Siber Güvenlik İyileştirme Hibesi (CySIG)

TÜRKÇE

Amaç:	**Akademik ve Araştırma Kurumlarında bilgi ve siber güvenlik seviyesini artırmak.** Hibeler, akademik ve araştırma kurumlarının, bilgisayar sistemlerine yetkisiz erişim yoluyla hassas araştırma ve tasarım verilerini çalmayı amaçlayan kötü amaçlı yapıların taşıdığı siber tehditlere yönelik savunma sağlama ve yanıt verme kapasitesini geliştirmek üzere verilmektedir.
Yarışma Açılışı:	**Gürcistan: Haziran 9, 2022** **Ermenistan: 29 Eylül 2022** **Türkiye, Azerbaycan, Bulgaristan: 23 Eylül 2022**
Son Başvuru Tarihi:	**Gürcistan: 22 Temmuz 2022** **Ermenistan, Türkiye, Azerbaycan, Bulgaristan: 7 Kasım 2022**
Uygunluk:	Başvuru Sahipleri - Akademik ve Araştırma Kurumları - aşağıdaki bölümleri kapsayan konular hakkında ileri seviye araştırma alanları: • Bilim ve teknoloji • Mühendislik (tüm türleri) • Sosyal bilimler • Tıp • Bilgi İşlem • Navigasyon ve Havacılık Elektroniği • Tahrik Sistemleri • Telekomünikasyon ve Bilgi Güvenliği • Elektronik Uygun ülkeler - Gürcistan, Ermenistan, Türkiye, Azerbaycan, Bulgaristan
Nasıl Başvurulur:	cysig@crdfglobal.org adresine e-posta gönderin
Genel Alan:	Siber Güvenlik
Hibe Tutarı:	30.000 dolara kadar
Hibe Süresi:	Bir yıl
Duyuru ve Başvuru:	http://www.crdfglobal.org/ (bkz. "Mevcut Finansman Fırsatları")

Genel Bakış

Bir çalıştay vasıtasıyla başarılı bir siber güvenlik programı için gereken bilgi, beceri ve araçları edinmenin, önerilen kontrolleri ve savunma mekanizmalarını hayata geçirmek üzere kapasite gelişimiyle desteklenmesi gereklidir. CRDF Global, çalıştaylardan birine temsilci gönderen araştırma kurumlarına ve üniversitelere donanım ve bununla ilişkili kurulum masrafları, bilgi ve siber güvenliği iyileştirecek malzemeler ve gereçler için hibe verecektir.

- Siber Güvenlik İyileştirme Hibeleri, uygunluk kriterleriyle eşleşen Akademik ve Araştırma Kurumlarında bilgi ve siber güvenlik seviyesini yükseltmek için CRDF Global sponsorluğundaki hibelerdir.
- CySIG'ler bir yılı kapsayan, her biri 30.000 dolara kadar olan tek seferlik hibelerdir
- Hibeler CRDF Global üzerinden gerçekleştirilir

Uygunluk

Siber hırsızlık program çalıştaylarından birine temsilci gönderen herhangi bir araştırma kurumu veya yüksek öğrenim kurumu başvuru hakkına sahiptir. Başvuru sahipleri bireysel kurum olarak veya konsorsiyum olarak başvurabilir. Baş Araştırmacı ve diğer araştırma hibe ekibi üyelerinin çalıştaya katılmasına gerek yoktur. Bu yarışmada başvuruların değerlendirilmesi için kurumsal onay gereklidir.

CySIG'ler, sıralanan kriterlerin tamamını karşılayan katılımcılara (kamu ve özel akademik ve araştırma kurumları) açıktır:

- Yukarıda sıralanan konular hakkında aktif araştırma. Diğer araştırma konularından adaylar uygun gerekçeyle başvurabilir.
- İleri seviye güvenlik iyileştirmelerine uygun olan mevcut bir BT altyapısı
- Uygun ülkelerin herhangi birinde bizzat bulunmak
- Kurumsal onay

Her teklif bağımsız olarak değerlendirileceği için bu programa gönderilen diğer programların başarısının bir parçası olmamalı ve buna bağlı olmamalıdır.

Her başvuru sahibinin (kurumun), bu hibe yarışmasına araştırma bölümü başına sadece bir başvuru göndermesine izin verilir.

CRDF Global herhangi bir kişinin veya kurumun kendi programlarına katılmasını kısıtlama hakkını saklı tutar. CRDF Global, ihracat denetimi ve yabancı uyruklu kişilerin veya kurumların faaliyetlerine katılmasıyla ilgili tüm ABD yasalarına ve yönetmeliklerine uygun hareket eder. ABD Hükümetinden uygun izin alınmadan ABD'nin kısıtladığı kurumlarla işlem yapmamak CRDF Global'in politikasıdır.

