M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

Yazılım ve Kariyer Fırsatları (Siber Güvenlik)

Mustafa DAYIOĞLU
Siber Güvenlik Uzmanı
Mimar ve Mühendisler Grubu Yönetim Kurulu Üyesi

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

- Siber Uzay
- Teknolojik Trendler
- Siber Güvenlik ve Kariyer
- Mülakatlar

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

SİBER UZAY

Siber Uzay Nedir ?

Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam

Siber Uzay Örnekler .....

- Ekonomik Faaliyetlerin İnternete Bağımlılığı
  - E-Ticaret, Borsa, Finans, Bankacılık

- Devletin Bilgi Sistemlerine Bağımlılığı
  - E-Devlet, Evrak ve İş Akış Sistemleri, Mesajlaşma

- Kritik Altyapılarının Bilgi Sistemlerine Bağımlılığı
  - Enerji, Su, Ulaşım, İletişim Altyapıları

- Toplumun İnternete Bağımlılığı
  - Sosyal Medya (Twitter, Facebook vb.), Google vb.

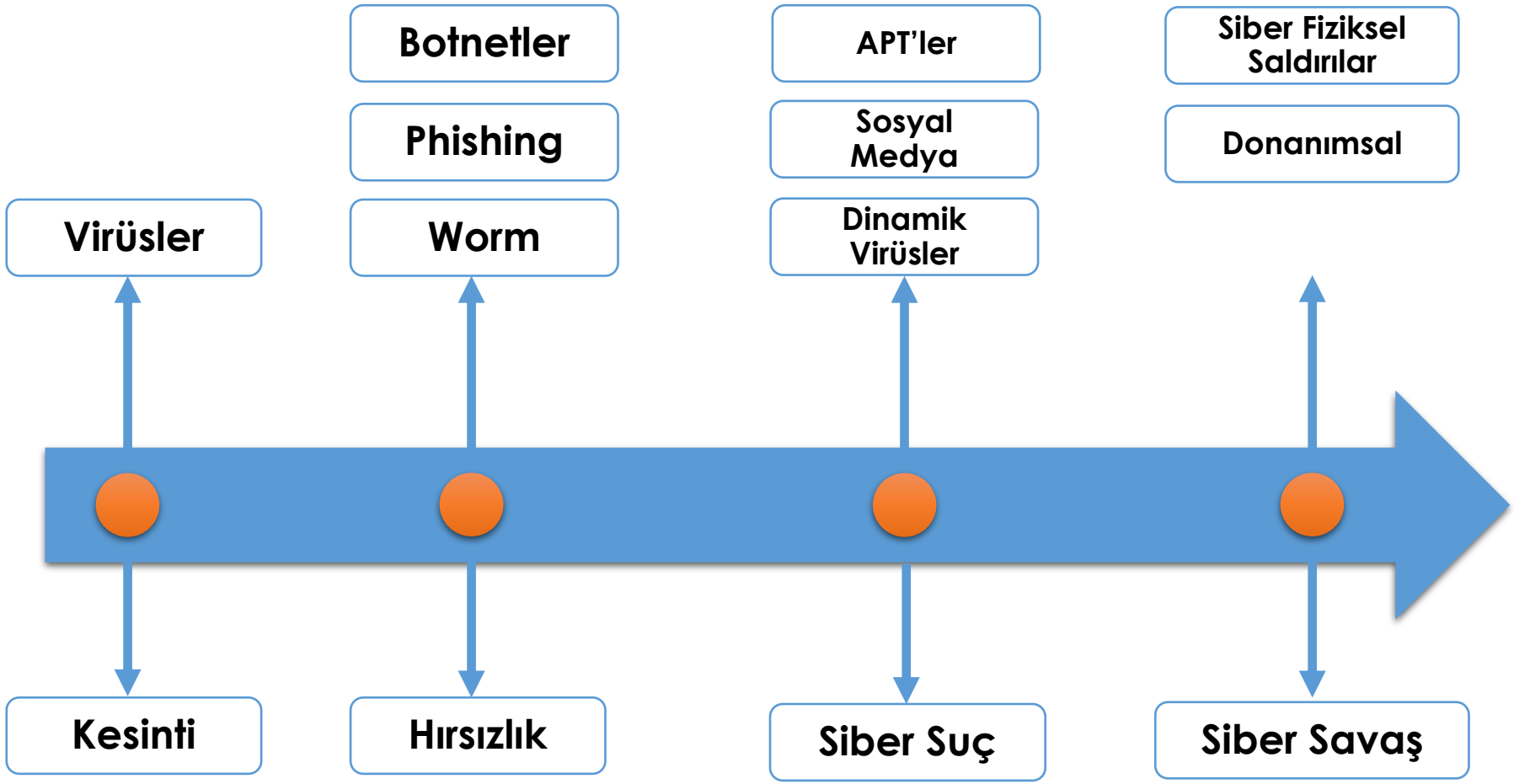
Siber Güvenlikte Amaç Nedir ?

"Yazılı ve elektronik ortamdaki kurumsal bilgiyi korumak"

- Gizli (yetkisiz kullanıcılar görmesin!)
- Bütün (bilgi bozulmasın! başkası tarafından değiştirilmesin!)
- Erişilebilir (yetkili kullanıcılar ihtiyaç duydukları an görebilsin!)

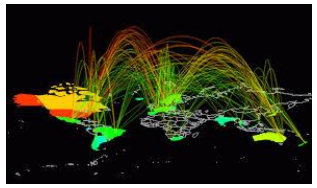
Ya da, kurum olağan işleyişini gerçekleştiremez ve itibar kaybeder.

Siber Saldırıların Evrimi



Neden Siber Güvenlikçiye İhtiyaç Duyuluyor ….

- Kontrol Edilemeyen Bilgi Akışı ve İnternet Trafiği Analiz Eksikliği



- Milli Ürün ve Çözümlerin Yetersizliği

- Güvenlik Önlemleri Eksik Tasarlanmış Uygulamalar
- İşletim Sistemleri ve Mobil Platformlar Üzerindeki Açıklıklar
  - Linux, Windows, Android, IOS vb.

