BİLGİ TEKNOLOJİLERİ YÖNETİMİ

MODELLER VE STANDARTLAR

TS ISO IEC 15408 Ortak Kriterler Belgesi

İÇİNDEKİLER;

1. TARİHÇESİ:

Bilgi Teknolojileri kullanıcıları arasında yapılan araştırmalar göstermektedir ki, kullanıcılar satın aldıkları ürün için satıcının garanti ettiği güvenlik düzeyine güvenmedikleri gibi, ürünlerin güvenlik testlerini kendileri de yapmak istememektedirler. Çözüm olarak da bağımsız üçüncü bir tarafın, BT ürünlerini analiz etmesini ve testler aracılığıyla güvenlik garanti düzeyini belirlemesini istemektedirler.

Bu ihtiyaç, ülkelerin kabul ettiği güvenlik kriterlerine uygun olarak test yapan laboratuvarların kurulmasını sağlamıştır. Başlangıçta her ülke, o ülkenin kabul ettiği güvenlik kriterlerini kullanarak test süreçlerini gerçekleştirmiştir. Bu süreçte Amerika'da da Savunma Bakanlığının hazırladığı TCSEC yani Trusted Computer Security Evaluation Criteria standardını, Avrupa ülkeleri ise TCSEC'i temel alarak ITSEC'i yani Information Technology Security Evaluation Criteria standardını kullanmaya başlamıştır. Bu iki standart ülkelerin ulusal ağlarında kullanacakları BT ürünleri için yeterli olmuş, ancak BT ürünlerinin ülkeler arasındaki ticareti artmaya başladıkça ortak bir kritere ihtiyaç duyulmuştur. Çünkü farklı ülkelerde ürününü satan bir üretici için hem ITSEC sertifikasyonu hem de TCSEC sertifikasyonu almak uzun süren masraflı bir süreç haline gelmiştir. Askeri projeler için geliştirilmiş TCSEC ve ITSEC standartları, özel sektörün ihtiyaçlarına cevap verememiştir. Bu sebeplerden dolayı ülkeler ortak bir standart geliştirmek için çalışmaya başlamışlardır.

ABD, Kanada, İngiltere, Almanya, Fransa, Avustralya ve Yeni Zelanda ülkelerinin çalışmaları sonucunda, 1996 yılında ilk sürümü yayınlanan Ortak Kriterler (Common Criteria) standardı geliştirilmiştir. Mayıs 1998'de yapılan değişikliklerin ardından standardın 2.0 versiyonu yayınlanmış ve aynı yılın Haziran ayında ISO Ortak Kriterler'i ISO 15408 numarasıyla uluslararası standart olarak kabul etmiştir. Bu sürüm uzun süre uluslararası alanda BT ürünlerinin güvenlik değerlendirmelerinde kullanılmıştır. Artan ihtiyaçların karşılanması için köklü değişiklikler içeren standardın 3.0 sürümü ve geliştiricilerden gelen talepler üzerine yapılan revizelerle standardın 3.1 sürümü 2009 yılında yayınlanmıştır. Gelişen teknoloji, güvenlik ve garanti algısı doğrultusunda standardın güncellenmesi için uluslararası bir komite sürekli olarak çalışmakta ve günümüzde 4.0 sürümü için çalışmalar tamamlanmak üzeredir.

Ortak Kriterler, halen geliştirilmekte olan güncel bir standarttır. Bu standardı tanıyan ülkelerin sayısı her geçen gün artmakta ve BT güvenliği alanında uluslararası geçerliliği olan bir standart olma yolunda hızla ilerlemektedir.

2. KULLANIM ALANI

2.1. ORTAK KRİTERLER STANDARDI

Ortak Kriterler'in iki temel kullanımı vardır. Bunlardan ilki, ulusal ve uluslararası sınırlarda yapılan değerlendirmeler arasında "karşılaştırılabilirlik" sağlamasıdır. Yani iki farklı ürünün fonksiyonlarının Ortak Kriterler'e uygun değerlendirmesinin sonuçları birbirleri ile kolayca karşılaştırılabilir olmasıdır. Bunun nedeni, değerlendirmeler sırasında ürünün karşıladığı özelliklerin Ortak Kriterler'de tanımlanmış geniş kapsamlı, kendi içinde tutarlı, belirli bağımlılıklara ve hiyerarşik bir yapıya sahip fonksiyonel gereksinimlerle (SFRs) gösterilmesidir. Bu gereksinimler Ortak Kriterler'in ikinci bölümünde yer almaktadır.

Ortak Kriterler'in diğer bir faydası da kullanıcıların ihtiyaç duydukları güvenlik gereksinimlerini ürünün yerine getirdiğinin garantisini sağlamasıdır. Bu garanti Ortak Kriterler'in üçüncü bölümünde tanımlanan kendi içinde tutarlı ve bağımlılıkları olan güvenlik garanti gereksinimlerinden (SARs) hangilerinin ürün tarafından karşılandığının ve hangilerinin karşılanmadığının incelenmesi sonucunda sağlanır. Ortak Kriterler'in teoride tüketiciler, ürün geliştiriciler, değerlendiriciler ve sponsorlar olmak üzere 4 temel kullanıcısı vardır. Fakat ürün geliştiriciler genelde sponsorluk işini de yaptıkları için üç tip kullanımdan bahsedebiliriz.

Tüketiciler; Ortak Kriterler'i istedikleri güvenlik özelliklerini sağlayan ürünler talep edebilmeleri için rehber olarak kullanırlar. Ayrıca sertifikalı ürün kütüphanesinden[1] faydalanıp isteklerini karşılayan ürün olup olmadığını kontrol edebilirler. Ürün geliştiriciler; ürünün tasarımından piyasaya çıkışına kadar olan süreci boyunca gerekli güvenlik özelliklerini sağlaması için Ortak Kriterler'i rehber olarak kullanabilirler. Değerlendiriciler; BT ürünlerini Ortak Kriterler standardına göre değerlendirirken temel kaynak olarak kullanırlar.

Sponsorların yapması gereken ürün değerlendirmesi esnasında geliştirici ile değerlendirici arasında ki iletişimi sağlamak ve değerlendirme sürecine maddi olarak sponsor olmaktır.

