyüğse: 5.500,00 USD

- veya -

aylık AWS ücretlerinin %10'u

Enterprise

Hangisi büyüğse: 15.000,00 USD

- veya -

ilk 0-150.000 USD aralığındaki aylık AWS ücretlerinin %10'u

150.000-500.000 USD aralığındaki aylık AWS ücretlerinin %7'si

500.000-1 milyon USD aralığındaki aylık AWS ücretlerinin %5'i

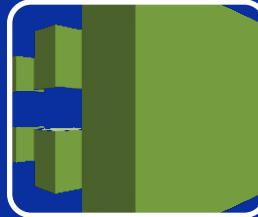
1 milyon USD üzerindeki aylık AWS ücretlerinin %3'ü

“

CLOSER LOOK

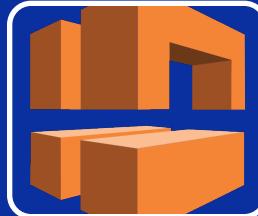
GuardDuty

- Tehdit algılama yönetimi servisidir.
- Servis makine öğrenimi kullanmaktadır.
- Otomatize ve devamlı güvenlik denetimleri sağlar.
- Herhangi bir agent vs. kurulumuna gerek duymaz.
- AWS servislerinde performansı etkilemez.
- Tek bir Dashboard ile tüm AWS hesapları için kullanılabilir.



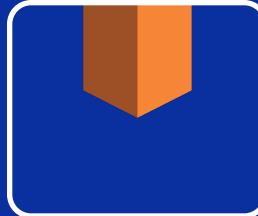
CloudTrail Event Logs

- API Call loglarıdır.



VPC Flow Logs

- VPC'nizdeki ağ trafigi loglarıdır.



DNS Query Logs

- Route53 DNS loglarıdır.

GuardDuty - Lists

White List

- GuardDuty tarafından engellenmeyecek IP listesidir.
- Yalnızca 1 White List tanımlanabilir.

Black List

- GuardDuty tarafından engellenenek IP listesidir.
- 6 adede kadar aktif tehdit listeniz olabilir.

HIGH (7.0 – 8.9)

Söz konusu kaynağın (EC2 Instance IAM kullanıcı kimlik bilgisi) güvenliğinin ihlal edildiğini ve yetkisiz amaçlar için etkin bir şekilde kullanıldığını gösterir.

MEDIUM (4.0 – 6.9)

Normal olarak gözlemlenen davranıştan sapan şüpheli etkinliği belirtir ve kullanım durumunuza bağlı olarak bir kaynak ihlalinin göstergesi olabilir.

LOW (0.1 – 3.9)

Ağınızın güvenliğini tehditeye atmayan, örneğin bir bağlantı noktası taraması veya başarısız bir izinsiz giriş girişimi gibi şüpheli etkinlik girişimi olduğunu gösterir.

Bölgeye göre fiyatlandırma

Bölge: Avrupa (İrlanda) ▾

AWS CloudTrail Yönetim Olayı Analizi

Ayda bir milyon olay başına	Bir milyon olay başına 4,40 USD
-----------------------------	---------------------------------

AWS CloudTrail S3 Veri Olayı Analizi

Ayda ilk 500 milyon olay başına	Bir milyon olay başına 0,80 USD
Ayda sonraki 4.500 milyon olay başına	Bir milyon olay başına 0,40 USD
Ayda 5.000 milyondan fazla olay başına	Bir milyon olay başına 0,20 USD

Amazon EKS Denetim Günlükleri

Ayda ilk 100 milyon olay	1 milyon olay başına 1,73 USD
Ayda sonraki 100 milyon olay	1 milyon olay başına 0,87 USD
Ayda 200 milyondan fazla olay	1 milyon olay başına 0,22 USD

