# Snipesec

CYBER SECURITY AGENCY

DETECT DEFEND SECURE

www.snipesec.com


www.snipesec.com

Snipesec
CYBER SECURITY AGENCY

# İÇİNDEKİLER

# HAKKIMIZDA

## Ana Görevimiz, Siber Uzayda İşletmenizin Güvenliğini Sağlamak.

***Snipesec Bilişim ve Siber Güvenlik, Eğitim ve Danışmanlık Ltd. ve SnipeNet Bilişim Hizmetleri Ltd., Türkiye ve Kıbrıs'ta Bilgi ve Siber Güvenlik alanında faaliyet gösteren Snipesec markasını kullanan SARIZADE Şirketler Grubu'na ait kuruluşlardır.***


Snipesec, Türkiye başta olmak üzere Kıbrıs ve Estonya'ya kadar uzanan operasyonları olan, müşterilerine üstün hizmet kalitesi sunan uluslararası bir siber güvenlik çözüm ortağıdır.

Bilişim sektöründe 10 yılı aşkın deneyime sahiptir ve ISO 9001:2015 (Kalite Yönetim Sistemi Standartları), ISO 27001:2013 (Bilgi Güvenliği Yönetim Sistemi Standartları) ve Genel Veri Koruma Tüzüğü (GDPR) akreditasyonlarını almıştır. Bu, şirketin tüm kalite standartlarını karşıladığı anlamına gelmektedir.
Ayrıca Snipesec, yeni Uzak Masaüstü Hizmeti "Neptün"ü kullanıma sundu. Start-up'ların, işletmelerin ve diğer kuruluşların tek bir ofisteymiş gibi uzaktan çalışmasına yardımcı olan bu hizmet, pazardaki yenilikçi çözümlerden biridir.

# SİBER GÜVENLİK
## NEDEN ÖNEMLİDİR?

Siber güvenlik, her ölçekteki kuruluş için vazgeçilmez bir gerekliliktir.

Her gün yaklaşık **4000 siber saldırı** oluyor.

### Siber suçlar artmaya devam ediyor çünkü

UCUZ > HIZLI > YÜKSEK KARLI

Siber suçlar, işletmelere milyonlarca dolarlık zarara mal olabilir. Ancak bu zararlar yalnızca finansal kayıplarla sınırlı değildir; aynı zamanda işletmelerin itibarına ve iş yapma becerilerine de zarar verebilir. Hatta bazı durumlarda, çalışanların, hastaların ve diğer bireylerin fiziksel güvenliğini ve sağlığını da tehlikeye atabilir.

Siber güvenlik, güven oluşturur. Müşteriler ve çalışanlar, verilerinin doğru şekilde korunduğunu ve gizliliğinin sağlandığını hissetmediklerinde, markaya, ürüne ve hizmetlere olan güvenlerini kaybetmeye başlarlar. Bu nedenle, güçlü bir siber güvenlik altyapısı, işletmelerin sürdürülebilirliği ve itibarı için kritik bir öneme sahiptir.

# HACKERLAR HER GÜN GELİŞİYOR!

Başarılı bir işletme ancak güvenli ve korumalı olduğunda gelişebilir.

Alanında uzman ekibimiz, verilerinizi izinsiz erişimlere ve kötü niyetli saldırılara karşı korumakta üst düzey tecrübe ve yetkinliğe sahiptir.

Siber tehditler artık sadece meraktan ibaret değil!

Siber güvenlik, etkin tespit ve yüksek kaliteli savunma sayesinde şirketinize değer katar, zamanınızı verimli kullanmanızı sağlar ve stresinizi azaltır.

Ve ekibimizin amacı da tam olarak bu güveni sağlamak ve işletmenizi korumaktır!

