

İçerik

CyCastle'a Katılma ve Hesap Oluşturma	3
Hediye 100 Kredimi Nasıl Alabilirim?	6
Nasıl Şirket Oluşturabilirim?	7
ThreatChaser Ürün Anahtarını Nasıl Bulabilirim?	9
ThreatChaser Nasıl Kurulur?	10
1.VMWare Pro Ajan Kurulumu	11
2.VMWare ESXI Kurulumu	16
3.Hyper-V Ajan Kurulumu	20
Web Taraması İçin Nasıl Alan Adı Ekleyebilirim?	28
Alan Adımı Nasıl Doğrulayabilirim?	29
Nasıl Web Taraması Başlatabilirim ?	31
Web Tarama Sonuçlarını Nasıl Görüntüleyebilirim?	33
CVE Zafiyetlerini Nasıl Görüntüleyebilirim ?	34
OVAS Zafiyetlerini Nasıl Görüntüleyebilirim ?	34
Zafiyet Raporumu Nasıl Görüntüleyebilirim?	35
Nasıl Ağ Taraması Başlatabilirim?	36
Ağ Tarama Sonuçlarını Nasıl Görüntüleyebilirim?	38
Siber Tehdit İstihbaratı (CTI) Nasıl Kullanabilirim ?	39
Alan Adlarını Nasıl İzleyebilirim ?	39
Kişisel E-posta Hesaplarını Nasıl İzleyebilirim?	40
Yeni E-posta Hesabı Nasıl Ekleyebilirim ?	40
Nasıl Alt Hesap Ekleyebilirim ?	41
Yeni Kullanıcı Nasıl Ekleyebilirim?	43
Şifremi Nasıl Değiştiririm?	44
Yeni Klasör Nasıl Oluştururum ve İçerisine Nasıl Şirket Ekleyebilirim?	47
Oturum Açma Aktivitelerimi Nasıl Görebilirim ?	48
Destek Kaydı Nasıl Oluşturabilirim ?	49
Beyaz Etiket (White Label) Ayarlarını ve Logonuzu Nasıl Özelleştirebilirsiniz?	52
5651 Loglama ve HotSpot Hizmetini Nasıl Aktif Edebilirim?	54
Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?	58
Watchguard Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?	58
FortiGate Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?	60
Sophos Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?	61
AIMdefense Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?	63

Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?	66
FortiGate API İşlemleri	66
FortiGate Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?	68
ThreatChaser Tarafındaki Ayarlamalar	68
Firewall Tarafındaki Ayarlamalar	71
Sophos Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?	75
ThreatChaser Tarafındaki Ayarlamalar	75
Firewall Tarafındaki Ayarlamalar	77
AIMdefense Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?	84
ThreatChaser Tarafındaki Ayarlamalar	84
Firewall Tarafındaki Ayarlamalar	86
SSL Kontrol Aracı Hizmetini Nasıl Aktif Edebilirim?	92
VPN Hizmetini Nasıl Aktif Edebilirim?	94
İki Faktörlü Doğrulamayı Nasıl Aktif Edebilirim?	96

CyCastle'a Katılma ve Hesap Oluřturma

Hesap oluřturma sayfasına eriřmek iin ařağıdaki baėlantıya tıklayabilirsiniz:

<https://cloud.cycastle.com/register>



Yeni Hesap Oluřtur

Adı Soyadı

E-Posta Adresi



Verify you are human



KAYIT OL

Zaten Hesabınız Var mı?

Hesabınıza Giriř Yapın!

Adınızı ve soyadınızı girerek, robot olmadığınızı doėruladıktan sonra “**Kayıt Ol**” butonuna tıklayınız. Kayıt iřleminin ardından e-posta adresinize bir onay mesajı iletilecektir. Gelen e-postada yer alan “**řifrenizi Oluřturun**” butonuna veya baėlantıya tıklayarak, kayıt srecinizi tamamlayabilirsiniz.

Eėer onay e-postası 24 saat ierisinde tarafınıza ulařmazsa, **support@cycastle.com** adresine e-posta gndererek destek talebinde bulunabilirsiniz.

Hesabınızı başarılı bir şekilde oluşturuldu.

Hesabınıza giriş yapabilmek için şifrenizi oluşturmanız gerekmektedir.

Şifrenizi Oluşturun

Eğer bu hesabı siz oluşturmadıysanız bir şey yapmanıza gerek yoktur.
48 saat içerisinde onaylanmayan hesaplar otomatik silinmektedir.

Saygılarımızla,
CyCastle

Eğer "Şifrenizi Oluşturun" butonuna tıklayamıyorsanız aşağıdaki açık linki
tarayıcınıza kopyalayıp hesabınızı onaylayabilirsiniz.
Tarayıcı Linki: <https://cloud.cycastle.com/activate-user/>

Gerekli bilgileri eksiksiz olarak doldurduktan sonra “**Hesabınızı Güncelleyin**” butonuna tıklayarak hesap oluşturma işlemini tamamlayabilirsiniz.



Hesabınız Başarılı Bir Şekilde Oluşturuldu. Hesabınıza Giriş Yapabilmeniz İçin Şifrenizi ve Diğer Gerekli Bilgileri Doldurarak Kayıt İşlemini Tamamlamanız Gereklemektedir.

Bir Şifre Belirleyin

* Şifre

* Şifreyi Onayla

Hesap Bilgilerinizi Güncelleyin

Şirket Adı

* İsim Soyisim

E-Posta Adresi

* Telefon Numarası

Ülke

Türkiye



Şehir

Adres

Hesabınızı Güncelleyin

Hediye 100 Kredimi Nasıl Alabilirim?

Yönetim Panelinde bulunan **“Bonus Kredinizi Aktif Edin”** butonuna tıklayarak hediye 100 kredinizi almak için başvuru yapabilirsiniz.

Vergi Bilgilerinizi Güncelleyin

❌ **Önemli Bilgilendirme:** Hesabınızı onaylatarak ücretsiz kredinizi kullanabilir ve gelecekte ek kredi satın alma fırsatlarından yararlanabilirsiniz. Onay sürecinde, adınıza fatura düzenlenebilmesi için vergi levhası ve imza sirküleri belgelerinin görsellerini sağlamanızı rica ederiz.

Vergi Levhası

İmza Sirküleri

Sözleşme

Vergi Levhası

Choose File

No file chosen

İmza Sirküleri

Choose File

No file chosen

İmzalı Sözleşme Belgesi

Choose File

No file chosen

Şirket Adı

Şirket Adı

Vergi Dairesi

Vergi Dairesi

Vergi Numarası

Vergi Numarası

Ülke

Afghanistan

Şehir

Şirket Adresi

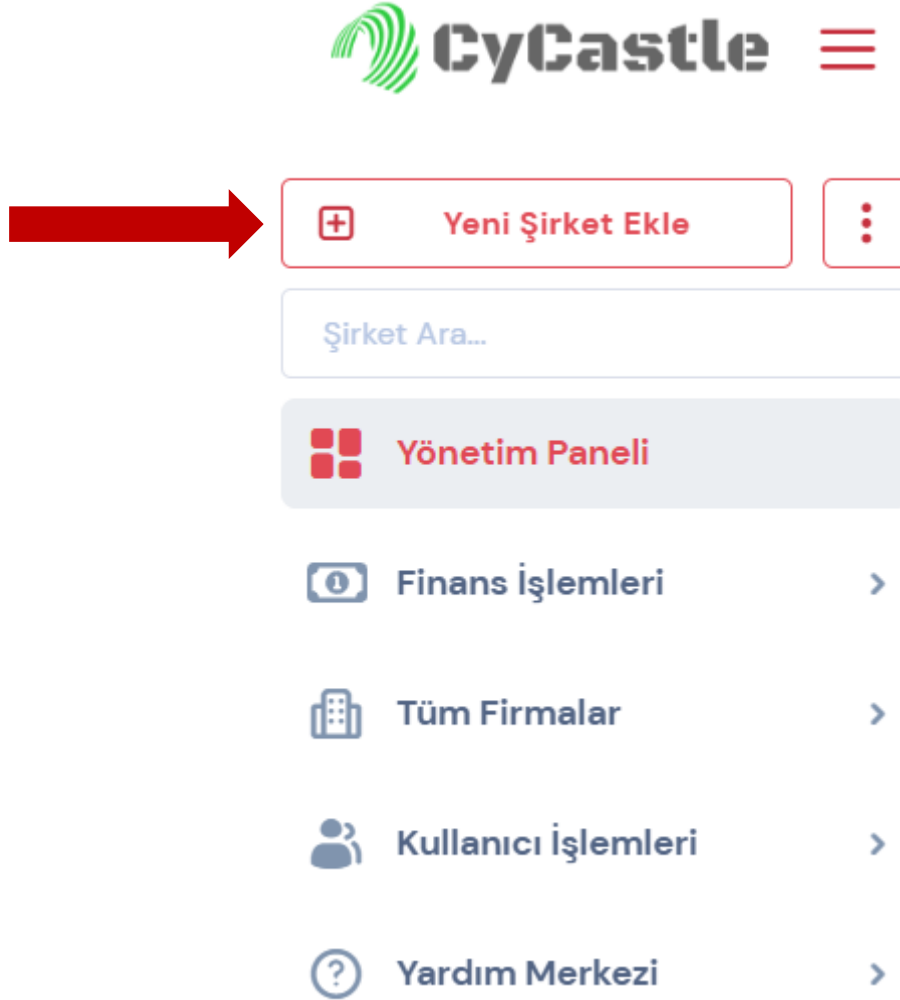
İptal

Güncelle

İletmiş olduğunuz bilgiler, onay sürecine alınacak olup, gerekli incelemelerin ardından hesabınıza 100 kredi tanımlanacaktır.

Nasıl Şirket Oluşturabilirim?

Menü üzerinden “**Yeni Şirket Ekle**” butonuna tıklayarak yeni bir şirket oluşturma sürecini başlatabilirsiniz.



Gerekli alanları eksiksiz şekilde doldurduktan sonra “**Kaydet**” butonuna tıklayarak işlemi tamamlayabilirsiniz.

Yeni Şirket Hesabı Oluştur

Aşağıdaki Formla Şirket Detaylarınızı Girin.

Şirket Detayları

Şirket Görünen Adı

Şirket Ünvanı

Adı Soyadı

E-Posta Adresi

Telefon Numarası

Şirketin Bulunduğu Ülke

Türkiye

Zaman Dilimi

Europe/İstanbul

Bölge

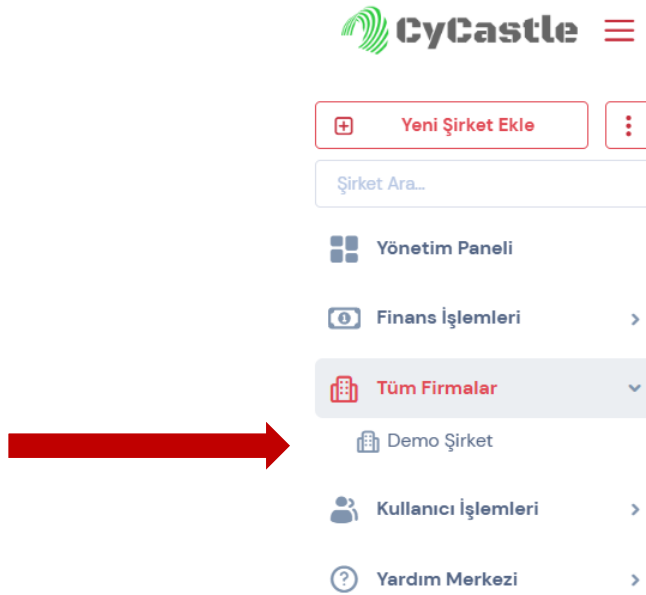
Şehir

Posta Kodu

Adresi

Kaydet

Oluşturduğunuz şirket, “**Tüm Firmalar**” menüsü altında listelenecektir.



ThreatChaser Ürün Anahtarını Nasıl Bulabilirim?

Ürün anahtarınızı almak için, menüden ilgili şirketi seçin ve "**Şirket Detayları**" butonuna tıklayın.



Yeni Şirket Ekle

Şirket Ara...

Yönetim Paneli

Finans İşlemleri

Tüm Firmalar

CyCastle Demo Şirket

Kullanıcı İşlemleri

Yardım Merkezi

Özet

Şirket Detayları

Alan Adı Yönetimi

ThreatChaser

ThreatChaser Web Tarama

ThreatChaser CTI

ThreatChaser 5651 Log ve HotSpot Hizmeti **New**

ThreatChaser SSL Kontrol Aracı **New**

ThreatChaser VPN Hizmetleri **New**

"**Şirket Detayları**" menüsünde ürün anahtarınızı bulabilirsiniz.

Demo Şirket



Ürün Anahtarı
[Redacted] OFX

ThreatChaser Nasıl Kurulur?

Ekranın üst kısmında bulunan “İndirmeler” butonuna tıklayarak, açılan sayfadan size uygun sanallaştırma çözümünü indirip, sunucunuza kurabilirsiniz.



İndirmeler

ThreatChaser Ajanını Bilgisayarınıza İndirin



VMWare / Virtualbox Çözümü

ThreatChaser ajanımızı VMWare ve Virtualbox platformlarında kullanmak için, aşağıdaki bağlantıdan VMWare ve Virtualbox uyumlu sanal ajan dosyasını indirerek kolayca çalıştırabilirsiniz.

Konsol Arayüzü Giriş Bilgisi

Kullanıcı Adı: wizard

Şifre: threatchaser

GUI Arayüzü Giriş Bilgisi

Kullanıcı Adı: admin

Şifre: threatchaser



Ajanı Bilgisayarınıza İndirin

Hyper-V Çözümü

ThreatChaser ajanımızın Hyper-V platformu için optimize edilmiş sürümünü kullanabilirsiniz. Aşağıdaki bağlantıya tıklayarak Hyper-V uyumlu sanal ajanı indirip hemen çalıştırabilirsiniz.

Konsol Arayüzü Giriş Bilgisi

Kullanıcı Adı: wizard

Şifre: threatchaser

GUI Arayüzü Giriş Bilgisi

Kullanıcı Adı: admin

Şifre: threatchaser



Ajanı Bilgisayarınıza İndirin

Minimum Sistem Gereksinimleri

İşletim Sistemi: Ubuntu 64-Bit

CPU: 4 Çekirdek

Ram: 8 GB

Hard Disk: 100 GB

Önerilen Minimum Sistem Gereksinimleri

İşletim Sistemi: Ubuntu 64-Bit

CPU: 8 Çekirdek

Ram: 16 GB

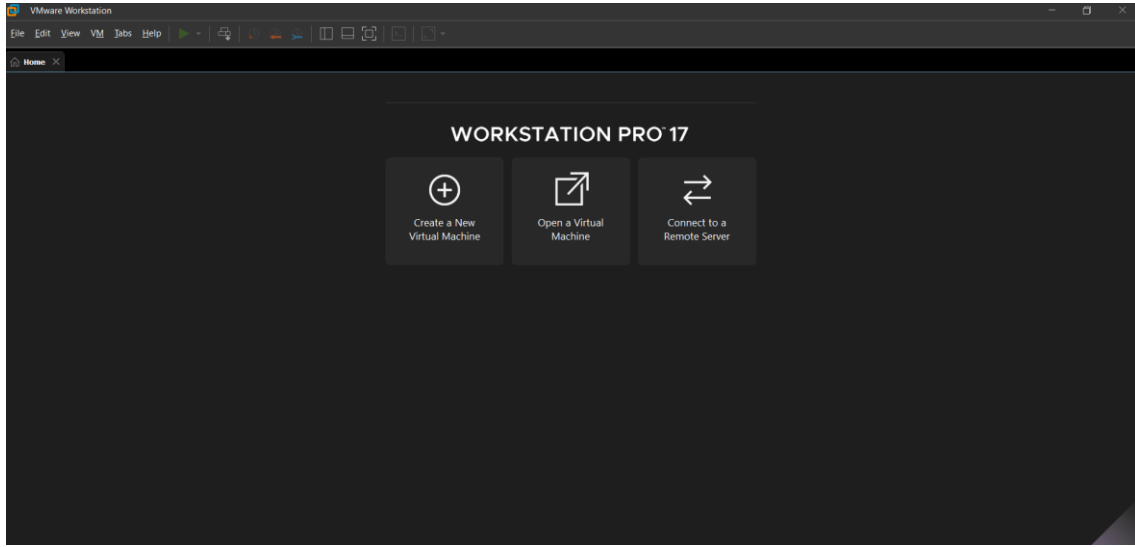
Hard Disk: 100 GB

Not: Yukarıdaki sistem gereksinimleri minimum değerleri göstermektedir. Orta ve Yüksek ölçekte ağlar için daha yüksek donanım özellikleri oluşturulmalıdır.

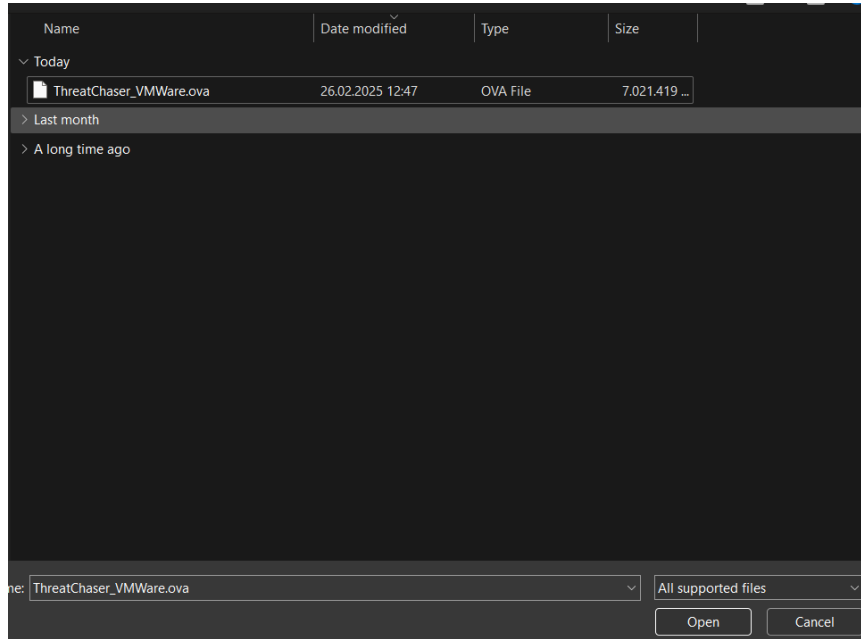
Önemli Bilgilendirme: Firmanızda konumlandırılmış SIEM ürünleri varsa, özel bir kural oluşturularak ThreatChaser ajanına izin vermeniz gerekmektedir. Çok yoğun Broadcast trafiği nedeniyle SIEM yazılımları tarafından ThreatChaser yazılımı engellenmektedir.

1.VMWare Pro Ajan Kurulumu

1.VMWare programını başlattıktan sonra sanal makineyi aç butonuna basıyoruz



2.Gelen pencerede ajanımızı seçip devam ediyoruz.



3.Sanal makinemize bir isim veriyoruz ve ilerliyoruz.

Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:

threatchaser

Storage path for the new virtual machine:

C:\Users\aatay\OneDrive\Documents\Virtual Machines\threat

Browse...

Help

Import

Cancel

4.Açılan pencerede sanal makinemizi başlatıyoruz.



5. Açılan ekranda varsayılan değerler gözükecektir fakat dilerseniz değiştirmek için “Enter” tuşuna basabilirsiniz ve daha sonra [Konsol Arayüzü Giriş](#) bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için “1” değerini giriniz.
- Statik IP için “2” değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

```

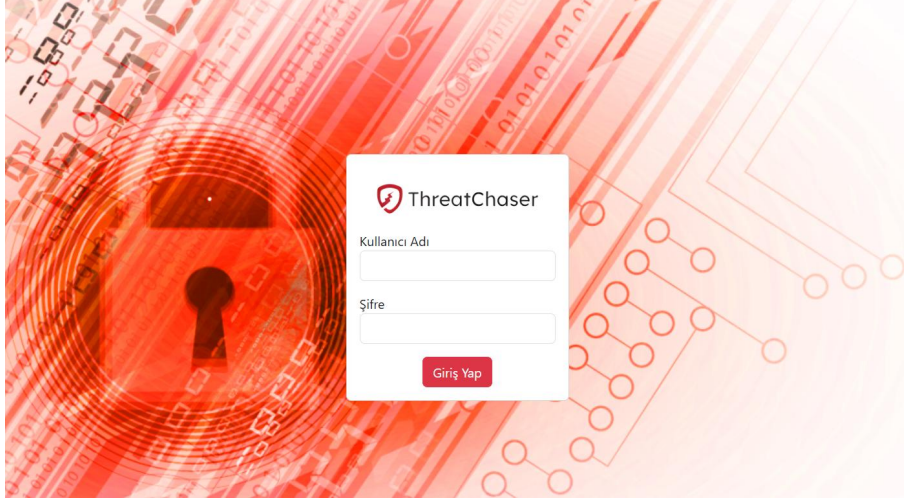
-----
ThreatChaser
-----

Ağ Bilgileri:
IP Adresi: 192.168.100.116
Netmask: 255.255.255.0
Gateway: 192.168.100.1
Hostname: ThreatChaser

=====
      Ana Menü
=====
1) Network Konfigürasyonu
2) Kullanıcı Şifre Sıfırlama
3) Fabrika Ayarlarına Dön
4) Yeniden Başlat
5) Sistemi Kapat
=====
Seçiminiz (1-5): 1
Ağ yapılandırma türünü seçin:
1) Dinamik IP (DHCP)
2) Statik IP
Seçiminiz (1/2): 2
IP adresini girin (Varsayılan: 192.168.100.116): 192.168.100.25
CIDR girin (0-32, Varsayılan: 24): 24
Gateway girin (Varsayılan: 192.168.100.1): 192.168.100.1
DNS girin (Varsayılan: 1.1.1.1): 1.1.1.1
Hostname girin (Varsayılan: ThreatChaser): ThreatChaser

```

6.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.