VPC Akış Günlüğü ve DNS Sorgu Günlüğü Analizi

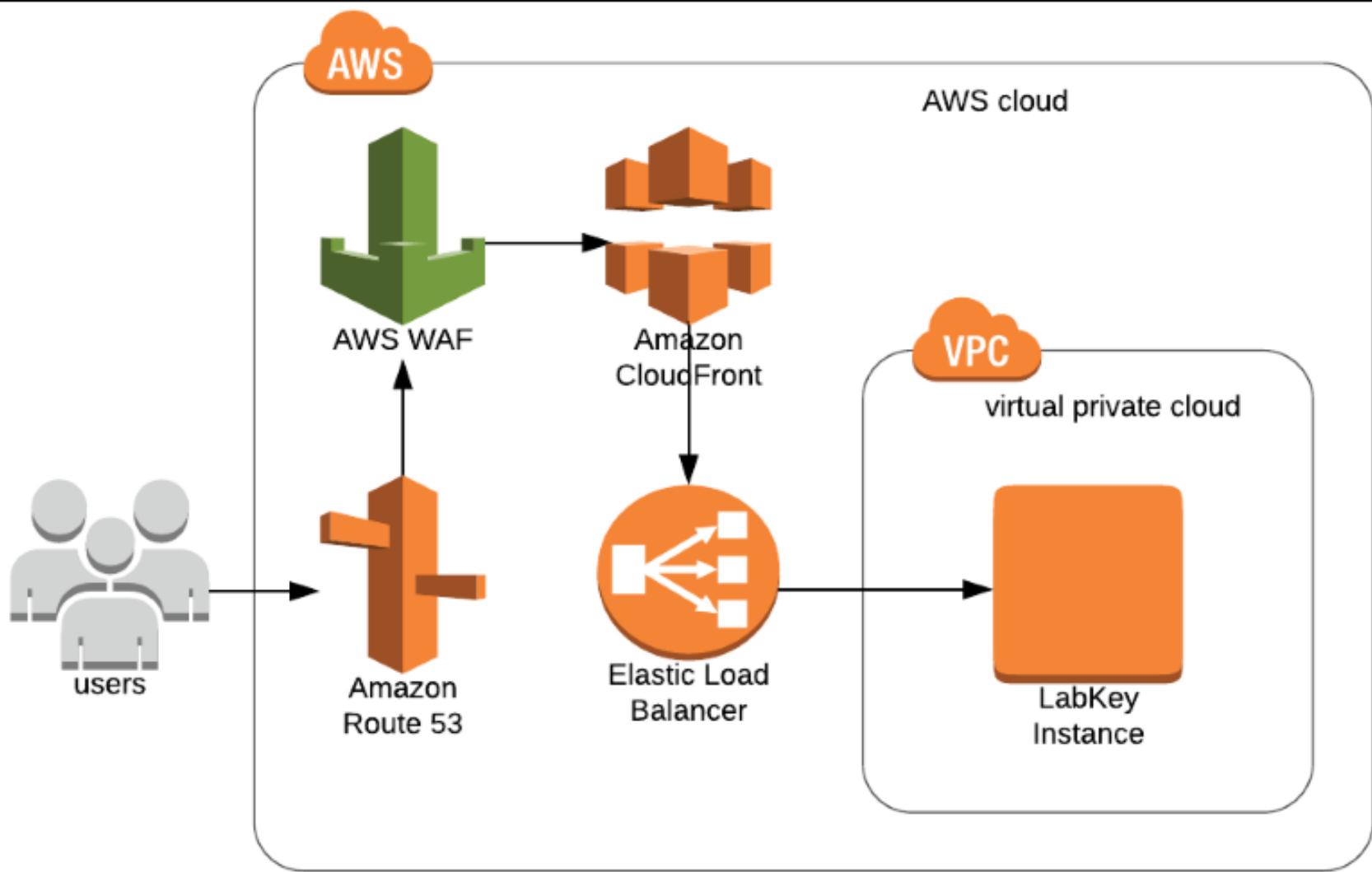
Ayda ilk 500 GB	GB başına 1,10 USD
-----------------	--------------------

“

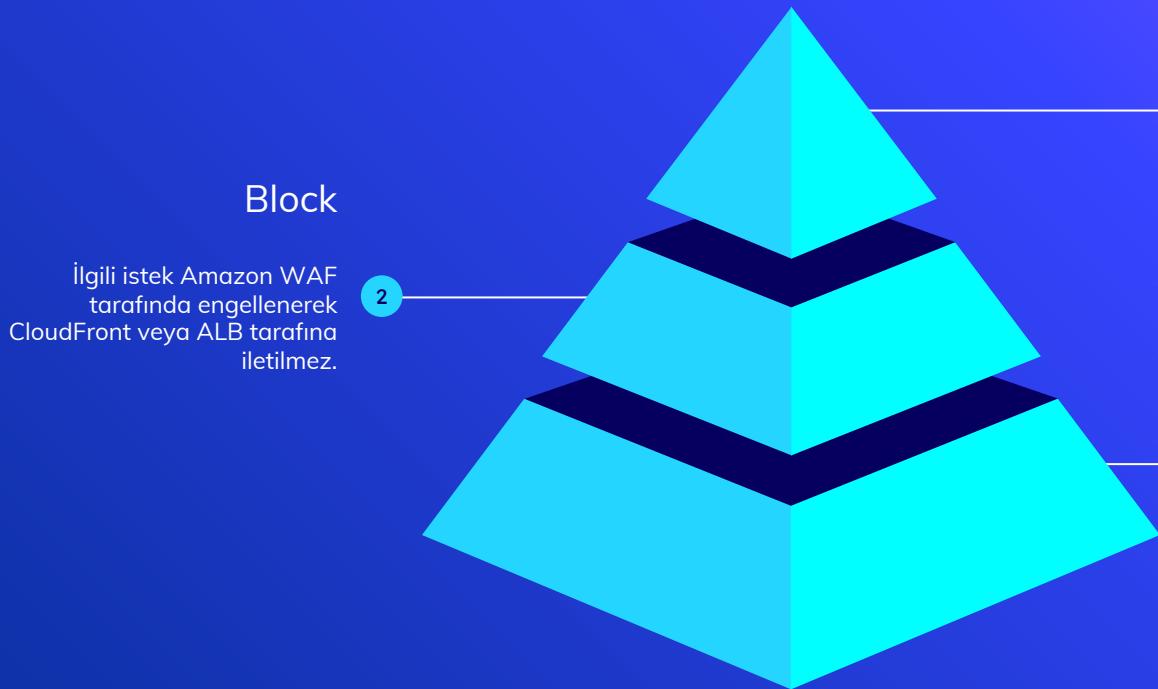
CLOSER LOOK

AWS WAF

- Web Application Firewall
- CloudFront ve Load Balancer'ların web isteklerini takip eder.
- Hem HTTP hem de HTTPS tarfiğini izler.
- PCI DSS 3.2 sertifikalı servistir.



Web ACL



Allow

İstek ilgili CloudFront'a veya ALB'ye iletilir. Herhangi bir engelleme yapılmaz.

Count

İlgili kuralların koşulları karşılayan isteklerin sayısını sayar

Firewall Manager

- AWS Organizations tarafından birden fazla AWS hesabınız varsa varlıklarınızı aynı şekilde korumak isteyeceksiniz.
- Aynı kuralları tekrar tekrar oluşturmak fazladan iş yükü getirecektir.

