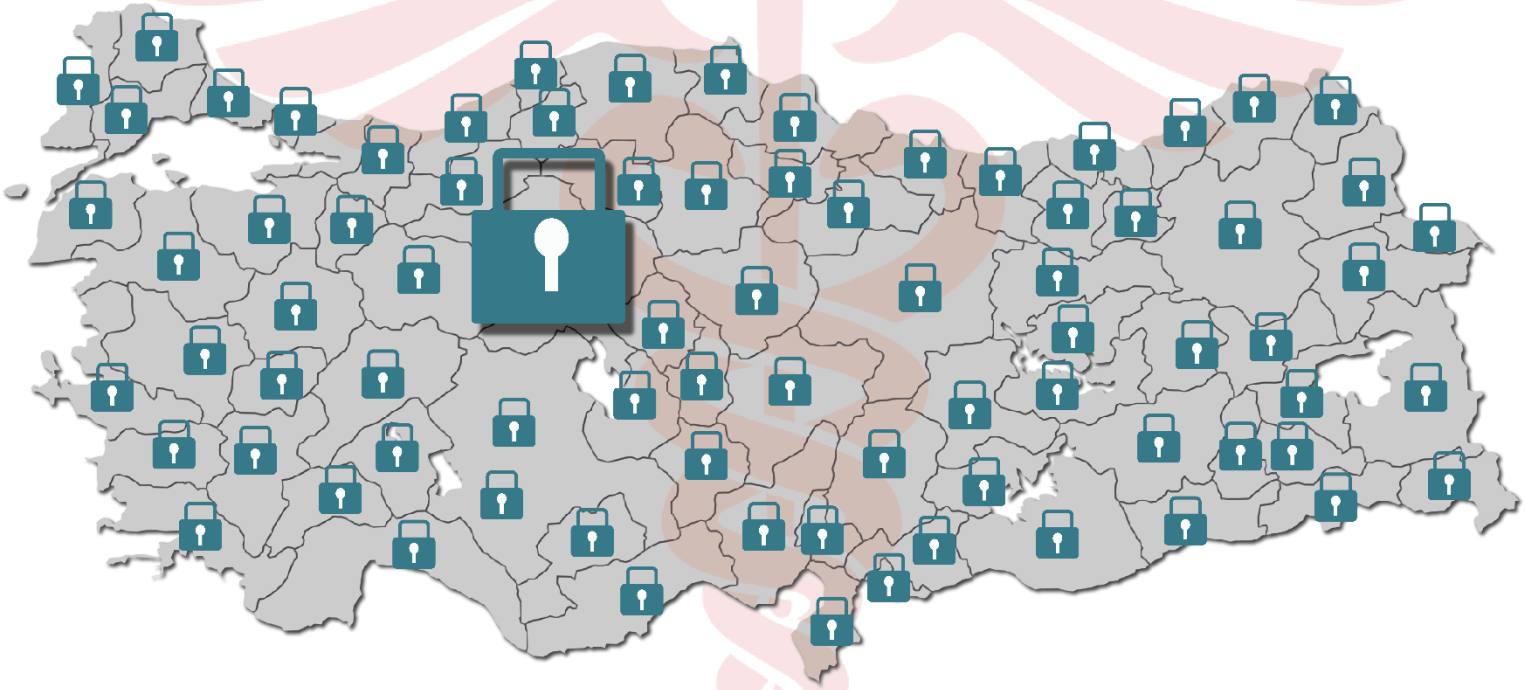
Kurumsal SOME
Kurulum ve Yönetim Rehberi
V.1



2019

T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Kurumsal SOME Kurulum ve Yönetim Rehberi V.1

MAYIS 2019

EDİTÖRLER

DR. M. MAHİR ÜLGÜ

M. FATİH ULUÇAM

MEHMET CAVLAMAZ

AYŞE GÜL ÇETİN

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

EKLER LİSTESİ

TABLOLAR LİSTESİ

1. GİRİŞ

Bilgi ve iletişim teknolojileri alanındaki gelişmelerle beraber siber ortam tehditlerinin sayısında büyük artış olmuştur. Siber tehditler kurum ve kuruluşlar açısından da büyük tehdit oluşturmaya başladığı için ulusal kapsamda bu alanda çalışmalar başlatılmıştır.

"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" 20 Ekim 2012 tarihli Resmi Gazetede Bakanlar Kurulu Kararı olarak yayımlanmış ve siber güvenliğe ilişkin program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla "Siber Güvenlik Kurulu" oluşturulmuştur.

Siber Güvenlik Kurulu, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nı kabul etmiş ve 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır. Söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME'ler, Sektörel SOME'ler) oluşturulmasına karar verilmiştir. Bu kapsamda, 11 Kasım 2013 tarihli ve 28818 sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" Resmi Gazetede yayımlanmıştır.

Bakanlığımız bünyesinde de, Sektörel SOME'ler ve Kurumsal SOME'lerin kurulması gerekli koordinasyonun sağlanması ve denetim mekanizmasının oluşturulması görevi 31.01.2016 Tarihli ve 67523305-719-E.509 Sayılı SOME Kurulması Konulu Bakanlık Makamı Onayı ile Bakanlığımız adına Sağlık Bilgi Sistemleri Genel Müdürlüğü'ne verilmiştir.

Bu rehber 02.05.2018 tarihli ve 98813779.719.54Bilgi Güvenliği Politikaları Yönergesinin eki olarak hazırlanmıştır.

Sağlık Bakanlığı'nın ve bağlı kuruluşlarının merkez ve taşra teşkilatları ile Sağlık Bakanlığı'na doğrudan hizmet veren özel sektör kuruluşları bünyesinde kurulacak olan Kurumsal SOME'ler bu rehberde yer alan esaslar çerçevesinde kurulacaktır. Rehber, Kurumsal SOME personelinin nitelikleri ve alması gereken eğitimleri, siber olay öncesi ve sonrasındaki çalışmaları, Kurumsal SOME'lerin kuruluş esaslarını içermektedir.

Rehber hazırlanırken Ulaştırma ve Altyapı Bakanlığının yayımlamış olduğu Kurumsal SOME Kurulum ve Yönetim Rehberindeki temel gereksinimler baz alınmıştır.

Kurumsal SOME yapısının etkin bir şekilde oluşturulmasında ve çalışmalarında ilgili kurum ve kuruluşun yöneticileri tarafından desteklenmesi büyük önem taşımaktadır.

1.1 Amaç

Rehber, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi kapsamında Sağlık Bakanlığının ve bağlı kuruluşlarının merkez ve taşra teşkilatı ile Sağlık Bakanlığına doğrudan hizmet veren özel sektör kuruluşlarının yararlanması için hazırlanmıştır.

1.2 Kapsam

Kurumsal SOME'ler, öncelikli olarak Sağlık Bakanlığının ve bağlı kuruluşlarının merkez ve taşra teşkilatı, ilerleyen süreçte Sağlık Bakanlığına doğrudan hizmet veren özel sektör kuruluşlarında kurulacaktır.

1.3 Tanımlar ve Kısaltmalar

- Bakanlık: Sağlık Bakanlığını,
- Bilgi Güvenliği Yönetim Komisyonu: Bakanlık genelinde bilgi güvenliği ve siber olay yönetimi ile ilgili konularda en üst düzeyde koordinasyon ve karar organı olarak görev yapan komisyonu,
- Bilgi Güvenliği Alt Komisyonu: Bakanlık merkez teşkilatı, bağlı kuruluşlar ve İl Sağlık Müdürlükleri bünyesinde bilgi güvenliği ve siber olaylara müdahale faaliyetlerini yürüten ve koordine eden komisyonu,
- Genel Müdürlük: Sağlık Bilgi Sistemleri Genel Müdürlüğünü,
- SBSGM: Sağlık Bilgi Sistemleri Genel Müdürlüğünü,
- BGYS: Bilgi Güvenliği Yönetim Sistemlerini,
- Sektörel SOME'ler: Sağlık sektöründe bulunan kritik altyapıları ve bilgi sistemlerini siber olaylardan korumak için önleyici ve düzenleyici çalışmalar yapan Sektörel Siber Olaylara Müdahale Ekibini,
- Kurumsal SOME: Kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibini,
- İz kaydı: Bilişim sistemlerinin işletilmesi esnasında ürettiği kayıtları,
- Siber Olay: Bilgi sistemleri ve endüstriyel kontrol sistemleri (ağa bağlanabilen diğer cihazlar, tıbbi cihazlar vb.) veya bu sistemlerde tutulan veya işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,
- Siber Ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,
- USOM: Temel görevleri, "Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esaslar "da yer alan Ulusal Siber Olaylara Müdahale Merkezini,
- ISO: Uluslararası Standartlar Organizasyonunu
  ifade eder.

1.4 Dayanak

Bu rehber, 11 Kasım 2013 tarihli ve 28818 sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi' ne dayanılarak hazırlanmıştır.

1.5 Güncelleme

Değişen şartlar dikkate alınarak bu rehber, Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından güncellenecektir.

1.6 Gizlilik

Kurumsal SOME birimlerinde görev yapan personel, görevleri sırasında edindikleri bilgileri, görev esnasında ve sonrasında saklamak zorundadır.

