Kibertəhlükəsizliyin təkmilləşdirilməsi üzrə qrant (CySIG)

İNGİLİS DİLİ

Hədəf:	**Akademik və elmi-tədqiqat müəssisələrində informasiya və kibertəhlükəsizlik səviyyəsinin yüksəldilməsi** Qrantlar akademik və elmi-tədqiqat institutlarının kompüter sistemlərinə icazəsiz giriş yolu ilə həssas elmi-tədqiqat və lahiyələndirmə məlumatlarını oğurlamaq istəyən hiyləgər qurumların törətdiyi kibertəhlükələrdən müdafiə olunma və bu təhlükələrə cavab vermə imkanlarını artırmaq üçün nəzərdə tutulub.
Müsabiqənin açılışı:	**Gürcüstan: 2022-ci il, 9 iyun** **Ermənistan: 2022-ci il, 29 sentyabr** **Türkiyə, Azərbaycan, Bolqarıstan: 2022-ci il, 23 sentyabr**
Son müraciət tarixi:	**Gürcüstan: 2022-ci il, 22 iyul** **Ermənistan, Türkiyə, Azərbaycan, Bolqarıstan:** 2022-ci il, 7 noyabr
Uyğunluq şərtləri:	Aşağıdakı mövzular üzrə qabaqcıl elmi-tədqiqat sahələrinə malik akademik və elmi-tədqiqat institutları müraciət edə bilər: • Elm və texnologiya • Mühəndislik (bütün növləri) • Sosial elmlər • Tibb • Kompüter texnologiyaları • Naviqasiya və aviasiya radioelektronikası • Hərəkətverici sistemlər • Telekommunikasiyalar və informasiya təhlükəsizliyi • Elektronika Uyğun ölkələr - Gürcüstan, Ermənistan, Türkiyə, Azərbaycan, Bolqarıstan
Müraciət qaydası:	cysig@crdfglobal.org e-poçt ünvanına elektron məktub göndərməklə
Ümumi sahə:	Kibertəhlükəsizlik
Mükafat məbləği:	30.000 ABŞ dolları
Mükafat müddəti:	Bir il
Elan və müraciət:	http://www.crdfglobal.org/ (bax“Cari maliyyələşdirmə imkanları”)

Ümumi təsvir

Seminar vasitəsilə uğurlu kibertəhlükəsizlik proqramı üzrə bilik, bacarıq və alətlərin əldə edilməsi tövsiyə olunan nəzarət və mühafizə tədbirlərinin həyata keçirilməsi üçün imkanların artırılması ilə optimallaşdırılmalıdır. "CRDF Global" təşkilatı informasiya və kibertəhlükəsizliyi təkmilləşdirən avadanlıq - və müvafiq quraşdırma xərcləri, materiallar və təchizatlar üçün seminarlardan birinə nümayəndələr göndərmiş elmi-tədqiqat institutlarına və universitetlərə qrantlar verəcək.

- Kibertəhlükəsizliyin təkmilləşdirilməsi üzrə qrantlar uyğunluq meyarlarına cavab verən akademik və elmi-tədqiqat institutlarında informasiya və kibertəhlükəsizliyin səviyyəsini yüksəltmək üçün "CRDF Global" təşkilatının sponsorluğu ilə verilən qrantlardır.
- CySIG-lər hər birinin məbləği 30 000 ABŞ dolları olan birdəfəlik və bir illik qrantlardır.
- Qrantlar "CRDF Global" təşkilatının vasitəçiliyi ilə verilir.

Uyğunluq şərtləri

Kiberoğurluqla bağlı proqram seminarlarından birinə öz nümayəndəsini göndərmiş istənilən elmi-tədqiqat və ya ali təhsil müəssisəsi müraciət edə bilər. Ərizəçilər ayrıca qurum və ya konsorsium kimi müraciət edə bilərlər. Aparıcı tədqiqatçının və elmi-tədqiqat üzrə qrant komandasının digər üzvlərinin seminarda iştirak etməsinə ehtiyac yoxdur. Bu müsabiqə üzrə müraciətlərin nəzərdən keçirilməsi üçün institusional təsdiq tələb olunur.