Firewall Manager - Prerequisites

- Hangi AWS hesabının Firewall Manager Admin olacağı seçilmelidir.
- AWS Config servisinin aktif olması gerekmektedir.
- AWS hesabınızı bir AWS Organization parçası olmalı.

Firewall Manager - Quotas

Mutable Quotas

- Artış talebi istenebilen kotalardır.

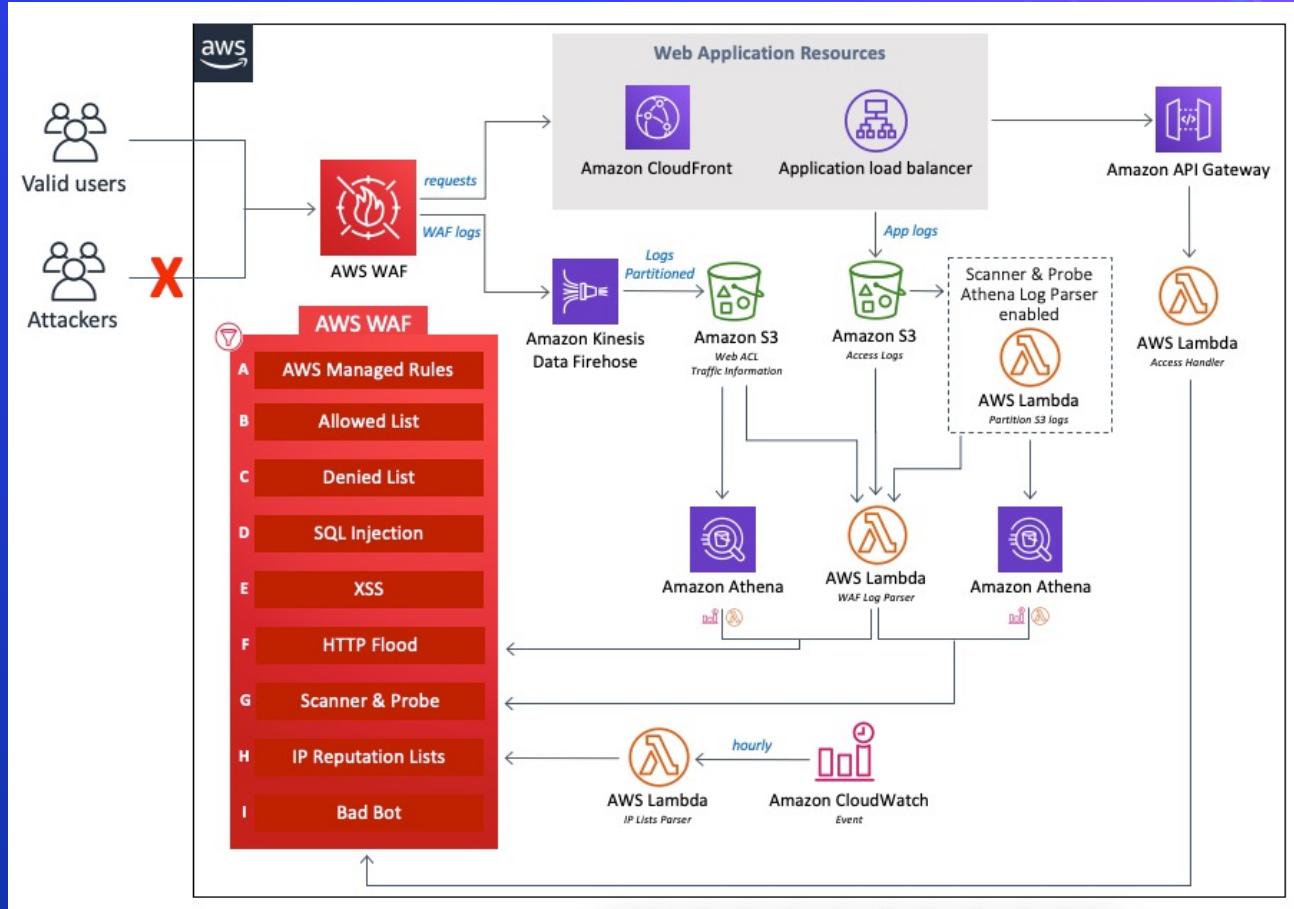
Immutable Quotas

- Tüm AWS kullanıcıları için sabit ve artış talebi istenemeyen kotalardır.