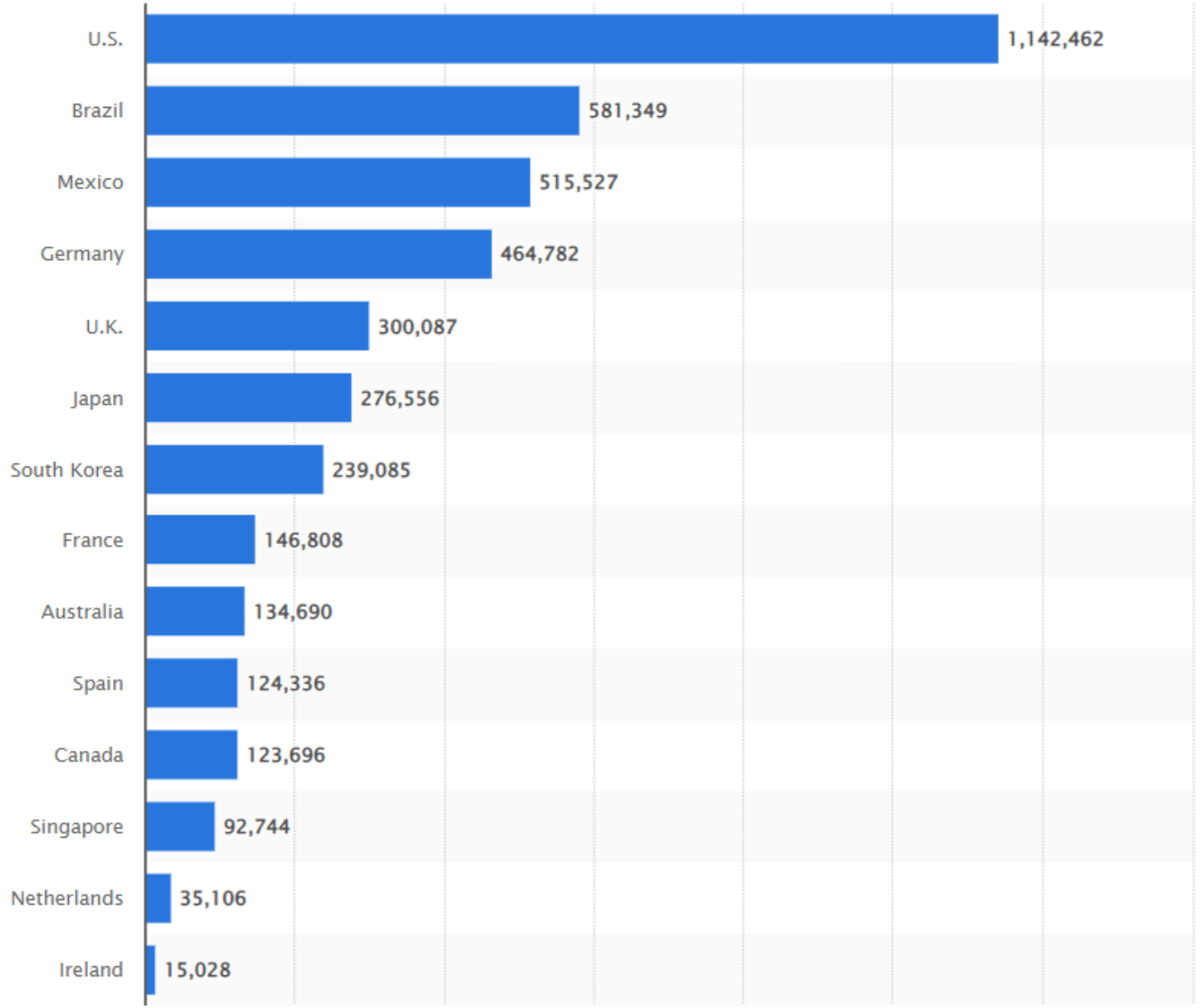


- Mobil Uygulamalar Üzerindeki Açıklıklar
  - Google Play, Appstore vb.

- Web Teknolojileri Üzerindeki Açıklıklar
  - Web Tarayıcıları, JAVA, .NET, PHP vb.

- Zararlı Yazılımların Tespit Edilememesi

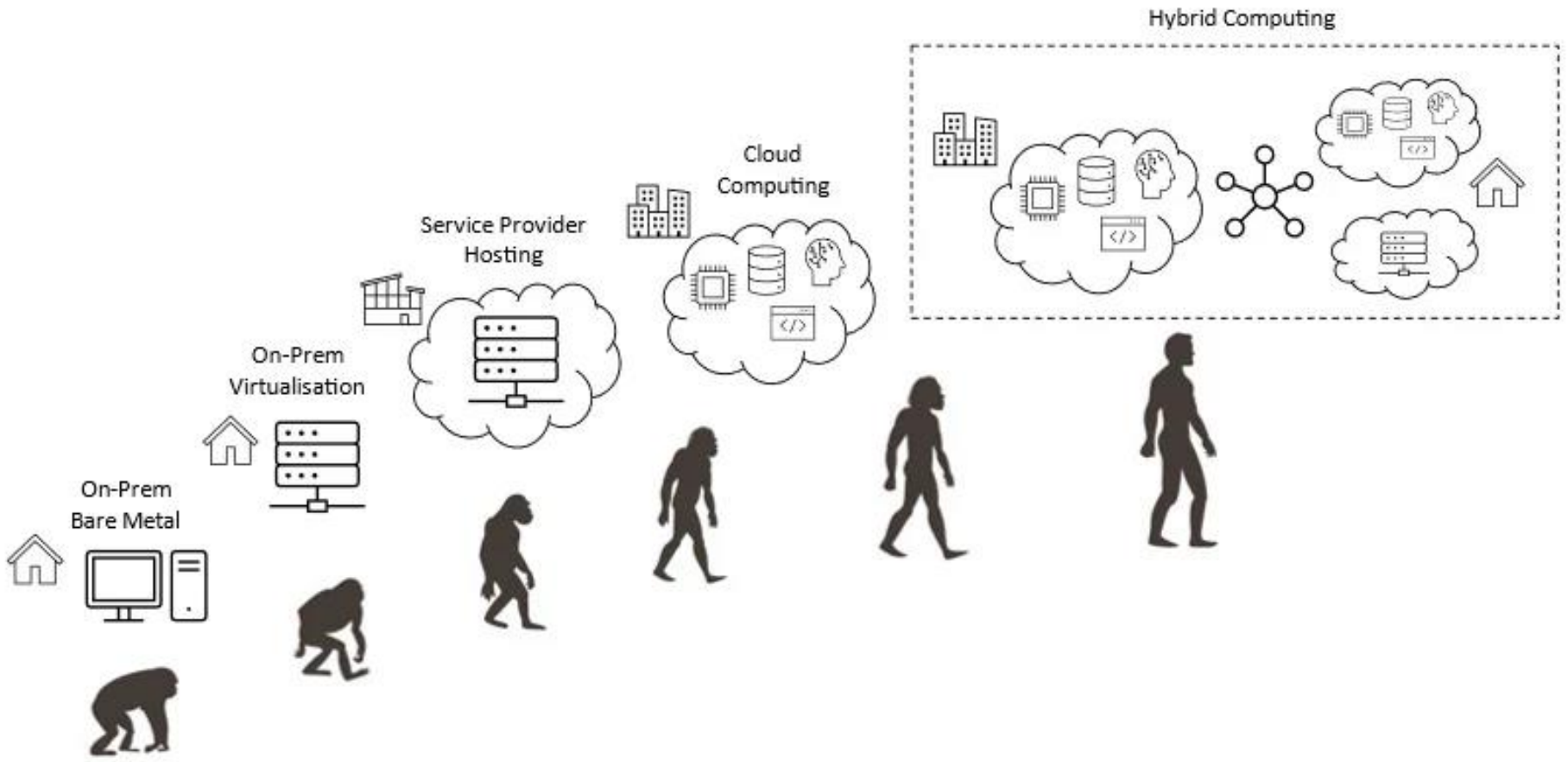
Dünyada Siber Güvenlik İstihdamı....



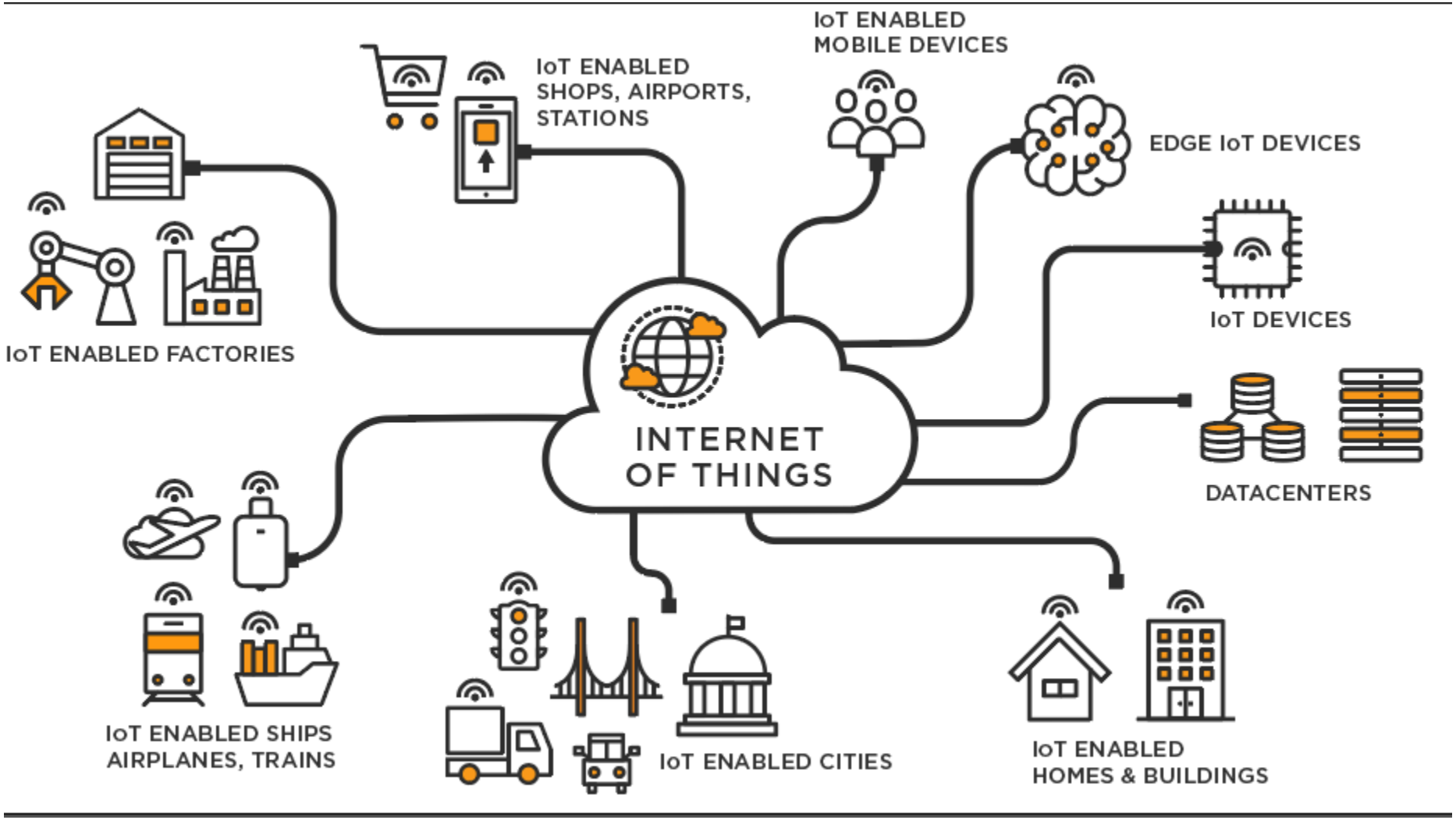
M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