Ortak Kriterler standardı üç bölümden oluşmaktadır. Birinci bölüm, Giriş ve Genel Model, Ortak Kriterler'in genel kavramlarını güvenlik hedef ve gereksinimlerinin neler olduğunu tanımlayan bir kılavuzdur. Ayrıca Security Target(ST) ve Protection Profile(PP)'ın içeriği de bu bölümde yer alır. İkinci bölüm SFR'ları yani güvenlik fonksiyonel gereksinimlerini listeleyen bir referans kitabıdır. Üçüncü bölüm ise güvenlik garanti fonksiyonlarını listeler. Ayrıca bu bölümde garanti seviyeleri ve bu seviyelerin içermesi gereken garanti aileleri gösterilmektedir.

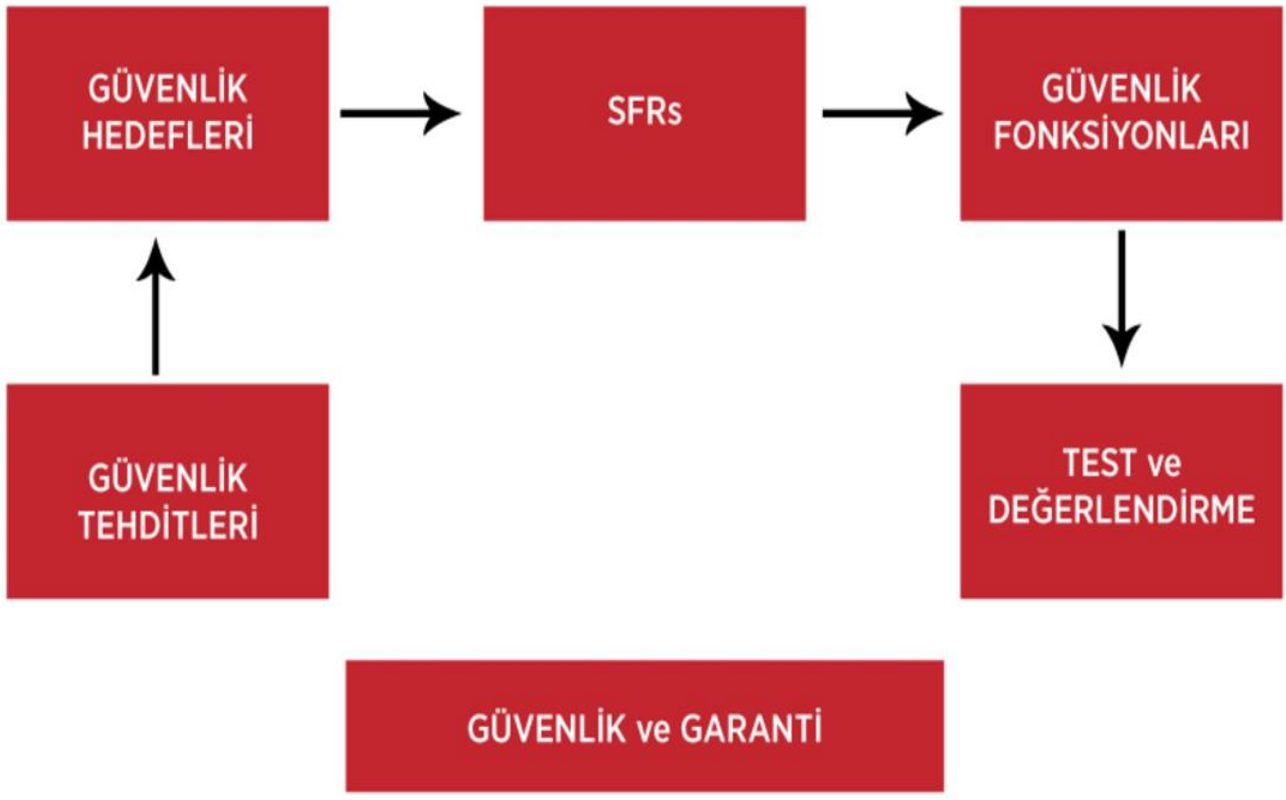
Ortak Kriterler Standardı'nda sıklıkla kullanılan ST, PP ve TOE'nin kavram ve kısaltmaların tanımları aşağıdaki gibidir.

TOE: (Target of Evaluation) Değerlendirme öğesi olan sistem veya ürüne verilen ismin kısaltmasıdır.

PP : (Protection Profile) Bir TOE sınıfı için üründen bağımsız olarak, istenen güvenlik gereksinimlerinin tanımlandığı dokümana verilen isimdir.

ST : (Security Target) Ürüne bağımlı olarak yazılan ve ürünün güvenlik özelliklerinin tanımlandığı dokümandır.

PP ve ST'ler Ortak Kriterler değerlendirmelerinin temel öğeleridir. PP'ler müşteriler tarafından yazılır ve ihtiyaç duyulan bir BT ürünü için gereksinimler belirtilir. ST'ler ise ürünü geliştiren firma tarafından, ürün, Ortak Kriterler değerlendirmesine girmeden önce hazırlanan ve ürünün hangi güvenlik özelliklerini ve hangi güvenlik seviyesini garanti ettiğinin belirtildiği dokümandır. İkisi de eşleştirme mantığı kullanılarak hazırlanır.



Şekil-1 Ortak Kriterler Güvenlik Yapısı

Bu dokümanlarda ilk olarak ürüne yönelik tehditler, politikalar ve kabullenmeler çıkartılır ve ortam tanımlandıktan sonra tehditleri ve politikaları karşılamak için güvenlik amaçları belirlenir. Bu güvenlik amaçlarını gerçekleştirmek için gerekli fonksiyonel gereksinimler Ortak Kriterler'in ikinci bölümü kullanılarak hazırlanır. Daha sonra fonksiyonel gereksinimleri ürünün hangi fonksiyonlarının nasıl yerine getirdiği dokümante edilir. Bu güvenlik fonksiyonlarının tehditleri karşılayıp karşılamadığı kontrol edilir ve eğer karşılıyorsa ürünün iddia ettiği güvenliği sağladığı sonucuna varılabilir.

Değerlendirici bir ST'yi veya PP'yi incelerken bütün bu eşleştirmelerin doğruluğunu kontrol eder. Ayrıca belirli bir ürünün, ST'si ile birlikte değerlendirilirken bütün fonksiyonlarının çalışıp çalışmadığı ve bütün tehditlerin karşılanıp karşılanmadığı kontrol edilir. Sonuç olarak ürün, değerlendirici testlerinden geçmişse iddia ettiği güvenliği sağladığına karar verilir. Bir sonraki aşama ürünün iddia ettiği garanti seviyesine uygunluğun incelenmesidir.