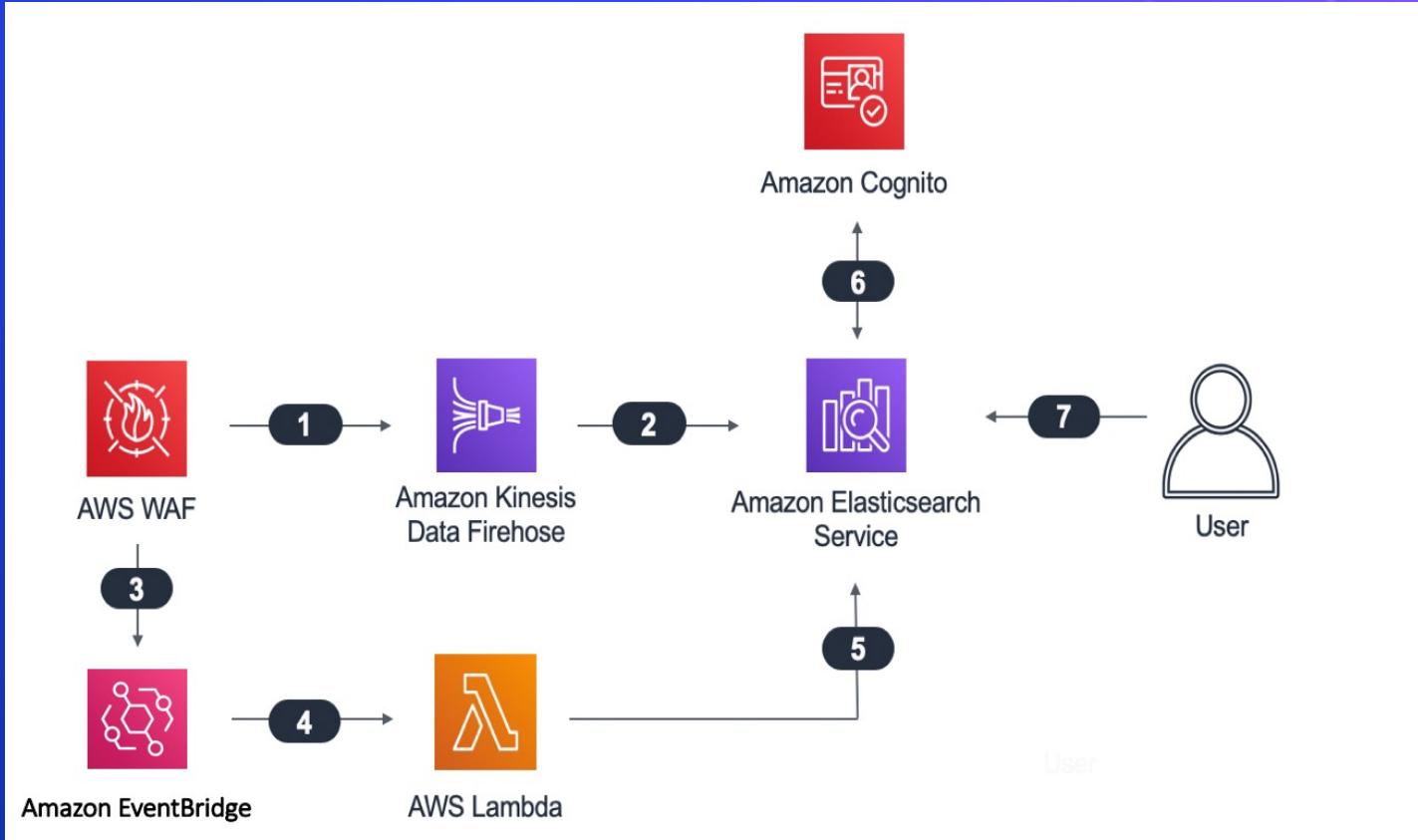
AWS WAF – Lab (Protection Against Brute Force)

- AWS WAF üzerinde giriş panelinize (Path: /login.php) yapılabilecek Brute Force (Kaba Kuvvet) saldırılarını engelleyecek custom rule oluşturun.

