Siber Güvenlik
06/06/2026

Ahmet PEKEL


Temel
Kavramlar

Siber Güvenlik

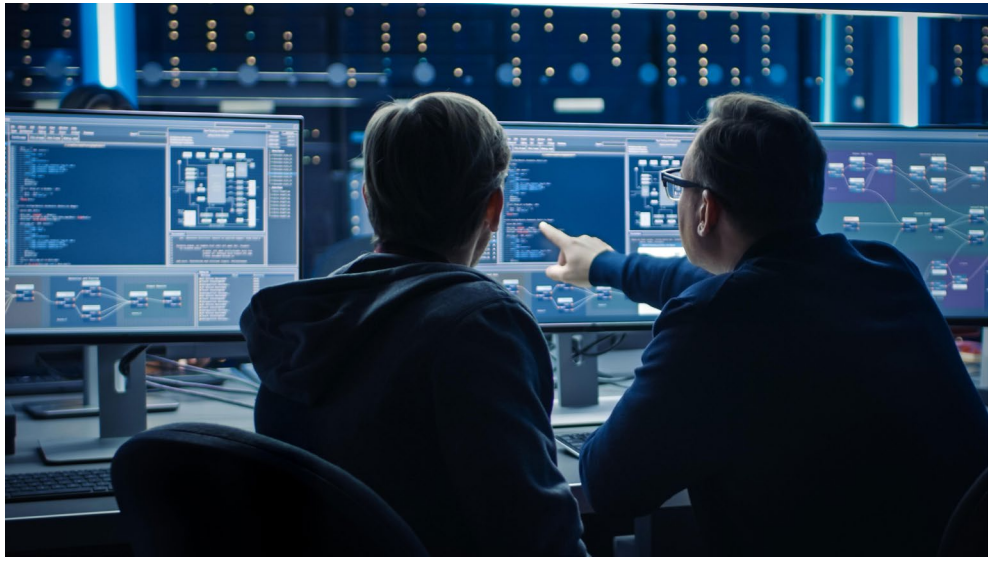
- Sistemleri, verileri, iletişim ağlarını ve programları siber saldırılardan korumak için alınan önlemler bütünüdür.

Siber Saldırgan

- Bilgisayar sistemine yetkisiz erişim sağlayan,
- Yasadışı olarak bir bilgisayar sistemine giren,
- Verilere yetkisiz erişim sağlamak için bilgisayar kullanan,
- Bilgisayarlı bir sistemde belirli bir hedefe ulaşmak veya belirli bir engeli aşmak için teknik bilgilerini kullanan kişidir.
- Siber saldırganlar genellikle hassas bilgilere erişmeyi, bunları değiştirmeyi veya yok etmeyi ya da bu bilgileri kullanıcılardan çalmayı ya da normal iş süreçlerini kesintiye uğratmayı amaçlarlar.

Siber Güvenlik Uzmanı

- Bilgi sistemlerinin güvenliğini sağlar; güvenlik olaylarını izleyerek, tehditleri saptayarak, araştırarak, çözümleyerek ve bunlara yanıt vererek, sistemleri siber güvenlik risklerinden, tehditlerinden ve güvenlik açıklarından korur.



Beyaz Şapkalı Güvenlik Uzmanı (*White Hat Hacker*): Bir kurumun güvenlik açıklarının ortaya çıkarılması amacıyla siber korsanların (*Black Hat Hacker*) kullandıkları teknikleri uygulayan ancak bunu etik kurallar çerçevesinde yapan güvenlik uzmanıdır.

Kırmızı Takım (*Red Team*): Bir kurumun tüm siber güvenlik yeterliliklerinin sınanması için saldırı benzetimi (*simulation*) yapan takıma verilen addır.

Mavi Takım (*Blue Team*): Bir kuruma karşı yöneltilebilecek olası saldırıları karşılamak amacıyla alınması gereken önlemleri belirleyen takımın adıdır.

Siber Saldırı

- Siber suçlular tarafından bir ya da daha çok bilgisayar kullanılarak tek ya da birden fazla bilgisayara veya ağa yapılan saldırıdır.
- Bir siber saldırıda, bilgisayarlar devre dışı kalabilir, veriler çalınabilir ve/veya ele geçirilen bir bilgisayar yeni bir saldırıyı başlatmak için kullanabilir.

Siber Saldırı Yöntemleri

- Kötücül yazılımlar (*malware*)
- Sistem ya da yazılım açıklıklarını sömürme
- Kullanıcı hesabı ele geçirme
- Kötücül kod yerleştirme
- Yanlış yapılandırılmış sistemlere yönelik saldırılar
- Kötücül istenmeyen (*spam*) iletiler
- Sahte sosyal hesaplar kullanılarak yapılan saldırılar
- Kötücül reklam kodları

Siber Saldırı Hedefleri

Siber saldırılarda en çok hedeflenen alanları aşağıdaki gibi özetleyebiliriz:

- Bireyler
- Sanayi kuruluşları
- Kamu
- Bilim-Teknik
- Sağlık
- Eğitim
- Destek hizmetleri
- Finans ve sigortacılık
- Konaklama ve yiyecek hizmetleri
- Satış ve kiralama hizmetleri
- Sanat ve eğlence
- İmalât
- Ödeme Sistemleri
- Emlâk
- Bilgi ve İletişim Teknolojileri

Siber Savaşlar ve Kritik Altyapılar

Siber savaşlarda en çok kullanılan saldırı noktaları kritik altyapılar olarak adlandırılan, ülkenin yaşamsal önemdeki kaynaklarıdır. Bunlar:

- Savunma,
- Enerji,
- Ulaşım,
- Finans,
- Sağlık,
- İletişim ve
- Su yönetimi altyapılarıdır.

Bu hedeflere yönelen siber saldırılar ülke düzeyinde yıkıcı etkiler oluşturabilmektedir.

Bir Siber Saldırının Olası Sonuçları - Örnekler

- Zararlı bir yazılımın, kurbanın bilgisayarına yüklenmesi sistemin donmasına ya da önemli bilgilerin açığa çıkmasına neden olabilir.
- Siber saldırılar elektrik kesintilerine, askeri gereçlerin arızalanmasına ve ulusal güvenlik sırlarının açığa çıkmasına neden olabilir.
- Tıbbi kayıtlar gibi değerli ve önemli verilerin çalınmasına neden olabilir.
- Telefon ve bilgisayar ağlarını bozabilir ya da sistemleri felç ederek verileri kullanılamaz hale getirebilir.
- Siber saldırılar toplum düzenini bozabilecek düzeyde etki oluşturabilir, saygınlık ve inandırıcılık kaybına neden olabilir.