# HİZMETLERİMİZ

## Güvenlik Test Hizmetleri

**?** **Şirketinizin güvenlik politikalarının gerçekten etkili olduğundan emin misiniz?**

**Kuruluşunuz BT altyapısına ne kadar bağımlı?**

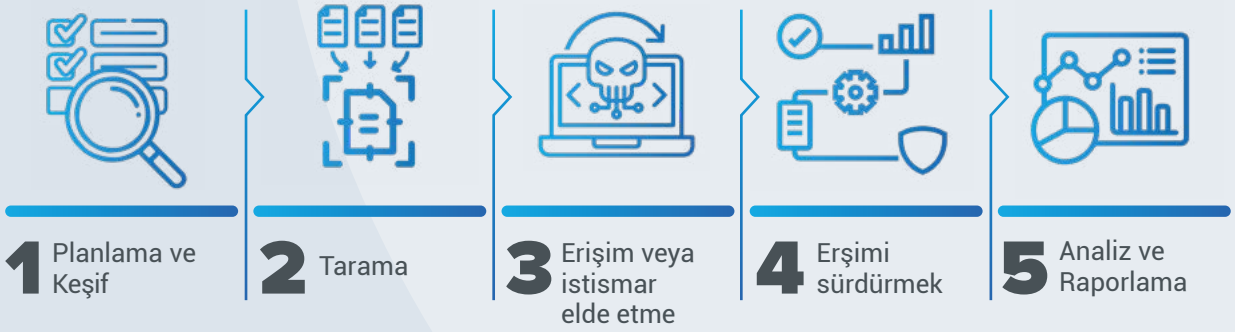
**O BT altyapısı bir günlüğüne bozulsa maliyeti ne kadar olur?**

**Bu soruları yanıtlayarak siber uzayda güvenliğin önemini öğreneceksiniz.**

Çoğu kuruluş, risklerin ve bunların onlar üzerindeki etkisinin farkında değildir. Sistemlerinin saldırıya uğramasının çeşitli yollarını hayal edemezler. Riski bildiğiniz zaman, tehdidi en aza indirmek veya önlemek için önlem alırsınız. Size yardımcı olabileceğimiz şey budur.

**Sisteminizi hackliyoruz.**

Tıpkı bir bilgisayar korsanının yapacağı gibi yetkili bir simüle saldırı gerçekleştiriyor, sisteminizi inceliyor ve kötü amaçlı saldırıları önlemek için güvenlik açıklarını keşfediyoruz.




İlk olarak bir hedef belirliyor ve sistemi analiz ediyoruz. Ardından, güvenlik açıklarını tespit ederek, bunların istismar edilebilir olup olmadığını kontrol ediyoruz. Eğer istismar edilebilir bir güvenlik açığı bulursak, saldırı gerçekleştiriyoruz. Erişim sağladıktan sonra, geri dönüş yapabilmek için güvenli bir arka kapı bırakmayı önemseyerek işlemi tamamlıyoruz. Pentest sürecinin sonunda, müşterimize sistemindeki güvenlik açıklarını ve bunları nasıl düzeltilebileceğini belirten bir rapor sunuyoruz.

# Olay Müdahale Hizmeti

SİBER AMBULANS

Sisteminizle ilgili herhangi bir sorunla karşılaşırsanız size bir telefon kadar yakınız.

Çalışanlarınız işe geliyor ve birdenbire bilgisayarlarının çalışmasına engel olan bilinmeyen bir virüs mü ortaya çıkıyor? Yoksa ağınızın çalışmasını durduran bir donanım sorunu mu var? Bu tür bir durumla karşılaştığınızda ve yardıma ihtiyacınız olduğunda, 7/24 SnipeSec'i arayabilirsiniz. Veri sızıntısı, hizmet kesintisi, felaket kurtarma ve yedekleme kaynaklarına yönelik saldırılar dahil olmak üzere farklı siber tehditlerin hepsine anında müdahale ediyor ve sorunları anında çözüyoruz.

Şirketinizin karşılaşabileceği bir siber olay durumunda, uzman olmayan kişiler tarafından çok geç ya da panik halinde müdahale edilmesi, verilen yanıtların şirketinize ciddi zararlar verilmesine yol açabilir.

**SnipeSec olarak, uzman ve uzmanlaşmış kişilerden oluşan Olay Müdahale ekiplerimiz (CSIRT), şirketinizin maruz kaldığı her türlü siber olayda, kurumsal operasyonlarınızın sürekliliğini ve güvenliğini korumak amacıyla Olay Müdahale hizmeti sunmaktadır.**

**Şirketinizdeki kritik müşteri bilgileri, finansal veriler veya çeşitli plan/projelerinizin sızmasına neden olabilecek veri sızıntılarına karşı gerekli tüm önlemleri alıyoruz.**

**Acil müdahale hizmetimiz 7/24/365 hizmet vermektedir.**

# HİZMETLERİMİZ

## Güvenlik Operasyon Merkezi Servisi

**Sisteminizin 7/24/365 gözetimi**

**Ağınızın 7/24/365 izlendiğinden ve herhangi bir olay durumunda anında önlem alındığından emin olmak ister misiniz?**

İşte tam da bu yüzden SOC hizmeti sunuyoruz. Şirketinizin tüm teknik güvenlik süreçleriyle ilgilenen uzman bir BT ekibimiz var. Üstelik SOC ile yalnızca hizmet için ödeme yaparsınız—ek çalışanlar, altyapı yatırımları, donanım veya ek ofis gibi ek maliyetler konusunda endişelenmenize gerek kalmaz.

