



Ulusal Akademik Ağ Güvenlik Birimi

Ulak-Csirt



İçerik

- Güvenlik Birimleri : CERT-CSIRT
- Çalışma Alanları
- UlakNet ' te ihtiyaç
- Organizasyon ve üyeler
- Organizasyonel yapı
- TI ve FIRST akreditasyonu



Csirt-Cert

- **Computer Emergency Response Team (CERT*)**
- **Computer Security Incident Response Team (CSIRT)**

*CERT ismi Carnegie Mellon Üniversitesi ait tescilli markadır



Görev Alanları

- Olay müdahale
- Uyarı
- Açıklarla mücadele
- Anonslar
- IDS
- Bilgi kaynaklığı
- Risk Analizi
- Koordinasyon
- İş devam planlaması
- Güvenlik Danışmanlığı
- Bilinçlendirme
- Eğitim-Çalıştay
- Ürün Değerlendirme
- Sızma Testi
- Teknoloji İzleme
- Güvenlik uygulamaları konfigürasyonu ve çalıştırılması

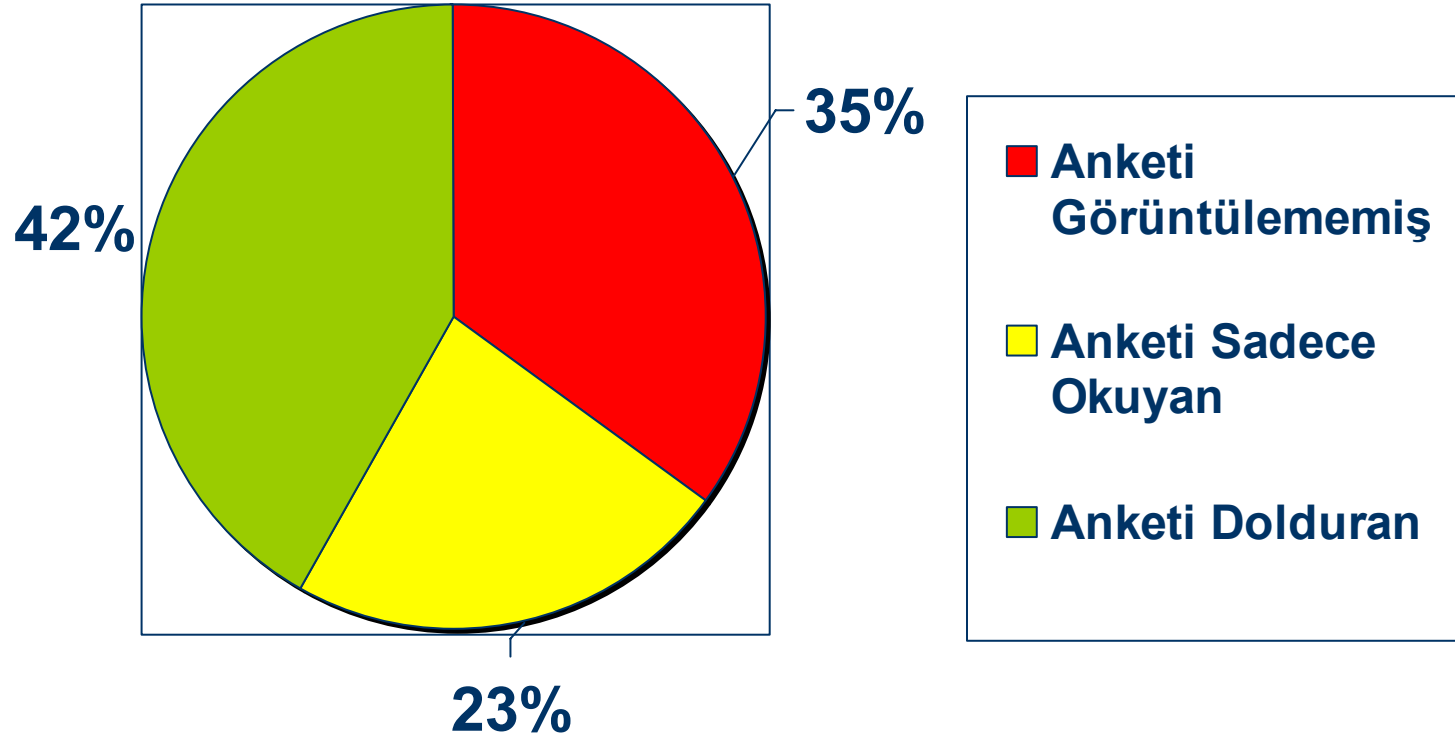


UlakNet İhtiyaçları

- Üniversite ağ yöneticileri ile iletişim sorunu
- Güvenlik bilinci eksikliği
- İnsan gücü eksikliği
- Yabancı dil problemi



