TÜRKİYE CUMHURİYETİ
CUMHURBAŞKANLIĞI
SİBER GÜVENLİK
BAŞKANLIĞI

SOME İLETİŞİM PLATFORMU (SİP)
BAŞVURU KILAVUZU

MAYIS 2026

BELGE ADI: SOME İletişim Platformu (SİP) Başvuru Kılavuzu

SÜRÜM NO: 1.0

SÜRÜM TARİHİ: 20.05.2026

GİZLİLİK DERECESİ: Tasnif Dışı

Değişiklik No	Değişiklik Tarihi	Değişiklik Nedeni
1.0	Mayıs 2026	İlk Yayın

1. TANIMLAR VE KISALTMALAR

Bu kılavuzda geçen;

Sıfırıncı Gün Zafiyeti: Güvenlik uzmanları veya yazılım geliştiricileri tarafından henüz keşfedilmemiş ve dolayısıyla onarımı yapılmamış güvenlik açıklarını (Üreticisi tarafından yama paketi yayımlanmamış zafiyetleri),

Siber Güvenlik Duyurusu: Siber güvenlik tehditleri, zafiyetler veya ihlaller hakkında bireyleri veya kurumları bilgilendirmek, alınması gereken önlemler ve uygulanacak güvenlik adımları hakkında kılavuzluk etmek için yapılan duyuruları,

Siber Olay: Bilgisayar ağları üzerinden gerçekleşen herhangi bir güvenlik ihlali veya saldırıyı ifade eden; veri hırsızlığından sistemlere yetkisiz erişime kadar geniş bir yelpazeyi kapsayan; depolanan, iletilen veya işlenen verilerin veya şebeke ve bilgi sistemleri tarafından sunulan veya bunlar aracılığıyla erişilebilen hizmetlerin kullanılabilirliğini, gerçekliğini, bütünlüğünü veya gizliliğini tehlikeye atan bir siber olayı,

Siber Tehdit İstihbaratı: Mevcut siber tehditlerin tanımlanması, toplanması, işlenmesi ve analiz edilmesi sonucunda elde edilen bilgilerdir. Bu bilgiler, tehditleri önceden belirleyerek önlem almak ve siber güvenliği artırmak için kullanılır. Bir kurumun ya da kişinin siber uzaydaki varlıklarına yönelik mevcut veya potansiyel siber tehdit unsurları hakkında, kurumun ya da kişinin karalarını ve müdahalesini sağlamak için kullanılabilecek, karar verme süreçleri için gerekli bağlamı sağlamak üzere bir araya getirilmiş, dönüştürülmüş, analiz edilmiş, yorumlanmış veya zenginleştirilmiş kanıta dayalı bilgiyi,

Başkanlık: Siber Güvenlik Başkanlığını,

SİP : SOME İletişim Platformunu,

SOME : Siber Olaylara Müdahale Ekibini,

SOME İletişim Platformu: Başkanlık ile Sektörel ve Kurumsal SOME'ler arasında elektronik güvenliği tesis edilmiş güvenli iletişim kanalını,

Zafiyet : Bir sistemin dışarıdan gelebilecek saldırılara veya zararlara karşı zayıf, güvensiz veya savunmasız olduğu durumu

ifade eder.

2. SOME İLETİŞİM PLATFORMU

Siber Güvenlik Başkanlığı ile Siber Olaylara Müdahale Ekipleri (SOME) arasında iletişim, elektronik güvenliği tesis edilmiş SOME İletişim Platformu (SİP) aracılığıyla sağlanmaktadır.

Siber güvenlik bildirimlerinin çift yönlü olarak iletildiği SİP uygulamasında;

- Sektörel SOME'ler,
- Sektörel SOME'lere bağlı SOME'ler ve
- Bağımsız SOME'ler

bulunmaktadır.

SİP Uygulamasının Sağladığı İmkânlar

SOME hesaplarının yönetiminde SOME'lere ilişkin dijital varlıklar, kullanılan teknolojiler ve kullanıcı listesi gibi bilgiler SİP üzerinde kaydedilmektedir. SOME'ler ile paylaşılacak bilgiler şu şekildedir:

Zafiyet Tarama Sonuçları: Başkanlık tarafından Türkiye genelinde sürekli taranan internetten erişime açık varlıklarda tespit edilen bulgular,

Siber Tehdit İstihbaratı: İlgili kuruluşa ait tespit edilen bilgiler,

Özel Güvenlik Duyuruları: Kuruluşun bildirdiği teknolojiler ile ilgili elde edilen bilgiler,

Genel Güvenlik Duyuruları: Kuruluş ve teknolojiler fark etmeksizin tespit edilen bulgulara göre yapılan siber güvenlik bildirimleri,

Sıfırıncı Gün Zafiyetleri: İlgili kuruluş tarafından geliştirilen ve/veya kullanılan teknolojilerde tespit edilen zafiyetler,

Olgunluk değerlendirmesi: Başkanlık tarafından SOME'lerin olgunluk değerlendirmesi yıllık yapılmakta ve bu değerlendirme sonucunda her SOME özelinde sahip olması gereken yetenekler ile geliştirmesi gereken yetenekler karşılaştırmalı olarak raporlanmaktadır.