Küçük ve Orta Ölçekli İşletmeler, altyapı büyüklüğüne ve kullanıcı sayısına göre belirlenen basit bir aylık faturalandırma modeli ile Güvenlik Operasyon Merkezi (SOCaaS) hizmetimizden hızlı ve verimli bir şekilde faydalanabilir.

Güvenlik Operasyon Merkezi (SOC), şirketinize yönelik iç ve dış tüm siber güvenlik olaylarını tespit etmek, analiz etmek, önlemek ve müdahale etmek amacıyla kurulmuş merkezi bir yapıdır. SOC, güvenlik durumunuzu sürekli izleyerek iyileştirmeler yapmanıza olanak tanır.


Hizmet olarak SOC, güvenliklerini geliştirmek isteyen hem olgun hem de yeni kurulan şirketler için mükemmel bir çözümdür.

**SOC hizmeti sırasında danışmanlarımız:**

- **Güvenlik açıklarını ve mevcut güvenlik durumunu analiz edip raporlama**
- **Maliyet optimizasyonu için en uygun siber güvenlik mimarisi ve stratejilerinin önerilmesi**
- **Gerekli güvenlik araç setlerinin uygulanması, özelleştirilmesi ve destekleyici süreçlerin oluşturulması**
- **Paket bazında tüm SOC sorumluluklarının üstlenilmesi**
- **Yeni bulgular ve iyileştirme önerileri hakkında düzenli raporlama**

**Şirketinizin güvenliğini en üst seviyeye çıkarmak için buradayız!**

# Güvenlik Operasyon Merkezi Servisi

## FAYDALAR

- **Her seviyedeki şirket için uygun**
- **Güvenlik seviyeleri ve koruma, şirketinize göre özelleştirilmiştir**
- **Talep edilen siber güvenlik yeteneğine ve alan uzmanlığına erişim**
- **Özelleştirilebilir güvenlik seviyeleri ve destek kapsamı**
- **Karşılık gelen tüm metriklerle yüksek hizmet seviyeler**
- **Teknoloji yatırım danışmanlığı ve uyum gerekliliklerinin karşılanması konusunda yardım**
- **Alışılmadık senaryolar için özel SOC kullanım durumlarının desteklenme Sürekli güvenlik iyileştirmeleri ve danışmanlık**

## ZORLUKLAR

- **BT altyapısı görünürlüğü gereklidir.**
  Bir SOC kurmadan önce, bileşenlerinin uçtan uca bir görünümünü elde etmek için bir altyapı denetimi yapmak çok önemlidir. Güvenlik uzmanları, verimli SOC performansı sağlamak için onlara kapsamlı bir varlık envanteri ve veri sınıflandırması sağlamanın öneminin altını çiziyor.

- **Etkili iletişim kurmak.**
  SOC'yi seçilen bir güvenlik sağlayıcısına devrettikten sonra, etkin işbirliğini sağlamak için tek bir irtibat noktası sağlanmalıdır. Bir kişiyi seçmek, SOC ekibinin verimliliğini artırabilir.

# HİZMETLERİMİZ

## Güvenlik Operasyon Merkezi Servisi

### SOCaaS hizmetine ihtiyacım var mı?

SOCaaS hizmetine ihtiyacınız olup olmadığı konusundaki düşünceleriniz, aşağıdaki sorulara vereceğiniz cevaplar ile daha net bir şekilde ortaya çıkacaktır.

- Sistem altyapınıza erişim sağlanır ve sisteminizde bir kullanıcı tanımlanarak firmanıza ait hassas bilgilere erişim sağlamaya başlanır ise bundan haberiniz olur mu/ne zaman olur?
- Sisteminizde erişimi bulunan mevcut kullanıcılarınızın yetkileri firmanız için güvenlik riski oluşturacak düzeyde değiştirilir veya yükseltilir ise bunu nasıl fark edersiniz?
- Güvenliğiniz için kullanmakta olduğunuz ve altyapınızda gerçekleşen tüm işlemleri denetlemek için kullandığınız kayıt tutma sistemleri devre dışı kalır veya artık kayıt tutmamaya başlar ise ne olur? Sizler bu durumu ne zaman fark edersiniz? Bu durumu ilgili kayıtlara ihtiyacınız olmadan önce fark eder misiniz?
- Sistem altyapınızda bulunan ve firmanız veya şahsınıza ait kritik önem arz eden dosyalarınıza yetkisiz erişim gerçekleşir veya yetkisiz erişim denemesi yapılır ise bunu bilmek ister misiniz?
- Firmanıza ait web uygulamaları üzerinden gerçekleşen bilgi akışı çalınmaya başlanır ise bu konudan haberiniz olur mu/ne zaman olur?