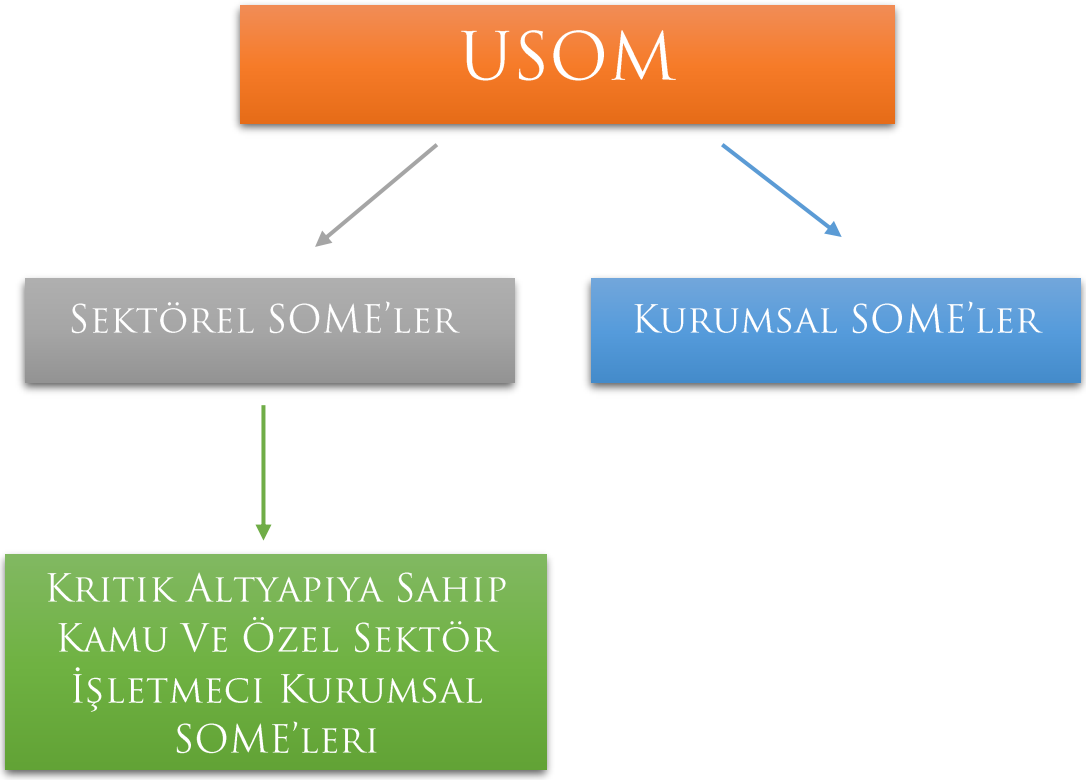
2. ULUSAL SİBER OLAYLARA MÜDAHALE ORGANİZASYONU

Siber olaylara müdahale organizasyonundaki temel unsurlar, USOM, Sektörel SOME ve Kurumsal SOME'lerdir.

Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur.

7/24 esasına göre çalışmak üzere 2013 yılında Bilgi Teknolojileri ve İletişim Kurumu bünyesinde kurulmuş ve faaliyete geçmiştir.

- TR-CERT (Computer Emergency Readiness Teams) – USOM
- CERT (Cyber Emergency Response Team) – SOME



Şekil 1. Ulusal Siber Olaylara Müdahale Organizasyonu

USOM, Sektörel SOME'ler ve Kurumsal SOME'ler Tablo 1'deki hizmet alanlarında siber güvenlik yönetimini gerçekleştirirler.

Organizasyon	Kurum / Kuruluş	Hizmet Alanı
USOM	Bilgi Teknolojileri ve İletişim Kurumu	Ulusal siber ortam
Sektörel SOME	Sağlık Bakanlığının merkez teşkilatı	Sağlık Bakanlığının ve bağlı kuruluşlarının merkez ve taşra teşkilatı ile kritik altyapı işleten özel sektör kuruluşların siber ortamları
Kurumsal SOME	Sağlık Bakanlığının ve bağlı kuruluşlarının merkez ve taşra teşkilatı ile kritik altyapı işleten özel sektör kuruluşları	Kurum ve Kuruluşların siber ortamları

Tablo 1. Hizmet Alanları

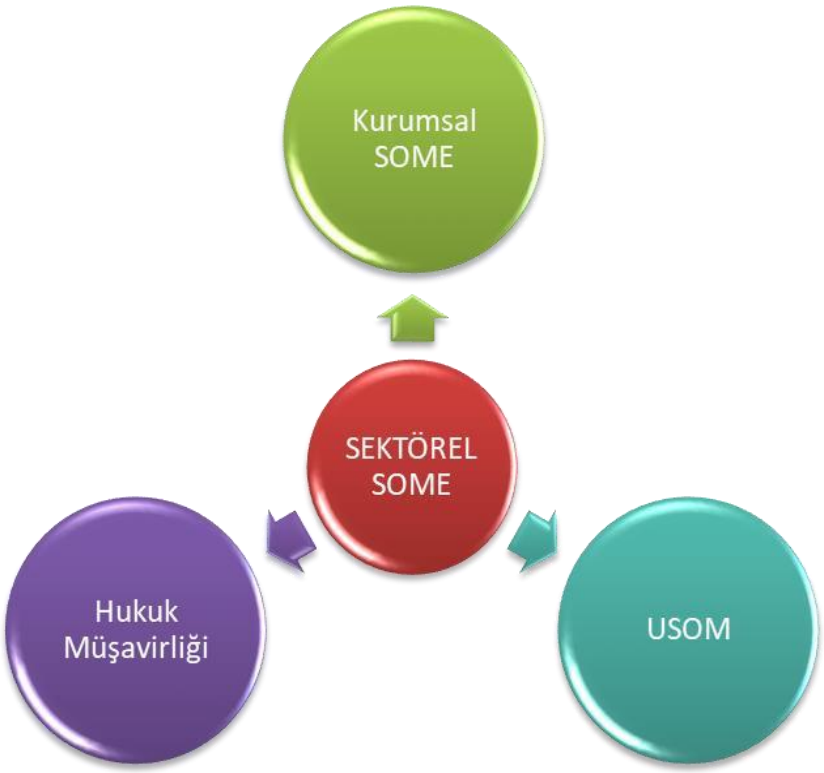
3. SEKTÖREL SOME

Sektörel SOME'ler, sorumluluk alanı kapsamındaki kurum ve kuruluşlarda siber güvenliğin sağlanmasından, koordinasyonundan, düzenlenmesinden ve denetlenmesinden sorumlu olan yapıdır.

Sektörel SOME'ler; USOM, Kurumsal SOME'ler ve hukuk müşavirliği ile koordineli olarak çalışır. Kurumsal SOME'lerin birbirleri ile ve USOM ile olan iletişim faaliyetlerini düzenler, Bakanlık dâhilinde kullanılacak iletişim yöntemleri ile ilgili usul ve esasları belirler.

Siber Güvenlik Kurulunun aldığı stratejik kararlar ve eylem planlarının uygulanması ve koordine edilmesi görevleri de Sektörel SOME'ler tarafından yerine getirilir.

Bakanlık genelinde siber güvenlik ve sosyal mühendislik tatbikatları düzenler, çalışma alanındaki konularda gerekli mevzuatları hazırlar.



Şekil 2. Sektörel SOME

3.1 Sektörel SOME'nin Bakanlık Teşkilatındaki Yeri ve Yapısı

Sektörel SOME'ler, Bilgi Güvenliği Yönetim Komisyonuna bağlı olarak çalışır.

Sektörel SOME'ler, sağlık sektörü ile ilgili yeterli tecrübeye sahip ve bilgi güvenliği/siber güvenlik konusunda eğitimli personelden oluşur.

3.2 Sektörel SOME'nin Kurum İçi ve Kurum Dışı Paydaşlarla İletişim Esasları

Sektörel SOME'ler, yıllık olarak hazırlanan "Sektörel Siber Güvenlik Faaliyet Raporu"nu Bilgi Güvenliği Yönetim Komisyonuna sunar.

Sektörel SOME'ler, Kurumsal SOME'lerden gelen "Siber Olay Müdahale Raporu"nu ve 7x24 ulaşılabilir durumda olan personelin iletişim bilgilerini USOM'a iletir.

3.3 Sektörel SOME'nin Görev ve Sorumlulukları

- Sektörel çalışma grubuyla beraber sektör içi asgari siber güvenlik kriterlerini belirler.
- Kurumsal SOME'lerden yapmasını talep ettiği risk analizlerinin metodunu, kapsamını, hazırlama periyodunu ve rapor formatını belirler.
- USOM tarafından yayımlanan duyuru ve bildirilerin Kurumsal SOME'lere aktarılmasını sağlar.
- Sorumluluk alanındaki kurum ve kuruluşlara siber güvenlik pratikleri hakkında bilgi sağlama hizmeti verir.
- Sektörel siber olay müdahale prosedürünü oluşturur ve tatbikatlarda test eder.
- Sektördeki Kurumsal SOME'lerin Ulusal Siber Güvenlik Tatbikatı başta olmak üzere test ve tatbikatlara katılmalarını teşvik eder.
- Siber olay esnasında Kurumsal SOME'lere imkânları ölçüsünde gerekli desteği sağlar.
- Siber olaydan elde edilen, olayın önlenmesine yönelik bilgi ve tecrübeleri Kurumsal SOME'ler ile paylaşır.
- Sorumluluk alanını oluşturan sağlık sektörünü kapsayacak şekilde siber saldırı uyarısı ve güvenlik açığı duyurusu yayımlar.
- Diğer kritik sektörlerdeki, Sektörel SOME'ler ile işbirliği ve koordinasyonu sağlar.

3.4 Sektörel SOME'nin Alması Gereken Eğitimler

Eğitimler	
Kayıt Yönetimi	- Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi
Siber Olay Yönetimi	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim Hukuku Eğitimi
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi

Tablo 2. Sektörel SOME'nin Alması Gereken Eğitimler

4. KURUMSAL SOME VE KURULUM AŞAMALARI

4.1 Prensipler

Kurumsal SOME'lerin kurulması, işletilmesi ve yönetilmesi aşamalarında uygulanacak kurallardır.