Gerekli Başvuru Materyalleri

Tüm başvurulara, CRDF Global'in Microsoft Word belge şablonu olarak indirebilecek *Akademi Hibe Başvurusunda Siber Hırsızlıkla Mücadele Kontrol Listeleri*'ndeki bilgiler ve destekleyici belgeler eklenmelidir. Başvuru materyalleri ve araştırma ürünleri, İngilizce dilinde veya standart bir yerel dilde gönderilebilir. Başvuru ve açıklamadaki maddeler tek satır aralıklı beş sayfayla sınırlı olmalıdır. Ek destekleyici belgeler ve çizelgeler, bu açıklamaya eklenebilir veya ayrı belgeler olarak gönderilebilir.

Aşağıdakiler dahil tamamlanmış CySIG başvuru formu ve destekleyici belgeler:

- **Tamamlanmış CySIG bütçe formu***(zorunludur)*
- Başvuru sahibi taraftaki her proje ekip üyesinin **özgeçmişi** (her biri Word veya PDF biçiminde maksimum 3 sayfa olmalıdır) ve başvuru sahibi kurumun Bilgi Güvenliği Yöneticisinin (CISO) iletişim numarası ve e-posta adresi (*zorunludur*)
- Rapor veya iç yazışma şeklinde **dahili veya harici siber güvenlik açığı değerlendirmesi** (*zorunludur*)
- **Kurumsal Onay Yazısı** (*zorunludur*)* *hak kazanmak için kurumunuzun yönetiminden alınan belgede, kurumunuzun bu hibeye başvurmak ve uygulamak için size destek verdiği belirtilmelidir. Form yönetim tarafından **imzalanmalıdır**.*
- Baş Araştırmacı veya proje ekibinin çalışmasına aşina olan bağımsız kişilerin **bir referans listesi** verilmelidir.

Tüm başvuru materyalleri Word veya PDF belgeleri olarak, CRDF Global'in sağladığı formlar kullanılarak ekte gönderilmelidir.

Hibe Kapsamı

*CySIG'ler **donanım(ve ilişkili kurulum ücretleri),** bilgi ve siber güvenliği iyileştiren **malzemeler ve gereçler** için kullanılabilir. **Başvuru sahibi taraftaki proje ekibi üyelerinin çalışma masraflarına bu hibe finansmanı kapsamında izin verilmez.**

İzin Verilen Masraflar
Ana İrtibat Kişisinin çalıştığı kuruma CRDF Global'in vereceği maksimum hibe tutarı 30.000 ABD dolarıdır. *Hibe verilmesi durumunda CRDF Global finansmanını isteyen bütçelerde değişikliğe gidilebilir.

İzin Verilen Giderler
- Donanım, Gereçler ve Hizmetler (ESS),
- Diğer Doğrudan Masraflar (ESS kurulumu ve bakımıyla ilgili olabilecek diğer tamamlayıcı giderler)

Teklif Değerlendirme Kriterleri
Tüm teklifler aşağıdaki kriterlere göre değerlendirilecektir:

1. **Siber güvenlik ilgisi ve etkisi:**
   - Teklif edilen güvenlik yükseltmeleri nelerdir ve kurum içinde güvenliği nasıl iyileştirecektir?
   - Başvuru sahibi bilgi kaynaklarına yönelik siber saldırı girişimlerinin emsallerini ne sıklıkla gözlemlemiştir?
   - Kilit bilgi kaynaklarına yönelik başarılı bir siber saldırı/siber hırsızlık olması durumunda bunun azami olası sonuçları ne olur?

2. **Sürdürülebilirlik ve bağlılık**:

- Başvuru sahibinin kurumu, karşılıksız finansal, lojistik ve/veya personel desteği sunarak projeye bağlılığını gösteriyor mu?
- Başvuru sahibinin net bir izleme/değerlendirme stratejisi veya planı var mı? Başvuru sahibi, istenen yükseltmenin amaçlanan etkiyi bırakacağını nasıl bilecek?
- Başvuru sahibinin kurumu, uzun vadeli finansal destek veya ayrıntılı bir bakım planı sunuyor mu?

3. **Açıklık, uygunluk ve ayrıntı**:
   - Projenin açık ve makul bir takvimi ve uygulama planı var mı?
   - Teklif edilen bütçe, faaliyetlere uygun mu ve makul mu?
   - Kurumun mevcut bilgileri ve telekomünikasyon sistemleri teklif edilen yükseltmeler için uygun mu?

4. **Geçmiş Performans:**
   - Başvuru sahibi; bilinçli bilimsel ve araştırma etikleri, dürüstlük, bilgi güvenliği, veri yönetişimi, bilinçli teknoloji, kurumsal uyum, çift kullanımlı teknoloji bilgisi ve ihracat denetimleriyle ilgili konularla ilgili yüksek kaliteli araştırma kaydına sahip mi?