Snipesec

CYBER SECURITY AGENCY

# HİZMETLERİMİZ

## Bilişim Altyapı Hizmetleri

Altyapınızı kuruyoruz.

Şirketinizin BT altyapısı düzgün bir şekilde uygulanmazsa, işletmeler bağlantı, üretkenlik ve sistem kesintileri ve ihlalleri gibi güvenlik sorunlarıyla karşı karşıya kalabilir. Müşteri Hizmetleri Departmanınız, Pazarlama ve Satış Departmanı ile sağlıklı iletişim kuramayacaksa veya İnsan Kaynakları sadece Muhasebe Ofisinde olması gereken bilgilere ulaşacaksa, organizasyonunuzda oluşacak kaosu tahmin edebilirsiniz.

60 kişiden oluşan ekibimizin tek odağı; **GÜVENLİK.**

Firmanızın bilişim altyapısına donanım ve yazılım bileşenleri kuruyor, firmanızın güvenlik ve kayıt sistemlerinin doğru yapılandırılmasını sağlıyoruz.

Kurulum sonrasında şirketinizin iş operasyonlarını geliştirmek için destek veriyor, bilgi sistemlerinizde oluşabilecek yazılım veya donanım arızalarına anında müdahale ediyoruz.

Tüm donanım ve yazılımların kurulumu, periyodik bakımları ve lisans yenilemeleri hakkında detaylı bir rapor alacaksınız.

# Bilişim Altyapı Hizmetleri

## Kurulum
Firmanızın bilişim altyapısındaki donanım ve yazılım bileşenlerinin kurulumunu uzman kadromuz ile gerçekleştiriyoruz.

## Yapılandırma
Firmanızın sahip olduğu güvenlik veya kayıt sistemlerinin uygun şekilde yapılandırılmasını sağlıyoruz.

## İşletim
Firmanızın sahip olduğu operasyonel sistemlerin işletimi konusunda sizlere uzman kadromuz ile destek veriyoruz.

## Sorun/Arıza Giderme
Firmanızın operasyon devamlılığı için bilişim sistemlerinizde oluşabilecek her türlü yazılımsal veya donanımsal arızalara anında müdahale ediyoruz.

## Raporlama
Firmanızın içerisinde gerçekleşen her türlü kurulum, bakım/onarım, işletim veya sorun/arıza giderme işlemlerini sizin için raporluyoruz.

## Güncelleme
Firmanızın bilişim sistemlerine ait donanım ve yazılımlarla ilgili tüm güncellemelerinizi sizler için uzman kadromuz ile yapıyoruz.

## Eğitimler
Firmanızda sahip olduğunuz bilişim sistemleri ile ilgili ihtiyacınız olan yönetici ve kullanıcı düzeylerindeki eğitimleri sizlere sağlıyoruz.

# HİZMETLERİMİZ

## Dijital Dönüşüm ve Danışmanlık

İşletmenizi modernleştirmenize yardımcı oluyoruz .

Daha yüksek düzeyde dijital olgunluğa sahip şirketlerin, rakiplerine kıyasla daha yüksek satış artışı ve dayanıklılıktan yararlandığını biliyor muydunuz? Dijital olgunluğu yüksek bir kuruluş, faaliyet gösterdiği her alanda dijital teknolojiyi, buna bağlı kültürü ve ağları en verimli şekilde kullanan şirkettir. Dijital olgunluk, günümüz dünyasına ve içindeki insanlara uyum sağlamayı gerektirir.

Dijital dönüşüm, mevcut süreçlerinizi otomatikleştirerek iyileştirebilir ve işletmenizin büyümesini önemli ölçüde hızlandırabilir. Ancak dijital dönüşümü hayata geçirmeden önce, şirketinizin mevcut durumunu ve geliştirilmesi gereken alanları belirlemek için Dijital Olgunluk Değerlendirmesi yapılması gerekir.

Bu hizmetimizin yanı sıra, firmanızın teknolojiye ayak uydurmasını ve operasyonlarını ülke sınırlarının ötesine taşımasını sağlıyoruz.

Firma profilinizin oluşturulması ve SWOT analizi ile başlayan danışmanlık sürecinde, şirketinizin tüm yönlerini analiz ediyor, dijital dönüşüm stratejinizi planlıyor ve firmanıza katma değer sağlayacak en uygun çözümleri sunuyoruz.

Danışmanlık hizmetimiz süresince sizlere teknolojik anlamda her konuda (alım-satım, yatırım, projelendirme, kâr-zarar analizi vb.) rehberlik sağlıyor; firmanızın teknoloji alanında yapmayı planladığı yatırımlarda, uluslararası bağlantılarımız kapsamında size destek veriyoruz.