7.Giriş başarıyla gerçekleştikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.

Abonelik Hizmetleri
Aşağıdaki listede abonelik hizmetlerinizi görüntülemektesiniz.

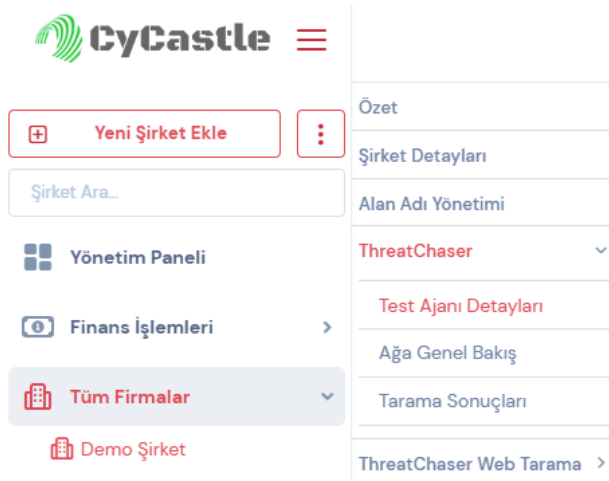
Aktif Bir Ürün Anahtarı Bulunamadı!

Ürün Anahtarı: 2PCHRK-ZTODB-XS2IX-90FX

Dil: Türkçe

Kaydet

8.Yazılımı yüklediğiniz şirketin menüsünde Test Ajanı Detayları bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



Sisteminize Kurulu Ajan Bilgisi

Aşağıda Tarama Ajanının Kurulu Olduğu Sistemin Bilgisi Görüntülenmektedir.



Çevrim İçi

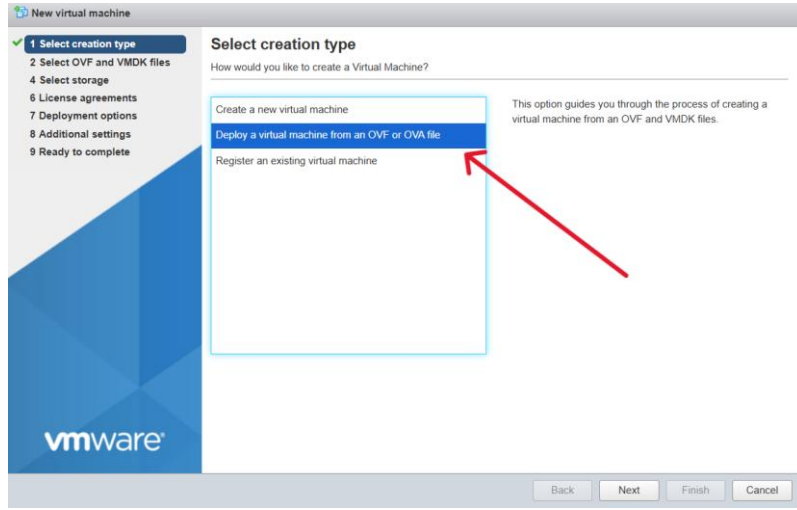
Bilgisayar Adı: ThreatChaser
IP Adresi: 127.0.0.1, 192.168.31.93
MAC Adresi: 00-0c-29-1e-07-78
Açılış Zamanı: 27.02.2025 12:28:00
Yazılım Versiyonu: V1.12
Public IP Adresi: [REDACTED]
Son Erişim Zamanı: 27.02.2025 12:30:03

SİSTEM BİLGİLERİ

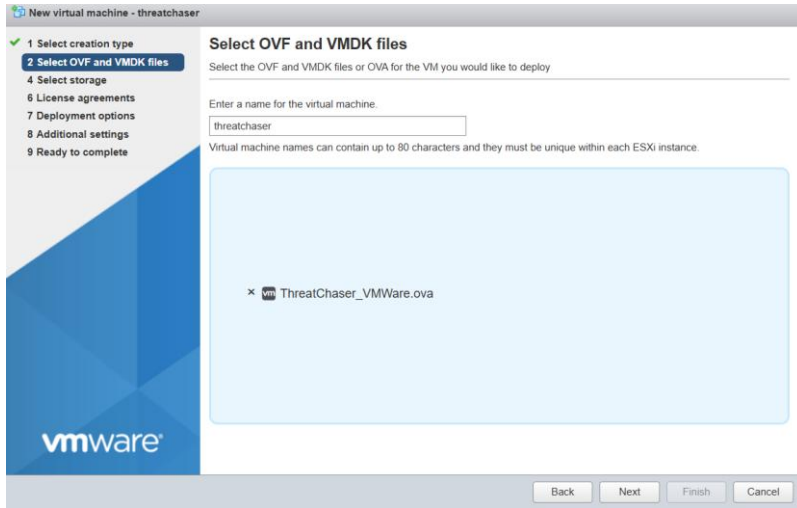
İşletim Sistemi:	Ubuntu 24.04.1 LTS	CPU Thread:	4 Thread
Versiyon:	24.04	CPU Hızı:	2295.688 GHZ
Üretici:	Ubuntu	CPU Model:	AMD Ryzen 5 5600U with Radeon Graphics
Kurulum Tarihi:	17.11.2024 15:53:56	Ram:	41 GB
Dil:	en_US.UTF-8	Ram Hızı:	
Saat Dilimi:	Europe/Istanbul (+03, +0300)	Hard Disk:	101.61 GB
Sistem Üreticisi:	VMware, Inc.	Sistem Tipi:	x86_64
Sistem Modeli:	VMware Virtual Platform	Bios Versiyonu:	6.00

2.VMWare ESXi Kurulumu

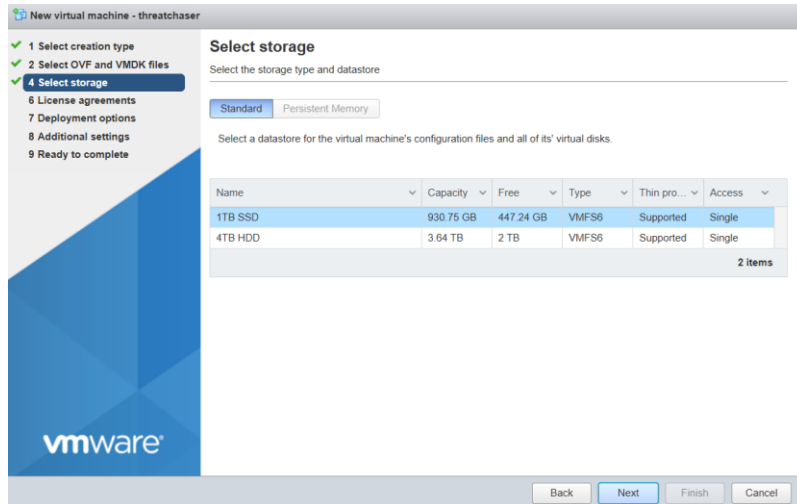
1.VMWare ESXi ekranında Virtual Machine > Create / Register VM butonuna tıkladıktan sonra aşağıdaki adımları takip ediniz.



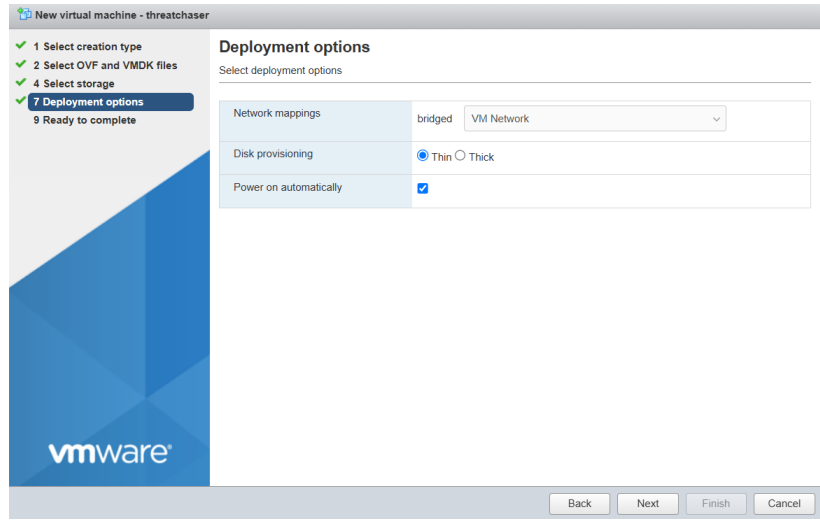
2.Gelen pencerede OVA dosyasını seçip ardından sanal makinenize bir isim veriniz



3.Kullanılacak disk alanını seçiniz.



4. Dağıtım ayarımızı ayarladıktan sonra işlemi bitirerek sanal makinemizi başlatıyoruz.



5. Açılan ekranda varsayılan değerler gözükecektir fakat derseniz değiştirmek için “Enter” tuşuna basabilirsiniz ve daha sonra [Konsol Arayüzü Giriş](#) bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

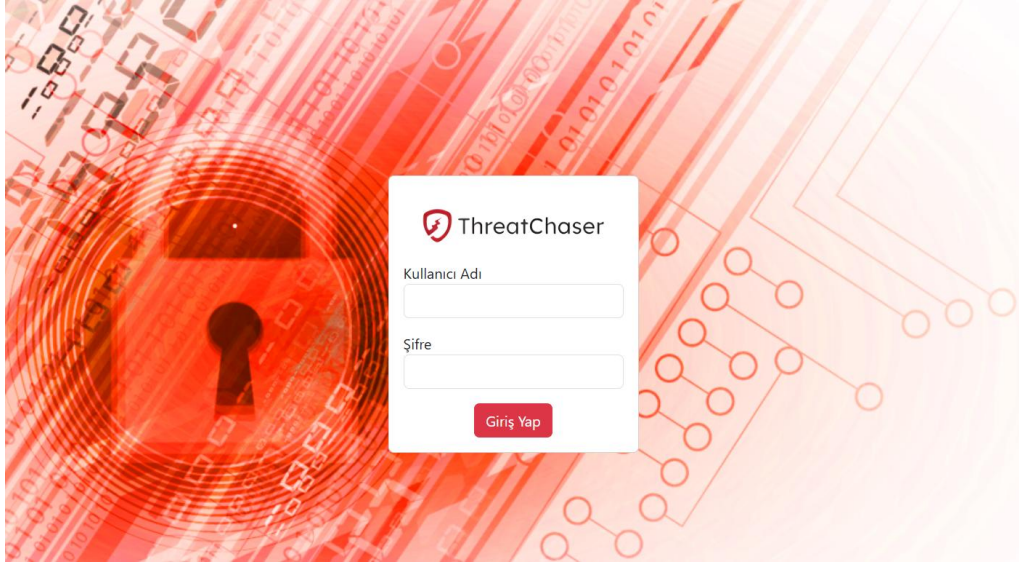
- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için “1” değerini giriniz.
- Statik IP için “2” değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

```
ThreatChaser

Ağ Bilgileri:
IP Adresi: 192.168.100.116
Netmask: 255.255.255.0
Gateway: 192.168.100.1
Hostname: ThreatChaser

=====
      Ana Menü
=====
1) Network Konfigürasyonu
2) Kullanıcı Şifre Sıfırlama
3) Fabrika Ayarlarına Dön
4) Yeniden Başlat
5) Sistemi Kapat
=====
Seçiminiz (1-5): 1
Ağ yapılandırma türünü seçin:
1) Dinamik IP (DHCP)
2) Statik IP
Seçiminiz (1/2): 2
IP adresini girin (Varsayılan: 192.168.100.116): 192.168.100.25
CIDR girin (0-32, Varsayılan: 24): 24
Gateway girin (Varsayılan: 192.168.100.1): 192.168.100.1
DNS girin (Varsayılan: 1.1.1.1): 1.1.1.1
Hostname girin (Varsayılan: ThreatChaser): ThreatChaser
```

6.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.



7.Giriş başarıyla gerçekleştikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.

Abonelik Hizmetleri

Aşağıdaki listede abonelik hizmetlerinizi görüntülemektesiniz.

Aktif Bir Ürün Anahtarı Bulunamadı!

Ürün Anahtarı

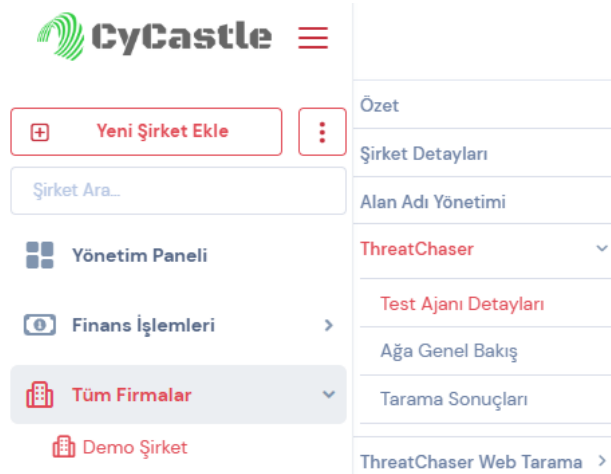
2PCHRK-ZTODB-XS2IX-90FX

Dil

Türkçe

Kaydet

8.Yazılımı yüklediğiniz şirketin menüsünde “**Test Ajanı Detayları**” bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



Sisteminize Kurulu Ajan Bilgisi

Aşağıda Tarama Ajanının Kurulu Olduğu Sistemin Bilgisi Görüntülenmektedir.



Çevrim İçi

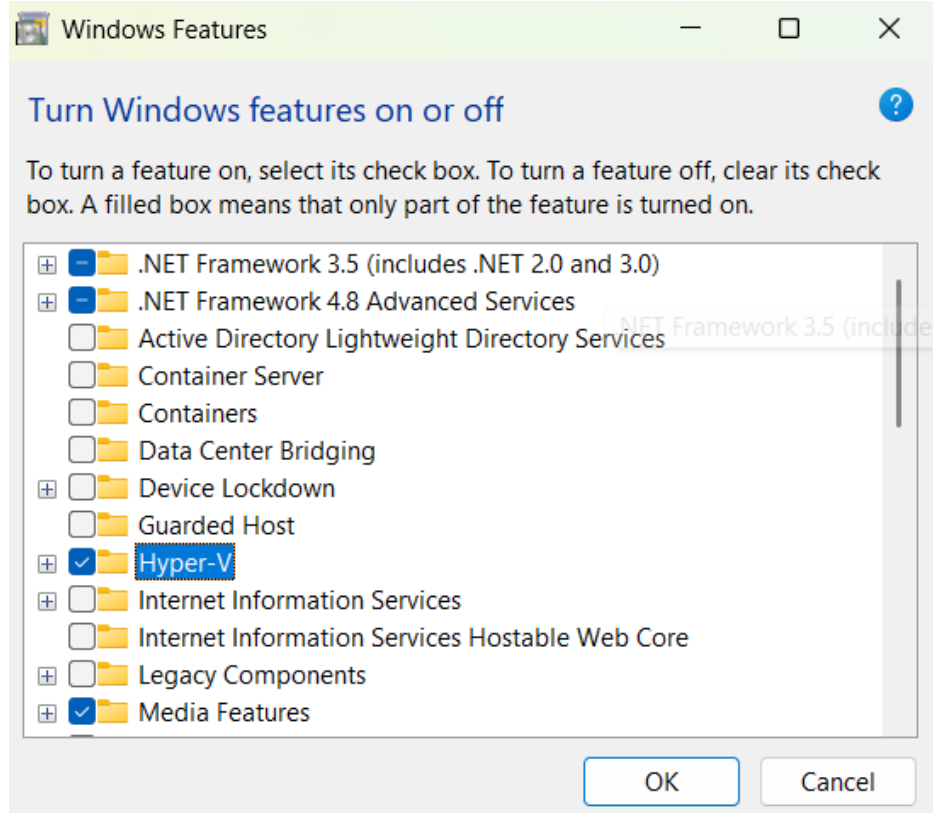
Bilgisayar Adı: ThreatChaser
IP Adresi: 127.0.0.1, 192.168.31.93
MAC Adresi:
Açılış Zamanı: 27.02.2025 12:28:00
Yazılım Versiyonu: V1.1.2
Public IP Adresi:
Son Erişim Zamanı: 27.02.2025 12:30:03

SİSTEM BİLGİLERİ

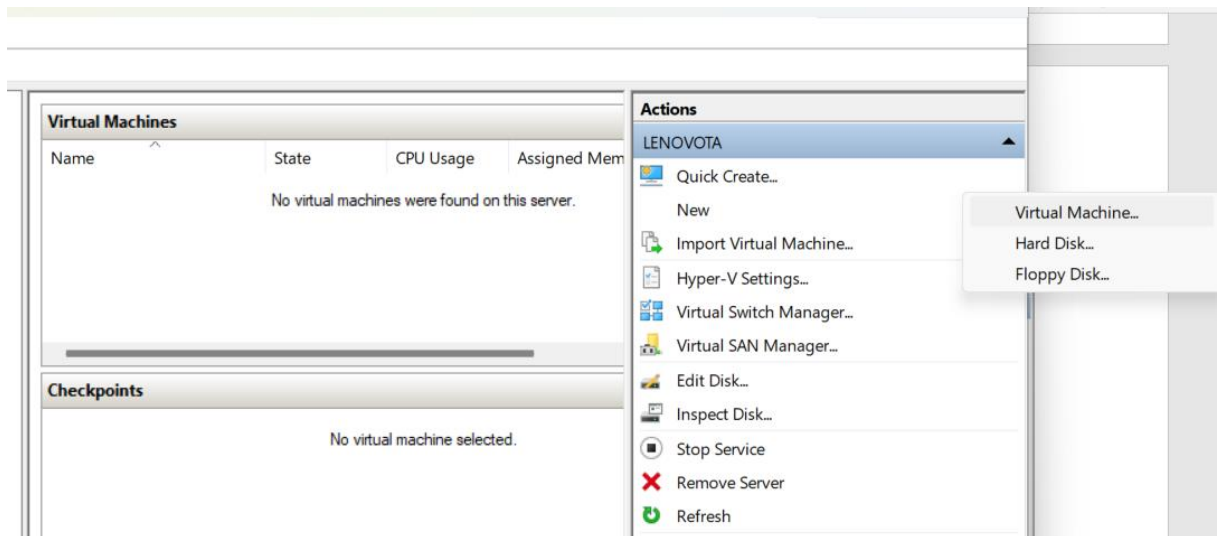
İşletim Sistemi:	Ubuntu 24.04.1 LTS	CPU Thread:	4 Thread
Versiyon:	24.04	CPU Hızı:	2295.688 GHZ
Üretici:	Ubuntu	CPU Model:	AMD Ryzen 5 5600U with Radeon Graphics
Kurulum Tarihi:	17.11.2024 15:53:56	Ram:	4.1 GB
Dil:	en_US.UTF-8	Ram Hızı:	
Saat Dilimi:	Europe/Istanbul (+03, +0300)	Hard Disk:	101.61 GB
Sistem Üreticisi:	VMware, Inc.	Sistem Tipi:	x86_64
Sistem Modeli:	VMware Virtual Platform	Bios Versiyonu:	6.00

3.Hyper-V Ajan Kurulumu

1.Denetim masasında “Programlar” kısmına gelindikten sonra “Windows Özelliklerini Aç / Kapat” kısmına tıklıyoruz. Açılan pencerede Hyper-V kutucuğuna tıklayıp OK (Tamam) butonuna tıklayabilirsiniz.



2.”New” diyerek “Virtual Machine” kısmına tıklıyoruz.



