

MEB Öğrenci Semineri

# Siber Güvenlik 360<sup>0</sup>

Dr. HAFZULLAH İŞ

BATMAN — 2024

# Sunum Akışı

1

Dijitalleşme

2

Siber  
Güvenlik

3

Bilinçli İnternet  
Kullanımı

4

Bilinçli Sosyal  
Medya  
Kullanımı

5

Cihaz Siber  
Güvenliği

6

Siber  
Dolandırıcılık  
Siber Zorbalık

+BONUS

# Dijitalleşen Yaşam

## Üretiyoruz!..

Endüstri 4.0  
(Mekanik, Elektrik, Otomasyon, İnternet)  
Nesnelerin İnterneti (IoT)  
Büyük Veri (Ölçülebilir, Büyük Hacimli)  
Bilgi Çağından 2. Makine Çağına

## Bağlantıdayız!..

- İnternet ile Her an Her Yerde
  - Akıllı Telefonlar
  - Aplikasyonlar
  - Web 2.0, Web 3.0

## Dijitalleşiyoruz!..

Birey, firma, kurumlar..  
İletişim, Etkileşim, Üretim, Eğitim  
Sürücüsüz Araçlardan Akıllı Evlere..  
Kriptoparalardan NFT lere..

## Sanallaşıyoruz!..

Sanal Kişilik, Etkileşim ve Yaşamlar..  
Sanal Sosyal Ağlar  
Metaverse



**Rakamlar  
olabileceklere dair  
geniř bir perspektif  
sunar!**

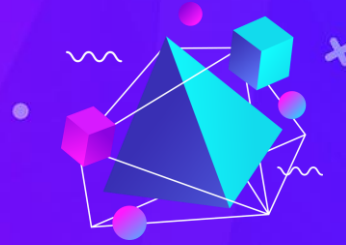
# Perspektif-2023

## We are Social 2023 Raporuna Göre:

- Dünya nüfusu 8.06 Milyar.
- Şahsi telefon kullanıcı sayısı, 5.60 Milyar. (%69.4)
- Toplam internet kullanıcı sayısı 5.30 Milyar. (%65.7)
- Aktif sosyal medya kullanıcı sayısı 4.95 Milyar (%61.4)

## Geçen yıla göre;

- Şahsi telefon kullanan sayısı, 145 Milyon arttı. (%2.7)
- Sosyal medya kullanıcıları 215 Milyon arttı. (%4.5)
- İnternet kullanıcıları 189 Milyon arttı. (%3.7)

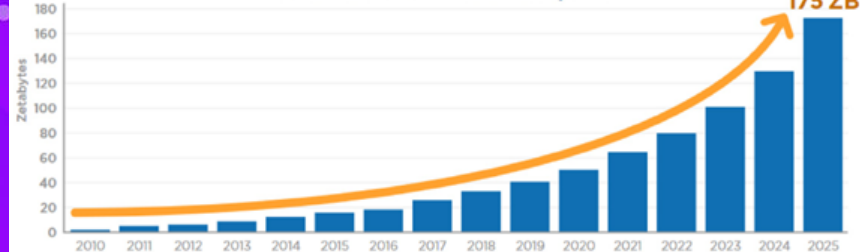


# Perspektif-2023

- Yıllık ortalama 175 Zettabyte veri üretiyoruz.
- Bu verilerden sadece %25 değerlendirilebilir.
- Değerlendirilebilir Verinin %0.05 işleniyor
- Dünya nüfusunun %60'ı sosyal medyada
- Tiktok ve youtube kullanıcılarının %48'i mobil erişimli..
- Mobil uygulamalara harcanan para 170 Milyon \$
- Yıllık kişi başı online alışveriş miktarı 1000 \$..
- Çin'de alışverişlerin %10'u online yapılmaktadır.
- Çalışan nüfustan internet kullanıcılarının %10'u Kriptoparalardan en az birini aldı.
- Gelişmekte olan ülkelerde kripto para pazarı diğerlerine göre çok daha hızlı artıyor. Türkiye'de Kripto para pazarı 2021 de %30 üzerinde arttı.



Annual Size of the Global Datasphere



# DONANIMSAL ÜRÜN KULLANIM İSTATİSTİKLERİ

Herhangi Bir  
Telefon Kullananlar!



97.6%

Akıllı Telefon  
Kullananlar



97.4%

Laptop yada PC  
Kullananlar



58.6%

Tablet  
Kullananlar



32.1%

Akıllı Saat  
Kullananlar



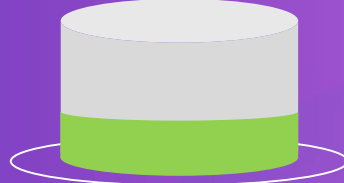
30.1%

Sanal Gerçeklik  
Cihazları

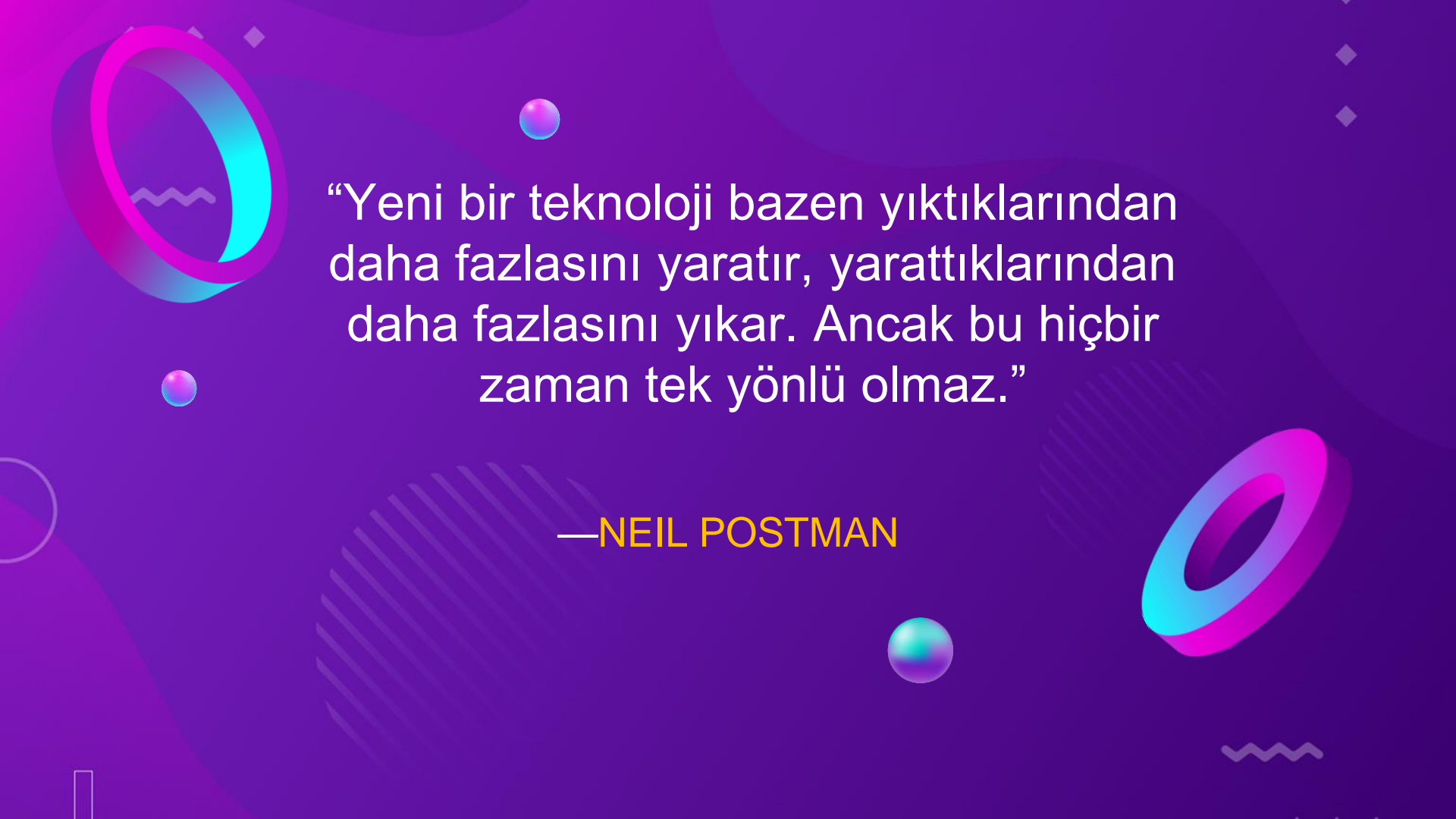


4.7%

Oyun Konsolları



19.3%

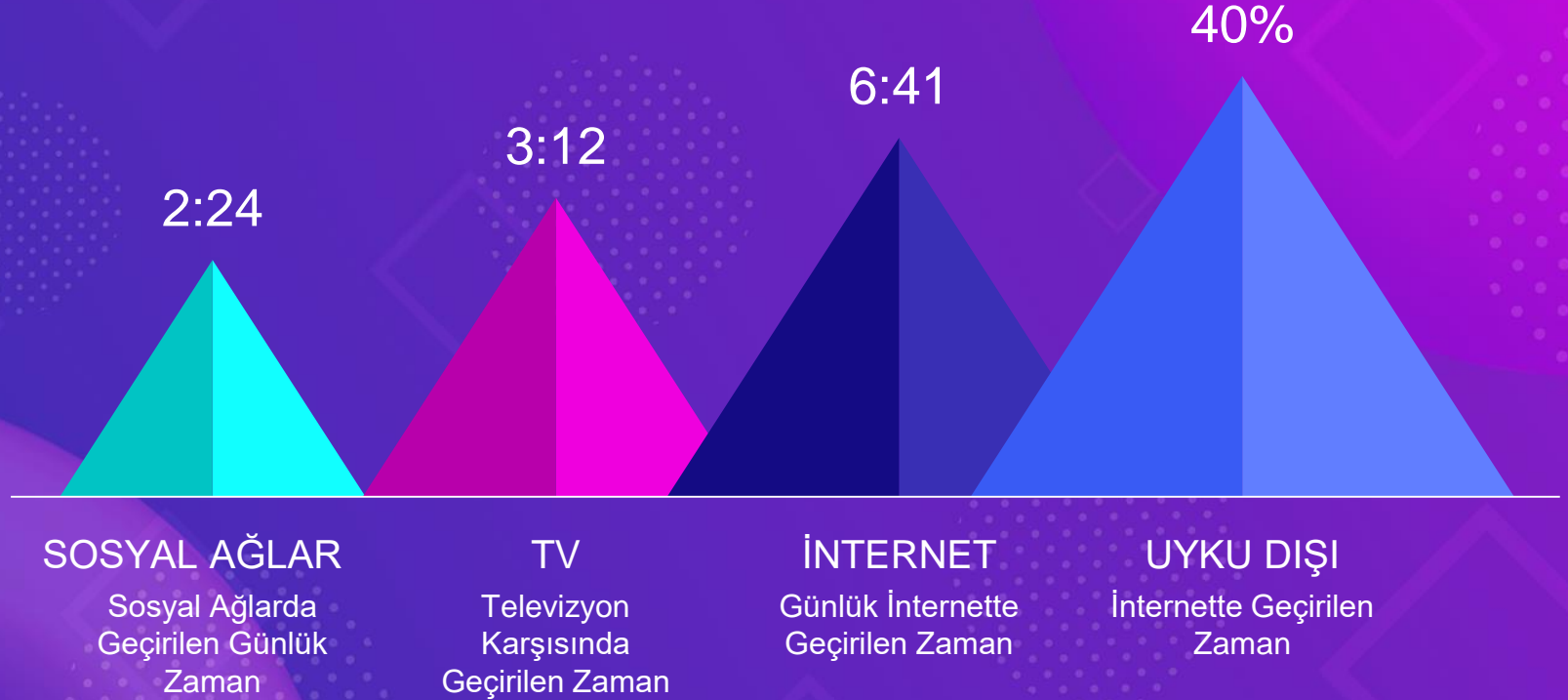


“Yeni bir teknoloji bazen yıktıklarından daha fazlasını yaratır, yarattıklarından daha fazlasını yıkar. Ancak bu hiçbir zaman tek yönlü olmaz.”

—NEIL POSTMAN



# SANAL SOSYAL YAŐAM



“Korkarım ki bir gün teknoloji, insan etkileşiminin önüne geçecek ve aptal bir nesil ortaya çıkacak.”

—ALBERT EINSTEIN



# Sunum Akışı

1

Dijitalleşme

2

Siber  
Güvenlik

3

Bilinçli İnternet  
Kullanımı

4

Sosyal Medya  
Kullanım Bilinci

5

Cihaz Siber  
Güvenliği

6

Siber  
Dolandırıcılık  
Siber Zorbalık

# Siber Güvenlik Nedir?

## Siber Nedir?

- Bilgisayarlar
- İnternet
- Dijital Teknolojiler
- Dijital Varlıklar



## Siber Güvenlik Nedir?

- Koruma
- Savunma ve Karşı Önlemler

# Siber Güvenlik Ne Değildir?

- Güvenliğe sadece OS seviyesinde ihtiyaç var.
- Firewall, Anti Virüs, vb. ile sistemlerimizi koruruz.
- Kriptografi kullanımı, yazılımın güvenliğini sağlar.
- Ürünlerin güvenliğini, tasarım bittiğinde test ediyoruz.
- Güvenlik özellikleri sistemleri güvenli kılar.
- Güvenli ortamlar (sunucular, sistem odaları) sistemleri güvenli kılar.
- “Biz sistemimizi/uygulamamızı izöle (kapalı ağ) ortamda tutuyoruz”
- “Güvenlik konularını bir sonraki sürümde ele alacağız ”

# Siber Güvenlik - The Triad

## 01

### Neyin siber güvenliđi?

-> Varlıklar

Confidentiality (Gizlilik)

Integrity (Eriřilebilirlik)

Availability (Bütünlük)

## 02

### Siber Güvenliđin Yapı Tařları

People (İnsanlar)

Process (Süreç)

Technology (Teknoloji)

## 03

### Neyi neyden koruyoruz?



# SİBER GÜVENLİK NEDEN ÖNEMLİ?



**Siber  
Saldırıların  
Artışı**



**Veri  
Değerinin  
Artması**



**Yapay Zeka ve  
Makine Öğrenmesi**



**IoT Cihazların  
Sayısındaki Artış**



**Devletler ve  
Şirketler**

# SİBER GÜVENLİK NEDEN ÖNEMLİ?

- 493.33 Milyon Ransomware Atak
- Günlük 3.4 milyar Phishing E-Mail
- Phishing nedeniyle 10.3 Milyar \$
- 4.1 Milyon websitesi & malware

## 2022 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
<b>Descriptors*</b>			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781