Bilgi güvenliği, bilginin korunmasına yönelik bir dizi kuralın uygulanmasıdır

Bilgi güvenliğinde;

- Geç kalınamaz!
- “Bilmiyordum!” özür olarak kabul edilemez.
- Yönetim desteği gereklidir.

Bilgi güvenliği,

Varılması gereken bir hedef değil, sürekli iyileştirilmesi gereken bir süreçtir.

- Bilişim dünyasının en değişken alanıdır.
- Zaman ve çaba gerektirir.
- Maliyetlidir; eğitimli ve yetkin işgücüne gereksinim duyar.
- Riskleri tamamen ortadan kaldırmak anlamına gelmez; risklerin yönetilmesidir.
- Tek başına teknolojiyle çözülemez; bilinçli insanlarla mümkündür, kültürel değişim gerektirir.

Bilgiyi hedef alan tehditler

- Yetkisiz erişim,
- Bilginin bozulması ya da çalınması,
- Ağ trafiğini meşgul etme,
- Hizmet durdurma,
- Virüs, Truva atı (*trojan*) veya ajan programlarca (*spyware*) verilebilecek zararlar,
- Sosyal mühendislik,
- İnternet üzerinden yapılan karşı propaganda,
- Kritik altyapılara yönelik fiziki saldırılar.

Bilgiyi Hedef Alan Tehditler: Sonuçlar ve Önlemler

Bu tehditler nedeniyle,

- Ülke ekonomisi,
- Kamu emniyeti ve düzeni,
- Kişisel gizlilik,
- Kişisel, kurumsal ve ülkesel saygınlık ile
- Ticari rekabet olumsuz etkilenebilmektedir.

Tehditlere karşı;

- Bilgi,
- Yazılım,
- Donanım,
- Fiziksel alanlar,
- Hizmetler,
- Veri depolama ortamları,
- İletişim ortamları,
- İnsan ve
- Saygınlık korunmalıdır.

Bilgi Güvenliğinin Üç Temel İlkesi

- Gizlilik, bütünlük ve kullanılabilirlik

  - *Gizlilik*, bilgiye yetkisiz erişimi önlemenin güvencesidir;
  - *Bütünlük*, bilginin doğru ve değişmemiş olduğunun güvencesidir;
  - *Kullanılabilirlik*, gereksinim duyulduğunda yetkili kişiler tarafından bilgiye erişilebileceğinin güvencesidir.

Bilgi Güvenliği Yönetim Sistemi (BGYS)

- Bilgi Güvenliği Yönetim Sistemi, bilgi güvenliği altyapısını bir kuruluşta kurmak, işletmek, izlemek, gözden geçirmek ve iyileştirmek amacıyla geliştirilmiş, işlerliği ve sürekliliği güvence altına alınmış bir yönetim sürecidir.

Bilgi Güvenliği Yönetim Sistemi (BGYS)

- Sistem, aşağıdaki süreçleri kapsar:
  - Bilgi Güvenliği Politikası
  - Bilgi Güvenliği Örgütlenmesi
  - Varlık Yönetimi
  - Erişim Denetimi
  - Yükümlülüklere Uyum (yasalar, yönetmelikler ve yönergeler)
  - Bilgi Güvenliği İhlalleri Yönetimi
  - İnsan Kaynakları Güvenliği
  - Fiziksel ve Çevresel Güvenlik
  - Kriptografi
  - Bilgi Sistemleri Edinim, Geliştirme, Bakım
  - İletişim ve İşletim
  - İş Sürekliliği Yönetimi
  - Risk Yönetimi
- BGYS'nin kurulması için yönetimin desteği zorunludur.
- Kurumsal bir varlık olan bilginin korunmasından tüm kurum çalışanları sorumludur.

Güvenlik Açığı

Güvenlik açığı, siber saldırgan tarafından bir bilgisayar sisteminde yetkisiz eylemler yapmak için kullanılabilecek bir zayıflıktır.

Bir güvenlik açığından yararlanmak için, saldırganın bir sistem zayıflığına bağlanabilecek en az bir uygulanabilir araca ya da tekniğe sahip olması gerekir.

Güvenlik açıkları saldırı yüzeyi bileşenleri olarak da bilinir.

Güvenlik Açıklarının Yönetimi

Güvenlik açıklarının yönetimi (*Vulnerability Management*), aşağıdaki ortak süreçleri içeren döngüsel bir uygulamadır:

- Tüm varlıkları keşfetme
- Varlıklara öncelik verme
- Tam bir güvenlik açığı taraması yapma, değerlendirme
- Sonuçları raporlama
- Güvenlik açıklarını düzeltme
- Düzeltmeyi doğrulama ve yineleme

Güvenlik Açığı Türleri

- ***Bilgisayar Güvenliği Açıkları:*** Bu açıklar, güvenlik açığının nerede olduğu, neden olduğu veya nasıl kullanılabileceği gibi farklı ölçütlere göre çok sayıda türe ayrılabilirler. Bilgisayar güvenlik açıkları; bilgisayar yazılımlarındaki hatalar, virüs bulaşmış yazılımlar, eksik veri şifreleme, vb. şekilde sınıflandırılabilirler.
- ***Ağ Güvenliği Açıkları:*** Bu tür açıklar, bir ağın donanım veya yazılımında bulunan ve dışarıdan bir tarafın izinsiz girişine olanak sağlayan zayıflıklardır. Güvenli olmayan kablosuz erişim noktaları ve kötü yapılandırılmış güvenlik duvarları bu açıklara örnek olarak verilebilir.
- ***İşletim Sistemi Güvenliği Açıkları:*** Bunlar, bilgisayar korsanları tarafından kötüye kullanılabilecek belirli bir işletim sistemindeki var olan güvenlik açıklarıdır.