5. **Bütçe:**
   - Başvuru sahibi, teklifteki etkinlikleri ve görevleri proje bütçesine eşitledi mi?
   - Proje bütçesi, teklif edilen performans döneminde teklif kapsamındaki görevleri gerçekleştirmek için yeterli mi?
   - Bütçe kalemleri, doğrudan ve dolaylı maliyetler arasında makul ve olağan maliyetleri ve uygun bir bakiyeyi temsil ediyor mu?

Lütfen CySIG'lerin rekabetçi hibeler olduğunu ve aynı kişiler veya kurumlar için tekrar eden finansmanın sınırlı olduğunu unutmayın.

Ek Bilgiler

- CySIG yarışması hakkında daha ayrıntılı bilgi için lütfen şurayı ziyaret edin:https://www.crdfglobal.org/docs/default-document-library/cysig-faq.docx
- Genel CRDF Global hibe politikaları hakkında ayrıntılı bilgi için lütfen şurayı ziyaret edin: http://www .crdfglobal .org/grants -and-grantees/faqs+
- CySIG yarışması hakkında daha fazla bilgi için lütfen CRDF Global ile cysig@crdfglobal.org adresinden iletişime geçin

Nasıl başvurulur?

- Tamamlanmış başvurunuzu, bütçeyi ve istenen belgeleri**cysig@crdfglobal.org**. adresine gönderin.

CRDF GLOBAL POLİTİKALARI

Eser Hırsızlığıyla Mücadele: CRDF Global eser hırsızlığının var olduğu bir başvuruya finansman sağlamayacaktır. CRDF Global'e gönderilen tüm finansman başvuruları, yayımlanmış araştırmalar, kitaplar, konferans özetleri ve web siteleri gibi farklı kaynaklarla eser hırsızlığı yönünden detaylı incelemeden geçirilecektir. Eser hırsızlığı tespit edildiğinde finansman fırsatıyla ilgili olan CRDF Global dahilindeki program, atılacak özel adımı belirleyecektir. Atılacak adımlar bunlarla sınırlı olmamak üzere şöyledir: a) başvuru sahibine eser hırsızlığının bulunduğuna dair bilgi vermek; b) başvuru sahibini finansman fırsatından çıkarmak; c) başvuru sahibinin kurumunu bilgilendirmek; d) inceleyenleri bilgilendirmek; e) CRDF Global ile finansman fırsatı hakkında iş birliği yapan kurumları bilgilendirmek; f) başvuru sahibinin gelecekteki finansman fırsatlarına katılmasını engellemek.

CySIG Proje Örnekleri

***CySIG'lerin eğitim veya çalıştay etkinliklerini finanse etmeyeceğini lütfen unutmayın. CySIG'ler sadece temin edilen siber güvenlik ekipmanının kullanımı veya siber güvenlik prosedürlerinin anlaşılmasıyla ilgili eğitimleri finanse edilecektir.**

Bilgi ve telekomünikasyon sistemlerinin (ITS) siber güvenliğini ve bilgi etkinliği nesnelerinin (OIA) fiziksel güvenliğini korumak için kullanılacak ekipman örnekleri aşağıdakileri içerir:

1. Bilgi etkinliği nesnelerine (OIA) ve/veya sunucu odalarına erişim kontrolü sistemleri (örn. kameralar, elektronik dijital kilitler)
2. Web Uygulama Koruma Ekranı (WAF)
3. Güvenlik duvarı (ağ güvenlik duvarı)
4. Saldırı Engelleme Sistemleri (IPS)
5. Güvenlik Bilgisi ve Güvenlik Etkinliği Yönetimi (SIEM) sistemleri (örneğin, McAfeeEnterprise Security Manager)
6. Anti-virüs yazılımı

***Yukarıdaki listenin, uygun projelerin bir listesi olmadığına lütfen dikkat edin. CRDF Global, başvuru sahiplerini, potansiyel bir konunun uygunluğu hakkında soru veya endişeleri olması halindecysig@crdfglobal.orgadresinden iletişime geçmeye teşvik eder.**

Siber güvenliği oluşturma veya iyileştirmeyle ilgili etkinlik örnekleri ve prosedürleri:

1. BT yönetim süreçlerinin denetimi ve geliştirilmesi (örneğin, COBIT 5 metodolojisine göre)
2. Buna bağlı olarak bilgi güvenliği denetimi ve öneri geliştirme (örneğin, ISO 270XX standartlar paketine göre)
3. Bilgi güvenliği olayı yönetim prosedürlerinin geliştirilmesi ve uygulanması (politikalar)
4. Bilgi sistemlerinde değişim yönetimi için prosedürlerin (politikalar) geliştirilmesi ve uygulanması
5. Bilgi kaynakları kontrol erişimi prosedürlerinin (politikalar) geliştirilmesi ve uygulanması
6. Uluslararası gereklilikler uyarınca bilgi güvenliği departmanı ekibinin eğitim ve sertifikasyonu (örneğin, ISACA programlarından biriyle sertifikasyon)