## BT Yöneticiler Bakış Açısı

24%

**BT varlıklarına ilişkin tam görünürlüğe sahip olduklarını hissediyorlar**

46%

**işletim sistemleri EOL/EOS nedeniyle savunmasızdır**

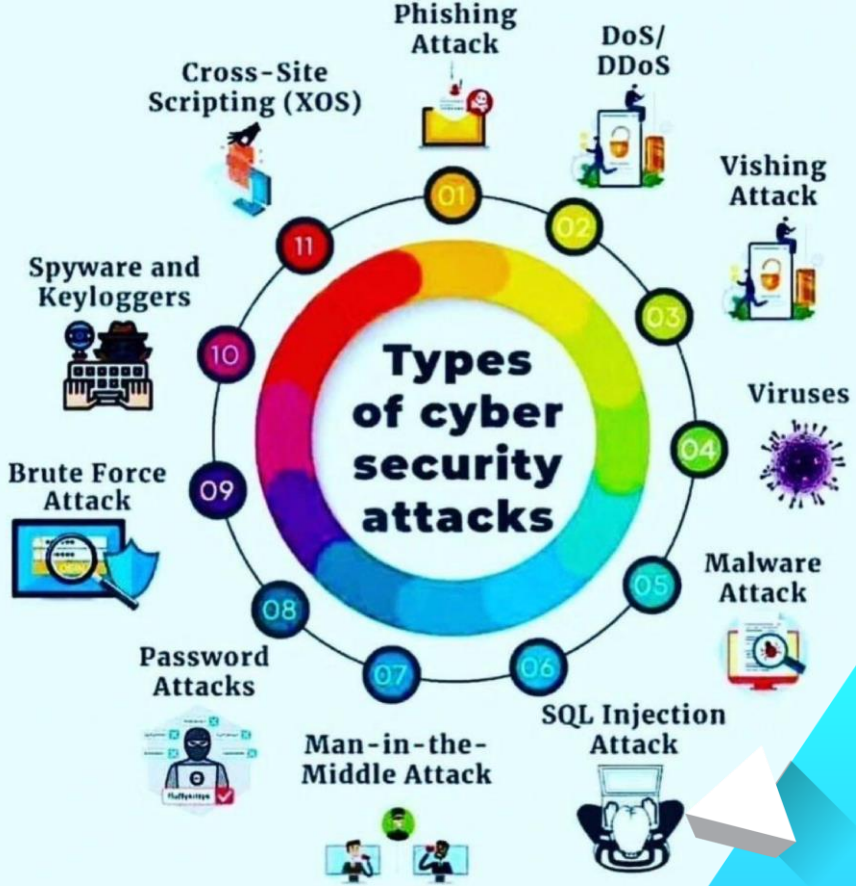
50%

**Yöneticiler güvenlik açıklarını en büyük endişeleri olarak belirtiyorlar**

3/dk

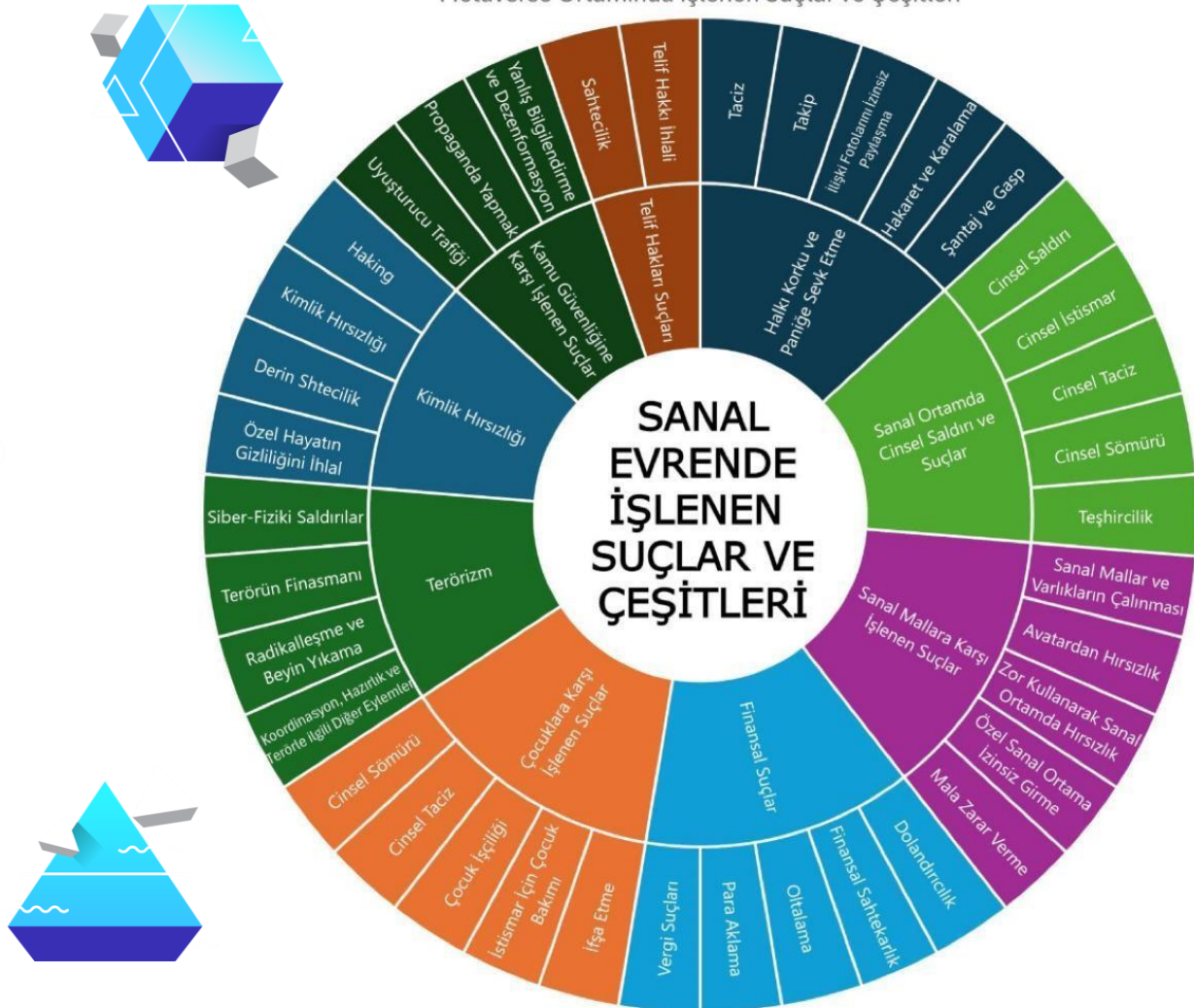
Türkiye'de Gerçekleşen  
Siber Saldırı Sayısı

# Types of cyber security attacks



# Cyber Security





# Bireysel Korunma, Cybersecurity Mindset

- Kltr, felsefe ve ahlak..
- evrenizdeki dnya ve o dnyanın neresinde olduėunuzla da ilgilidir.
- Her an her Őey olabilir ve bu konuda bir birey olarak ne yapabilirim?
- Kurban olmamak iin ne yapabilirim?
- **Siber gvenlik bakıŐ aısının geliŐtirilmesi ile siber tehditlere karŐı daha direnli hale gelebiliriz.**
- **Sosyal Medya Tehlikesinin farkında olmak.**

# Peki Gerçek Dünyada Durum Nasıl?

## Güvensiz Yazılım Geliştirme

- Kod kontrolü zaman kaybıdır.
- Yeni sürüm hemen devreye alınmalıdır.
- Yazılım geliştiriciler rahat çalışmalıdır.
- Güvenlik sonradan sağlanabilir.
- Çalışan sisteme dokunmayın.
- Yetki eksikliği yüzünden hata almayın.

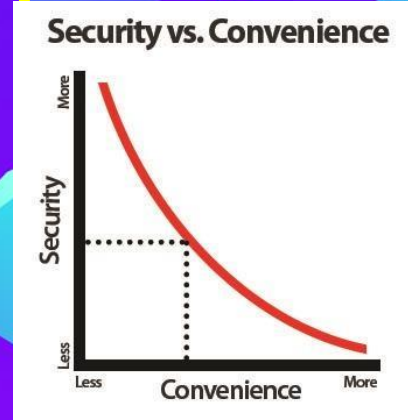


# Neden oęu Yazılım Güvensizdir?

- oęu geliřtirici «güvenli» yazılım geliřtirmeyi bilmemektedir.
  - oęu okulda güvenli yazılım geliřtirme eęitimi bulunmamaktadır.
  - oęu programlama kitabında güvenlik hakkında detaylar bulunmuyor.
  - Bazı diller doęaları gereęi güvensizdir. (örneęin; C)
  - oęu geliřtirici, bir saldırgan gibi düşünmez.
- Müřteriler kolaylıkla yazılımın güvenlięini kontrol edemez.
- Yöneticiler her zaman yeterli eęitimi saęlayamayabilir.

# Neden Çoğu Yazılım Güvensizdir?

- **Güvenlik her zaman ikinci plana atılıyor.**
  - Ana hedef her zaman bir işlevsellik sunmaktır.
  - Riskler göz ardı edilerek, risk yönetimi ikinci plana atılmaktadır.
- **Sıklıkla güvenlik ve kullanılabilirlik arasında bir çatışma çıkar.**





# Güvenli Yazılım Geliştirme İlkeleri

- **Gerekli Miktarda Yetki Verilmesi**
- **Erişimlerin Denetlenmesi**
- **Yetkilerin Ayrılması**
- **Varsayılan Değer Kontrolü**
- **Ortak Erişilen Kanalların Kontrol Edilmesi**
- **Zayıf Halkayı Güçlendirme**
- **Saldırı Yüzey Alanını Azaltma**
- **Savunma Derinliğinin Oluşturulması**
- **Güvenlik Mekanizmalarının Tasarlanması**



# Yazılım Geliştirme Yaşam Döngüsü

- Belirli temel adımları takip ederek yazılımın gereksinimlerinin belirlenmesi aşamasından devreye alma aşamasına kadar süreçlerin tanımlanmasıdır.

## Yazılım Geliştirme Yaşam Döngüsü



# Güvenli Yazılım Geliştirme Yaşam Döngüsü

Yazılım geliştirme yaşam döngüsünde her adımda güvenlik ile ilgili süreçlerin tanımlanmasıdır.

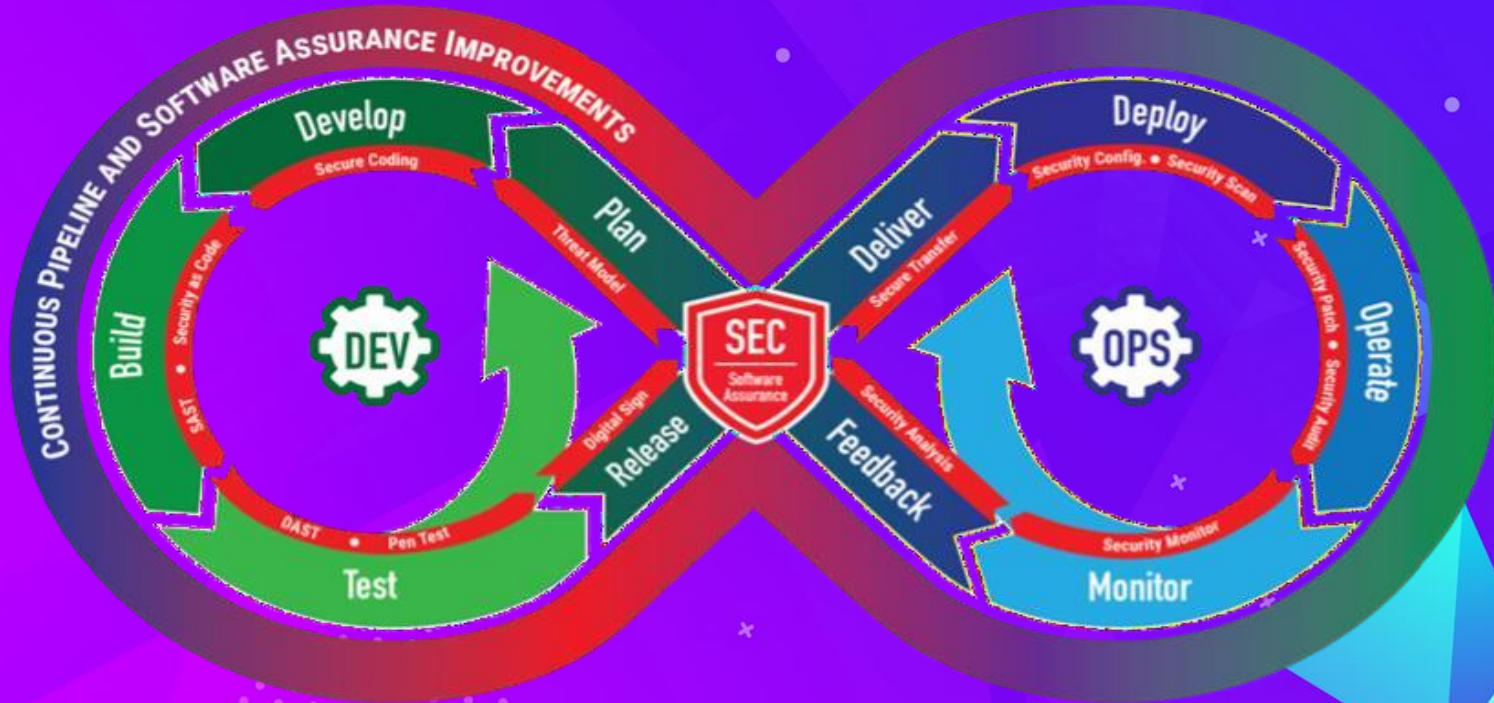


## Güvenli Yazılım Geliştirme Yaşam Döngüsü

- ✓ İlk andan itibaren güvenlik odaklı düşünme
- ✓ Sürekli güvenlik yaklaşımı
- ✓ Kültürel değişim
- ✓ DevOps → DevSecOps

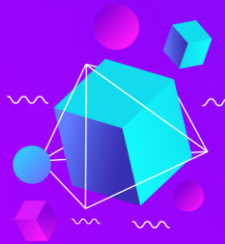
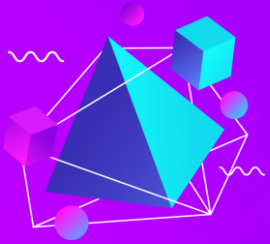
# DevSecOps

DevSecOps, geliştirme (development), security (güvenlik) ve operasyon (operation) kavramlarını bir araya getiren teknik ve idari yöntemler bütünü olarak tanımlanabilir.

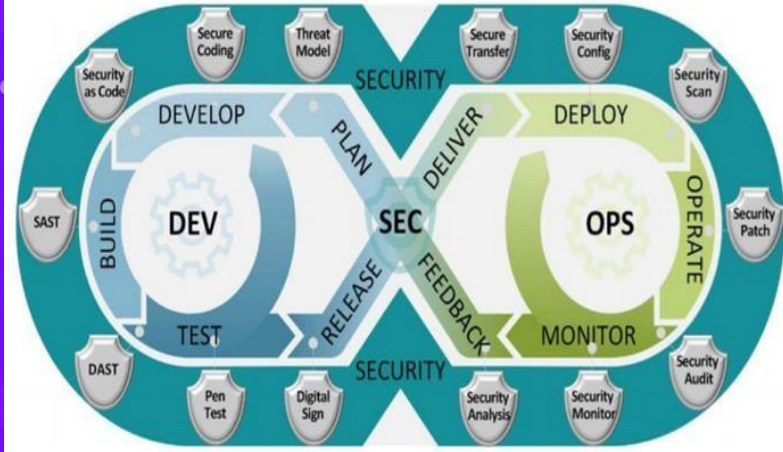


# DevSecOps

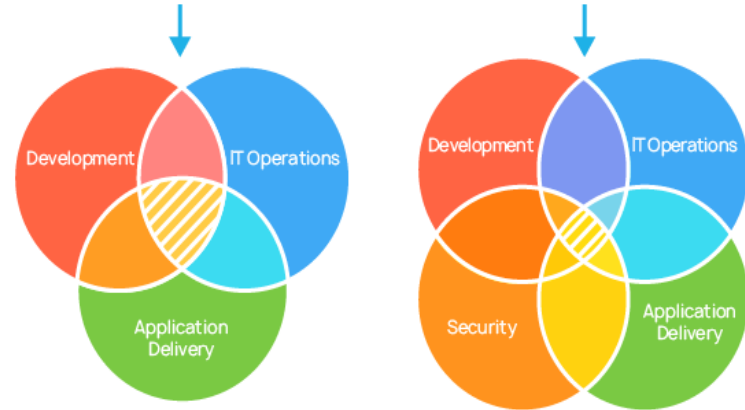
- Güvenli Yazılım Geliştirme
- Hızlı ve Sürekli dağıtım
- Ekip işbirliği
- Otomasyon



## DevSecOps Software Lifecycle



## DevOps VS DevSecOps



# Sistem Güvenliđi Mühendisliđi

## Amaç:

- Sistemlerdeki güvenlik açıkları ve tehditleri **önceden** belirlemek ve bu güvenlik açıklarıyla ilişkili riskleri **en aza** indirmek için bilimsel ve mühendislik ilkelerini uygulayan Sistem Mühendisliđi'nin **artık** en temel unsurlarından birisidir.



# Siber Gvenlik Alanında Kariyer

- **Bilgisayar ve İşletim Sistemi Bilgisi**
- **Ađ gvenliđi**
- **Programlama ve Kod Analizi**
- **Sertifikasyon**
- **Srekli Gncel Kalmak**



# Abalı Yaklaşım

## ✔ Firewalls

- iptables
- firewalld
- ufw
- Guarddog
- Vuurmuur
- Gufw
- Shorewall

## ✔ Security Audit

- openSCAP
- openVAS
- Nmap
- Nikto
- Lynis
- SpiderFoot

## ✔ Rootkit/Malware Detection

- Wazuh
- chkrootkit
- rkhunter
- Tiger
- LMD

## ✔ Access Control

- SELinux
- AppArmor
- Smack
- Grsecurity \$
- Yama

## ✔ Sandboxing

- Bubblewrap
- Firejail
- Flatpak
- Snappy
- Chroot Jail

## ✔ IDS/IPS

- Snort
- Suricata
- Zeek
- OSSEC
- AIDE
- Security Onion
- OSSIM \$
- CrowdSec

## ✔ File Integrity Monitoring

- Tripwire
- Auditd
- Samhain
- OSSEC
- Wazuh
- Osquery
- Atomic OSSEC \$

## ✔ Antivirus

- CrowdStrike \$
- ClamAV
- Rspamd

## ✔ Log Monitoring

- Logwatch
- ELK Stack \$
- Graylog \$
- Sagan
- Fluentd
- OpenObserve
- Dynatrace \$

## ✔ Disk/Filesystem Encryption

- dm-crypt
- fscrypt
- EncFS
- Veracrypt
- Gocryptfs
- eCryptfs
- SecureFS

## ✔ Secure Shell

- SSHGard
- DenyHosts
- Knockd
- Fail2ban

## ✔ Password Sec

- John the Ripper
- Hashcat
- KeePassXC
- pwgen
- GoPass

## ✔ VPN

- strongSwan
- OpenVPN
- WireGuard
- Libreswan
- SoftEther

## ✔ Patch Manager

- Spacewalk
- Katello
- RH Satellite \$
- Landscape \$
- NinjaOne \$

## ✔ WAFs

- ModSecurity
- NAXSI
- BunkerWeb
- Coraza
- open-appsec

## ✔ Container Sec

- Docker Bench
- Calico
- Clair
- gVisor
- Grafeas
- Falco
- Dagda
- Cilium
- Dockle