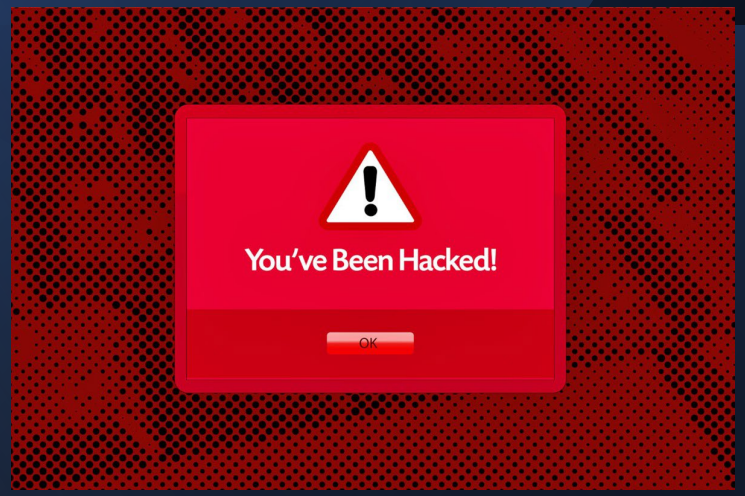
Güvenlik Açığı Türleri (devam)

- ***İnsan Kaynaklı Güvenlik Açıkları:*** Siber güvenlikte en zayıf halkalardan biri de siber güvenlik bilinci gelişmemiş insandır. Kullanıcı hataları; önemli bilgileri kolayca açığa çıkarabilir, saldırganlar için yararlanılabilir erişim noktalarını oluşturabilir veya sistemlerin çalışamaz duruma gelmesine neden olabilir.
- ***Süreç Kaynaklı Güvenlik Açıkları:*** Bazı güvenlik açıkları, belirli süreç denetimlerinin eksikliğinden kaynaklanabilir: düzenli sızma testlerinin yapılmaması ya da yaptırılan testlerden sonra iyileştirme çalışmasının yapılmaması gibi.

Kötücül Yazılımlar (Malware)

- Bunlar virüsler, fidye yazılımları ve casus yazılımlar olarak adlandırabileceğimiz bir dizi kötü amaçlı yazılımlardır.
- Kötücül yazılımlar siber saldırganlar tarafından geliştirilen, verilere ve sistemlere zarar vermek ya da bir ağa yetkisiz erişim sağlamak için tasarlanmış kodlardan oluşur.
- Bunlar genellikle e-posta üzerinden gönderilen bir bağlantı ya da dosya biçiminde sunulur ve kullanıcının kötücül yazılımı çalıştırması için bağlantıyı tıklamasını ya da dosyayı açmasını gerektirir.

Kötücül Yazılım Türleri



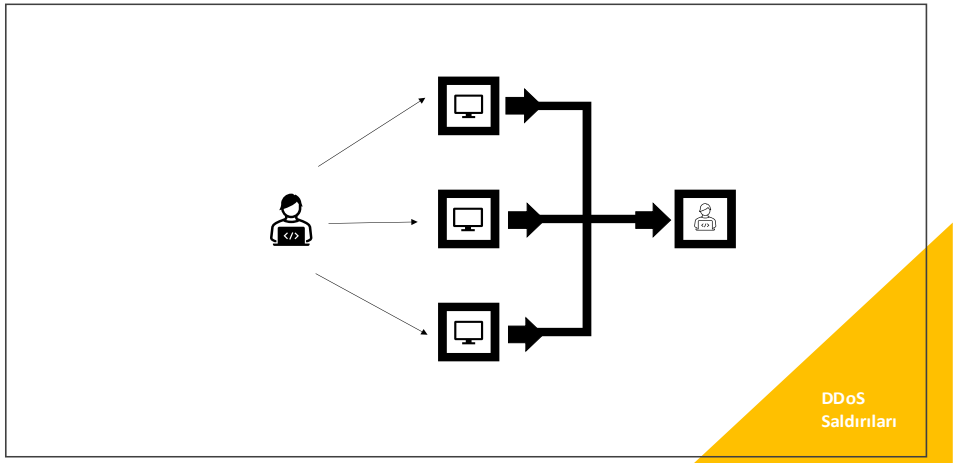
- Kötücül yazılım türleri şöyle özetlenebilir: *Trojan* (Truva Atı), *Spyware* (Casus Yazılım), *Adware* (Reklâm Yazılımı), *Bloatware* ya da *Crapware* (bilgisayarlara önceden yüklenmiş, bilgisayarları yavaşlatabilen tanıtım -promosyon- yazılımları), Virüs, *Ransomware* (Fidye Yazılımı), *Scareware* (Korkutucu Yazılım), *Worm* (Kendisini Çoğaltan Solucan Yazılım, Kurtçuk), *Rootkits* (kendisini gizleyen, uzaktan denetim sağlayan yazılımlar).

Oltalama Saldırısı (*Phishing*)

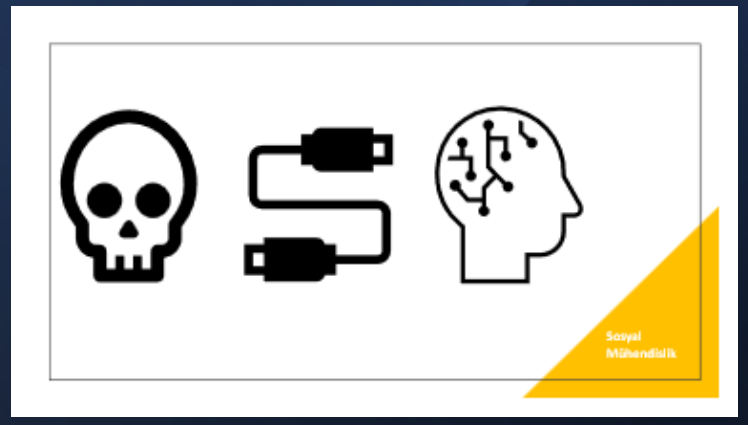
- Oltalama saldırısı, genellikle kimlik bilgileri ve kredi kartı numaraları olmak üzere kullanıcı verilerini çalmak için kullanılan bir tür sosyal mühendislik saldırısıdır. Güvenilir bir kişi kılığına giren saldırgan gönderdiği bir e-posta, anlık ya da kısa ileti ile hedef aldığı bireyi kandırır.
- Hedef alınan birey bu iletilerde yer alan bağlantı ya da eklentileri açtığında bilgisayarına saldırgan tarafından hazırlanmış kötücül yazılım yerleşir; oltalama saldırısı amacına ulaşır.