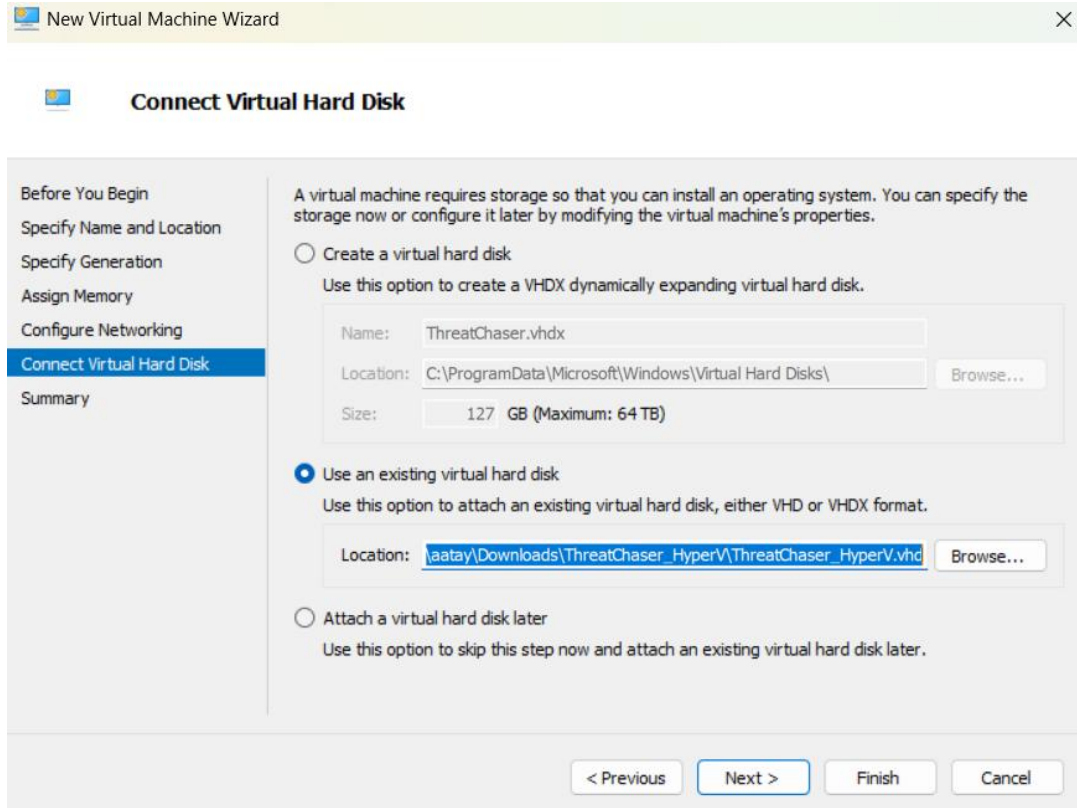
3.Açılan pencerede sanal makinemize isim veriyoruz.

The screenshot shows the 'Specify Name and Location' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area has a title bar 'Specify Name and Location' and a close button. Below the title bar, there is a section 'Choose a name and location for this virtual machine.' with a text box for 'Name' containing 'ThreatChaser'. A note states: 'The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' Below this, there is a checkbox 'Store the virtual machine in a different location' which is unchecked. A 'Location' text box shows 'C:\ProgramData\Microsoft\Windows\Hyper-V\' and a 'Browse...' button. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

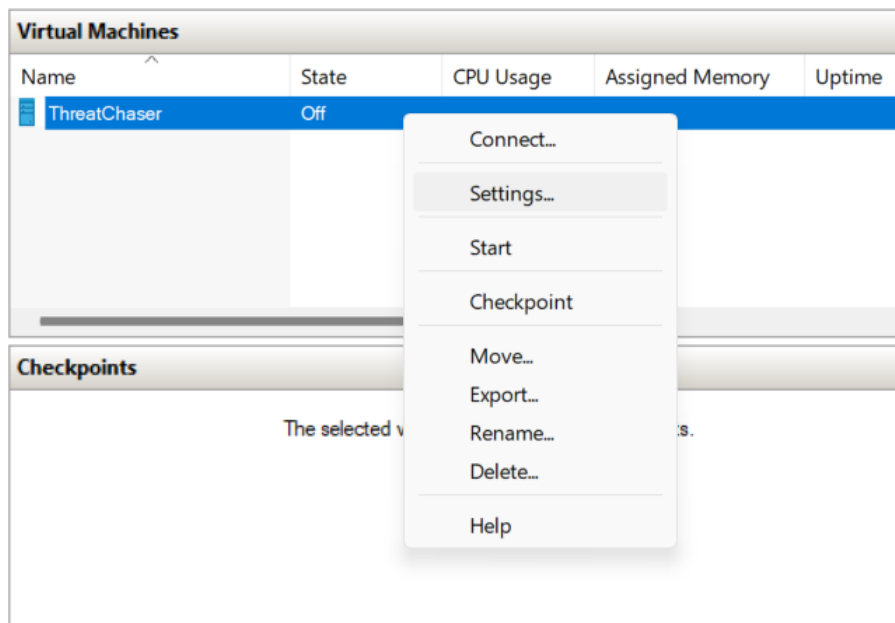
4.Ağ konfigürasyon kısmında “Default Switch” seçeneğini seçip devam ediyoruz.

The screenshot shows the 'Configure Networking' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory', 'Configure Networking' (highlighted), 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area has a title bar 'Configure Networking' and a close button. Below the title bar, there is a section 'Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.' with a 'Connection:' label and a dropdown menu. The dropdown menu is open, showing three options: 'Not Connected', 'Not Connected', and 'Default Switch' (highlighted). At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

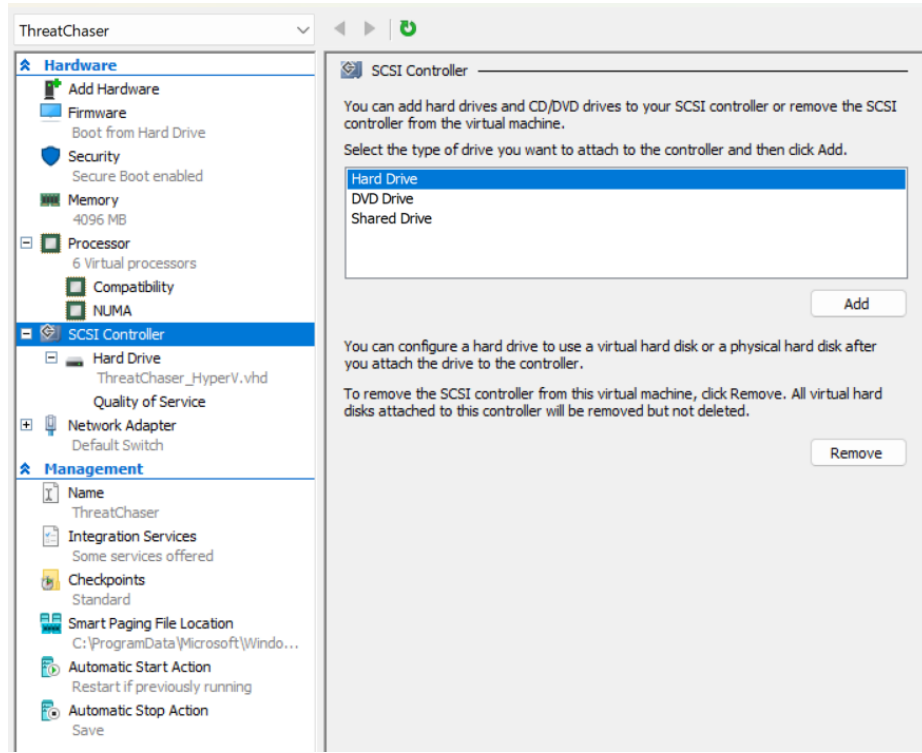
5.Öncesinde indirdiğimiz zip dosyasında çıkarttığımız “ThreatChaser_Hyper.vhd” dosya konumunu var olan sanal hard diskler kısmından ekliyoruz ve devam ediyoruz.



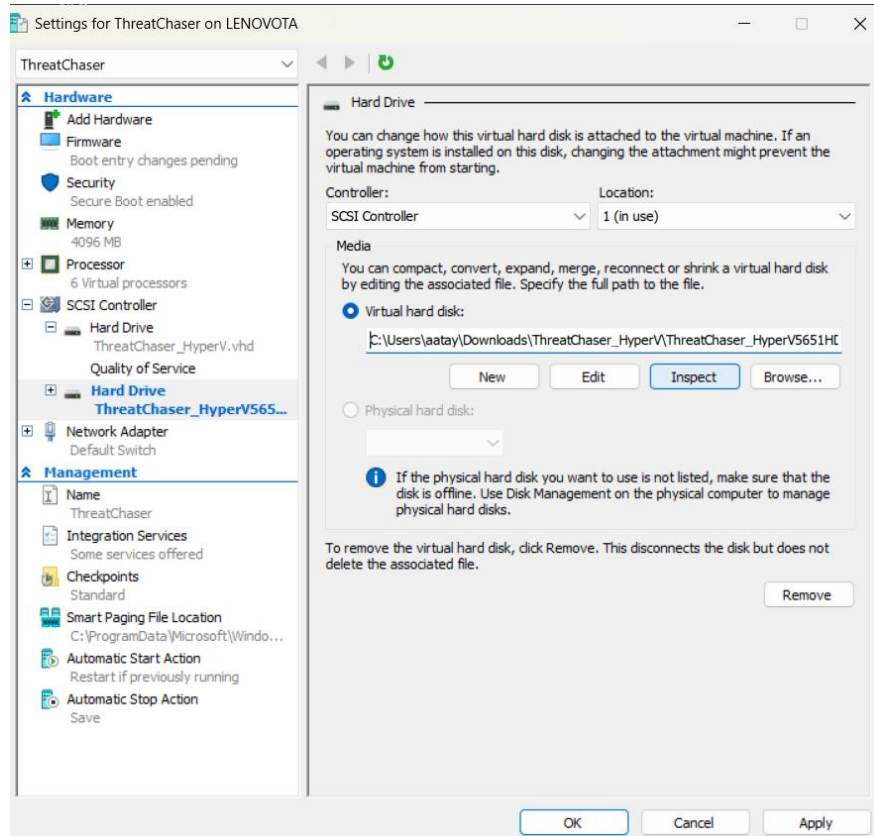
6. Oluşan sanal makinemizin üstüne gelip sağ tıklayarak açılan sekmelerde Settings (Ayarlar) kısmına tıklıyoruz.



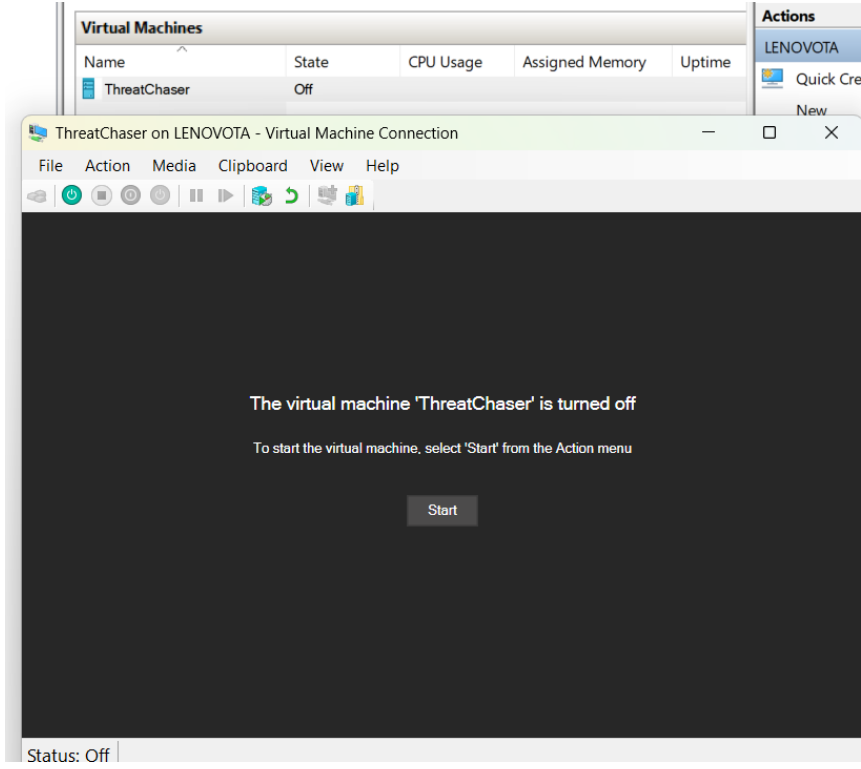
7.SCSI Controller kısmına gelip Hard Drive seçiliyken “Add” butonuna basıp ilerliyoruz.



8.Daha sonra önceden indirdiğimiz dosyamızın içindeki “ThreatChaser_HyperV5651HDD.vhd” diskimizin dosya yolunu ekliyoruz



9.Diskler başarıyla eklendikten sonra makinemizin üstüne gelerek “Connect” kısmını seçiyoruz ve ardından açılan pencerede “Start” diyerek sanal makinemizi başlatıyoruz.



10. Açılan ekranda varsayılan değerler gözükecektir fakat derseniz değiştirmek için **“Enter”** tuşuna basabilirsiniz ve daha sonra [Konsol Arayüzü Giriş](#) bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için “1” değerini giriniz.
- Statik IP için “2” değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

```

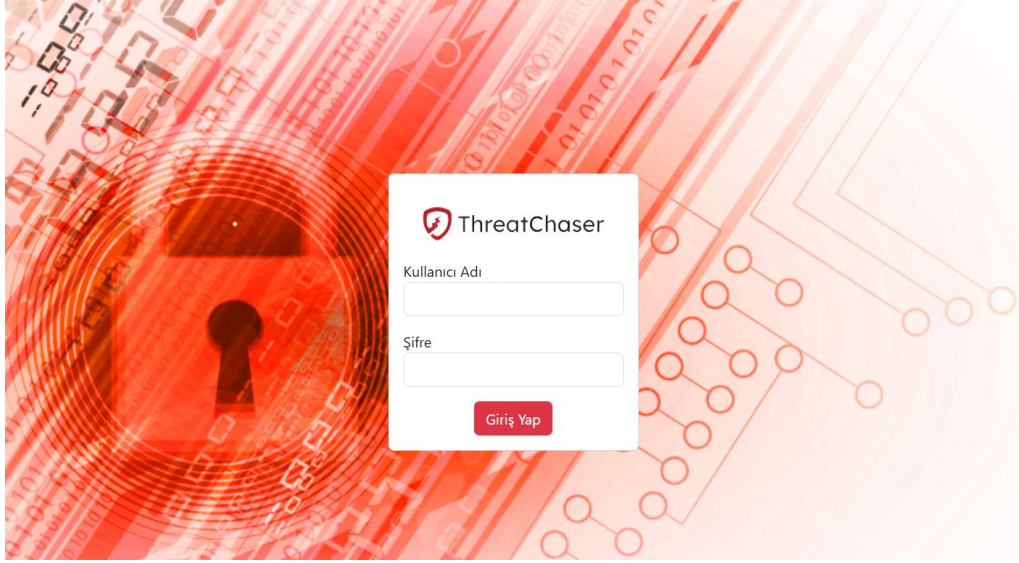
-----
ThreatChaser
-----

Ağ Bilgileri:
IP Adresi: 192.168.100.116
Netmask: 255.255.255.0
Gateway: 192.168.100.1
Hostname: ThreatChaser

=====
      Ana Menü
=====
1) Network Konfigürasyonu
2) Kullanıcı Şifre Sıfırlama
3) Fabrika Ayarlarına Dön
4) Yeniden Başlat
5) Sistemi Kapat
=====
Seçiminiz (1-5): 1
Ağ yapılandırma türünü seçin:
1) Dinamik IP (DHCP)
2) Statik IP
Seçiminiz (1/2): 2
IP adresini girin (Varsayılan: 192.168.100.116): 192.168.100.25
CIDR girin (0-32, Varsayılan: 24): 24
Gateway girin (Varsayılan: 192.168.100.1): 192.168.100.1
DNS girin (Varsayılan: 1.1.1.1): 1.1.1.1
Hostname girin (Varsayılan: ThreatChaser): ThreatChaser

```

11.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.



12.Giriş başarıyla gerçekleşikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.

Abonelik Hizmetleri

Aşağıdaki listede abonelik hizmetlerinizi görüntülemektesiniz.

Aktif Bir Ürün Anahtarı Bulunamadı!

Ürün Anahtarı

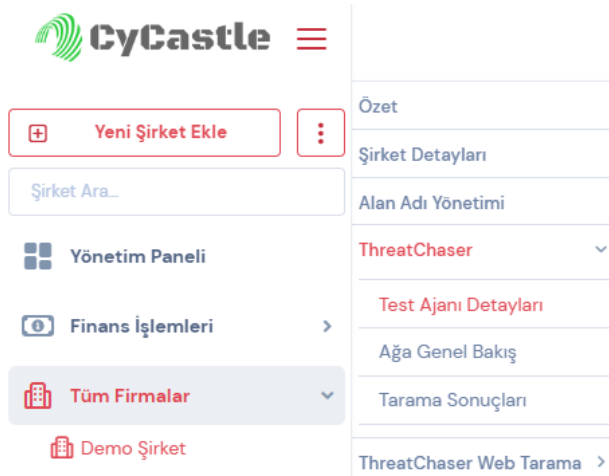
2PCHRK-ZTODB-XS2IX-90FX

Dil

Türkçe

Kaydet

13.Yazılımı yüklediğiniz şirketin menüsünde “**Test Ajanı Detayları**” bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



Sisteminize Kurulu Ajan Bilgisi

Aşağıda Tarama Ajanının Kurulu Olduğu Sistemin Bilgisi Görüntülenmektedir.



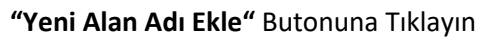
Çevrim İçi

Bilgisayar Adı: ThreatChaser
IP Adresi: 127.0.0.1, 192.168.31.93
MAC Adresi:
Açılış Zamanı: 27.02.2025 12:28:00
Yazılım Versiyonu: V1.1.2
Public IP Adresi:
Son Erişim Zamanı: 27.02.2025 12:30:03

SİSTEM BİLGİLERİ

İşletim Sistemi:	Ubuntu 24.04.1 LTS	CPU Thread:	4 Thread
Versiyon:	24.04	CPU Hızı:	2295.688 GHZ
Üretici:	Ubuntu	CPU Model:	AMD Ryzen 5 5600U with Radeon Graphics
Kurulum Tarihi:	17.11.2024 15:53:56	Ram:	4.1 GB
Dil:	en_US.UTF-8	Ram Hızı:	
Saat Dilimi:	Europe/Istanbul (+03, +0300)	Hard Disk:	101.61 GB
Sistem Üreticisi:	VMware, Inc.	Sistem Tipi:	x86_64
Sistem Modeli:	VMware Virtual Platform	Bios Versiyonu:	6.00

Domain eklemek istediğiniz şirketin menüsünde **“Alan Adı Yönetimi”** bölümüne gidin.



Aşağıdaki listede Alan Adlarınız listelenmektedir. Web Site Zafiyet taraması ve Dark Web izleme işlemleri için Alan Adı kaydını doğrulamanız gerekmektedir.

+ Yeni Alan Adı Ekle

Yeni Alan Adı Ekle

Alan Adı

✖

Önemli Bilgilendirme: Yeni Alan Adınızı ekledikten sonra bu Alan Adının size ait olduğunu teyit etmemiz için doğrulama işlemi yapmanız gerekmektedir. Sizden DNS kaydı veya üretilen bir TXT dosyasını web sitenizin root dizinine eklemeniz istenecektir. (Örnek: <https://alanadiniz.com/threatchaser-absadqwec.txt>)

İptal

Kaydet

Alan Adımı Nasıl Doğrulayabilirim?

Eklediğiniz alan adının yanında yer alan “**Doğrula**” butonuna tıklayarak doğrulama sürecini başlatabilirsiniz.

Alan Adı Yönetimi					
Aşağıdaki listede Alan Adlarınız listelenmektedir. Web Site Zafiyet taraması ve Dark Web izleme işlemleri için Alan Adı kayıtları doğrulanması gerekmektedir.					
Yeni Alan Adı Ekle					
Arama Tipi					
ID					
Durum	Alan Adı	Alt Alan Adı	Doğrulama Kodu	Doğrulama Yöntemi	
Doğrulandı		public	Otomatik Oluşturuldu	Otomatik Oluşturuldu	
Doğrulanmadı		Çözümlenemedi() DNS Çözümlenemedi() Alt Alan Adı Ekle		Doğrula	
Göstere: 1 - 2 / 2					
Önceki 1 Sonraki					

Açılan pencereadaki adımları takip ederek işlemi tamamlayabilirsiniz.

Alan Adı Sahipliğini Doğrulayın

DNS Kaydı ile Doğrulama Adımları

1 Alan adı sağlayıcınızda (ör. cloudflare.com, godaddy.com veya namecheap.com) oturum açın,

2 Yeni DNS kaydı ekleme adımına gelin,

3 Kayıt Türü: TXT seçin,

4 TXT kaydını seobso için aşağıdaki DNS yapılandırmasına kopyalayın,

threatchaser- Kopyala

5 Doğrula butonuna tıklayın

TXT Dosyası ile Doğrulama Adımları

1 FTP veya Dosya Yöneticisi ile web sitenizin kurulu olduğu klasöre gelin (ör. public_html, public veya /var/www/ olabilir. Bilginiz yoksa Hosting firmanız ile görüşün.),

2 Aşağıdaki TXT dosyasını indirin,

3 Bu TXT dosyası seobso için geçerlidir. Dosyada hiç bir değişiklik yapmadan olduğu gibi web sitenizin ana dizinine kopyalayın,

4 TXT dosyasını aşağıdaki butona tıklayarak indirebilirsiniz.

threatchaser-

5 Doğrula butonuna tıklayın

Not: Yukarıdaki 2 yöntemden sadece 1 tanesini denemeniz yeterlidir. İki yöntemi de uygulamak olumsuz bir şey teşkil etmemektedir.

Not: DNS önbelleginin güncellenmesi bazen zaman alabilir. Sistemlerimiz, her 5 dakikada bir kayıtları otomatik olarak sorgular. Başarılı bir şekilde eklenen kayıtlar, sistem tarafından otomatik olarak aktif hale getirilir.

Deha Sonra Doğrula

Doğrula

Adımları uyguladıktan sonra menüdeki “**Doğrula**” butonuna tıklayarak işlemi tamamlayın.