2.2. DEĞERLENDİRME METODOLOJİSİ

Ortak Kriterler standardına uygun olarak değerlendirme yapılabilmesi için, standardı hazırlayan ülkeler ayrıca değerlendirme metodolojisi hazırlamışlardır. CEM (Common Evaluation Methodology) adı verilen bu kılavuz PP, ST ve TOE değerlendirmelerinin nasıl yapılacağını adım adım anlatmaktadır. Değerlendirmeyi yapan laboratuvar bu metodolojiye uygun davranmak zorundadır. Aksi halde yaptığı değerlendirmelerin uluslararası geçerliliği bulunmamaktadır.

Ürünün ST'si değerlendirilip onaylandıktan sonra TOE değerlendirilmeye başlanır. Standarda göre yedi farklı değerlendirme seviyesi vardır. EAL1 ve EAL2 düşük garanti seviyeleridir. EAL3 ve EAL4 orta düzeyde garanti sağlayan ürünlere verilen seviyelerdir. EAL5 ve EAL6 yüksek derecede garanti veren seviyelerdir. EAL7 ise tam anlamıyla dört dörtlük garanti düzeyi sağlar. ST yazılırken üretici, iddia ettiği garanti düzeyini ve ürünün sağladığı garanti gereksinimlerini belirtir. Değerlendiricinin kontrol etmesi gereken; ürünün sağladığı güvenlik gereksinimlerinin iddia edilen garanti düzeyi için yeterli olup olmadığı ve bu gereksinimlerin doğruluğudur. Değerlendirici TOE'nin değerlendirilmesi sırasında birtakım dokümanları üreticiden talep eder. Bunlara değerlendirme delilleri adı verilir. Üretici bu dokümanları değerlendiriciye sağlamak zorundadır.

Metodolojiye uygun olarak değerlendirilen ürün, değerlendirme teknik raporu ile birlikte ürüne uluslararası Ortak Kriterler sertifikasını verecek olan sertifikasyon kurumuna gönderilir.

2.3. CCRA ve ORTAK KRİTERLER YAPISI

Standardı oluşturan ülkeler Common Criteria Recognition Arrangement adı verilen karşılıklı tanıma sözleşmesi imzalamışlardır. Bu sözleşmenin amacı bu ülkelerden herhangi birinde yapılan değerlendirmenin diğer ülkeler tarafından da tanınmasını sağlamaktır. Sözleşmeyi iki şekilde imzalamak mümkündür. Bunlardan ilki sözleşmeyi sertifika müşterisi olarak imzalamaktır. CCRA'i (Common Criteria Recognition Arrangement) sertifika müşterisi olarak imzalayan ülkenin uluslararası tanınabilecek sertifika üretme yetkisi yoktur.

Ülke, sadece bu yetkiye sahip diğer ülkelerin sertifikalarına müşteri olabilmektedir. Diğer bir imzalama seçeneği de sertifika üreticisi olarak imzalamaktır. Bu durumda ülke Ortak Kriterler değerlendirmeleri yapabilmekte ve ürettiği sertifikalar üye ülkelerce tanınmaktadır. CCRA sözleşmesini sertifika üreticisi olarak imzalayabilmek için ülkede kurulmuş ve çalışan bir Ortak Kriterler yapısını göstermek mecburiyeti vardır.

Ortak Kriterler yapısının temel taşı sertifikasyon kurumudur. Bu kurum değerlendirmeleri yapacak olan bağımsız laboratuvarlara değerlendirme lisanslarını verir ve bütün değerlendirmeler sırasında denetleme görevini yerine getirir. Ayrıca değerlendirme sonucunda değerlendirme teknik raporunu inceler ve başarılı ürünlere Ortak Kriterler sertifikalarını verir.

Sertifikasyon kurumu ülkenin güvencesiyle devlete bağlı bir kurumun altında çalışır. Kurumun ürettiği bütün sertifikalardan ülke sorumludur. Sertifikasyon kurumu ülkede Ortak Kriterler yapısını oluşturmaya başlar. Lisans verme prosedürleri de dahil olmak üzere Ortak Kriterler değerlendirmeleri için gerekli bütün prosedürleri tanımlar ve şeffaf olarak çalışır. Yapının diğer önemli bölümü de bağımsız test laboratuvarlarıdır.

Sertifikasyon kurumunun denetiminde çalışırlar ve çalıştıkları yapının bütün kurallarına uyma zorunlulukları vardır. Genel olarak Ortak Kriterler yapısı denildiğinde sertifikasyon kurumu, bağımsız laboratuvarlar ve bu kurumlar arasındaki ilişkiler anlaşılabilir.

Türkiye, CCRA sözleşmesini 2003 yılında Sertifika Müşterisi olarak imzalamış ve Kasım 2010 itibariyle statüsünü Sertifika Üreticisi ülke olarak güncellemiştir. Bu tarihten itibaren Türk Standartları Enstitüsü'nün Sertifika Makamı olarak faaliyet gösterdiği Ulusal Ortak Kriterler Yapısı altında sertifikalandırılan tüm ürünlerin Ortak Kriterler Belgeleri, uluslararası alanda geçerlidir.