WAF Automation on AWS



WAF Dashboard

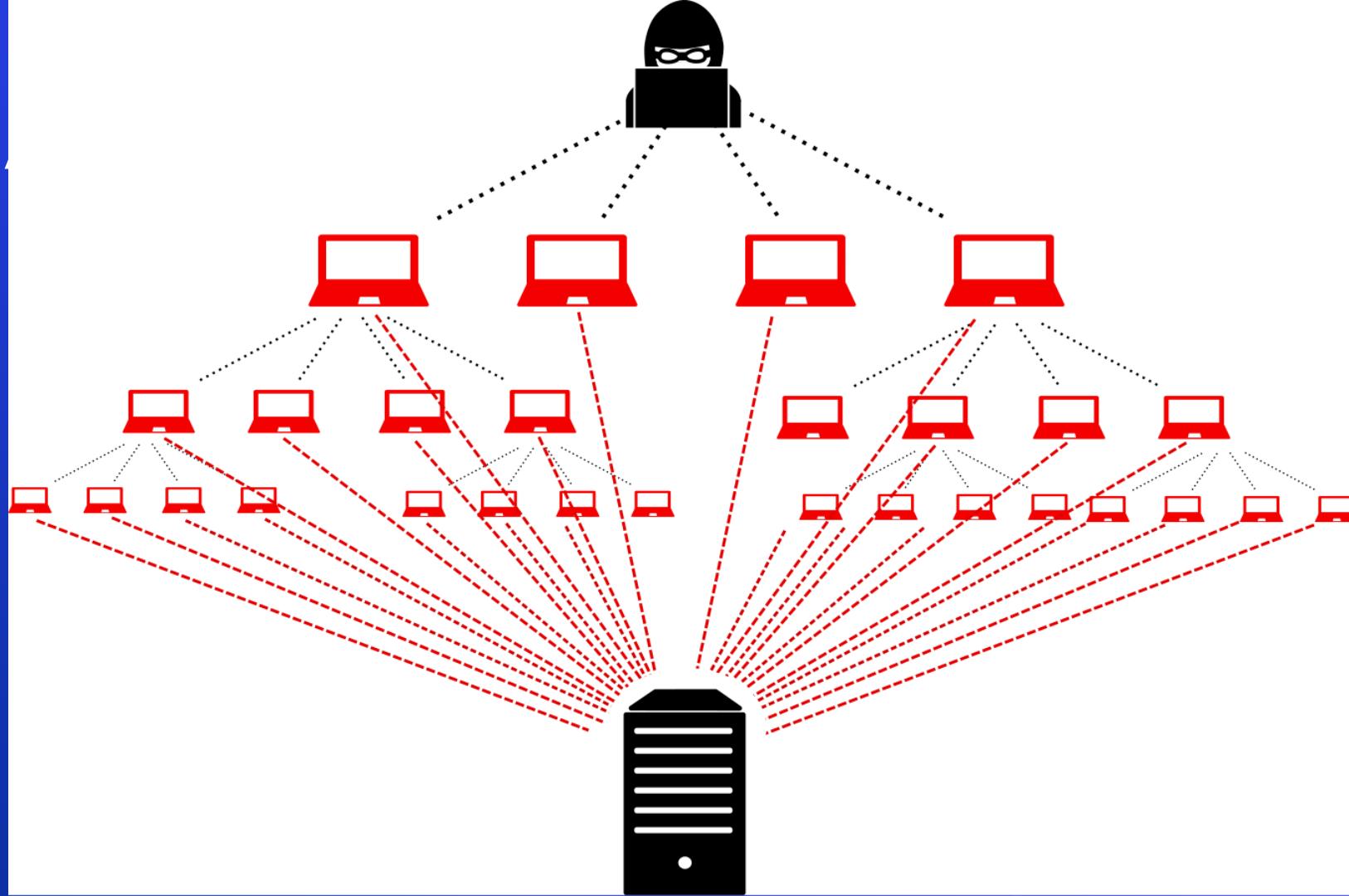


Web ACL'ınızde etkinleştirilebilen isteğe bağlı güvenlik özelliklerinin ücretleri aşağıdaki tabloda listelenmiştir. Bu ücretler, önceki tabloda listelenen AWS WAF ücretlerine eklenir. AWS Shield Advanced kaynak korumasını etkinleştirerek elde edeceğiniz maliyet tasarrufu, aşağıdaki tabloda yer alan güvenlik özellikleri için geçerli değildir. Fiyatlandırma tüm AWS Bölgelerinde aynıdır. Abonelik ücreti (saate göre orantılı olarak hesaplanır), istek ücreti ve geçerli olduğu durumlarda analiz ücreti ödersiniz.

	Abonelik ücreti	İstek ücreti	Analiz ücreti
AWS WAF Robot Kontrolü			
Robot Kontrolü	Aylık 10,00 USD	Denetlenen bir milyon istek başına 1,00 USD	-
Captcha	-	-	Analiz edilen 1.000 görev denemesi başına 0,40 USD
AWS WAF Dolandırıcılık Kontrolü			
Hesabın Ele Geçirilmesini Önleme	Aylık 10,00 USD	-	Analiz edilen 1.000 oturum açma denemesi başına 1,00 USD

AWS Shield

- Altyapınızı DDoS saldırılarına karşı korumak için tasarlanmıştır.



001

AWS Shield - Types

Standart

- Herkes için ücretsizdir.
- Layer 3 (Network) ve Layer 4 (Transport) noktasında koruma sağlar.

Advanced

- Layer 3, Layer 4 ve Layer 7'de koruma sağlar.
- 7/24 AWS tarafından sağlanan uzman DDoS Response Team desteği bulunur.
- Real-time ölçüm yapar.



AWS Shield Advanced İçin Dışarı Veri Aktarımı Kullanım Ücretleri (GB başına)

	Amazon CloudFront	Elastic Load Balancing (ELB)	AWS Elastic IP (EC2 ve Network Load Balancer)	AWS Global Accelerator	Amazon Route 53
İlk 100 TB	0,025 USD	0,05 USD	0,05 USD	0,025 USD	Ek ücret yoktur
Sonraki 400 TB	0,02 USD	0,04 USD	0,04 USD	0,02 USD	Ek ücret yoktur
Sonraki 500 TB	0,015 USD	0,03 USD	0,03 USD	0,015 USD	Ek ücret yoktur
Sonraki 4 PB	0,01 USD	Bize Ulaşın	Bize Ulaşın	0,01 USD	Ek ücret yoktur
5 PB üstü	Bize Ulaşın	Bize Ulaşın	Bize Ulaşın	Bize Ulaşın	Ek ücret yoktur

AWS Config

- AWS kaynaklarınızın yapılandırmalarını incelemenizi, denetlemenizi ve değerlendirmenizi sağlayan bir hizmettir.
- İçerisinde hazır çok sayıda Rule Set barındırır.
- Hangi kaynaklara sahibim, kaynaklarımda zaman içerisinde nasıl değişiklikler yapıldı, doğru denetim bilgisine sahip miyim gibi sorulara cevap bulmanızı sağlar.

AWS Config

- Her bir Region için en fazla 50 kural işletebilirsiniz.
- Config geçmiş dosyalarını S3 Bucket'larda depolamanıza onak tanır.
- Özette, AWS Config, kaynaklar arasındaki ilişkileri tanımlar.

CloudTrail entegrasyonu vardır.

Konfigürasyon geçmişini saklar.

Güvenlik analizleri gerçekleştirir.

Konfigürasyonlarla ilgili snapshot almanızı sağlar.

Compliance uyumluluk kontrolü sağlar.

Değişikliklerle ilgili notification sağlar.

Region spesifiktir.

AWS Config kuralları

1 Ağustos 2019 itibariyle geçerli olmak üzere bölge başına hesabınızdaki etkin kuralların sayısı yerine kaydedilen AWS Config kural değerlendirme melerinin sayısına göre ücretlendirilirsiniz. Bir kaynak, AWS Config kuralına uygunluk açısından değerlendirildiğinde bir kural değerlendirilmesi de kaydedilir.

AWS Config kural değerlendirme	Fiyat
İlk 100.000 kural değerlendirme	Bölge başına kural değerlendirme bazında 0,001 USD
Sonraki 400.000 kural değerlendirme (100.001-500.000)	Bölge başına kural değerlendirme bazında 0,0008 USD

AWS Birleştirilmiş faturalama ile birlikte hangi fiyatlandırma katmanının geçerli olduğunu belirlemek için yüksek seviyelerde düşük bir genel fiyat vermek suretiyle tüm hesaplarınıza ilişkin toplam AWS Config kural değerlendirme sayısını ölçecektir.