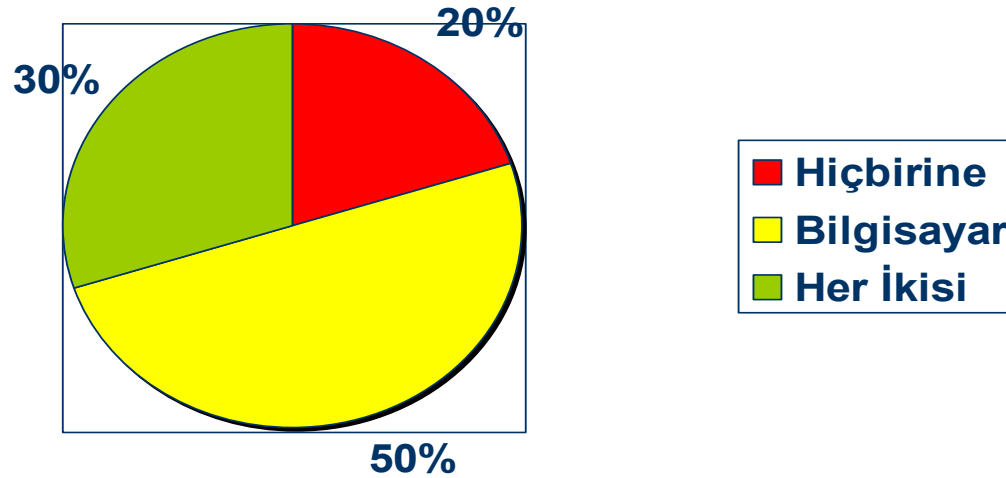
Ağ yöneticileri ile iletişim





Kullanıcı Tespit

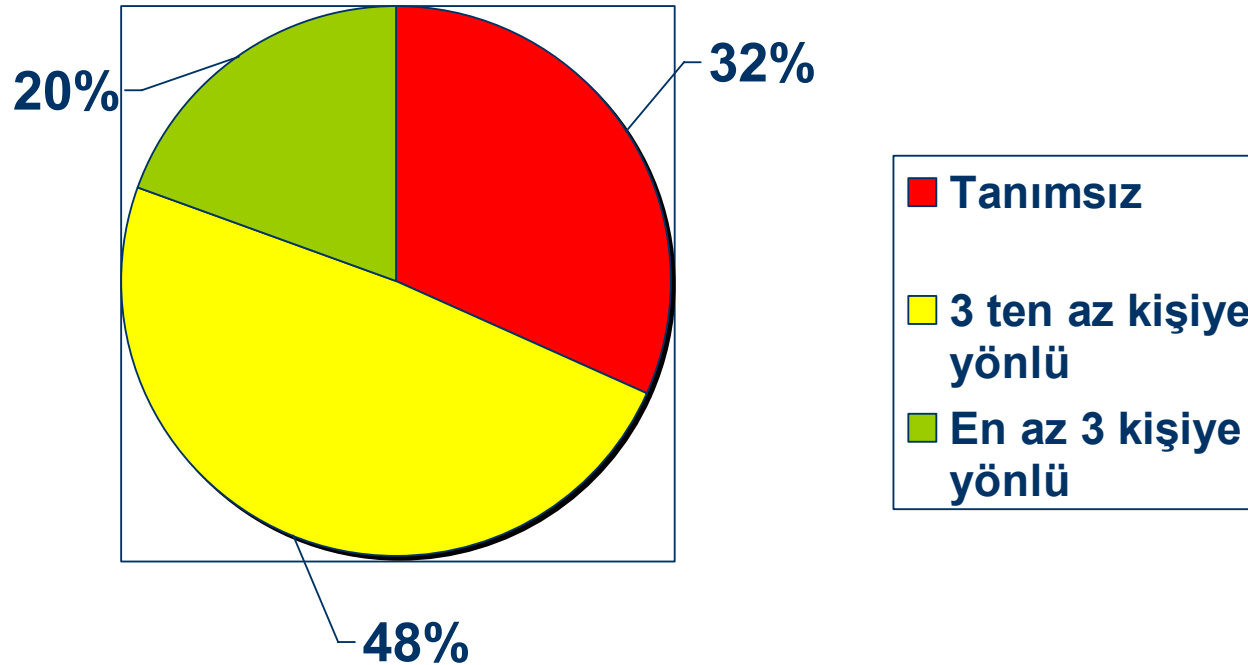
İp ve zaman bilgisinden yola çıkarak bilgisayar ve kullanıcıya ulaşım:





Mevcut Durum

Abuse aliasının tanımlanması ve yönlendirildiği kişi sayısı:





Ulak-Csirt

Ulusal Akademik Ağ
Bilgisayar Olaylarına Müdahale Birimi (BOMB)

