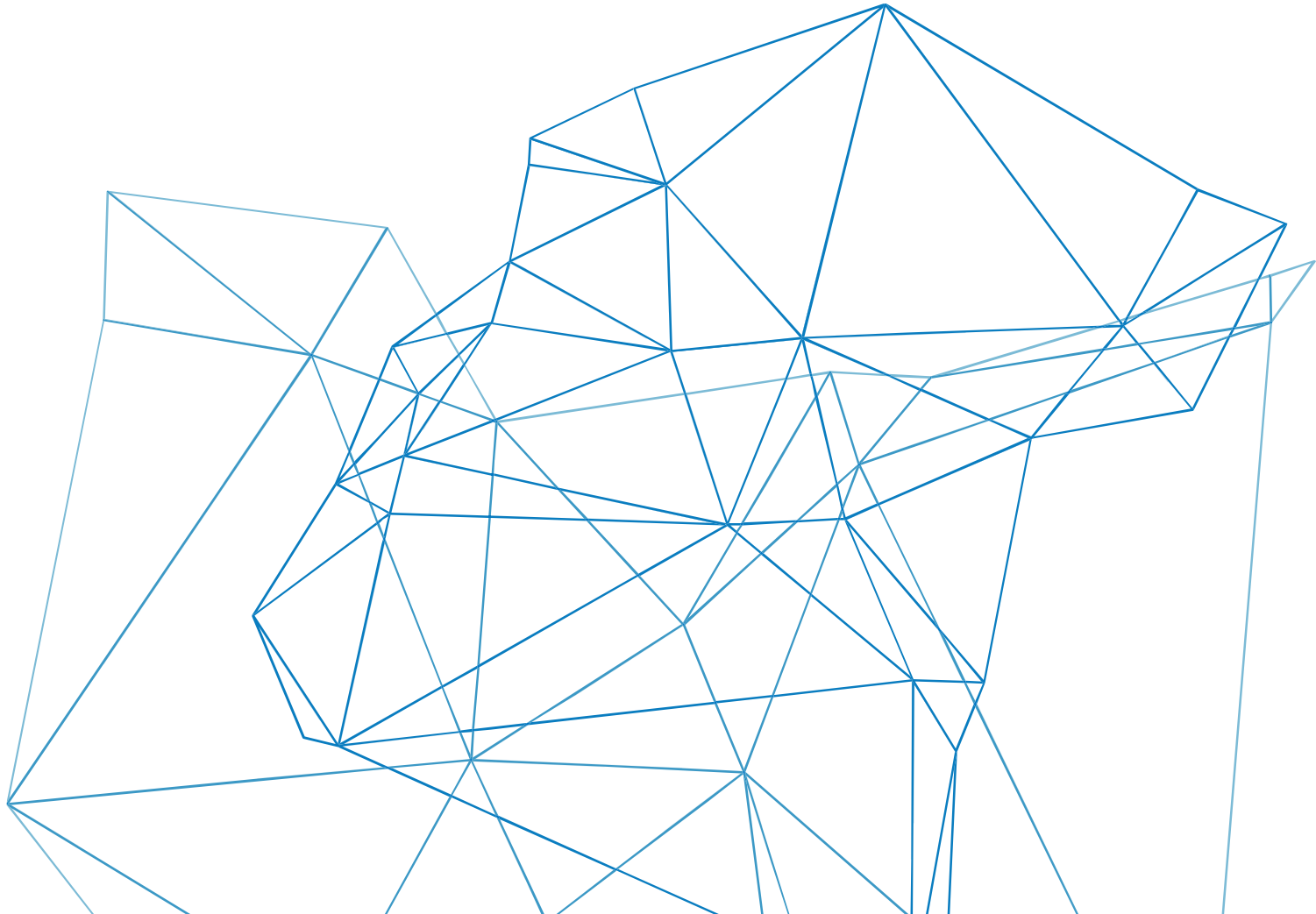
ARCHITECHT

FİNANS & SİBER GÜVENLİK



Ahmet Akan

Uygulama Güvenlik Analisti

Karabük Üniversitesi Bilgisayar Mühendisliği Mezunu

(Eski) Ortak Kriterler Değerlendirme Uzmanı

Uygulama Güvenlik Analisti, Uygulama Geliştirici

ARCHITECHT

 @ahm3t7

 akn.ahmet@msn.com

 /ahmetakan

ahmetakan.com

CYBERSPACE

CYBERSPACE

ARCHITECHT

Bilgisayarlar, network cihazları, internet bağlantısı olan tüm cihazların birbirlerine bağlanması ile oluşturulan **“Virtual World”**