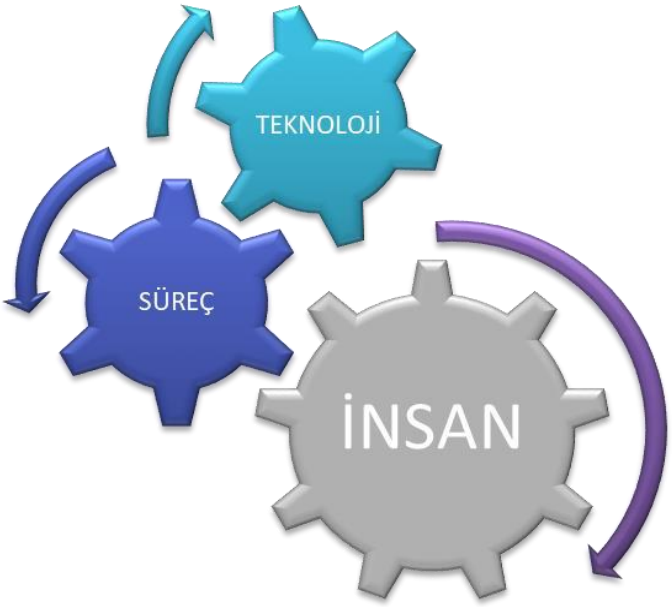
- İnsan, Süreç ve Teknoloji Yaklaşımı
- Olgunluk Modeli Yaklaşımı
- Boşluk Analizi
- Güvenlik Prensipleri

4.1.1 İnsan, Süreç ve Teknoloji Yaklaşımı

Kurumsal SOME'lerin en önemli unsuru insandır. Kurumsal SOME içerisinde görev alan personel, kurum personeli ve SOME'ler ile doğrudan etkileşime giren üçüncü tarafları ifade etmektedir.

Kurumsal SOME'lerin kurulumu ve işletimi sırasında kullanılan tüm politikalar, süreçler, kontrol listeleri ve dokümanlar da süreç unsuru kapsamında değerlendirilir.

Teknoloji ise, Kurumsal SOME'lerin kurulumu ve çalışmaları kapsamında gerçekleştirilecek faaliyetlerin başarılı bir şekilde sonuçlandırılması için gerekli olan tüm araç, gereç, yazılım ve donanımı kapsamaktadır.



Şekil 3. İnsan, Süreç ve Teknoloji Yaklaşımı

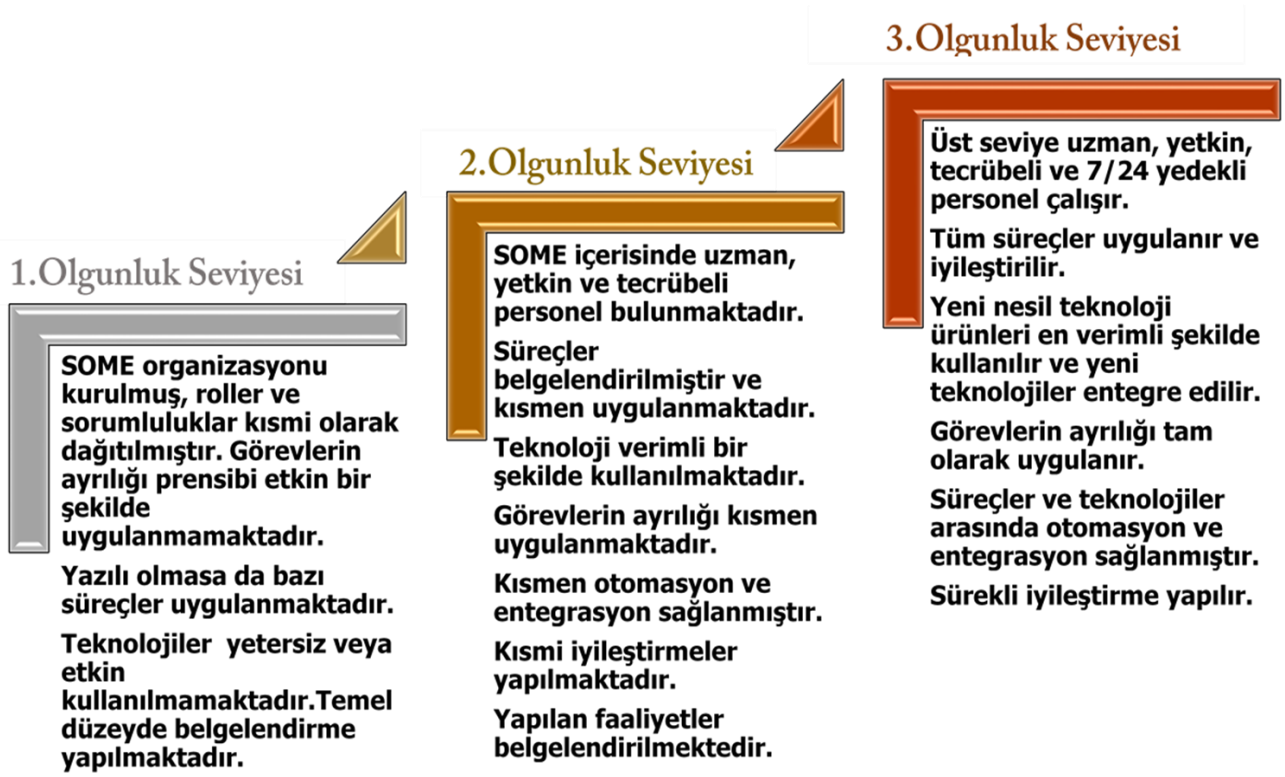
Kurumsal SOME'lerin başarılı bir şekilde kurulması ve çalışması için insan, süreç ve teknoloji bileşenlerinin uyumlu bir şekilde bir arada değerlendirilmesi önemlidir. Bu üç bileşenden herhangi birinde ortaya çıkabilecek eksiklikler veya uyumsuzluklar kurulum ve işletim çalışmalarını aksatacaktır.

Kurumsal SOME'lerin fonksiyon ve faaliyetlerine ait bileşenlerin insan, süreç ve teknoloji olarak gruplanması ve aralarındaki ilişkilerin belirlenmesi; ihtiyaçların doğru ve hızlı bir şekilde tespit edilerek temin edilmesine, yapılacak faaliyetlerin gruplanabilmesi ve bu sayede projenin daha hızlı ve kontrollü yürütülmesine imkan sağlayacaktır.

4.1.2 Olgunluk Modeli Yaklaşımı

Olgunluk modeli yaklaşımı, kurulacak Kurumsal SOME'ler için mevcut durumu tespit etmek ve iş planı oluşturmak için kullanılacak olan bir yöntemdir.

Süreklilik arz eden iyileştirme faaliyetlerini tespit edebilmek için, bu faaliyetlerin çıktılarının belirlenmesi ve belirlenen çıktıların ölçülmesi ve değerlendirilmesi gerekmektedir. Ölçme ve değerlendirme sırasında kullanılacak kriterlerin belirlendiği seviyeler olgunluk seviyesi olarak isimlendirilir. Kişi, ekip, kurum/kuruluş, uygulama veya süreçler adım adım bu seviyelerdeki kriterlere erişmek için gerekli olan faaliyetlerin gerçekleştirilmesiyle istenilen seviyeye erişirler.



Şekil 4. Kurumsal SOME Olgunluk Modeli

4.1.3 Boşluk Analizi

Boşluk analizi, mevcut durum ile hedeflenen durum arasındaki farkları tespit etmek için yapılan bir analizdir. Bu analiz sayesinde, kurumun hedeflenen duruma ulaşabilmesi için gerekli olan ihtiyaçların ve bu ihtiyaçları karşılamak için gerçekleştirilmesi gereken faaliyetlerin belirlenmesi sağlanır.

Mevcut durum tespit edildikten sonra, hangi olgunluk seviyesine ulaşılmak istendiği belirlenir. Hedeflenen olgunluk seviyesi ile mevcut durum arasındaki farklar insan, süreç ve teknoloji bileşenlerine göre ayrı ayrı değerlendirilir ve eksiklikler belirlenir.

Şekil 5. Kurumsal SOME Boşluk Analizi

Kurumun 1. Olgunluk seviyesindeki eksiklikleri tamamlanmadan, 2. veya 3. Olgunluk seviyelerinde yapmış oldukları faaliyetler olsa bile seviyesinin 1 olduğu kabul edilecektir.

1. ve 2. Olgunluk seviyesindeki tüm maddeler ve kontroller sağlandıktan sonra 2. Seviye, 1, 2 ve 3. olgunluk seviyelerindeki tüm maddeler ve kontroller sağlandıktan sonra 3. Olgunluk seviyesinde olduğu kabul edilir.

Belirlenen eksiklikler, ihtiyaçlar ve bu ihtiyaçları gidermek için yapılması gereken faaliyetler listelenir. Faaliyetler sıralanır, sorumluları atanır ve faaliyetlerin gerçekleştirilmesi için gerekli olan plan yapılarak üst yönetime sunulur.