# Abalı Yaklaşım



# RedTeam

T O O L K I T

## Privilege Escalation

- BloodHound
- BeRoot

## Command and control

- Empire Project
- Pupy
- Cobalt Strike

## Reconnaissance

- Nmap
- Shodan
- sqlmap
- Crt.sh
- OpenVAS
- RustScan
- Nikto
- Amass

## Credential Dumping

- Mimikatz
- LaZagne
- Pypykatz
- Dumpert
- forkatz
- nanodump

## Phishing

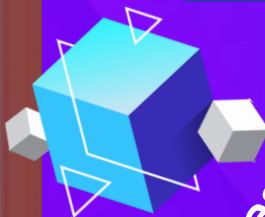
- Gophish
- King Phisher
- EvilURL

## OSINT

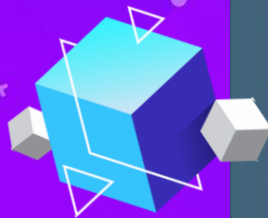
- Maltego
- Spiderfoot
- OSINT Framework

## Exfiltration

- SharpExfiltrate
- DNSExfiltrator
- Egress-Assess



Abalı Yaklaşım



# BlueTeam

T O O L K I T

## Network Analysis

- Wireshark
- pfSense
- Arkime
- Snort

## Incident Management

- TheHive
- GRR Rapid Response

## Threat Intelligence

- Misp
- MSTICPy

## EDR

- Cortex XDR
- Cynet 360
- FortiEDR

## OS Analysis

- HELK
- Volatility
- Wazuh
- RegRipper
- OSSEC
- osquery

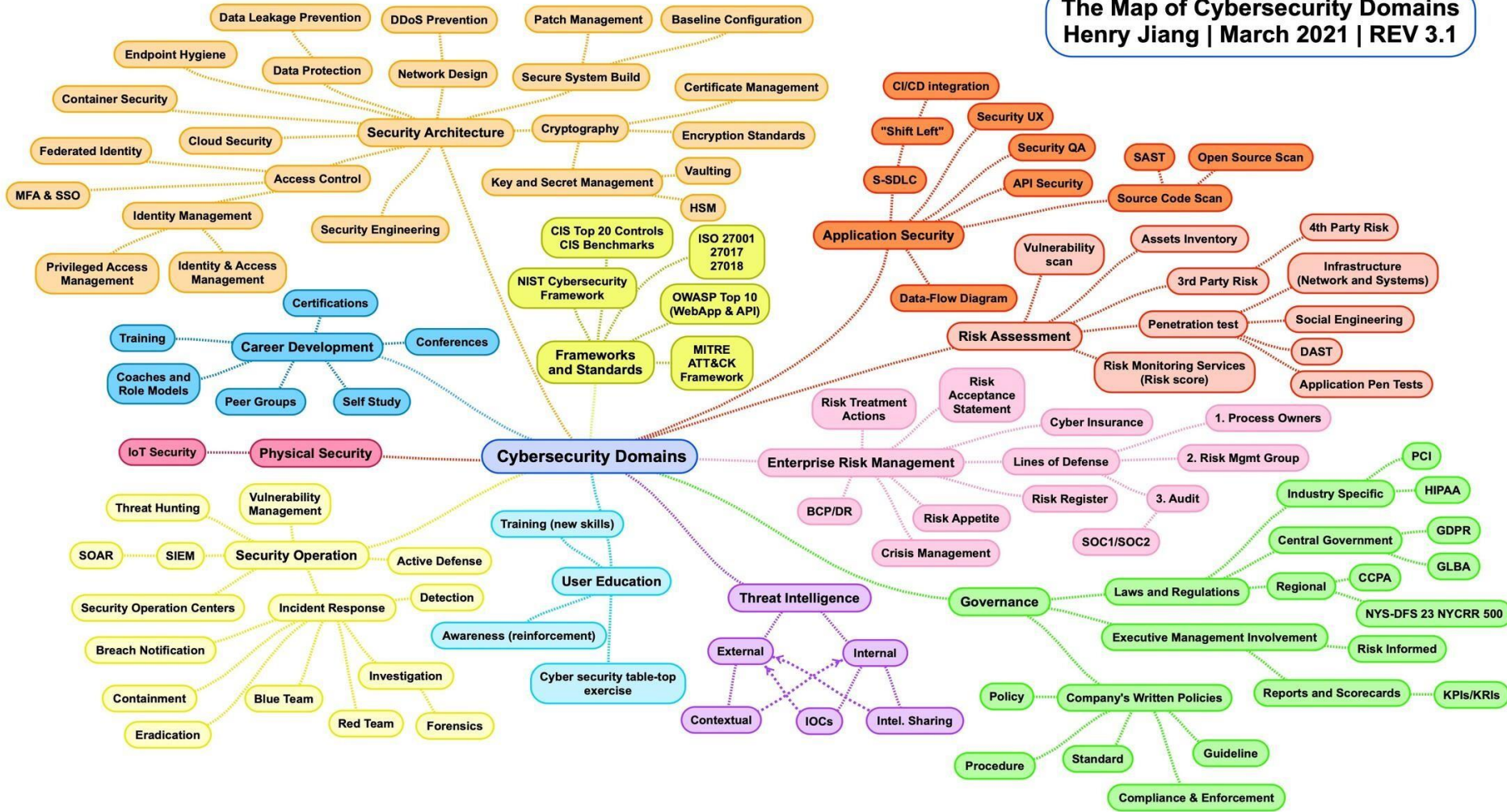
## Honeypots

- Kippo
- Cowrie
- Dockpot
- HonSSH

## SIEM

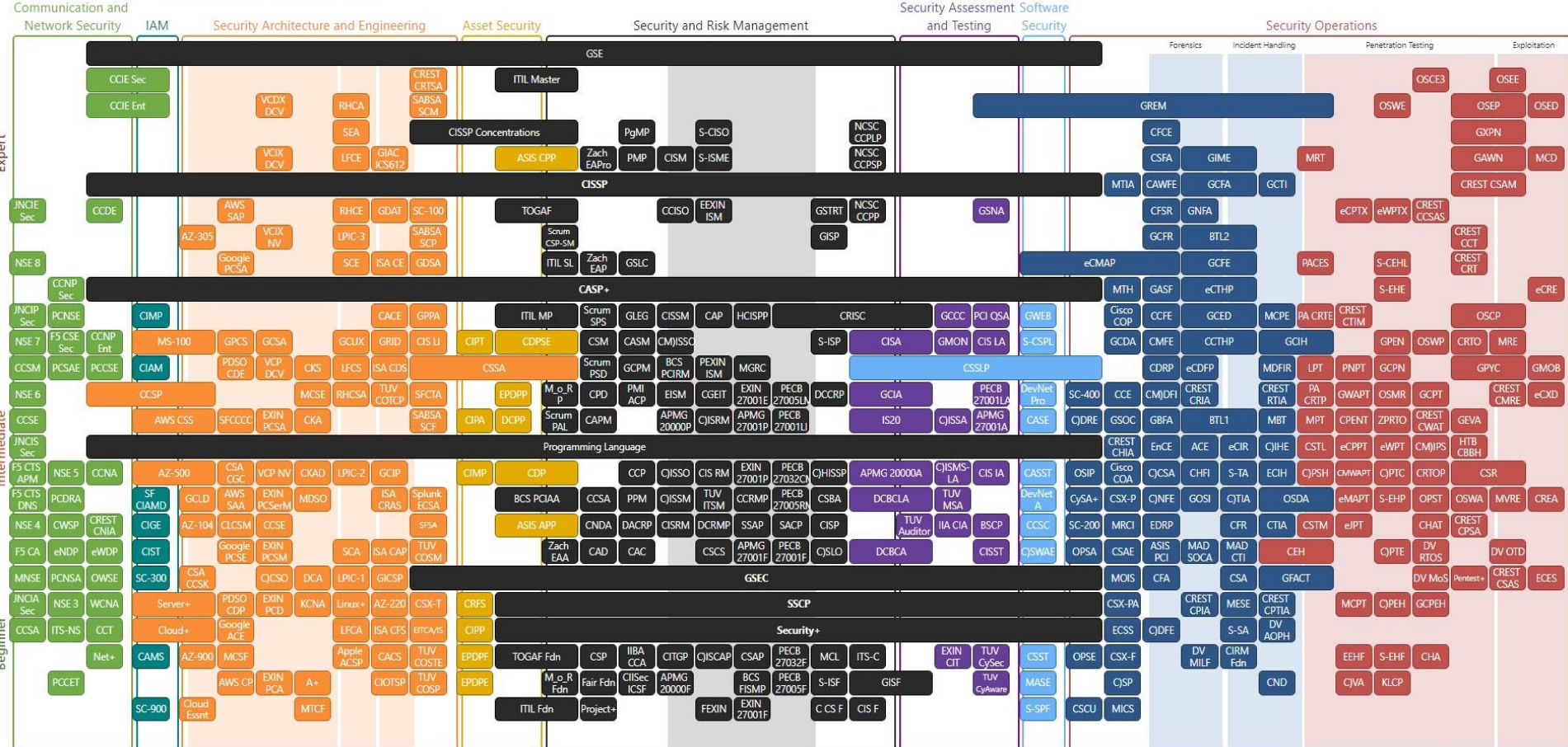
- OSSIM
- Splunk
- LogRhythm

**The Map of Cybersecurity Domains**  
 Henry Jiang | March 2021 | REV 3.1



# Siber Güvenlik Sertifikasyon Yol Haritası

## Security Certification Roadmap



# COOLEST CAREERS IN CYBERBER



Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in-demand by employers. Which jobs are the coolest and most in-demand? We know; let us show you the hottest cybersecurity jobs for 2023.

Curricula: **Cyber Defense** **Digital Forensics** **Offensive Operations** **Cybersecurity Leadership** **Cloud Security** **Industrial Control Systems** **Purple Team** **SEC460 (new)** — GIAC Certification with course

### 01 Threat Hunter (Threat/Warning Analyst)

This expert applies their threat intelligence skills to identify indicators that have slipped through real-time detection mechanisms. The practice of threat hunting requires a deep understanding of an organization's network and systems, as well as the ability to identify and analyze suspicious activity. This role involves identifying indicators of compromise (IOCs) and analyzing them to determine if they represent a threat to the organization's security.

**Why is this role important?**  
Threat hunting is a proactive security measure that allows organizations to identify and neutralize threats before they can cause significant damage. It involves analyzing network logs, system logs, and other data to identify suspicious activity that may indicate a threat.