TEKNOLOJİK TRENDLER VE PARADİGMA DEĞİŞİMİ

Bulut Bilişim ….



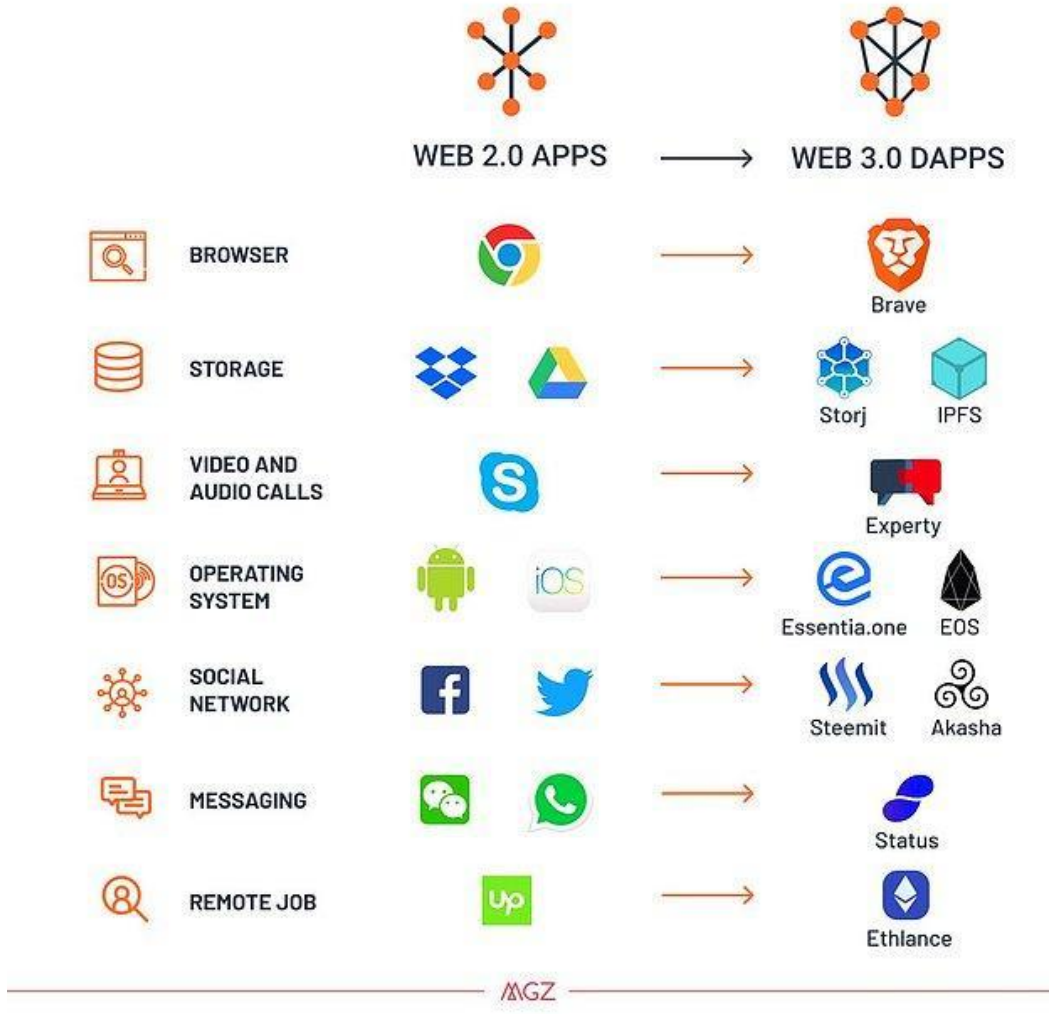
Nesnelerin İnterneti ….



Web 3.0 ….


Yahoo!
Google
msn
Web 1.0
"Read Only",
Decentralized
aws
Uber
Web 2.0
Participatory,
Centralized
IPFS
sia
Web 3
No Intermediaries,
Decentralized

Web 3.0 ….


WEB 2.0 APPS
WEB 3.0 DAPPS
BROWSER
Brave
STORAGE
Storj
IPFS
VIDEO AND AUDIO CALLS
Experty
OPERATING SYSTEM
iOS
Essentia.one
EOS
SOCIAL NETWORK
Steemit
Akasha
MESSAGING
Status
REMOTE JOB
Ethlance
MGZ

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

SİBER GÜVENLİK VE KARİYER

Olmazsa olmazı….

Ön koşullar ….

1. Lisans Mezunu Olmak

2. Yabancı Dil (İngilizce)

3. Sertifikasyonlar

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

GELENEKSEL İŞ TANIMLARI

Önce Çıkan İş İlanları

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improve their security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard - testing applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Better catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. You implement active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your IT and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

You implement and tune firewalls, IPS/IDS, patching, admin rights, monitoring, application white listing, more.

More Advanced Jobs – Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting, "The system's dead!," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are creative and on top of the game both technically and in business; You design and build defensible systems and are part of an adept team.

8 SECURE SOFTWARE DEVELOPMENT MANAGER

"Coolest software developers"

You protect the development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST / REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