Daha Sonra Doğrula	Doğrula
--------------------	---------

Nasıl Web Taraması Başlatabilirim ?

Web taraması başlatmak istediğiniz şirketin menüsünde yer alan “**Web Siteleri**” bölümüne gidiniz ve taramak istediğiniz alan adlarını seçiniz.

**CyCastle** 

**Yeni Şirket Ekle**



Şirket Ara...

**Yönetim Paneli**

**Finans İşlemleri**



**Tüm Firmalar**



**CyCastle Demo Şirket**

**Kullanıcı İşlemleri**



**Yardım Merkezi**



Özet

Şirket Detayları

Alan Adı Yönetimi

ThreatChaser 

ThreatChaser Web Tarama 

Adresler

Tarama Sonuçları

ThreatChaser CTI

ThreatChaser 5651 Log ve HotSpot Hizmeti **New**

ThreatChaser SSL Kontrol Aracı **New**

“Seilen Web Sitelerini Tara” butonuna tıklayarak tarama işlemini başlatabilirsiniz.

Genel IP ve Web Zafiyet Analizi Hizmeti

Aşğıdaki listede Alan Adlarınızın ve Genel IP adresinize ait bir liste bulunmaktadır. Web sitenize zafiyet taramasını bu sayfadan yapabilirsiniz.

☐	Alan Adı Durumu	Alan Adı	Alt Alan Adı
☐	Doğrulandı		PUBLIC IP
☐	Doğrulanmadı		(DNS Çözümlemedi!) www. (DNS Çözümlemedi!)

Gösterilen: 1 – 2 / 2

Önceki

1

Sonraki

Not: Tarama hızı ve sayısı, ağ trafiğinin yoğunluğunu etkileyebilir. Özellikle yoğun ağ trafiği olan sistemlerde, bu değerlerin çok yüksek tutulması önerilmez.

Taranacak Alan adlarını seçip “**Kaydet**” diyerek devam ediniz.

E-Posta Bildirimi

Tarama tamamlandığında rapor dosyasını E-Posta adresine gönderebilirsiniz.

E-Posta Adresi

Hangi Durumda Oluşturulan Rapor E-Posta Adresinize Gönderilsin?

☐ Hiçbir Zaman E-Posta Gönderme

☒ Tamamlandığında Anında E-Posta ile Rapor Dosyasını Gönder

☐ Sadece Yüksek veya Kritik Seviyede Güvenlik Açığı Tespit Edildiğinde E-Posta ile Rapor Dosyasını Gönder

Toplam Kredi

Gereken Kredi

Taranacak Hedef Sayısı

Taranacak Alan Adları

Aşğıda taranmasını istediğiniz Alan Adlarını seçip çıkarabilirsiniz.

İptal

Kaydet

Web Tarama Sonuçlarımı Nasıl Görüntüleyebilirim?

“ThreatChaser Web Tarama” sekmesine tıklayıp ardından “Tarama Sonuçları” kısmına tıklayabilirsiniz.

Özet

Şirket Detayları

Alan Adı Yönetimi

ThreatChaser

ThreatChaser Web Tarama

Adresler

Tarama Sonuçları

Açılan sayfada okla gösterilen butonlara tıklayarak detaylı şekilde zafiyetleri görüntüleyebilir veya sizin için hazırlanan zafiyet raporunu görüntüleyebilirsiniz.

Tarama Sonuçları

Aşağıdaki listede tarama listelerinizi görüntüleyebilirsiniz.

Durum	Tarama Durumu	Tarama Adı	Tespit Edilen Zafiyet	Başlangıç Tarihi	Bitiş Tarihi	Süre	Anlık	Çalıştırma	Tarama Hızı	#
Tamamlandı	%100	Web Taraması 26.02.2025 11:51	604	26.02.2025 11:52	27.02.2025 21:37	121499.04 sn	Manuel	Normal		
Tamamlandı	%100	Web Taraması 12.02.2025 10:08	32	12.02.2025 10:09	12.02.2025 12:05	1022.69 sn	Manuel	Normal		
Tamamlandı	%100	Web Taraması 12.02.2025 09:55	0	12.02.2025 09:56	12.02.2025 09:57	11.00 sn	Manuel	Normal		
Tamamlandı	%100	Web Taraması 10.02.2025 15:27	31	10.02.2025 15:28	10.02.2025 17:26	744.36 sn	Manuel	Hızlı		
Tamamlandı	%100	Web Taraması 06.02.2025 10:32	314		06.02.2025 15:48	17523.94 sn	Manuel	Hızlı		
Tamamlandı	%100	Web Taraması 05.02.2025 09:16	638	05.02.2025 09:36	07.02.2025 18:19	17523.94 sn	Manuel	Hızlı		
Tamamlandı	%100	Web Taraması 04.02.2025 17:40	0	04.02.2025 17:41	04.02.2025 17:41	28.87 sn	Manuel	Hızlı		

CVE Zafiyetlerini Nasıl Görüntüleyebilirim ?

Görüntüleme (Göz) ikonuna tıkladıktan sonra açılan sayfada görüntülemek istediğiniz alan adına tıkladığınızda, açılacak ekranda CVE zafiyetlerini görüntüleyebilirsiniz.

[Önceki Sayfaya Geri Dön](#)

✓ **www.s[REDACTED]** – Alan Adı Detayları

Aşağıdaki **www.s[REDACTED]** m Alan Adına Ait Detaylı Bilgileri Bulabilirsiniz.

CVE Zafiyetleri (11)

OVAS Zafiyetleri (47)

Arama Yap

10

CVE Kodu	Başlık	Keşfedilen Port	Saldırı Seviyesi	Skor	Keşif Tarihi
CVE-2015-4000		8010/TCP	Orta	4.3/10	21.05.2015
CVE-2011-5094		143/TCP	Orta	4.3/10	17.06.2012
CVE-2011-5094		110/TCP	Orta	4.3/10	17.06.2012
CVE-2011-5094		8010/TCP	Orta	4.3/10	17.06.2012
CVE-2011-1473		8010/TCP	Orta	5.0/10	16.06.2012
CVE-2011-1473		110/TCP	Orta	5.0/10	16.06.2012
CVE-2011-1473		143/TCP	Orta	5.0/10	16.06.2012
CVE-2013-2566		8010/TCP	Orta	4.3/10	14.03.2013
CVE-2015-0204		8010/TCP	Orta	4.3/10	09.01.2015
CVE-2011-3389		8010/TCP	Orta	4.3/10	06.09.2011

OVAS Zafiyetlerini Nasıl Görüntüleyebilirim ?

CVE kısmının hemen yanındaki OVAS Zafiyetleri kısmına tıklayarak görüntüleyebilirsiniz.

[Önceki Sayfaya Geri Dön](#)

✓ **[REDACTED]** – Alan Adı Detayları

Aşağıdaki **[REDACTED]** Alan Adına Ait Detaylı Bilgileri Bulabilirsiniz.

CVE Zafiyetleri (11)

OVAS Zafiyetleri (47)

Arama Yap

10

OID	Başlık	Port	Saldırı Seviyesi	Skor	Keşif Tarihi
13.6.1.4.1.25623.1.0.117761 → CVE-2011-1473 → CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	143/TCP	Orta	5.0/10	29.10.2021
13.6.1.4.1.25623.1.0.117761 → CVE-2011-1473 → CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	143/TCP	Orta	5.0/10	29.10.2021
13.6.1.4.1.25623.1.0.117761 → CVE-2011-1473 → CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	143/TCP	Orta	5.0/10	29.10.2021
13.6.1.4.1.25623.1.0.117757	SSL/TLS: Safe/Secure Renegotiation Support Status	443/TCP	Kabul Edilebilir	0.0/10	27.10.2021
13.6.1.4.1.25623.1.0.117757	SSL/TLS: Safe/Secure Renegotiation Support Status	443/TCP	Kabul Edilebilir	0.0/10	27.10.2021
13.6.1.4.1.25623.1.0.117757	SSL/TLS: Safe/Secure Renegotiation Support Status	443/TCP	Kabul Edilebilir	0.0/10	27.10.2021
13.6.1.4.1.25623.1.0.117757	SSL/TLS: Safe/Secure Renegotiation Support Status	443/TCP	Kabul Edilebilir	0.0/10	27.10.2021

Zafiyet Raporumu Nasıl Görüntüleyebilirim?

Tarama sonuçlar kısmındaki  ikonuna tıklayarak raporunuzu görüntüleyebilirsiniz.



Nasıl Ağ Taraması Başlatabilirim?

Ağ taraması başlatmak istediğiniz şirketin menüsünde “**Ağa Genel Bakış**” bölümüne giderek taramak istediğiniz ağı veya ağları seçiniz.

Özet
Şirket Detayları
Alan Adı Yönetimi
ThreatChaser
Test Ajansı Detayları
Ağa Genel Bakış
Tarama Sonuçları
ThreatChaser Web Tarama >
ThreatChaser CTI

Taramak istediğiniz ağı veya ağları seçin. “**Seçilen Ağları Tara**” butonuna tıklayarak taramayı başlatın.

Ağ Listeniz

Aşağıdaki listede ağlarınız listelenmektedir.

Durum

Ağ Keşfini Başlat

Seçilen Ağları Tara

Tablo Görünümü

Grafik Görünümü

Arama Yap

10

☒	Durum	Ağ	Ağ Maskesi	IP Sayısı	
☒	Aktif	192.168.31.0	255.255.255.0	14	 

Gösterilen: 1 - 1 / 1

Önceki

1

Sonraki

Tarama sayısını artırmak, ağınızdaki trafik yoğunluğunu yükseltebilir. Özellikle yoğun trafiğe sahip ağlarda bu sayıyı fazla artırmamanız önerilir.

Seilen Aęlar İin Tarama Bařlat

Tarama Adı

Tarama 03.03.2025 11:52

Anlık Tarama Sayısı

Anlık 1 Cihaz Tarama

E-Posta Bildirimi

Tarama tamamlandığında rapor dosyasını E-Posta adresine g nderebilirsiniz.

E-Posta Adresi

Hangi Durumda Oluřturulan Rapor E-Posta Adresinize G nderilsin?

☐ Hibir Zaman E-Posta G nderme

☒ Tamamlandığında Anında E-Posta ile Rapor Dosyasını G nder

☐ Sadece Y ksek veya Kritik Seviyede G venlik Aığı Tespit Edildiğinde E-Posta ile Rapor Dosyasını G nder

Kredi Bilgileri

Ařaęıda Mevcut Krediniz ve Harcanacak Kredi Miktarını G rebilirsiniz.

Toplam Kredi

899

Gereken Kredi

28

Taranacak IP Sayısı

14

Taranacak IP Adreslerinizi Seip “**Kaydet**” Butonuna tıklayarak devam ediniz

Taranacak IP Adresleri

Ařaęıda taranmasını istedięiniz IP adreslerini seip ıkarabilirsiniz.

☒

☒

192.168.31.0 / 255.255.255.0

☒

☒

192.168.31.69

☒

☒

192.168.31.71

☒

☒

192.168.31.72

☒

☒

192.168.31.73

☒

☒

192.168.31.76

☒

☒

192.168.31.77

☒

☒

192.168.31.78

☒

☒

192.168.31.82

☒

☒

192.168.31.84

☒

☒

192.168.31.85

☒

☒

192.168.31.86

☒

☒

192.168.31.87

Pasif olan IP adresleri listede g r nt lenmemektedir.  nce ilgili IP adreslerini aktif duruma getirip tekrar bu sayfaya gelin.

İptal

Kaydet

Ağ Tarama Sonuçlarını Nasıl Görüntüleyebilirim?

Ağ tarama sonuçlarını görmek istediğiniz şirketin menüsünde **“Tarama Sonuçları”** bölümüne giderek tarama sonuçlarınızı görüntüleyebilirsiniz

- Özet
- Şirket Detayları
- Alan Adı Yönetimi
- ThreatChaser** 
- Test Ajanı Detayları
- Ağa Genel Bakış
- Tarama Sonuçları**
- ThreatChaser Web Tarama 
- ThreatChaser CTI

Görüntülemek istediğiniz tarama raporunun **“PDF”** butonuna tıklayarak raporu görüntüleyebilirsiniz

Tarama Sonuçları

Aşağıdaki listede tarama listelerinizi görüntüleyebilirsiniz.

10

Durum	Tarama Durumu	Tarama Adı	Zarflı Sayısı	Başlangıç Tarihi	Bitiş Tarihi	Süre	Anlık	Çalıştırma	#
Tamamlandı	100%	Tarama 03.03.2025 11:55	19	03.03.2025 11:56	03.03.2025 12:14	1083.58 sn	1	Manuel	

Gösterilen: 1 - 1 / 1

Önceki
1
Sonraki

Siber Tehdit İstihbaratı (CTI) Nasıl Kullanabilirim ?

“ThreatChaser CTI” bölümüne giderek Alan Adlarınızı veya Kişisel E-posta hesaplarınızı izleyebilirsiniz.

Özet
Şirket Detayları
Alan Adı Yönetimi
ThreatChaser >
ThreatChaser Web Tarama >
ThreatChaser CTI

Alan Adlarınızı Nasıl İzleyebilirim ?

Aşağıdaki listede Alan Adlarınızın bir listesi bulunmaktadır. **Siber Tehdit İstihbaratı (CTI)** ile alan adlarınıza dair olası bir veri sızıntısında anlık bildirim alabilirsiniz. Durumu aktif hale getirdiğiniz de Monitör sütunu İzleniyor olarak değişir ve Siber Tehdit İstihbaratı (CTI) devreye girer.

Siber Tehdit İstihbaratı (CTI)

Aşağıdaki listede Alan Adlarınızın bir listesi bulunmaktadır. Siber Tehdit İstihbaratı (CTI) ile alan adlarınıza dair olası bir veri sızıntısında anlık bildirim alabilirsiniz. Durumu aktif hale getirdiğiniz de Monitör sütunu İzleniyor olarak değişir ve Siber Tehdit İstihbaratı (CTI) devreye girer.

Alan Adı Ekleme İçin Tıklayın

Arama Yap

10

Pasif/Aktif	Alan Adı Durumu	Monitör	Alan Adı	Bildirim Adresi	Yeni İhlal	Kilitli Açılan İhlal	Bilgilendirme	Son Kontrol	
☐	Doğrulandı	İzlenmiyor	ibank.com.tr	benli@ibank.com.tr	926	0	23.12.2024 18:45:44	23.12.2024 19:13:52	
☐	Doğrulandı	İzlenmiyor	ibank.com.tr	benli@ibank.com.tr	784	0	23.12.2024 18:45:44	23.12.2024 19:04:22	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	96	0	13.02.2025 09:23:06	03.03.2025 12:14:45	
☐	Doğrulandı	İzlenmiyor	ibank.com.tr	benli@ibank.com.tr	27	0	26.12.2024 02:45:33	26.12.2024 03:06:56	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	16	0	27.02.2025 19:23:16	03.03.2025 12:15:25	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	3	0	12.12.2024 23:14:01	03.03.2025 12:15:51	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	1	0	12.02.2025 11:43:14	03.03.2025 12:14:06	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	0	0	-	03.03.2025 12:14:55	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	0	1	13.12.2024 17:33:11	03.03.2025 12:15:31	
☒	Doğrulandı	İzleniyor	ibank.com.tr	benli@ibank.com.tr	0	1	-	03.03.2025 12:15:35	

Gösterilen: 1 - 10 / 19

Önceki 1 2 Sonraki

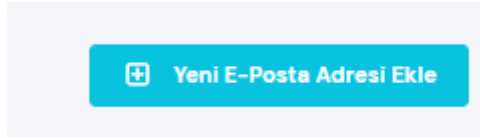
Kişisel E-posta Hesaplarımı Nasıl İzleyebilirim?

“ThreatChaser CTI” sayfasında sayfayı aşağıya kaydırıp listede onayladığınız E-Posta adreslerinin ihlallerini izleyebilirsiniz.

Kişisel E-Posta Hesabı İzleme										
Aşağıdaki listede onayladığınız E-Posta adreslerinin ihlallerini izleyebilirsiniz.										
Arama Yap										
10										
Pasif/Aktif	E-Posta Doğrulaması	Monitör	İzlenen E-Posta Adresi	Bildirim E-Posta Adresi	Yeni İhlal	Kilidi Açılan İhlal	Bildirim	Son Kontrol		
☐	Doğrulandı	İzleniyor	negreney@gmail.com	benli@neg@gmail.com	636	0	06.01.2025 03:19:38	09.01.2025 10:45:57		
☐	Doğrulandı	İzleniyor	denizay@gmail.com	benli@neg@gmail.com	106	0	06.01.2025 07:07:22	09.01.2025 10:45:57		
☒	Doğrulandı	İzleniyor	gi-000@neg.com	benli@neg@gmail.com	1	0	18.12.2024 19:01:07	03.03.2025 13:15:41		
☒	Doğrulandı	İzleniyor	benli@neg@gmail.com	benli@neg@gmail.com	0	0	-	03.03.2025 13:15:41		
☒	Doğrulandı	İzleniyor	denizay@gmail.com	negreney@gmail.com	0	4	23.02.2025 01:22:46	03.03.2025 13:15:41		
☒	Doğrulandı	İzleniyor	benli@neg@gmail.com	benli@neg@gmail.com	0	0	-	03.03.2025 13:15:42		
☒	Doğrulandı	İzleniyor	benli@neg@gmail.com	negreney@gmail.com	0	0	-	03.03.2025 13:15:42		
☒	Doğrulandı	İzleniyor	denizay@gmail.com	benli@neg@gmail.com	0	0	-	03.03.2025 13:15:42		
☒	Doğrulandı	İzleniyor	benli@neg@gmail.com	benli@neg@gmail.com	0	0	-	03.03.2025 13:15:43		
☒	Doğrulandı	İzleniyor	benli@neg@gmail.com	benli@neg@gmail.com	0	0	-	03.03.2025 13:15:41		
Gösterilen: 1 - 10 / 12										
Önceki 1 2 Sonraki										

Yeni E-posta Hesabı Nasıl Ekleyebilirim ?

Kişisel e-posta hesabı izleme kısmında bulunan “Yeni E-Posta Adresi Ekle” butonuna tıklayın.



Açılan pencerede izlemek istenen kişisel e-postanızı girerek kaydet tuşuna basabilirsiniz.

Yeni E-Posta Adresi Ekle

Durum

☒

E-Posta Adresi

E-Posta Bildirim Adresi

Bildirim Dili

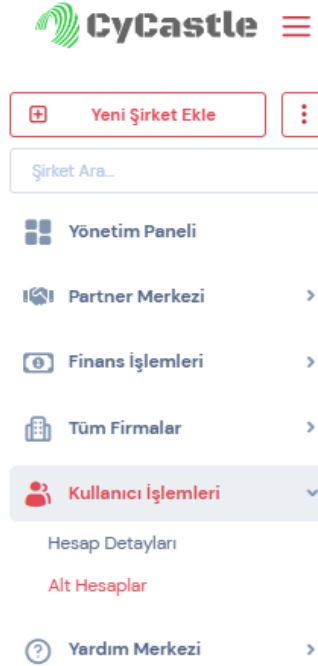
Türkçe

İptal

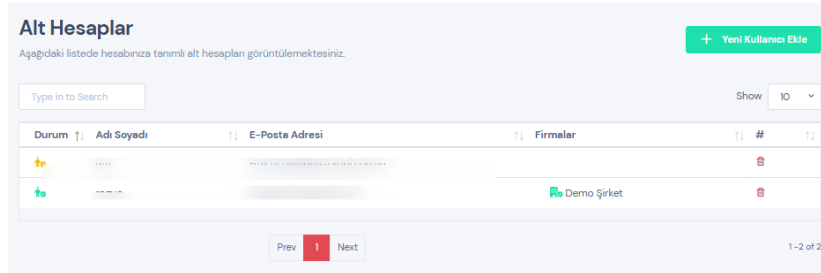
Kaydet

Nasıl Alt Hesap Ekleyebilirim ?

Menüden “**Kullanıcı İşlemleri**” kısmını açarak alt menülerden “**Alt Hesaplar**” kısmını seçiniz.



Alt Hesaplar sayfasında ekranın sağında bulunan “**Yeni Kullanıcı Ekle**” butonuna tıklayın.



Açılan pencerede gerekli alanları doldurduktan sonra e-postanıza gelen doğrulama işlemini başarıyla gerçekleştirdiğinizde alt kullanıcı hesabınız başarıyla eklenmiş olacaktır.

Hesabınıza Bir Alt Hesap Oluşturun

İsim Soyisim

E-Posta Adresi

E-Posta adresini doğru girdiğinize emin olun. Kullanıcı E-Posta Adresine gönderilen bir link aracılığıyla hesap bilgilerini kendisi oluşturacaktır.

İptal

Kaydet

Ardından mailinize gelen aktivasyonu onaylayarak işlemi tamamlayabilirsiniz.



Merhaba,

CYCastle tarafından izlenen Demo Şirket firmanıza ait aşağıda belirtilen e-posta adresiniz, olası bilgi sızıntılarına karşı izleme listesine eklenmek üzere işaretlenmiştir.

İzleme Listesine Eklenecek E-Posta Adresi: [REDACTED]

E-posta adresinize ait bir şifre veya hesap bilgisi sızıntısı yaşanması durumunda, size ihlal bildirimi gönderilecektir.

Bu hizmetten yararlanmaya devam etmek için e-posta adresinizi onaylamak adına aşağıdaki butona tıklamanız yeterlidir.