Cyberspace terimi ilk olarak 1982 yılında Wiiliam Gibson isimli bir yazar tarafından “Neuromance” isimli kitapta kullanılmıştır.

CYBERSPACE

1.7 Milyar

World Wide Web üzerinde bulunan website sayısı

3.986 Milyar

Mobil cihaz üzerinde internete erişim sağlayan kullanıcı sayısı

4.388 Milyar

İnternete erişim sağlayan kullanıcı sayısı

6 Saat 42 Dakika

İnternet üzerinde geçirilen günlük ortalama süre

CYBERSPACE

ARCHITECHT

Her gün yaklaşık 65 milyar mesaj Whatsup üzerinden gönderiliyor

Her gün yaklaşık 293.6 Milyar e-posta gönderilip/alınıyor

Her gün yaklaşık 90 milyon yeni fotoğraf yükleniyor

Her gün yaklaşık 500 milyon twet gönderilmektedir

Amazon firmasının günlük satış gerçekleştirdiği miktar yaklaşık olarak 410 milyon dolardır. Yani dakikada 283 bin dolar kazanmakta

Her gün yaklaşık 3739 uygulama Android markete eklenmektedir

CYBERSPACE

ARCHITECHT

01

>2 Milyar Dolar

2019 yılında gerçekleştirilen siber saldırılar sonucunda yaşanan kayıp

02

4.1 Miyar Satır Veri

2019 yılının ilk yarısında gerçekleşen veri sızıntısının boyutu

03

6 Trilyon Dolar

Siber suçlar sonucunda meydana gelmesi beklenen kayıp miktarı (2021 yılına kadar)

04

150 Dolar

Siber saldırılar sonrasında çalınan bir satır verinin ortalama maliyeti

05

584 - 1178 Dolar

2012 yılında siber güvenlik alanındaki bir çalışana ortalama 584 dolar harcanırken, 2018 yılında bu miktar 1178 dolar seviyesindedir

06

3.9 Milyar Dolar

Siber saldırılar sonucunda meydana gelen veri sızıntılarının ortalama maliyeti

HACK - ER

HACKER

ARCHITECHT

Halk arasında hacker **“asosyal, siyah giyen, sadece hazır gıda tüketen, çoğunluğu aşırı kilolu, büyük gözlüklere sahip bilgisayarcı çocuklar“** şeklinde tanımlanmaktadır. Birde geleceğin mesleği olacak diyorlar ☺

HACKER

HACK, yapılan/gerçekleştirilen işlemler için bir kısa yol bulma/kolaya kaçma işlemi olarak tanımlanabilmektedir.

HACKER ise kolay/kaçamak yolları tespit eden ve kullanan kişiler olarak tanımlanabilmektedir.

HACKER

ARCHITECHT

Black Hat

White Hat

Gray Hat

HACKER

ARCHITECHT

Peki nasıl beyaz şapkalı hacker olabilirim?