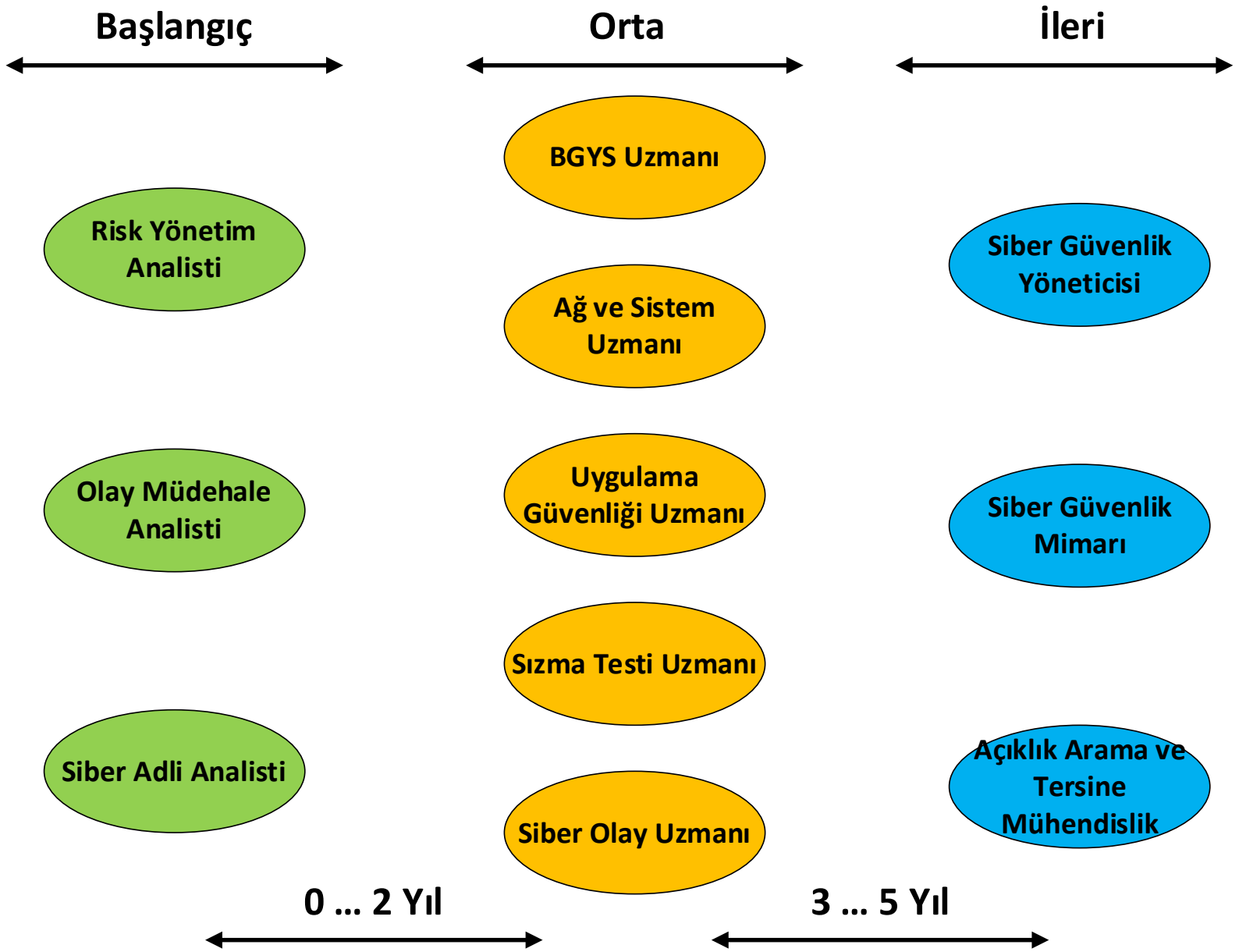
You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it is trying to do or has done.

10 TECHNICAL DIRECTOR /CISO

"Making decisions; making things happen. That's coolness."

You are at the top of the tech ladder. A strategic thinker, you're hands on the design and deployment of solutions. You hold the keys to tech infrastructure.

Kariyer Yol Haritası ….



Temel Seviye ….

Python ve Javascript

Web Sunucular ve Veritabanları
(IIS, Apache, Postgresql, Mysql)

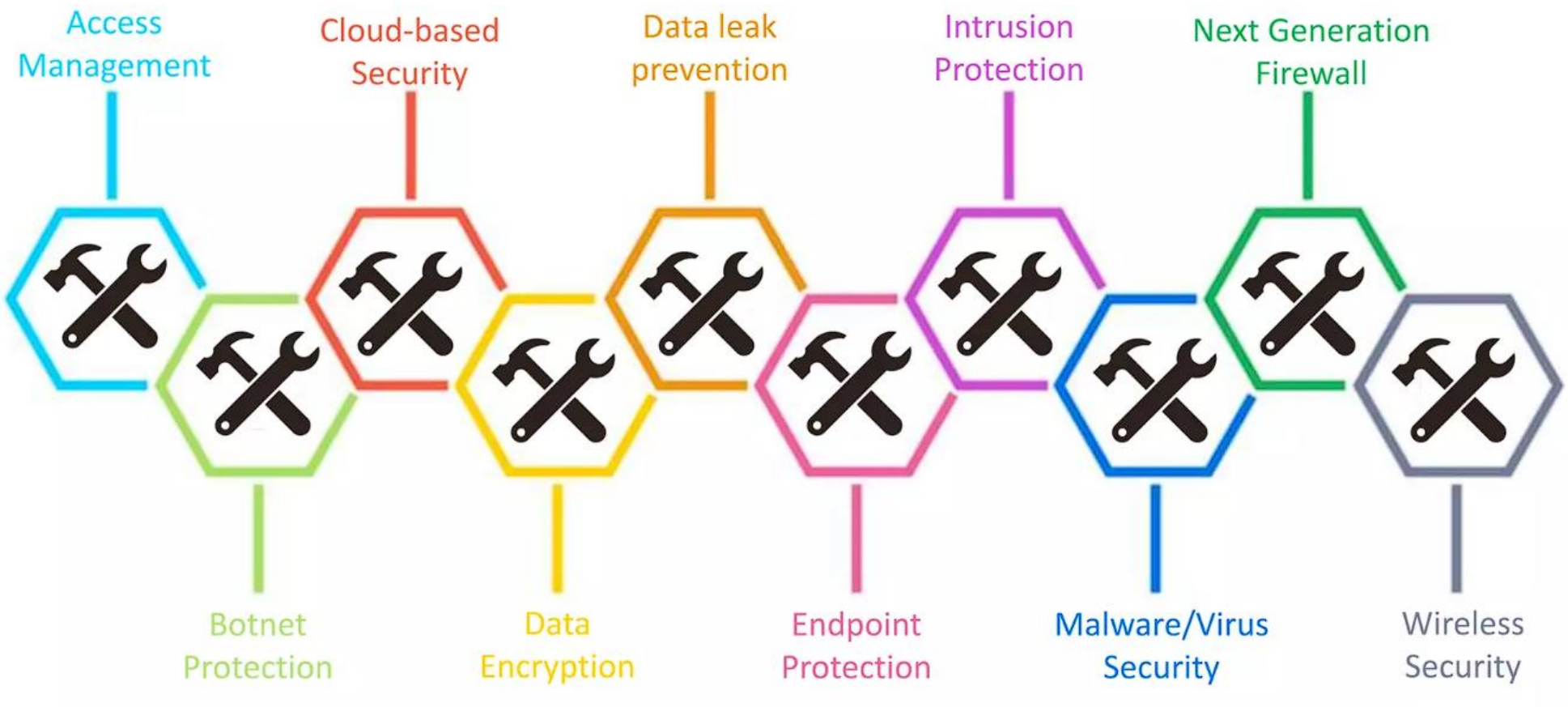
Ağ Protokolleri ve Teknolojileri
(TCP/IP, routing ,namespace, iptables, Suricata)

Betik Programlama
(Bash, Powershell)

İşletim Sistemleri ve Komutları
(Linux ve Windows)

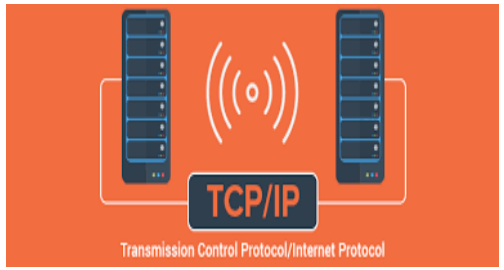
Temel Siber Güvenlik Kavramları

Anahtar Kavramlar ….



M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

Anahtar Yetkinlikler ....



Linux

OpenLDAP

Active Directory

BASH
THE BOURNE-AGAIN SHELL

PowerShell

APACHE

Microsoft IIS

OAuth 2.0

python

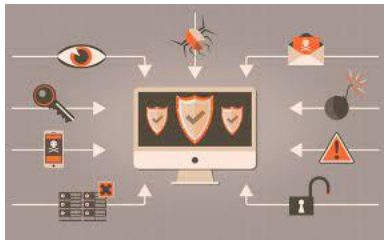
{JavaScript}

docker

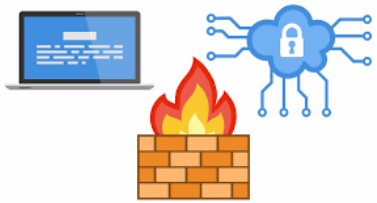
Siber Savunma - Anahtar Teknolojiler ….