# Dijital Olgunluk Değerlendirmesi

Dijital olgunluğunuza yatırım yapmak, başarınıza yatırım yapmaktır.

Günümüzde teknolojinin iyileştiremeyeceği neredeyse hiçbir şey yok. Bu nedenle, dijital olgunluk değerlendirmesi yapmak, teknolojinin işletmenizdeki en büyük sorunları nasıl çözebileceğini belirlemek ve çalışanlarınızı daha verimli, motive ve üretken kılacak yollar bulmak için zaman ve çaba harcamaya değer.

Yenilikçi bir bakış açısıyla hareket ederek, işletmenizin karşılaştığı engelleri aşabilir ve başarınızı kesintisiz bir şekilde sürdürebilirsiniz.

Dijital olgunluğunuzu araştırdıktan sonra, dijital olgunluğunuzu ölçme ve iyileştirme konusunda rehberlik ve tavsiyeler alacak; ayrıca dijital olgunluk içgörülerinizi, dijital bir strateji oluşturmak için kullanmanıza yardımcı olacağız.

Firmanız, zaman ve teknolojiye ayak uydurmadığı takdirde ömrü kısalacaktır.

# HİZMETLERİMİZ

## Zararlı Yazılım Analizi

### KÖTÜ AMAÇLI DOSYALARIN KONTROLÜ

Günümüzde işletmenizin performansını bozabilecek 20'den fazla kötü amaçlı yazılım türü bulunmaktadır. Tüm kötü amaçlı yazılımların ortak özelliği, şirketlere milyonlarca lira kaybettirmesidir. Dünyanın dört bir yanındaki bilgisayar korsanları, küçük, orta ölçekli ve büyük kurumları hedef alarak bu şirketlerden büyük miktarda kâr elde etmektedir. Eskiden insanlar, doğrudan mağazanızdan hırsızlık yapabiliyorlardı. Bu nedenle her binada, hırsızlardan korunmak ya da onları tespit edip cezalandırmak için gözetleme kameraları kullanılıyordu. Ancak dijital ortamda gerçekleştirilen hırsızlık, fiziksel mağaza hırsızlığından çok daha kolay, ucuz ve karlıdır.

Bu sebeple, dünya çapında çeşitli türlerde karmaşık kötü amaçlı yazılımlar üreten binlerce bilgisayar korsanı bulunmaktadır. İnternet ortamındaki sınırsızlık nedeniyle, hedefledikleri kişiler veya kuruluşlar artık ülke, dil veya diğer sınırlamalara tabi değildir.

Kurumlar, ağlarına kötü amaçlı yazılım bulaştığının farkında bile olmayabilirler. Bilgisayar korsanları, hiç beklemedikleri bir anda, kurum için değerli olabilecek her şeyi altüst ederek performanslarını duraklatabilir ve ciddi zararlar verebilirler.

Kötü Amaçlı Yazılım Analizi hizmeti ile şirketinizi veya tüm bilgi işlem altyapınızı hedef alarak, sistemlerinize zarar veren kötü amaçlı yazılım türevlerinin (kötü amaçlı yazılım, fidye yazılımı, dropper, casus yazılım vb.) derinlemesine analizi ve temizlenmesi sağlanır.

Kötü amaçlı yazılımların kurbanı olan şirketinizin altyapısındaki ve ticari faaliyetleriniz için kritik öneme sahip tüm verilerinizin kurtarılmasını ve bu tür saldırıların tekrarlanmaması için gerekli tüm önlemlerin alınmasını sağlıyoruz.

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### FİDYE YAZILIMI

Firmanızdaki bilgisayarlar veya bilgisayarlardaki veriler ne kadar güvende? Ya sahip olduğunuz tüm ağlar bir günlüğüne çalışmayı durdurursa? Firmanız bir günde ne kadar para kaybeder?