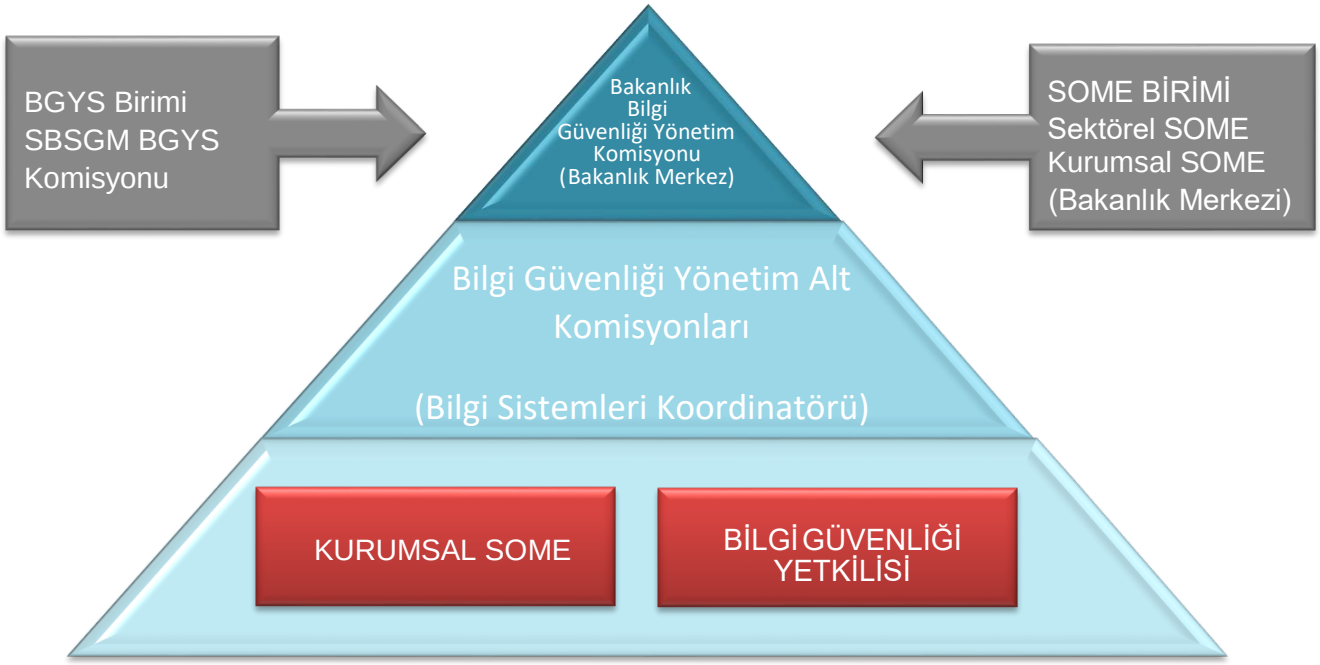
4.1.4 Güvenlik Prensipleri

Kurumsal SOME'lerin kurulması, işletilmesi ve iyileştirilmesi aşamalarında aşağıda listelenen temel güvenlik prensipleri göz önünde bulundurulur. Bu prensiplerin hepsi birbirine bağlı olup tüm güvenlik çalışmalarında dikkate alınır.

- Bütünlük
- Erişilebilirlik
- Gizlilik
- En az yetki
- Bilmesi gerektiği kadar (need to know)

4.2 Kurumsal SOME Organizasyonu

Kurumsal SOME'ler, bilgi işlem birimi bünyesinde veya bilgi işlem birimi dışında temel sorumluluğu siber güvenlik olan bir ekip lideri koordinatörlüğünde kurulur.



Şekil 6. T.C. Sağlık Bakanlığı SOME Organizasyonu

Kurumsal SOME'ler ekip lideri tercihen lisans (en az önlisans) derecesine sahip olan ve bilişim teknolojileri konusunda uzmanlaşmış personel arasından seçilir. Kurumsal SOME'ler nin gerçekleştirmesi gereken faaliyetlerin koordine edilmesini ve takibini sağlar.

- SOME organizasyonu bu rehber doğrultusunda oluşturulur, organizasyonda yer alan rollere uygun personel atanır.
- Kurumsal SOME ile diğer birimler arasında eşgüdüm sağlanır.
- Kurumu etkileyebilecek siber risklere karşı tedbirlerin alınması sağlanır.
- Siber olay esnasında, olay müdahale fonksiyonuna destek olarak koordinasyon ve paydaşlarla iletişim sağlanır.
- Siber olay sonrası adli süreçlerin takibi ve koordinasyonu sağlanır.

4.3 Fonksiyonlar

Kurumsal SOME'nin gerçekleştirmesi gereken faaliyetler, Şekil 7'de yer almaktadır.

Şekil 7. Kurumsal SOME Fonksiyonları

4.3.1 Yönetim ve Koordinasyon

SOME yönetim ve koordinasyon kapsamında temel olarak aşağıdaki faaliyetler gerçekleştirilir;

- Kurumsal siber güvenlik politikaları oluşturur.
- Siber güvenlik politika ve süreçlerinin uygulanmasını sağlar.
- Ulusal siber güvenlik stratejileri ve eylem planları kapsamındaki görevlerini eksiksiz yerine getirir.
- SOME organizasyonu bu rehber doğrultusunda oluşturulur, organizasyonda yer alan rollere uygun personel atanır.
- Kurumsal SOME ile diğer birimler arasındaki eşgüdüm sağlanır.
- Kurumu etkileyebilecek siber risklere karşı tedbirlerin alınması sağlanır.

- Siber olay esnasında, olay müdahale fonksiyonuna destek olarak koordinasyon ve paydaşlarla iletişim sağlanır.
- Siber olay sonrası adli süreçlerin takibi ve koordinasyonu sağlanır.

4.3.2 Güvenlik Yönetimi

Güvenlik yönetimi, Kurumsal SOME'ler (personel, paydaş ve üçüncü taraflar) tarafından kullanılan güvenlik teknolojilerinin kurulumu, yapılandırılması, bakımı, güncellenmesi, iyileştirilmesi ve yönetilmesi faaliyetleri ile bu faaliyetlerin güvenli bir şekilde gerçekleştirilmesine yönelik kural ve talimatların geliştirilmesini ve uygulanmasını kapsamaktadır.

Güvenlik teknolojileri dışında kalan ağ, sunucu, altyapı ve kullanıcı teknolojilerinin güvenli bir şekilde kurulması ve kullanılmasına ilişkin kural ve talimatnamelerin oluşturulması ile SOME'lerin etkileşim içerisinde olduğu diğer birimlere güvenlik konusunda verilecek destek ve yönlendirme faaliyetleri de güvenlik operasyonları içerisinde yer almaktadır.

4.3.3 Olay Müdahale

Olay müdahale fonksiyonunun amacı; ortaya çıkabilecek herhangi bir güvenlik olayına en hızlı ve doğru şekilde müdahale etmek ve etkilerini azaltacak önlemleri almaktır.

Kurumsal SOME'ler, kurumda ortaya çıkabilecek siber güvenlik olaylarını analiz eder, güvenlik olaylarına ilişkin kurum içerisinde alınacak önlemleri belirler ve gerekli tedbirleri alır.

Kurumsal SOME'ler, siber olay esnasında bilişim sistemlerine yetkisiz erişim yapılmaması ve delil bütünlüğünün bozulmaması için gerekli tedbirleri alır veya aldırır.

4.3.4 Sürekli Güvenlik İzleme

Kurum bünyesinde kullanılan ağ, sistem ve güvenlik cihazlarının durumlarını, tespit edilen güvenlik olaylarını, sistemlerde oluşabilecek kesintileri, saldırıları, hataları, uyarı ve alarmları en kısa sürede fark edip müdahale edilmesini sağlamaktır.

Sürekli Güvenlik İzleme fonksiyonunu yerine getirebilmek için; belirlenen kurum kaynaklarından uygun formatta iz kayıtları merkezi bir sistemde toplanır ve belirlenen kriterlerde anlamlandırılır ve ilişkilendirilir. Tüm süreçlerin doğru bir şekilde çalıştığının kontrol edilerek iz kayıtları arasındaki siber güvenlik olayları tespit edilir. Güvenlik İzleme fonksiyonunun 7x24 aktif olması önerilir.

4.3.5 Zafiyet Yönetimi

Zafiyet yönetimi fonksiyonunun amacı, kurum bilişim sistemlerini tehdit edebilecek yazılımsal veya donanımsal zafiyetlerin araştırılması, analiz edilmesi, tespit edilen zafiyetlerin giderilmesine ilişkin alınacak önlemlerin belirlenmesi, bu önlemlerin uygulanması yoluyla güvenlik seviyesinin arttırılmasıdır.

Zafiyet yönetimi fonksiyonu kapsamında tespit edilen zafiyetler ve tehditler için oluşturulacak iyileştirme önerileri ve alınması gereken önlemlerin uygulanması Güvenlik Yönetimi ile gerçekleştirilir.

Kurumsal SOME'ler;

- Güncel zafiyetleri sürekli olarak takip eder.
- Olgunluk seviyesine göre tespit ettiği zafiyetlerin teknik analizini yapar.
- Zafiyetlerin etkilediği sistemleri ve etkilenme seviyelerini araştırır ve alınması gereken önlemleri belirler.
- İyileştirme stratejilerini belirler ve uygulanmasını sağlar.

4.3.6 Uyumluluk ve Denetim

Kurumun bilişim altyapısı ile kurumun sorumlu olduğu siber güvenlik ile ilgili mevzuat, politika, standart vb. ile olan uyumluluğu ölçmek, kurumun bilişim altyapısı ile gerekli denetimleri gerçekleştirmek ve iyileştirme faaliyetlerini yürütmektir.

