TSE BİLİŞİM TEKNOLOJİLERİ STANDARTLARI VE BELGELENDİRMELERİ

Bilginin giderek en değerli varlık haline geldiği çağımızda, tüm dünyada Bilişim Teknolojileri ve Bilgi Güvenliği konularında yapılan çalışmalar her geçen gün artmaktadır.

Günümüzde bilişim teknolojilerinde de standardizasyon, güvenlik, performans ve kalite kontrolleri çok önemli hale gelmiştir. Yazılım ürünlerinin güvenliği, kalitesi, performansı, ürün oluşturulurken izlenen yollar, şifreleme-kriptoloji gibi konular BT ürün ve sistemleri için vazgeçilmez olmakla birlikte, uluslar arası standartlara göre bağımsız laboratuvarlarda test edilip, bağımsız belgelendirme kuruluşları tarafından sertifikasyonu ayrıca önem arz etmektedir.

Türk Standardları Enstitüsü Ürün Belgelendirme Merkez Başkanlığı Bilişim Teknolojileri Belgelendirme Müdürlüğü (http://bilisim.tse.org.tr/) "Bilişim Teknolojileri" ve "Siber Güvenlik" alanlarında, hızla ilerleyen teknolojiye paralel olarak, uluslar arası standartlardan ulusal ve uluslar arası akreditasyona sahip olarak, BT ürün ve sistemleri için test ve belgelendirme hizmeti vermektedir, bunlar özetle;

- **ORTAK KRİTERLER (Common Criteria)-TSE-CCCS sertifikası:**
  TS ISO/IEC 15408 serisi BT ürünlerinin güvenliği için değerlendirme kriterleri

- **SPICE-TSE-SPICE sertifikası:**
  TS ISO 15504-SPICE Yazılım Süreçleri Değerlendirilmesi ve İyileştirmesi (ISO CMMI)

- **BİLİŞİM TEKNOLOJİSİ- TSE-sertifikası:**
  TS 13298 Elektronik Belge Yönetimi
  TS ISO/IEC 25051 Yazılım Paketleri Belgelendirmesi
  TS ISO 9241-151 Web Sayfalarının Belgelendirmesi

- **UYGUNLUK DEĞERLENDİRMESİ :**
  TS ISO/IEC 12207 Yazılım Yaşam Döngüsü
  TS ISO/IEC 15288 Sistem Yaşam Döngüsü

- **KRİPTO MODÜL ve ALGORİTMA BELGELENDİRMESİ (ISO FIPS 140-2)**
  TSE-CMVP ve TSE-CAVP sertifikaları:

  TS ISO/IEC 19790: Kripto Modülleri Güvenlik Gereksinimleri
  TS ISO/IEC 24759: Kripto Modülleri Test Gereksinimleri

BT ürünlerin ve/veya sistemlerinin tüm bu standartlara uygunluğunun ölçülebilmesi, ve değerlendirilebilmesi bağımsız test laboratuvarlarında yapılmaktadır.

TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü olarak TS ISO/IEC 15408-BT Ürün Güvenliği Ortak Kriterler alanında 3 lisanslı ve 2 aday laboratuvar vardır:

- TÜBİTAK BİLGEM OKTEM-lisanslı
- EPOCHE & ESPRİ-lisanslı
- CYGNACOM (Amerika)-geçici lisanslı
- APPLUS LGAI (İspanya)-aday
- BEAM TEKNOLOJİ (Türkiye)-aday

Diğer BT standartlarında taşeron laboratuvarlarımız:

- TÜBİTAK BİLGEM BTE-lisanslı
- EPOCHE & ESPRİ-lisanslı
- ODTÜ İBE Laboratuvarı-lisanslı
- TÜBİTAK BİLGEM UEKAE-Birlikte Çalışabilirlik Laboratuvarı -aday

SİBER SAVAŞLAR, SİBER SAVUNMA VE SİBER GÜVENLİK

Dünyada artık "**Siber Saldırı**", "**Siber Güvenlik**", "**Siber Ordu**", "**Siber Terorizm**" "**Siber Bakan**", "**Siber Savunma**" terimleri sıklıkla kullanılmaktadır. 2010 Kasım ayında ABD`de "Wikileaks" olarak adlandırılan Gizli Diplomatik ve Askeri Belgelerin ifşası, 2007 yılında Rusya-Estonya Siber Savaşı, İran Nükleer Sisteminin Rusya tarafından durdurulması vb. Siber Savaşların dünyadaki örneklerinden sadece birkaçıdır.