Şifreleme Teknolojileri

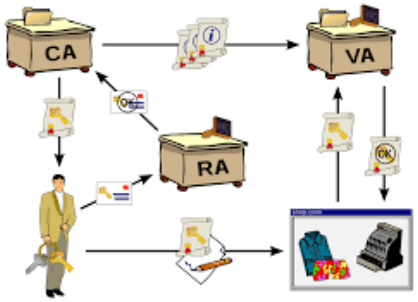
Açıklık Tarama Araçları



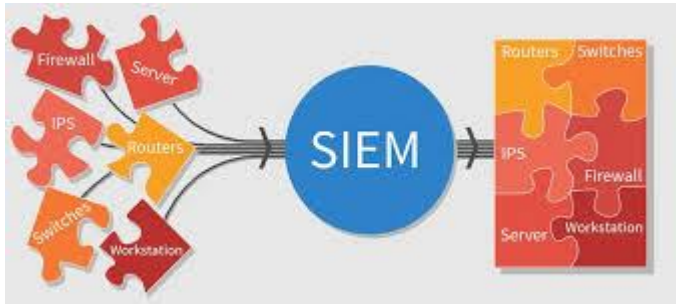
Yeni Nesil Antivirüsler



Yeni Nesil Güvenlik Duvarları



Açık Anahtar Altyapısı



SIEM

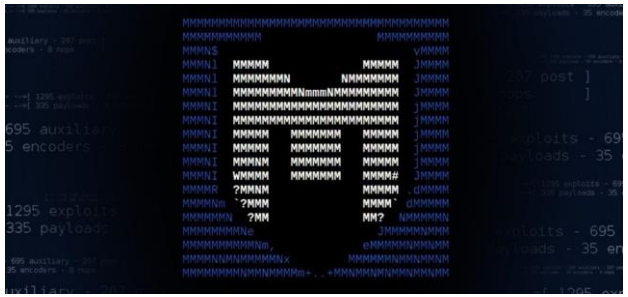
Veri Kaçağı Önleme Sistemleri

Siber Saldırı - Anahtar Araçlar….

NMAP PROJECT

HASHCAT

Advanced Password Recovery Utility
on Linux



acunetix
WEB APPLICATION SECURITY

AIRCRACK-NG

WIRESHARK

Ettercap

BURPSUITE

MALTEGO

SOC Uzmanlığı....

Siber Olaylara Müdehale

Siber Tehdit İstihbaratı - OSINT

SIEM

Kayıt Analizi ve Yönetimi

Risk Analizi ve Yönetimi

TEMEL YETENEKLER

Siber Güvenlik Sistem Yöneticiliği....

Uygulama ve Veri Güvenliği

Kimlik ve Erişim Yönetimi

Ağ ve Kullanıcı Güvenliği Sistemleri

Linux ve Microsoft Sistemleri Güvenliği

Risk Analizi ve Yönetimi

TEMEL YETENEKLER

Siber Güvenlik Sızma Testi Uzmanı....

Açıklık Kodlarını Düzenleyebilme

Web Temelli Saldırılar

Yetki Yükseltme Saldırıları

Aktif ve Pasif Bilgi Edinme

Mitre Attack Framework

TEMEL YETENEKLER

Zararlı Yazılım Analizi Uzmanı ....

Statik ve Dinamik Analiz Teknikleri

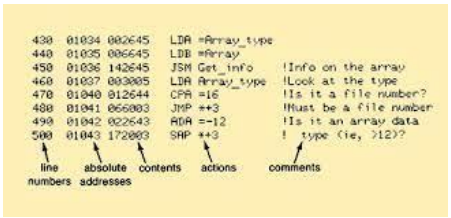
Zararlı Yazılım Analiz Platformları

Tersine Mühendislik Araçları ve Uygulamaları

Bellek, Process ve I/O Analizi

Assembler ve C/C++

TEMEL YETENEKLER



Adli Analiz Uzmanı ....

Ağ Trafik Analizi

Bellek Analizi

Mobil Cihaz ve Uygulama Analizi

Sabit Disk Analizi (Windows ve Linux)

Veri Çıkartma / Kurtarma

TEMEL YETENEKLER

Sertifikasyonlar ….

CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

CISA

CISM Certified Information Security Manager®

An ISACA® Certification

CISSP® Certified Information Systems Security Professional

C|EH

CERTIFIED ETHICAL HACKER

SANS | GIAC CERTIFICATIONS

sans.org giac.org

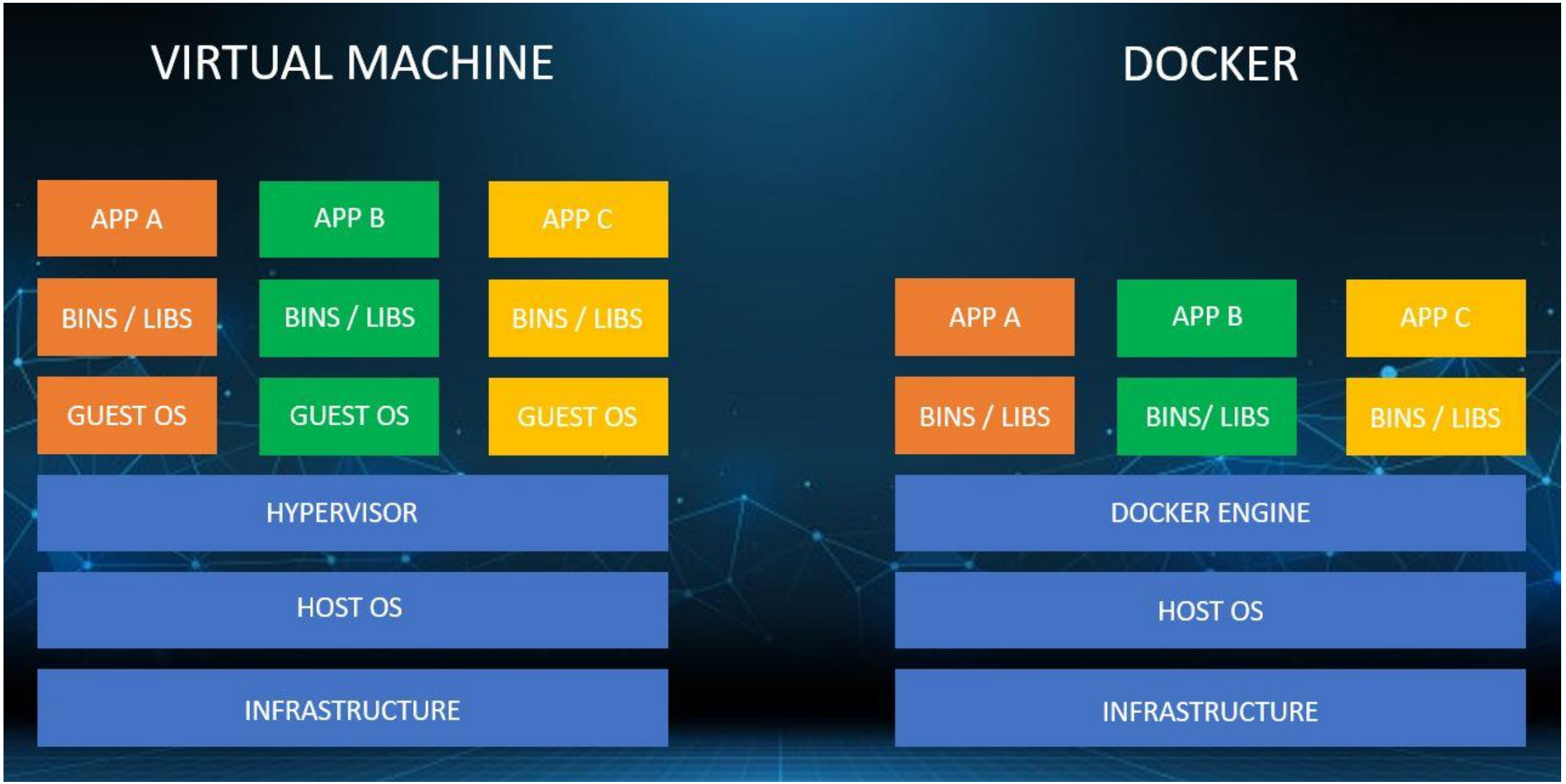
OFFENSIVE security OSCP

OFFENSIVE security OSWP

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

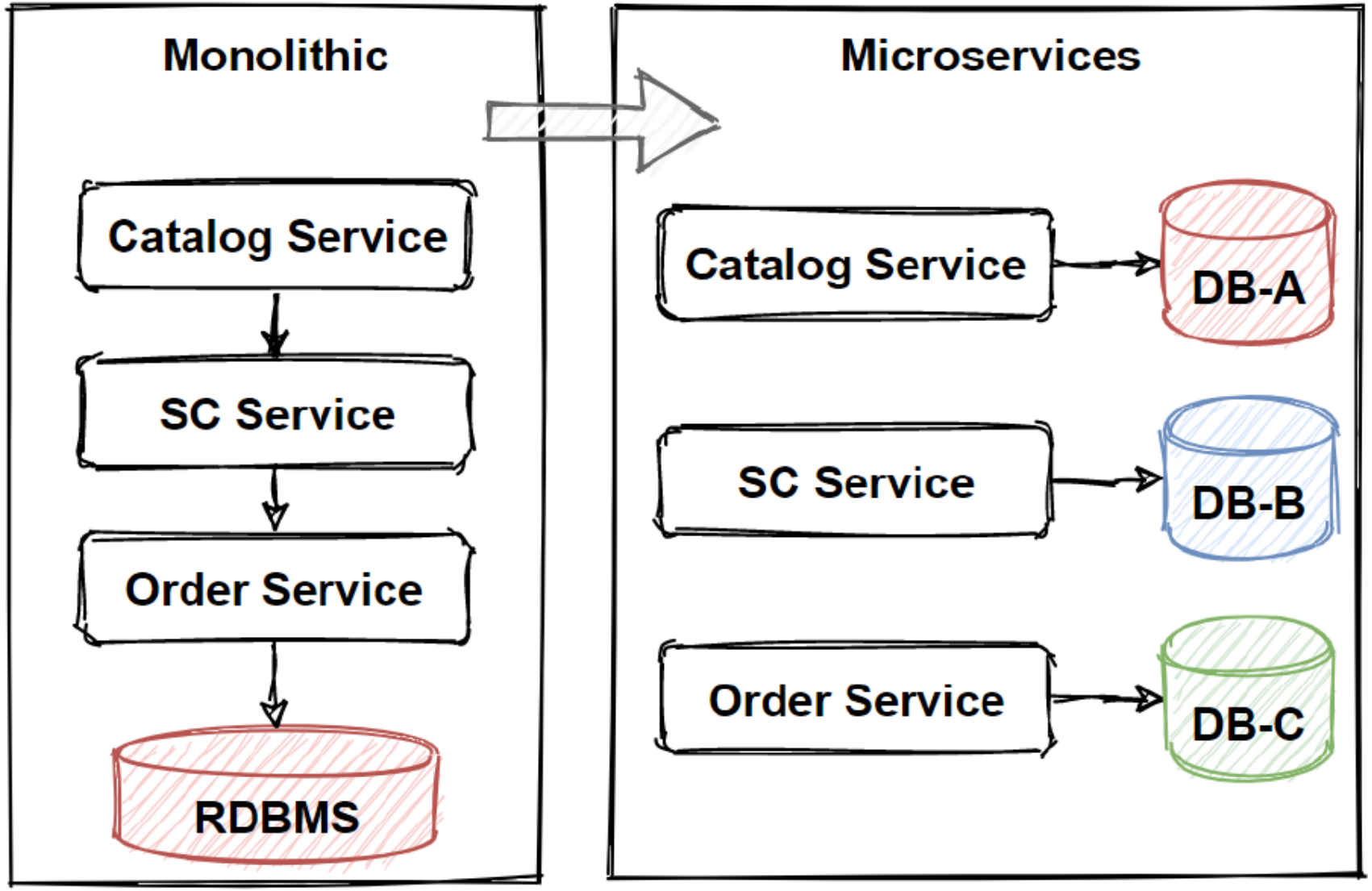
DEV-SEC-OPS

VM vs Container ….

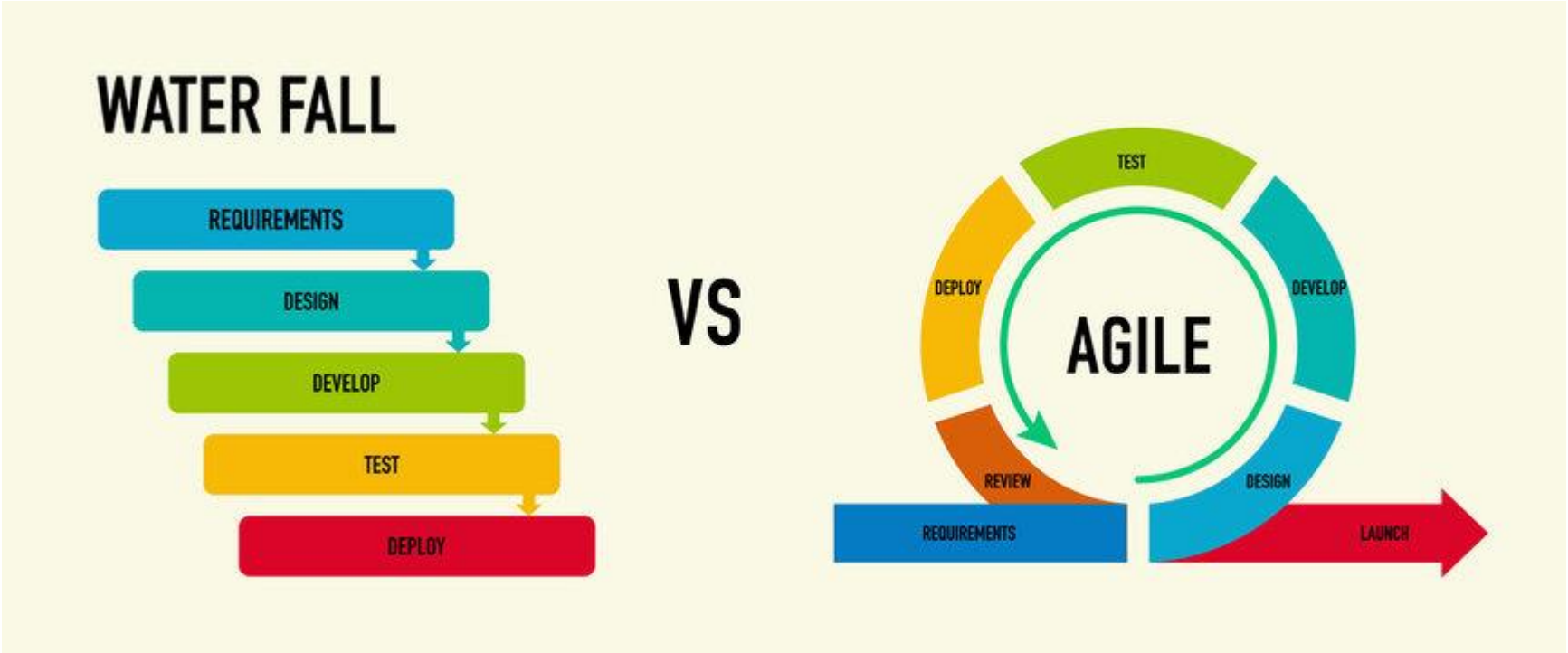


Platformlar ....

