Cloud Forensics Fundamentals

Hacktrick, 2022

Sena YAKUT, PurpleBox

PurpleBox

Sena YAKUT

Senior Cloud Security Engineer

sena-yakut

senayktt

Genel Bakış

- **Cloud Computing Nedir?**
- **Cloud Forensics Nedir?**
- **Cloud vs. Digital Forensics**
  - Bulut Mimarisi Türleri
  - Bulut Türleri
- **Cloud Forensics Adımları**
  - Tanımlama (Identification)
  - Koruma ve Toplama (Preservation and Collection)
  - Tespit Etme (Detection)
  - Analiz (Analysis)
- **Cloud Forensics Zorlukları**
- **AWS'te Cloud Forensics**

Cloud Computing Nedir?

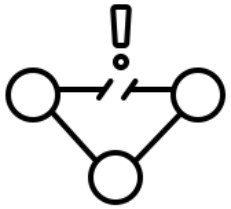
Bulut Bilişim:

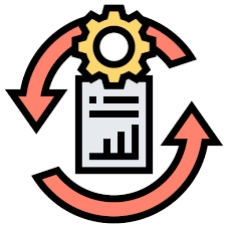
- Geleceğin teknolojisi → birçok organizasyonun stratejisinin, operasyonlarının ve altyapısının ayrılmaz bir bileşeni.
- Özel ve kamu sektörü kuruluşları,
  - ✓Maliyetleri azaltmak,
  - ✓Veri yönetimini iyileştirmek
  - ✓İletişim ve işbirliğini geliştirmek.

Cloud Computing Nedir?

Avantajlar:

- Yüksek kullanılabilirlik (High Availability)
- Ölçeklenebilirlik, esneklik ve çeviklik
- Hata Toleransı (Fault Tolerance)
- Olağanüstü durum kurtarma (Disaster Recovery)
- Maliyet optimizasyonu





Cloud Computing Nedir?

Dezavantajlar / Zorluklar:

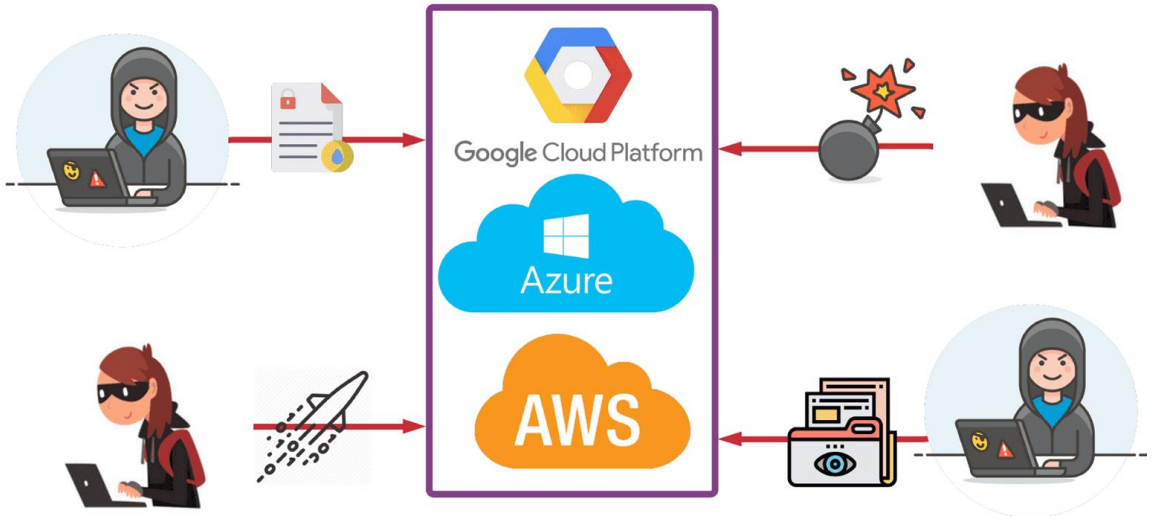
- Regülasyonlar
- Sınırlı kontrol
- **Güvenlik ve Gizlilik**
- **Atak Yüzeyi Fazlalığı**
- İş gücü eksikliği

