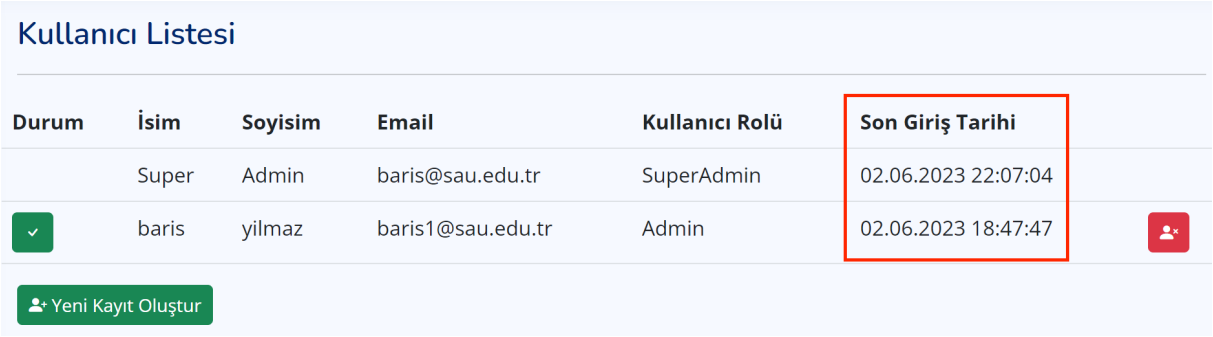
UTM DASHBOARD

Projede son düzenlemelerin üzerine öncelikle SuperAdmin kullanıcısının Kullanıcı Listesi sayfasında kullanıcıların son oturum açma tarihlerini görebilmesini sağladık.



Kullanıcının ve SuperAdmin'in yaptığı işlemlerin loglarını tuttuk ve bu logları loglar sayfasında Kullanıcı Logları adında bir tabloda gösterdik. Yöneticinin işlem yaptığı durumlarda ise durum olarak Yönetici badge'i gözükmektedir.

Yalnızca SuperAdmin kullanıcılarının veritabanı indirebilmesi için SuperAdmin paneline Veritabanı İşlemleri sayfası ekledik ve bu sayfada veritabanı yedeğini alabilmektedir. Ayrıca yedeği alan kullanıcıların logları da tutulmakta ve gözükmektedir.

Veritabanı İşlemleri

Oluşturan Kişi	Tarih
baris@sau.edu.tr	18-05-2023 01:19:56
baris@sau.edu.tr	18-05-2023 01:31:39
baris@sau.edu.tr	18-05-2023 01:49:26
baris@sau.edu.tr	02-06-2023 22:14:51

Veritabanı Yedeği İndir

Malware için daha önceden oluşturduğumuz daire grafiğinde loğların mesajları görüntülenemediğinden dolayı Malware sayfasına ek olarak kayıtların tablosunu da ekledik.

Malwares

5 kayıt görüntüle

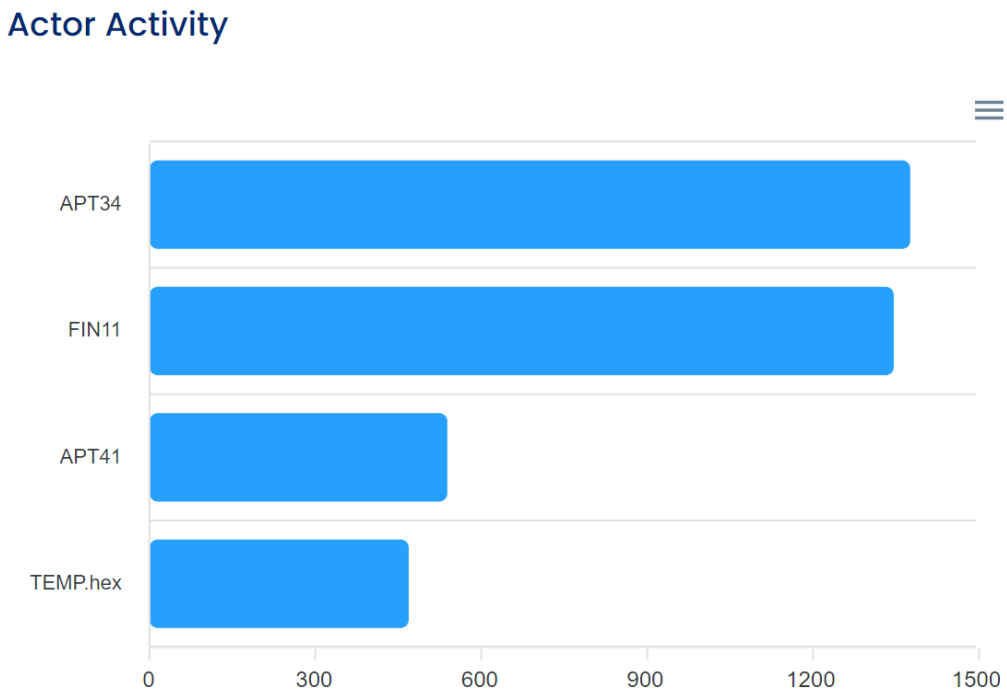
Arama...