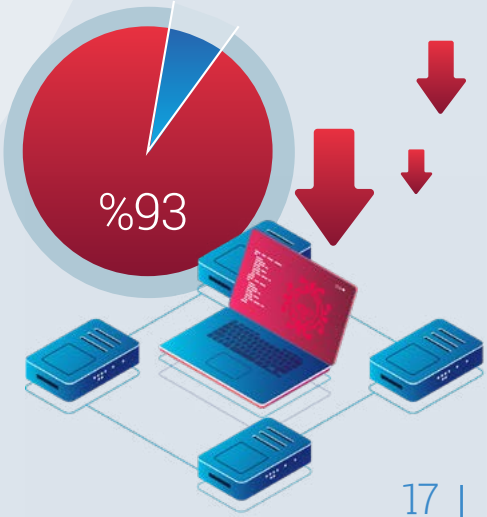
Peki ya haftalar? Bilgisayar korsanlarının şu anda hesapladığı şey tam olarak budur. Hesaplamalarını yaptıktan sonra, sisteminize girer, dosyalarınızı şifreler veya şifrenizi değiştirirler. Ya da ödeme yapana kadar sisteminizi tutmak için başka bir yöntem uygularlar. Bir gün ofisinize giriyorsunuz, bilgisayarınızı açıyorsunuz ve şu yazıyı görüyorsunuz: "Bilgisayarınız kilitlendi. 10.000 $ ceza ödemeniz gerekiyor ve bu bağlantıyı kullanarak Bitcoin ile ödeyebilirsiniz. Geri erişim için ödeme yaparsanız, size gizli kilit açma kodunu vereceğim. Ardından, kodu küçük beyaz kutuya girip 'Tamam' butonuna basabilirsiniz."

Çoğu zaman, ödeme yapsanız bile, anahtara tekrar erişmenize izin vermezler. En iyi durumda, yaparlar. En kötü durumda ise, paranızı almışlardır ve karşılığında size gösterecek hiçbir şeyleri yoktur.

Fidye yazılımı, son derece acı verici olabilir. Saldırganlar, firmanızı ciddi zararlara uğratabilirler. Fidye saldırılarında büyük paralar döner; yılda yüz milyonlarca dolar, belki de milyarlarca dolar. Dünyanın en iyi siber suçluları, St. Petersburg'daki veya dünyanın diğer şehirlerindeki bazı genç adamlar, ayda bir milyon dolar kazanmaktadır. Ve küçükten büyüğe her türden firmayı hedef almaktadırlar.

Siber suçlular şirket ağlarının %93'üne girebilir.

**Vakaların yüzde 93'ünde, harici bir saldırgan bir kuruluşun ağ çevresini ihlal edebilir ve yerel ağ kaynaklarına erişim sağlayabilir.**



# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### VİRÜSLER

Virüsler, bilginiz dışında bilgisayarlarda çalışabilir. Belki de işiniz için ihtiyaç duyduğunuz bir web sitesinden yeni bir program indirmeye gittiniz. Ancak, içindeki kurulum dosyasını indirdiğinizde bazı kötü amaçlı kodlar içerebilir. Programı yüklemek için çalıştırdığınızda, kodun bilgisayarınıza yüklenmesine izin vermiş olursunuz ve bu virüs artık bilgisayarınıza bulaşabilir. Bu noktada, virüs çoğalmaya ve yayılmaya başlayacaktır. Bunu, sizin bir kullanıcı olarak gerçekleştirdiğiniz eylem sayesinde yapar. Bu örnekte, programı yüklediniz ve bu, kodun çalışmasına ve virüsün kötü şeyler yapmaya başlamasına olanak tanıdı. Virüs, ağınızda çoğalmaya ve yayılmaya başlar. Farklı karmaşıklık düzeylerine sahip çeşitli virüs türleri vardır. Antivirüs sağlayıcılarımız, virüsleri, nasıl çalıştıklarını ve onları nasıl durduracaklarını anlamada her geçen gün daha iyi hale geliyor. Ancak, virüs üreticileri, bu tür virüsleri tespit etmeyi zorlaştıran şifrelenmiş virüsler üretmektedir. Bu durum, kötü niyetli kişilerin başarılı olamaması için, iyi niyetli kişilerin sürekli olarak daha iyi hale gelmesi gerektiğini gösterir.

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### TRUVA ATI

**Bu kötü amaçlı yazılım parçasına dalmadan önce, size hızlı bir tarih dersi vermemize izin verin.**

Birkaç bin yıl öncesine dönersek, Yunanistan ve Truva savaş halindeydi. Bu, görünürde sonu olmadan yaklaşık 10 yıl sürdü. Uzun bir kuşatmanın ardından Yunanlılar huzursuz olmaya başladılar ve farklı bir şey denemeye karar verdiler. Dışarı çıkıp büyük bir tahta at yaptılar. Onu, Truva şehrine barış teklifi olarak vereceklerdi. Bu görünüşte zararsız hediye, aslında Yunan askerleriyle doluydu ve şehre girdiklerinde gece gündüze döndü. İçeriden askerler atın içinden çıktılar. Surlarla çevrili şehrin kapılarını açarak, işgalci Yunan ordusunun şehre girmesini sağladılar ve şehri yerle bir ettiler. Bu, Truva Atı'nın ilk örneğiydi.