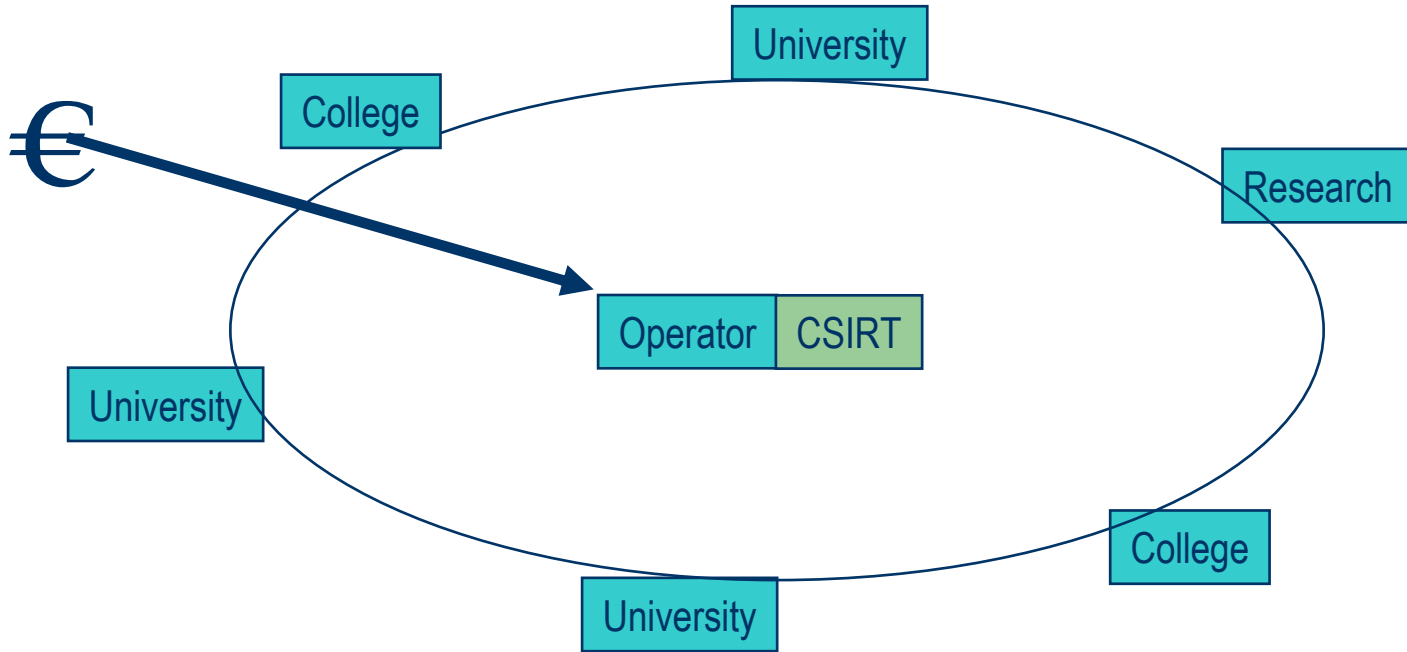
<http://csirt.ulakbim.gov.tr>

csirt@ulakbim.gov.tr



Örnek Oluşum – Dağıtık Çalışma

Ulusal Akademik Ağ



Terena Csirt Çalıştayı

Murat SOYSAL, AB2006



TRANSITS



Birim Elemanları

Ulak-Teknik listesi ve toplantılarda güvenlik konularına ilgi

Murat SOYSAL

- *ULAKBİM*

Enis Karaaslan

- *Ege Üniversitesi*

Gökhan Eryol

- *O.D.T.Ü*

Hüseyin Yüce

- *Marmara Üniversitesi*



Amaçlar

- Bilgi güvenliği bilinci sağlamak
- Ağı güvenli hale getirmek
- Saldırgan tespitinin koordinasyonu
- Güncel açıkları ve çözümlerini bildirmek
- Türkçe doküman sağlamak
- Ağın saygınlığını dış dünyada artırmak



Sorumluluk Paylaşımı

- Olay bildirim formu işletimi (trouble ticket)
 - Her saldırı için bir giriş yapılması
 - Hedefini bilgilendirme
 - Kaynak ağ yöneticisinden talep
 - Sonuç aşamasına kadar koordinasyon
- Türkçe doküman organizasyonu
 - Mevcut dokümanların toparlanması
 - Eksik alanların belirlenmesi
 - Çeviri ya da üretim koordinasyonu
- Güncel açıkların izlenmesi
 - Web sayfasında anonslar yayınlanması
 - Türkçe uyarılar sağlanması
- Hukuki konularda takip ve bilgilendirme
 - Mevcut yasalar
 - Ulakbim ve uçların hukuki sorumlulukları



Umutlar

- Kara listelerden ve kara delik sıfatından uzaklaşma
- Uçlarla tam koordinasyon
- Güvenlik bilinçli ağ
- Devlet organizasyonlarına öncü olmak



Sonu

- Koordinasyon birimi, destek Őart
- GvenliĐe nem vermek
- Gven-Beklenti-Yaptırım



Sorular - Yorumlar