GDPR

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Cloud vs. Digital Forensics

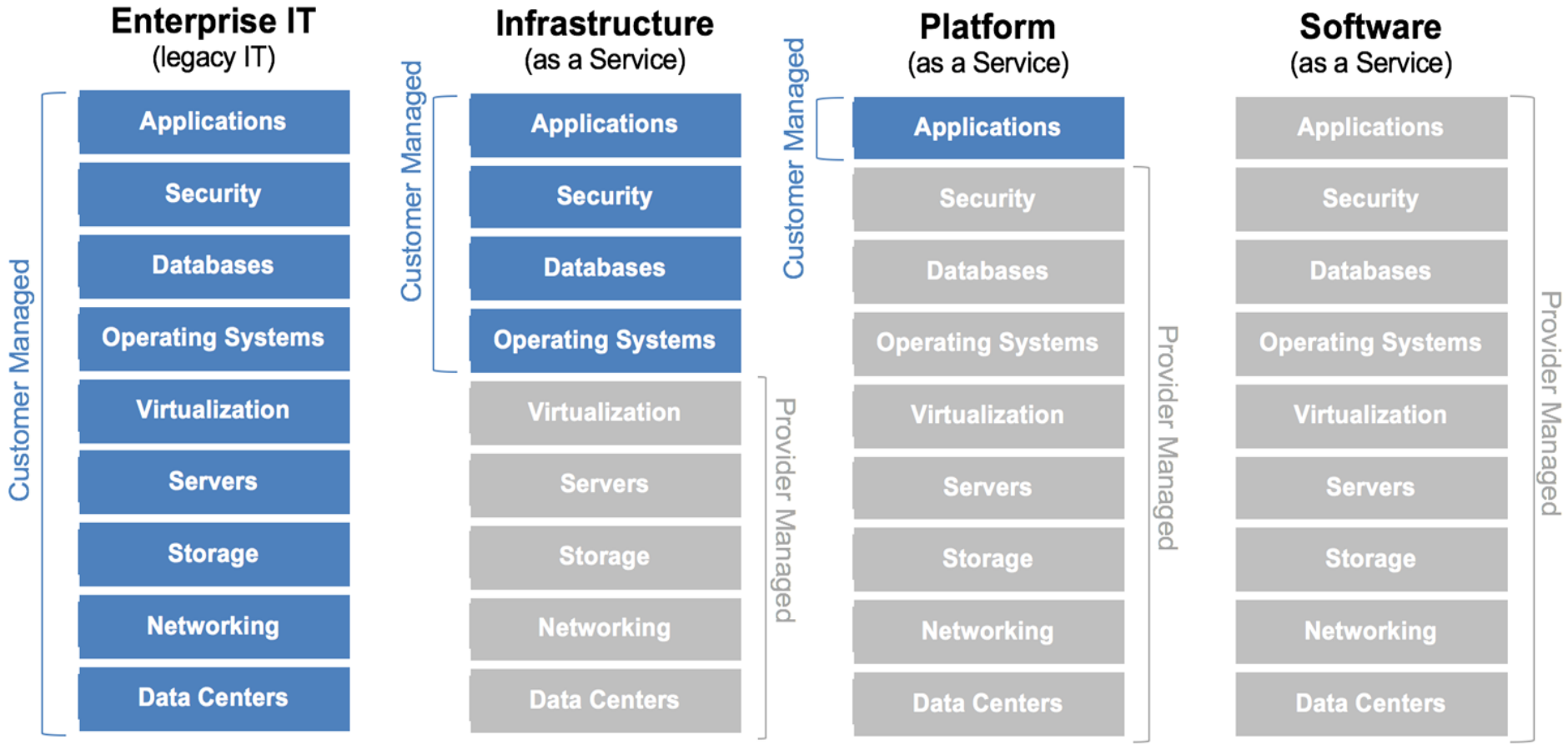
- Bulut bilişim→ saldırganlar için yeni bir saldırı alanı.
- Bu vakaları araştırmak için **bulut adli bilişim (Cloud Forensics)**
- **Cloud Forensics → Daha karmaşık**
  - Veriler üçüncü tarafa ait bir sunucuda?
  - Bulut işlemi sağlayıcıları (Cloud Providers)
    - AWS
    - Google
    - Azure



"Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics to gather and preserve evidence in a way that is suitable for presentation in a court of law."