GIAC WEB APP PEN TESTER GWAPT

C|EH Certified Ethical Hacker

L|P|T Licensed Penetration Tester

OFFENSIVE security OSCP

TSE

Web Security Academy

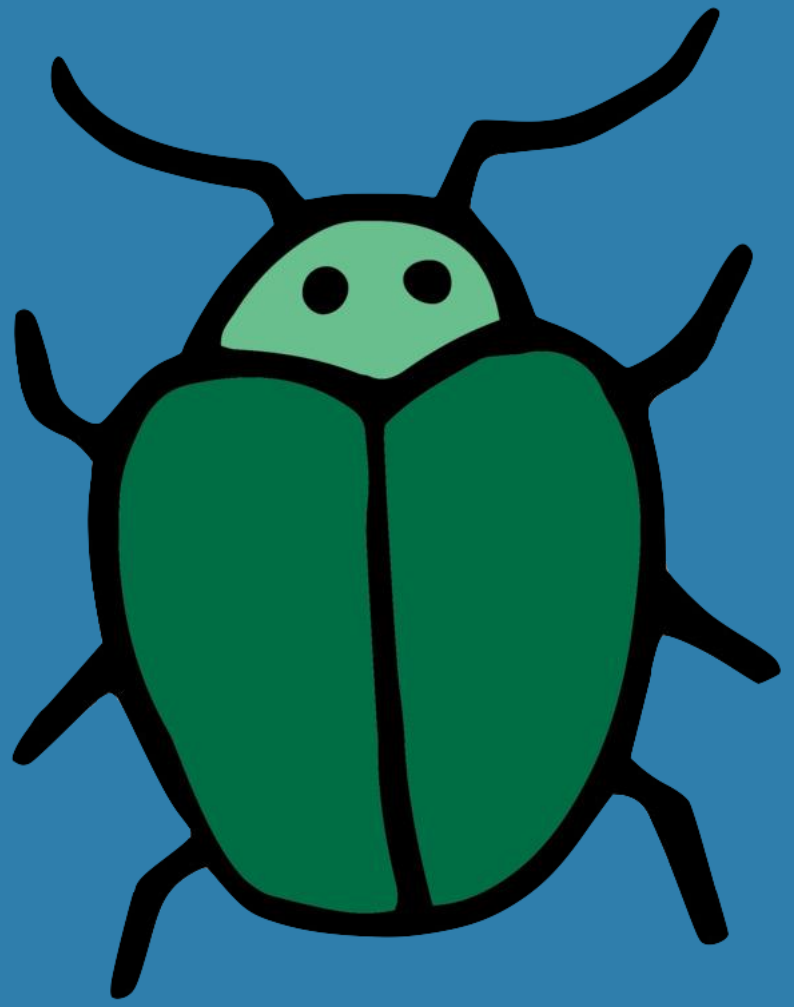
HACKTHEBOX

PentesterLab

10 10 1110 0101 01 01 010 01

Try Hack Me

INFORMATION SECURITY



ASSET

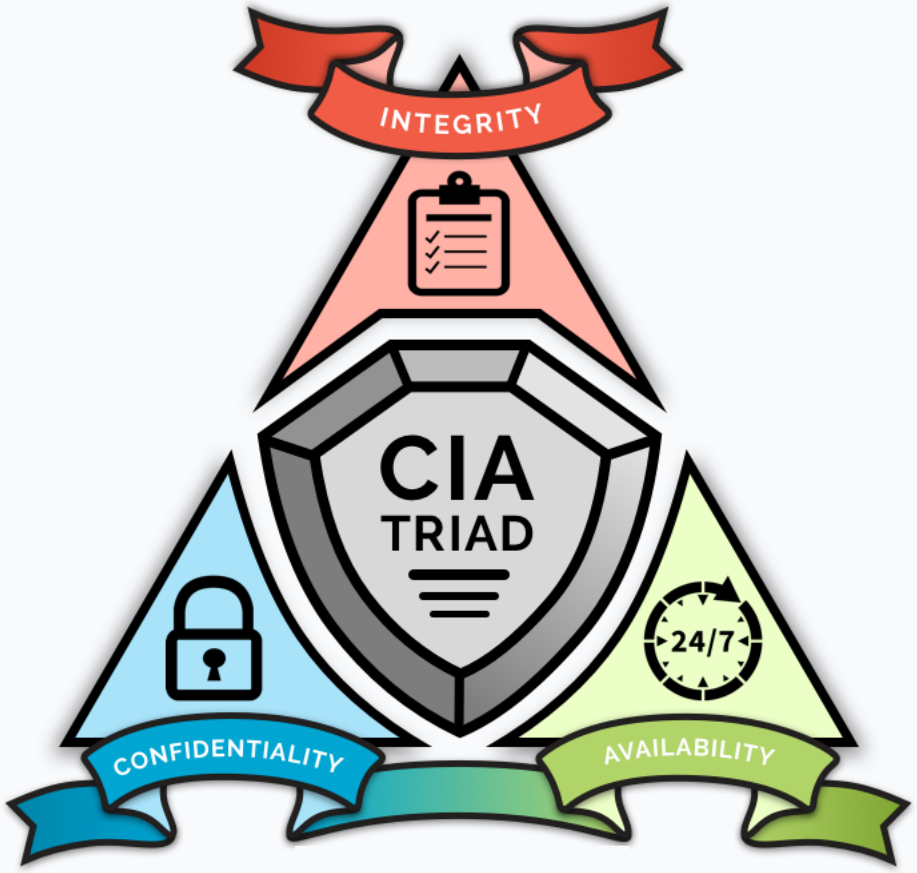
Asset / Varlık

- Korunması elzem olan;
  - Bilgi
  - Belge
  - Fiziksel Cihaz, vb.

VULNERABILITY

Vulnerability / Security Bug

- Vulnerability ⊆ Software Bug
- CIA Triad;
  - Integrity – Bütünlük
  - Confidentiality - Gizlilik
  - Availability – Erişilebilirlik



THREAT

ARCHITECHT

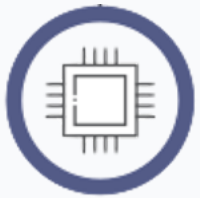
Web application (SQL injection, cross site scripting, etc)

Software vulnerability

Use of stolen credentials (logins, encryption keys)

Strategic web compromise (watering hole attack)

DDOS (Distributed Denial of Service)