Dağıtımlı Hizmet Durdurma (DDOS) Saldırısı

- DDoS saldırısı hedef bir iletişim ağını ya da bilgisayar altyapısını bir İnternet trafiği seliyle baskılayarak bir sunucunun, hizmetin ya da ağın olağan trafiğini aksatmaya yönelik kötü niyetli bir girişimdir. Bir *DDoS* saldırısı, otobanı tıkayan beklenmedik bir trafik sıkışıklığını andırır, normal iletişim trafiğinin hedefine ulaşmasını engeller.
- DDoS saldırıları, saldırı trafiği kaynağı olarak birden çok ele geçirilmiş bilgisayar sistemi kullanılarak etkinlik sağlar. Kötüye kullanılan bilişim aygıtları; bilgisayarlar ve nesneağı [nesnelerin interneti: *IoT (Internet of Things)]* aygıtlarını ya da ağa bağlı diğer kaynakları içerebilir.



Sosyal Mühendislik



- Sosyal mühendislik, insan etkileşimleri yoluyla yapılan çok çeşitli ve kötü niyetli eylemler için kullanılan bir yöntemdir.
- Bu yöntem, kullanıcıları güvenlik yanlışları yapmaları ya da önemli bilgileri vermeleri için kandırmayı amaçlar.
- Sosyal mühendislik, siber saldırılar öncesinde hedefle ilgili bilgi toplamaya yönelik olarak yapılan bir ön çalışmadır, aynı zamanda.
- Saldırganlar bu yöntemle genellikle insani duyguları kötüye kullanırlar.

Siber Güvenlik Terimleri - devam

- **Derin Ağ** (*DeepWeb*)**:** Özel yazılımlarla ve yetkilendirmelerle erişilebilen bilgi ağlarıdır.
- **Karanlık Ağ** (*DarkNet* ya da *DarkWeb*)**:** Bir vekil sunucu (*Proxy, tor2web*) üzerinden, *candle, torch*, vb. yazılımlarla erişilebilen, İnternet'in gizli ve karanlık yüzüdür. Çalıntı kişisel bilgilerin ve uygunsuz içeriklerin yer aldığı, kaçakçılık ve silah satışı gibi amaçlarla kullanılan İnternet adresleri "karanlık ağ"dadır.
- **Tor:** "The Onion Routing" sözcüklerinin kısaltmasıdır; Türkçede "Soğan Tipi Yönlendirme" olarak adlandırılabilir. İnternet'e kimliksiz olarak erişim olanağı sağlayan ağ ve yazılım projesidir.
- **Derin Sahte** (*Deepfake*): Kişinin görüntüsünün başka bir kişinin ya da videoda yer alan bir kişinin görüntüsüyle değiştirilmesidir. Bu yapılırken ses ve görüntü uyumu için yapay zekâdan yararlanılmaktadır.
- **Sıfır Güven** (*Zero Trust*)**: "**Hiçbir kullanıcı ya da aygıta güvenme; her defasında doğrula" ilkesine dayanan güvenlik yaklaşımıdır.

Siber Tehdit İstihbaratı

- Siber tehdit istihbaratı, siber tehditlerle ilgili bilgilerin toplanması, çözümlenmesi ve yayılmasına odaklanan bir siber güvenlik çalışma alanıdır.

- Siber tehdit istihbarat kaynakları:
  - açık kaynaklar,
  - sosyal paylaşım uygulamaları,
  - insan kaynaklı istihbarat,
  - teknik istihbarat,
  - aygıtlarca üretilen günlük kayıtlar,
  - adli olaylar,
  - internet trafiği,
  - derin ve karanlık bilgiağları.

Güvenlik Operasyon Merkezi (SOC)

- Güvenlik Operasyon Merkezi, BT altyapısındaki çeşitli güvenlik olaylarını izlemek, tehditleri saptamak, çözümlemek ve bunlara yanıt vermek için oluşturulan merkezi bir güvenlik birimidir.
- Birincil amacı, siber saldırıların etkisini en aza indirmek, çok önemli verileri korumak ve bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamaktır.

Siber Dayanıklılık

- Siber dayanıklılık, bir kuruluşun siber saldırıları öngörme, bunlara karşı koyma, bunlardan kurtulma ve bunlara uyum sağlama yeteneğidir.


Siber
Güvenlik
Uzmanlıkları

Nasıl Siber Güvenlik Uzmanı Olunur?

Bilişim-Mühendislik-Örgün Öğretim

Bilgisayar Mühendisliği	Yazılım Mühendisliği	Bilişim Sistemleri Mühendisliği
Bilgisayar Programlama	Bilgisayar Programlama	Bilgisayar Programlama
Bilgisayar Mimarisi	Yazılım Mimarisi	BT Mimarisi
Bilgisayar Ağları ve İşletim Sistemleri	Bilgisayar Ağları ve İşletim Sistemleri	Bilgisayar Ağları ve İşletim Sistemleri
Veri Yapıları	Veri Yapıları	Veri Yapıları
Mikroişlemciler	Yazılım Gereksinim Mühendisliği	Veri Ambarı ve Veri Madenciliği
Sayısal Devreler	Çözümleme (Analiz) ve Tasarım	Bilgi Sistemleri Geliştirilmesi
Olasılık	Yazılım Kalite Güvencesi	Olasılık
İstatistik	Sistem Yazılımı Sınama ve Geçerleme	İstatistik
Veritabanı Tasarımı ve Yönetimi	Veritabanı Tasarımı ve Yönetimi	Veri Tabanı Tasarımı ve Yönetimi
Algoritma	Algoritma	Algoritma
Eniyileme (Optimizasyon)	Eniyileme (Optimizasyon)	Eniyileme (Optimizasyon)
Matematik-Fizik-Kimya	Matematik-Fizik-Kimya	Matematik-Fizik-Kimya
Yazılım Mühendisliği	Yazılım Proje Yönetimi ve Ekonomisi	Yazılım Mühendisliği
		Yönetim Bilişim Sistemlerine Giriş
		Bilgisayar Güvenliği