Cloud vs. Digital Forensics

Bulut Mimarisi Türleri



Cloud vs. Digital Forensics

Bulut Mimarisi Türleri

- IaaS
- PaaS
- SaaS

Amazon EC2

Google Compute Engine

DigitalOcean

Elastic Beanstalk

App Engine

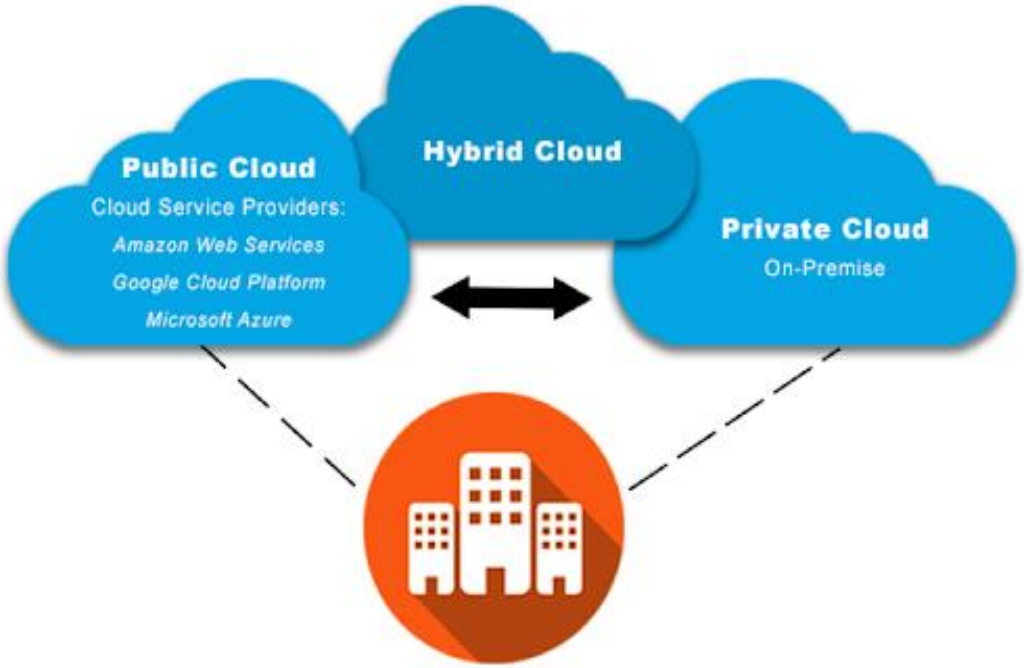
OPENSHIFT

Dropbox

HubSpot

Cloud vs. Digital Forensics

Bulut Türleri



Cloud Forensics Adımları

Tanımlama (Identification):

Faaliyetleri tanımlama aşaması:

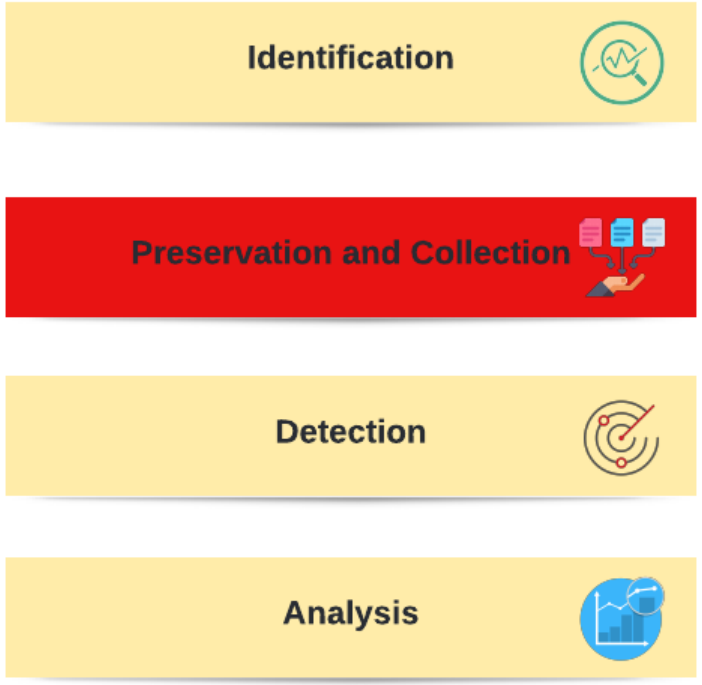
- Bir kişi tarafından yapılan bir şikayet,
- IDS tarafından tespit edilen anormallikler,
- Bir denetim izi nedeniyle izleme ve profil oluşturma,
- Bir buluttaki şüpheli olaylar.

Cloud Forensics Adımları

Koruma ve Toplama (Preservation and Collection):

Hukuki ve adli standartlara uygun olarak, bütün kaynaktan, bütünlüğüne zarar vermeden veri toplama aşaması:

- Büyük veri depolama alanlarına ihtiyaç,
- Veri koruma ve gizlilik sorunları,
- Bulutta depolanan kanıtlar üzerindeki etkilerine ilişkin kural ve düzenlemeler.



Cloud Forensics Adımları

Tespit Etme (Detection):

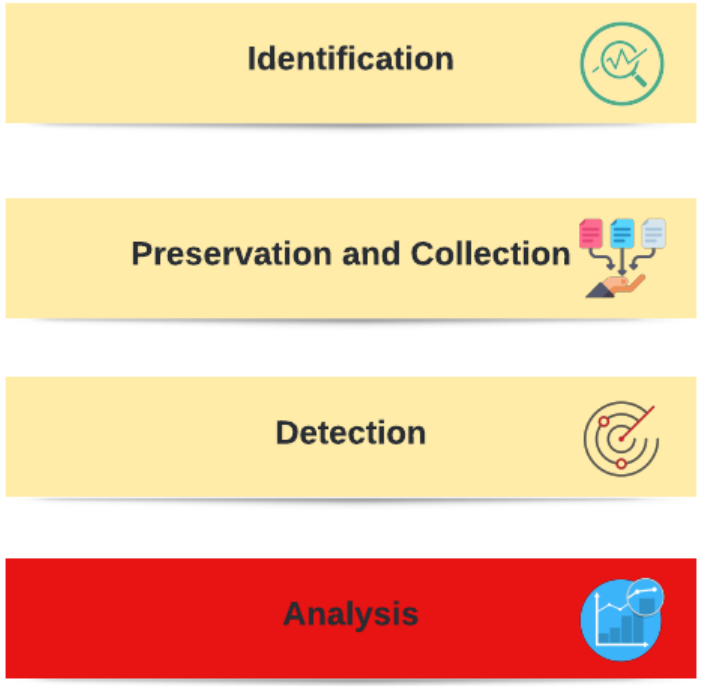
Birden fazla yol ve algoritma kullanarak (Filtering, Pattern Matching) şüpheli etkinliği veya kötü amaçlı kodu tespit etme aşaması.