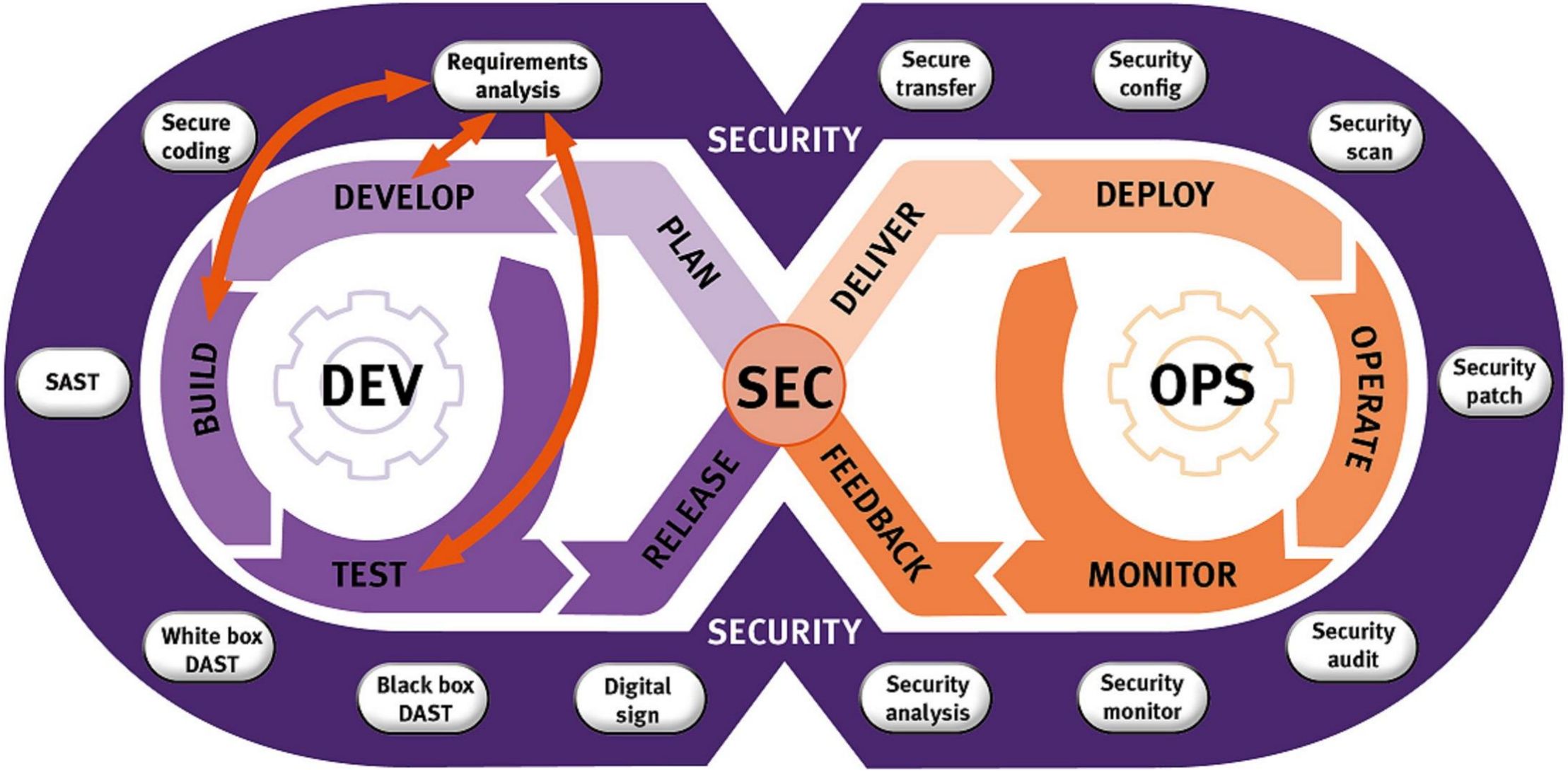
Microservis Mimarisi ....



Yazılım Yaşam Döngüsü ....



DEVSECOPS Yaşam Döngüsü ….



DEVSECOPS Yetkinlik Kazanımı ....

HashiCorp Terraform

Istio

HELM

Prometheus

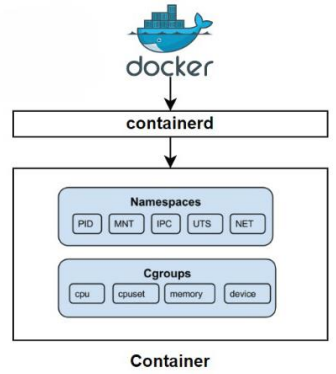
kubernetes

docker

OpenSSL
Cryptography and SSL/TLS Toolkit

etcd

IPTABLES



Container

ubuntu

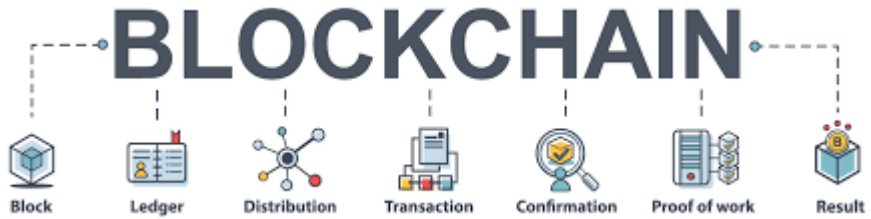
redhat

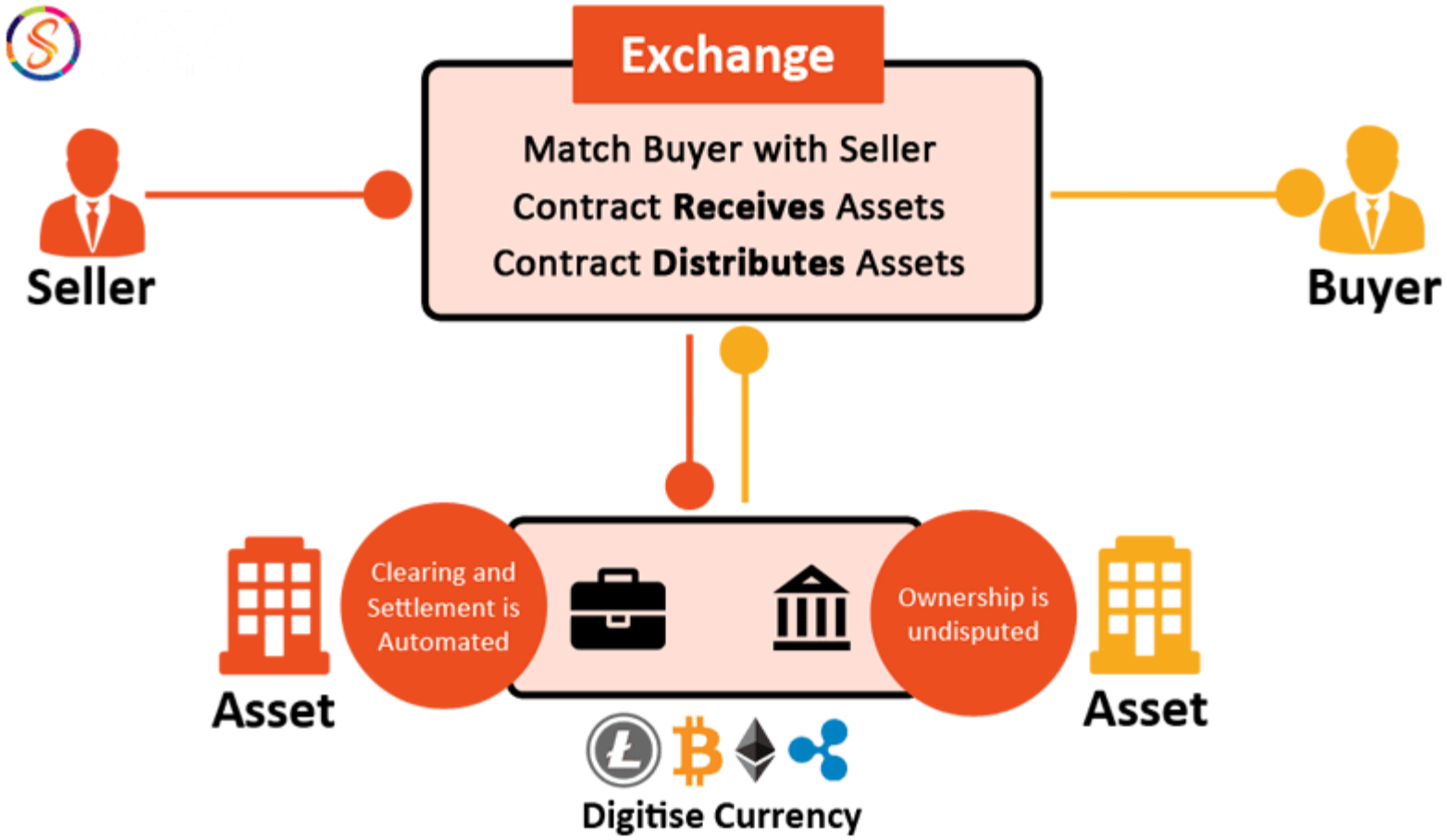
DEVSECOPS Sertifikasyon ….