Günümüzde "Siber Savaşlara" karşı "Siber Güvenlik ve Savunma" stratejileri geliştirmemiz ve ülkemizin "Kritik Altyapıları" olan "Bilgi ve iletişim, Enerji, finans, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği, nükleer biyolojik ve kimyasal tesisler" imizi korumak için gereken tedbirleri almamız son derece önemlidir.

İçinde bulunduğumuz "Bilgi ve İletişim" çağında bahsi geçen ve Kritik Altyapılarımız olan "Enerji, finans, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği, nükleer biyolojik ve kimyasal tesisler" artık manual fiziksel yöntemlerle kontrol edilmemekte, bu sistemler "Uygulama Yazılım" larıyla uzaktan kontrol edilmektedir. Bu uzaktan kontrol hız ve performans kazancı sağlarken, malesef kötü niyetli kişi/kurum vb. lar için de "Siber Saldırı" ortamı haline gelmekte, güvensiz test edilmemiş yazılımlar ve donanımlar yüzünden çok değerli olan "Kritik Altyapılarda" tolere edilemeyecek maddi kayıplar yaşanabilmektedir.

İran siber saldırılardan büyük yara almış ve SCADA sistemleri ciddi zarar görmüştür.

Siber savaşların önemini vurgulayacak başka bir örnek de, ABD'nin siber ordu kurmasıdır.

Siber güvenliğin önemini bizlere gösteren diğer örnekler ise;

- **Wikileaks :** ABD`nin Gizli Diplomatik ve Askeri Belgelerin ifşası, **Kasım 2010**

- **DDOS Saldırıları :** Hemen her gün bir siteye yapılan bu saldırılar temel olarak hack olarak kabul edilmese de, o siteye ulaşılabilirliği kısıtlaması, hatta durdurması yüzünden kişilere ve kurumlara büyük zararlar verebilmektedir.

Rusya-Estonya Siber Savaşı ise diğer örneklerden biridir.

Her ülkenin kritik varlıkları vardır. Bunlar korunamadığı takdirde ülke güvenliği büyük risk altına girer. Bu da çok daha büyük sorunları beraberinde getirir. Bu kritik varlıklar;

- Enerji
- Savunma
- Finans
- Sağlık
- Gıda
- Su
- Ulaşım
- Bilgi ve iletişim
- Kamu güvenliği
- Nükleer, biyolojik ve kimyasal tesisler

olarak sıralanabilir.

Bahsi geçen ülke kritik altyapılarından herhangi birinde bir sorun çıkması, ülkenin kaosa sürüklenmesine neden olabilecektir. Bu sorun tamamen kaldırılamayacağı gibi, büyük oranda azaltılabilir.

Ortak Kriterler ve Siber Güvenlik

TS ISO/IEC 15408- BT Ürünleri Güvenliği-Ortak Kriterler

Ortak Kriterler, Bilişim teknolojisi ürünleri için geliştirilmiş güvenlik değerlendirme standartları olan ISO/IEC 15408 ve ISO/IEC 18045 standartlarıdır. CTCPEC (Kanada), TCSEC (A.B.D) ve ITSEC (Avrupa) standartlarının "Common Criteria" adı altında birleşmesi ile Ocak 1996'da yayınlanmıştır.

CCRA-Ortak Kriterler Tanıma Anlaşması:

Ortak Kriterler Uluslararası Tanıma anlaşmasıdır. Bu anlaşmayı imzalayan ülkeler, ürün hangi ülkeden sertifika almış olursa olsun o ürünün belirtilen seviyede güvenli olduğunu kabul etmiş sayılırlar.

Ortak Kriterler standardı 2012 itibariyle 26 ülkede geçerliliği bulunan bir standarttır. Bu 26 ülkeden 15'i Certificate Authorising Member (sertifika üretici üye), 11'i ise Certificate Consumer Member (sertifika müşterisi üye) ülkelerdir.