Cloud Forensics Adımları

Analiz (Analysis):

Analiz etme aşaması:

- Araştırma,
- Kanıt bulmak için sorular sorma,
- Raporlama.



Cloud Forensics Zorlukları

- **Mimari:** Çeşitlilik, karmaşıklık, kaynak, çoklu kiracılık ve veri ayrımı ile ilgilenme.
- **Veri toplama:** Veri bütünlüğü, veri kurtarma, veri konumu ve görüntüleme adresleme.
- **Analiz:** Korelasyon, yeniden yapılandırma, zaman senkronizasyonu, günlükler, meta veriler ve zaman çizelgesi sorunlarının belirlenmesi.
- **Anti-adli:** Adli analizleri önlemek veya yanlış yönlendirmek için tasarlanmış şaşırtma, veri gizleme ve kötü amaçlı yazılımlar.

Cloud Forensics Zorlukları

- **Olaya ilk müdahale eden kişiler:** Bulut sağlayıcılarının güvenilirliğini, yanıt süresini ve yeniden yapılandırmayı doğrulama.
- **Rol yönetimi:** Veri sahiplerine hitap etme, kimlik yönetimi, kullanıcılar ve erişim kontrolleri.
- **Hukuki:** Yargı bölgelerine, yasalara, hizmet düzeyi anlaşmalarına, sözleşmeler.
- **Standartlar:** Standart işletim prosedürlerini, birlikte çalışabilirliği, test etme ve doğrulama.
- **Eğitim:** Adli müfettişlerin ve bulut sağlayıcılarının yeterli bilgiye sahip olmasını sağlamak.

AWS’te Cloud Forensics

- **Amazon Web Services (AWS),** lider ve en yaygın kullanılan bulut platformu,
- Dünya çapındaki veri merkezlerinden 200'ün üzerinde servis,
- En hızlı büyüyen startup'lar, en büyük kuruluşlar ve önde gelen devlet kurumlarının dahil olduğu milyonlarca müşteri.

AWS'te Cloud Forensics

- AWS, müşterilere karmaşık, kurumsal ölçekli AWS ortamlarında cloud forensics konusunda yardımcı olacak çeşitli araçlar sağlar.
- Bu araçları ve servisleri kullanmak ve yönetimi bizim sorumluluğumuzda!