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

WEB 3.0

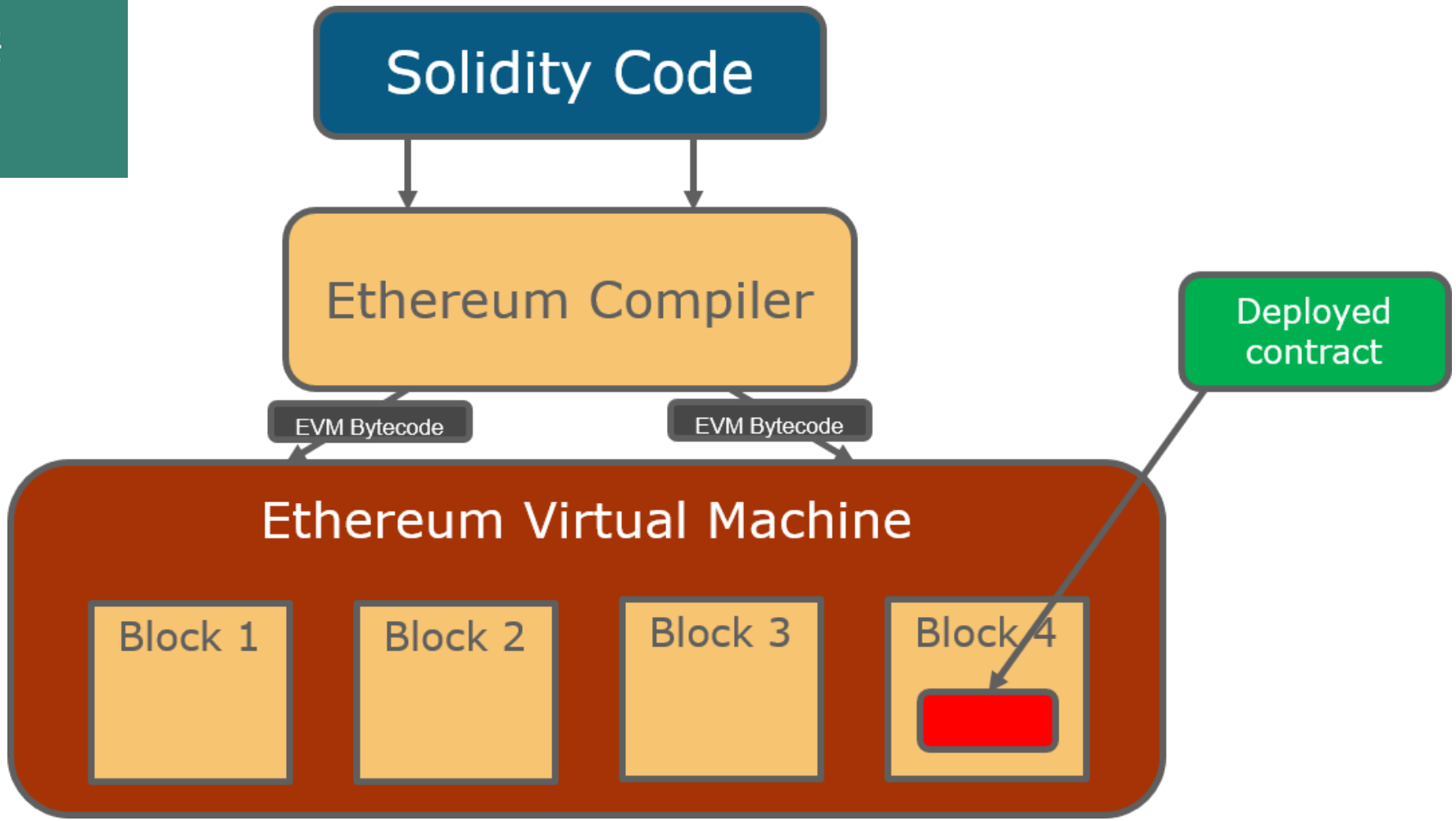
Akıllı Kontratlar ….





Programlama Dili ....

RUST



M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

ÇEVRİMİÇİ KAYNAKLAR

Çevrimiçi Kaynaklar ….

BTK AKADEMİ

Udemy

edX

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

AKADEMİ

Akademik Çalışma Alanları.....

- Güvenlik Quantum Haberleşmesi
- Uzay ve Havacılık Teknolojilerinde Güvenli Haberleşme
- Siber Güvenlik Otomasyonu
- Siber Fiziksel Sistemlerin Güvenliği
- Veri Mahremiyeti
- Yasal Düzenlemeler ve Etik
- Güvenli Yazılım Mühendisliği
- Ulusal Güvenlik ve Siber Güvenlik Politikaları
- Siber Suçların Aydınlatılması
- Kritik Altyapıların Güvenliği

M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

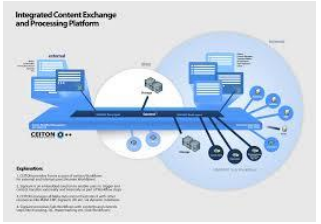
MÜLAKATLAR

Olmazsa olmazlar .....

- Girişken olmak ....
- Elini kirletmek ....
- Sosyal medya paylaşımları ....
- Github hesabı olmak ....
- Konferans ve etkinliklere katılım ..
- Yarışma ve projelere katılım ...

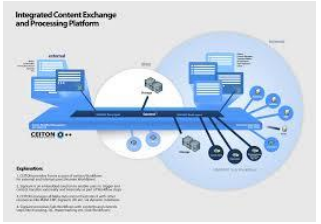
Sık Karşılaşılan Mülakat Soruları – 1 .....

- Şifreleme nedir ? Neden Önemlidir ?
- Simetrik ve asimetrik şifrelemenin farkı nedir ?
- Siber güvenlik alanında CIA neyi ifade eder ?
- Zaafiyet, risk ve tehdit nedir ?
- IDS ve IPS sistemlerinin farkı nedir ?
- SSL nedir ve nerede kullanılır ?
- SSL ve TLS'in farkı nedir ?
- Salted Hash nedir ?
- Kimlik hırsızlıklarının nasıl önüne geçilir ?
- Man in the Middle Attack nedir ? Nasıl Önlenir ?
- Encoding, hash ve encryption farkı nedir ?
- Herhangi bir sunucuyu nasıl güvenli hale getirebilirsin ?



Sık Karşılaşılan Mülakat Soruları – 2 .....

- DDoS saldırıları nedir ve nasıl önlenir ?
- DNS neden ihtiyaç duyarız ?
- Three-way handshake nedir ?
- Yazılım testi ile penetrasyon testinin farkı nedir ?
- Tracart/traceroute ne zaman ihtiyaç duyarız ?
- En sık karşılaşılan siber tehditler nelerdir ?
- OSI katmaları nelerdir ?
- Cross-site scripting ya da XSS saldırıları nasıl gerçekleşir ?
- Veri kaçağı nasıl önlenir ?
- ARP protokolü nedir ve nasıl çalışır ?
- 2FA nedir ve web sitelerinde nasıl uygulanır ?
- VLAN ile VPN'in farkı nedir ?



M M G
Mimar ve Mühendisler Grubu
Architects & Engineers Group
1996

Çok teşekkür ederim ....