İlgili bölümlerin sayıları ve 2025 yılı için açıklanan kontenjanlar

BÖLÜMLER	ÜNİVERSİTE SAYISI	BÖLÜM SAYISI	KONTENJAN
Adli Bilişim Mühendisliği	1	1	55
Bilgisayar Mühendisliği	173	189	14656
Bilişim Sistemleri Mühendisliği	10	10	495
Siber Güvenlik Mühendisliği	4	4	139
Yazılım Mühendisliği	78	85	5402
Yapay Zekâ Müh. Grubu			
YZ Mühendisliği	7	7	353
YZ ve Makine Öğr. Müh.	3	3	169
YZ ve Veri Müh.	13	13	451
TOPLAM	**289**	**312**	**21.720**

Kaynak:
dergi.bmo.org.tr

SİBER GÜVENLİK UZMAN YETKİNLİĞİ (temel düzey)

- 4 yıllık bilgisayar mühendisliği veya ilgili mühendislik bölümlerinden mezun olmak için
  - Matematik: Türev, integral, ayrık matematik
  - Temel bilimler: Fizik, kimya, biyoloji
  - Olasılık
  - İstatistik
  - Bilgisayar bilimleri bilgisi
  - Mühendislik bilgisi
  - Yazılım ve donanım bilgisi

VEYA (uyum programları);

- Temel Bilimler
- Temel işletim sistemleri bilgisi
- Temel veri yapıları bilgisi
- Temel iletişim ağları bilgisi
- Temel yazılım geliştirme bilgisi (yapısal ve nesneye yönelik yazılım geliştirme)
- Temel düzeyde şifreleme bilgisi

*ABET (Accreditation Board for Engineering and Technology), ABD

- EUR-ACE (EURopean ACcredited Engineer Label)
- MÜDEK (Avrupa Mühendislik Eğitimi Akreditasyon Ağı: ENAEE-European Network for Accreditation of Engineering Education).

SİBER GÜVENLİK UZMAN YETKİNLİĞİ (ileri düzey/seçmeli)

Seçmeli Dersler

- Siber güvenlikte makine öğrenme
- Sızma ve siber saldırı önleme teknikleri
- Bilgi güvenliği denetimi
- …

Veya Onaylanmış Yetkinlikler (Sertifikasyon)

- OSCP (Offensive Security Certified Professional)
- OSEP (Offensive Security Experienced Penetration Tester)
- OSWE (Offensive Security Web Expert)
- GPEN (GIAC* Certified Penetration Tester)
- GREM (GIAC Reverse Engineering Malware)
- GCFA (GIAC Certified Forensic Analyst)
- …

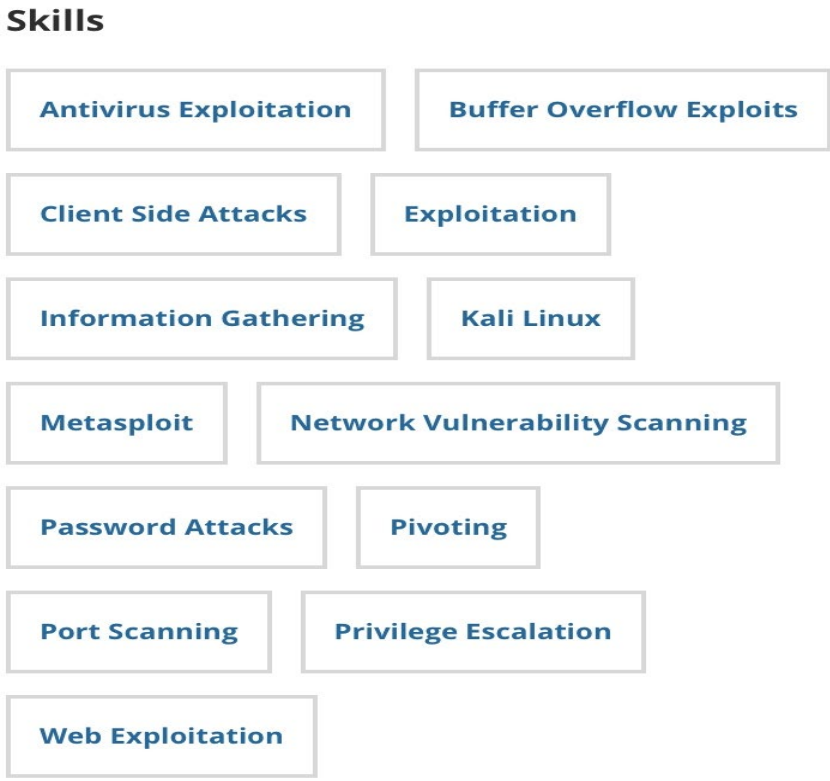
* Global Information Assurance Certification

SİBER GÜVENLİK UZMAN YETKİNLİĞİ (örnek onay belgeleri)

1. Siber Güvenlik Yönetimi
2. Siber Güvenlik Mimarisi
3. Siber Güvenlik Çözümlemesi
4. Siber Güvenlik Savunma Yöntemleri
5. Siber Saldırı Yöntemleri
6. Siber Güvenlik Mühendisliği

SİBER GÜVENLİK UZMAN YETKİNLİĞİ (onaylanmış yetkinlikler, örnek)

- OSCP (Offensive Security Certified Professional)
  - Yetenekler:
    - Virüs sistemini atlatma
    - Bellek taşırma
    - İstemci saldırıları
    - İstismar yöntemleri
    - Bilgi toplama
    - Kali Linux bilgisi
    - İstismar yazılımlarını kullanma
    - Ağ zayıflık kontrolleri
    - Şifre saldırıları
    - Ağ bağlantı noktalarının taranması/tespiti
    - Yetki yükseltme
    - Web sömürme



SİBER GÜVENLİK UZMAN YETKİNLİĞİ (onaylanmış yetkinlikler, örnek)

- CISSP (Certified Information Systems Security Professional)
  - Yetenekler:
    - Güvenlik ve Risk Yönetimi
    - Varlık Güvenliği
    - Güvenlik Mühendisliği
    - İletişim ve Ağ Güvenliği
    - Kimlik ve Erişim Yönetimi
    - Güvenlik Değerlendirme ve Test
    - Güvenlik Operasyonları
    - Yazılım Geliştirme Güvenliği

CISSP® Domains

The CISSP examination domains and weights are:

Domains	Weight
1. Security and Risk Management	16%
2. Asset Security	10%
3. Security Engineering	12%
4. Communication and Network Security	12%
5. Identity and Access Management	13%
6. Security Assessment and Testing	11%
7. Security Operations	16%
8. Software Development Security	10%
Total	**100%**