AWS CloudTrail

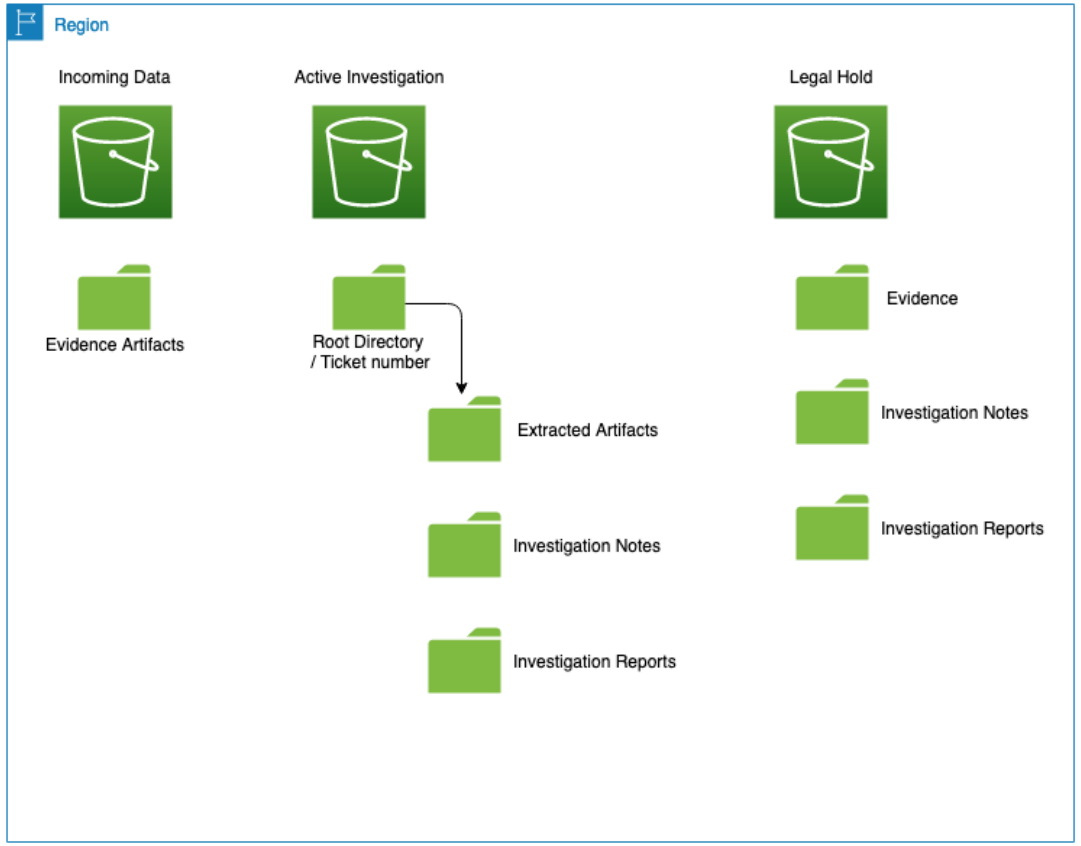
AWS Config

Amazon GuardDuty

VPC Flow Logs

PurpleBox

AWS’te Cloud Forensics

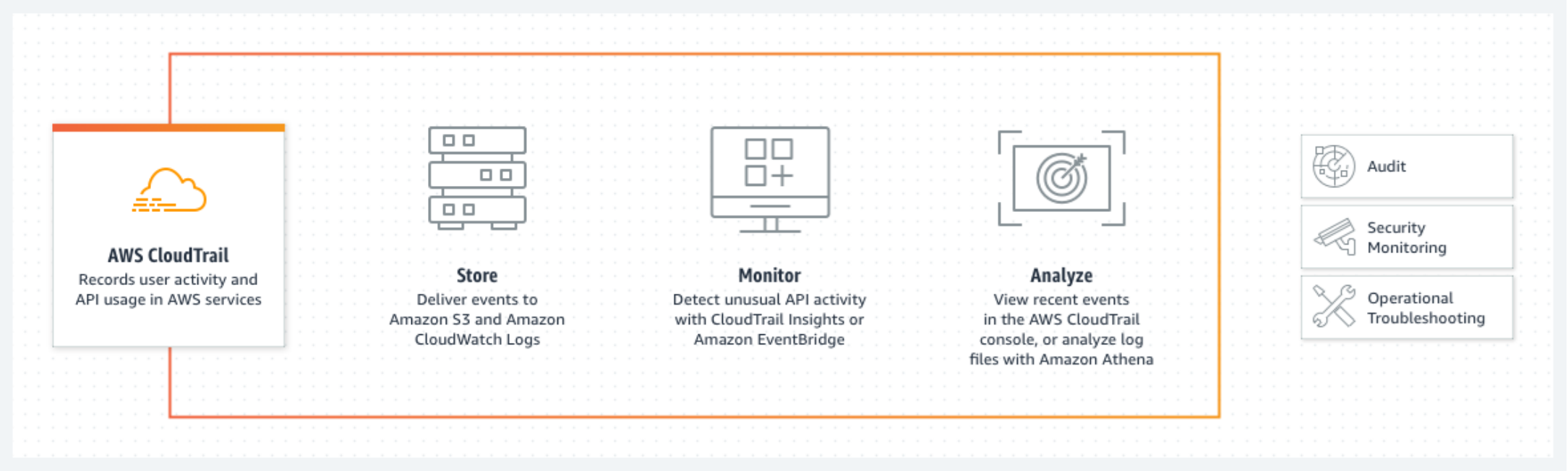


AWS'te Cloud Forensics

AWS CloudTrail:

AWS CloudTrail

- Hesap etkinliğini izleyip kaydederek depolama, analiz ve düzeltme eylemleri,
- **"Who to blame?"**



PurpleBox

AWS’te Cloud Forensics

AWS CloudTrail:

Filter: Select attribute | Enter lookup value | Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2016-08-31, 12:01:55 AM	skeddly-91617669819b49b…	CreateTags		snap-073936e644d3c0c22
2016-08-31, 12:01:55 AM	skeddly-91617669819b49b…	CreateTags		snap-0f94c0668d6367137
2016-08-31, 12:01:43 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Volume and 1 more	vol-0bc4a5a21549590d5 a…
2016-08-31, 12:01:41 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-0c05588186ff04bfe a…
2016-08-31, 12:01:41 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-06731e20f5eeabd83 …
2016-08-31, 12:01:40 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-05c0663fc1942d5af a…
2016-08-31, 12:01:39 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-02210794c53ad5d34 …
2016-08-31, 12:01:38 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-092ba9daa0e61287b…
2016-08-31, 12:01:22 AM	skeddly-271ecadd5ab6425…	CreateTags		vol-05047478457ee4707
2016-08-31, 12:01:19 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Volume and 1 more	vol-559aafba and 1 more
2016-08-31, 12:01:18 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Volume and 1 more	vol-d9cdc3c2 and 1 more
2016-08-31, 12:01:17 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Snapshot and 1 more	snap-0e2a04d2173ae1fa4 …
2016-08-31, 12:01:16 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Volume and 1 more	vol-58a43340 and 1 more
2016-08-31, 12:01:16 AM	skeddly-91617669819b49b…	CreateSnapshot	EC2 Volume and 1 more	vol-0f3dfe0b0b6ad3029 an…

AWS'te Cloud Forensics

AWS CloudTrail:

AWS CloudTrail

Filter: Resource type | Enter resource type | Date range: Select date range

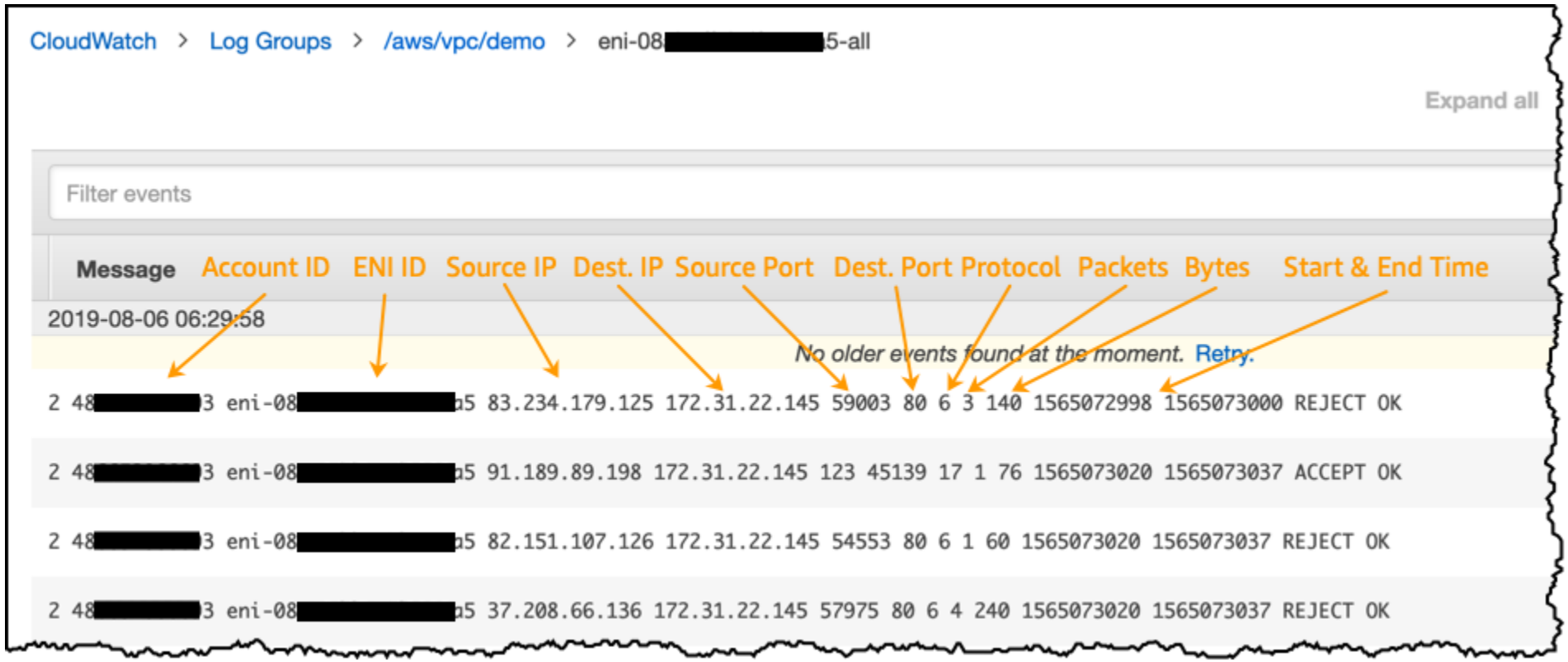
Event time	User name	Event name	Resource type	Resource name
2015-03-04, 10:54:42 AM	John	StopInstances	Instance	i-8891d772
2015-03-04, 10:53:18 AM	John	ConsoleLogin		
2015-03-04, 10:51:59 AM	JeffBarr	CreateLoginProfile	User	John
2015-03-04, 10:51:29 AM	JeffBarr	CreateUser	User	[redacted]
2015-03-04, 10:50:59 AM	JeffBarr	ConsoleLogin		
2015-03-04, 10:47:55 AM	JohnDoe	ConsoleLogin		
2015-03-04, 10:45:08 AM	JeffBarr	CreateLoginProfile	User	JohnDoe
2015-03-04, 10:44:48 AM	JeffBarr	AddUserToGroup	Group and 1 more	admins and 1 more
2015-03-04, 10:44:34 AM	JeffBarr	CreateUser	User	[redacted]
2015-03-04, 10:43:59 AM	Sivakanth	RunInstances	SecurityGroup and 6 more	sg-e6fd7182 and 7 more
2015-03-04, 10:43:58 AM	Sivakanth	CreateSecurityGroup	SecurityGroup and 1 more	sg-e6fd7182 and 2 more
2015-03-04, 10:43:58 AM	Sivakanth	AuthorizeSecurityGroupIngress	SecurityGroup	sg-e6fd7182
2015-03-04, 10:16:14 AM	jaymul	UpdateTrail	Bucket and 1 more	cloudtrail-2014-launches and ...