Aktivasyonu Onayla

Teşekkürler,
CYCastle Ekibi

Yeni Kullanıcı Nasıl Ekleyebilirim?

Menümüzdeki “Şirket Detayları” kısmına tıkladıktan sonra açılan pencerede ekranın sağında bulunan “Yeni Kullanıcı Ekle” butonuna tıklayınız.

Demo Şirket



Ürün Anahtarı

Zaman Dilimi
Europe/Istanbul

İletişim ve Fatura Bilgileri

Yetkili Kişi
Burak Kaya

E-Posta Adresi

Telefon Numarası

Şirket Ünvanı
Demo

Adres

[+ Yeni Kullanıcı Ekle](#)

Hesap Yöneticileri

Type in to Search

Show 10

Durum	Adı Soyadı	E-Posta Adresi	Yetki
✓	demo 2		Yönetici
✓	Burak Kaya		Yönetici
✓			Yönetici
✓			Yönetici

1-4 of 4

Sonrasında açılan pencerede kullanıcı bilgilerini girerek istenilen özellikleri aktif edebilirsiniz.

Yeni Kullanıcı Oluşturun

Adı Soyadı

E-Posta Adresi

E-Posta adresini doğru girdiğinizden emin olun. Kullanıcı E-Posta Adresine gönderilen bir link aracılığıyla hesap bilgilerini kendisi oluşturacaktır.

Yönetim Yetkisi

Yetkileri Sınırla

Özet

Şirket Detayları

Alan Adı Yönetimi Sayfasına Erişim

Alan Adı Yönetimi Ekle/Dogrula

ThreatChaser

ThreatChaser Web Tarama

ThreatChaser CTI

DDOS Simülasyonu

ThreatChaser 5651 Logger

ThreatChaser Hotspot

Oltalama Testi

ThreatChaser Patch Managment

SIEM Hizmeti

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

Engelle / İzin Ver

İptal

Kaydet

Şifremi Nasıl Değiştiririm?

1. Yol:

En kısa yoldan sayfaya ulaşmak için aşağıdaki linke tıklayın,

[Parola ve Güvenlik Ayarları](#)

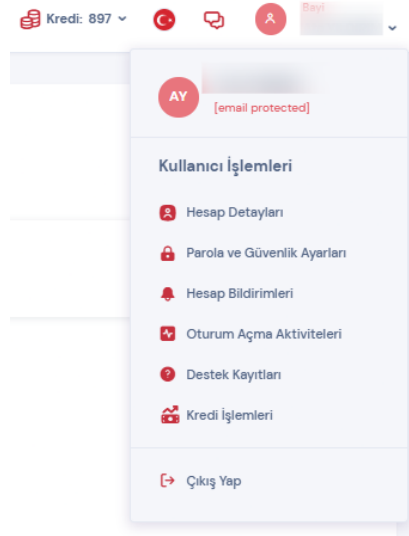
Açılan sayfada Şifre Değiştir butonuna tıklayın.

Karşınıza açılır pencere çıkacak, bu form alanında şu anki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir. Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

2. Yol:

Sitenin en üstünde bulunan Header Toolbar alanında “**Profil**” alanına tıklayın,

Aşağıya doğru açılan menüde “**Parola ve Güvenlik Ayarları**” linkine tıklayın.



Açılan sayfada “**Şifre Değiştir**” butonuna tıklayın.

Parola ve Güvenlik Ayarları

Hesap güvenliği ile ilgili ayarları bu sayfada bulabilirsiniz.

Şifre Değiştir

Hesabınızı korumak için benzersiz bir şifre belirleyin.

Şifre Değiştir

Karşınıza açılır pencere çıkacak, bu form alanında şu an ki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir.

Şifre Değişikliği

Şuanki Şifreniz

Yeni Şifreniz

× Şifreniz en az 8 karakter uzunluğunda olmalı
× En az bir büyük harf olmalı
× En az bir küçük harf olmalı
× En az bir rakam olmalı
× En az bir özel karakter olmalı @\$!%*?&

Yeni Şifrenizi Doğrulayın

[Şifreyi Güncelle](#) [İptal](#)

Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

3. Yol:

Şifrenizi değiştirmek için sol taraftaki menüde “**Kullanıcı İşlemleri > Hesap Detayları**” linkine tıklayın.

Açılan sayfada alt menü de “**Parola ve Güvenlik Ayarları**” linkine tıklayın.



[Yeni Şirket Ekle](#)

Şirket Ara...

Yönetim Paneli

Partner Merkezi

Finans İşlemleri

Tüm Firmalar

Kullanıcı İşlemleri

Hesap Detayları

Alt Hesaplar

Yardım Merkezi

AY

HESAP ID

1234567890

Hesap ve Profil Bilgisi

Parola ve Güvenlik Ayarları

Hesap Bildirimleri

Oturum Açma Aktiviteleri

Açılan sayfada “**Şifre Değiştir**” butonuna tıklayın.

Parola ve Güvenlik Ayarları

Hesap güvenliği ile ilgili ayarları bu sayfada bulabilirsiniz.

Şifre Değiştir
Hesabınızı korumak için benzersiz bir şifre belirleyin.

[Şifre Değiştir](#)

Karşınıza açılır pencere çıkacak, bu form alanında şu an ki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir.

Şifre Değişikliği

Şuanki Şifreniz

Yeni Şifreniz

- ✗ Şifreniz en az 8 karakter uzunluğunda olmalı
- ✗ En az bir büyük harf olmalı
- ✗ En az bir küçük harf olmalı
- ✗ En az bir rakam olmalı
- ✗ En az bir özel karakter olmalı @\$!%*?&

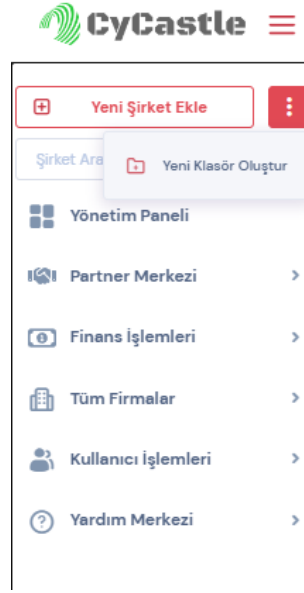
Yeni Şifrenizi Doğrulayın

Şifreyi Güncelleİptal

Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

Yeni Klasör Nasıl Oluştururum ve İçerisine Nasıl Şirket Ekleyebilirim?

Sol tarafta bulunan menü üzerindeki üç noktaya tıkladıktan sonra açılan “Yeni Klasör Oluştur” kısmına tıklıyoruz.



Açılan pencerede klasör adı belirttikten sonra eklemek istediğiniz şirketleri seçerek ortadaki butonlarla ekleyip çıkartabilirsiniz. Dilerseniz eklemek istediğiniz şirketi sürükleyip eklenen şirketler kısmına bırakabilirsiniz.

Yeni Klasör Oluşturun

Klasör Adı

Ark Klasörü

Search

Search

Eklenebilir Şirketler

ThreatChaser A.Ş.

Ark 2 Inc

Demo Şirket

>>

>

<

<<

Eklenen Şirketler

Ark Inc

* Yukarıdaki listede daha önce bir klasöre eklenmemiş şirketlerin listesini görebilirsiniz.

* Listedeki şirketinizi göremiyorsanız henüz aktif etmemiş olabilirsiniz.

* Eğer şirketinizi aktif ettiğiniz halde listede görmüyorsanız muhtemelen başka bir klasöre eklemiş olabilirsiniz.

* Bir klasöre eklenen şirket başka bir klasöre eklenemez.

* Eğer daha önce bir klasöre eklenen şirketi başka bir klasöre eklemek istiyorsanız, önce şirketi o klasörden çıkartmalısınız.

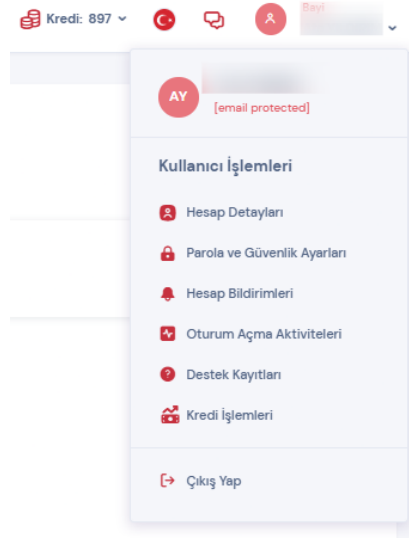
İptal

Kaydet

Oturum Açma Aktivitelerimi Nasıl Görebilirim ?

Sitenin en üstünde bulunan Header Toolbar alanında “**Profil**” linkine tıklayın,

Aşağıya doğru açılan menüde “**Oturum Açma Aktiviteleri**” linkine tıklayın.



Açılan pencerede hesabınızla yapılmış oturum açma girişimlerini görüntüleyebilirsiniz.

Oturum Açma Aktiviteleri

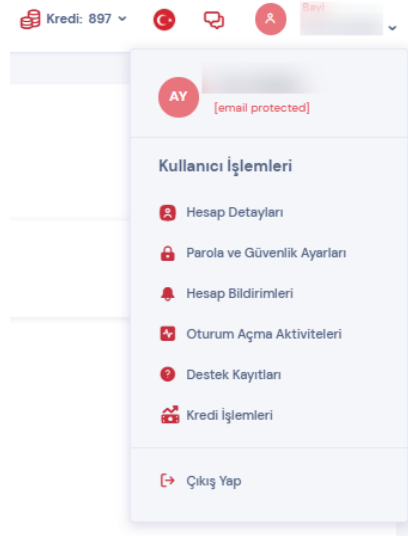
Hesabınıza son giriş yaptığınız 20 kayıt aşağıda listelenmektedir. ⓘ

DURUM	TARAYICI	IP ADRESİ	TARİH
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		04.03.2025 10:47:56
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:44:42
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:43:19
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:15:37
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:11:36
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 12:23:09
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 11:51:00
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 11:49:39
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 10:25:12
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		27.02.2025 16:49:51
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		27.02.2025 16:24:12
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 15:51:59
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 15:48:21
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 10:56:34
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		25.02.2025 16:29:14
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		25.02.2025 15:07:07
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		24.02.2025 09:35:30
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		18.02.2025 11:28:50
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		17.02.2025 10:37:20
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		14.02.2025 14:56:59

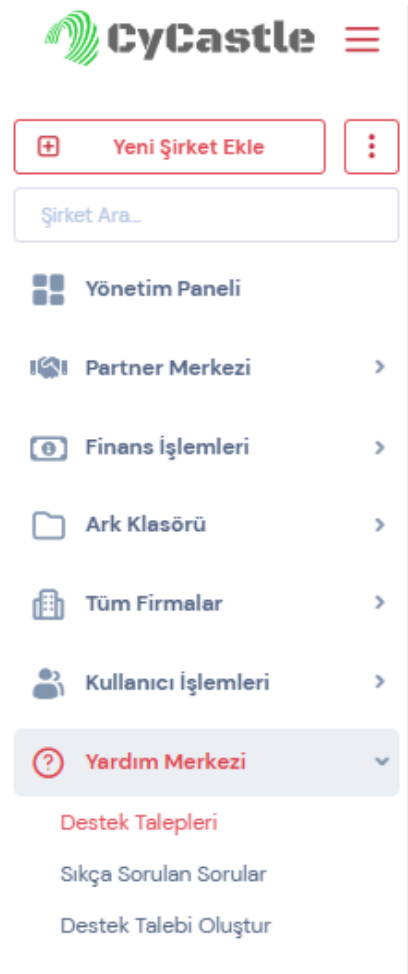
Destek Kaydı Nasıl Oluşturabilirim ?

Sitenin en üstünde bulunan Header Toolbar alanında “**Profil**” linkine tıklayın,

Aşağıya doğru açılan menüde “**Destek kayıtları**” linkine tıklayın.



Diğer bir yol ise sol menüdeki “**Yardım Merkezi**” altındaki “**Destek Talepleri**” kısmına tıklamanız.



Açılan ekranda “Yeni Bir Destek Talebi Oluştur” butonuna tıklayınız.



Destek Talebi Bulunamadı!

Hiç destek talebiniz bulunmamaktadır. Aşağıdaki butona tıklayarak bir destek talebi oluşturabilirsiniz.

[Yeni Bir Destek Talebi Oluştur](#)

Formdaki gerekli alanları doldurduktan sonra gönderme butonuna basarak işleminizi tamamlayabilirsiniz.

[← Sıkça Sorulan Sorular](#)

Yeni Destek Talebi

Aşağıdaki form aracılığıyla bizimle iletişime geçebilirsiniz. Yaşadığınız problemi ayrıntılı bir şekilde yazabilir, varsa bir görsel veya metin belgesi paylaşabilirsiniz.

Destek Talebi Formu

Destek Kategorisi

Bir Kategori Seçin

Destek Konusu

Destek Konusunu Bu Alana Yazabilirsiniz.

Destek İçeriği

Yaşadığınız problemi ayrıntılı bir şekilde yazabilirsiniz.

Problemin Yaşandığı Şirket Hesabı

Bir Şirket Seçin

Dosya Ekleri

Dosya Seçin

Browse

Yaşadığınız problem bir firma ile ilgili değilse bu alanı boş bırakın!

[Destek Talebini Gönder](#)

Destek taleplerinizi yine aynı sayfadan görüntüleyebilirsiniz.

AY

Lisans Hatası

04.03.2025 13:43:36

Yazılım

Çözüm Bekleniyor

AY

Diğer

04.03.2025 12:21:44

Çözüm Bekleniyor

Lisans Hatası

Yazılım

✓ Çözüm bulundu Olarak İşaretle

AY

04.03.2025 13:43:36

Lisansınız başka bir yazılım tarafından kullanılıyor hatası nedir?

1 Dosya Ekl

Tümünü İndir

Cevap Yaz

Cevaplayan: AY

Bir Cevap Yazın...

Gönder

Destek Kaydı Oluştur

AY

Bayı

KULLANICI BİLGİLERİ

✉

☎

📍 İstanbul

DESTEK BİLGİLERİ

Referans ID: SID-5

Talep Eden:

Çözüm Bekleniyor

Durum:

Çözüm Bekleniyor

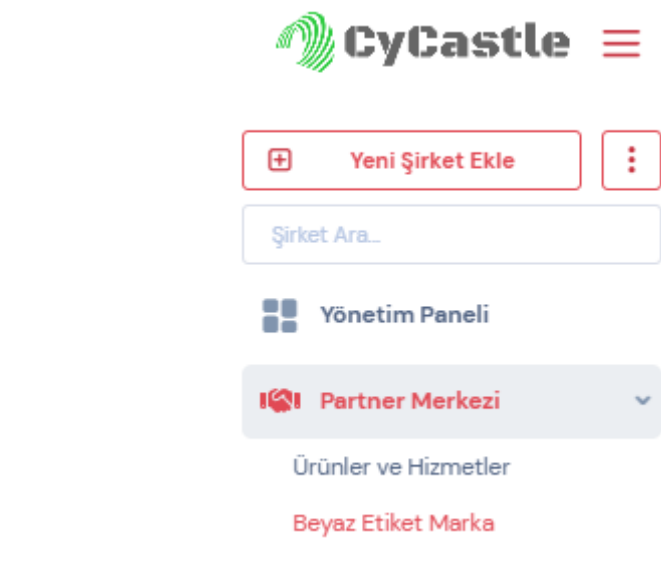
Destek: Yazılım

Kategori:

Beyaz Etiket (White Label) Ayarlarını ve Logonuzu Nasıl Özelleştirebilirsiniz?

Bilgilendirme : Whitelabel hizmeti sadece bayilerimiz tarafından kullanılabilir.

Sol tarafta bulunan menüde “Partner Merkezi” altındaki “Beyaz Etiket Marka” kısmına tıklayınız.



Ekranınızın sağ üstünde bulunan “Düzenle” butonuna tıklayarak markanızı özelleştirmeye başlayabilirsiniz.

Beyaz Etiket

Beyaz Etiket (White-Label) yöntemi ile alan adınızı yönlendirerek yönetim panelini özelleştirebilir, logo, site adı gibi ayarları değiştirerek platformu firmanızın kimliğine uygun hale getirebilirsiniz. Bu sayede, müşterilerinize tamamen size ait bir platform deneyimi sunabilirsiniz.

Özelleştirilebilir Alanlar

Düzenle

Kaldır

Logo

Favicon

Filigran

Bilgi: Filigran eklemeniz durumunda raporlarınızda son sayfada bu görsel görülmeyecektir. Arka plan rengi transparan olmalıdır.

Şirket Adı

CyCastle

E-Posta Adresi:

info@cycastle.com

Alan Adı:

cloud.cycastle.com

CNAME:

whitelabel.cycastle.com

Önemli Bilgi: Alan adınızın aktif olması için yukarıdaki CNAME adresine ilgili alan adınızı yönlendirmeniz gerekmektedir.
Örnek CNAME: cloud.sizinsiteniz.com => whitelabel.cycastle.com

Durum

Pasif

SSL Sertifika Bilgileri

Önemli Bilgiler

- Logo ve Favicon eklemeniz durumunda firmanızın sitenizdeki tüm alanlarda görüntülenecektir.
- Logo maksimum 175px genişliğe sahip olması gerekmektedir. Yükseklik isteğinize göre değişebilir. Yükseklik 50px geçmemesi tavsiye edilir.
- Favicon uzantısı .ico formatında olmalıdır. Farklı formatta görseliniz varsa online ico converter sitelerinden ilgili görseli .ico formatına çevirmelisiniz.
- Alan Adı kayıtlarının Root DNS sunucuları arasında değişimi bazen 48 saati bulabilir. Yukarıdaki Alan Adı için CNAME kayıtlarını yönlendirdiğinizde emin olun.
- Alan Adı kayıtları sürekli kontrol edilmektedir. DNS kayıtları doğru şekilde yönlendirildiğinde otomatik sistem aktif olur.
- Alan Adı kayıtları tamamlandıktan sonra ilgili alan adı için ücretsiz SSL sertifikası oluşturulmaktadır.
- Alan Adı CloudFlare, Amazon AWS vb. Proxy hizmetleri tarafından korunuyorsa Proxy özelliğini kapatmanız gerekmektedir. Aksi durumda CNAME adresi doğrulanamaz.
- CloudFlare Proxy ve DNS hizmeti alan müşterilerimizin bize bildirmeleri gereklidir. CloudFlare politikası gereği, birden fazla farklı hesaptan iç içe yönlendirme yapılması durumunda size ekstre oluşturacağımız DNS kayıtlarını eklemeniz gerekmektedir.
- Sunucularımız CloudFlare tarafından korunmaktadır.

Dikkat Edilmesi Gerekenler :

- Logo ve favicon eklemeniz durumunda, firmanıza ait logo tüm alanlarda görüntülenecektir.
- Logonun maksimum genişliği 175px olmalıdır. Yükseklik isteğinize göre değişebilir, ancak 50px'i geçmemesi tavsiye edilir.
- Favicon dosyanız .ico formatında olmalıdır. Eğer farklı bir formatta görseliniz varsa, online ico converter araçlarını kullanarak uygun formata dönüştürebilirsiniz.
- Alan adı kayıtlarının root DNS sunucuları arasında dağıtılması bazen 48 saate kadar sürebilir. Yukarıdaki alan adı için CNAME kayıtlarını doğru şekilde yönlendirdiğinizden emin olun.
- Alan adı kayıtları düzenli olarak kontrol edilmektedir. DNS kayıtları doğru yapılandırıldığında, sistem otomatik olarak aktif hale gelir.
- Alan adı kaydı tamamlandıktan sonra, ilgili alan adı için ücretsiz SSL sertifikası oluşturulacaktır.
- Eğer alan adınız Cloudflare, Amazon AWS gibi proxy hizmetleri tarafından korunuyorsa, proxy özelliğini devre dışı bırakmanız gerekir. Aksi durumda, CNAME kaydı doğrulanamaz.
- Cloudflare proxy ve DNS hizmeti kullanan müşterilerimizin durumu bize bildirmesi gerekmektedir. Cloudflare politikaları gereği, birden fazla hesaptan iç içe yönlendirme yapılması durumunda, sizinle ek olarak paylaşacağımız DNS kayıtlarını sisteme eklemeniz gerekecektir.
- Sunucularımız Cloudflare koruması altındadır.

Gerekli düzenlemeleri yaptıktan sonra “Kaydet” butonuna tıklayarak işlemi gerçekleştirebilirsiniz.

Markanızı Özelleştirin

Logo

Favicon

Watermark

Logo

Favicon

Watermark

Şirket Adı

CyCastle

Bilgi: Şirket Adı alanını doldurun. Rapor üzerinde şirketinizin adı görünecektir.

E-Posta Adresi

info@cycastle.com

Bilgi: E-Posta alanını doldurun. Rapor üzerinde şirketinize ait E-Posta adresi görünecektir.

Alan Adı

cloud.cycastle.com

Önemli Bilgi: Alan Adının başına http:// ve https:// olmadan yazmanız gerekmektedir.

Örnek Alan Adı: sizinsiteniz.com veya cloud.sizinsiteniz.com

CNAME

whitelabel.cycastle.com

Önemli Bilgi: Yukarıdaki DNS kaydını yönlendirmek istediğiniz alan adına CNAME olarak eklemeniz gerekmektedir.