3. TANIM

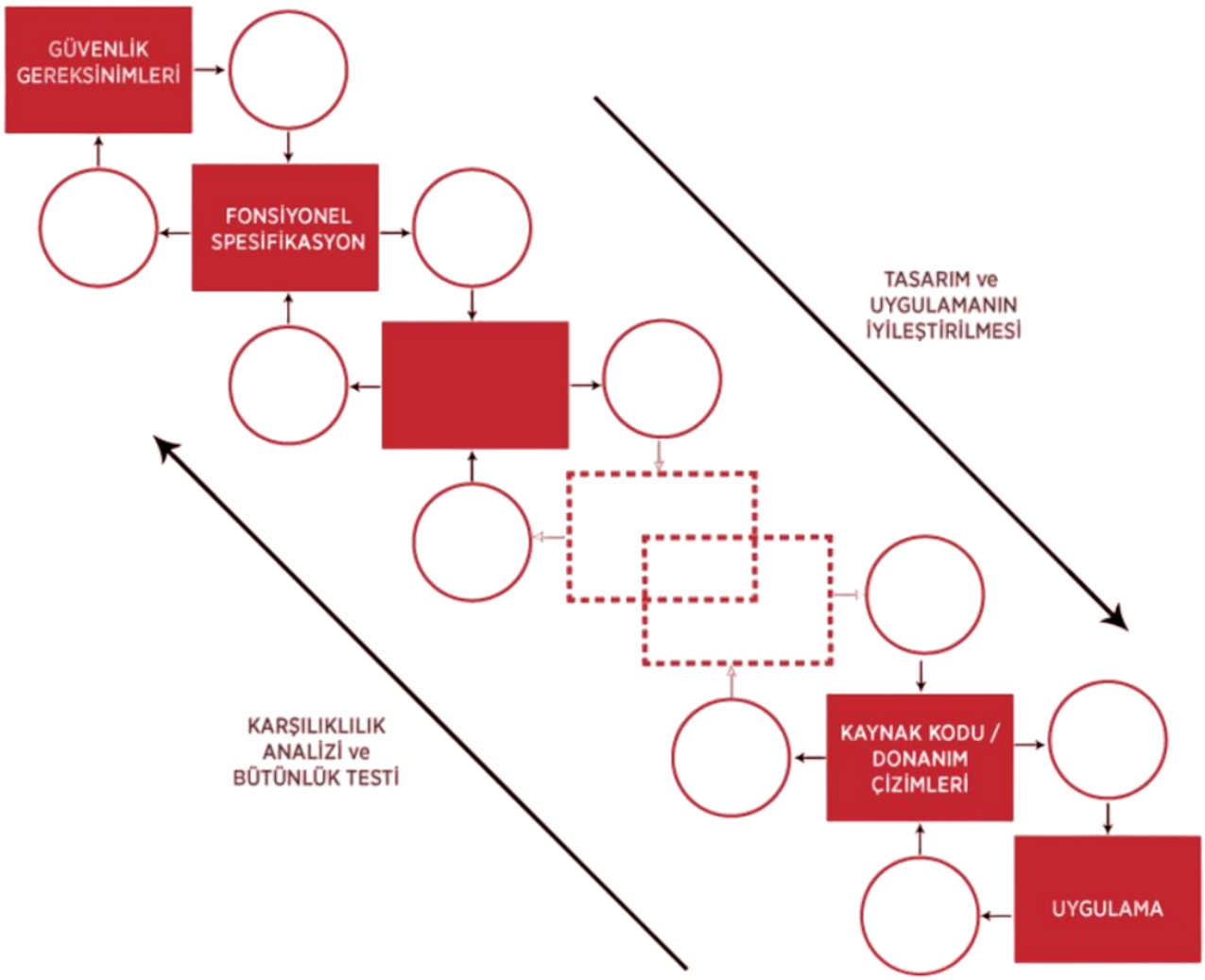
3.1. ORTAK KRİTERLER'E UYGUN ÜRÜN DEĞERLENDİRMESİ

Ortak Kriterler standardı güvenlik gereksinimleri göz önüne alınarak ürün geliştirilebilmesi için tasarım aşamasından itibaren uyulması gereken bir metodoloji önermektedir. Ürün değerlendirilmesinde ise bu aşamalar karşılık analizleri ve bütünlük testleri ile doğrulanmakta ve müşterilerin ürün konusunda ihtiyaç duyduğu güvenliğe ve garantiye sahip olması sağlanmaktadır.

Standardın önerdiği şekilde güvenlik gereksinimlerinin test edilecek ürün için tespit edilmesinden sonra her bir güvenlik gereksinimi için iç ve dış etkileşimleri de içerecek bir fonksiyonel spesifikasyon oluşturmakla tasarım aşamasına başlanmalıdır. Ardından bu fonksiyonel spesifikasyonda garanti seviyesine göre biçimsel veya biçimsel olmayan metotlarla tanımlanan güvenlik fonksiyonlarının üst düzey tasarımları hazırlanmalıdır. Bu tasarımın ardından her bir güvenlik fonksiyonunun detaylı bir şekilde tasarımının gösterileceği alt düzey tasarım dokümantasyonu oluşturulmalı ve bu alt düzey tasarıma uygun olarak kaynak kodu ve/veya donanım çizimleri oluşturulmalıdır. Son olarak da bu çizimler uygulanarak ürün geliştirilmelidir.

Ortak Kriterler'e uygun olarak ürün değerlendirmesi gerçekleştirilirken, laboratuvar, ürün geliştiriciden bu adımlara uygun olarak tasarımı ve uygulamayı gerçekleştirdiğine dair değerlendirme kanıtları talep etmektedir. Özellikle EAL4 ve üzerindeki garanti seviyelerinde bu adımların tamamına uygun olarak ürün geliştirilmesi gerekmektedir. Fakat EAL3 ve altındaki seviyelerde bu adımlara uygunluk kısmen daha az aranmaktadır.

Şekil 2'de Ortak Kriterler'e uygun olarak ürün geliştirilmesinde ve bu ürünlerin değerlendirme delillerinden olan geliştirme delillerinde gerekli olan adımlar gösterilmektedir