Uygunluk paketleri

Aşağıdaki katmana uygun olarak AWS Bölgesi başına AWS hesabınızdaki uygunluk paket değerlendirme başına ücretlendirilirsiniz. Bir uygunluk paketi değerlendirme, uygunluk paketindeki bir Config kuralı tarafından bir kaynağın değerlendirilmesi olarak tanımlanmaktadır.

Uygunluk paketi değerlendirme	Fiyat
İlk 1.000.000 uygunluk paketi değerlendirme	Bölge başına uygunluk paketi değerlendirme bazında 0,0012 USD
1.000.001 - 25.000.000 uygunluk paketi değerlendirme	Bölge başına uygunluk paketi değerlendirme bazında 0,001 USD
25.000.001 ve fazlası	Bölge başına uygunluk paketi değerlendirme bazında 0,0008 USD

AWS Birleştirilmiş faturalama ile birlikte hangi fiyatlandırma katmanının geçerli olduğunu belirlemek için yüksek seviyelerde düşük bir genel fiyat vermek suretiyle tüm hesaplarınıza ilişkin toplam AWS Config uygunluk paketi değerlendirme sayısını ölçecektir.

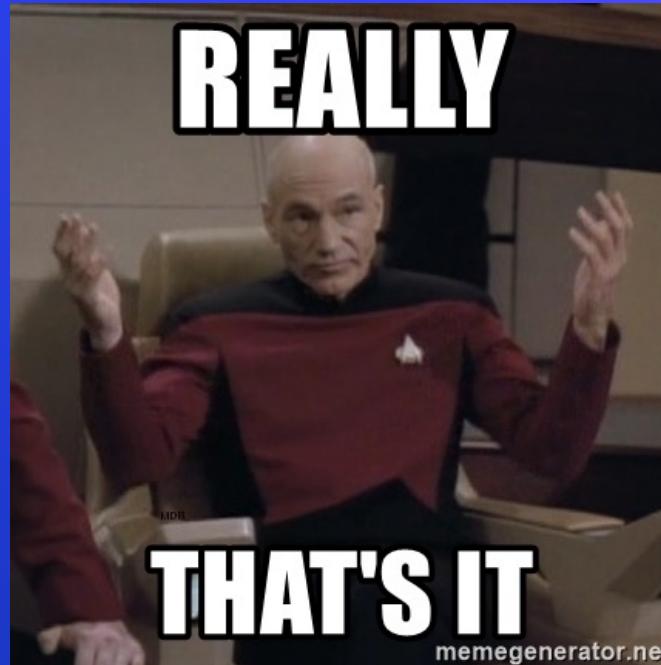
Detect The Bad Guy

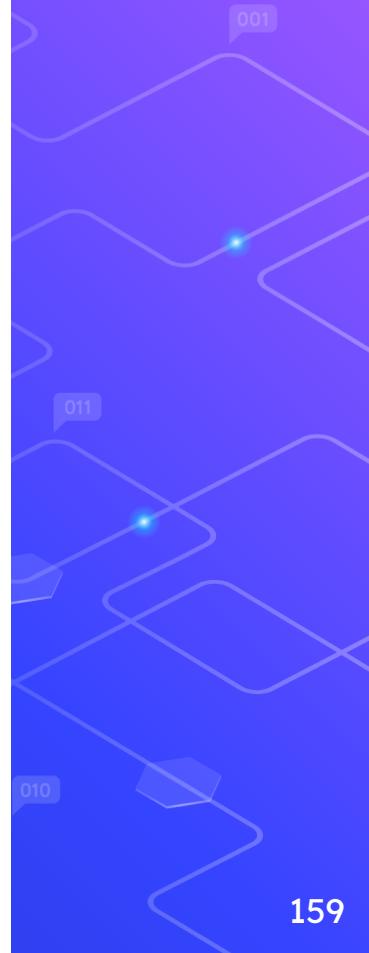
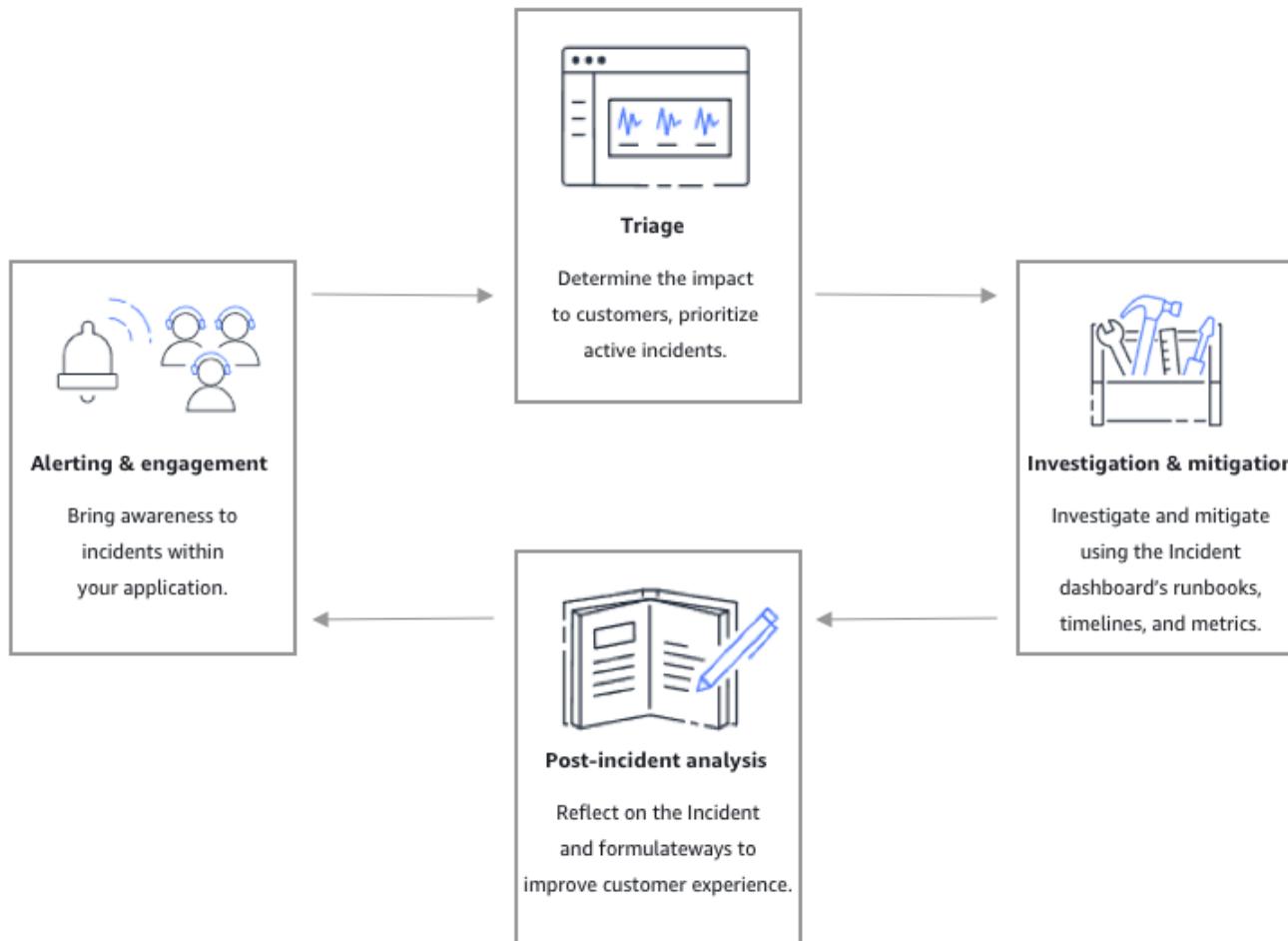
Incident Response on AWS