Malware/ ransomware

Phishing/ Spear phishing

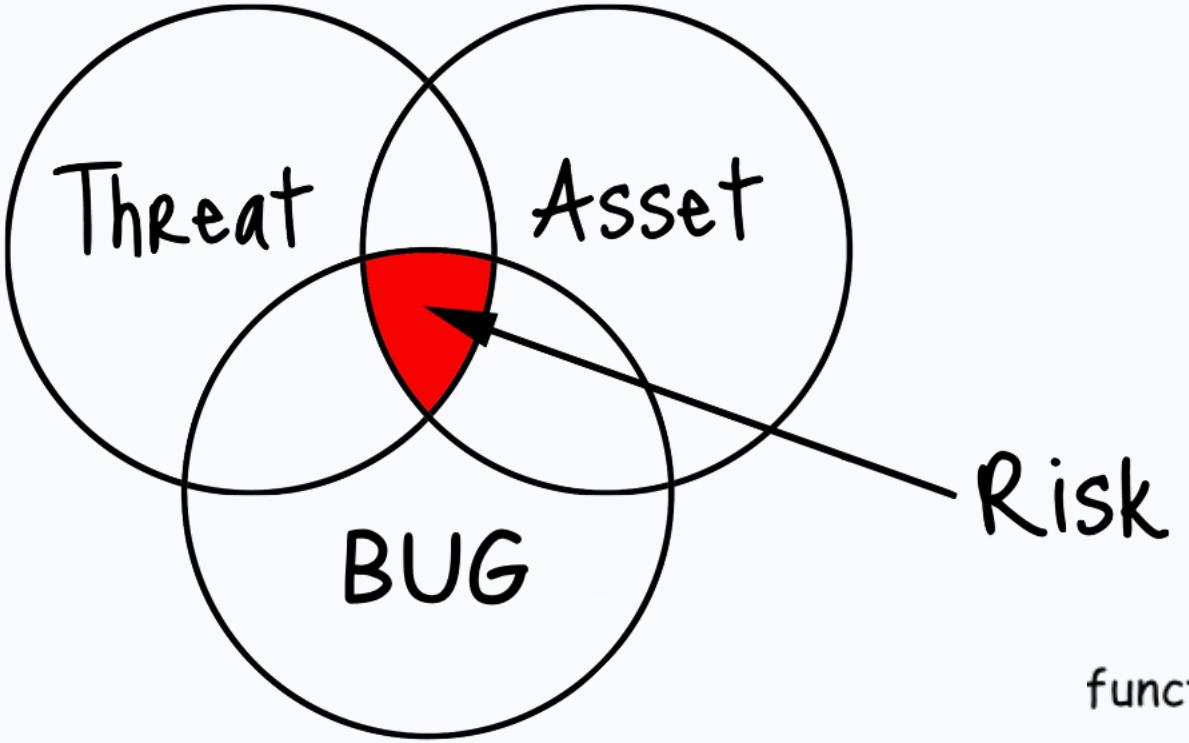
Social engineering

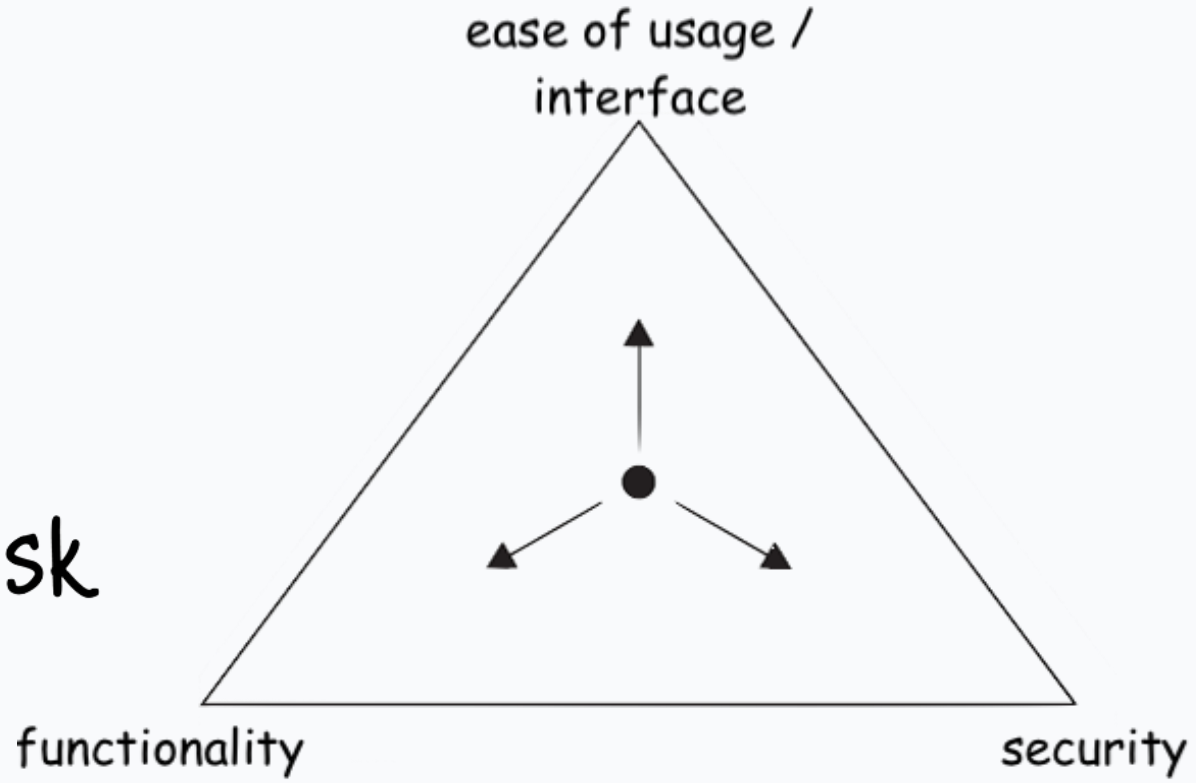
THREAT-ACTORS

Threat-Actors / Tehdit Aktörleri

- Bad and Cool Guys
  - Hacktivist
  - Cybercriminals
  - Insider
  - Espionage

RISK


Threat
Asset
BUG
Risk

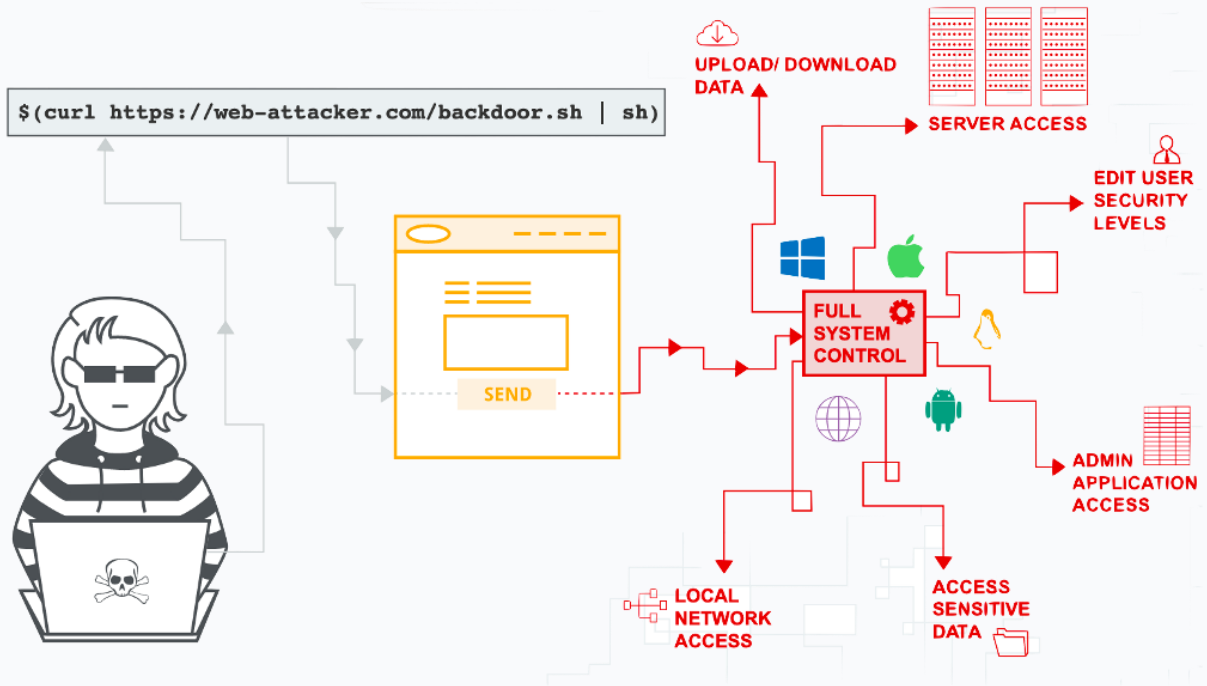

ease of usage /
interface
functionality
security

EXPLOIT

ARCHITECHT

Exploit / Sömürme

- Zafiyetlerin tehdit aktörleri tarafından sömürülmesi
- Exploit Database
- Script-Kiddie
- Zero-Day



RISK-RATING

Risk Rating / Risk Derecelendirme

- Likelihood / İhtimal
  - Threat Agent Factor / Tehdit Faktörü
    - Skill Level / Yetenek Seviyesi
    - Motive / Motivasyon