Örnek CNAME: cloud.sizinsiteniz.com => whitelabel.cycastle.com

Logo

Choose File

No file chosen

Favicon

Choose File

No file chosen

Watermark

Choose File

No file chosen

Bilgi: Watermark görseliniz raporlarınızın arka planında filigran olarak görüntülenecektir.

İptal

Kaydet

5651 Loglama ve HotSpot Hizmetini Nasıl Aktif Edebilirim?

Her bir 5651 loglama hizmeti için bir adet hotspot kullanım hakkınız bulunmaktadır.

Web taraması başlatmak istediğiniz şirketin menüsünde yer alan “**ThreatChaser 5651 Log ve HotSpot Hizmeti**” bölümüne gidiniz “**Yeni Log Hizmeti Ekle**” Butonuna tıklayın.



Yeni Şirket Ekle

Şirket Ara...

Yönetim Paneli

Finans İşlemleri

Tüm Firmalar

CyCastle Demo Şirket

Kullanıcı İşlemleri

Yardım Merkezi

Özet

Şirket Detayları

Alan Adı Yönetimi

ThreatChaser

ThreatChaser Web Tarama

ThreatChaser CTI

ThreatChaser 5651 Log ve HotSpot Hizmeti

New

ThreatChaser SSL Kontrol Aracı

New

ThreatChaser VPN Hizmetleri

New

ThreatChaser 5651 Log Hizmeti

Aşağıdaki Listede ThreatChaser 5651 Log Hizmetlerini Görüntülemektesiniz. Bu hizmet ile 5651 Log Kayıt Hizmetini Aktif Edebilir, Düzenleyebilirsiniz.

[Yeni Log Hizmeti Ekle](#)

Başlık: 5651 Log Hizmetinin Adı

Seri Numarası: Syslog gönderecek cihazın seri numarasını giriniz.

Ürün: 5651 Logunu tutmak istediğiniz ürünü seçiniz.

Model: 5651 Logunu tutacağınız ürünün modelini belirtiniz.

Syslog Portu: Syslog gönderen cihazda tanımlı portu giriniz.

5651 Log Hizmeti Oluştur



Şirket Ünvanı

CyCastle Demo Şirket

Başlık

CyCastle Gebze

Seri Numarası

Syslog Gönderecek Cihazınızın Seri Numarası

Ürün

FortiGate



Model

FG-40F



Lisans Süresi

1 Ay

Her Ay Yenilenir



Syslog Port

516

5651 Log Depolama
Süresi

24 Ay (Devletin Zorunlu Tuttuğu Süre)



Web Raporu
Depolama Süresi

6 Ay



Kredi Bilgileri

Aşağıda mevcut krediniz ve harcanacak kredi miktarını görebilirsiniz.

Toplam Kredi

100

Gereken Kredi

4

Başlangıç Tarihi

24.06.2025

Bitiş Tarihi

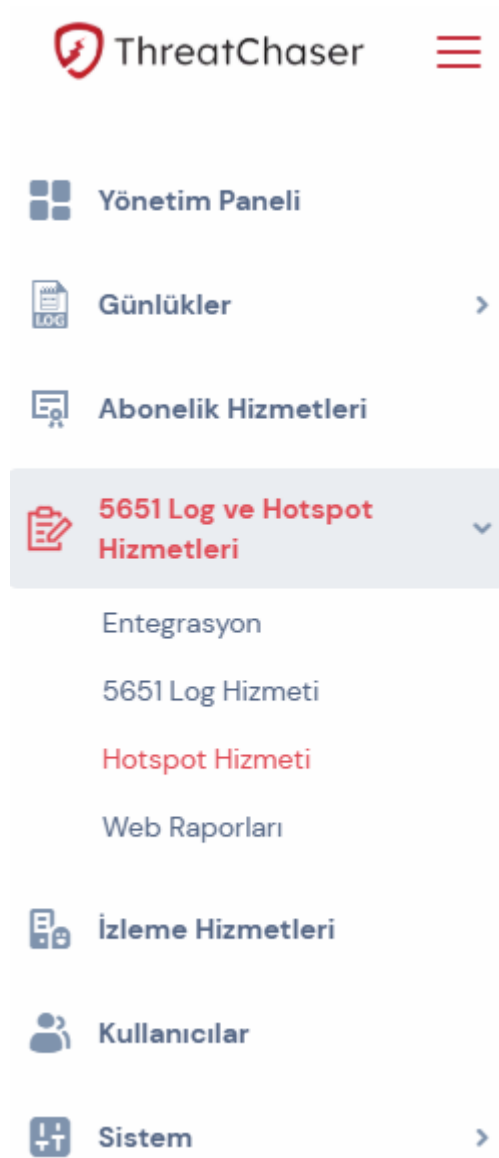
24.07.2025

İptal

Kaydet

Hotspot Hizmetini Aktif hale getirmek için ThreatChaser'ın web arayüzüne giriş yapınız

5651 Log ve Hotspot Hizmetleri -> Hotspot Hizmeti



“Yeni Hostpot Hizmeti Ekle” Butonuna tıklayınız

Kullanılabilir hizmetler arasından hotspot yayını yapmak istediğiniz cihazı seçiniz

HotSpot yayını yapmak istediğiniz port numarasını belirtiniz

HotSpot oturum süresini belirtiniz

FortiGate tarafında oluşturduğunuz Misafir Grubu ismini giriniz

Yönlendirme linkini belirtiniz

Yeni Hotspot Hizmeti Ekle



Durum



Pasif/Aktif

Kullanılabilir
Hizmetler

Fortigate - FGT60FTK20030352



Port

7558

Oturum Süresi

1440

dakika

Misafir Grubu

ThreatChaserGuest

Yönlendirme Linki

https://www.google.com

İptal

Kaydet

Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

Watchguard Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

Watchguard Cihazınıza Web Arayüzü üzerinden giriş yapın

System -> Logging -> Syslog Server menüsüne gidin

“Send log messages to these Syslog servers” kutucuğunu işaretleyin

“Add” Butonuna Tıklayınız

The screenshot displays the WatchGuard Fireware Web UI. The left sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, SYSTEM, Information, Feature Key, NTP, SNMP, NetFlow, WatchGuard Cloud, Managed Device, Logging, Diagnostic Log, Global Settings, Certificates, Proxy Auto-Configuration, Upgrade OS, Backup and Restore Image, Technology Integrations, Users and Roles, Configuration File, Support Access, Logon Disclaimer, and About. The 'SYSTEM' menu item is highlighted with a red arrow. The 'Logging' sub-menu item is also highlighted with a red arrow. The main content area shows the 'Syslog Server' tab selected, indicated by a red arrow. The 'Send log messages to these syslog servers' checkbox is checked. Below this, there is a table with columns for 'IP ADDRESS' and 'PORT'. An 'ADD' button is located next to the table, and a 'SAVE' button is at the bottom of the page.

“IP Address” bölümüne ThreatChaser’ın ip adresini giriniz

Syslog Server



IP Address	ThreatChaser IP Adresi
Port	514
Log Format	Syslog
Description	



Select the details to include in syslog messages:

- ☐ The time stamp
- ☐ The serial number of the device

Select the syslog facility for each type of device log message:

Alarm	Local0
Traffic	Local1
Event	Local2
Diagnostic	Local3
Performance	Local4

[RESTORE DEFAULTS](#)

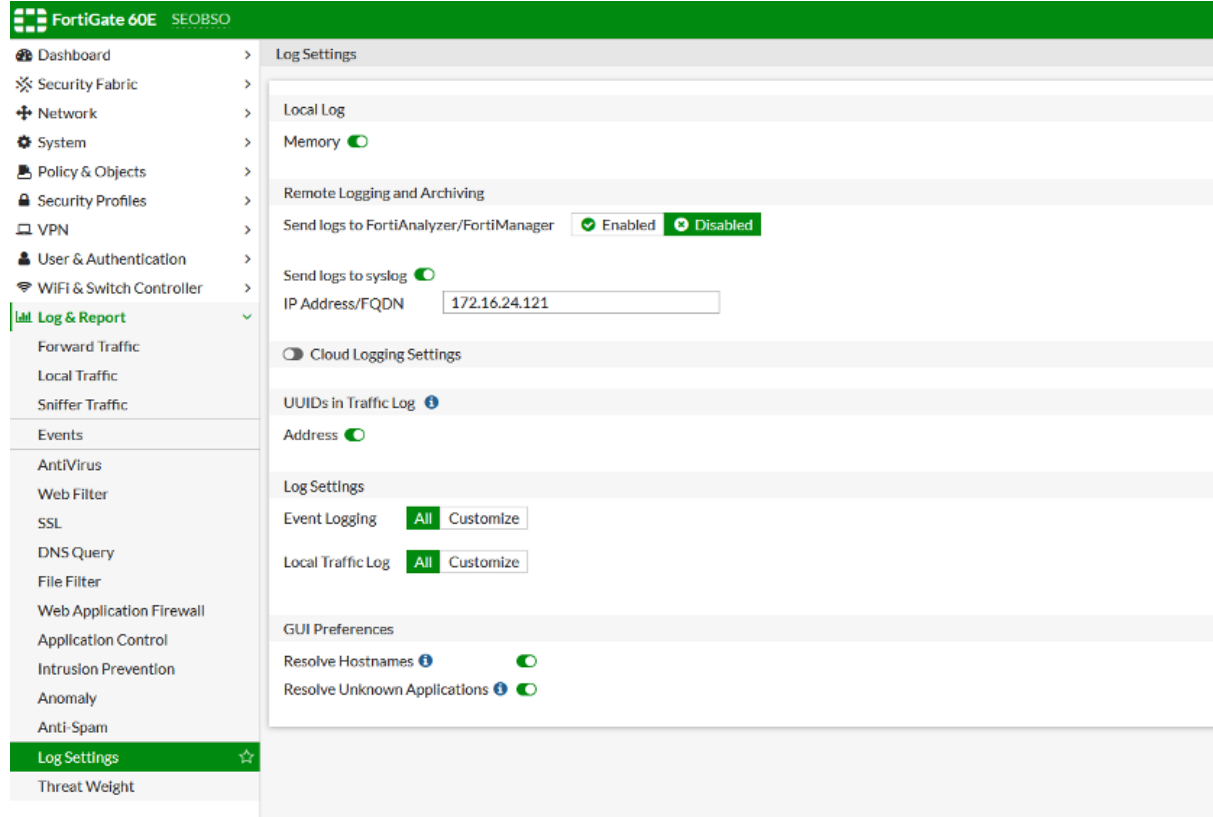
OK

CANCEL

FortiGate Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

FortiGate Cihazınıza Web Arayüzü üzerinden giriş yapın

Log & Report > Log Settings sayfasına gidin.



“Send logs to Syslog” aktif edilir ve ThreatChaser ip adresi bu alana girilir.

Event Logging “All” seçilir.

Local Traffic Log “All” seçilir.

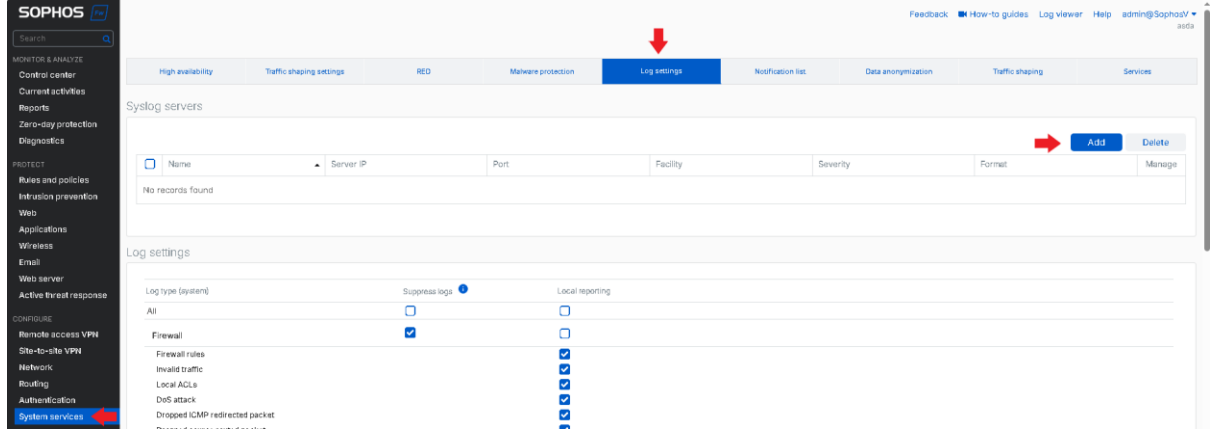
“Apply” butonuna basılarak bu işlem bitirilir.

Sophos Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

Sophos Cihazınıza Web Arayüzü üzerinden giriş yapın

CONFIGURE & System services > Log settings sayfasına gidin.

“Add” Butonuna tıklayın



Name *

ThreatChaser

IP address / Domain *

ThreatChaser Ajanının IP Adrsi

Secure log transmission

☐

Port *

Port

Facility *

DAEMON

Severity level *

Debug

Format *

Standard syslog protocol

“IP Address” bölümüne ThreatChaser’ın ip adresini giriniz.

“PORT” bölümüne cloud.cycastle.com üzerinden belirlediğiniz port numarasını giriniz.

“Facility” bölümünde DAEMON seçeneğini işaretleyiniz.

“Severity” “Level bölümünde Debug seçeneğini işaretleyiniz.

“Format” bölümünde Standart Syslog Protocol seçeneğini işaretleyiniz.

Tüm ayarları yaptıktan sonra Save butonuna basarak işlemi tamamlayınız.

CONFIGURE & System services > Log settings sayfasından eklediğiniz Syslog sunucusunda “All” seçeneğini işaretleyerek tüm logların gönderilmesini sağlayınız.

Syslog servers

☐	Name	Server IP	Port	Facility
☐	ThreatChaser	192.168.100.3	520	DAEMON

Log settings

Log type (system)	Suppress logs ⓘ	Local reporting	ThreatChaser
All	☐	☐	 ☒
Firewall	☒	☐	☒
Firewall rules		☒	☒
Invalid traffic		☒	☒
Local ACLs		☒	☒
DoS attack		☒	☒
Dropped ICMP redirected packet		☒	☒
Dropped source routed packet		☒	☒
Dropped fragmented traffic		☒	☒
MAC filtering		☒	☒
IP-MAC pair filtering		☒	☒
IP spoof prevention		☒	☒
SSL VPN tunnel		☒	☒
Protected application server		☒	☒
Heartbeat		☒	☒
ICMP error message		☒	☒
Private ACLs		☒	☒

Apply

AIMdefense Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

AIM Defence Cihazınıza Web Arayüzü üzerinden giriş yapın

System -> Settings -> General Sayfasına gidin.

“Time Zone” bölümünden bulunduğunuz bölgeyi seçiniz

The screenshot shows the AIMdefense web interface. On the left is a sidebar menu with the following items: Lobby, Reporting, System (expanded), Firmware, Settings (with a gear icon), Administration, Cron, General (highlighted), Logging, AIMdefense Menuchanger, Miscellaneous, Tunables, Snapshots, Wizard, Log Files, and Diagnostics. The main content area is titled "System: Settings: General". It contains a "System" section with the following settings: Hostname (AIM), Domain (s2f.local), Time zone (Europe/Istanbul), Language (English), Theme (AIMdefense-light), and Picture (Dosya Seç | Dosya seçilmedi). Below this is a "Networking" section.

System > Logging > Remote sayfasına gidin.

The screenshot shows the AIMdefense web interface with the System menu expanded. The "Logging" option is highlighted in the sidebar. The main content area is currently empty, showing only the top header and the sidebar.

System: Settings: Logging

Local

Remote

Statistics

☐ Enabled Transport

«

<

1

>

»

Apply

“+” Butonuna Tıklayın

Q

Search

↺

7

≡

Commands

+

🗑

Showing 0 to 0 of 0 entries

Reset Log Files

Applications, Levels ve Facilities bölümlerinde “Select All” seçeneğini seçiniz

“Hostname” bölümüne ThreatChaser’ın ip adresini giriniz.

“PORT” bölümüne cloud.cycastle.com üzerinden belirlediğiniz port numarasını giriniz.

Tüm ayarları tamamladıktan sonra “Save” butonuna basarak işlemi kaydediniz. Ardından, ayarların geçerli olabilmesi için “Apply” butonuna tıklayınız.

Edit destination

full help

Enabled

☒

Transport

UDP(4)

Applications

audit (audit), configd (configd.py), ddclient (ddclient)

Clear All

Select All

Levels

debug, info, notice, warn, error, critical, alert, emerge

Clear All

Select All

Facilities

kernel messages, user-level messages, mail system, s

Clear All

Select All

Hostname

10.1.253.111

Port

514

System: Settings: Logging

Local

Remote

Statistics

Enabled

Transport

☒

UDP(4)

<<

<

1

>

>>

Apply

FortiGate API İşlemleri

Aşağıdaki gibi bir profil oluşturunuz

System -> Administrators Sayfasına gidin

Açılan sayfada yeni bir API kullanıcısı oluşturuyoruz.

Administrator Profile kısmında oluşturduğumuz API profilini seçiyoruz.

Trusted Hosts kısmında ThreatChaser yazılımının IP adresini yazıyoruz.

Önemli Not: Burada bize verilen API key bilgisini ThreatChaser ayarlarına kayıt edeceğiz.

FortiGate 60FFortiGate-60F

Favorites

>

Dashboard

>

Security Fabric

>

FortiView

>

Network

>

System

>

Administrators

>

Admin Profiles

>

Firmware

>

Settings

>

HA

>

SNMP

>

Replacement Messages

>

FortiGuard

>

Feature Visibility

>

Policy & Objects

>

Security Profiles

>

VPN

>

User & Device

>

WiFi & Switch Controller

>

Log & Report

>

Monitor

>

New REST API Admin

Username

ThreatChaserAPI

Comments

0/255

Administrator Profile

ThreatChaser_API

PKI Group

REST API clients must use client certificate authentication. Only certificates from this PKI group will be authorized.

CORS Allow Origin

Restrict login to trusted hosts

Trusted Hosts

10.1.253.111/32

OK

Cancel

FortiGate Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



 Yönetim Paneli

 Günlükler >

 Abonelik Hizmetleri

 **5651 Log ve Hotspot Hizmetleri** v

Entegrasyon

5651 Log Hizmeti

Hotspot Hizmeti

Web Raporları

 VPN Hizmeti

 İzleme Hizmetleri

 Kullanıcılar

 Sistem >

Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

“IP Adresi” bölümüne FortiGate’in ip adresini giriniz.

“GUI Port” bölümüne FortiGate’in port numarasını giriniz.

“API Anahtarı” bölümüne FortiGate’te oluşturduğunuz API Anahtarını giriniz.

“Misafir Grubu” Bu bölümün User Groups menüsüne eklediğiniz isimle aynı olması gerekiyor.

“Radius Şifresi” Bu bölüme FortiGate’in ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.

“Radius Adı” Bu bölümün FortiGate tarafında Radius Server ismiyle aynı olması gerekiyor.

Entegrasyonu Düzenle

 **Ayarlar**

Cihaz Senkronizasyonu  → 

Ürün	FortiGate
Model	FG-60F
Seri Numarası	FGT60FTK20083923
IP Adresi	10.1.253.1
GUI Port	443
API Anahtarı	 
Misafir Grubu	ThreatChaserGuest
Radius Şifresi	 
Radius Adı	ThreatChaserRadius

Bilgi: Radius bağlantısı kurulmadığı durumlarda, FortiGate konsol ekranında source-ip tanımını yapmanız gerekmektedir.

İptal

Kaydet

Eğer FortiGate tarafında kullanıcı grubunu oluşturmak ve RADIUS yapılandırmasını otomatik olarak yapmak istiyorsanız, bu işlemi Cihaz Senkronizasyonu üzerinden gerçekleştirebilirsiniz.

Not: Bu işlemi manuel yapmak istiyorsanız, bu adımı atlayabilirsiniz.

Entegrasyonu Düzenle

 Ayarlar

Cihaz Senkronizasyonu  → 

IP Adresi	10.1253.1
GUI Port	443
API Key	 
Radius Secret	 
Misafir Grubu	ThreatChaserGuest
Radius Adı	ThreatChaserRadius

☒ Kullanıcı Grubunu Oluştur

☒ Radius İstemcisini Yapılandır

Senkronizasyonu Başlat

Bilgi: Entegrasyon ayarlarında değişiklik yapmanız durumunda geçerli olması için formu kayıt etmeniz ve daha sonra bu işlemi yapmanı gereklidir. Güncel bilgiler yukarıda belirtilmiştir.

İptal

Kaydet

Firewall Tarafındaki Ayarlamalar

FortiGate Cihazınıza Web Arayüzü üzerinden giriş yapın

User & Device -> RADIUS Server menüsüne gidin

“Create New” Butonuna tıklayın

Name: Oluşturduğunuz RADIUS server'ına bir isim verin

IP Adresini kısmına ThreatChaser'ın ip adresini giriniz

ThreatChaser'ın Radius ile haberleşmesi için bir şifre oluşturun. Bu şifre ThreatChaser Entegrasyon bölümünde girdiğiniz Radius Şifresi ile aynı olması gerekmektedir.