Tarih	Cihaz	Malware Tipi	Mesaj
2022-09-01 00:11:16	7UT85	Rootkit	Sayaç sistemine yerleşen bir rootkit, kullanıcı verilerini çalmaya çalışarak cihazların güvenliğini riske attı.
2023-05-02 03:30:14	6MD85	Worm	Sayaç sistemine bulaşan bir worm, kullanıcı verilerini çalmaya ve kötü amaçlar için kullanmaya çalıştı.
2023-10-26 19:08:28	7UT85	Rootkit	Sayaç sistemine yerleşen bir rootkit, kullanıcı verilerini çalmaya çalışarak cihazların güvenliğini riske attı.
2023-06-05 07:12:51	6MD85	Spyware	Sayaç kullanıcı verilerini toplayan bir spyware, kötü amaçlar için kullanılmak üzere harici bir sunucuya gönderdiği tespit edildi.
2022-09-22 16:55:01	6MD85	Adware	Sayaç kullanıcı arayüzünde istenmeyen reklam içerikleri gösteren bir adware tespit edildi ve kaldırıldı.

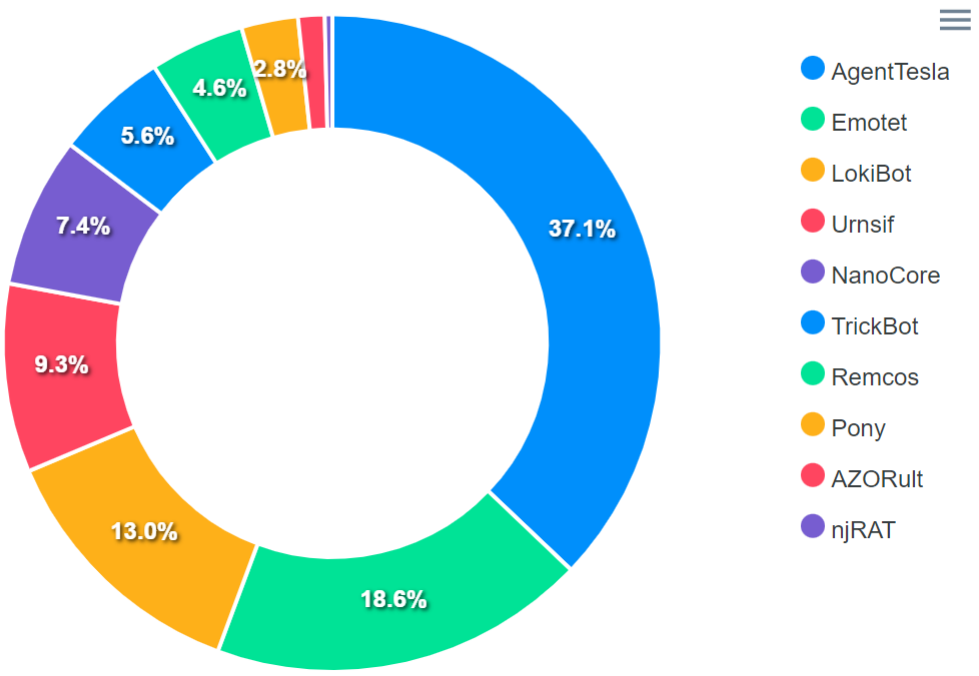
399 kayıttan 1 ile 5 arası gösteriliyor

1 2 3 4 5 6 7 ... 80 ›

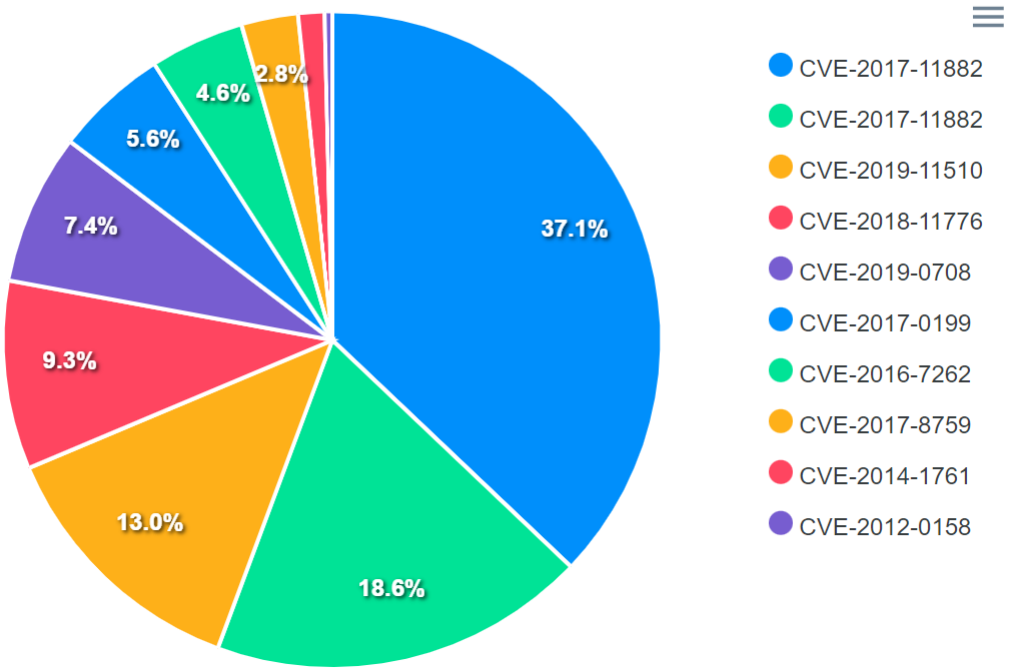
Ayrıca Dashboard'da daha gerçekçi görünmesi açısından Threat Intelligence ve Malware Analysis modüllerini de ekledik. Threat Intelligence sayfasındaki grafikler şu şekildedir:



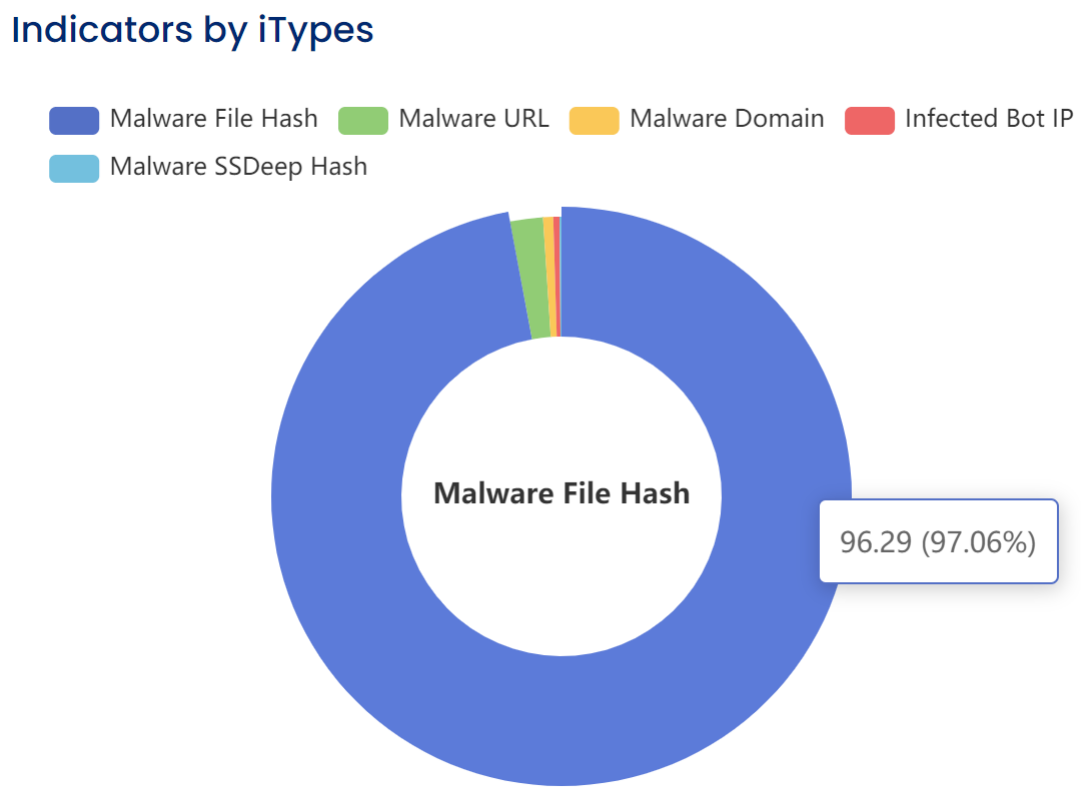
Most Active Malware TOP 10

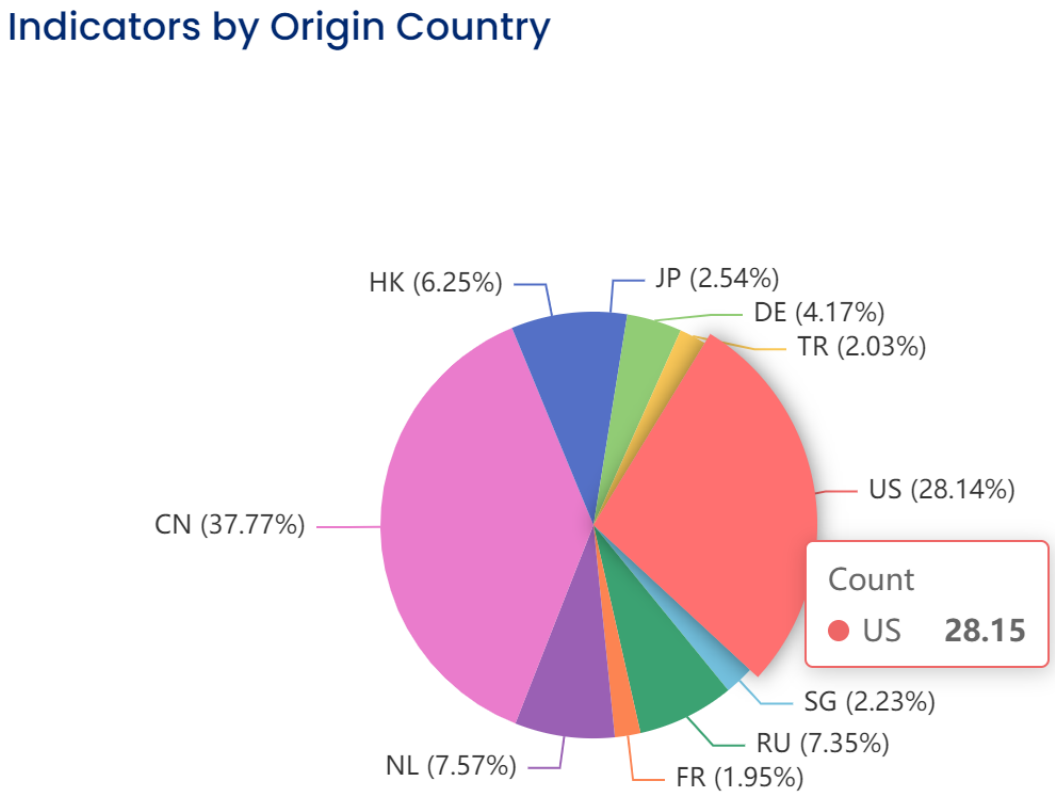