**Recommended courses**  
[SEC409 \(new\)](#) [SEC504 \(new\)](#) [FOR327 \(new\)](#) [FOR511 \(new\)](#) [FOR512 \(new\)](#) [FOR513 \(new\)](#) [FOR514 \(new\)](#) [FOR515 \(new\)](#) [FOR516 \(new\)](#) [FOR517 \(new\)](#) [FOR518 \(new\)](#) [FOR519 \(new\)](#) [FOR520 \(new\)](#) [FOR521 \(new\)](#) [FOR522 \(new\)](#) [FOR523 \(new\)](#) [FOR524 \(new\)](#) [FOR525 \(new\)](#) [FOR526 \(new\)](#) [FOR527 \(new\)](#) [FOR528 \(new\)](#) [FOR529 \(new\)](#) [FOR530 \(new\)](#) [FOR531 \(new\)](#) [FOR532 \(new\)](#) [FOR533 \(new\)](#) [FOR534 \(new\)](#) [FOR535 \(new\)](#) [FOR536 \(new\)](#) [FOR537 \(new\)](#) [FOR538 \(new\)](#) [FOR539 \(new\)](#) [FOR540 \(new\)](#) [FOR541 \(new\)](#) [FOR542 \(new\)](#) [FOR543 \(new\)](#) [FOR544 \(new\)](#) [FOR545 \(new\)](#) [FOR546 \(new\)](#) [FOR547 \(new\)](#) [FOR548 \(new\)](#) [FOR549 \(new\)](#) [FOR550 \(new\)](#) [FOR551 \(new\)](#) [FOR552 \(new\)](#) [FOR553 \(new\)](#) [FOR554 \(new\)](#) [FOR555 \(new\)](#) [FOR556 \(new\)](#) [FOR557 \(new\)](#) [FOR558 \(new\)](#) [FOR559 \(new\)](#) [FOR560 \(new\)](#) [FOR561 \(new\)](#) [FOR562 \(new\)](#) [FOR563 \(new\)](#) [FOR564 \(new\)](#) [FOR565 \(new\)](#) [FOR566 \(new\)](#) [FOR567 \(new\)](#) [FOR568 \(new\)](#) [FOR569 \(new\)](#) [FOR570 \(new\)](#) [FOR571 \(new\)](#) [FOR572 \(new\)](#) [FOR573 \(new\)](#) [FOR574 \(new\)](#) [FOR575 \(new\)](#) [FOR576 \(new\)](#) [FOR577 \(new\)](#) [FOR578 \(new\)](#) [FOR579 \(new\)](#) [FOR580 \(new\)](#) [FOR581 \(new\)](#) [FOR582 \(new\)](#) [FOR583 \(new\)](#) [FOR584 \(new\)](#) [FOR585 \(new\)](#) [FOR586 \(new\)](#) [FOR587 \(new\)](#) [FOR588 \(new\)](#) [FOR589 \(new\)](#) [FOR590 \(new\)](#) [FOR591 \(new\)](#) [FOR592 \(new\)](#) [FOR593 \(new\)](#) [FOR594 \(new\)](#) [FOR595 \(new\)](#) [FOR596 \(new\)](#) [FOR597 \(new\)](#) [FOR598 \(new\)](#) [FOR599 \(new\)](#) [FOR600 \(new\)](#) [FOR601 \(new\)](#) [FOR602 \(new\)](#) [FOR603 \(new\)](#) [FOR604 \(new\)](#) [FOR605 \(new\)](#) [FOR606 \(new\)](#) [FOR607 \(new\)](#) [FOR608 \(new\)](#) [FOR609 \(new\)](#) [FOR610 \(new\)](#) [FOR611 \(new\)](#) [FOR612 \(new\)](#) [FOR613 \(new\)](#) [FOR614 \(new\)](#) [FOR615 \(new\)](#) [FOR616 \(new\)](#) [FOR617 \(new\)](#) [FOR618 \(new\)](#) [FOR619 \(new\)](#) [FOR620 \(new\)](#) [FOR621 \(new\)](#) [FOR622 \(new\)](#) [FOR623 \(new\)](#) [FOR624 \(new\)](#) [FOR625 \(new\)](#) [FOR626 \(new\)](#) [FOR627 \(new\)](#) [FOR628 \(new\)](#) [FOR629 \(new\)](#) [FOR630 \(new\)](#) [FOR631 \(new\)](#) [FOR632 \(new\)](#) [FOR633 \(new\)](#) [FOR634 \(new\)](#) [FOR635 \(new\)](#) [FOR636 \(new\)](#) [FOR637 \(new\)](#) [FOR638 \(new\)](#) [FOR639 \(new\)](#) [FOR640 \(new\)](#) [FOR641 \(new\)](#) [FOR642 \(new\)](#) [FOR643 \(new\)](#) [FOR644 \(new\)](#) [FOR645 \(new\)](#) [FOR646 \(new\)](#) [FOR647 \(new\)](#) [FOR648 \(new\)](#) [FOR649 \(new\)](#) [FOR650 \(new\)](#) [FOR651 \(new\)](#) [FOR652 \(new\)](#) [FOR653 \(new\)](#) [FOR654 \(new\)](#) [FOR655 \(new\)](#) [FOR656 \(new\)](#) [FOR657 \(new\)](#) [FOR658 \(new\)](#) [FOR659 \(new\)](#) [FOR660 \(new\)](#) [FOR661 \(new\)](#) [FOR662 \(new\)](#) [FOR663 \(new\)](#) [FOR664 \(new\)](#) [FOR665 \(new\)](#) [FOR666 \(new\)](#) [FOR667 \(new\)](#) [FOR668 \(new\)](#) [FOR669 \(new\)](#) [FOR670 \(new\)](#) [FOR671 \(new\)](#) [FOR672 \(new\)](#) [FOR673 \(new\)](#) [FOR674 \(new\)](#) [FOR675 \(new\)](#) [FOR676 \(new\)](#) [FOR677 \(new\)](#) [FOR678 \(new\)](#) [FOR679 \(new\)](#) [FOR680 \(new\)](#) [FOR681 \(new\)](#) [FOR682 \(new\)](#) [FOR683 \(new\)](#) [FOR684 \(new\)](#) [FOR685 \(new\)](#) [FOR686 \(new\)](#) [FOR687 \(new\)](#) [FOR688 \(new\)](#) [FOR689 \(new\)](#) [FOR690 \(new\)](#) [FOR691 \(new\)](#) [FOR692 \(new\)](#) [FOR693 \(new\)](#) [FOR694 \(new\)](#) [FOR695 \(new\)](#) [FOR696 \(new\)](#) [FOR697 \(new\)](#) [FOR698 \(new\)](#) [FOR699 \(new\)](#) [FOR700 \(new\)](#) [FOR701 \(new\)](#) [FOR702 \(new\)](#) [FOR703 \(new\)](#) [FOR704 \(new\)](#) [FOR705 \(new\)](#) [FOR706 \(new\)](#) [FOR707 \(new\)](#) [FOR708 \(new\)](#) [FOR709 \(new\)](#) [FOR710 \(new\)](#) [FOR711 \(new\)](#) [FOR712 \(new\)](#) [FOR713 \(new\)](#) [FOR714 \(new\)](#) [FOR715 \(new\)](#) [FOR716 \(new\)](#) [FOR717 \(new\)](#) [FOR718 \(new\)](#) [FOR719 \(new\)](#) [FOR720 \(new\)](#) [FOR721 \(new\)](#) [FOR722 \(new\)](#) [FOR723 \(new\)](#) [FOR724 \(new\)](#) [FOR725 \(new\)](#) [FOR726 \(new\)](#) [FOR727 \(new\)](#) [FOR728 \(new\)](#) [FOR729 \(new\)](#) [FOR730 \(new\)](#) [FOR731 \(new\)](#) [FOR732 \(new\)](#) [FOR733 \(new\)](#) [FOR734 \(new\)](#) [FOR735 \(new\)](#) [FOR736 \(new\)](#) [FOR737 \(new\)](#) [FOR738 \(new\)](#) [FOR739 \(new\)](#) [FOR740 \(new\)](#) [FOR741 \(new\)](#) [FOR742 \(new\)](#) [FOR743 \(new\)](#) [FOR744 \(new\)](#) [FOR745 \(new\)](#) [FOR746 \(new\)](#) [FOR747 \(new\)](#) [FOR748 \(new\)](#) [FOR749 \(new\)](#) [FOR750 \(new\)](#) [FOR751 \(new\)](#) [FOR752 \(new\)](#) [FOR753 \(new\)](#) [FOR754 \(new\)](#) [FOR755 \(new\)](#) [FOR756 \(new\)](#) [FOR757 \(new\)](#) [FOR758 \(new\)](#) [FOR759 \(new\)](#) [FOR760 \(new\)](#) [FOR761 \(new\)](#) [FOR762 \(new\)](#) [FOR763 \(new\)](#) [FOR764 \(new\)](#) [FOR765 \(new\)](#) [FOR766 \(new\)](#) [FOR767 \(new\)](#) [FOR768 \(new\)](#) [FOR769 \(new\)](#) [FOR770 \(new\)](#) [FOR771 \(new\)](#) [FOR772 \(new\)](#) [FOR773 \(new\)](#) [FOR774 \(new\)](#) [FOR775 \(new\)](#) [FOR776 \(new\)](#) [FOR777 \(new\)](#) [FOR778 \(new\)](#) [FOR779 \(new\)](#) [FOR780 \(new\)](#) [FOR781 \(new\)](#) [FOR782 \(new\)](#) [FOR783 \(new\)](#) [FOR784 \(new\)](#) [FOR785 \(new\)](#) [FOR786 \(new\)](#) [FOR787 \(new\)](#) [FOR788 \(new\)](#) [FOR789 \(new\)](#) [FOR790 \(new\)](#) [FOR791 \(new\)](#) [FOR792 \(new\)](#) [FOR793 \(new\)](#) [FOR794 \(new\)](#) [FOR795 \(new\)](#) [FOR796 \(new\)](#) [FOR797 \(new\)](#) [FOR798 \(new\)](#) [FOR799 \(new\)](#) [FOR800 \(new\)](#) [FOR801 \(new\)](#) [FOR802 \(new\)](#) [FOR803 \(new\)](#) [FOR804 \(new\)](#) [FOR805 \(new\)](#) [FOR806 \(new\)](#) [FOR807 \(new\)](#) [FOR808 \(new\)](#) [FOR809 \(new\)](#) [FOR810 \(new\)](#) [FOR811 \(new\)](#) [FOR812 \(new\)](#) [FOR813 \(new\)](#) [FOR814 \(new\)](#) [FOR815 \(new\)](#) [FOR816 \(new\)](#) [FOR817 \(new\)](#) [FOR818 \(new\)](#) [FOR819 \(new\)](#) [FOR820 \(new\)](#) [FOR821 \(new\)](#) [FOR822 \(new\)](#) [FOR823 \(new\)](#) [FOR824 \(new\)](#) [FOR825 \(new\)](#) [FOR826 \(new\)](#) [FOR827 \(new\)](#) [FOR828 \(new\)](#) [FOR829 \(new\)](#) [FOR830 \(new\)](#) [FOR831 \(new\)](#) [FOR832 \(new\)](#) [FOR833 \(new\)](#) [FOR834 \(new\)](#) [FOR835 \(new\)](#) [FOR836 \(new\)](#) [FOR837 \(new\)](#) [FOR838 \(new\)](#) [FOR839 \(new\)](#) [FOR840 \(new\)](#) [FOR841 \(new\)](#) [FOR842 \(new\)](#) [FOR843 \(new\)](#) [FOR844 \(new\)](#) [FOR845 \(new\)](#) [FOR846 \(new\)](#) [FOR847 \(new\)](#) [FOR848 \(new\)](#) [FOR849 \(new\)](#) [FOR850 \(new\)](#) [FOR851 \(new\)](#) [FOR852 \(new\)](#) [FOR853 \(new\)](#) [FOR854 \(new\)](#) [FOR855 \(new\)](#) [FOR856 \(new\)](#) [FOR857 \(new\)](#) [FOR858 \(new\)](#) [FOR859 \(new\)](#) [FOR860 \(new\)](#) [FOR861 \(new\)](#) [FOR862 \(new\)](#) [FOR863 \(new\)](#) [FOR864 \(new\)](#) [FOR865 \(new\)](#) [FOR866 \(new\)](#) [FOR867 \(new\)](#) [FOR868 \(new\)](#) [FOR869 \(new\)](#) [FOR870 \(new\)](#) [FOR871 \(new\)](#) [FOR872 \(new\)](#) [FOR873 \(new\)](#) [FOR874 \(new\)](#) [FOR875 \(new\)](#) [FOR876 \(new\)](#) [FOR877 \(new\)](#) [FOR878 \(new\)](#) [FOR879 \(new\)](#) [FOR880 \(new\)](#) [FOR881 \(new\)](#) [FOR882 \(new\)](#) [FOR883 \(new\)](#) [FOR884 \(new\)](#) [FOR885 \(new\)](#) [FOR886 \(new\)](#) [FOR887 \(new\)](#) [FOR888 \(new\)](#) [FOR889 \(new\)](#) [FOR890 \(new\)](#) [FOR891 \(new\)](#) [FOR892 \(new\)](#) [FOR893 \(new\)](#) [FOR894 \(new\)](#) [FOR895 \(new\)](#) [FOR896 \(new\)](#) [FOR897 \(new\)](#) [FOR898 \(new\)](#) [FOR899 \(new\)](#) [FOR900 \(new\)](#) [FOR901 \(new\)](#) [FOR902 \(new\)](#) [FOR903 \(new\)](#) [FOR904 \(new\)](#) [FOR905 \(new\)](#) [FOR906 \(new\)](#) [FOR907 \(new\)](#) [FOR908 \(new\)](#) [FOR909 \(new\)](#) [FOR910 \(new\)](#) [FOR911 \(new\)](#) [FOR912 \(new\)](#) [FOR913 \(new\)](#) [FOR914 \(new\)](#) [FOR915 \(new\)](#) [FOR916 \(new\)](#) [FOR917 \(new\)](#) [FOR918 \(new\)](#) [FOR919 \(new\)](#) [FOR920 \(new\)](#) [FOR921 \(new\)](#) [FOR922 \(new\)](#) [FOR923 \(new\)](#) [FOR924 \(new\)](#) [FOR925 \(new\)](#) [FOR926 \(new\)](#) [FOR927 \(new\)](#) [FOR928 \(new\)](#) [FOR929 \(new\)](#) [FOR930 \(new\)](#) [FOR931 \(new\)](#) [FOR932 \(new\)](#) [FOR933 \(new\)](#) [FOR934 \(new\)](#) [FOR935 \(new\)](#) [FOR936 \(new\)](#) [FOR937 \(new\)](#) [FOR938 \(new\)](#) [FOR939 \(new\)](#) [FOR940 \(new\)](#) [FOR941 \(new\)](#) [FOR942 \(new\)](#) [FOR943 \(new\)](#) [FOR944 \(new\)](#) [FOR945 \(new\)](#) [FOR946 \(new\)](#) [FOR947 \(new\)](#) [FOR948 \(new\)](#) [FOR949 \(new\)](#) [FOR950 \(new\)](#) [FOR951 \(new\)](#) [FOR952 \(new\)](#) [FOR953 \(new\)](#) [FOR954 \(new\)](#) [FOR955 \(new\)](#) [FOR956 \(new\)](#) [FOR957 \(new\)](#) [FOR958 \(new\)](#) [FOR959 \(new\)](#) [FOR960 \(new\)](#) [FOR961 \(new\)](#) [FOR962 \(new\)](#) [FOR963 \(new\)](#) [FOR964 \(new\)](#) [FOR965 \(new\)](#) [FOR966 \(new\)](#) [FOR967 \(new\)](#) [FOR968 \(new\)](#) [FOR969 \(new\)](#) [FOR970 \(new\)](#) [FOR971 \(new\)](#) [FOR972 \(new\)](#) [FOR973 \(new\)](#) [FOR974 \(new\)](#) [FOR975 \(new\)](#) [FOR976 \(new\)](#) [FOR977 \(new\)](#) [FOR978 \(new\)](#) [FOR979 \(new\)](#) [FOR980 \(new\)](#) [FOR981 \(new\)](#) [FOR982 \(new\)](#) [FOR983 \(new\)](#) [FOR984 \(new\)](#) [FOR985 \(new\)](#) [FOR986 \(new\)](#) [FOR987 \(new\)](#) [FOR988 \(new\)](#) [FOR989 \(new\)](#) [FOR990 \(new\)](#) [FOR991 \(new\)](#) [FOR992 \(new\)](#) [FOR993 \(new\)](#) [FOR994 \(new\)](#) [FOR995 \(new\)](#) [FOR996 \(new\)](#) [FOR997 \(new\)](#) [FOR998 \(new\)](#) [FOR999 \(new\)](#) [FOR1000 \(new\)](#)

### 02 Red Teamer (Adversary Emulation Specialist)

This role involves simulating the tactics, techniques, and procedures (TTPs) of a threat actor to identify and exploit vulnerabilities in an organization's systems and networks. Red teamers work to identify weaknesses in an organization's security posture and provide recommendations for improvement.

**Why is this role important?**  
Red teaming is a critical component of an organization's security program. It allows organizations to identify and address vulnerabilities in their systems and networks before they can be exploited by a real-world threat actor.

**Recommended courses**  
[SEC504 \(new\)](#) [SEC505 \(new\)](#) [SEC506 \(new\)](#) [SEC507 \(new\)](#) [SEC508 \(new\)](#) [SEC509 \(new\)](#) [SEC510 \(new\)](#) [SEC511 \(new\)](#) [SEC512 \(new\)](#) [SEC513 \(new\)](#) [SEC514 \(new\)](#) [SEC515 \(new\)](#) [SEC516 \(new\)](#) [SEC517 \(new\)](#) [SEC518 \(new\)](#) [SEC519 \(new\)](#) [SEC520 \(new\)](#) [SEC521 \(new\)](#) [SEC522 \(new\)](#) [SEC523 \(new\)](#) [SEC524 \(new\)](#) [SEC525 \(new\)](#) [SEC526 \(new\)](#) [SEC527 \(new\)](#) [SEC528 \(new\)](#) [SEC529 \(new\)](#) [SEC530 \(new\)](#) [SEC531 \(new\)](#) [SEC532 \(new\)](#) [SEC533 \(new\)](#) [SEC534 \(new\)](#) [SEC535 \(new\)](#) [SEC536 \(new\)](#) [SEC537 \(new\)](#) [SEC538 \(new\)](#) [SEC539 \(new\)](#) [SEC540 \(new\)](#) [SEC541 \(new\)](#) [SEC542 \(new\)](#) [SEC543 \(new\)](#) [SEC544 \(new\)](#) [SEC545 \(new\)](#) [SEC546 \(new\)](#) [SEC547 \(new\)](#) [SEC548 \(new\)](#) [SEC549 \(new\)](#) [SEC550 \(new\)](#) [SEC551 \(new\)](#) [SEC552 \(new\)](#) [SEC553 \(new\)](#) [SEC554 \(new\)](#) [SEC555 \(new\)](#) [SEC556 \(new\)](#) [SEC557 \(new\)](#) [SEC558 \(new\)](#) [SEC559 \(new\)](#) [SEC560 \(new\)](#) [SEC561 \(new\)](#) [SEC562 \(new\)](#) [SEC563 \(new\)](#) [SEC564 \(new\)](#) [SEC565 \(new\)](#) [SEC566 \(new\)](#) [SEC567 \(new\)](#) [SEC568 \(new\)](#) [SEC569 \(new\)](#) [SEC570 \(new\)](#) [SEC571 \(new\)](#) [SEC572 \(new\)](#) [SEC573 \(new\)](#) [SEC574 \(new\)](#) [SEC575 \(new\)](#) [SEC576 \(new\)](#) [SEC577 \(new\)](#) [SEC578 \(new\)](#) [SEC579 \(new\)](#) [SEC580 \(new\)](#) [SEC581 \(new\)](#) [SEC582 \(new\)](#) [SEC583 \(new\)](#) [SEC584 \(new\)](#) [SEC585 \(new\)](#) [SEC586 \(new\)](#) [SEC587 \(new\)](#) [SEC588 \(new\)](#) [SEC589 \(new\)](#) [SEC590 \(new\)](#) [SEC591 \(new\)](#) [SEC592 \(new\)](#) [SEC593 \(new\)](#) [SEC594 \(new\)](#) [SEC595 \(new\)](#) [SEC596 \(new\)](#) [SEC597 \(new\)](#) [SEC598 \(new\)](#) [SEC599 \(new\)](#) [SEC600 \(new\)](#) [SEC601 \(new\)](#) [SEC602 \(new\)](#) [SEC603 \(new\)](#) [SEC604 \(new\)](#) [SEC605 \(new\)](#) [SEC606 \(new\)](#) [SEC607 \(new\)](#) [SEC608 \(new\)](#) [SEC609 \(new\)](#) [SEC610 \(new\)](#) [SEC611 \(new\)](#) [SEC612 \(new\)](#) [SEC613 \(new\)](#) [SEC614 \(new\)](#) [SEC615 \(new\)](#) [SEC616 \(new\)](#) [SEC617 \(new\)](#) [SEC618 \(new\)](#) [SEC619 \(new\)](#) [SEC620 \(new\)](#) [SEC621 \(new\)](#) [SEC622 \(new\)](#) [SEC623 \(new\)](#) [SEC624 \(new\)](#) [SEC625 \(new\)](#) [SEC626 \(new\)](#) [SEC627 \(new\)](#) [SEC628 \(new\)](#) [SEC629 \(new\)](#) [SEC630 \(new\)](#) [SEC631 \(new\)](#) [SEC632 \(new\)](#) [SEC633 \(new\)](#) [SEC634 \(new\)](#) [SEC635 \(new\)](#) [SEC636 \(new\)](#) [SEC637 \(new\)](#) [SEC638 \(new\)](#) [SEC639 \(new\)](#) [SEC640 \(new\)](#) [SEC641 \(new\)](#) [SEC642 \(new\)](#) [SEC643 \(new\)](#) [SEC644 \(new\)](#) [SEC645 \(new\)](#) [SEC646 \(new\)](#) [SEC647 \(new\)](#) [SEC648 \(new\)](#) [SEC649 \(new\)](#) [SEC650 \(new\)](#) [SEC651 \(new\)](#) [SEC652 \(new\)](#) [SEC653 \(new\)](#) [SEC654 \(new\)](#) [SEC655 \(new\)](#) [SEC656 \(new\)](#) [SEC657 \(new\)](#) [SEC658 \(new\)](#) [SEC659 \(new\)](#) [SEC660 \(new\)](#) [SEC661 \(new\)](#) [SEC662 \(new\)](#) [SEC663 \(new\)](#) [SEC664 \(new\)](#) [SEC665 \(new\)](#) [SEC666 \(new\)](#) [SEC667 \(new\)](#) [SEC668 \(new\)](#) [SEC669 \(new\)](#) [SEC670 \(new\)](#) [SEC671 \(new\)](#) [SEC672 \(new\)](#) [SEC673 \(new\)](#) [SEC674 \(new\)](#) [SEC675 \(new\)](#) [SEC676 \(new\)](#) [SEC677 \(new\)](#) [SEC678 \(new\)](#) [SEC679 \(new\)](#) [SEC680 \(new\)](#) [SEC681 \(new\)](#) [SEC682 \(new\)](#) [SEC683 \(new\)](#) [SEC684 \(new\)](#) [SEC685 \(new\)](#) [SEC686 \(new\)](#) [SEC687 \(new\)](#) [SEC688 \(new\)](#) [SEC689 \(new\)](#) [SEC690 \(new\)](#) [SEC691 \(new\)](#) [SEC692 \(new\)](#) [SEC693 \(new\)](#) [SEC694 \(new\)](#) [SEC695 \(new\)](#) [SEC696 \(new\)](#) [SEC697 \(new\)](#) [SEC698 \(new\)](#) [SEC699 \(new\)](#) [SEC700 \(new\)](#) [SEC701 \(new\)](#) [SEC702 \(new\)](#) [SEC703 \(new\)](#) [SEC704 \(new\)](#) [SEC705 \(new\)](#) [SEC706 \(new\)](#) [SEC707 \(new\)](#) [SEC708 \(new\)](#) [SEC709 \(new\)](#) [SEC710 \(new\)](#) [SEC711 \(new\)](#) [SEC712 \(new\)](#) [SEC713 \(new\)](#) [SEC714 \(new\)](#) [SEC715 \(new\)](#) [SEC716 \(new\)](#) [SEC717 \(new\)](#) [SEC718 \(new\)](#) [SEC719 \(new\)](#) [SEC720 \(new\)](#) [SEC721 \(new\)](#) [SEC722 \(new\)](#) [SEC723 \(new\)](#) [SEC724 \(new\)](#) [SEC725 \(new\)](#) [SEC726 \(new\)](#) [SEC727 \(new\)](#) [SEC728 \(new\)](#) [SEC729 \(new\)](#) [SEC730 \(new\)](#) [SEC731 \(new\)](#) [SEC732 \(new\)](#) [SEC733 \(new\)](#) [SEC734 \(new\)](#) [SEC735 \(new\)](#) [SEC736 \(new\)](#) [SEC737 \(new\)](#) [SEC738 \(new\)](#) [SEC739 \(new\)](#) [SEC740 \(new\)](#) [SEC741 \(new\)](#) [SEC742 \(new\)](#) [SEC743 \(new\)](#) [SEC744 \(new\)](#) [SEC745 \(new\)](#) [SEC746 \(new\)](#) [SEC747 \(new\)](#) [SEC748 \(new\)](#) [SEC749 \(new\)](#) [SEC750 \(new\)](#) [SEC751 \(new\)](#) [SEC752 \(new\)](#) [SEC753 \(new\)](#) [SEC754 \(new\)](#) [SEC755 \(new\)](#) [SEC756 \(new\)](#) [SEC757 \(new\)](#) [SEC758 \(new\)](#) [SEC759 \(new\)](#) [SEC760 \(new\)](#) [SEC761 \(new\)](#) [SEC762 \(new\)](#) [SEC763 \(new\)](#) [SEC764 \(new\)](#) [SEC765 \(new\)](#) [SEC766 \(new\)](#) [SEC767 \(new\)](#) [SEC768 \(new\)](#) [SEC769 \(new\)](#) [SEC770 \(new\)](#) [SEC771 \(new\)](#) [SEC772 \(new\)](#) [SEC773 \(new\)](#) [SEC774 \(new\)](#) [SEC775 \(new\)](#) [SEC776 \(new\)](#) [SEC777 \(new\)](#) [SEC778 \(new\)](#) [SEC779 \(new\)](#) [SEC780 \(new\)](#) [SEC781 \(new\)](#) [SEC782 \(new\)](#) [SEC783 \(new\)](#) [SEC784 \(new\)](#) [SEC785 \(new\)](#) [SEC786 \(new\)](#) [SEC787 \(new\)](#) [SEC788 \(new\)](#) [SEC789 \(new\)](#) [SEC790 \(new\)](#) [SEC791 \(new\)](#) [SEC792 \(new\)](#) [SEC793 \(new\)](#) [SEC794 \(new\)](#) [SEC795 \(new\)](#) [SEC796 \(new\)](#) [SEC797 \(new\)](#) [SEC798 \(new\)](#) [SEC799 \(new\)](#) [SEC800 \(new\)](#) [SEC801 \(new\)](#) [SEC802 \(new\)](#) [SEC803 \(new\)](#) [SEC804 \(new\)](#) [SEC805 \(new\)](#) [SEC806 \(new\)](#) [SEC807 \(new\)](#) [SEC808 \(new\)](#) [SEC809 \(new\)](#) [SEC810 \(new\)](#) [SEC811 \(new\)](#) [SEC812 \(new\)](#) [SEC813 \(new\)](#) [SEC814 \(new\)](#) [SEC815 \(new\)](#) [SEC816 \(new\)](#) [SEC817 \(new\)](#) [SEC818 \(new\)](#) [SEC819 \(new\)](#) [SEC820 \(new\)](#) [SEC821 \(new\)](#) [SEC822 \(new\)](#) [SEC823 \(new\)](#) [SEC824 \(new\)](#) [SEC825 \(new\)](#) [SEC826 \(new\)](#) [SEC827 \(new\)](#) [SEC828 \(new\)](#) [SEC829 \(new\)](#) [SEC830 \(new\)](#) [SEC831 \(new\)](#) [SEC832 \(new\)](#) [SEC833 \(new\)](#) [SEC834 \(new\)](#) [SEC835 \(new\)](#) [SEC836 \(new\)](#) [SEC837 \(new\)](#) [SEC838 \(new\)](#) [SEC839 \(new\)](#) [SEC840 \(new\)](#) [SEC841 \(new\)](#) [SEC842 \(new\)](#) [SEC843 \(new\)](#) [SEC844 \(new\)](#) [SEC845 \(new\)](#) [SEC846 \(new\)](#) [SEC847 \(new\)](#) [SEC848 \(new\)](#) [SEC849 \(new\)](#) [SEC850 \(new\)](#) [SEC851 \(new\)](#) [SEC852 \(new\)](#) [SEC853 \(new\)](#) [SEC854 \(new\)](#) [SEC855 \(new\)](#) [SEC856 \(new\)](#) [SEC857 \(new\)](#) [SEC858 \(new\)](#) [SEC859 \(new\)](#) [SEC860 \(new\)](#) [SEC861 \(new\)](#) [SEC862 \(new\)](#) [SEC863 \(new\)](#) [SEC864 \(new\)](#) [SEC865 \(new\)](#) [SEC866 \(new\)](#) [SEC867 \(new\)](#) [SEC868 \(new\)](#) [SEC869 \(new\)](#) [SEC870 \(new\)](#) [SEC871 \(new\)](#) [SEC872 \(new\)](#) [SEC873 \(new\)](#) [SEC874 \(new\)](#) [SEC875 \(new\)](#) [SEC876 \(new\)](#) [SEC877 \(new\)](#) [SEC878 \(new\)](#) [SEC879 \(new\)](#) [SEC880 \(new\)](#) [SEC881 \(new\)](#) [SEC882 \(new\)](#) [SEC883 \(new\)](#) [SEC884 \(new\)](#) [SEC885 \(new\)](#) [SEC886 \(new\)](#) [SEC887 \(new\)](#) [SEC888 \(new\)](#) [SEC889 \(new\)](#) [SEC890 \(new\)](#) [SEC891 \(new\)](#) [SEC892 \(new\)](#) [SEC893 \(new\)](#) [SEC894 \(new\)](#) [SEC895 \(new\)](#) [SEC896 \(new\)](#) [SEC897 \(new\)](#) [SEC898 \(new\)](#) [SEC899 \(new\)](#) [SEC900 \(new\)](#) [SEC901 \(new\)](#) [SEC902 \(new\)](#) [SEC903 \(new\)](#) [SEC904 \(new\)](#) [SEC905 \(new\)](#) [SEC906 \(new\)](#) [SEC907 \(new\)](#) [SEC908 \(new\)](#) [SEC909 \(new\)](#) [SEC910 \(new\)](#) [SEC911 \(new\)</](#)