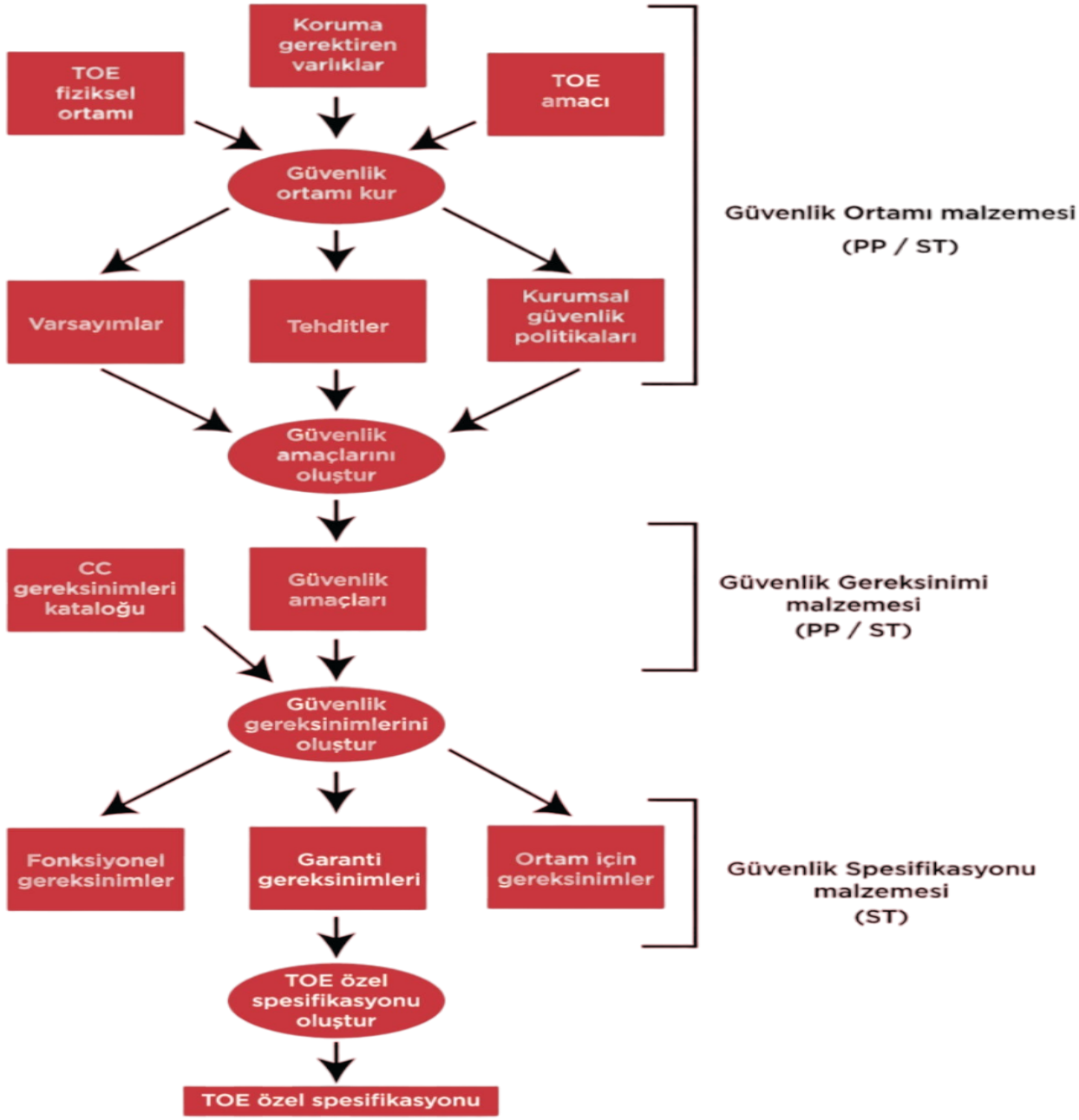
Şekil-2 Ortak Kriterler' e uygun ürün geliştirme adımları

3.2. GÜVENLİK HEDEFİ'NİN HAZIRLANMASI

Ortak Kriterler'e uygun olarak ürün değerlendirmelerinde gerçekleştirilen ilk adım ürünün Güvenlik Hedefi dokümanının değerlendirmesi olmaktadır çünkü Güvenlik Hedefi üreticinin geliştirdiği ürün için hazırlaması gereken, ürünün güvenlik ve garanti özelliklerini tanımladığı dokümandır.

Bu doküman oluşturulurken ilk olarak ürünün koruması gereken varlıklar, TOE'nin fiziksel ortamı ve TOE'nin amacı göz önüne alınarak güvenlik ortamı tanımlanmalıdır. Sonraki adımda ise bu güvenlik ortamına olabilecek tehditler, bu ortam ile ilgili kabullenmeler ve organizasyonel güvenlik politikaları ürün geliştiricisi tarafından belirlenmelidir.

Ortam ile ilgili tehditlerin, kabullenmelerin ve organizasyonel kurum politikalarının tespit edilmesinin ardından güvenlik amaçları ve bu amaçları karşılayabilmek için güvenlik fonksiyonel ve garanti gereksinimleri ile ortak gereksinimler çıkartılmalıdır. Son olarak bütün bu gereksinimlerin karşılanabilmesi için ürün spesifikasyonu çıkartılır ve bu adımlar arasındaki eşleştirmelerin gerekçeleri belirtilir. Şekil 3'de Güvenlik Hedefi dokümanının hazırlanış aşamaları adım adım gösterilmektedir.



Şekil-3 Güvenlik Hedefi Bölümleri

Bu yapının oluşturulmasındaki adımlar aşağıdaki gibidir;

1. Ürünün çalıştığı ortamın tanımlanması gerekmektedir. Bu tanımlamalarda cevap verilmesi gereken sorular bulunmaktadır. Bunlardan bazıları;

- Ürünün koruma sağlaması gereken varlıklara karşı ne gibi tehditler bulunmaktadır?
- Bu ortam hakkında ne gibi kabullenmeler yapılabilir?
- Ortamda geçerli olan politikalardan (kanunlar veya kurumsal politikalar) hangilerine ürünün uyması gerekmektedir.

2. Korunması gereken varlıkların karşılaşabileceği olası tehditlerin önlenmesi için spesifik amaçların belirlenmesi gerekmektedir. Amaçlar, belirlenmiş tehditlerin basit olarak olumsuz karşılıkları olmamalı bununla birlikte uygulanabilir ve istenilen sonuçları verebilir nitelikte olmalıdır. ST'nin kapsamı bu aşamada belirginleşmektedir.