SERTİFİKA ÜRETİCİLERİ

1. **Türkiye- 3 (2 aday)**
2. **Almanya - 12**
3. **Amerika – 9**
4. **İtalya - 6**
5. **Fransa – 5**
6. **Güney Kore – 5**
7. **Japonya – 4**
8. **Norveç - 4**
9. **İngiltere – 3**
10. **Kanada – 3**
11. **Avustralya ve Yeni Zelanda – 3**
12. **İspanya - 3**
13. **İsveç - 2**
14. **Hollanda – 1**
15. **Malezya-2**

SERTİFİKA MÜŞTERİLERİ

1. **Avusturya**
2. **Çek Cumhuriyeti**
3. **Danimarka**
4. **Finlandiya**
5. **Yunanistan**
6. **Macaristan**
7. **Hindistan**
8. **İsrail**
9. **Singapur**
10. **Pakistan**

ADAY: Çin

Sertifika üretici ülkelerin yanındaki sayılar, o ülkelerin laboratuvar sayısını göstermektedir.

Sertifika Üretici Ülke olabilmek için, öncelikle Sertifika Müşterisi Ülke olmak ve gerekli şartları yerine getirdikten sonra başvurunun onaylanması gerekmektedir.

TÜRKİYE`DE ORTAK KRİTERLER TARİHÇESİ

TSE-ORTAK KRİTERLER BELGELENDİRME SİSTEMİ (OKBS)

- Türkiye`de Ortak Kriterler programı ilk defa **2001** yılında **Genel Kurmay Başkanlığı(TGS) tarafından Türk Silahlı Kuvvetleri** için başlatıldı.
- Türkiye'nin belgelendirme kuruluşu olarak **TSE**, **2003** yılında CCRA'ya imzaladığı anlaşma ile **"Sertifika Müşterisi"** olarak üye olmuştur.
- Türkiye`de ilk Kamu Ortak Kriterler Değerlendirme Laboratuvarı **2003**'te **TUBİTAK UEKAE** bünyesinde **Ortak Kriterler Test Merkezi(OKTEM)** adı altında bağımsız olarak çalışmalarına başladı.
- Ortak Kriterler Belgelendirme Sistemi**(OKBS) 2005** yılında TSE Ürün Belgelendirme Merkezi altında kuruldu.
- TSE, **2008** yılında CCRA'da yapılan düzenleme gereğince "**Sertifika Üreten Ülke – Authorizing Country"** olmak için başvuruda bulundu.
- **12-16 Nisan 2010** tarihleri arasında TSE OKBS, CCRA tarafından yapılan Uluslar arası Tetkikten (Shadow Assesment) **"Başarı"** ile geçti.
- **17 Kasım 2010** tarihinde Türkiye`nin "**Sertifika Üreten Ülke – Authorizing Country"** olarak resmi duyurusu yapıldı ve Türkiye bu alandaki 15 ülkeden biri oldu.

TS ISO/IEC 15408-BT Ürünleri Güvenliği Ortak Kriterler standardı hangi kontrolleri yapar?

1. Tasarım sürecini sorgular,
2. Teslim & Kurulum sürecini sorgular,
3. Tasarım dokümanlarının içerik yeterliliğini sorgular,
4. Kaynak kodu sorgular,
5. Kılavuz dokümanları sorgular,
6. Yaşam Döngüsü Modeli'ni sorgular,
7. Geliştirme araçlarını sorgular,
8. Geliştirme ortamının güvenliğini sorgular,
9. Test dokümanlarını sorgular (fonksiyonel, bağımsız ve sızma testleri),

suretiyle gerçekleştirir.

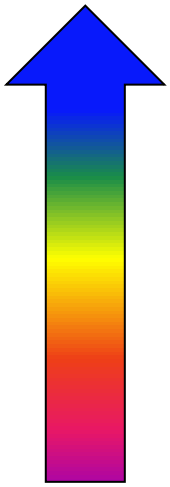
Özetle; Ortak Kriterler, BT ürününün BT ürününün yeterli bir geliştirme ortamında gerçeklenip gerçeklenmediğini kontrol eder, var olan tehditleri analiz eder, **Fonksiyonel**, **Bağımsız** ve **Sızma** testleri (Açıklık Analizi çalışması) yapar ve ürüne uygun garanti seviyesini verir.