Ukrayna Devleti olarak ilk hibrit savařla karşı karşıyayız. Karada olduđu gibi siber uzayda da savařıyoruz. Elektrik řebekelerimize, nükleer santrallerimize, İletiřim hatlarımıza ve siber vatanımızdaki diđer kurum ađlarımıza yapılan saldırılar karşısında siber savunma geliřtiriyoruz!

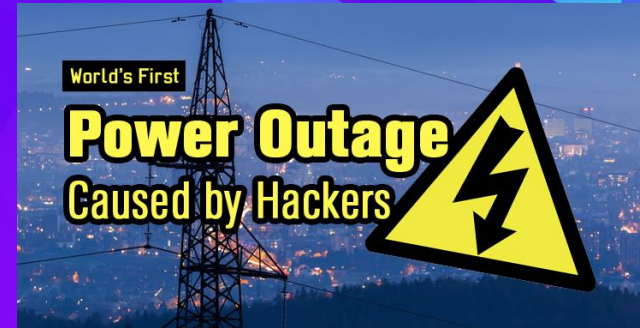
Viktor Zahora, Ukrayna Başkan Yardımcısı



# Ukrayna Siber Saldırıları-2016



Phishing  
mailleri



# 2007 Estonya

- Estonya hükümetinin Talin meydanında bulunan Rus meçhul asker anıtını sökülmesine karar vermesi üzerine başlayan DDoS karakterli siber saldırılar sonucunda;
- Hükümet Siteleri,
- Bankalar,
- Kamu Kurumlarının Bilişim Sistemleri,
- Kritik Altyapı Sektörleri,
- Trafik ışıkları dahil... Felç edilmiştir.

GROUP	SUPPORTING	ATTACKS	COMMS	LOC	Date started
AgainstTheWest (ATW)	Ukraine	Data Breach & ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	FEB 2022
GhostSec	Ukraine	Hack	Telegram	UNK	FEB 2022
IT Army of Ukraine	Ukraine	DDoS	Telegram	Ukraine	FEB 2022
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	FEB 2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	FEB 2022
Anonymous Liberland & the PWN-BAR hack team	Ukraine	DDoS	Twitter	Global	FEB 2022
Raidforums Admin	Ukraine	Sanction	Raidforums	UNK	FEB 2022
Netsec	UNK	Hack	Twitter	UNK	FEB 2022
Free Civilian	Russia	Data Breach	Onion	UNK	JAN 2022
Cooming Project	Russia	Data Breach	Onion	UNK	2021
Conti Ransomware	Russia	Ransomware	Onion	Russia	2019
The Red Bandits	Russia	Data Breach	Twitter	Russia	2021
CyberGhost	Russia	Hack	UNK	Belarus	UNK
SandWorm	Russia	Hack & DDoS	UNK	Russia	UNK
28 FEB	----	-----	-----	-----	-----
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
Raidforums2	Ukraine	DDoS	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hacks/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hacks/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belarus	Hacks	Twitter	Global	2022





# Stuxnet 2009

- İran'daki nükleer tesiste santifrjlerin imha olmasına sebep olan virüsün, **USB ile sisteme sızdığı** değerlendirilmektedir.
- Stuxnet virüsü, uranyum zenginleştirmek için kullanılan santrafjleri yöneten **SCADA sistemlerini hedef almıştır**,
- Sistemlerin internet ile bağlantısı sanal hava boşluğu ile sağlanıyor olmasına rağmen **8700 santrafjün 2200'ü imha** olmuştur,



# Colonial Pipeline



Colonial Pipeline, Teksas'tan New York'a kadar benzin, dizel ve jet yakıtı taşıyan **ABD'nin en büyük petrol boru hattı**,



Saldırganlar ayrıca yaklaşık **100 gigabayt** veriyi çaldı ve fidyenin ödenmemesi halinde bunları **internette yayınlamakla** tehdit etti.



Saldırının birincil hedefi şirketin **faturalandırma altyapısı** tamamen **ransomware** ile kilitlenmiştir.



Saldırdan sonra şirketin, bir şifre çözme aracı karşılığında bilgisayar korsanlarına yaklaşık **75 Bitcoin (5 milyon dolar)** fidye ödendiği tahmin ediliyor,



# Dünyada Ses Getiren Siber Saldırılar

- Melissa Virüsü (1999)
- Nasa Siber Saldırısı (1999)
- Estonya Siber Saldırısı (2007)
- Sony Playstation Ağı Siber Saldırısı (2011)
- Adobe Systems Siber Saldırısı (2013)
- Yahoo Siber Saldırısı (2013)
- Ukrayna Elektrik Şebekesi Siber Saldırısı (2015)
- WannaCry Ransomware (2017)
- Marriott Otelleri Siber Saldırısı (2018)
- RockYou2021 (2021)
- İran Siber Saldırıları (2010-2021)
- Türkiye Root DNS (Nic. TR) Saldırıları (2015)
- Rusya'nın Ukrayna Saldırısı (2017-2022)
- Sri Lanka Siber Saldırıları (2019-2020-2021)
- OpsIsrael Cyber Attacks
- Romania Cyber Attacks (2022)

# Dünyada Ses Getiren Siber Saldırıları

1. **Melissa Virüsü:** Microsoft'un tüm sistemlerini çökertip 80 milyon dolarlık hasar bıraktı.
2. **NASA Siber Saldırısı:** 15 yaşında bir çocuk, NASA'nın 41.000 dosyasını indirdi..
3. **Estonya Siber Saldırısı:** Dünya tarihinde ülkeler arasındaki ilk siber saldırı bir Avrupa ülkesi olan Estonya'da yaşandı. Estonya'ya ait banka ve medya kuruluşlarının web siteleri ele geçirildi.
4. **Sony Playstation Ağı Siber Saldırısı:** Kullanıcılar online servislere erişemezken, 100 milyondan fazla kişinin şahsi bilgileri de çalındı.
5. **Adobe Systems Siber Saldırısı:** 2.9 milyon müşterisinin kredi kartı ve parola bilgilerinin de ele geçirildi.
6. **Yahoo Siber Saldırısı:** 500 milyon kişinin hesabı hackerların eline geçti..
7. **Ukrayna Elektrik Şebekesi Siber Saldırısı:** 225 bin kişi elektriksiz kaldı. Enerji firmaları, saldırının BlackEnergy virüsü aracılığı ile gerçekleştiğini belirtti.
8. **WannaCry Ransomware:** Melissa Virüsü'nün ardından bir de WannaCry. Microsoft Windows'u hedef alan WannaCry virüsü, 2017 yılında 150'den fazla ülkede yaklaşık 200 bin bilgisayara ulaştı. Saldırının küresel maliyeti toplamda 6 milyar Sterlin oldu.
9. **Marriott Otelleri Siber Saldırısı:** 339 milyon misafirin kişisel bilgileri çalındı. Bir süre gizli tutulan ancak 2018 yılında ortaya çıkan bu olay sonrası İngiltere Hükümeti, Marriot Hotels'a 18.4 milyon Sterlin para cezası kesti.
10. **RockYou2021:** Siber saldırı tarihindeki en büyük şifre hırsızlıklarından bir, 8.4 milyar çalıntı şifreden oluşan 100 GB'lık bir TXT dosyası..
11. **Bitcoin Saldırısı ile 148.000.000.000 BTC üretim atağı**



Hollanda Savunma Bakanlığı Hacklendi.  
Yine Fortinet - Yine Zeroday vakası...

Siber casuslar, ABD'li ağ güvenliği şirketi Fortinet'in FortiGate Firewall cihazlarındaki bir 0-day zafiyetini kullanarak, Coathanger adı verilen kötü amaçlı yazılımla bakanlığın sistemlerine sızmışlar..

Hollanda Savunma Bakanlığı Hacklendi!: Hollanda Savunma Bakanlığından 6 Şubat 2024'te yapılan açıklamada, Hollanda İstihbarat Servisi (AIVD) ve Hollanda Askeri İstihbarat Servisinin (MIVD), Çinli siber casusların Bakanlığın ağına sızarak bir yıldır gizlice izlediğini tespit ettikleri belirtildi.

Hollanda Savunma Bakanı Kajsja Ollongren, siber casusluk operasyonunun Çin istihbarat servisleri tarafından gerçekleştirildiğini doğruladı.

(Haber Hollanda Savunma .nl haber alınmıştır)



## Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT

*This advisory is a joint publication of the MIVD and AIVD, the intelligence and security services of the Netherlands. An accompanying press release was published on the website of the Ministry of Defence of the Netherlands.*



### 1. Overview

- The Ministry of Defence (MOD) of the Netherlands was impacted in 2023 by an intrusion into one of its networks. The effects were limited because of prior network segmentation.
- Incident response uncovered previously unpublished malware, a remote access trojan (RAT) designed specifically for Fortigate appliances. It is used as second-stage malware, and does *not* exploit a new vulnerability. Intelligence services MIVD & AIVD refer to the malware as COATHANGER based on a string present in the code.
- The COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that could reveal its presence. It survives reboots and firmware upgrades.
- MIVD & AIVD assess with high confidence that the malicious activity was conducted by a state-sponsored actor from the People's Republic of China.

limited because the victim network was segmented from the wider MOD networks.

The victim network had fewer than 50 users. Its purpose was research and development (R&D) of unclassified projects and collaboration with two third-party research institutes. These organizations have been notified of the incident.

### 2.1 Attribution

MIVD & AIVD assess with high confidence that the intrusion at the MOD, as well as the development of the malware described in this report, was conducted by a state-sponsored actor from the People's Republic of China.

MIVD & AIVD emphasize that this incident does not stand on its own, but is part of a wider trend of Chinese political espionage against the Netherlands and its allies.