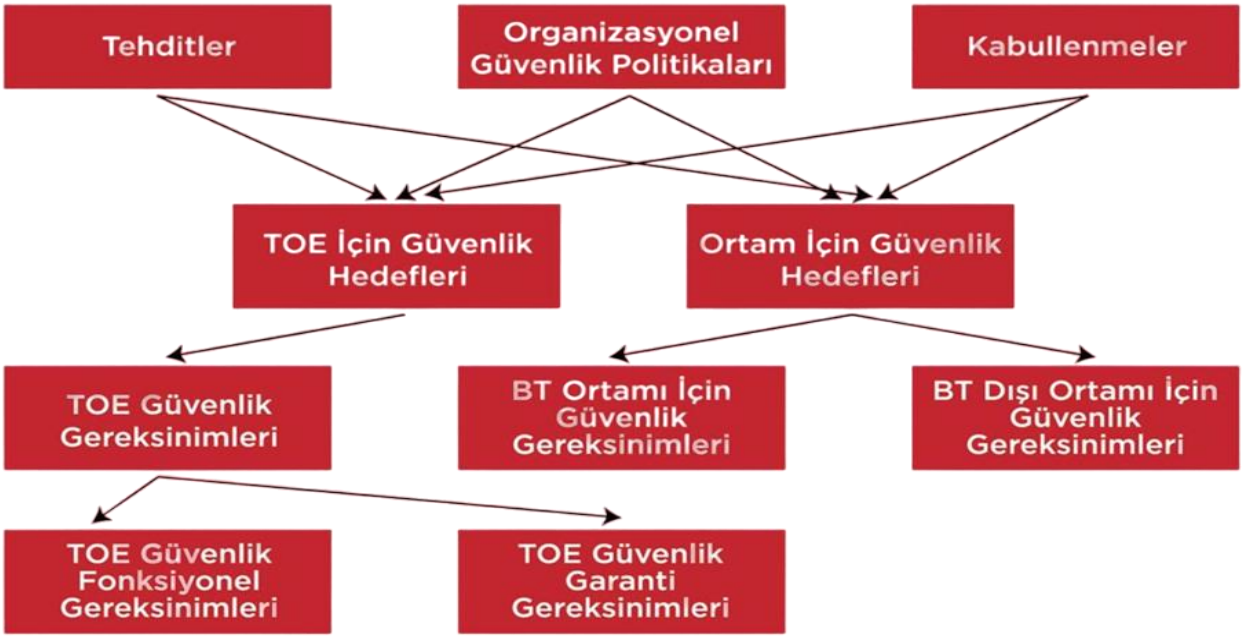
Amaçlar, TOE (değerlendirilen ürün) tarafından karşılanacak olanlar, BT ve BT dışı ortam tarafından karşılanacak olanlar ve bu ikisinin bileşimi sonucu karşılanacak olanlar olmak üzere üç kısma ayrılır.

3. Ürün ve ortamdaki diğer BT ürünlerinde, tespit edilmiş her bir güvenlik amacını karşılayacak fonksiyonelliği belirlemek için Ortak Kriter standardının ikinci bölümünde bulunan Güvenlik Fonksiyonel Gereksinimleri kısmı kullanılmalıdır. Standardın ikinci bölümündeki genel gereksinimlerin yetersiz kaldığı durumlarda standardın tanımladığı işlemler yapılmalıdır. Ayrıca ihtiyaç duyulan bir gereksinimin ikinci bölümde tanımlanmadığı durumlarda gereksinim formatına uygun olarak yeni bir bileşen tanımlanabilmektedir.

4. Amaçların karşılanacağına dair gerekli garantinin sağlanması için Ortak Kriterler standardının üçüncü bölümündeki Güvenlik Garanti Gereksinimleri kullanılır. İhtiyaç duyulan gereksinimler Ortak Kriterler standardının üçüncü bölümündeki Garanti Gereksinimleri kısmından seçilmeli ve bir garanti paketi oluşturulmalıdır veya daha önceden belirlenmiş bir paketi (EAL paketleri) kullanılabilir, veya bu iki yaklaşımın bir birleşimi ST'de uygulanabilir.

5. Tespit edilen Güvenlik Fonksiyonel Gereksinimlerin üründe hangi güvenlik fonksiyonları ile uygulandığı ve Güvenlik Garanti Gereksinimleri için hangi garanti tedbirlerinin alındığı da belirtilmelidir.

6. Son bölümde ise seçilen fonksiyonel ve garanti gereksinimleri bileşenlerinin ürünün kullanılacağı ortamdaki tehditleri nasıl karşıladığına dair ve güvenlik fonksiyonları ile garanti tedbirlerinin bu gereksinimleri nasıl karşıladığına dair gerekçeler belirtilmelidir. Aşağıda gösterilen şekil söz konusu aşamalarda yapılması gereken eşleştirmeleri tam olarak belirtmektedir.



Şekil-4 Güvenlik Hedefi Eşleştirmeler

4. UYGULAMA

4.1. GÜVENLİK HEDEFİ DEĞERLENDİRMESİ

Bir ürünün Güvenlik Hedefinin değerlendirilmesi sırasında yukarıda belirtilen altı maddenin Güvenlik Hedefi'nde bütün, anlaşılabilir ve tutarlı bir şekilde uygulandığı öncelikli olarak kontrol edilir. Bu kontrollerden sonra ürünün Güvenlik Hedefi, Ortak Kriterler Değerlendirme Metodolojisinde belirtilen değerlendirme eylemlerine tabi tutularak değerlendirilir. Güvenlik Hedefinin başarılı sayılabilmesi ve ürünün bu Güvenlik Hedefine uygun olarak değerlendirilebilmesi için bu bölümdeki bütün eylemlerden "Geçti" sonucu alması gerekmektedir.

4.2. ÜRÜN DEĞERLENDİRMESİ

Ortak Kriterler standardına uygun ürün değerlendirmesi ürün geliştirici tarafından hazırlanmış olan Güvenlik Hedefi içerisinde bulunan Garanti Seviyesi iddiasına uygun olarak gerçekleştirilir. Şekil 5'de bulunan tablo EAL seviyelerinin içermesi gereken garanti sınıflarını göstermektedir. Ürün geliştirici bu tabloya uygun olarak iddia ettiği garanti seviyesinin gerektirdiği garanti bileşenlerini güvenlik hedefi içeriğinde iddia eder ve ürün değerlendirmesi kapsamında bu garanti ailelerinin gereksinimlerinin sağlanıp sağlanmadığı kontrol edilir.

Örneğin; EAL 4 seviyesinde ürün geliştiren bir firma Ortak Kriterler sertifikasyonu için Geliştirme Sınıfı içerisinde ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3 bileşenlerine uygunluğu iddia etmek ve kanıtlamak durumundadır.

Söz konusu bileşenlere uygunluk değerlendirme kanıtları aracılığı ile gerçekleştirilir. Bu bölümde temel garanti sınıfları içerisinde bulunan bileşenler ve bu bileşenlere uygunluk için hazırlanması gereken değerlendirme delilleri tanımlanacaktır.