CySIG-lər aşağıda sadalanan bütün meyarlara cavab verən ərizəçilər - dövlət və özəl akademik və elmi-tədqiqat institutları üçün əlçatandır:

- Yuxarıda sadalanan mövzular üzrə fəal elmi-tədqiqat. Digər elmi-tədqiqat mövzuları ilə məşğul olan namizədlər lazımi əsaslandırma ilə müraciət edə bilərlər.
- Qabaqcıl təhlükəsizlik təkmilləşdirmələri üçün uyğun olan mövcud İT infrastrukturu
- Uyğun ölkələrdən hər hansı birində şəxsən fiziki mövcudluq
- İnstitusional təsdiq

Hər bir təklif müstəqil şəkildə qiymətləndirilir və buna görə də bu proqrama təqdim edilən digər təkliflərin bir hissəsini təşkil etməməli və onların uğurundan asılı olmamalıdır.

Hər bir ərizəçi-müəssisə - hər bir elmi-tədqiqat şöbəsi üçün bu qrant müsabiqəsinə yalnız bir ərizə təqdim edə bilər.

"CRDF Global" təşkilatı hər hansı fiziki şəxsin və ya qurumun öz proqramlarında iştirakını məhdudlaşdırmaq hüququnu özündə saxlayır. "CRDF Global" təşkilatı ixraca nəzarət və xarici vətəndaşların və ya qurumların onun fəaliyyətlərində iştirakı ilə bağlı ABŞ-ın bütün qanun və normalarına riayət edir. "CRDF Global" təşkilatının siyasəti ABŞ Hökümətinin müvafiq icazəsi olmadan, ABŞ tərəfindən məhdudlaşdırılmış qurumlar ilə heç bir sövdələşmənin aparılmamasından ibarətdir.

Tələb olunan müraciət materialları

Bütün ərizəçilər məlumatları və köməkçi sənədləri MS Word sənəd şablonu kimi endirilə bilən "CRDFG Global" təşkilatının *Elmi dairələrdə kiber oğurluğa qarşı cavab tədbirləri ilə bağlı qrant müraciətinin yoxlama siyahısına* daxil etməlidirlər. Müraciət materialları və elmi-tədqiqat məhsulları ingilis dilində və ya standartlaşdırılmış milli dildə təqdim oluna bilər. Müraciət və mətndəki elementlər birintervallı beş səhifə ilə məhdudlaşdırılmalıdır. Əlavə köməkçi sənədlər və elektron cədvəllər bu mətnə əlavə edilə və ya ayrıca sənədlər kimi göndərilə bilər.

Doldurulmuş CySIG ərizə forması və köməkçi sənədlər, o cümlədən:

- **Doldurulmuş CySIG büdcə forması*** *(məcburi)*
- Ərizəçinin layihə komandasının hər bir üzvünün **tərcümeyi halı (CV)** — hər biri maksimum 3 səhifə, Word və ya PDF formatında - müraciət edən qurumun informasiya təhlükəsizliyi üzrə baş mütəxəssisinin (CISO) göstərilmiş əlaqə telefonu və e-poçtu *(məcburi)*
- **Kibertəhlükəsizliyin daxili və ya xarici zəif tərəflərinin qiymətləndirilməsi** — hesabat və ya daxili sənəd şəklində *(məcburi)*
- **İnstitusional Təsdiq Məktubu** *(məcburi) *uyğun olmaq üçün qurumunuzun rəhbərliyinin sənədində bu qranta müraciət etmək və onu həyata keçirmək üçün qurumunuz tərəfindən dəstəkləndiyiniz bildirilməlidir. Sənəd rəhbərlik tərəfindən* ***imzalanmalıdır.***
- Aparıcı tədqiqatçının və ya layihə komandasının işi ilə tanış olan müstəqil fiziki şəxslərin **istinadlar siyahısı** təqdim edilməlidir.

Bütün müraciət materialları "CRDF Global" təşkilatı tərəfindən verilmiş formalardan istifadə etməklə, Word və ya PDF fayllarında əlavələr kimi təqdim edilməlidir.

Qrantın əhatə dairəsi

*CySIG qrantları informasiya və kibertəhlükəsizliyi təkmilləşdirən **avadanlıq (və müvafiq quraşdırma xərcləri), materiallar və təchizatlar** üçün nəzərdə tutulub. **Ərizəçinin layihə komandası üzvlərinin əməkhaqqılarının hazırkı qrant maliyyələşməsi əsasında ödənilməsinə icazə verilmir.**

Yolverilən xərclər
"CRDF Global" təşkilatı tərəfindən birbaşa olaraq, ilk əlaqədar şəxsin çalışdığı quruma verilən qrantın maksimum ümumi dəyəri 30.000 ABŞ dolları təşkil edir. **Qrant verildiyi halda, "CRDF Global" təşkilatı tərəfindən maliyyələşməni tələb edən büdcələrə düzəlişlər edilə bilər.