FortiGate 60F FortiGate-60F

★ Favorites > New RADIUS Server

📊 Dashboard >

🔒 Security Fabric >

🏠 FortiView >

🔌 Network >

⚙️ System >

📁 Policy & Objects >

🔒 Security Profiles >

🖥️ VPN >

👤 User & Device >

👤 User Definition

👤 User Groups

👤 Guest Management

📁 Device Inventory

📁 LDAP Servers

★ RADIUS Servers

⚙️ Authentication Settings

📶 FortiTokens

📶 WiFi & Switch Controller >

📊 Log & Report >

📊 Monitor >

Name ThreatChaser

Authentication method Default Specify

NAS IP

Include in every user group ☒

Primary Server

IP/Name 10.1.253.111

Secret

Connection status ☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK Cancel

New Address

Select Ent

Search

ADDR

Benim

Cloud

FABRI

gmail

HotSp

intern

login

login

login

SSLVP

tckim

Threat

Category Address IPv6 Address Multicast Address Proxy Address

Name ThreatChaserSrv

Color Change

Type Subnet

IP/Netmask 10.1.253.111/32

Interface any

Show in address list ☒

Static route configuration ☐

Comments Write a comment... 0/255

OK Cancel

ThreatChaser için yeni bir adres oluşturunuz

User & Devices -> User Groups menüsüne gidin

“Create New” butona tıklayın

Name kısmına oluşturacağınız grup için bir isim belirleyiniz daha sonra bu ismi threatchaser ayarlarında belirtmeniz gerekecek

Type kısmını Firewall olarak seçiniz

Remote Groups başlığının altındaki “Add” butonuna tıklayınız

FortiGate 60F FortiGate-60F

- ★ Favorites >
- Dashboard >
- Security Fabric >
- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
- VPN >
- User & Device** >
 - User Definition
 - User Groups** ☆
 - Guest Management
 - Device Inventory
 - LDAP Servers
 - RADIUS Servers
 - Authentication Settings
 - FortiTokens
- WiFi & Switch Controller >
- Log & Report >
- Monitor >

New User Group

Name: ThreatChaserGuestUser

Type: Firewall

Members: +

Remote Groups

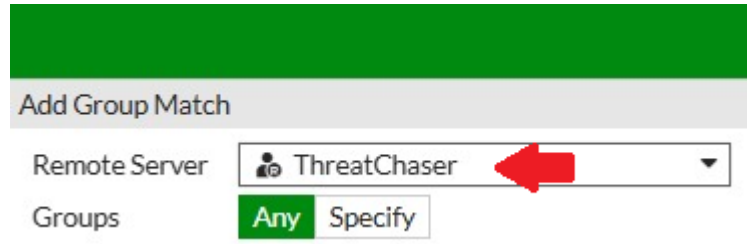
+ Add Edit Delete

Remote Server Group Name

No results

0

Sağ tarafta açılan sayfada oluşturduğunuz RADIUS Server'ı seçiniz



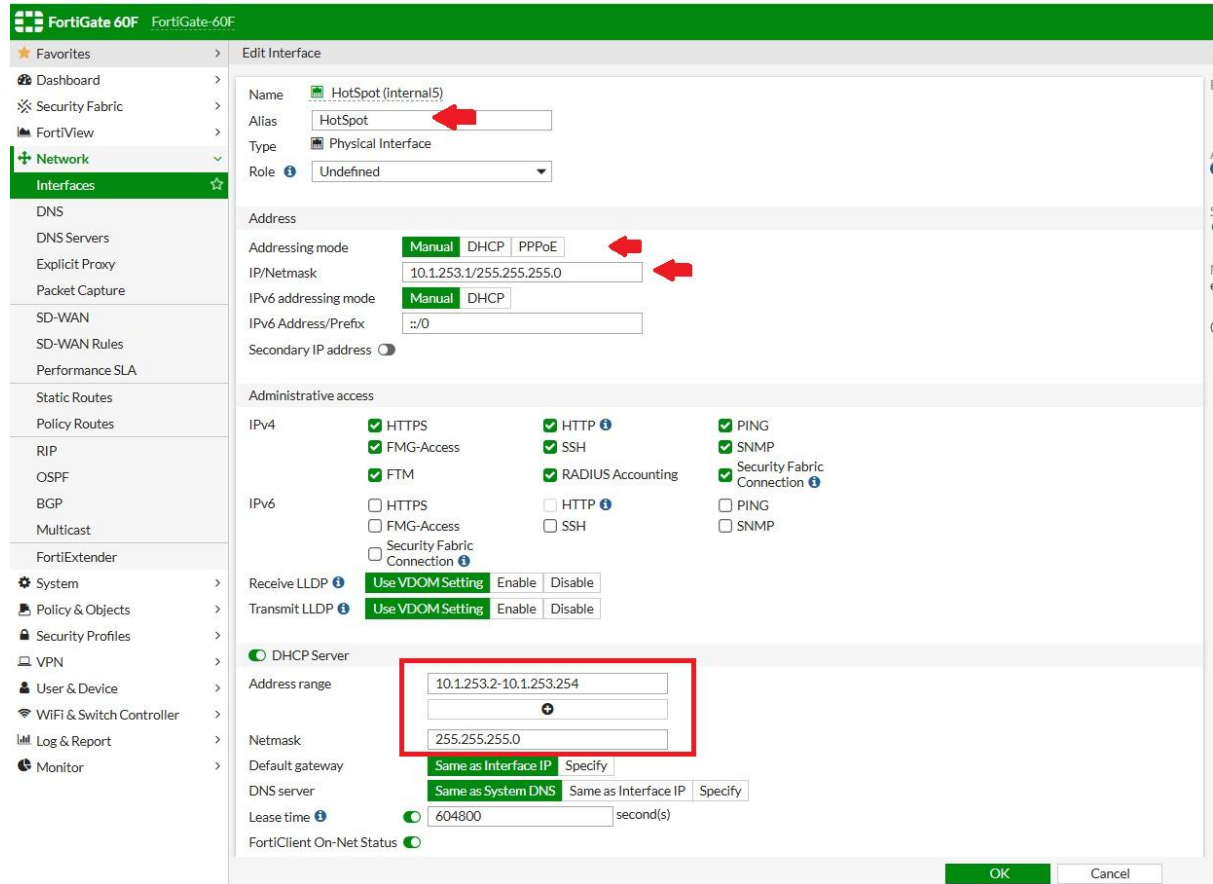
Network – Interface menüsüne gidin

HotSpot yayını yapacağınız interface'i düzenleyiniz

Alias bölümüne bir takma ad giriniz

Address bölümüne hotspot yayınında kullanmak istediğiniz ip ve netmask bilgilerini giriniz

DHCP Server bölümünde hotspot ip aralığınızı belirtiniz



Network kısmından

Security Mode'u aktif hale getirin ve Captive Portal'ı seçin

Authentication Portal'ı External olarak seçiniz

URL olarak <http://ThreatChaser/IPAdresi:PortNumarasi/auth> değerini giriniz

User Access'i Restricted to Groups olarak seçiniz

User Group kısmına daha önceden oluşturduğumuz grubu seçiniz

Exempt sources bölümünde threatchaser ürününün internete çıkabilmesi için izin verin

Exempt destinations/services ise eğer threatchaser ürünü farklı bir ağda ise hotspot ağındaki cihazların thraetchaser'a erişebilmesi için bu bölüme eklemeniz gerekmektedir

Redirect after Captive Portal kısmından "Specific URL" seçiniz

URL olarak <http://ThreatChaserIPAdresi:PortNumarası/redirect> değerini giriniz

Network

Device detection ☐

Explicit web proxy ☐

Security mode ☒ Captive Portal

Authentication portal ☐ Local ☒ External

User access ☒ Restricted to Groups ☐ Allow all

User groups ThreatChaserGuest

Customize portal messages ☐

Exempt sources ThreatChaserSrv

Exempt destinations/services CloudFlare ThreatChaserSrv

Redirect after Captive Portal ☐ Original Request ☒ Specific URL

Traffic Shaping

Outbound shaping profile ☐

Miscellaneous

Comments 0/255

Status ☒ Enabled ☐ Disabled

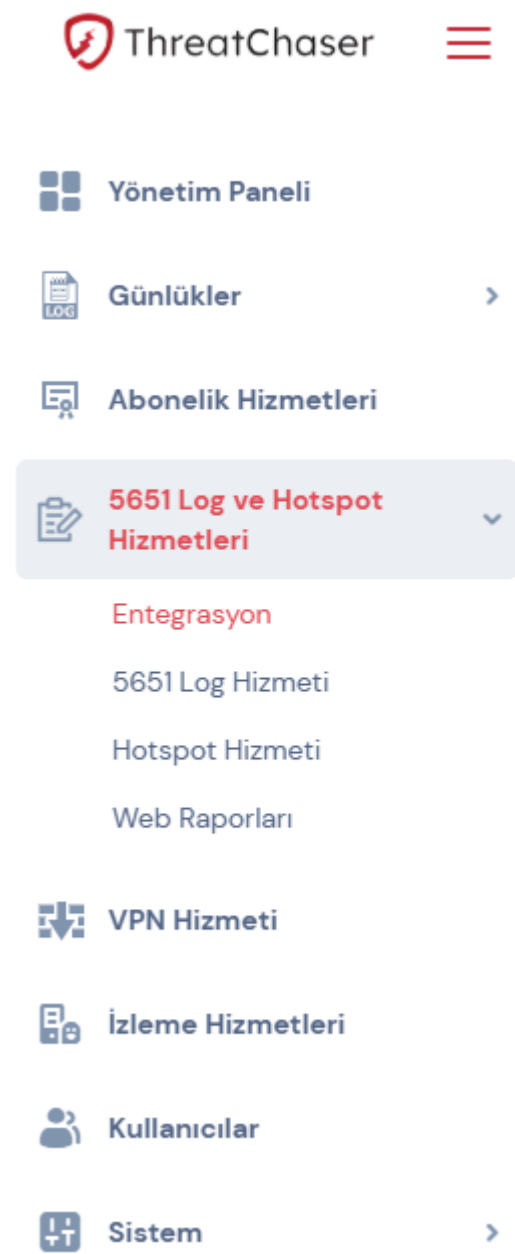
OK Cancel

Sophos Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

“IP Adresi” bölümüne Sophos’un ip adresini giriniz.

“Misafir Grubu” Bu bölümün Authentication -> Groups menüsüne eklediğiniz isimle aynı olması gerekiyor.

“Radius Şifresi” Bu bölüme Sophos’un ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.

Entegrasyonu Düzenle

Ayarlar

Ürün

Sophos

Model

SG105

Seri Numarası

V010016BWW9T709

IP Adresi

172.16.16.16

Misafir Grubu

ThreatChaserGuest

Radius Şifresi

.....

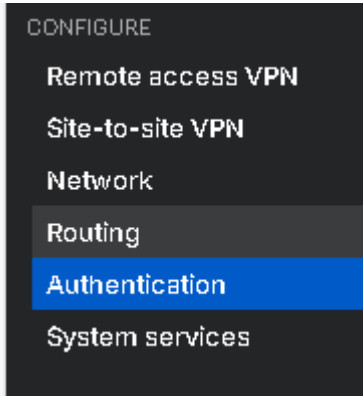
İptal

Kaydet

Firewall Tarafındaki Ayarlamalar

Sophos Cihazınıza Web Arayüzü üzerinden giriş yapın

Configure -> Authentication sayfasına gidin



“Add” Butonuna tıklayın

“Group Name” bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.

“Group Type” bölümünü Normal olarak seçin

“Surfing quota” bölümünü “Unlimited Internet Access” olarak seçin. Eğer bir sınırlama yapmak isterseniz bu bölümden belirtebilirsiniz.

“Access time” bölümünü “Access Time” olarak seçin. Eğer bir sınırlama yapmak isterseniz bu bölümden belirtebilirsiniz.

“SSL VPN policy” bölümünü “No policy applied” olarak seçin

“Clientless SSL VPN policy” bölümünü “No policy applied” olarak seçin

“L2TP” bölümünü “Disable” olarak seçin

“PPTP” bölümünü “Disable” olarak seçin

“Quarantine digest” bölümünü “Enable” olarak seçin

“Quarantine digest” bölümünü “Any node” olarak seçin

Authentication

Servers

Services

Groups

Users

Multi

Group name *

ThreatChaserGuest

Description

Description

Group type *

Normal

Policies

Surfing quota *

Unlimited Internet Access

Access time *

Allowed all the time

Network traffic

None

Traffic shaping

None

VPN

SSL VPN policy *

No policy applied

Clientless SSL VPN policy *

No policy applied

L2TP *

☐ Enable ☒ Disable

PPTP *

☐ Enable ☒ Disable

Other settings

Quarantine digest *

☒ Enable ☐ Disable

MAC binding

☐ Enable ☒ Disable

IPsec remote access *

☐ Enable ☒ Disable

Save

Cancel

“Authentication -> Servers” sayfasına gidin

Add butonuna tıklayın

Server Type bölümünü **RADIUS Server** olarak seçin

Server IP bölümüne **ThreatChaser’ın ip adresini** giriniz

Authentication port bölümünü **1812** olarak giriniz

Accounting Port bölümünü **1813** giriniz

Shared secret bölümünü **ThreatChaser’da girdiğiniz Radius şifresini** giriniz

Group name attributes bölümünü **ThreatChaser’da girdiğiniz Misafir Grubu Adı** ile aynı giriniz

Add external server

Servers	Services	Groups	Users	Mu
Server type	RADIUS server			
Server name *	ThreatChaserRadius			
Server IP *	172.16.16.111			
Authentication port *	1812			
Time-out *	3			
	☒ Enable accounting			
Accounting port	1813			
Shared secret *	*****			
Domain name	Enter Domain name			
Group name attribute *	ThreatChaserGuest			
	☐ Enable additional settings			

“Authentication -> Services” sayfasına gidin

Oluşturduğunuz Radius Server’ı seçin

“Authentication -> Web Authentication” sayfasına gidin

“Show user portal link” ve “Show web page after sign-in” işaretini kaldırın

Captive portal appearance bölümünü **Custom HTML** olarak işaretleyin

Aşağıdaki metinde cihazın ip adresini ve portunu düzenleyerek **Custom HTML** sayfasına yapıştırınız