SİBER GÜVENLİK UZMAN YETKİNLİĞİ (diğer onaylanmış yetkinlikler)

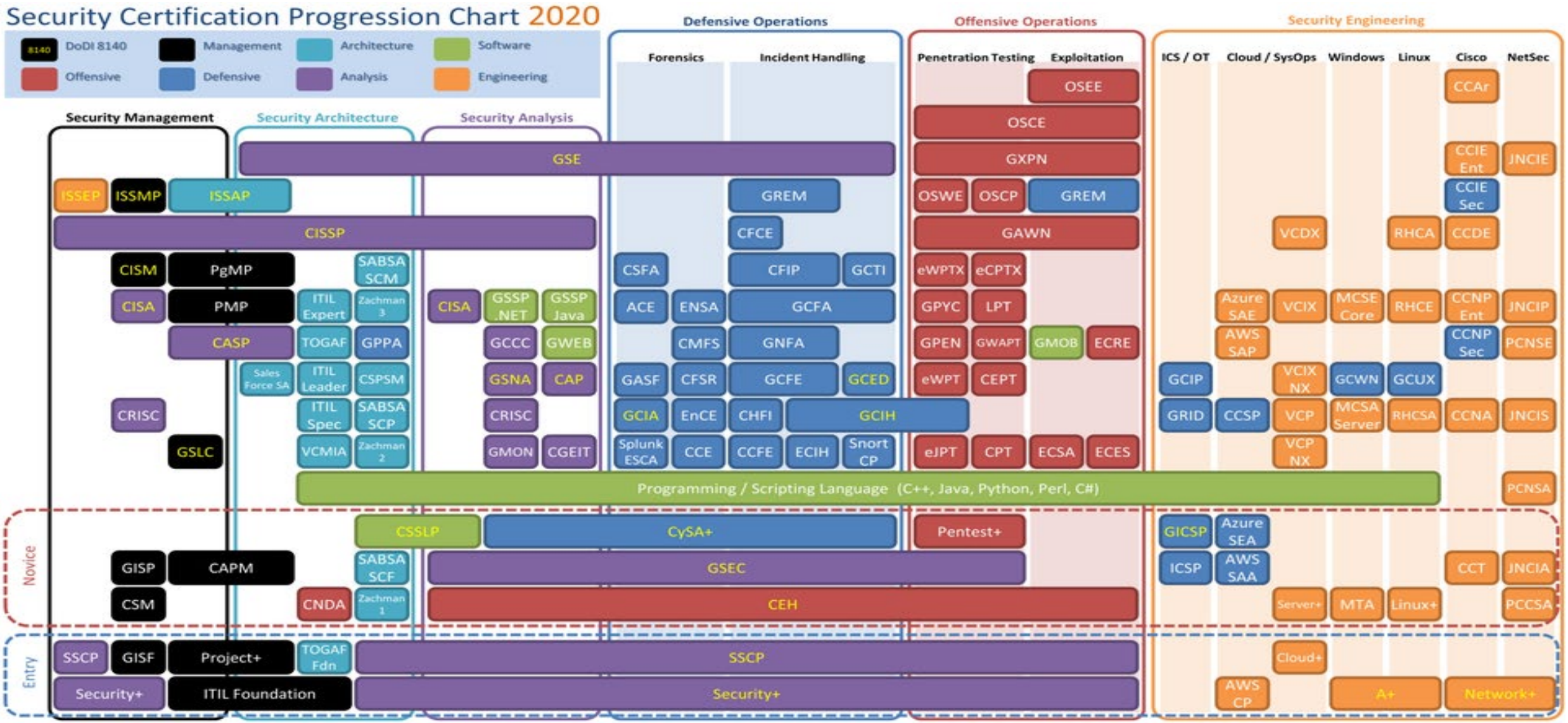
- CISA (Certified Information Security Auditor)
- GCIH (GIAC Certified Incident Handler)
- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Information Systems Security Engineering Professional (CISSP-ISSEP)
- Information Systems Security Management Professional (CISSP-ISSMP)

Siber Güvenlik Uzmanlıkları

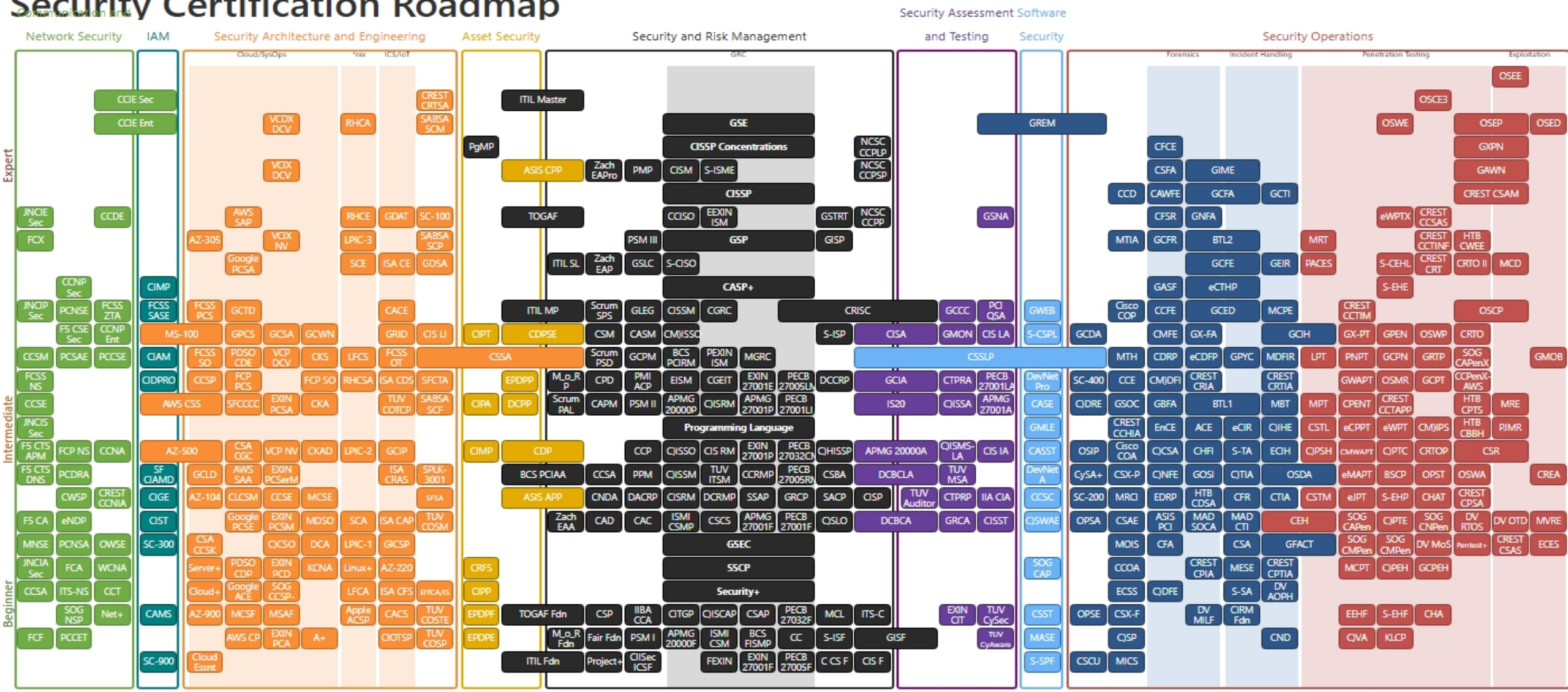
- Siber Güvenlik Danışmanı
- Siber Güvenlik Mimarı
- Siber Güvenlik Mühendisi
- Siber Güvenlik Olay İzleme / Önleme Uzmanı
- Tersine Mühendislik / Zararlı Yazılım Çözümleme Uzmanı
- Siber Güvenlik Sızma Testi Uzmanı
- Kırmızı Takım (Siber Atak) Mühendisi
- Mavi Takım (Siber Savunma) Mühendisi
- Bilgi Güvenliği Risk Yöneticisi
- Şifreleme (*Crypthology*) Uzmanı
- Adli Bilişim Uzmanı
- Siber Güvenlik Denetim Uzmanı
- Güvenli Yazılım Denetçisi
- Zayıflık Yönetimi Uzmanı
- Bilgi Güvenliği Uyum Uzmanı
- → YZ Güvenlik Uzmanı