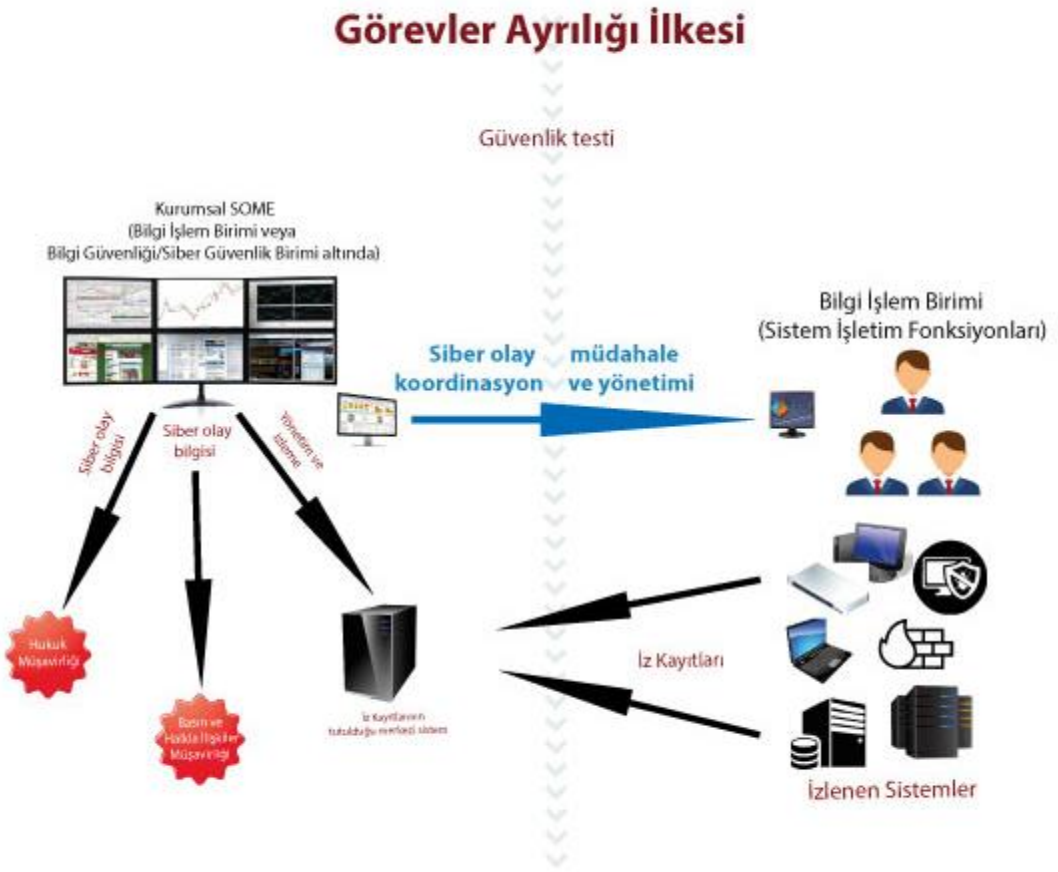
Uyumluluk ve Denetim Fonksiyonu; Sektörel SOME'ler ve USOM tarafından yürütülen çalışmalar da dikkate alınarak kurumun bilişim altyapısında kullanılan ağ, sistem ve güvenlik bileşenlerinin kurumsal politika, standart ve en iyi pratiklere uygun bir şekilde kurulup yapılandırılmasını ve işletilmesini kapsar.

4.3.7 Eğitim ve Farkındalık

Kurum bünyesinde çalışan personelin bilişim süreçlerindeki farkındalığını arttırmak ve kurumun güvenlik süreçlerinin sağlıklı bir şekilde katkıda bulunmasını sağlamak için gerekli çalışmaları devam ettirir.

4.4 Kurum İçi ve Kurum Dışı Paydaşlarla İletişim Esasları

Kurumsal SOME kurumun bilgi işlem birimi ile koordineli çalışır. Bilgi işlem birimi bilgi sistemlerini yönetirken, Kurumsal SOME siber güvenliği sağlar ve herhangi bir saldırı durumunda gerekli müdahaleyi uygular. Siber olay öncesi, bilgi işlem varlıkları üzerinde rutin güvenlik testleri yapar veya yaptırır, rutin olarak iz kayıtlarını takip eder.



Şekil 8. Kurum İçi Paydaşlar

Şekil 8'de gösterildiği üzere siber olay öncesi, bilgi işlem varlıkları üzerinde rutin güvenlik testleri yapar veya yaptırır, kayıt yönetimi ara yüzünden rutin olarak iz kayıtlarını takip eder. Kurumsal SOME kurumun bilgi işlem birimi ile koordineli çalışır. Bilgi işlem birimi bilgi sistemlerini yönetirken, Kurumsal SOME siber güvenliği sağlar ve herhangi bir saldırı

durumunda bilgi işlem biriminin yapacağı müdahaleyi yönetir ve bilgi işlem birimindeki ilgili personeli koordine eder.

Kurumsal SOME'ler, kurum dışında ise Sektörel SOME ve diğer Kurumsal SOME'ler ile iletişim halindedir ve 7x24 ulaşılabilir durumdadır. Personelin iletişim bilgilerini EK-1'de yer alan SOME İletişim Formu vasıtasıyla Sektörel SOME'ye iletir. İletişim bilgilerinde değişiklik olması durumunda Kurumsal SOME'ler bu değişikliği gecikmeksizin Sektörel SOME'ye bildirir. SOME'lerin birbirleriyle e-Posta yoluyla yapacağı iletişimin şifreli olması önerilir. Ayrıca iletişim kanalının güvenli olduğundan ve paylaşılan verinin değiştirilmeden iletildiğinden emin olunur.

Şekil 9. Kurum Dışı Paydaşlar

Kurumsal SOME'ler kanunen soruşturmaya yetkili makamlar ile sürekli iletişim halindedir. Bu iletişimin güvenli bir şekilde gerçekleştirilebilmesi için gerekli önlemler alınır.

4.5 Kurulum

Kurumun kapasitesi ve personel sayısı doğrultusunda yeterli sayıda ve kabiliyette personel belirlenir. İletişim bilgileri, İletişim Formu aracılığıyla Sektörel SOME'ye iletilir ve kapsamı Sektörel SOME tarafından belirlenen bir iş planı hazırlanır. SOME fonksiyonlarını devreye almak ve işletmek için gerekli olan politikalar, iş akışları, dokümanlar ve kontrol listeleri oluşturulur.

Sağlık Bakanlığı Merkez Teşkilatında Kurumsal SOME;

Merkez teşkilatında Kurumsal SOME, Genel Müdürlüğün ilgili birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

- Siber Güvenlik Ekip Lideri
- Siber Güvenlik Analisti
- Siber Olay Müdahale Uzmanı
- Sızma Testi Uzmanından oluşan bir ekip olarak kurulur.

Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğünde Kurumsal SOME Organizasyonu;

Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

- 1 ekip lideri,
- 3 analistten oluşur.

Türkiye İlaç ve Tıbbi Cihaz Kurumunda Kurumsal SOME Organizasyonu;

Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

- 1 ekip lideri,
- 3 analistten oluşur

Sağlık Bakanlığı Taşra Teşkilatında Kurumsal SOME:

İl Sağlık Müdürlüklerinde Kurumsal SOME, temel sorumluluğu siber güvenlik olan bir ekip lideri koordinatörlüğünde kurulur. İl grubu seviyesine bağlı olarak her ilde kendi grubuna özgü yapıda teşkil edilir.

- İ1 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 8 analistten oluşur.

- İ2 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 6 analistten oluşur.

- İ3 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 5 analistten oluşur.

- İ4 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 4 analistten oluşur.

- İ5 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 4 analistten oluşur.

- İ6 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 3 analistten oluşur.

- İ7 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

➢ 1 ekip lideri,
➢ 2 analistten oluşur.

- İ8 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

- 1 ekip lideri,
- 2 analistten oluşur.

- İ9 İl Grubu: Kurumların Bilgi İşlem Birimlerinde çalışan, teknik açıdan yeterli bilgi ve donanıma sahip personel öncelikli olmak üzere en az;

- 1 ekip lideri,
- 1 analistten oluşur.

4.6 Görevler

4.6.1 Kurumsal SOME'nin Kurulması ve İyileştirilmesi

- İnsan, süreç ve teknoloji bileşenlerinin sağlıklı ve uyumlu bir şekilde çalıştırılmasını sağlar.
- SOME fonksiyonlarının hayata geçirilmesini sağlar.
- Fonksiyonlar arasındaki koordinasyon ve uyumu sağlar.
- Fonksiyonlar arasındaki etkileşimin verimli olması için gerekli iletişim altyapısının sürekliliğini ve SOME içerisindeki iletişimin en üst seviyede tutulmasını sağlar.
- Siber güvenlik politika ve süreçlerinin uygulanmasını sağlar.
- Sektörel SOME ve USOM ile gerektiği durumlarda diğer Kurumsal SOME, paydaşlar ve üçüncü taraflar ile yapılan iletişimi koordine eder.
- Belirli periyodlarda üretilmesi gereken raporların/dokümanların oluşturulmasını sağlar ve durumlarını takip eder.
- Kuruma özgü siber güvenlik stratejilerini oluşturur.

4.6.2 Güvenlik Yönetimi

- Kurumun güvenlik ihtiyaçlarını belirler ve tanımlar.
- Tanımlanan güvenlik ihtiyaçlarını destekleyen politika, talimatname, güvenli yapılandırma ve kontrol listelerini oluşturur.
- Kurumun güvenlik ihtiyaçlarına bağlı olarak güncel güvenlik teknolojilerinin araştırılması, test edilmesi ve devreye alınması faaliyetlerini yürütür.
- Kurum iş ihtiyaçlarını karşılamak amacıyla temin edilecek olan araç, gereç, yazılım, donanım ve uygulamaların, kurum güvenlik ihtiyaçlarını karşılayıp karşılamadığını değerlendirir ve ihtiyaç halinde danışmanlık faaliyetlerini yerine getirir.
- Güvenlik teknolojilerinin, kurulumu, yapılandırılması, bakımı, yedeklenmesi ve güncellenmesi faaliyetlerini gerçekleştirir.