Garanti Seviyeleri

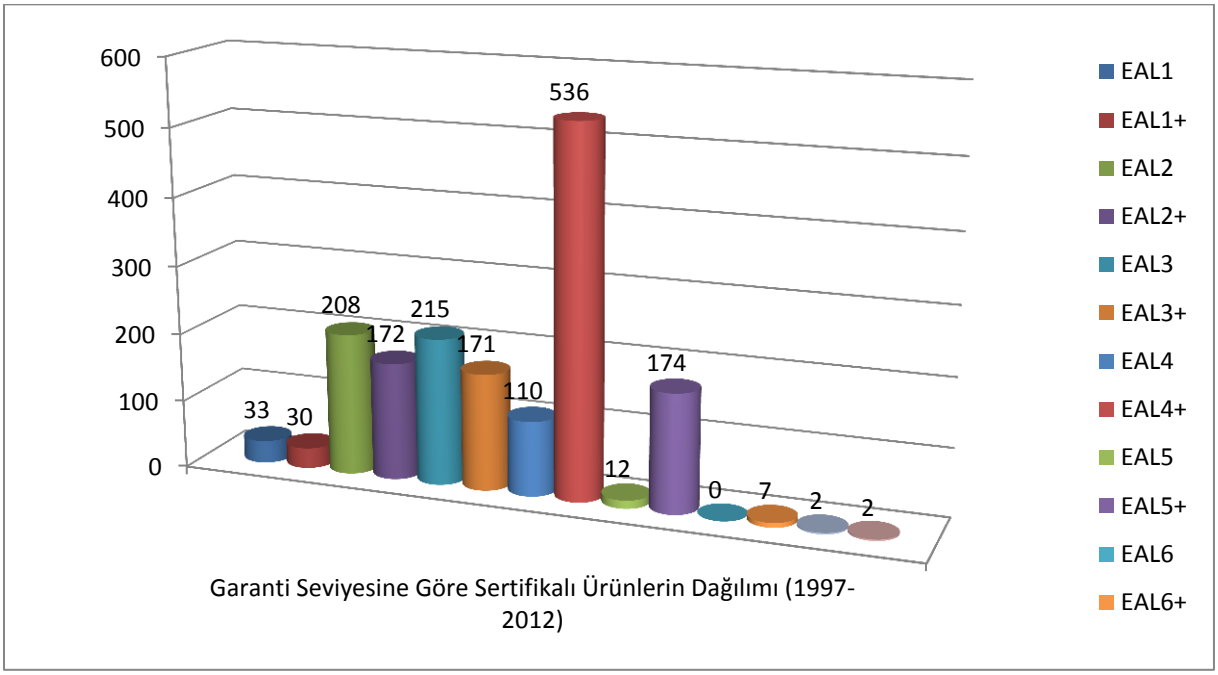
Ortak Kriterler tanımlanmış, garanti seviyesi gittikçe artan ve Değerlendirme Garanti Seviyesi (EAL) olarak bilinen 7 adet Güvenlik Seviyesi (garanti paketi)sağlamaktadır:

YÜKSEK ATAK POTANSİYELİ, WHITE BOX TEST, YÜKSEK KALİTE

- **EAL7:**
- **EAL6:**
- **EAL5:**
- **EAL4:**
- **EAL3:**
- **EAL2:**
- **EAL1:**



DÜŞÜK ATAK POTANSİYELİ, BLACK BOX TEST, DÜŞÜK KALİTE



Garanti Seviyesine Göre Sertifikalı Ürünlerin Dağılımı (1997-2012)

TSE-OKBS Son Durumu:

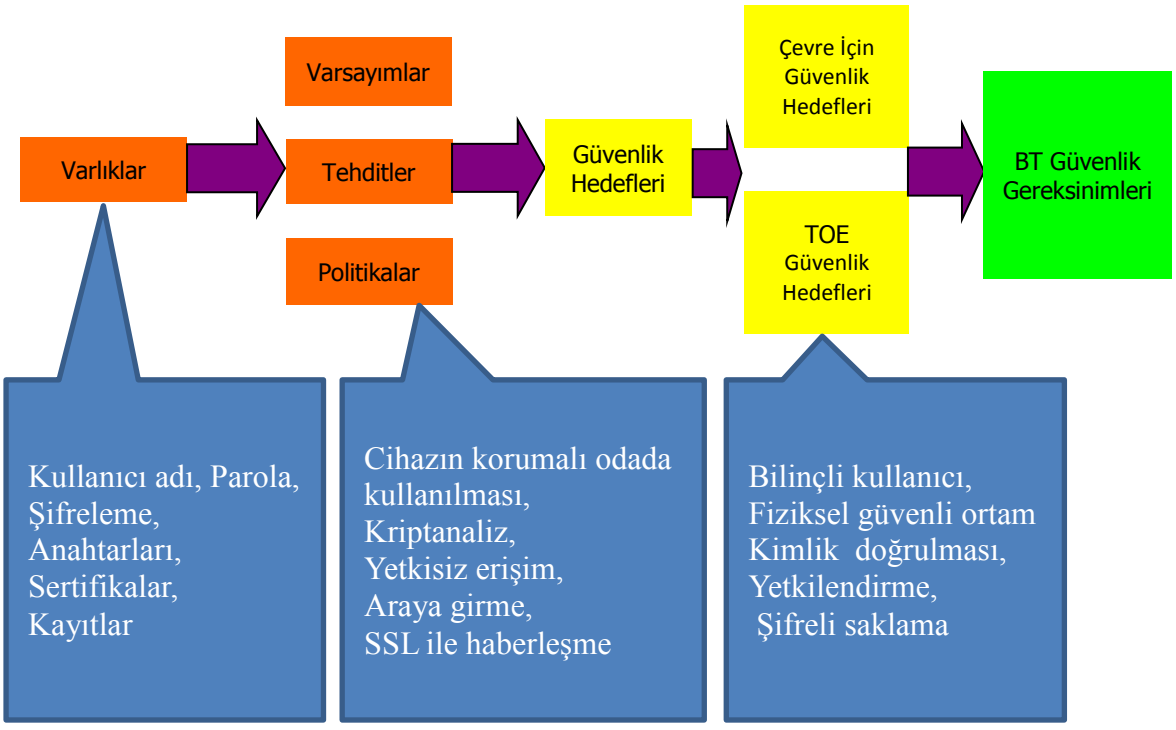
- **12 ürün** sertifikalandırılmış,
- **1 PP** sertifikalı, **1 PP** değerlendirmede

- **12 ürün** değerlendirmede
- **5 PP** geliştirilmekte. (Ulusal Koruma Profili Havuzu)
- Sertifika üreten ülkelerin değerlendirip, sertifikalandırdığı ürünler "Uluslar arası geçerli Güvenli BT Ürünü" olmakta ve www.commoncriteriaportal.org adresinde yayınlanmaktadırlar.
- **3 adet Lisanslı CC lab**. mevcut.
- **2 adet Aday CC lab**.