SİBER GÜVENLİK UZMAN YETKİNLİĞİ

örnek onay belgeleri (https://www.reddit.com/)



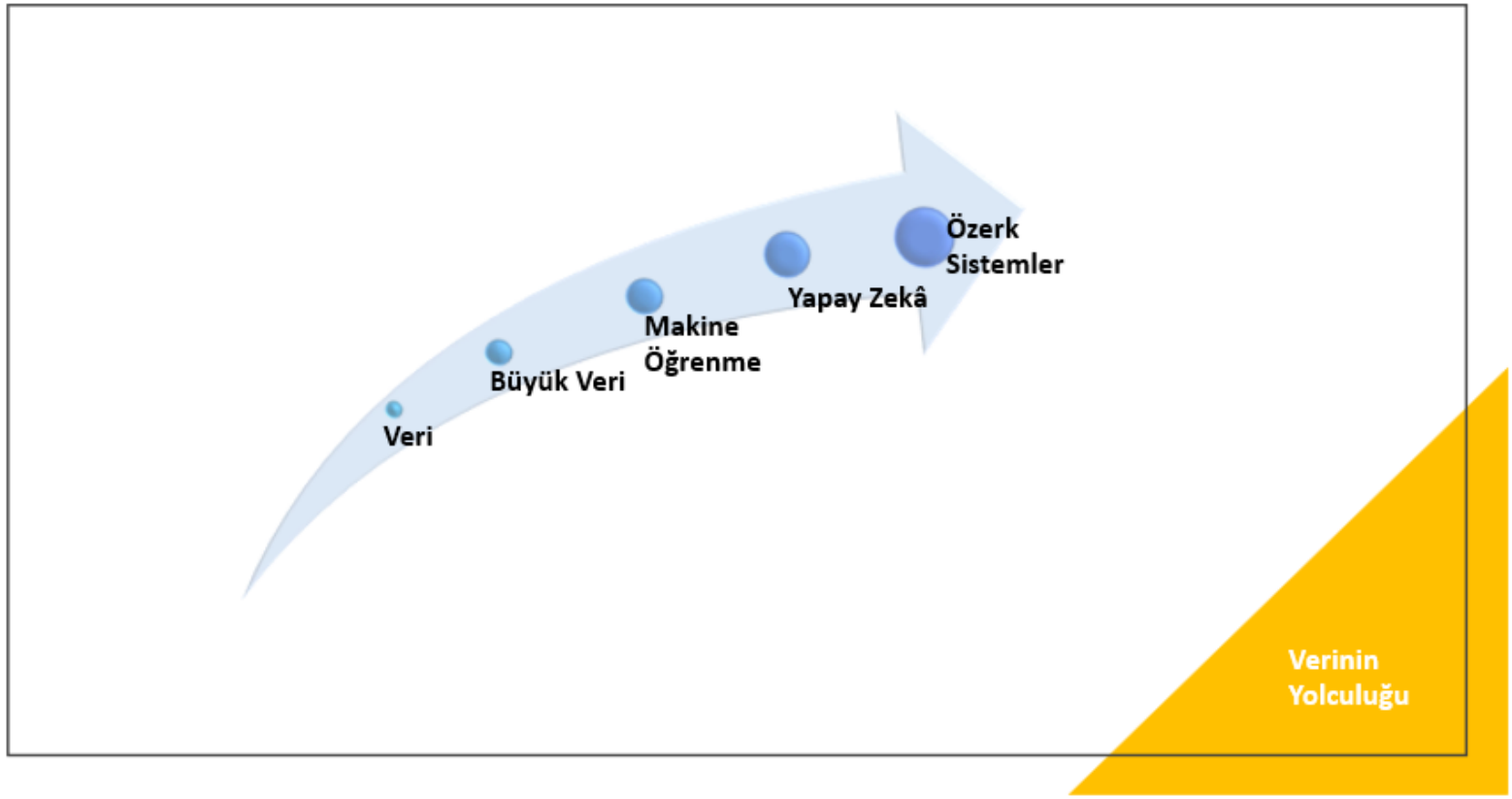
Security Certification Roadmap



481 certifications listed | July 202


Yeni Teknolojiler ve Siber Güvenliğe Etkisi

Verinin Yolculuğu



Yapay Zekâ ve Kuantum Bilgisayarlar Siber Güvenlikte Oyunun Kurallarını Yeniden Yazdırıyor