Garanti Sınıfı	Garanti Ailesi	Garanti Seviyeleri						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Geliştirme	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Kılavuz Dokümanlar	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Yaşam Döngüsü Desteği	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Güvenlik Hedefi Değerlendirmesi	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Testler	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Açıklık Değerlendirmesi	AVA_VAN	1	2	2	3	4	5	5

Şekil-5 Garanti Seviyeleri

4.2.1. GELİŞTİRME

Bu Garanti Sınıfı değerlendirmeye giren ürünün güvenlik fonksiyonlarının geliştirme aşamasında belirli niteliklere uygun olarak tasarlanmasını ve uygulanmasını kapsamaktadır. Bu sınıf içerisinde farklı seviyelerde sunulacak değerlendirme delillerinin içeriği ve kapsamı genişlemekle birlikte aşağıdaki değerlendirme delilleri laboratuvar tarafından talep edilir ve Ortak Kriterler Değerlendirme Metodolojisi'ne uygun olarak değerlendirilir;

- **Güvenlik Mimarisi Dokümanı:** EAL2 ve üzeri seviyelerde talep edilen bu doküman ile ürün geliştirici güvenlik mimarisini ve teste girecek olan ürünün güvenlik fonksiyonlarının by-pass edilemeyeceğini, ürünün kendini koruma mekanizmalarını ve alan ayrıştırma niteliklerini tanımlamalıdır.

- **Fonksiyonel Spesifikasyon:** Her seviyede talep edilen bu doküman ile ürün geliştirici Güvenlik Hedefi'nde iddia ettiği güvenlik fonksiyonlarını, bu fonksiyonların iç ve dış arayüzleri doğrultusunda spesifikasyonlarını tanımlamalıdır. Söz konusu spesifikasyon, arayüzlerin tanımlamalarını, kullandıkları metotları, parametre ve parametre tanımlarını, arayüz üzerinden gerçekleştirilen tüm aksiyonları ve hata mesajlarını içermelidir.

- **Uygulama Temsili:** EAL4 ve üzeri seviyelerde talep edilen uygulama, temsili tasarımı yapılmış olan yazılım ve/veya donanımın uygulama detaylarını (kaynak kod, uygulama bileşenler) içermelidir.

- **Güvenlik Politikası Modeli:** EAL6 ve EAL7 seviyesinde talep edilen bu değerlendirme delili, formal bir güvenlik politikası modelinin tasarlanmasını ve güvenlik fonksiyonları üzerinde uygulanmasını tanımlamalıdır.

- **TSF Internals:** EAL5 ve üzeri seviyelerde talep edilen bu değerlendirme delili, test edilen ürünün güvenlik fonksiyonlarının ayrıntılı tasarım ve bileşenlerinin tanımlarını içermelidir.

4.2.2. KILAVUZ DOKÜMANLAR

Bu Garanti Sınıfı'nda değerlendirilecek ürüne ait kılavuz dokümanlar değerlendirme delili olarak laboratuvara teslim edilecektir. Her seviye için standart olarak talep edilen bu kılavuz dokümanlar iki farklı bölüm içermelidir;

- **Kullanıcı Kılavuzu:** Bu doküman farklı rollerdeki tüm kullanıcıların ürünü güvenli durumda tutmaları ve kullanabilmeleri için gerekli tüm içeriği barındırmalıdır. Söz konusu kılavuzun içeriği Ortak Kriterler Değerlendirme Metodolojisi'nde detaylı olarak aktarılmaktadır.

- **Kurulum Prosedürleri:** Kurulum prosedürleri test edilen ürünün kurulum ve konfigürasyon aşamalarını detaylı olarak tanımlamalı ve son kullanıcıların kullanımına hazır hale getirmek için gerekli tüm adımları içermelidir.

4.2.3. YAŞAM DÖNGÜSÜ DESTEĞİ

Bu Garanti Sınıfı'nda değerlendirilecek ürünün tüm geliştirme aşamalarında uygulanan ürün geliştirme süreçleri ve yaşam döngüsü adımlarına dair gereksinimleri bulunmaktadır. Bu sınıf içerisinde farklı seviyelerde sunulacak değerlendirme delilinin içeriği ve kapsamı genişlemekle birlikte aşağıdaki değerlendirme delilleri laboratuvar tarafından talep edilir ve Ortak Kriterler Değerlendirme Metodolojisi'ne uygun olarak değerlendirilir;

- **Konfigürasyon Yönetim Planı:** Bu değerlendirme delili ürünün yaşam döngüsü kapsamında uygulanacak konfigürasyon yönetimi adımlarını içermektedir. Farklı seviyelerde gereksinimleri değişen söz konusu plan, EAL4 ve üzeri seviyelerde konfigürasyon yönetiminin otomasyon araçları ile yapılmasını zorunlu kılmaktadır.

- **Konfigürasyon Yönetim Kapsamı:** Bu değerlendirme delili, hazırlanmış olan konfigürasyon yönetim planına tabi tutulacak olan konfigürasyon öğelerinin listelerini içermektedir.

- **Teslim Prosedürleri:** Bu değerlendirme delili, teste tabi tutulan ürünün son kullanıcıya güvenli bir şekilde ulaştırılması için tanımlanan prosedürleri içermelidir.

- **Geliştirme Ortamı Güvenliği:** Bu değerlendirme delili, ürün geliştirme yaşam döngüsü içerisinde tanımlı tüm aşamalarda güvenliğin fiziksel olarak sağlanması için gerekli politika ve prosedürleri tanımlamalıdır.

- **Yaşam Döngüsü Tanımları:** Bu değerlendirme delili, teste tabi tutulan ürünün yaşam döngüsünün tüm aşamalarını (gereksinim analizi, tasarım, uygulama geliştirme, test, bakım vs.) ayrıntılı olarak tanımlamalı ve bu aşamaların birbiri ile ilişkileri ile süreç sahiplerini ayrıntılı olarak tanımlamalıdır.

- **Araç ve Teknikler:** Bu değerlendirme delili, yaşam döngüsü kapsamında kullanılan tüm araç ve yöntemleri tanımlamalıdır.

- **Zafiyet ve Hata Giderme Prosedürleri:** Bu değerlendirme delili zorunlu olarak hiç bir seviyede bulunmamakla birlikte özellikle sahada aktif olarak kullanılan üründe tespit edilen zafiyet ve hataların zamanında ve doğru olarak giderilmesi için gerekli kurumsal politikaları tanımlamalıdır.

4.2.4. GÜVENLİK HEDEFİ DEĞERLENDİRMESİ

Bu Garanti Sınıfı için değerlendirme adımları Bölüm 4.1'de tanımlanmıştır.

4.2.5. TESTLER

Bu Garanti Sınıfı, Güvenlik Hedefi'nde iddia edilen Güvenlik Fonksiyonlarının, ürün geliştirici tarafından yeterli kapsamda ve derinlikte test edilmesi için gereksinimleri tanımlamakta ve bu eylemlerin laboratuvar tarafından doğrulanması için gerekli değerlendirme delillerini belirlemektedir.