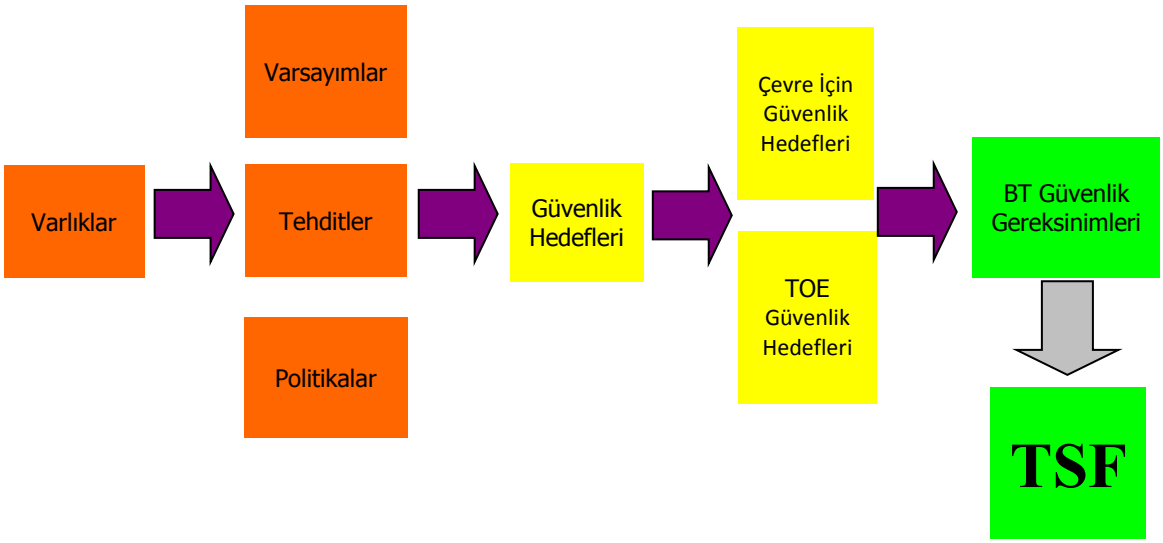
Ortak Kriterler Genel Kavramlar

- **TOE** (Target of Evaluation): Ürün'ün Değerlendirme Hedefi
- **ST** (Security Target): Güvenlik Hedefi, TOE güvenlik iddialarının belirtildiği dokümandır.
- **PP** (Protection Profile): Koruma Profili, CC standardına uygun olarak yazılmış Teknik Şartnamelerdir. ST'ler için şablon dokümanlardır.

PP-Koruma Profili:



ST-Güvenlik Hedefi:



Ortak Kriterler Sertifikasyonu **Siber Savaş** için en büyük önlemlerden birisidir.

Türkiye`de BT Ürünleri Güvenliği ile İlgili Yeni Projeler

- **Ulusal Koruma Profili (PP) Havuzu Projesi:**

  Bu proje kapsamında aşağıdaki ürün gruplarında Koruma Profilleri oluşturulacaktır:
  - EBYS
  - HBYS
  - E-Ticaret
  - CBS
  - Akıllı Sayaçlar
  - Web Uygulamaları Güvenliği
  - Information Gateway…

- **Smart Card Security Turkey Consortium (SCS-Turkey):**
  TOBB, SABANCI, İTÜ ,TÜBİTAK ve TSE olmak üzere 5 ortakla kurulmuş olup, amaç SOGIS-MRA ya girmektir, Japonya` da da benzeri bir konsorsiyum oluşturulmuştur.

SCS TURKEY
SMART CARD SECURITY
TURKEY CONSORTIUM

TSE KRİPTO BELGELENDİRMESİ

TSE
CRYPTO

Kripto Modül Doğrulama Programı (CMVP)

Kripto Algoritma Doğrulama Programı (CAVP)

(ISO FIPS 140-2,3):

Kripto Modülleri İçin Güvenlik Gereksinimleri(TS ISO/IEC 19790)

Kripto Modülleri İçin Test Gereksinimleri(TS ISO/IEC 24759)

- **4 adet güvelik seviyesi vardır.**
  i) Güvenlik Seviyesi 1
  ii) Güvenlik Seviyesi 2
  iii) Güvenlik Seviyesi 3
  iv) Güvenlik Seviyesi 4

- **Değerlendirmeler 10 ayrı alana göre yapılmaktadır. Bu alanlar;**

1) Kriptografik Modül Spesifikasyonu(Cryptographic Module Specification)
2) Kriptografik Modül Port ve Arayüzleri(Cryptographic Module Ports and Interfaces)
3) Roller, Servisler ve Kimlik Doğrulama(Roles, Services and Authentication)
4) Finite State Model
5) Fiziksel Güvenlik(Physical Security)
6) Çalışma Ortamı(Operational Environment)
7) Kriptografik Anahtar Yönetimi(Cryptographic Key Management)
8) Self Tests
9) Tasarım Güvencesi(Design Assurance)
10) Diğer Ataklara Karşı Savunma(Mitigation of Other Attacks)

TSE YAZILIM TEST LABORATUVARI

2013 ün ilk çeyreğinde faaliyete geçecek olan Yazılım Test Laboratuvarında il aşamada aşağıdaki testler yapılacaktır;

- TS ISO/IEC 27001 kapsamında Network ve Web Uygulamaları Sızma-Penetrasyon Testleri
- Yazılımlara Beyaz Kutu(White Box)-Source Code Sızma Testleri
- Yazılımlara Kara Kutu (Black Box) Testleri
- TS ISO/IEC 25051 Fonksiyonel Testleri
- TS ISO/IEC 13298 Performans Testleri

SONUÇ

TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü, gelişen teknolojiyi takip ederek, test ve belgelendirme çalışmalarını hızla sürdürmekte ve ülkemize Bilişim Teknolojileri ve özellikle de Siber Güvenlik alanında yeni ve faydalı hizmetler sunmaya devam edecektir.