    - Opportunity / Olanak
    - Size / Büyüklük
  - Vulnerability Factor / Zafiyet Faktörü
    - Ease of discovery / Keşif kolaylığı
    - Ease of exploit / Sömürme kolaylığı
    - Awareness / Farkındalık
    - Intrusion Detection / İhlal Tespiti

RISK-RATING

Risk Rating / Risk Derecelendirme

- Impact / Etki
  - Technical Impact / Teknik Etki
    - Loss of confidentiality / Gizlilik kaybı
    - Loss of integrity / Bütünlük kaybı
    - Loss of availability / Erişilebilirlik Kaybı
    - Loss of accountability / Takip edilebilirlik kaybı
  - Business Impact / İş Etkisi
    - Financial Damage / Finansal Hasar
    - Reputation Damage / Marka Kimlik Hasarı
    - Non-Compliance / Uyumsuzluk
    - Privacy Violation/ Gizlilik İhlali

RISK-RATING

ARCHITECHT

Risk Rating / Risk Derecelendirme

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
6 - Network and programming skills	9 - High reward	9 - No access or resources required	9 - Anonymous Internet users		7 - Easy	5 - Easy	6 - Obvious	8 - Logged without review
			Overall likelihood:	7,375	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9 - All data disclosed	9 - All data totally corrupt	9 - All services completely lost	7 - Possibly traceable		7 - Significant effect on annual profit	9 - Brand damage	7 - High profile violation	7 - Thousands of people
		Overall technical impact:	8,500	HIGH			Overall business impact:	7,500	HIGH
			Overall impact:	8,000	HIGH			