Artık bilgisayarlarda Truva atları çok benzer şekilde çalışıyor. Temel olarak, bir Trojan (Truva Atı), "Bu işlevi sizin için gerçekleştireceğim" diyor. İstenilen işlevi yerine getirecek, ancak aynı zamanda kötü niyetli bir işlevi de yerine getirecektir.

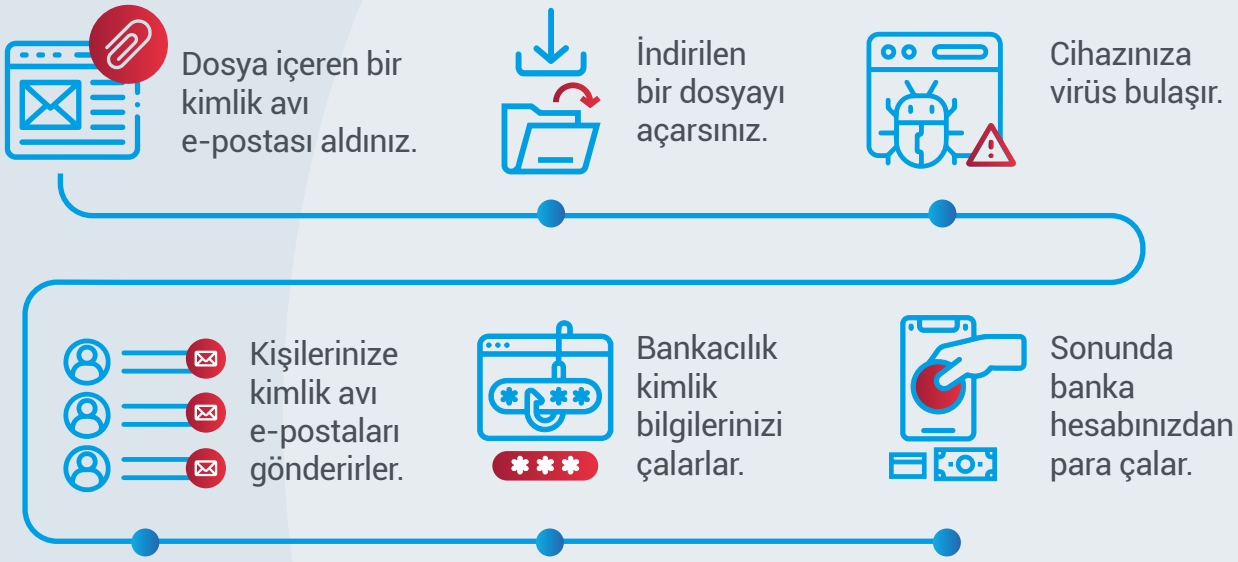
Şimdi, biz çocukken Tetris adında yeni bir oyun çıkmıştı. Son derece popüler bir oyundu ve herkes bir kopyasını almak istiyordu. Ve böylece, çoğu zaman arkadaşlarınız size bir disk verip "Hey, devam edin ve bunu kurun, Tetris oynayabilirsiniz" derdi. Bu kişi gerçekten zekiydi ve Tetris'in bir kopyasını kullanmaya karar verdi ve içine bir Truva Atı yerleştirdi. Yani, diski alırsınız, bilgisayarınıza takarsınız, oyunu açarsınız ve her şey normal gibi görünür. Ancak perde arkasında gerçekte olan şey, sizin sisteminizle onların sistemi arasında bir bağlantı kurarak, arkadaşınızın makinenizi uzaktan kontrol etmesine izin vermekti. Bu da, kritik verilerin çalınmasına ve başka bir yere gönderilmesine, dosyaların silinmesine veya değiştirilmesine ya da aksi halde BT altyapınızın düzenli kullanımını kesintiye uğratmaya neden olabilirdi.

Gizliliğinizi koruyarak güvenliğinizi güçlendiriyoruz.

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### KÖTÜ AMAÇLI SPAM




Emotet, öncelikle e-posta spam'i (malspam) yoluyla yayılan bir saldırıdır. Amazon'dan, bankanızdan ya da tanıdığınız birinden gelen ve güvenilir gibi görünen bir e-posta, bağlantıya tıklamanızı veya ek indirmenizi isteyen bir mesajla karşılaşabilirsiniz. Bu tür bir e-postayı, mesru olduğunu düşünerek açabilirsiniz, özellikle de tanıdık birinden geliyorsa. İlk enfeksiyon genellikle bu şekilde gerçekleşir.