Yolverilən məsrəflər
- Avadanlıq, təchizatlar və xidmətlər (ATX),
- Digər birbaşa xərclər (ATX-nin quraşdırılması və ona texniki xidmət ilə əlaqədar baş verə biləcək digər əlavə məsrəflər)

Təklifin qiymətləndirilməsi üzrə meyarlar
Bütün təkliflər aşağıdakı meyarlar əsasında qiymətləndiriləcək:

1. **Kibertəhlükəsizliyin aktuallığı və təsiri:**
   - Təklif olunan təhlükəsizlik təkmilləşdirmələri hansılardır və onlar qurum daxilində təhlükəsizliyi necə yaxşılaşdıracaq?
   - Ərizəçi onun informasiya resurslarına yönəlmiş kiberhücum cəhdlərinin presedentlərini neçə dəfə müşahidə edib?
   - Əsas informasiya resurslarına uğurlu kiberhücumun/kiberoğurluğun maksimum mümkün nəticələri hansılardır?

2. **Davamlılıq və öhdəçilik:**

- Ərizəçinin təşkilatı hər hansı pulsuz maliyyə, maddi-texniki və/və ya kadr dəstəyi təklif etməklə layihə öhdəçiliyini nümayiş etdirirmi?
- Ərizəçinin aydın monitorinq/qiymətləndirmə strategiyası və ya planı varmı? Ərizəçi tələb olunan təkmilləşdirmənin nəzərdə tutulan təsirə malik olduğunu necə biləcək?
- Müraciət edən qurum uzunmüddətli maliyyə dəstəyi və ya ətraflı texniki xidmət planı təklif edirmi?

3. **Aydınlıq, əlverişlilik və təfərrüat:**
   - Layihənin həyata keçirilməsi üçün aydın və ağlabatan vaxt qrafiki və plan mövcuddurmu?
   - Təklif olunan büdcə fəaliyyətlər üçün uyğun və ağlabatandırmı?
   - Qurumun cari informasiya və telekommunikasiya sistemi təklif olunan təkmilləşdirmələrə uyğundurmu?

4. **Keçmiş fəaliyyət:**
   - Ərizəçi məsul elmi və elmi-tədqiqat etikası, bütövlük, informasiya təhlükəsizliyi, məlumatların idarə edilməsi, məsul texnologiya, institusional uyğunluq ilə əlaqədar məsələlər üzrə yüksək keyfiyyətli elmi-tədqiqat tarixçəsinə, habelə ikitəyinatlı texnologiya və ixrac nəzarətlərinə dair biliklərə malikdirmi?

5. **Büdcə:**
   - Ərizəçi təklifdəki fəaliyyət və tapşırıqları layihə büdcəsinə uyğun olaraq planlaşdırıbmı?
   - Layihənin büdcəsi təklif olunan icra müddətində təklifdəki tapşırıqları yerinə yetirmək üçün kifayətdirmi?
   - Büdcə maddələri ağlabatan və adi xərcləri, habelə birbaşa və dolayı xərclər arasında lazımi tarazlığı göstərirmi?

Nəzərə alın ki, CySIG-lər rəqabətqabiliyyətli qrantlardır və eyni fiziki şəxslər və ya qurumlar üçün təkrar maliyyələşdirmə məhduddur.

Əlavə məlumat

- CySIG müsabiqəsi ilə bağlı ətraflı məlumat üçün xahiş olunur,https://www.crdfglobal.org/docs/default-document-library/cysig-faq.docxveb-saytına daxil olun.
- "CRDF Global" təşkilatının ümumi qrant siyasətlərinə dair ətraflı məlumat üçün xahiş olunur,http://www.crdfglobal.org/grants-and-grantees/faqs+veb-saytına daxil olun.
- CySIG müsabiqəsi ilə bağlı əlavə suallar üçün cysig@crdfglobal.org e-poçt ünvanında "CRDF Global" təşkilatı ilə əlaqə saxlayın.

Müraciət qaydası

- Doldurulmuş ərizə, büdcə və tələb olunan sənədləri **cysig@crdfglobal.org**e-poçt ünvanına göndərin.