Ayrıca SOME'ler SİP uygulaması aracılığıyla Başkanlığa bildirimlerde bulunabilmektedir.

Yukarıda belirtilen tüm imkânlardan etkin bir şekilde faydalanabilmek için SOME'ler tarafından bilgilerin eksiksiz olarak bildirilmesi gerekmektedir.

Hesap Türleri, Roller ve Yetkiler

SİP üzerinde "SOME hesabı" ve "kullanıcı hesabı" olmak üzere iki türlü hesap bulunmaktadır.

SOME hesapları, her SOME için bir adet oluşturulan ve özel yetkili kullanıcı hesaplarıyla yönetilen kullanıcı grubu hesaplarıdır.

SOME hesaplarının;

- SOME,
- Sektörel SOME

olmak üzere iki (2) rolü bulunmaktadır.

Bir sektörel SOME'ye bağlı olsun veya olmasın, her SOME "SİP Uygulamasının Sağladığı İmkânlar" bölümünde belirtilen ve kendisi ile paylaşılan bildirimlere erişebilmektedir.

Sektörel SOME'ler ise SOME imkânlarına ek olarak kendisine bağlı SOME'lerin bildirimlerine de erişebilmektedir.

Bir SOME'ye iletilen bildirim, SOME'ye dâhil tüm kullanıcılar tarafından görüntülenebilmektedir.

SİP uygulamasında kayıtlı SOME hesaplarına bir veya birden fazla personel farklı rollerde eklenebilmektedir.

SOME hesapları, kurumsal e-posta adresleri ile kayıt edilebilmektedir. Aynı zamanda SOME hesabının iletişim e-postası bir kişiye ait olmamalıdır. Örneğin; deniz[.]taskiner[@]siberguvenlik[.]gov[.]tr adresi bir SOME hesabı için kullanılmamalıdır. Doğru kullanım some[@]siberguvenlik [.]gov[.]tr veya iletisim[@]siberguvenlik [.]gov[.]tr şeklindedir.

Kullanıcı hesabı, SOME personeli için oluşturulan hesap türüdür. SİP uygulamasında giriş daima kullanıcı hesapları ile yapılmaktadır. SOME hesapları ile giriş yapılmamaktadır.

Kullanıcı hesaplarının rolleri şunlardır:

- Yönetici yetkili hesap
- Standart yetkili hesap

Başvuru esnasında en az bir yönetici hesabı bildirilmesi gerekmektedir. SOME hesaplarının birden fazla yönetici rolünde kullanıcısı olabilir ve bu yönetici rolüne sahip kişiler, SOME hesaplarına yeni kullanıcı ekleyebilirler, kullanıcı yetkilerini düzenleyebilirler ve kullanıcı kayıt durumlarını aktif-pasif olarak değiştirebilirler.

Kullanıcı hesapları, kurumsal e-posta adresleri ile kaydedilebilmektedir.

SİP uygulamasına erişim mutlaka iki faktörlü doğrulama ile yapılmaktadır. Varsayılan ve güvenilir ayar olarak ikinci doğrulama faktörü SMS doğrulama uygulaması kullanılmaktadır. Zorunlu durumlarda ikinci doğrulama faktörünün değiştirilebilmesi mümkün olmakla birlikte bu imkân opsiyonel değildir. İkinci doğrulama faktörünün değiştirilmesi için zaruri bir sebep aranmaktadır. Bu nedenle ikinci doğrulama faktörünün değiştirilebilmesi için sip[@]siberguvenlik [.]gov[.]tr hesabına e-posta ile başvurulması gerekmektedir.

SİP'e bireysel başvuru kabul edilmemektedir. Hesap başvurusu yapılabilmesi için kamu veya özel, bir kuruluşun SOME birimi olma şartı aranmaktadır.

3. SOME İLETİŞİM PLATFORMU BAŞVURUSU

SİP üzerinden SOME hesap başvurusu yapılabilmesi için Ek-1'de yer alan SOME İletişim Bilgileri Formunun doldurulup resmi yazıyla birlikte aşağıdaki adreslerden birisine gönderilmesi gerekmektedir.

İletişim Adresi: T.C. Cumhurbaşkanlığı Çankaya Yerleşkesi Ziaur Rahman Cad.

Çankaya / ANKARA

KEP Adresi: siberguvenlikbaskanligi@hs01.kep.tr

4. EKLER

Ek-1 SOME İletişim Bilgileri Formu