AWS'te Cloud Forensics

AWS VPC Flow Logs:

VPC Flow Logs

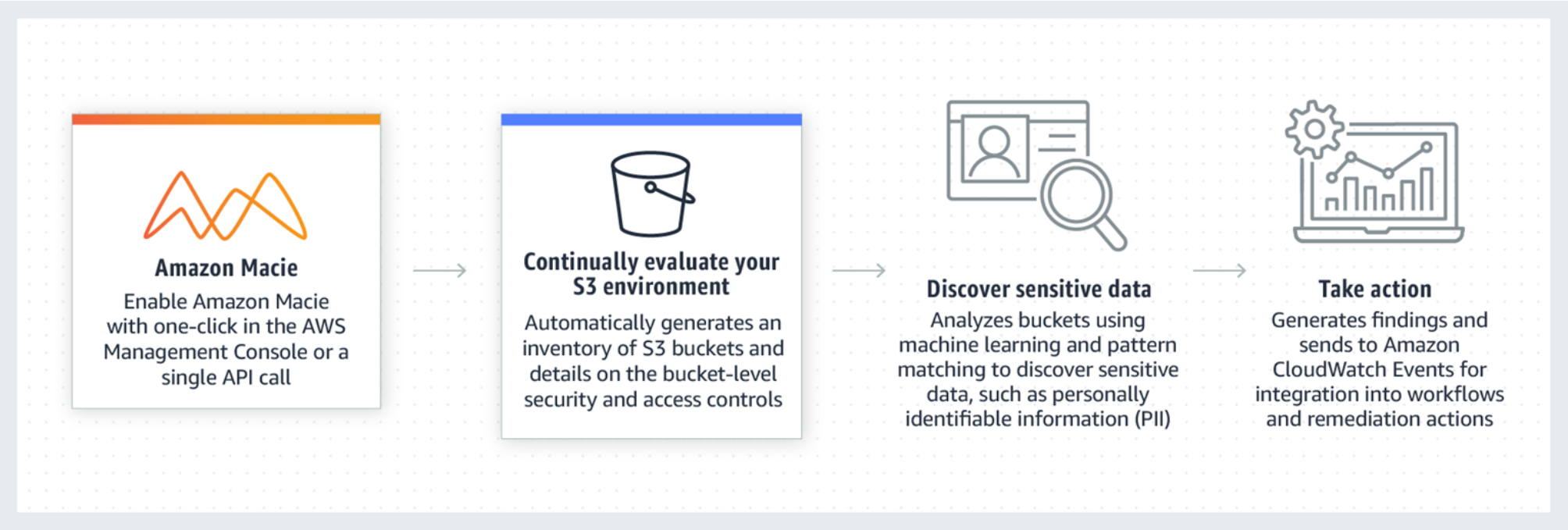
- VPC'deki ağ arayüzlerine gelen ve giden IP trafiği hakkında loglama.



AWS'te Cloud Forensics

AWS Macie:

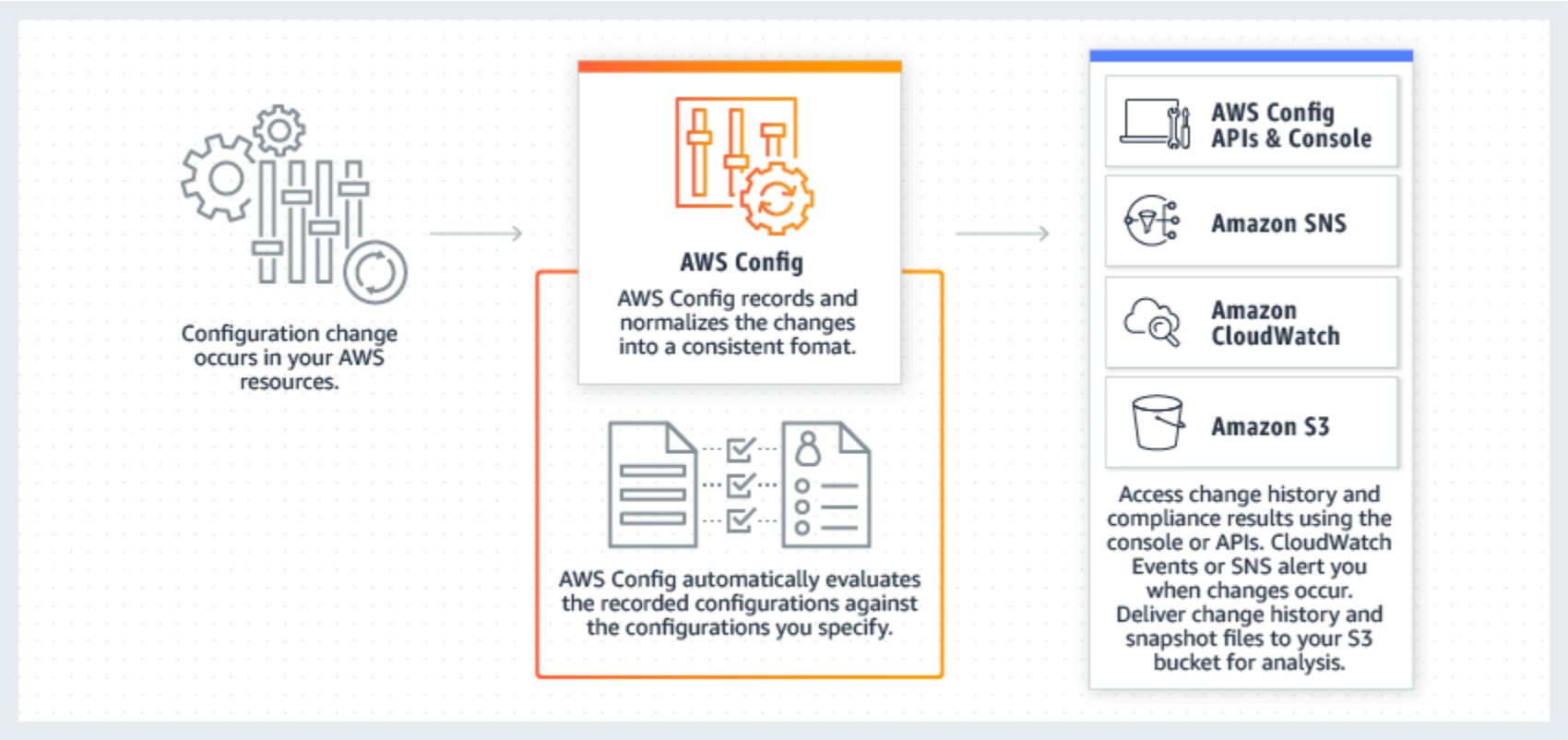
- S3 servisinde depolanan hassas verileri otomatik olarak keşfedip sınıflandırarak veri kaybını önleyen AWS servisi.