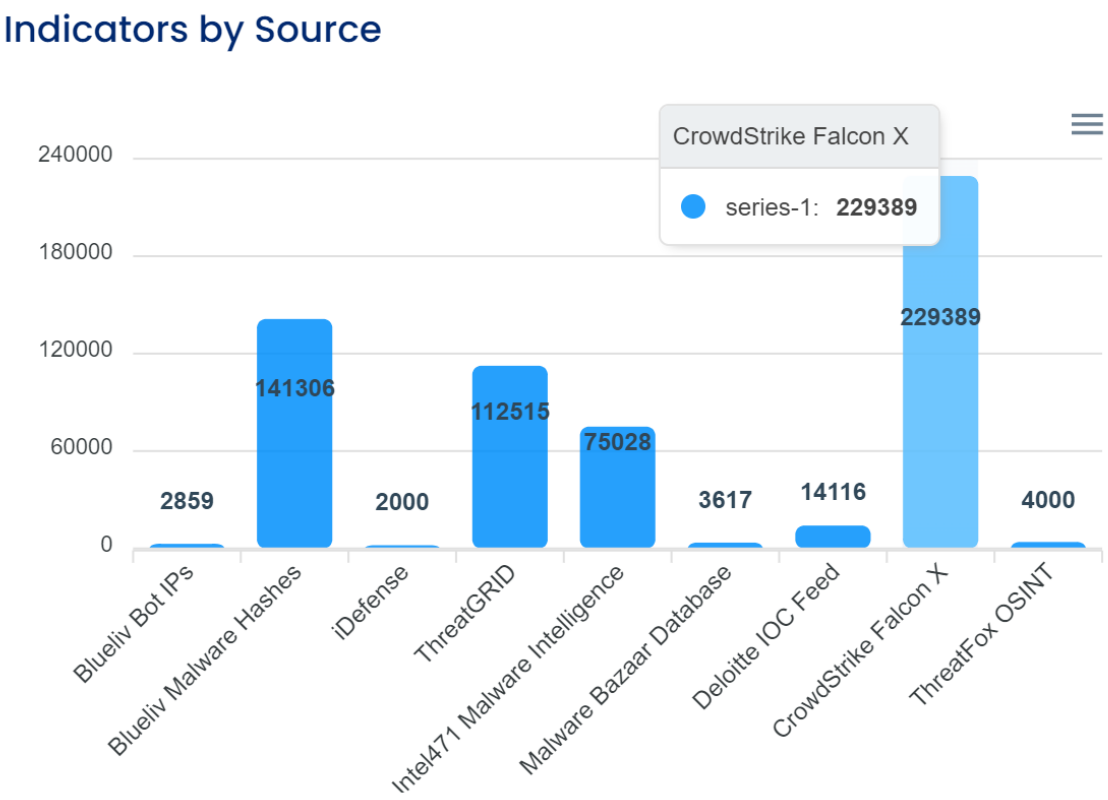
Most Active Vulnerabilities TOP 10



Malware Analysis sayfasındaki grafikler ise şu şekildedir:



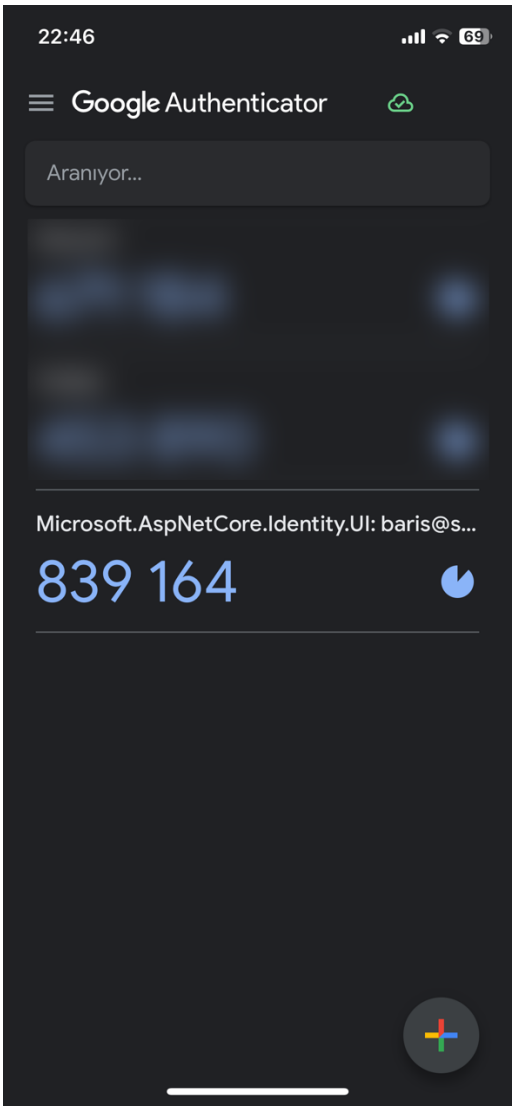




Ayrıca 2 adımlı doğrulama özelliğini ekledik ve sistemi daha güvenilir hale getirdik. Kullanıcı profilinden kurulum aşağıdaki şekilde görünmektedir:

Kurulum yapıldığında ise 5 adet saklanması gereken kurtarma kodu verilmektedir, kullanıcı girişte yalnızca eğer authenticator kurulu cihaza erişimi yoksa bu kodlardan biriyle veya kurulum yapılan uygulamadaki doğrulama koduyla giriş yapabilmektedir. Doğrulama yapılmadığı taktirde giriş mümkün değildir. Kullanıcı kurulumu yaptıktan sonra giriş yaptığında ise aşağıdaki şekilde doğrulama kodu sorulmaktadır:

Örneğin Google Authenticator uygulamasından kurulum yapıldığı varsayılırsa, doğrulama kodu şu şekilde görünmektedir:



Bunlara ek olarak güvenliği daha da sağlamlaştırmak için her kullanıcının 2 adımlı doğrulamayı etkinleştirilmesi zorunlu kılındı ve eğer kullanıcı doğrulamayı etkinleştirmediyse giriş yaptığında otomatik olarak 2 adımlı doğrulama kurulum ekranına yönlendirilmektedir ve bu kurulumu yapmadan herhangi bir sayfaya erişememektedir. Bu işlemi de bir middleware ekleyerek yaptık. (İşlemleri gerçekleştirmek için oluşturduğumuz sınıfın ismi "Authenticator2faResourceFilter")

```
builder.Services.AddMvc(o =>
{
    o.Filters.Add(typeof(ChangePasswordResourceFilter));
    o.Filters.Add(typeof(AuthenticatorResourceFilter2fa));
});
```

Tasarımda hazırlamış olduğumuz güvenli yazılım geliştirme ilkelerine ait checklistte ise son rapordan bu yana gelmiş olduğumuz durum aşağıdadır.

✓ Yüksek güvenlik gerektiren işlemlerde tek bir koşula bağlı olarak izin verilmemeli
✓ Sistem ve yazılım içerisindeki modüller arasında yalıtım sağlanmalı
✓ Sunucuda yapılan girdi doğrulama hataları, isteğin reddi ile sonuçlanmalı ve iz kaydı oluşturulmalıdır.
✓ Yetkisiz bir kullanıcının yazılım ortamından veri alabileceği, girebileceği veya yetkisiz işlemlerde bulunabileceği noktalar tespit edilmeli, sınırlandırılmalıdır.
✓ Kullanılan veritabanının dışarıya aktarımı ancak veritabanı yönetim yetkisi olan hesaplarla yapılmalı.
✓ Hassas işlevler gerçekleştirilmeden önce, yeniden kimlik doğrulama, daha güçlü bir mekanizmayla kimlik doğrulama, ikinci faktör veya işlem imzalama gibi yöntemler uygulanmalıdır.
✓ Uygulama, başarısız sistem başlatma, başarısız sonlandırma veya başarısız kapatma gibi işlemlerde güvenli bir duruma geçmelidir.
✓ SQL Injection engellemek için bütün veritabanı sorguları, parametre olarak yapılmalı ve veritabanına erişimde kullanılan dile karşı önleyecek denetimler yapılmalıdır.