"CRDF GLOBAL" TƏŞKİLATININ SİYASƏTLƏRİ

Antiplagiat mexanizmləri: "CRDF Global" təşkilatı plagiatın mövcud olduğu müraciət üçün maliyyələşmə təmin etməyəcək. "CRDF Global" təşkilatına maliyyələşdirmə ilə bağlı təqdim edilən bütün müraciətlər nəşr edilmiş elmi-tədqiqat məqalələri, kitablar, konfrans tezisləri və veb-saytlar daxil olmaqla, çoxlu sayda mənbələrə qarşı plagiat üçün hərtərəfli yoxlanılacaq. Plagiat aşkar edildikdə, "CRDF Global" təşkilatının daxilində maliyyələşdirmə imkanlarına nəzarət edən proqram həyata keçiriləcək konkret tədbirləri təyin edəcək. Həyata keçirilən tədbirlərə bunlar daxildir, lakin bunlarla məhdudlaşmır a) plagiatın aşkar edildiyi barədə ərizəçiyə məlumat vermək; b) ərizəçini maliyyələşdirmə imkanından məhrum etmək; c) ərizəçinin qurumunu məlumatlandırmaq; d) icmalçıları məlumatlandırmaq; e) "CRDF Global" təşkilatı ilə əməkdaşlıq edən təşkilatları maliyyələşdirmə imkanları barədə məlumatlandırmaq; f) ərizəçinin gələcək maliyyələşdirmə imkanlarında iştirakına qadağa qoymaq.

CySIG QRANTI ÜZRƏ LAYİHƏ NÜMUNƏLƏRİ

*** Nəzərə alın ki, CySIG qrantları təlim və ya seminar tədbirlərini maliyyələşdirməyəcək. CySIG qrantları yalnız satın alınmış kibertəhlükəsizlik avadanlığından istifadə və ya kibertəhlükəsizlik prosedurlarının öyrənilməsi ilə bağlı təlimləri maliyyələşdirəcək.**

İnformasiya və telekommunikasiya sistemlərinin (ITS) kibertəhlükəsizliyini və informasiya fəaliyyəti obyektlərinin (OIA) fiziki təhlükəsizliyini təmin etmək üçün istifadə ediləcək avadanlığın nümunələrinə aşağıdakılar daxildir:

1. İnformasiya fəaliyyəti obyektlərinə (İFO) və/və ya server otaqlarına (məsələn, kameralar, elektron rəqəmsal kilidlər) girişə nəzarət sistemləri
2. Veb-tətbiqi mühafizə ekranı (WAF)
3. Şəbəkə mühafizəsi (şəbəkələrarası ekran)
4. Soxulmanın qarşısını alan sistemlər (IPS)
5. Təhlükəsizlik informasiyası və təhlükəsizlik hadisələrini idarəetmə (SIEM) sistemləri (məsələn, McAfeeEnterprise Security Manager)
6. Antivirus proqramı

***Nəzərə alın ki, yuxarıda göstərilənlər uyğun layihələrin tam siyahısı deyil. "CRDF Global" təşkilatı ərizəçilərdən potensial mövzunun uyğunluğu ilə bağlı hər hansı suallar və ya narahatlıqlar halında, cysig@crdfglobal.org e-poçt ünvanı ilə əlaqə saxlamağı xahiş edir.**

Kibertəhlükəsizliyin yaradılması və ya gücləndirilməsi üzrə fəaliyyət və prosedurların nümunələri:

1. İT idarəetmə proseslərinin auditi və işlənib hazırlanması (məsələn, COBIT 5 metodologiyası əsasında)
2. İnformasiya təhlükəsizliyinin auditi və bu audit əsasında tövsiyələrin hazırlanması (məsələn, ISO 270XX standartlar paketi əsasında)
3. İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi prosedurlarının (siyasətləri) hazırlanması və həyata keçirilməsi
4. İnformasiya sistemlərində dəyişikliklərin idarə edilməsi üzrə prosedurların (siyasətlərin) işlənib hazırlanması və həyata keçirilməsi
5. İnformasiya resurslarına giriş üzrə nəzarət prosedurlarının (siyasətlərinin) işlənib hazırlanması və həyata keçirilməsi
6. Beynəlxalq tələblərə uyğun olaraq, informasiya təhlükəsizliyi şöbəsinin işçi heyətinə təlim keçirilməsi və onların sertifikatlaşdırılması (məsələn, ISACA proqramlarından biri əsasında sertifikatlaşdırma).