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

CYBERSECURITY IN FINANCE

CYBERSECURITY in FINANCE

Dünya üzerinde gerçekleşen veri sızıntılarının %76'lık bölümü finansal motivasyon kaynaklı

Siber saldırılar sonucunda firma başına yıllık 18.3 milyon dolar zarar uğrayan finans firmaları bu alanda lider konumda

2017 yılında gerçekleştirilen güvenlik testleri sonucunda bankaların %65'inin sistemlerinin güvenilir olmadığı tespit edilmiştir (America)

Carbank çetesi, 30 farklı ülkedeki 100 bankanın malware yardımı ile soyulduğu ve kaybın 1 milyar dolar olduğunu belirtmiştir

Amazon uygulamasının 40 dakikalık çöküntü yaşaması sonucunda meydana gelen kayıp 4.8 milyon dolar olarak açıklanmıştır

Finans servisler üzerinden sızan ortalama veri miktarı 352,771 iken bu değer sağlık sektöründe 113,491 değerindedir.

CYBERSECURITY in FINANCE

Kayıp: 1.8 Milyar Dolar
Yıl: 2018
Yer: Hindistan

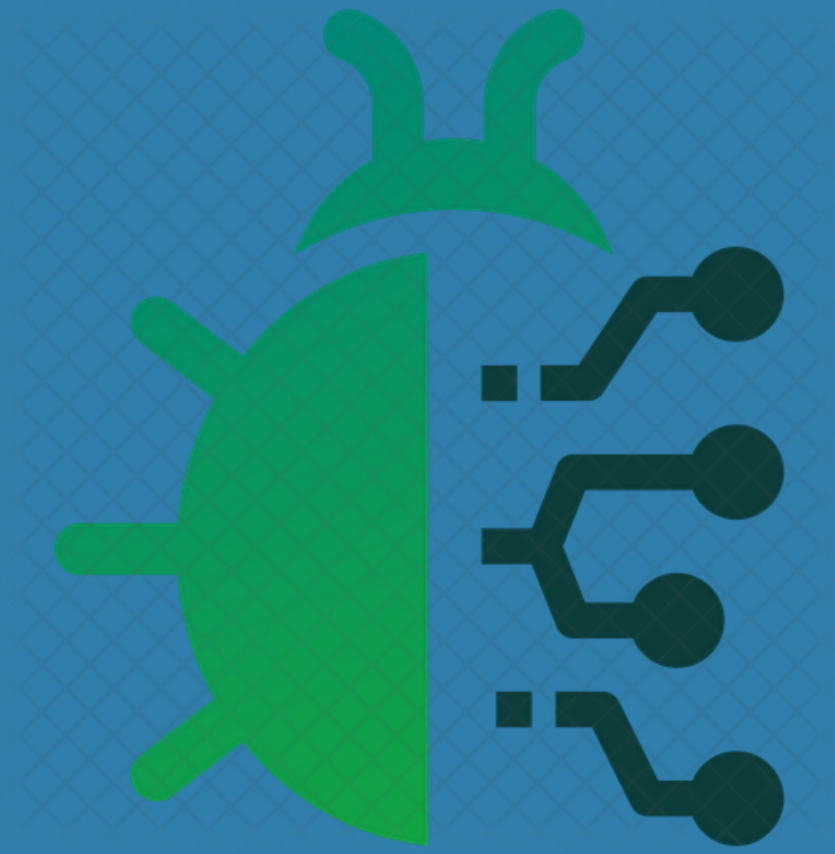
Kayıp: ~60 Milyon Dolar
Yıl: 2017
Yer: Taiwan