01

Dış Erişim  
Kısıtlama

02

Dos/DDoS Atağı  
Engelleme

03

Web Uygulama  
Güvenlik Duvarı Güvenliği

04

Güncellemeler  
Güvenlik Yama Yönetimi

05

Erişim ve Yetkilerin  
Düzenli Kontrolü

06

Yedekleme  
Yedekten Geri Dönme

07

Katmanlı Güvenlik  
Mimarileri  
(Güvenlik Duvarı,  
DMZ)

08

Sosyal  
Mühendislik  
Önlemleri

09

SOME  
Müdahale Planları



## Deep Security

### Network Security



Intrusion  
Prevention



Firewall



Vulnerability  
Scanning

### System Security



Application  
Control



Integrity  
Monitoring



Log  
Inspection

Workload Security License

### Malware Prevention



Anti-  
Malware



Behavioral  
Analysis



Machine  
Learning

### Detection & Response (activity monitoring)



Detect



Respond

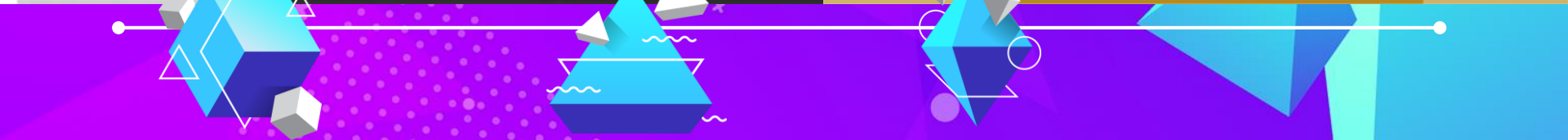
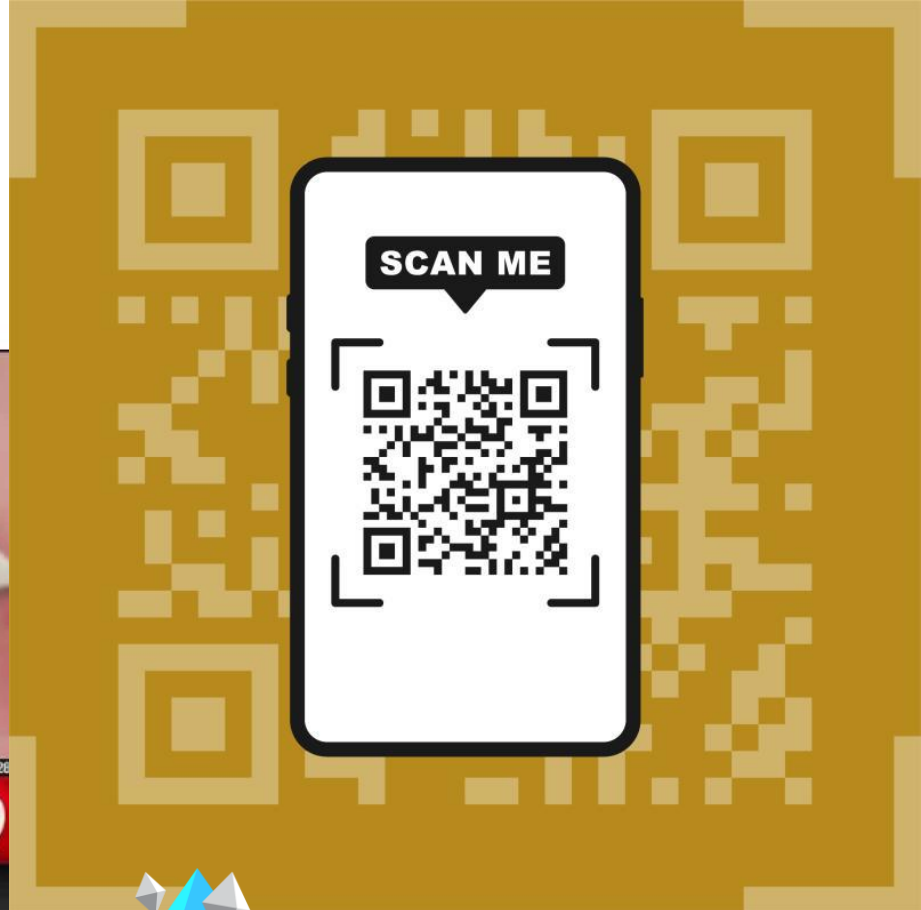


Investigate

Scammers now have the technology to not only spoof your loved one's phone number but even clone their voice. Watch Managing Director of Remediation Services **Paul Sems** and Mobile and Hardware Security Practice Lead **Robert Simon** discuss and demonstrate AI voice cloning on Cleveland 19 News.

#AI #VoiceCloning #security #scams

<https://hubs.la/Q02kHBJs0>



# YAKIN GELECEKTE BEKLENENİ

- Bir siber saldırı sonrasında G20 ülkelerinden birinin bu saldırıya fiziki saldırı ile karşılık vereceği,
- Kritik altyapılarda geleneksel siber güvenlik tedbirlerinin ve ürünlerinin yaklaşık %80'ninin değiştirileceği,
- Cyber-Physical Systems diye yeni bir güvenlik kategorisinin oluşacağını,
- Bu alanla ilgili devletlerin çeşitli regülasyonlar yayınlayacağını,
- Hızla bu regülasyonlara uyum için yatırımlar yapılacağı değerlendirilmekte.

# Sunum Akışı

1

Dijitalleşme

2

Siber Güvenlik

3

Bilinçli İnternet Kullanımı

4

Bilinçli Sosyal Medya Kullanımı

5

Cihaz Siber Güvenliği

6

Siber Dolandırıcılık  
Siber Zorbalık

Dikkatsiz internette gezinmek veri ihlallerine yol açarak hassas kişisel ve finansal bilgilerin siber suçluların eline geçmesine neden olabilir.

Kimlik hırsızlığı, saldırganların kişisel bilgilerinizi adınıza dolandırıcılık veya diğer yasa dışı faaliyetlerde bulunmak için kullanabileceği bir başka ciddi sonuçtur.

Çevrimiçi güvenliği artırmak için, güvenlik açıklarını düzeltmek üzere yazılımınızı ve tarayıcılarınızı düzenli olarak güncelleyin.

Farklı siteler için güçlü, benzersiz şifreler kullanın ve bunları güvenli bir şekilde takip etmek için bir şifre yöneticisi kullanmayı düşünün.

Mümkün olduğunda iki faktörlü kimlik doğrulamayı (2FA) etkinleştirerek yalnızca parolaların ötesinde ekstra bir güvenlik katmanı ekleyin.



# Sunum Akışı

1

Dijitalleşme

2

Siber Güvenlik

3

Bilinçli İnternet Kullanımı

4

Bilinçli Sosyal Medya Kullanımı

5

Cihaz Siber Güvenliği

6

Siber Dolandırıcılık  
Siber Zorbalık

Sosyal medyanın yoğun kullanımı, sürekli karşılaştırma ve gerçekçi olmayan beklentileri karşılama baskısı nedeniyle kaygı, depresyon ve yalnızlık gibi zihinsel sağlık sorunlarının artan riskleriyle ilişkilendirilmiştir.

Başkalarının hayatlarının seçilmiş önemli anlarına sürekli olarak maruz kalmak, kişisel öz saygıyı ve beden imajını çarpıtarak, olumsuz zihinsel sağlık sonuçlarına katkıda bulunabilir.

Gizlilik ayarları, kişisel bilgilerin korunmasında ve çevrimiçi etkileşimlerin yönetilmesinde önemli bir rol oynayarak siber zorbalık ve yetkisiz veri erişimi risklerinin azaltılmasına yardımcı olur.

Sosyal medya platformlarındaki gizlilik ayarlarının düzenli olarak gözden geçirilmesi ve düzenlenmesi, kişisel verilerin izinsiz olarak ticari kullanım amacıyla kullanılmasının önüne geçebilir.

Sık sık gizlilik kontrolleri yapmak ve neyin paylaşılacağı konusunda seçici olmak da dahil olmak üzere, sosyal medya kullanımına duyarlı bir yaklaşımın teşvik edilmesi, zihinsel sağlık üzerindeki olumsuz etkileri önemli ölçüde azaltabilir ve kişisel bilgileri koruyabilir.

# Sunum Akışı

1

Dijitalleşme

2

Siber Güvenlik

3

Bilinçli İnternet Kullanımı

4

Bilinçli Sosyal Medya Kullanımı

5

Cihaz Siber Güvenliği

6

Siber Dolandırıcılık  
Siber Zorbalık



Düzenli güncellemeler, bilgisayar korsanlarının yararlanabileceği güvenlik açıklarını düzelttiğinden, yazılımı güncel tutmak siber güvenlik açısından temel öneme sahiptir.

Güvenilir antivirüs yazılımı kullanmak, kötü amaçlı yazılımlara, fidye yazılımlarına ve diğer kötü amaçlı siber tehditlere karşı önemli bir savunma katmanı sağlar.

Her çevrimiçi hesap için güçlü, benzersiz şifreler oluşturmak, yetkisiz erişimi önlemek ve veri ihlali riskini azaltmak açısından çok önemlidir.

Çok faktörlü kimlik doğrulama (MFA), dijital hesaplarınıza erişim sağlamak için iki veya daha fazla doğrulama yöntemi gerektiren ek bir güvenlik katmanı ekler ve güvenlik ihlali riskini önemli ölçüde azaltır.

Kendini ve başkalarını bu uygulamaların önemi konusunda eğitmek, genel dijital güvenliğini artırır ve hassas kişisel ve finansal bilgilerin korunmasına yardımcı olur.

# Sunum Akışı

1

Dijitalleşme

2

Siber Güvenlik

3

Bilinçli İnternet Kullanımı

4

Bilinçli Sosyal Medya Kullanımı

5

Cihaz Siber Güvenliği

6

Siber Dolandırıcılık  
Siber Zorbalık

Bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.

**En yaygın 5 siber dolandırıcılık yöntemi**

**Para kuryesi dolandırıcılığı**

**Piyango ve ödül dolandırıcılığı**

**Vergi dolandırıcılığı**

**Yatırım dolandırıcılığı**

**Sipariş dolandırıcılığı**

**10.02.2024 |** Batman İl Emniyet Müdürlüğü'nden yapılan açıklamada, ocak ayı içerisinde yürütülen çalışmalar kapsamında "Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle Dolandırıcılık" suçundan aranan 204 şüpheli şahsın yakalandığı bildirildi.

Kimlik avı e-postalarını ve dolandırıcılık web sitelerini tanımak, siber dolandırıcılığı önlemenin anahtarıdır; kişisel veya finansal bilgi talep eden istenmeyen iletişime karşı dikkatli olun.

Kimlik avı girişimleri genellikle meşru işletmeleri veya kişileri taklit eder ancak olağandışı e-posta adresleri, yazım hataları ve şüpheli bağlantılar kontrol edilerek tespit edilebilir.

Hassas bilgileri girmeden önce web sitelerinin orijinalliğini doğrulamak, kimlik hırsızlığının önlenmesine yardımcı olur; "https://" ve kilit simgesi gibi güvenli bağlantı göstergelerini arayın.

Kişisel bilgi taleplerine yanıt vermeden önce, özellikle de beklenmedik bir şekilde iletişime geçilmesi durumunda, kaynağı her zaman doğrudan resmi kanallar aracılığıyla doğrulayın.

Kendinizi ve başkalarını siber suçluların kullandığı ortak taktikler konusunda eğitmek, siber dolandırıcılığın kurbanı olma riskini önemli ölçüde azaltabilir.

Siber zorbalık, bireyleri taciz etmek, tehdit etmek veya utandırmak için dijital platformların kullanılmasını içerir ve çoğu zaman önemli duygusal ve psikolojik sıkıntılara yol açar.

Etkilerini anlamak çok önemlidir; Mağdurlar kaygı, depresyon ve ağır vakalarda intihar düşünceleri yaşayabilir; bu da etkili önleme ve müdahale stratejilerine olan ihtiyacın altını çizer.

Çevrimiçi deneyimler hakkında açık diyalogu teşvik etmek ve destekleyici bir ortam oluşturmak, mağdurların kendilerini daha az yalnız hissetmelerine ve yardım arama konusunda daha güçlü olmalarına yardımcı olabilir.

Mağdurlar ve olaya tanık olan kişiler, zorbayla etkileşime girmemek, istismarı belgelemek ve ilgili makamlara veya platformlara bildirmek de dahil olmak üzere siber zorbalığa nasıl müdahale edecekleri konusunda eğitilmelidir.

Okullar, aileler ve çevrimiçi topluluklar, güvenli dijital ortamlar oluşturmada, çevrimiçi nezaketi, saygıyı ve sorumluluğu teşvik etmede hayati bir rol oynamaktadır.

## Siber Zorbalık

Instagram ve Facebook'un çatı kuruluđu olan Meta'nın Ocak ayı ortasında kamuoyuyla paylaşılan şirket içi belgelerine göre, her gün kendi platformlarında 100 bin kadar çocuk çevrimiçi cinsel istismara uğruyor.

Meta'da yapılan bir iç yazışmada, bir çalışanın diğerine "çocukların çevrimiçi pazarlanması konusunda spesifik olarak ne yapıyoruz?" şeklindeki sorusuna başka bir çalışan: "sıfır ile neredeyse hiç arasında bir yerdeyiz"!

Instagram'da 13-15 yaş aralığındaki sekiz çocuktan birinin, cinsel saldırılara maruz kaldıkları tespit edilmiştir!

Geçtiğimiz hafta Ankara merkezli 20 ilde sosyal medyadan çocukların cinsel istismarıyla ilgili ürettiği içerikleri paylaştığı, sosyal medya araçlarında sohbet uygulamalarında çocuklarla aktif temas kurduğu ileri sürülen 35 şüpheli eş zamanlı bir operasyonla gözaltına alındı.

Ancak işin bir de dijital okuryazarlık ve farkındalık boyutu var ve polisiye tedbirlerin bu yönde bir eğitimle el ele ilerlemesi şart.

# SİBER ZORBALIKTAN KORKMA!



Siber Zorbalık; İnternet ortamındaki aşağılama, iftira, dedikodu, taciz, tehdit, dışlama, rencide etme amaçlı davranışlardır. Siber zorbalığa uğruyorsanız bunun sizin suçunuz olmadığını ve herkesin başına gelebileceğini unutmayın. Yukarıdaki tavsiyelere uyarak siber zorbalığın olumsuz etkilerinden korunun.

güvenli  
internet

"seçmek  
özgürdür"



TAMAMEN  
ÜCRETSİZ

Güvenli İnternet Hizmeti 7 Yaşında

GÜVENLİ İNTERNET  
HİZMETİ İLE  
DAHA GÜVENLİ BİR  
GELECEK

Seçmek  
Özgürlük tür

İstedığınız zaman ücretsiz  
olarak profilinizi değiştirebilir  
ya da hizmet almayı  
bırakabilirsiniz.



güvenli  
internet  
hizmeti

[www.guvenlinet.org](http://www.guvenlinet.org)

Güvenli İnternet Hizmeti,  
sizi ve ailenizi İnternetteki  
zararlı içeriklerden  
korur.



Güvenli İnternet Hizmeti  
iki profilden oluşmaktadır.



Profilinizi belirleyin;  
- Aile Profili  
- Çocuk Profili



SMS ile  
ücretsiz olarak  
seçebilirsiniz.

Ücretsizdir  
Kurulum gerektirmez



Kullanıcıları İnternetteki  
zararlı içeriklerden  
yüksek oranda  
korur.



Güvenli İnternet Hizmetinde  
arama motorları  
"Güvenli Arama"  
özellliği ile çalışır.

İnternet Servis Sağlayıcınızın  
online işlem merkezinden ya da  
çağrı merkezinden de ücretsiz  
olarak seçebilirsiniz.



SMS İLE  
AİLE PROFİLİNE ÜCRETSİZ GEÇİŞ

OPERATÖR	YAZ	GÖNDER
TURKCELL	: GÜVENLİ AİLE	2200
SUPERONLINE*	: AİLE HİZMETNO	2220
TÜRK TELEKOM	: EVET	3399
TTNET	: AİLE	6606
VODAFONE	: AİLE	7005
TURKSAT*	: AİLE HİZMETNO	5126
DSMART*	: PRAİLE HİZMETNO	2850
TURKNET	: AİLE	3371

\* HİZMETNO: Abonelik Numaranız

SMS İLE  
ÇOCUK PROFİLİNE ÜCRETSİZ GEÇİŞ

OPERATÖR	YAZ	GÖNDER
TURKCELL	: GÜVENLİ ÇOCUK	2200
SUPERONLINE*	: ÇOCUK HİZMETNO	2220
TÜRK TELEKOM	: EVET	3399
TTNET	: ÇOCUK	6606
VODAFONE	: ÇOCUK	7005
TURKSAT*	: ÇOCUK HİZMETNO	5126
DSMART*	: PROÇOCUK HİZMETNO	2850
TURKNET	: ÇOCUK	3371

\* HİZMETNO: Abonelik Numaranız





## Sosyal Ağlar Manipölasyon ve Dezenformasyon İerir!

**Teyit EtmediĐiniz hibir bilgiye itibar etmeyin, Özelinizi paylaşmayın.  
Kendinizi ve Ailenizi Koruyun!**

İnternette gizlenen bir tehdit var. Mali durumunuzu yok etme, kişisel verilerinizi çalma ve hayatınızı tehlikeye atma gücüne sahip gizli bir savaş.

[Spam Nation, Brian Krebs – New York Times Best Seller]

**BONUS** | **OYUNLAŐTIRMA**



# OYUNLAŐTIRILMIŐ DERS PLANI 32

**DERS** : İngilizce  
**KONU** : Weather Cyle  
**SINIF** : 5  
**SÜRE** : 5 Gün

## **KAZANIM :**

1. Hava durumu ve iklim arasındaki farkı ayırt eder.
2. Meteoroloji uzmanı ve hava tahmircisi arasındaki farkı ayırt eder.
3. İklim türlerini ifade eder, gruplara ayırabilir.
4. Hangi iklim türünde hangi ev türünün olabileceğini bilir.