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="pragma" content="no-cache" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta http-equiv="expires" content="-1" />
</head>
<body>
<h3>Yönlendiriliyorsunuz lütfen bekleyiniz...</h3>
  <script>location.href =
"http://172.16.16.111:7561/auth?post="+window.location.hostname</script>
</body>
</html>
```

“Protect -> Rules and Policies” sayfasına gidin

Add Firewall Rule -> New firewall rule butonuna tıklayın

Action bölümünü “Accept” olarak seçin

Rule Position bölümünü “Top” olarak seçin

Source Zones Hotspot yayını yapacağınız interface’i seçin

Destination Zones hotspot interface’inin hangi internetten çıkmasını istiyorsanız onu seçiniz

Match known users bölümünü işaretleyin

Use web authentication for unkown users bölümünü işaretleyin

User or groups bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.

☒ Rule status

Rule name *

CaptivePortal

Action

Accept

☐ Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description

Enter Description

Rule position

Top

Rule group

None

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *

WiFi

Add new item

Source networks and devices *

Any

Add new item

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week.

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *

WAN

Add new item

Destination networks *

Any

Add new item

Services *

Any

Add new item

Services are traffic types based on a combination of protocols and ports.

☒ Match known users

☒ Use web authentication for unknown users

User or groups *

ThreatChaserGuest

Add new item

☐ Exclude this user activity from data accounting

“Protect -> Rules and Policies” sayfasına gidin

Add Firewall Rule -> New firewall rule butonuna tıklayın

Action bölümünü “Accept” olarak seçin

Rule Position bölümünü “Top” olarak seçin

Source Zones Hotspot yayını yapacağınız interface’i seçin

Source networks and devices bölümüne ThreatChaser’ın ip adresini girin

Destination Zones ThreatChaser’ın hangi internetten çıkmasını istiyorsanız onu seçiniz

Match known users bölümünü işaretleyin

Use web authentication for unkown users bölümünü işaretleyin

User or groups bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.

Add firewall rule Feedback How-to guides Log view

☒ Rule status

Rule name *
ThreatChaser

Action
Accept

☐ Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
Enter Description

Rule position
Top

Rule group
None

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
WiFi
Add new item

Source networks and devices *
Any
All types
Add
Any
Country group
FQDN host
FQDN host group
Host group
IP
IP list
IP range
MAC address
MAC list
Network

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
Add new item

Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports

Add IP host

Name *

ThreatChaserIP

Description

Enter description

IP version *

☒ IPv4

☐ IPv6

Type *

☒ IP

☐ Network

☐ IP range

☐ IP list

IP address *

172.16.16.11

IP host group

Add new item

Save

Cancel

Add firewall rule

Feedback

How-to guides

Log viewer

Help

Rule status

Rule name *

ThreatChaser

Action

Accept

☐ Log firewall traffic

Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description

Enter Description

Rule position

Top

Rule group

None

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *

WIFI

Add new item

Source networks and devices *

ThreatChaserIP

Add new item

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week.

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *

WAN

Add new item

Destination networks *

Any

Add new item

Services *

Any

Add new item

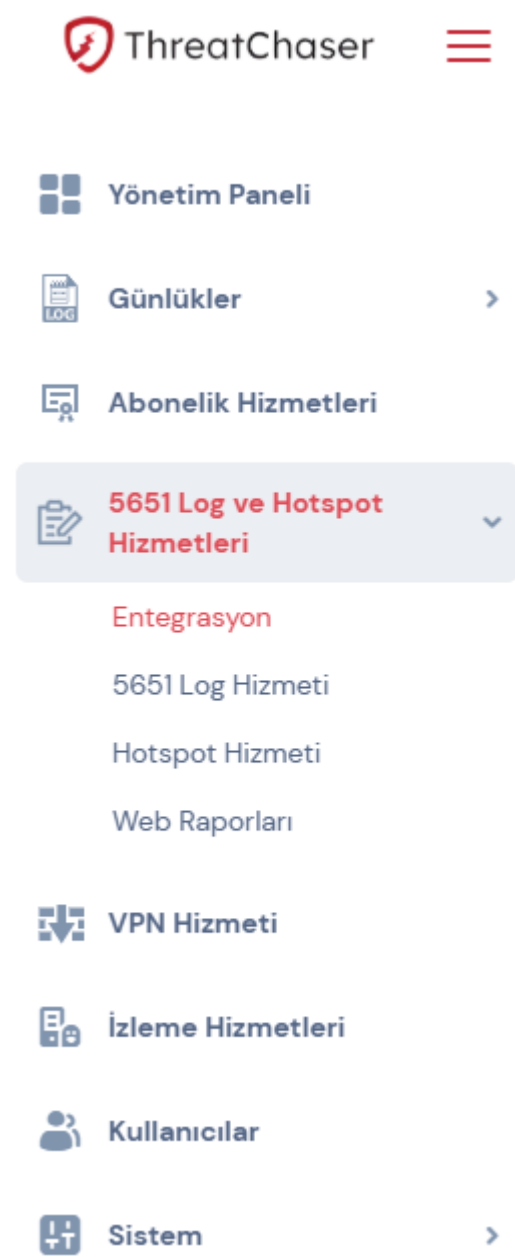
Services are traffic types based on a combination of protocols and ports.

AIMdefense Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

IP Adresi bölümüne AIMdefense'ın ip adresini giriniz.

SSH Kullanıcı Adı bölümüne AIMdefense'ın SSH kullanıcı adını giriniz

SSH Parolası bölümüne AIMdefense'ın SSH parolasını giriniz

SSH Portu bölümüne AIMdefense'ın SSH portunu giriniz

ThreatChaser IP alanına, ThreatChaser'ın IP adresini giriniz. Eğer bulunduğunuz lokasyonda ürüne dışarıdan port yönlendirmesi ile erişiyorsanız, bu alana cihazın iç IP adresini yazmanız gerekmektedir.

Misafir Grubu Bu bölümün AIMdefense tarafında oluşturduğunuz grup ismi ile aynı olması gerekiyor

Radius Şifresi Bu bölüme AIMdefense'ın ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.

Entegrasyonu Düzenle

Ayarlar

Otomatik Firewall Konfigürasyonu

Ürün

AIMdefense

Model

FW-100

Seri Numarası

AIMDefense

IP Adresi

SSH Kullanıcı Adı

SSH Kullanıcı Adını Giriniz

SSH Parolası

SSH Parolasını Giriniz

SSH Portu

22

ThreatChaser IP

172.16.24.111

Misafir Grubu

ThreatChaserGuest

Radius Şifresi

Radius Secret Giriniz

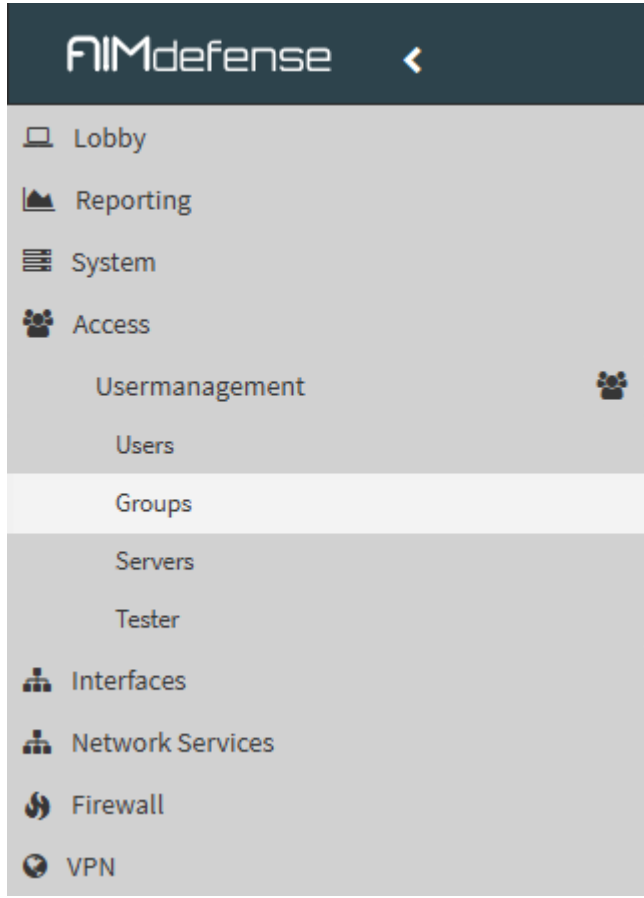
İptal

Kaydet

Firewall Tarafındaki Ayarlamalar

AIMdefense Cihazınıza Web Arayüzü üzerinden giriş yapın

Access -> Groups sayfasına gidin



Add Butonuna tıklayın

Group Name bölümüne ThreatChaser'da girdiğiniz misafir grubu adını girin.

Access: Usermanagement: Groups

Defined by

Group name: ThreatChaserGuest

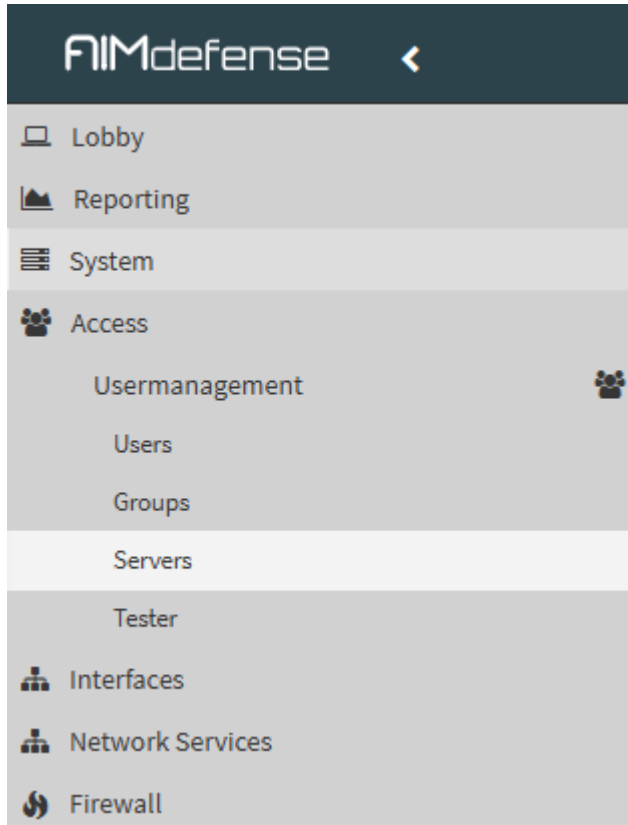
Description

Group Memberships

Not Member Of		Member Of
root	→ ←	

Save Cancel

Access -> Servers sayfasına gidin



Add Butonuna tıklayın

Type bölümünü **RADIUS** olarak seçin

Hostname or IP Address bölümüne **ThreatChaser'ın ip adresini** giriniz

Shared secret bölümünü **ThreatChaser'da girdiğiniz Radius şifresini** giriniz

Authentication port value bölümünü **1812** olarak giriniz

Accounting Port value bölümünü **1813** giriniz

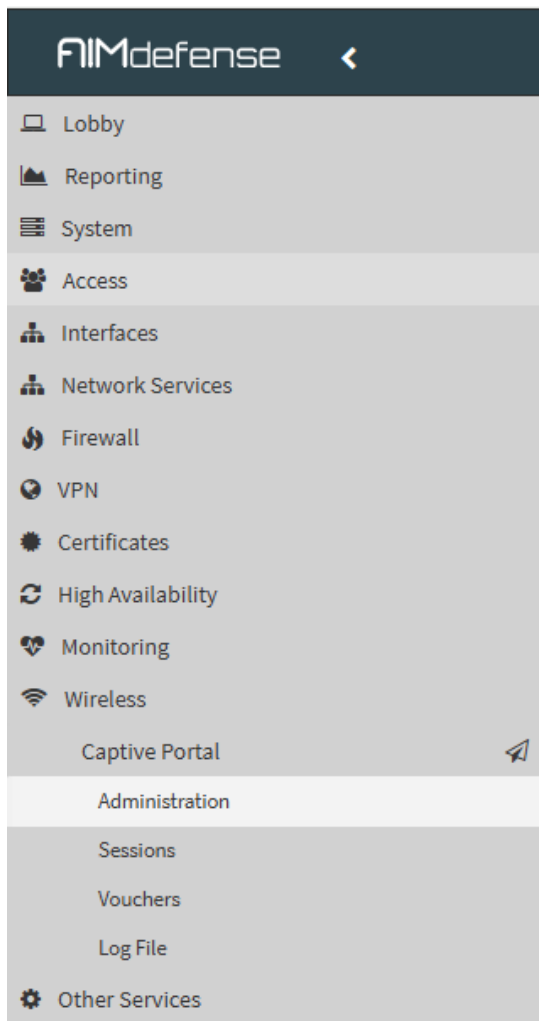
Limit groups bölümünden **daha önceden oluşturduğunuz Radius grubunuzu** seçin

Protocol bölümünü **PAP** olarak seçiniz

Access: Usermanagement: Servers

Descriptive name	ThreatChaserRadius
Type	Radius
Hostname or IP address	10.1.253.111
Shared Secret	*****
Services offered	Authentication and Accounting
Authentication port value	1812
Accounting port value	1813
Authentication Timeout	
Synchronize groups	☐
Limit groups	ThreatChaserGuest
Automatic user creation	☐
Protocol	PAP
<button>Save</button>	

Wireless -> Administration sayfasına gidin



Add Butonuna tıklayın

Enabled bölümünü işaretleyin

interface bölümünde Misafir yayını yapmak istediğiniz ağ arayüzünü giriniz

Authenticate using bölümünde önceden oluşturduğunuz Radius server'ı giriniz

Concurrent user logins bölümünü işaretleyin

Allowed addresses bölümüne ThreatChaser'ın ip adresini giriniz

Description bölümünde Misafir yayınıza isim verin

Save butonuna tıklayın

Edit zone

×

⌵ advanced mode

full help ⌵

ⓘ Enabled

☒

ⓘ Zone number

0

ⓘ Interfaces

HS

✖ Clear All ✔ Select All

ⓘ Allow inbound

Nothing selected

✖ Clear All ✔ Select All

ⓘ Authenticate using

ThreatChaserRadius

✖ Clear All ✔ Select All

ⓘ Always send accounting requests

☐

ⓘ Enforce local group

None

ⓘ Idle timeout (minutes)

0

ⓘ Hard timeout (minutes)

0

ⓘ Concurrent user logins

☒

ⓘ SSL certificate

None

ⓘ Hostname

ⓘ Allowed addresses

10.1.253.111 ✖

✖ Clear All 📋 Copy 📄 Paste 📄 Text

ⓘ Custom template

None

ⓘ Description

HS

A value is required.

Cancel

Save

Apply diyerek ayarlarınızı kaydedin

Wireless: Captive Portal: Administration

Zones

Templates

☐ Enabled	Description
☒	HS

«

<

1

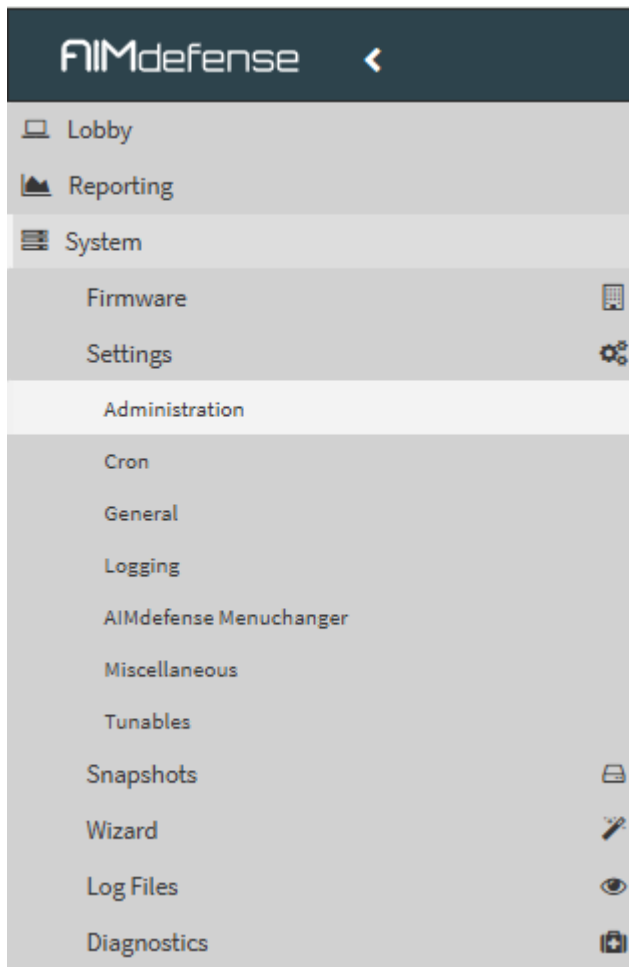
>

»

After changing settings, please remember to apply them with the button below

Apply

System -> Administration sayfasına gidin



Secure Shell Server bölümünü **işaretleyin**

Root Login bölümünde **Permit root user login**'i işaretleyin

Authentication Method bölümünden **Permit password login**'i işaretleyin

Secure Shell	
Secure Shell Server	☒ Enable Secure Shell
Login Group	wheel, admins
Root Login	☒ Permit root user login
Authentication Method	☒ Permit password login
SSH port	22
Listen Interfaces	All (recommended)
Advanced	Show cryptographic overrides

SSL Kontrol Aracı Hizmetini Nasıl Aktif Edebilirim?

Şirket menüsünde yer alan “ThreatChaser SSL Kontrol Aracı” bölümüne gidiniz

**CyCastle** 

 **Yeni Şirket Ekle**



 **Yönetim Paneli**

 **Finans İşlemleri** >

 **Tüm Firmalar** v

 **CyCastle Demo Şirket**

 **Kullanıcı İşlemleri** >

 **Yardım Merkezi** >

Özet

Şirket Detayları

Alan Adı Yönetimi

ThreatChaser >

ThreatChaser Web Tarama >

ThreatChaser CTI

ThreatChaser 5651 Log ve HotSpot Hizmeti **New**

ThreatChaser SSL Kontrol Aracı **New**

ThreatChaser VPN Hizmetleri **New**

SSL kontrolünü etkinleştirmek istediğiniz domainin sol tarafında bulunan butonu aktif konuma getiriniz.

SSL Kontrol Aracı

Aşağıdaki tabloda SSL sertifikalarınızı kontrol edebilir, süresi dolmuş sertifikalar ziyaretçilerinizin güvenini sarsabilir.

Pasif/Aktif	Durum	Alan Adı
☒	Doğrulandı	cycastle.com

Yeni SSL Kontrol Aracı Ekle



Şirket Ünvanı

CyCastle Demo Şirket

Alan Adı

cycastle.com

E-Posta Adresi

demo@cycastle.com

Bildirim Dili

Türkçe



Bildirimler



30 Gün



14 Gün



7 Gün



3 Gün



1 Gün



Bittiğinde Bildirim Gönder

Yukarıdaki bildirim seçenekleri, SSL sertifikası kontrollerinde 30 gün, 14 gün, 7 gün, 3 gün ve 1 gün öncesinde size bildirim göndermek için kullanılacaktır. Ayrıca, sertifika süresi dolduğunda da bildirim alacaksınız. Bu sayede, SSL sertifikalarınızın süresini takip edebilir ve zamanında yenileyebilirsiniz.

“Kaydet” butonuna tıklayarak işlemi sonlandırın.

SSL Kontrol Aracı

Aşağıdaki tabloda SSL sertifikalarınızı kontrol edebilir, süresi dolmuş veya geçersiz sertifikaları tespit edebilirsiniz. SSL sertifikası, web sitenizin güvenliğini sağlamak için önemlidir ve süresi dolmuş sertifikalar ziyaretçilerinizin güvenliğini sarsabilir.

[Alan Adı Ekleme İçin Tıklayın](#)

Arama Yap

10

Pasif/Aktif

Durum

Alan Adı

Alt Alan Adı



Doğrulandı

cycastle.com

Alan Adı

Ortak Ad (CN)

Kuruluş (O)

Ülke (C)

Durum

Kalan Gün

Başlangıç Tarihi

Bitiş Tarihi

cycastle.com

cycastle.com

Symantec Secure Site Pro EV

US

Geçerli

40 Gün

07.07.2025

05.10.2025

www.cycastle.com

www.cycastle.com

Symantec Secure Site Pro EV

US

Geçerli

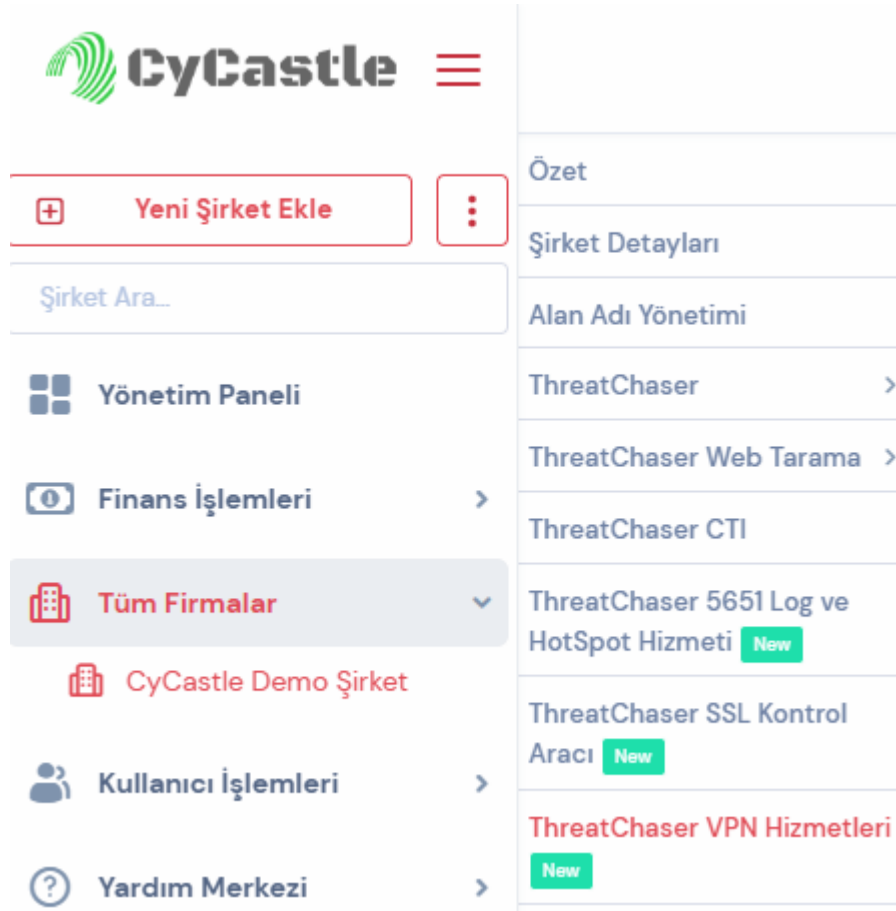
40 Gün

07.07.2025

05.10.2025

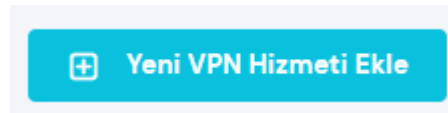
VPN Hizmetini Nasıl Aktif Edebilirim?

Şirket menüsünde yer alan “ThreatChaser VPN Hizmetleri” bölümüne gidiniz



The screenshot shows the CyCastle management interface. On the left, there is a sidebar with the CyCastle logo and a menu. The menu items are: 'Yeni Şirket Ekle' (Add New Company), 'Şirket Ara...' (Search Company), 'Yönetim Paneli' (Management Panel), 'Finans İşlemleri' (Financial Transactions), 'Tüm Firmalar' (All Companies) - which is highlighted, 'CyCastle Demo Şirket' (CyCastle Demo Company), 'Kullanıcı İşlemleri' (User Transactions), and 'Yardım Merkezi' (Help Center). On the right, there is a list of services under the 'ThreatChaser' section. The services listed are: 'Özet' (Summary), 'Şirket Detayları' (Company Details), 'Alan Adı Yönetimi' (Domain Name Management), 'ThreatChaser', 'ThreatChaser Web Tarama' (ThreatChaser Web Scanning), 'ThreatChaser CTI', 'ThreatChaser 5651 Log ve HotSpot Hizmeti' (ThreatChaser 5651 Log and HotSpot Service) with a 'New' tag, 'ThreatChaser SSL Kontrol Aracı' (ThreatChaser SSL Control Tool) with a 'New' tag, and 'ThreatChaser VPN Hizmetleri' (ThreatChaser VPN Services) with a 'New' tag.

“Yeni VPN Hizmeti Ekle” Butonuna Tıklayınız



The screenshot shows a blue button with a white plus icon and the text 'Yeni VPN Hizmeti Ekle' (Add New VPN Service).

“IP Adresi” bölümüne public IP adresinizi girmeniz gerekmektedir. Kullanacağınız public IP adresinin statik olması zorunludur. Eğer firewall kullanıyorsanız VPN portu için yönlendirmeyi firewall üzerinden yapmanız gerekir, firewall kullanmıyorsanız bu işlemi modem üzerinden gerçekleştirmeniz gerekir.

Sanal Ağ Adresi ve Sanal Ağ Maskesi, VPN tüneli için kullanılmaktadır. Burada, hali hazırda kullanılmayan bir ağ adresi girmeniz gerekmektedir.

Yerel Ağlar, VPN üzerinden erişilmesini istediğiniz ağları ifade eder.

“Tüm İstemci Trafiğini Tünel Üzerinden Geçmeye Zorlayın” seçeneği etkinleştirildiğinde, tüm internet trafiği VPN tüneline geçirilir. Böylece VPN’e bağlanan kullanıcılar internete firmanın dış IP adresi üzerinden erişmiş olur.

Yeni VPN Hizmeti Ekle



Şirket Ünvanı

CyCastle Demo Şirket

Başlık

Başlık

IP Adresi

Public IP Adresiniz

Port

10443

Protokol

UDP



Sanal Ağ Adresi

10.203.254.0

Sanal Ağ Maskesi

255.255.255.0

Yerel Ağlar

192.168.1.0/255.255.255.0

DNS 1

1.1.1.1

DNS 2

4.2.2.2

Tüm İstemci Trafiğini
Tünel Üzerinden
Geçmeye Zorlayın



Pasif / Aktif

Bu seçenek etkinleştirildiğinde, VPN istemcisi tüm internet trafiğini VPN tüneli üzerinden yönlendirecektir. Bu, istemcinin ağınıza bağlanarak internetinizi kullanması anlamına gelir.

“Kaydet” butonuna tıklayarak işlemi sonlandırın.

İki Faktörlü Doğrulamayı Nasıl Aktif Edebilirim?

Yeni kayıt olduysanız ilk girişte, veya daha önceden kayıtlı olup iki faktörlü doğrulama aktif değilse, giriş yaptıktan sonra karşınıza aşağıdaki ekran gelecektir. Aktivasyon işlemini bu ekrandan gerçekleştireceğiz.

İki Faktörlü Doğrulama

Lütfen İki Faktörlü Doğrulama Yönteminizi Seçiniz

☐ E-Posta Doğrulaması

Her girişte <strong class="text-info">buraksampl@gmail.com adresine bir kod gönderilir.

☐ Authenticator ile Doğrulama

Google vb. Authenticator uygulamaları üzerinden üretilen kod ile doğrulama

Not: CyCastle kullanıcıları için artık iki faktörlü doğrulama zorunludur. Bu nedenle lütfen yukarıdaki doğrulama yöntemlerinden birini seçerek iki faktörlü doğrulama kurulumunuzu tamamlayın.

Devam Et

1. Yöntem E-Posta Doğrulaması

Giriş yapmak istediğinizde, sistemde kayıtlı olan e-posta adresinize iki faktörlü doğrulama kodu gönderilecektir. Bu kodu kullanarak sisteme giriş yapabilirsiniz.

2. Authenticator ile Doğrulama



Authenticator ile Doğrulama

Authenticator uygulamanızı açın ve aşağıdaki QR kodu okutun:

Bu QR kodu Authenticator uygulamanıza okutun:



Doğrula

Doğrulama Yöntemini Değiştir

E-Posta ile Doğrulama Yönetimini Kullan

Ekranınıza gelen QR kodu Authenticator uygulamanıza okutun

QR kodunu okuttuktan sonra sistemdeki kodu aşağıdaki gibi girin



Authenticator ile Doğrulama

Authenticator uygulamanızı açın ve aşağıdaki QR kodu okutun:

Bu QR kodu Authenticator uygulamanıza okutun:



8

4

1

7

6

0

Doğrula



Doğrulama Yöntemini Değiştir

E-Posta ile Doğrulama Yönetimini Kullan