4.6.3 Siber Olaya Müdahale

- Olay müdahale planlarını oluşturur, güncelliğini sağlar ve yayımlar.
- Olay müdahale sürecini oluşturur ve devreye alır.
- Güvenlik olayları sonucu etkilenen veya tehdit altında olan sistemleri ve ağları korumak için aşağıdaki faaliyetleri gerçekleştirir;

  - ✓ İçeri ve dışarı doğru ağ trafiklerini filtreler, erişim kontrol listelerini oluşturur ve ağ erişimlerini sıkılaştırır.
  - ✓ Gerektiği durumlarda sistemlerin sıfırdan kurulumunu sağlar.
  - ✓ Sistemleri güvenlik risklerine karşı güncel tutar ve yamaları zamanında gerçekleştirir.
  - ✓ Güncelleme ve yamalama faaliyetlerinin yapılamadığı eski, güncelliğini yitirmiş, üretici tarafından destek verilemeyen, kapatılması veya durdurulması mümkün olmayan risk altındaki kritik sistemleri mümkün olan en güvenli hale getirecek faaliyetleri gerçekleştirir.
- Ulusal ve sektörel düzeyde etkileri olan bir güvenlik olayı tespit etmesi durumunda önce Sektörel SOME ile gerekli hallerde USOM ile paylaşır.
- Güvenlik olayı ile ilgili istatistikleri toplar, araştırır, paylaşır, gerekli duyuruları hazırlar, olayın yayılmasını engellemek için gerekli olan faaliyetleri gerçekleştirir ve/veya koordine eder.

4.6.4 Sürekli Güvenlik İzleme

- İz kayıtlarının merkezi bir şekilde tutulmasını, anlamlandırılmasını ve yönetilmesini sağlar.
- Olgunluk seviyesine göre 7x24 saat ya da 5x8 saat sistemlerinde oluşan güvenlik iz kayıtlarını izler.
- Sürekli güvenlik izlemenin etkin, verimli ve otomasyonu sağlayacak şekilde gerçekleştirilmesi için gerekli teknolojileri temin eder.
- Tespit edilen muhtemel güvenlik olaylarını analiz eder, analiz sonucunda ilgili birimler ile koordineli olarak olaya müdahale ederler.
- Siber güvenlik olaylarının tespit edilmesine yönelik alarm ve uyarı mekanizmalarının oluşturulmasını sağlar.

4.6.5 Eğitim ve Farkındalık

- SOME personelinin bilgi, beceri, eğitim ve tecrübe seviyelerini ölçer, değerlendirir ve eğitim ihtiyaçlarını tespit eder, bilinçlendirme ve farkındalık eğitimlerine katılmasını sağlar.

- SOME personelinin olaylara müdahale tecrübelerini arttırmak için bireysel veya takım halinde yapılacak tatbikat faaliyetlerini planlar ve uygulanmasını sağlar.
- SOME personelinin rolüne uygun kariyer gelişimi için alması gerekli eğitim ve sertifikaları planlar ve uygulanmasını sağlar.
- Kurum personelinin farkındalığı için sosyal mühendislik testleri yapar veya yaptırır.
- Kurum için eğitim ve farkındalık programı oluşturur.
- Kurum personeline dağıtılmak üzere, güncel siber güvenlik haberleri, tehditleri, olayları, korunma yöntemlerinden oluşan bültenlerin hazırlanmasını ve yayımlanmasını sağlar.

4.6.6 Zafiyet Yönetimi

4.6.6.1 Yama ve Güncelleme Yönetimi

- Kurumun bilişim sistemlerinden oluşan envanter listesini çıkarır, araç, gereç, yazılım, donanım ve uygulamaların güvenlik güncellemeleri ile yama durumlarını takip eder.
- Zafiyetleri gidermek için belirlenen faaliyetleri uygular veya kurum bünyesindeki diğer birimler tarafından uygulanmasını sağlar ve uygulandığını kontrol eder.
- Kurum sistemlerini etkileyebilecek zafiyetleri, bu zafiyetlerin oluşturabileceği tehditleri, korunma, önleme ve engelleme yollarını, e-posta, telefon, seminer, çalıştay vb. iletişim yöntemlerini kullanarak kurum personeline, ihtiyaç halinde paydaş ve üçüncü taraflara bildirir. Mümkünse bu işin otomatik ve gerçek zamanlı yapılması için gerekli teknolojileri temin eder.
- Güncel ve güncelliğini koruyan saldırı ve güvenlik olaylarını sürekli olarak takip eder.
- Kurumun etkileşim içerisinde olduğu diğer kurum, paydaş, üçüncü taraf ve üreticiler ile beraber gerçekleştirilen zafiyet ile mücadele faaliyetlerini koordine eder.

4.6.6.2 Sızma Testleri

Sızma Testleri, sistemlerdeki zafiyetlerin ve bu zafiyetlerin sömürülebilme durumlarının, saldırgan bakış açısıyla denetlenmesini içeren güvenlik testleridir. Kurumsal SOME'lerin en az yılda bir kez kurumları bünyesinde sızma testi yapması veya yaptırması tavsiye edilir.

Testlerde TSE "TS 13638 Sızma Testi Yapan Personel ve Firmalar İçin Şartlar" standardı kapsamında en az aşağıdaki belirtilen türlerde testleri yapar veya yaptırması tavsiye edilir.

- Ağ ve sistem altyapısı sızma testleri
  - Yerel ağ sızma testleri
  - İnternet sızma testleri
  - Güvenlik duvarı sızma testleri
  - Saldırı tespit ve/veya engelleme sistemleri sızma testleri
  - DMZ bölgesi sızma testleri
- Web uygulamaları ve veri tabanları sızma testleri

- Mobil uygulamalar sızma testleri
- Kablosuz ağlar sızma testleri
- Hizmeti aksatma saldırıları (DoS/DDoS)
- Sosyal mühendislik sızma testleri
- Endüstriyel kontrol sistemleri sızma testleri
- Fiziksel sızma testleri

Test sonuç raporlarının içermesi beklenen minimum bilgi aşağıda listelenmiştir:

- Zafiyetin önem derecesi (Acil, Kritik, Yüksek, Orta, Düşük)
- Zafiyetin etkisi
- Zafiyetin bulunduğu bileşenler
- Zafiyetin açıklaması ve nasıl tespit edildiği
- Alınması gereken önlemler

4.6.6.3 Siber Tehdit İstihbaratı

Kurumsal SOME'ler güvenlik operasyonları gereği faaliyet göstermekte olduğu kurumun ağını siber tehditlere karşı korumakla yükümlüdür. Gerekli insan, süreç ve teknoloji bileşenleri ile sağlanan güvenlik seviyesine ek olarak bir takım dış kaynaklardan siber tehdit istihbaratı verilerinin alınması ve değerlendirilmesi çalışmalarını yürütmeleri önerilir.

- Ücretli veya ücretsiz siber tehdit istihbaratı servislerine üye olur.
- Üye olunan servislerden düzenli ve otomatik bir şekilde toplanan istihbarat verilerini analiz, doğrulama ve değerlendirme çalışmaları sonrasında, kurum güvenlik cihazlarında engellenmesini sağlar.
- Toplanan istihbarat verileri ile kurum içerisindeki sistemlerden toplanan iz kayıtlarının karşılaştırılmasını ve bağlantı tespit edilmesi durumunda olay müdahalenin hayata geçirilmesini sağlar.
- Paydaşlar (Sektörel SOME, USOM vb.) tarafından bildirilen tehdit istihbaratı verilerinin değerlendirilmesini ve tespit edilen bir saldırıya ait teknik, taktik ve yöntem bilgisinin başta Sektörel SOME olmak üzere USOM ile hızlı bir şekilde paylaşılmasını sağlar.

4.6.6.4 Varlık ve Risk Değerlerinin Belirlenmesi

Kurumsal SOME, üstünde zafiyet bulunduğu tespit edilen varlıklar için başta bilgi işlem birimi olmak üzere kurumun ilgili birimleri ile iş birliği içinde varlık değerlerini belirler. Test sonuç raporundan gelen zafiyet değerleri ile varlık değerlerini kullanarak risk değerlerini hesaplar. "Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi Raporu" nu hazırlar ve kurum üst yönetimine sunar.

Şekil 10. Risk Yönetimi

Risk yönetiminin hayata geçirilmesi sırasında aşağıdaki bilgi güvenliği yönetim sistemlerinde yer alan çerçevelerden faydalanılabilir.

- Bilgi Güvenliği Politikalar Kılavuzu (Önerilen),
- ISO 27001,
- ISO 31000,
- ISO 27005,
- Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Risk değerlendirme çalışmalarının periyodik olarak en az yılda bir kez ve güvenlik yapısına yapılacak kritik değişiklikler öncesinde yapılması önerilir.

Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi Raporu,

- Risk tanımı
- Risk önceliği (Acil, Kritik, Yüksek, Orta, Düşük)
- Riskin etkisi/değeri
- Riski taşıyan varlıklar (zafiyet içeren sistemler, kritik süreçler vb.)

- Riske sebep olan zafiyetler, açıklaması ve nasıl tespit edildiği
- Alınması gereken önlemleri kapsar.

4.6.7 Uyumluluk ve Denetim

- Kurulum ve çalışma aşamalarında kullanılan politika, süreç, iş akışı, kontrol listesi ve güvenli yapılandırmaların tutarlılığını kontrol eder ve gerekli iyileştirme faaliyetlerini belirler.
- Kurulum sonrasında devreye alınan SOME fonksiyonlarını işletmek için kullanılan insan, süreç ve teknoloji kaynaklarının, hedeflenen olgunluk seviyesi ile uyumluluğunu periyodik olarak denetler.
- Zafiyet tarama, sızma testi vb. yöntemler ile insan, süreç ve teknoloji bileşenlerinde ortaya çıkan zafiyet, eksiklik, yanlış kullanım vb. azaltacak, önleyecek, iyileştirilecek faaliyetlerin listelenmesi, önceliklendirilmesi, atanması ve takip edilmesi faaliyetlerini gerçekleştirir.
- SOME fonksiyonlarının sağlıklı bir şekilde işletildiğini kontrol etmek, devreye alınan fonksiyonların verimliliğini ölçmek, yapılması gereken iyileştirme faaliyetlerini belirlemek amacıyla en az yılda bir kere kurum içi tatbikat düzenler.