Kayıp: ~100 Milyon Dolar
Yıl: 2015-2016
Yer: Vietnam

Kayıp: ~4 Milyon Dolar
Yıl: 2016
Yer: Türkiye

Hackliyorum.avi

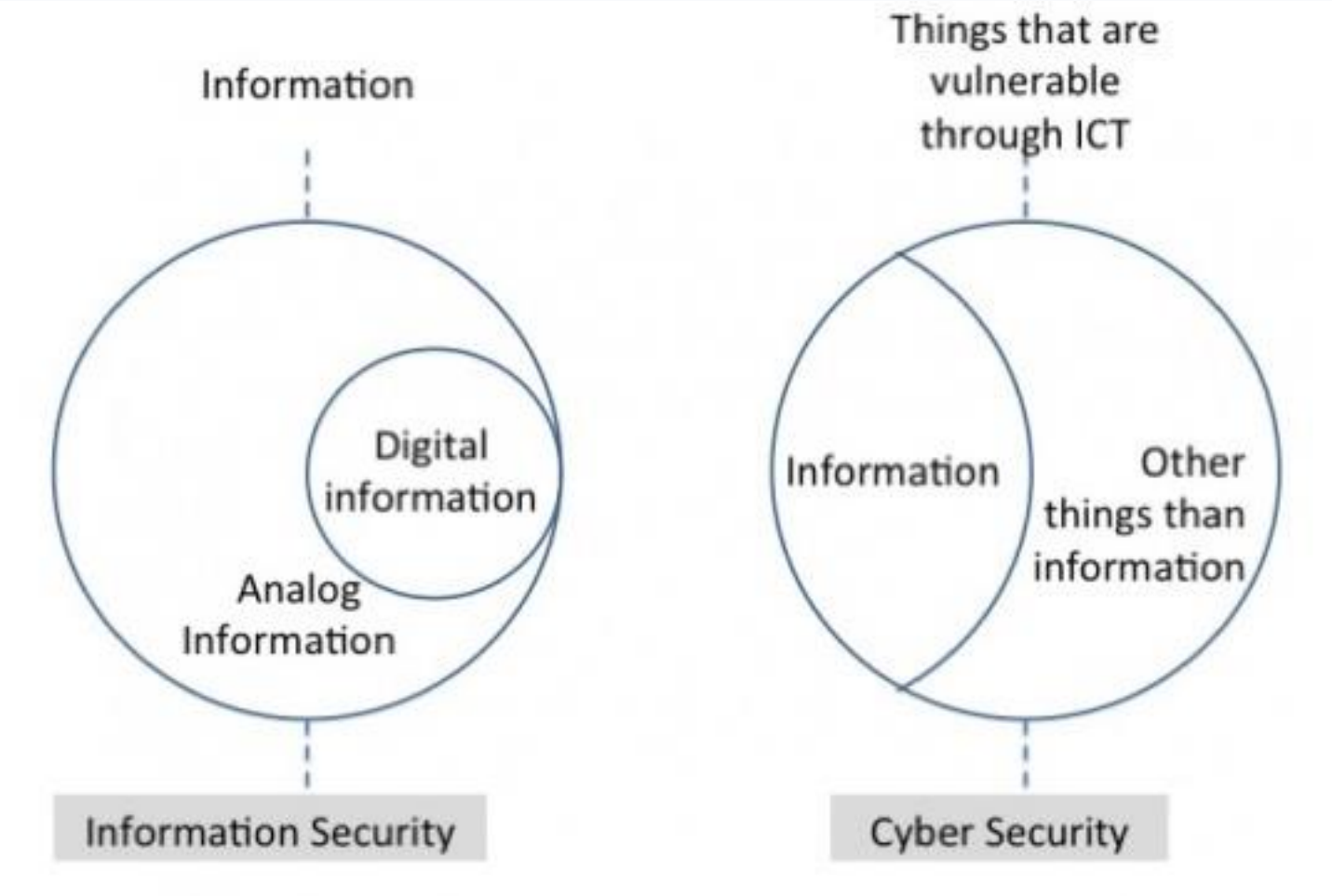
CYBERSECURITY



CYBERSECURITY

Siber güvenlik terimi NIST7298 dokümanı içerisinde ”***Siberuzayın (cyberspace) siber saldırılardan (cyber attacks) korunması, savunulması***” olarak tanımlanmıştır.

CYBERSECURITY - INFORMATION SECURITY



ICT Security