Civilization VI



SimCity



Türkiye'de;

31  
Kuluçka  
Merkezi

5  
Venture  
Builder

11  
Girişim Sermayesi  
Yatırım Ortaklığı  
(Fon büyüklüğü  
575 Milyon dolar)

109  
Girişim  
Sermayesi  
Yatırım Fonu  
(Fon büyüklüğü  
810 Milyon  
dolar)

3  
SPK tarafından  
listelenmiş Kitle  
Fonlama Şirketi

1  
Aktif Paya  
Dayalı Kitle  
Fonlama  
Platformu

643  
Melek  
Yatırımcı

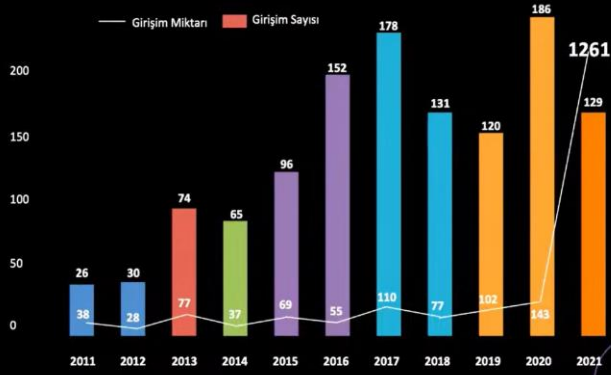
14  
Melek  
Yatırım  
Ağı

Türk Girişim  
Ekosisteminin değeri:

**4.1 milyar USD**

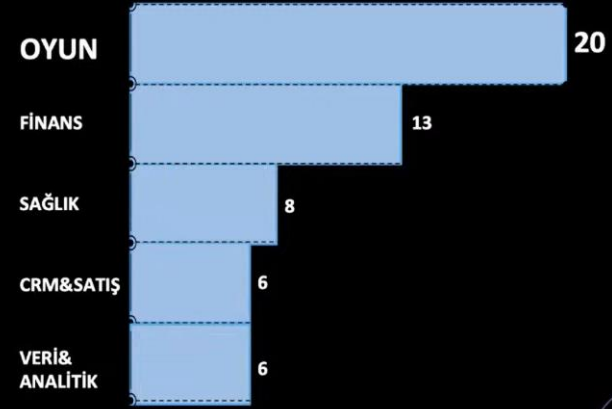


## TÜRKİYE'DEKİ GİRİŞİM YATIRIMLARI



2020'nin 2. yarısından 2021'in ilk yarısına kadar yapılan yatırım tutarı, 2011'in 2. yarısından 2020'nin ilk yarısına kadar olan toplam yatırım tutarının yaklaşık 2 katıdır.

## 2021 – ilk 6 ay – Yatırım alan girişim sayısı



8 EKİM 2022

Elyzio, vgames liderliğinde gerçekleşen yatırım turunda 2 milyon dolar yatırım aldı. Yatırım turuna vgames'in haricinde ise kripto ve web3 odaklı yatırım fonlarından Shima Capital, Solana Ventures, Paribu Ventures ile melek yatırımcı Abdelmounaim Derraz da katıldı. Elyzio aldığı bu yatırımı blockchain bazlı bir oyun evreni kurmak için kullanacak. Elyzio Blockchain altyapısı üzerinde yeni nesil yüksek kaliteli ve ücretsiz oynanabilen oyunlar geliştirmeyi amaçlayan bir girişim Elyzio tarafından aktarılan bilgilere göre alınan 2 milyon dolarlık yatırım, girişiminin ekibini büyütmesi ve ilk oyunu olan Warden's Will'e odaklanması için de kullanılacak.

# Bazı Başarılı Türk Oyun Girişimleri

Peak Games (Zynga 1,8B USD)

Dream Games

Gram Games (Zynga 250M USD)

Rollic Games (Zynga 200M USD)

Masamo (MiniClip 200M USD)

Tale Worlds

Ruby Games (Rovio)

Alictus

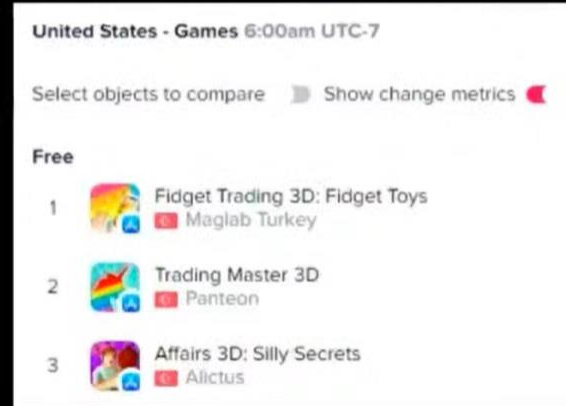
Good Job

Magic Lab

Loop Games

APPS

ODTU Teknokent ATOM Mezunları;  
MagicLab Game Technologies, Panteon  
ve Alictus oyunları ABD'de top



**Türkiye'de 1000den fazla oyun stüdyosu bulunmaktadır.**

**PEAK GAMES'I ALAN ZYNGA YONETICISI BERNARD KIM KONUSTU:  
1.8 MİLYAR DOLARI O EKİBE VERDİK**



**GAMING  
INDUSTRY  
IN TURKEY**  
[www.gaminginturkey.com](http://www.gaminginturkey.com)

**ZYNGA  
ACQUIRED  
MOBILE GAME  
DEVELOPER  
GRAM GAMES  
FOR \$250  
MILLION!**



**TÜRK OYUN FİRMASI  
168 MİLYON DOLARA  
ZYNGA'YA SATILDI!**



**HUNTER  
ASSASSIN**

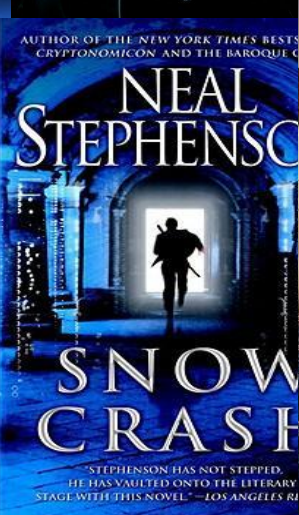
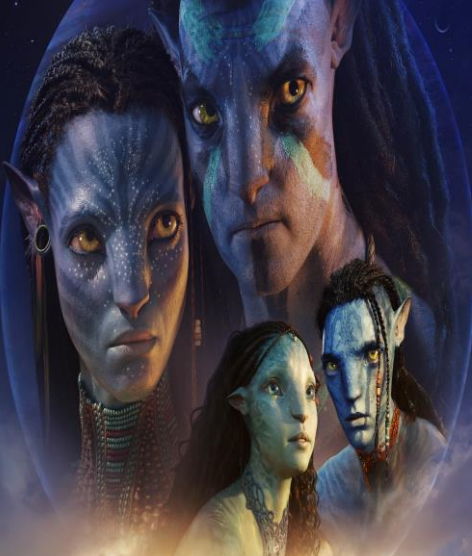
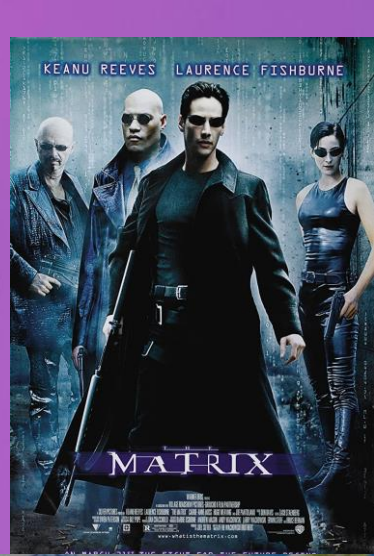
**ANGRY BIRDS**

Angry Birds'ün geliştiricisi talip oldu

**TÜRK OYUN ŞİRKETİNİ  
SATIN ALIYORLAR**

**BONUS**

**METaverse**  
**AR, VR, MR**





**V**irtual  
**R**eality

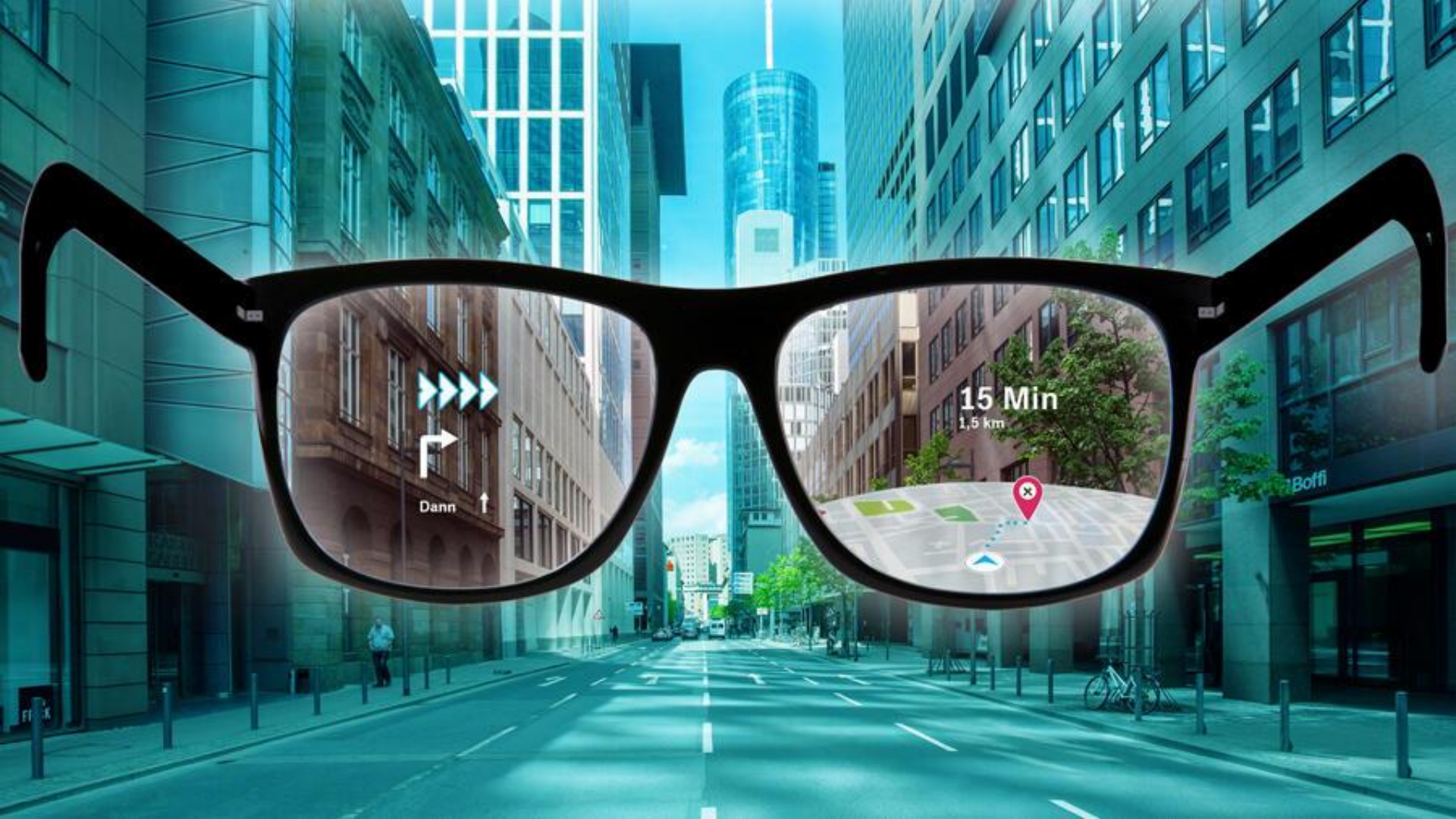


**A**ugmented  
**R**eality



**M**ixed  
**R**eality





Dann



15 Min  
1,5 km



Boffi



## Web 1.0

"Read Only",  
Decentralized



## Web 2.0

Participatory,  
Centralized



## Web 3

No Intermediaries,  
Decentralized



**i** IMMERSED'S METAVERSE MARKET MAP 2022 (V2)  
 AS WE BRING THE WORLD'S ECONOMY INTO VR, WE WANTED TO HIGHLIGHT SOME OF THE BEST METAVERSE APPLICATIONS LEADING THE WAY IN 2022.

<p><b>FOCUS</b> Tagging and end-user experience</p>	<p><b>FOCUS</b> User empowerment through trust, security, and privacy</p>
<p><b>TECHNOLOGY</b> AJAX and JavaScript</p>	<p><b>TECHNOLOGY</b> Semantic Web, AI, Decentralized technologies</p>
<p><b>OWNERSHIP</b> Owned by the network</p>	<p><b>OWNERSHIP</b> Owned by an entity &amp; shared through the network</p>
<p><b>3D GRAPHICS</b> No</p>	<p><b>3D GRAPHICS</b> Yes</p>



<p><b>TARGET REACH</b> Community</p>	<p><b>TARGET REACH</b> Individual</p>
<p><b>TYPE OF APPLICATIONS</b> Web Applications</p>	<p><b>TYPE OF APPLICATIONS</b> Smart applications that leverage AI and ML</p>
<p><b>ADVERTISING</b> Interactive advertising</p>	<p><b>ADVERTISING</b> Behavioral advertising</p>

<p><b>Hardware</b> Hardware infrastructure on which Metaverse applications are built on top of.</p> <p>Meta Quest ByteDance PlayStation.VR Apple VIVE Microsoft HoloLens VALVE Magic Leap</p>	<p><b>Decentralized Worlds</b> Platforms where users have the freedom to control their own digital assets.</p> <p>SANDBOX Decentraland immersed WILDER WORLD SOMNIUM SPACE neos WORLDWIDE WEBB CRYPTOVOXELS</p>	<p><b>Centralized Worlds</b> Metaverse platforms which are created and managed by one core entity.</p> <p>ROBLOX MINECRAFT FORTNITE SECOND LIFE</p>	<p><b>Virtual Real Estate</b> Entities that are focused on building and investing in metaverse platforms.</p> <p>LANDIAH!T SANDSTORM EVERYREALM pangea Parcel</p>	<p><b>Gaming &amp; P2E</b> These platforms are focused on building Metaverse gaming experiences. Leveraging gaming economies.</p> <p>AXIE INFINITY animoca BRANDS BYOPLES MYTHICAL HUMAN PARK STAR ATLAS zed HOUSE OF KIBAA L3</p>
		<p><b>Guilds</b> Gaming Guilds are organizations that provide training, tools, NFTs, &amp; funds to players.</p> <p>WILD GUILD GAMEFI EMPIRE</p>	<p><b>Consortiums</b> Entities that are focused on creating Web3 &amp; metaverse creation standards</p> <p>Metaverse W3C KRONOS OMIgroup</p>	<p><b>Marketplaces &amp; Game Launchers</b> Marketplace platforms that enable users to list and sell metaverse assets.</p> <p>elixir METAMUNDO FRACTAL</p>

<p><b>Gaming Engines</b> A software framework used for the development of video games &amp; VR applications which includes relevant libraries.</p> <p>Unity UNREAL ENGINE CRYENGINE lumberyard</p>	<p><b>Social, Art, &amp; Entertainment</b> Metaverse applications focused on connecting users and players through dynamic social &amp; immersive experiences.</p> <p>VRCHAT horizon Worlds MONA AltspaceVR MALOKA ROOFTOP Spatial bigscreen</p>	<p><b>Digital Identity</b> Companies tackling digital identity by building avatar creation platforms and interoperability systems.</p> <p>READY PLAYER ME Genies+ soul machines Tafi YUGALABS RTFKT</p>	<p><b>Tools</b> Companies building tools to streamline metaverse asset creation.</p> <p>Rove zesty STEAM VR blender</p>
--	---	---	---



BROWSER



STORAGE



VIDEO AND  
AUDIO CALLS



OPERATING  
SYSTEM



SOCIAL  
NETWORK



MESSAGING



REMOTE JOB

CHROME



DROPBOX



SKYPE



ANDROID



FACEBOOK



WHATSAPP



UPWORK



BRAVE



IPFS



EXPERTY



EOS



STEEMIT



STATUS



ETHLANCE



WEB 2.0  
APPS



WEB 3.0  
DAPPS

Google  
Daydream



**Google**  
Daydream

**SAMSUNG**  
Gear VR  
Powered by  **oculus**



**Samsung**  
Gear VR

  
**oculus**



**Oculus**  
Rift

  
**PlayStation.VR**  
EXPERIENCE



**Sony**  
Playstation VR

  
**VIVE**  
htc |  **STEAM VR**



**HTC / Valve**  
Vive



Oculus founder Palmer Luckey says he has designed a new VR headset loaded with explosives that can actually kill you: "If you die in the game, you die in real life". - Copyright  
Courtesy Palmer Luckey

BATMAN ÜNİVERSİTESİ

# BİLİŞİM FESTİVALI IFEST 2023

DIJİTAL BLOKZİNCİR SİBER  
DÖNÜŞÜM TEKNOLOJİLERİ GÜVENLİK

ANATEMALARILYLA

## DEĞİŞİM BİLİŞİMİLE GELECEK

Bilişim  
Teknolojileri  
Fuarı

Kamu Bilişim  
Çalıştayı

Uluslararası  
Bilişim Kongresi

Bilişim Akademisi

ETKİNLİKLER  
KATILIM ÜCRETSİZ!