Don't Forget This Again

Bulut bilişim de aslında normal sunuculardan oluşur.





AWS System Manager Incident Manager

- AWS Systems Manager Incident Manager, kullanıcıların AWS tarafından barındırılan uygulamalarını etkileyen olayları azaltmalarına ve bu olaylardan kurtarmalarına yardımcı olmak için tasarlanmış bir olay yönetimi konsoludur.



Incident Manager

- Response Plans
- Runbook Automation
- Engagement and Escalation
- Active Collaboration
- Incident Tracking



Incident Manager

- AWS Incident Manager, adım adım bir Incident durumuna size hazırlar.

How it works

Respond faster to incidents by preparing an incident response plan. Let us help you create one.



General settings

In general settings you configure which AWS Regions Incident Manager will replicate data to and how the data will be encrypted.

[Set up](#)



Contact details - optional

Define contacts and their contact channels to engage them quickly and efficiently during an incident.

[Create contact](#)



Escalation plans - optional

Escalation plans engage your contacts in timed stages to ensure the correct contacts are reached during an incident at the correct time.

[Create escalation plan](#)



Response plan

Respond quickly and automatically using response plans. Response plans bring together contacts, escalation plans, runbooks, automation, and metrics.

[Create response plan](#)

ThreatResponse Tools

- **AWS_IR** aracı IR süreçlerinizi otomatize etmenize yardımcı olur.
- **Incident Pony**, AWS ortamlarında IR süreçlerini işletmeniz için bir orkestrasyon aracıdır.
- **Margarita Shotgun**, uzaktan EC2 belleklerinin imajını almanıza olanak tanır.



IR - Lab (Isolate EC2 for IR)

- İlgili EC2 makinesini tag'leyin.
- Sunucunun mevcut Security Group'unu kaldırın.
- Outbond ve Inbound trafiği tamamen engelleyen yeni bir SG ekleyin.
- Sunucuya atanmış IAM rolünü kaldırın.
- Instance'in Root diskinin Snapshot'ını alın.

“

CLOSER LOOK

IaC Security

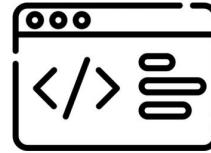


IaC?

- Infrastructure as Code
- Uygulamalarınızı çalıştırmak için kullandığınız tüm alt yapının devamlı farklı nedenlerden ötürü, aynı şekilde, hatasız olarak oluşturulması için yazılan bir deklerasyon veya bir script veya bir kod parçası gibi diyebiliriz.



Templates



Scripts



Policies



ANSIBLE



Terraform



CHEF



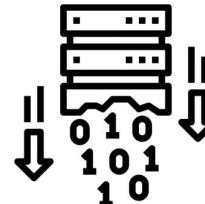
puppet



Network



Application



Storage



Security



Cloud
Infrastructure

“

Don't Trust Copy/Paste



IaC - Open Source Scanners

- Checkov
- Kics
- Trivy
- TFSec

“

CLOSER LOOK

Checkov

“

CLOSER LOOK

Kics

Rising Stars

AWS Security Best Practises



In This Section

- Security Best Practise'lar ve Benchmark'lar bir sistemi güvenli ve sıkılaştırılmış bir hale getirmenin güzel bir yoludur.
- Size izlemeniz gereken yolları listeler.
- Gereksinimleri kurumunuza göre özelleştirmeniz gerekebilir.