AWS'te Cloud Forensics

AWS Config:

- AWS kaynak yapılandırmalarını sürekli olarak izleyen, kaydeden ve beklenmedik bir yapılandırma olduğunda alarm ya da bildirim sistemlerinin entegre edilebildiği AWS servisi.

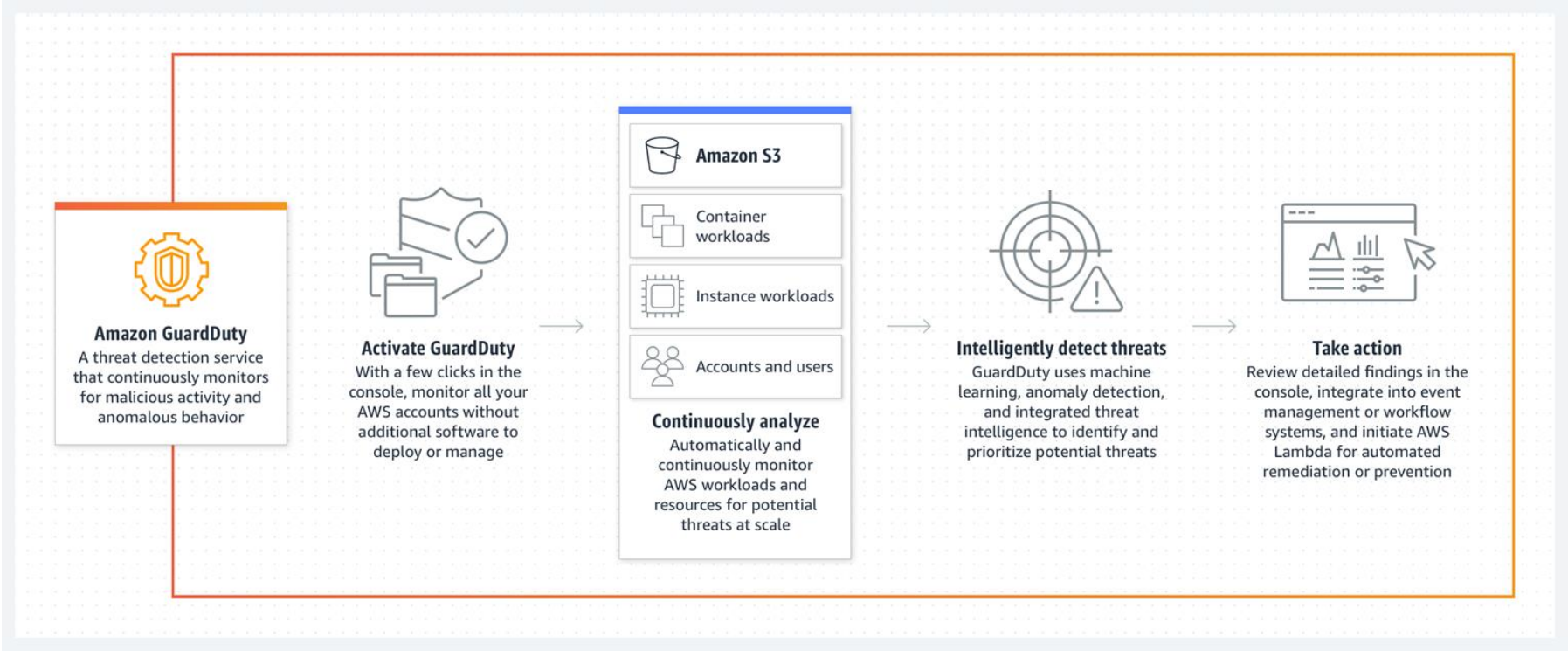


AWS’te Cloud Forensics

AWS GuardDuty:

Amazon GuardDuty

- AWS hesaplarınızı korumak için kötü amaçlı etkinlikleri veya anormal davranışları sürekli olarak izleyen bir tehdit algılama hizmeti.



Sorular?