Bilişim  
Teknolojileri  
Konferansı

Sosyal Etkinlikler

Ödüller  
Çekilişler

Deneyap  
Atölyeleri

9-11 ŞUBAT 2023 | BATMAN ÜNİVERSİTESİ

ifest@batman.edu.tr ifest.batman.edu.tr bilisimbatmanda @ ifest batman.edu.tr #bilisimbatmanda



# ULUSLARARASI BİLİŞİM KONGRESİ

IIC2023

DIJİTAL BLOKZİNCİR SİBER  
DÖNÜŞÜM TEKNOLOJİLERİ GÜVENLİK

ANATEMALARILYLA

KONGRE NİTELİKLERİ

DERGİLERİMİZ

- Uluslararası Katılımlı Kongre
- En az 2 Hakemli Değerlendirme (En az 1 hakem kurum dışından)
- ISBN Kitaplarda Makale Yayını
- Seçilen Makaleleri İndeksli ve Açık Erişimli Dergilerde Yayınlama İmkanı

- Balkan Journal of Electrical and Computer Engineering (BAJECE)
- European Journal of Technique (EJT)
- Journal of Engineering and Technology (JETECH)
- Cyber Politik Journal Siber Politikalar Dergisi

## KONULAR

Siber Güvenlik  
Blokzinciri  
Metaverse,NFT  
Haberleşme Teknolojileri  
İnsansız Hava Araçları  
Robotik

Yapay Zeka  
Roket Teknolojileri  
Savunma & Uzay Teknolojileri  
Dijital Dönüşüm Uygulamaları  
Dijital Güvenlik Sistemleri  
Akıllı Şehir Sistemleri

Veri Merkezleri  
Akıllı Sistem Odaları  
Akıllı Ev Sistemleri  
Siber İstihbarat  
Sağlık Bilişimi  
Veri Güvenliği

Veri Sıkıştırma Algoritmaları  
Oyunlaştırma Teknolojileri  
GameFI,DeFi,SocialFI  
Kriptografi  
Büyük Veri  
Elektrikli Araç Teknolojileri

Makine Öğrenmesi  
Derin Öğrenme  
Dijital Yaşam  
E-Ticaret  
Kayıt Zinciri,kripto Paralar  
Dijital Ekonomi

Bulut Bilişim  
Sosyal Ağlar  
Bilişim Hukuku  
Sanallaştırma  
Güvenlik Duvarları  
Veri Depolama Üniteleri

İş Zekası Uygulamaları  
Adli Bilişim  
Nesnelerin İnterneti  
Bilgisayar Ağ Güvenliği  
Mobil Uygulamalar  
Enerji Bilişim Sistemleri

Yönetişim Sistemleri  
Sanal Gerçeklik  
Kablosuz Ağ Uygulamaları  
İnsan-makine Etkileşimi  
Veri Modelleme  
Güvenlik Sistemleri

25.01.2023

MAKALE SON KABUL TARİHİ

@ bilisimbatmanda

@ ifest.batman.edu.tr

@ ifest@batman.edu.tr

BİLİŞİM FESTİVALI  
IFEST 2023



9 - 11 ŞUBAT 2023

BATMAN / TÜRKİYE

BATMAN ÜNİVERSİTESİ

# BİLİŞİM FESTİVALI IFEST 2023

DIJİTAL DÖNÜŞÜM BLOKZİNCİR TEKNOLOJİLERİ SİBER GÜVENLİK

ANATEMALARıyla

## DEĞİŞİM BİLİŞİMİLE GELECEK

Bilişim  
Teknolojileri  
Fuarı

Kamu Bilişim  
Çalıştayı

Uluslararası  
Bilişim Kongresi

Bilişim  
Akademisi

ETKİNLİKLER  
KATILIM ÜCRETSİZ!

Bilişim  
Teknolojileri  
Konferansı

Sosyal  
Etkinlikler

Ödüller  
Çekilişler

Deneyap  
Atölyeleri

12-14 EKİM 2023 | BATMAN ÜNİVERSİTESİ

#fest@batman.edu.tr #fest.batman.edu.tr #bilisimbatmanda



BATMAN ÜNİVERSİTESİ  
BİLİŞİM FESTİVALI  
IFEST 2023

## DEĞİŞİM BİLİŞİMİLE GELECEK

HEĐİVELER  
ÇERİLSER  
IKRAMLAR

•FUAR •KONGRE •ÇALIŞTAY •  
•AKADEMİ •KONFERANSLAR •ATÖLYELER •

KATILIM  
ÜCRETSİZ



1 EKİM  
SON KAYIT

12-14 EKİM 2023  
BATI RAMAN KAMPÜSÜ

#fest.batman.edu.tr #fest@batman.edu.tr IFEST2023





# ULUSLARARASI BİLİŞİM KONGRESİ IIC 2024

DİJİTAL  
DÖNÜŞÜM YAPAY  
ZEKA SİBER  
GÜVENLİK

## ANA TEMALARıyla

### KONGRE NİTELİKLERİ

- Uluslararası Katılımlı Kongre
- En az 2 Hakemli Değerlendirme (En az 1 hakem kurum dışından)
- ISBN Kitaplarda Makale Yayımlı
- Seçilen Makaleleri İndeksli ve Açık Erişimli Dergilerde Yayımlama İmkânı

### DERGİLERİMİZ

- Balkan Journal of Electrical and Computer Engineering (BAJECE)
- European Journal of Technique (EJT)
- Journal of Engineering and Technology (JETECH)
- Cyber Politik Journal Siber Politikalar Dergisi

## KONULAR

Siber Güvenlik  
Blokzinciri  
Metaverse,NFT  
Haberleşme Teknolojileri  
İnsansız Hava Araçları  
Robotik

Yapay Zeka  
Raket Teknolojileri  
Savunma & Uzay Teknolojileri  
Dijital Dönüşüm Uygulamaları  
Dijital Güvenlik Sistemleri  
Akıllı Şehir Sistemleri

Veri Merkezleri  
Akıllı Sistem Odaları  
Akıllı Ev Sistemleri  
Siber İstihbarat  
Sağlık Bilişimi  
Veri Güvenliği

Veri Saklama Algoritmaları  
Oyunlaştırma Teknolojileri  
GameFI,DeFi,SocialFI  
Kriptografi  
Büyük Veri  
Elektrikli Araç Teknolojileri

Makine Öğrenmesi  
Derin Öğrenme  
Dijital Yaşam  
E-Ticaret  
Kayıt Zinciri,kripto Paralar  
Dijital Ekonomi

Bulut Bilişim  
Sosyal Ağlar  
Bilişim Hukuku  
Sanatlıştırma  
Güvenlik Duvarları  
Veri Depolama Üniteleri

İş Zekası Uygulamaları  
Adli Bilişim  
Nesnelerin İnterneti  
Bilgisayar Ağ Güvenliği  
Mobil Uygulamalar  
Enerji Bilişim Sistemleri

Yönetişim Sistemleri  
Sanal Gerçeklik  
Kablosuz Ağ Uygulamaları  
İnsan-makine Etkileşimi  
Veri Modelleme  
Güvenlik Sistemleri

24.04.2024 MAKALE  
SON KABUL TARİHİ

BİLİŞİM FESTİVALI  
IFEST2024  
ifest.batman.edu.tr



2-4 MAYIS 2024

BATMAN / TÜRKİYE



# INTERNATIONAL INFORMATICS CONGRESS IIC 2024

DIGITAL  
TRANSFORMATION CYBER  
SECURITY ARTIFICIAL  
INTELLIGENCE

## MAIN THEMES

### CONGRESS QUALIFICATIONS

- Congress with International Participation
- At least 2 Peer Reviews (At least 1 referee is from outside the institution)
- ISBN Article Publication in Books
- Selected Articles Indexed and Open Opportunity to publish in accessible journals

### OUR JOURNALS

- Balkan Journal of Electrical and Computer Engineering (BAJECE)
- European Journal of Technique (EJT)
- Journal of Engineering and Technology (JETECH)
- Cyber Politik Journal

## TOPICS

Cyber security • Artificial intelligence  
Blockchain • Rocket Technologies  
Metaverse,NFT • Defense & Space Technologies  
Communication Technologies • Digital Transformation Applications  
Unmanned Aerial Vehicles • Digital Security Systems  
Robotics • Smart City Systems

Data Centers • Data Compression Algorithms  
Smart System Rooms • Camification Technologies  
Smart home systems • GameFI,DeFi,SocialFI  
Cyber Intelligence • Cryptography  
Health Informatics • Big Data  
Data security • Electric Vehicle Technologies

Machine Learning • Cloud computing  
Deep Learning • Social networks  
Digital Life • IT law  
E-Commerce • Virtualization  
Registry Chain, Cryptocurrencies • Firewalls  
Digital Economy • Data Storage Units

Business Intelligence Applications • Governance Systems  
Forensics • Virtual Reality  
Internet of Things • Wireless Network Applications  
Computer Network Security • Human-machine Interaction  
Mobile Applications • Data Modeling  
Energy Information Systems • Security systems

24.04.2024 ARTICLE LAST  
ACCEPTANCE DATE

INFORMATICS FESTIVAL  
IFEST2024  
ifest.batman.edu.tr



2-4 MAY 2024

BATMAN / TURKEY





BATMAN ÜNİVERSİTESİ

# NECAT NASIROĞLU PROJE YARIŞMASI

“Enerji’de İnnovasyon”

Proje Değerlendirme Süreci

- 1 Proje başvurularının alımı için ilana çıkılması ve ilan askı süreci [15 Eylül – 15 Ocak]
- 2 Proje başvurularının ön değerlendirmeleri ve sergiye katılacak projelerin seçilmesi [15 Ocak – 30 Ocak Ocak]
- 3 Fikir ve Ürün’ler için Sergi [ 17 Şubat 2024]
- 4 Konferans ve sonuç oylaması [17 Şubat 2024]



BATMAN  
UNIVERSITY



BATMAN  
ÜNİVERSİTESİ

# NECAT NASIROĞLU

PROJECT  
COMPETITION

PROJE  
YARIŞMALARI

MAIN THEMES

ANA TEMALAR

DİJİTAL  
TRANSFORMATION

BLOCK CHAIN  
TECHNOLOGY

DİJİTAL  
DÖNÜŞÜM

BLOK ZİNCİR  
TEKNOLOJİLERİ

“DEĞİŞİM BİLİŞİMLE GELECEK”

*Prof. Dr. İdris Demir*

REKTÖR

2025

Important Dates

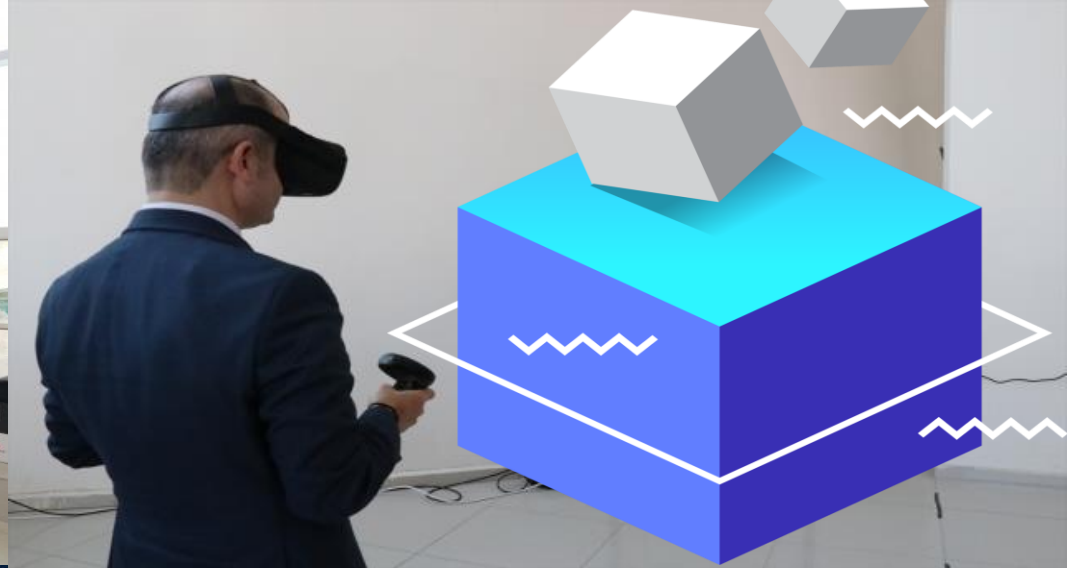
Project Submission  
Deadline  
January  
17 – 2025

Project  
Presentation  
February  
17 – 2025

Önemli Tarihler

Proje  
Son Teslim Tarihi  
17 Ocak  
2025

Proje  
Sunumları  
17 Şubat  
2025







Saray Güli

YAKA KARTI SPONSORU  
BARİKAT

100.15  
DELLI SPONSORU  
reşat Akın  
CANLA SPONSORU  
hp  
Türkiye  
GOLD SPONSORU  
SAMSUNG  
SILVER SPONSORU  
SAMSUNG  
YAKA KARTI SPONSORU  
BARİKAT

PANELLER

PANELLER

26. yıl  
www.ikem.com.tr

ilke

getirecem.com

www.ikem.com.tr



BATMAN ÜNİVERSİTESİ  
ULUSLARARASI BİLİŞİM KONGRESİ

IC202



# reset



DIGITAL TRANSFORMATION

Dell Technologies  
GOLD



# reset

ASLAR

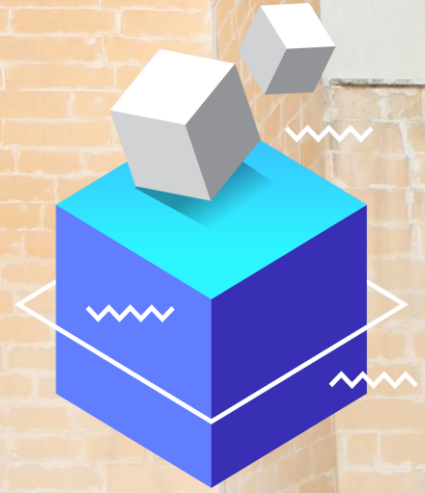
# reset

Dell

om.ir



# HASANKEYF UYGULAMA OTELİ



BATMAN ÜNİVERSİTESİ HASANKEYF UYGULAMA OTELİ





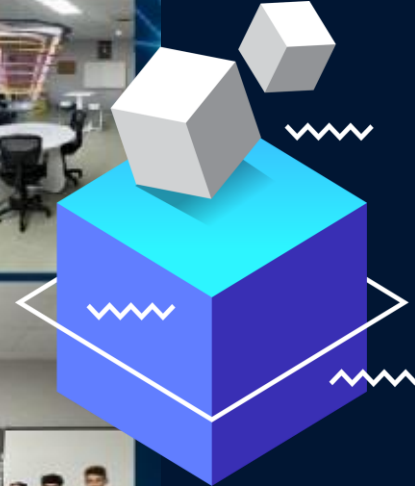
 **TOME**  
**HOŞGELDİNİZ**







# BATMAN ÜNİVERSİTESİNDE SİBER KOZA MERKEZİ AÇILDI !



# BATMAN ÜNİVERSİTESİ TÜYAFED İŞBİRLİĞİ PROTOKOLÜ İMZALANDI



# Kaynaklar

<https://portswigger.net/web-security/>

<https://overthewire.org> <https://tryhackme.com>

<https://hackthebox.com> <https://www.root-me.org>

<https://pwnable.kr> <https://www.hacking-lab.com>

<https://hackthissite.org> <https://ctf365.com>

<https://www.hacker101.com> <https://www.wechall.net>

<https://www.youtube.com/TheCyberMentor>

<https://www.youtube.com/LiveOverflow>

<https://www.youtube.com/JohnHammond010>

<https://www.youtube.com/TechWorldwithNana>

<https://www.youtube.com/BlackHatOfficialYT>

<https://www.youtube.com/DEFCONConference>

<https://www.youtube.com/Computerphile>

<https://www.youtube.com/numberphile>

<https://www.youtube.com/Freecodecamp>

<https://www.youtube.com/c/SimplilearnOfficial>

Ahmet Anil Dündar, Aselsan, [aadundar@aselsan.com.tr](mailto:aadundar@aselsan.com.tr)

Hasan Mutlu, Gais Cyber Security



# TEŞEKKÜRLER

Dr. Hafzullah İŞ

[Linkedin](#) /hafzullahis



AWESOME  
WORDS

# MULTIMEDIA

You can insert your multimedia content here





# Instructions for use

In order to use this template, you must credit [Slidesgo](#) by keeping the **Thanks** slide.

## You are allowed to:

- Modify this template.
- Use it for both personal and commercial projects.

## You are not allowed to:

- Sublicense, sell or rent any of Slidesgo Content (or a modified version of Slidesgo Content).
- Distribute Slidesgo Content unless it has been expressly authorized by Slidesgo.
- Include Slidesgo Content in an online or offline database or file.
- Offer Slidesgo templates (or modified versions of Slidesgo templates) for download.
- Acquire the copyright of Slidesgo Content.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

<https://slidesgo.com/faqs> and <https://slidesgo.com/slidesgo-school>

# Instructions for use (premium users)

In order to use this template, you must be a Premium user on [Slidesgo](#).

## You are allowed to:

- Modify this template.
- Use it for both personal and commercial purposes.
- Hide or delete the “Thanks” slide and the mention to Slidesgo in the credits.
- Share this template in an editable format with people who are not part of your team.

## You are not allowed to:

- Sublicense, sell or rent this Slidesgo Template (or a modified version of this Slidesgo Template).
- Distribute this Slidesgo Template (or a modified version of this Slidesgo Template) or include it in a database or in any other product or service that offers downloadable images, icons or presentations that may be subject to distribution or resale.
- Use any of the elements that are part of this Slidesgo Template in an isolated and separated way from this Template.
- Register any of the elements that are part of this template as a trademark or logo, or register it as a work in an intellectual property registry or similar.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

<https://slidesgo.com/faqs> and <https://slidesgo.com/slidesgo-school>