4.7 Dokümanlar

Doküman Adı	Ana başlıklar	Oluşturma /Güncelleme	Paylaşım
Kurumsal SOME Politikası	Amaç, Kapsam, Hedefler, Roller, Sorumluluklar ve Görevler, Siber Güvenlik Politikası, Süreçler, Talimatnameler, Politikalar	-	-
Faaliyet Raporu	Yaşanan Güvenlik Olayları Gerçekleştirilen Eğitimler, Tatbikatlar Edinilen Tecrübeler ve Uygulanan Düzeltici ve Önleyici Faaliyetler Kurum İçi ve Dışı Paydaşlarla Yapılan Çalışmalar	Yıllık	Sektörel SOME
İletişim Dokümanı	Kurumsal SOME İletişim Bilgileri	-	Sektörel SOME
Olay Bildirim / Müdahale Formu	Ön Olay Tanımı Ön Bulgular, Emareler, Olay Bilgileri, Olay ile İlgili IP, Port, Protokol, İşletim Sistemi vb. Teknik Bilgiler	Olay müdahale aşamasında ve sonrasında	USOM Sektörel SOME Gerektiğinde savcılık/ kolluk

Tablo 3. Kurumsal SOME'nin Oluşturması Gereken Doküman Listesi

4.8 Olgunluk Seviyeleri

	1. Olgunluk Seviyesi	2. Olgunluk Seviyesi	3. Olgunluk Seviyesi
İNSAN	SOME organizasyonu mevcuttur.	Kurulu ve işleyen bir SOME mevcuttur.	Kurulu, işleyen ve sürekli iyileştirilen bir SOME mevcuttur.
	SOME faaliyetleri BT personeli tarafından yapılır.	SOME kapsamındaki tüm roller kurum bünyesinde yer almamakla birlikte siber güvenlik konusunda uzmanlaşmış personel istihdam edilmektedir.	Kurum bünyesinde, siber güvenlik alanında kullanılan ürün ve teknolojilerde dikeyde uzmanlaşmış, üst düzey bilgi, beceri ve tecrübe ile üst seviye ürün ve teknoloji sertifikalarına sahip personel mevcuttur.
	Görevlerin ayrılığı uygulanmaz.	Görevlerin ayrılığı kısmen uygulanır.	Görevlerin ayrılığı prensibi tamamen uygulanır.
	Kullanıcılar ve çalışanlar yeterli eğitim ve farkındalığa sahip değildir.	Kullanıcılar ve çalışanlar güvenlik konusunda farkındalık ve eğitim faaliyetlerine katılmıştır.	Kurumda SOME faaliyetlerinin tamamı uygulanır, personelin uzmanlaşması teşvik edilir, eğitim, sertifikasyon çalışmaları ile personelin teknolojileri takip etmesi sağlanır.
	Kurumun güvenlik konusundaki amaçları, hedefleri ve stratejileri belirgin değildir.	Kurumun güvenlik konusunda amaçları ve kısa dönem hedefleri belirlenmiştir.	Kurumun siber güvenlik konusunda amaçları, hedefleri, vizyonu ve stratejileri belirlenmiştir.
		Güvenlik operasyonlarında yedeklik sağlanmış olmasına rağmen ikincil personelin tecrübe ve yeterlilik konusunda eksiklikleri bulunur.	Güvenlik operasyonlarında tamamen yedeklilik sağlanır.
		Kurum 5/8 esasına göre çalışır.	Kurum 7/24 esasına göre çalışır.
		Güvenlik yönetim ve koordinasyon faaliyetleri genellikle BT yöneticisi tarafından yapılır.	SOME, bilgi güvenliği ve siber güvenlik konularında yeterli bilgi ve tecrübeye sahip bir güvenlik yöneticisi tarafından yönetilir.
		BT faaliyetleri ile SOME faaliyetleri kısmen ayrılmıştır.	BT faaliyetleri ile SOME faaliyetleri tamamen birbirinden ayrılmıştır.
		Üst yönetim güvenlik konusunda farkındalık sahibidir.	Üst yönetim güvenlik konusunda üst seviye farkındalık sahibidir.
		BT faaliyetlerine ve iş süreçlerine güvenlik faaliyetleri entegre edilmemiştir.	Tüm BT ve iş faaliyetleri siber güvenlik göz önüne alınarak gerçekleştirilir, bu faaliyetlerin çıktıları sürekli olarak denetlenir ve iyileştirmelerin ivedi bir şekilde yapılması sağlanır.

		Personelin eğitimi teşvik edilir.	Kurum bünyesinde siber güvenlik eğitim ve farkındalığı bir program çatısı altında tüm kullanıcı ve çalışanlara sürekli ve periyodik olarak verilir.
SÜREÇ	Kurumun SOME faaliyetlerini işletmek ve desteklemek amacıyla kullandığı politika, süreç, talimatname, topoloji, envanter vb. , kontrol listesi eksiktir veya güncel değildir.	Kurumun SOME faaliyetlerini işletmek ve desteklemek amacıyla kullanılan politika, süreç, talimatname, kontrol listesi, topoloji, envanter vb. oluşturulur ve belgelendirilir.	Kurumun SOME faaliyetlerini işletmek ve desteklemek amacıyla kullanılan politika, süreç, talimatname, kontrol listesi, topoloji, envanter vb. oluşturulmuş ve belgelendirilmiştir.
	Kurum bünyesinde gerçekleştirilen SOME faaliyetleri genellikle e-posta üzerinden veya sözlü olarak işletilir, herhangi bir süreç veya otomasyon yoktur.	Kurum bünyesinde gerçekleştirilen tüm SOME faaliyetleri, yapılan değişiklikler, ortaya çıkan siber güvenlik olayları kayıt altına alınır.	Kurum bünyesinde gerçekleştirilen tüm SOME faaliyetleri, yapılan değişiklikler, ortaya çıkan siber güvenlik olayları kayıt altına alınır.
		SOME faaliyetlerini gerçekleştirmek için gerekli olan süreçler devreye alınmıştır.	SOME faaliyetlerini gerçekleştirmek için gerekli olan tüm süreçler devreye alınmıştır.
		SOME faaliyetleri gerçekleştirilirken yapılan tüm işler belgelendirilir, mevcut dokümanlar sürekli olarak güncellenir.	Devreye alınan süreçlerin iyileştirilmesi için gerekli olan ölçme ve değerlendirme faaliyetleri sürekli ve periyodik olarak yapılır.
		SOME, BT ve iş süreçleri arasında herhangi bir entegrasyon mevcut değildir.	SOME faaliyetleri ile, BT ve iş faaliyetleri arasındaki etkileşim ve ilişkinin sağlıklı bir şekilde, izlenmesi, ölçülmesi ve aksaklıkların kısa sürede tespit edilebilmesi için SOME, BT ve iş süreçleri arasında entegrasyon ve otomasyon sağlanır.
			SOME faaliyetleri gerçekleştirilirken yapılan tüm işler belgelendirilir, mevcut dokümanların iyileştirilmeleri için gerekli olan ölçme ve değerlendirme faaliyetleri sürekli ve periyodik olarak yapılır.
TEKNOLOJİ	SOME bünyesinde kullanılması gereken teknoloji ihtiyacı kısmen belirlenmiştir.	Önceden tanımlanmış SOME faaliyetlerini gerçekleştirmek için gereken temel teknoloji ihtiyacı belirlenmiştir.	Mevcuttaki tüm SOME faaliyetlerini gerçekleştirmek için gereken teknoloji ihtiyacı ile iyileştirme hedefleri belirlenmiştir.
	Kullanılan teknoloji bileşenleri verimli bir şekilde kullanılmaz.	Kullanılan temel teknoloji bileşenleri önceden tanımlanmış olan SOME faaliyetlerindeki ihtiyacı karşılamaz ve verimli bir şekilde kullanılır.	SOME bünyesinde güncel ürün ve teknolojiler verimli bir şekilde kullanılır.

	Teknoloji bileşenleri arasında bir entegrasyon bulunmaz.	Teknoloji bileşenleri arasında kısmen bir entegrasyon bulunmaz.	Kullanılan teknolojilerin verimliliği, sürekli ve periyodik ölçme ve değerlendirme faaliyetleri ile desteklenerek sürekli iyileştirmeler yapılır.
	Teknoloji bileşenlerinin yönetimi ve kullanımına dair bir standart mevcut değildir.	Teknoloji bileşenlerinin kurulumunda ve işletiminde belgelendirilmiş politika, talimatname ve kontrol listeleri kullanılır.	Yeni siber güvenlik teknolojileri takip edilmekte, test edilmekte ve ihtiyaç halinde temin edilerek kurum sistemlerine entegre edilir.

Tablo 4. Kurumsal SOME Olgunluk Seviyeleri

4.9 Kurumsal SOME Personeli Eğitimleri

Kurumsal SOME'lerde istihdam edilecek personelin alması gereken ve tavsiye edilen eğitimler Tablo 5'de verilmiştir. Eğitimler, kurumsal SOME personelinin sistemli bir şekilde kayıt analizi ve yönetimi yapabilmesi, kurumun bilişim sistemlerindeki önemli güvenlik zafiyetlerini tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinlikleri vermeyi hedeflemektedir. İhtiyaç duyulan asgari eğitimlerden bazıları Sektörel SOME tarafından verilir ya da koordine edilir.