- 2009 Bulut Bilişim
- 2013 Büyük Veri, Nesnelerin İnterneti
- 2015 Özerk Sistemler
- 2016 Makine Öğrenme
- 2017 YZ, Gelişmiş Derin Öğrenme, Blokzincir
- 2019 YZ Destekli Yazılım Geliştirme, Kuantum Bilişim
- 2021 YZ Mühendisliği, Davranışların İnterneti
- 2022 YZ Güvenliği, Üretken YZ (verilerden yeni veri üretme, yazı, görüntü)
- 2023 Uyarlanır YZ, YZ Risk ve Güvenlik Yönetimi
- 2024 YZ Risk ve Güvenlik Yönetimi
- 2025 Kuantum Sonrası Kriptografi
- 2026 YZ Güvenlik Uygulamaları

Yapay Zekâ ve Siber Güvenlik

YZ;
İnsan hatalarını azaltmada,
Doğru karar ve sonuç almada,
Benzetim (simülasyon) yapmada,
Örnek senaryoların uygulanmasında daha etkili duruma gelecek.

YZ;
İzleme, tehdit saptama ve önleme süreçlerin kotarılmasında,
Güvenlik açıklarının saptanması ve yönetilmesinde,
Tehdit istibaratının toplanmasında,
Siber güvenlik otomasyonunda,
Şifre yönetiminde,
YZ destekli güvenli kod geliştirmede,
Risk çözümlemede,
Güvenlik eğitimleri düzenlenmesinde ve değerlendirilmesinde,
Sızma testlerinin, kırmızı takım simülasyonların yapılmasında,
Olay çözümlemede kullanılabilir.

Kötü taraf: sosyal mühendislik, yanıltıcı bilgi, saldırı öncesi keşif, sömürü (exploit) yazılımları geliştirme ve siber saldırılar…

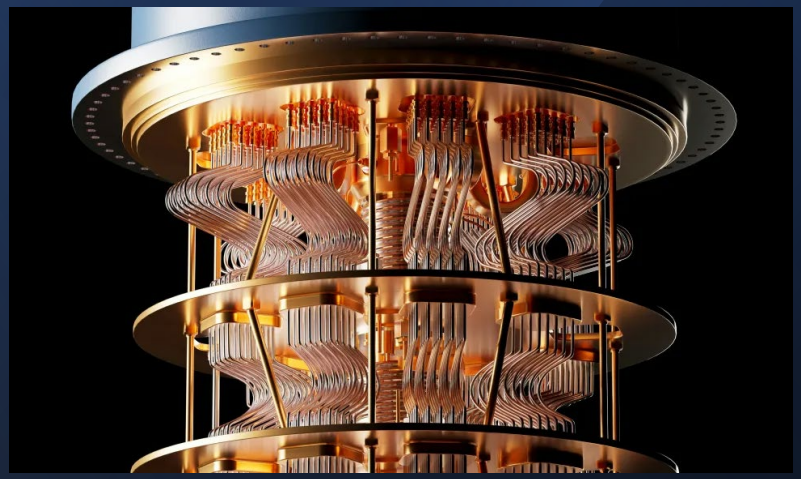
YZ YZ’ye Karşı...

YZ;

Hem saldırı hem de savunma tarafında olacak!

Atak yüzeyinin yeni bileşeni YZ… (istismar yazılımları (exploits), prompt injection (istem yerleştirme), deepfake (derinsahte))…

Kuantum Bilgisayarlar ve Siber Güvenlik



Kuantum bilgisayarlarla;

Kriptolama / kripto çözme,

Eniyileme,

DNA dizilimi,

İlaç etkileşimleri, vb.

işlemler daha hızlı sonuçlandırılacak.

Kriptografi kırılmazlık algısına dayanır,

Kuantum bu algıyı yıkıyor!!!

RSA 2048 bit şifrelemeyi kırmak için 300 trilyon yıl gerekiyor. Kuantum bilgisayar 4096 kararlı kübitle bunu 10 sn'de yapılabilecek...

Kuantum Bilgisayarlar ve Siber Güvenlik

Q-day/k-günü/kuantum günü:
Binlerce yıl sürecek işlemler sn'ler içinde tamamlanabilir.

2024 yılında Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) kuantum sonrası şifreleme standartları belgesini yayımladı.

- Kuantumun etkilerini azaltmayı amaçlıyor.

Kuantum farkındalığı zamanı! Kuantum sonrası için güvenli şifreleme ve anahtarlama konusu önemli!

Kuantum farkındalığı:
Planlama, envanter çıkarma (şifrelenmiş veriler), şifreleme anahtarlarının döndürülmesi…

Kuantumla ilgili gelişmelerin dikkatle izlenmesi gerekiyor…

Kötü taraf: YZ ve Kuantum'un insan denetiminin önüne geçmesi öngörülemeyen sonuçlara yol açabilir.

Siber Güvenlik Teknolojilerinde Dün Bugün Yarın

Yakın Geçmiş

İmza Tabanlı Saldırı Önleme Sistemleri

İnsan müdahalesine bağımlı güvenlik süreçleri

Bugün

Davranış Tabanlı Saldırı Önleme Sistemleri

Büyük Veri Çözümleme (log, dosya, paket) Uygulamaları

Yapay Zekâ Kullanımı

Makine Öğrenme Süreci

Tam Otomasyon

Siber Dayanıklılık

Yakın Gelecek

Siber Güvenlikte Nicem (Kuantum) Bilgisayarların Kullanımı

(Kapasite ve Hız Kazanımı)

Siber Güvenlik Uzmanlığı Açığının Kapatılmasında Yapay Zekâdan Yararlanılması

(Güvenlik Verilerinin Hızlı ve Doğru Bir Şekilde Çözümlenmesine Yardımcı Olması)

Bulut Uygulamalarının Artması

Siber güvenli bir gelecek dileğiyle…

Basit ama etkili önlemler:

- Bilişim araçlarında ve uygulamalarda güçlü parolalar kullanmak,
- Önemli bilgileri düzenli olarak yedeklemek,
- Donanım ve yazılımları güncel tutmak,
- Şüpheli bağlantıları açmamak,
- Sanal ortam hesaplarını ve gizlilik ayarlarını dikkatli yönetmek.


https://pekelahmet.com