CIS AWS Foundations Benchmark

- Center for Internet Security
- Benchmark'ları ücretsizdir ve sizde katkıda bulunabilirsiniz.
- İçerisinde çok sayıda kontrol maddesi bulunur.

PCI DSS

- Payment Card Industry Data Security Standard
- Kart ödemelerinin güvenli bir şekilde yapılması hedeflenir.
- Çok sayıda kontrol maddesi içermektedir.

AWS Foundational Security Best Practices

- AWS tarafından sunulan güvenlik best practise'lerini içerir.
- Identify, Protect, Detect, Respond ve Recover ana kategorilerinde çok sayıda kontrol maddesi içerir.

AWS Well-Architected Framework

- AWS Well-Architected Framework, AWS'de sistemler oluştururken aldığınız kararların artılarını ve eksilerini anlamanıza yardımcı olur. Framework'ü kullanarak, bulutta güvenilir, güvenli, verimli ve uygun maliyetli sistemler tasarlamak ve çalıştırmak için en iyi mimari uygulamaları öğrenebilirsiniz.

CSA CCM

- CSA Cloud Controls Matrix (CCM) bulut bilişim için bir siber güvenlik kontrol çerçevesidir.
- Bulut teknolojisinin tüm önemli yönlerini kapsayan 17 etki alanında yapılandırılmış 197 kontrol hedefinden oluşur.

Which security domains are covered by the CCM?

A&A	Audit and Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization Security
CCC	Change Control and Configuration Management	LOG	Logging and Monitoring
CEK	Cryptography, Encryption and Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency & Accountability
DSP	Data Security and Privacy	TVM	Threat & Vulnerability Management
GRC	Governance, Risk Management and Compliance	UEM	Universal EndPoint Management
HRS	Human Resources Security		

Complete AWS Security Maturity Model

- AWS kaynaklarınızın güvenlik noktasındaki olgunluk seviyesini ölçen modeldir.
- Organizational, Identity and Access, Protection and Prevention, Detection, Response ve Recovery alt başlıklarından oluşur.

	Phase 1: Quick Wins	Phase 2: Foundational	Phase 3: Efficient	Phase 4: Optimized
Organizational	<ul style="list-style-type: none"> Assign Security contacts Select the region(s) 	<ul style="list-style-type: none"> Identify regulatory requirements Identify the most sensitive data - crown jewels Cloud Security Training Plan Involve security teams in development 	<ul style="list-style-type: none"> Security Champions in Development Perform threat modeling 	<ul style="list-style-type: none"> Forming a Red Team (Attacker's Point of View) Forming a Blue Team (Incident Response) Forming a Chaos Engineering team (Resilience) Sharing security work and responsibility
Identity and Access	<ul style="list-style-type: none"> Multi-Factor Authentication Avoid using Root and audit it Access and role analysis with IAM Access Analyzer 	<ul style="list-style-type: none"> Centralized user repository Organization Policies - SCPs 	<ul style="list-style-type: none"> Privilege review (Least Privilege) Tagging strategy Customer IAM: security of your customers 	<ul style="list-style-type: none"> Context-based access control IAM Policy Generation Pipeline
Protection and prevention	<ul style="list-style-type: none"> Limit Security Groups AWS WAF with managed rules Amazon S3 Block Public Access 	<ul style="list-style-type: none"> Manage your instances with Fleet Manager Data Encryption - AWS KMS No secrets in your code - AWS Secrets Manager Network segmentation - Public/Private Networks (VPCs) Multi-account management with AWS Control Tower 	<ul style="list-style-type: none"> Image Generation Pipeline Shield Advanced: Advanced DDoS Mitigation Anti-Malware/EDR Encryption in transit WAF with custom rules Outbound Traffic Control Create your reports for compliance (such as PCI-DSS) 	<ul style="list-style-type: none"> Process standardization with Service Catalog DevSecOps
Detection	<ul style="list-style-type: none"> Threat Detection with Amazon GuardDuty and review your findings Audit API calls with AWS CloudTrail Analyze data security posture with Amazon Macie Remediate security findings found by AWS Trusted Advisor Automate alignment with best practices using AWS Security Hub Billing alarms for anomaly detection 	<ul style="list-style-type: none"> Configuration monitoring with AWS Config Manage vulnerabilities in your Infrastructure and perform pentesting Manage vulnerabilities in your applications Discover sensitive data with Amazon Macie 	<ul style="list-style-type: none"> Use abstract services Integration with SIEM/SOAR Network Flows analysis (VPC Flow Logs) 	<ul style="list-style-type: none"> Simulate failures (Chaos Monkey) Amazon Fraud Detector Integration with additional intelligence feeds
Response	<ul style="list-style-type: none"> Act on Amazon GuardDuty findings 	<ul style="list-style-type: none"> Define Incident response playbooks - TableTop Exercises Investigate ALL Amazon GuardDuty findings including S3 Protection 	<ul style="list-style-type: none"> Automate critical and most frequently run Playbooks Automate deviation correction in configurations 	<ul style="list-style-type: none"> Automate most playbooks Amazon Detective: Root cause analysis
Recovery		<ul style="list-style-type: none"> Backups Redundancy using multiple Availability Zones 	<ul style="list-style-type: none"> Using infrastructure as code (CloudFormation, CDK) 	<ul style="list-style-type: none"> Multi-region disaster recovery automation

Automation

- AWS Config
- Prowler
- Nessus
- Qualys
- CloudSploit
- CloudMapper
- ScoutSuite



“

CLOSER LOOK

CloudMapper

“

CLOSER LOOK

ScoutSuite