Alması Gereken Eğitimler	Tavsiye Edilen Eğitimler
1. Siber Güvenliğin Temelleri Eğitimi 2. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi 3. Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi 4. Siber Savunma Teknolojileri Eğitimi 5. Güvenli Ağ Tasarımı Eğitimi 6. Ağ Savunma Sistemleri Eğitimi 7. İşletim Sistemi Güvenliği (Windows) 8. İşletim Sistemi Güvenliği (Linux) 9. Web Uygulama Güvenliği 10. Veri tabanı Güvenliği 11. Olay Müdahale Eğitimi 12. Bilgi Güvenliği Farkındalık Eğitimi	1. Bilgisayar Adli Analizi -Derinlemesine Windows Eğitimi 2. Ağ Adli Analizi Eğitimi 3. Zararlı Yazılım Analiz Yöntemleri Eğitimi 4. DDoS Saldırıları ve Korunma Yolları Eğitimi 5. Güvenli Yapılandırma Denetimi Eğitimi 6. Saldırı Teknikleri Eğitimi 7. Siber Tehdit İstihbaratı Eğitimi 8. Saldırı Tespit ve Kayıt Yönetimi Eğitimi 9. Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi 10. Bilişim Sistemleri Adli Analizi Eğitimi

Tablo 5. Kurumsal SOME'nin Alması Gereken Eğitimler

Ek 1. Kurumsal SOME İletişim Bilgileri Formu

<table>
<tr><th colspan="6">KURUMSAL SOME İLETİŞİM BİLGİLERİ FORMU</th></tr>
<tr><td colspan="2">Kurum Adı</td><td colspan="3"></td><td>Tarih:</td></tr>
<tr><td colspan="2" rowspan="2">SOME Takımı
7/24 İletişim Bilgileri</td><td>Telefon</td><td>Cep telefonu</td><td>Faks</td><td>Kurumsal e-Posta</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Hizmet aldığı İSS</td><td colspan="4"></td></tr>
<tr><td colspan="2">İSS’den almış olduğu güvenlik hizmetleri</td><td>DDOS</td><td colspan="3">Diğer:</td></tr>
<tr><td colspan="2">Kullanılan güvenlik cihazları</td><td>Firewall ☐</td><td>IPS ☐</td><td>WAF ☐</td><td>Diğer:</td></tr>
<tr><td colspan="2">Kurum Dış IP’leri</td><td colspan="4"></td></tr>
<tr><td rowspan="6">SOME Personelinin*</td><td>Adı Soyadı</td><td>Unvanı</td><td>İş telefonu</td><td>Cep telefonu</td><td>Kurumsal e-Posta adresi</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="5">İzlenmesi Talep Edilen Sistemlerin</td><td>Alan Adı</td><td>IP Adresi</td><td colspan="3">Açıklama</td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
</table>

Ek 2. Siber Olay Bildirim ve Müdahale

OLAY BİLDİRİM ve MÜDAHALE FORMU

OLAY BİLDİRİM BÖLÜMÜ

1. Bildirimi yapan birim:

2. Bildirimi yapan personelin

Ad, Soyadı :
Unvan/Birim :
Telefon :
e-Posta :

3. Olay türü:

□ Servis Dışı Bırakma Saldırısı (DoS/DDoS)
□ Bilgi Sızdırma (Data Leakage)
□ Zararlı Yazılım (Malware)
□ Dolandırıcılık (Fraud)
□ Port Tarama
□ Veritabanı Saldırısı
□ Diğer (Lütfen açıklayınız):

□ Web Uygulamaları Güvenlik İhlalleri
□ Sosyal Mühendislik
□ Veri Kaybı/ Veri İfşası
□ Zararlı Elektronik Posta(Spam)
□ Parola Ele Geçirme
□ Taşınır Cihaz Kaybı
□ Kimlik Taklidi
□ Oltalama (Phishing)
□ Kişisel Bilgilerin Kötüye Kullanımı

4. Olay sistem kesintisine sebep oldu mu? □ Evet □ Hayır

5. Olayın:

Tahmini başlangıç zamanı
Tarih : …….. Saat : ……..

Tespit edildiği zaman
Tarih : …….. Saat : ……..

6. Eklemek istedikleriniz:

OLAY MÜDAHALE BÖLÜMÜ
Dikkat: Bu kısım Bilgi Güvenliği / SOME Olay Müdahale Ekibi tarafından doldurulur.
7. Siber olaylara ait iz (log) kayıtları tespit edildi mi? □ Hayır □ Evet **Kaynak IP** : _____ **Hedef IP** : _____ **Port** : _____ **Diğer** : _____
8. Olayın etkisini azaltıcı ilk önlemler:
9. Olayın muhtemel sebepleri:
10. Olayın tekrarlanmaması için alınan önlemler:
11. Tahmini Olay Maliyeti
12. Eklemek istedikleriniz:

5. OLAY SONRASINDA İNCELENMEK ÜZERE GÜVENİLİR DELİLLERİN ELDE EDİLMESİ İÇİN TUTULACAK KAYITLARIN ASGARİ NİTELİKLERİ

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 3. Maddesi çerçevesinde **"Siber Olayların Delillendirilmesi"** eyleminin **"Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin belirlenmesi"** alt eyleminde İçişleri Bakanlığı sorumlu kuruluş olarak belirlenmiştir.

İçişleri Bakanlığının eşgüdümünde ve ilgili kurum/kuruluşların katılımı ile tamamlanan **"Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri"**ne ilişkin çalışma tamamlanmıştır.

Bu çalışma kurumlar için bir kılavuz niteliğinde olup kurumların kendi sistemlerine ilişkin risk değerlendirmesi yaparak hangi sistemleri kuracaklarını ve hangi sistemlerden, ne seviyede kayıt toplayacaklarını belirlemeleri gerekmektedir.

Çalışma sonucunda oluşturulan rapor 7 başlık altında toplanmış olup bunlar aşağıdaki gibidir:

1. İz Kayıtlarının Alınması Gereken Sistemler
2. İz Kayıtlarında Bulunması Gereken Asgari Nitelikler
3. İz Kayıtlarının Güvenliği
4. İz Kayıtlarının Yönetimi ile İlgili Roller
5. İz Kayıtlarının Saklanma Süresi
6. Ortak Zaman Sunucusu Kullanımı
7. Merkezi İz Kayıtları Yönetiminin Sağlanması

1. İz Kaydı Alınması Gereken Sistemler

A. Fiziksel ortam kayıtları:

1) Kritik Bilişim sistemleri odaları giriş-çıkış kayıtları,
2) Kritik Bilişim sistemleri odaları giriş-çıkış kamera kayıtları,
3) Çalışma ortamları giriş-çıkış kayıtları,
4) Çalışma ortamları giriş-çıkış kamera kayıtları.

B. Sanal ortam kayıtları:

1) Güvenlik duvarları,

2) Antivirüs yazılımları,

3) Saldırı tespit/önleme sistemleri,

4) Yönlendiriciler ve anahtarlama cihazları,

5) Sunucular,

6) İş uygulamaları (Kritik Kurumsal projeler),

7) Veri tabanları,

8) Sanal özel ağ sistemleri

2. İz Kayıtlarında Bulunması Gereken Asgari Nitelikler

A. Kaydı Oluşturan Sistem

B. Kaydın Oluşturulma Zamanı (Tarih, saat, zaman dilimi)

C. Kaydı Oluşturan Olay

D. Kaydın İlişkili Olduğu Kişi (IP-Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı)

3. İz Kayıtlarının Güvenliği

A. Gizlilik

- Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri yapılandırılmalıdır.

- Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında teknik imkânlar dâhilinde trafiğin şifreli olarak transfer edilmesi sağlanmalıdır.

B. Bütünlük

- İz kayıtlarının tek yönlü kriptografik özet değerleri (hash) hesaplatılmalı ve iz kayıtları güvenli ortamlarda saklanmalıdır.

- Siber olaylara ilişkin iz kayıtlarının saklanması için kurulacak yapının kayıtları, olayların olduğu sistem dışında merkezi bir sunucuda saklanmalıdır. Kurum kritik olaylarını belirlemelidir. Kritik olayların iz kayıtları merkezi sunucuya anlık olarak (olay oluştuğu zaman) gönderilmeli, kritik olmayan olayların iz kayıtları da kurumun belirlediği aralıklarda merkezi sunucuya iletilmelidir.

- Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi sunucularda yedeklenmeli, silinmelerine ve değiştirilmelerine izin verilmemelidir.

- Merkezi iz kaydı sunucuları sadece yeni iz kayıtlarının saklanması için fonksiyonlar içermeli, iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere kapalı olmalıdır.

C. Erişilebilirlik

İz kayıtlarının periyodik olarak yedeklenmesi ve yedeklerin uygun şekilde muhafaza edilmesi sağlanmalıdır.

4. İz Kayıtlarının Yönetimi ile İlgili Roller

Kurumların iz kayıtlarının yönetimi; iz kayıtlarının üretilmesi, transfer edilmesi, depolanması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi aşamalarını kapsar. Bu süreçlerde sistem, veri tabanı, ağ ve güvenlik yöneticileri, Siber Olaylara Müdahale Ekipleri (SOME), yazılım geliştiriciler ve denetçilere ait görev ve sorumluluklar belirlenmelidir.

5. İz Kayıtlarının Saklanma Süresi

İz kayıtlarının saklanma süresinin belirlenmesinde, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulmalıdır. İz kayıtları bu bilgiler ışığında asgari olarak 2 yıl süre ile saklanmalıdır. Kurumların kendi mevzuatları gereği uyması gereken süreler saklıdır.

6. Ortak Zaman Sunucusu Kullanımı

Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması gerekmektedir. Bütün sistemlerin zamanlarının aynı yapılması işlemi için Ağ Zaman Protokolü (NTP - Network Time Protocol) sunucusu kurulup kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesi sağlanmalıdır. Bunun yanında farklı ülkelerde birimleri olan kurumlar için saat dilimi (timezone) de dikkate alınmalıdır.

7. Merkezi İz Kayıtları Yönetiminin Sağlanması

Yukarıda asgari nitelikleri belirtilen iz kayıtlarının daha etkin, verimli ve güvenli bir şekilde toplanması, ilişkilendirilmesi, arşivlenmesi, raporlanması amacıyla Merkezi İz Kayıtları Yönetimi Mekanizmaları devreye alınmalıdır.