Bu kapsamda ürün geliştirici tüm güvenlik fonksiyonlarını belirli bir Test Planı doğrultusunda test etmeli ve sonuçlarını Fonksiyonel Test Dokümanı'nda raporlamalıdır. Ayrıca gerçekleştirilen testlerin kapsamının ve derinliğinin yeterli olduğuna dair analizi laboratuvara sunmalıdır.

4.2.6. AÇIKLIK DEĞERLENDİRMESİ

Bu Garanti Sınıfı, teste tabi tutulan ürünün operasyonel ortamda bulunan saldırgan potansiyeli doğrultusunda zafiyet analizine tabi tutulması için gereksinimleri tanımlamaktadır. Bu sınıf laboratuvar tarafından gerçekleştirilir ve ürün geliştirici sadece teste tabi tutulan yeterli sayıda ürünü laboratuvara teslim eder.

5. ZORLUKLARI

Ortak Kriterler standardını uygulamak ve bu standarda uygun sertifikasyon sürecini başarı ile tamamlamak özellikle ilk ürün için oldukça zaman alan ve maliyetli bir süreçtir. Ürünü geliştiren kurumda özellikle yerleşik bir Ürün Geliştirme Süreci 5 bulunmuyorsa, değerlendirme delillerini hazırlamak ürün geliştirici için çoğu zaman danışmanlık gerektiren bir süreçtir. Ancak özellikle ilk ürün belgelendirme sürecinde elde edilen bilgi birikimi ve uygulanan yaşam döngüsü prosedürleri, sonraki ürünlerin Ortak Kriterler standardına uygun olarak geliştirilmesini oldukça kolaylaştırmaktadır.

Ortak Kriterler belgelendirmesi birçok test ve değerlendirme faaliyeti kapsamaktadır. Özellikle süreç içerisinde gerçekleştirilen değerlendirme faaliyetleri değerlendiricinin tecrübesi ve sertifika makamının yönlendirmesi ile doğrudan ilişkilidir. Bu nedenle sertifikasyon sürecinin zorluğu laboratuvardan laboratuvara ve hatta ülkeden ülkeye değişmektedir.

Ortak Kriterler standardının temel prensibi, ürün geliştiricinin iddialarının bağımsız bir laboratuvar tarafından doğrulanması ve ulusal bir otorite tarafından belgelendirilebilmesi için bir altyapının oluşturulmasıdır. Bu süreçte özellikle ürün müşterilerinin ve kullanıcılarının doğru ürünü seçmek için belgelendirilmiş olan ürünleri Güvenlik Hedefi dokümanlarını detaylı olarak incelemesi ve kendi operasyonel ortamlarında belgenin geçerli olup olmadığını doğrulaması son derece önemlidir.

Belgelendirilmiş bir ürünün Güvenlik Hedefi kapsamında yapmış olduğu bir varsayım, müşteri sahasında uygulanması mümkün olmayan bir varsayım olabilir. Bu durumda ürünün belgesinin o ortam için geçerliliğinden söz edilemez. Bu kapsamda ürün geliştiricilerin bilinçlendirilmesi son derece önemlidir.

BT ürünlerinin özellikle güvenlik gereksinimleri dikkate alınarak ve test odaklı olarak geliştirilmesi ve belirli bir kalite düzeyinde üretilebilmesi için Ortak Kriterler oldukça kullanışlı bir standarttır. Ancak bu standardın uygulama maliyetlerinin yüksek oluşu nedeni ile özellikle yerel üreticilerin bu standarda uygun ürün geliştirme konusunda teşvik edilmesi ve bu sayede uluslararası rekabet gücünün arttırılması gerekmektedir.

Bu kapsamda Türkiye'de üretilen BT ürünlerinin uluslararası pazarlara girmesi için Ekonomi Bakanlığı da Ortak Kriterler sertifikasyonunu % 50 oranında desteklenen sertifikalar kapsamında değerlendirmektedir. Ulusal pazarda Ortak Kriterler Değerlendirmesi kamu kurumlarınca tanınmakta olup hizmet alımlarında bir ön koşul olarak sunulmaktadır.

6. İLGİLİ STANDART ve MODELLER

Ortak Kriterler sertifikasyonu diğer kalite, süreç ve standartlardan farklı olarak, BT ürünlerinin güvenlik yönünden belgelendirilmesi amacı ile belirli bir seviyede kalite süreci işletilerek geliştirilmiş ve uluslararası alanda kullanılan bir standarttır. Ortak Kriterler'in ürün güvenliğine yönelik gereksinimleri ISO/IEC 27001 standardında ağ bileşenlerinin doğrulanması konu başlığı ile paralellik göstermektedir. Bilgi güvenliği yönetim sistemi kurulan ve işletilen şirketlerde ürünlerin altyapıya kurulumu ve entegrasyonu sırasında Ortak Kriterler benzeri doğrulama yöntemlerinin kullanılması önerilmektedir.

Örneğin; CMMI, SPICE gibi ürün geliştirme süreçlerinin olgunlaştırılmasına yönelik modellerin uygulandığı BT ürün çıktıları, Ortak Kriterler sertifikasyon sürecinin daha hızlı tamamlamasında son derece etkindir.

Ortak Kriterler, satın alınan BT çözümünün operasyonel ortamda bulunan tehditlere karşı yeterli dirençte güvenlik fonksiyonları geliştirildiğinin, üçüncü taraf bağımsız bir laboratuvar tarafından doğrulanması ve zafiyet analizinin gerçekleştirilmesini içerir. Bu kapsamda söz konusu belgelendirilmiş ürünlerin sistemde oluşturabileceği zafiyet veya risklerin ürün geliştirici tarafından değerlendirilmiş ve karşılanmış olduğunun güvencesi Ortak Kriterler sertifikasyonu ile garanti edilmiş olur. Bu doğrultuda özellikle kritik altyapılarda sertifikalı ürün tercih etmek diğer ilgili standart ve modellerin de tam olarak işletilebilmesi açısından önem kazanmaktadır.

Mehmet Akif Ersoy Mah. 286. Sok.
Profis A Blok 6/10 Yenimahelle/Ankara
Phone: +90 (505)9760930
info@bigdata.tr www.bigdata.tr