Daha sonra, bağlı sistemlere üç ana yolla yayılmaya çalışacaktır. İlk olarak, kişilerinize erişim sağlayarak, sizden gelmiş gibi görünen bir kimlik avı e-postası gönderecektir. Ardından, ağınızdaki diğer sistemlere (evdeki ya da kuruluşunuzdaki diğer bilgisayarlar olabilir) yayılmak için bilinen yazılım güvenlik açıklarını kullanmaya çalışacaktır. Son olarak, şifreleri kırarak tüm bilgileri çalmaya çalışacaktır.

**Emotet, zirvesinde dünya çapında 1,5 milyon bilgisayara bulaştı ve çevrimdışı hale getirilmeden önce tahmini 2,5 milyar dolar tutarında zarara neden oldu.**

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### BOTNET

Telefonunuzun veya dizüstü bilgisayarınızın şu anda botnet'in bir parçası olabileceğini biliyor musunuz? Bir botnet, bilgisayar korsanlarının cihazınızdan botlar oluşturması ve onlar aracılığıyla saldırılar gerçekleştirmesidir. Cihazınıza virüs bulaşmış olsa bile farkında olmayacaksınız. Çoğu zaman siber suçlular binlerce, onbinlerce ve hatta milyonlarca bilgisayarı etkilemeye ve kontrol etmeye çalışır. Böylece büyük bir zombi ağının veya bot ağının efendisi olarak hareket edebilirler.

Bir botnet'in parçası olmanın sonuçları çok ciddi olabilir. Bazı riskler şunları içerir:

- Yüksek İnternet Faturaları
- Yavaş ve Dengesiz Bilgisayar Performansı
- Çalınan Kişisel Veriler

Bilinmeyen bir web sitesinden ücretsiz olarak bir şeyler indirerek veya dosya paylaşarak bir botnet'in parçası olmak kolaydır. Sosyal medya siteleri veya uygulamaları bile bilgisayarınızı bir bot'a çevirebilir.

Botnet'in en başarılı parçalarından biri Zeus olarak adlandırılıyor. Milyonlarca cihazı etkiledi. Dahası, virüs yeni varyantlar üretmeye, yeni ana bilgisayarlarda üremeye ve erişimini genişletmeye devam ediyor. Zeus virüsü kendisini cihazınıza yükledikten sonra iki ciddi eylem gerçekleştirebilir. İlk olarak, bir botnet'in parçasını oluşturur. Botnet, sahibinin büyük miktarda bilgi toplamasına ve büyük ölçekli saldırılar gerçekleştirmesine olanak tanır. İkincisi, kötü amaçlı yazılım, Keylog'daki web sitesini izleyerek bankacılık kimlik bilgilerini çalan bir finansal hizmetler Truva Atı görevi görebilir. Zeus virüsü, bir kullanıcının bir bankacılık web sitesinde olduğunu fark eder ve oturum açmak için kullanılan tuş vuruşlarını çalar. Sonunda banka hesaplarınızdaki parayı çalar.

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### BOTNET


Botnet kötü amaçlı yazılımlarının bir başka örneği de Mirai olarak adlandırılır. Aynı zamanda solucan olarak da adlandırılır. Mirai, akıllı TV'ler, oyuncaklar, akıllı buzdolapları, akıllı kapı kilitleri, sensörler vb. gibi sahip olduğunuz tüm akıllı cihazları içeren ev ağınızdaki akıllı cihazları hedefler. Bu kötü amaçlı yazılım, şimdiye kadar kaydedilen en büyük siber saldırıların bazılarında kullanılmıştır.

2016'da bilgisayar korsanları, tıpkı evinizde olabilecekler gibi yazıcılar, bebek monitörleri, kameralar ve akıllı buzdolapları gibi binlerce ve binlerce ev cihazına bulaşmayı başardı. Akıllı cihazların kontrolünü ele geçirdiler ve sunucuları doldurmak için kullandılar ve milyonlarca İnternet konumundan geliyormuş gibi görünen kötü amaçlı trafiğe sahip önemli bir internet altyapı şirketine sahip oldular. Birçok büyük web sitesi, Avrupa ve Kuzey Amerika'daki kullanıcılar tarafından kullanılamaz hale geldi. Bu saldırının büyük bir örneği, Avrupa ve Kuzey Amerika'ya DNS sağlayıcısı olan Dyn web sitesine yapılan bir siber saldırıdır. İnternet, alan adlarından oluşur ve alan adı sağlayıcınızın çalışmaması, web sitenizin çalışmaması ve müşterilerin ona ulaşamaması anlamına gelir. Bu nedenle saldırıdan sonra Dyn müşterilerinin yaklaşık %8'ini kaybetti. Twitter, Spotify ve PayPal gibi büyük ABD web sitelerinin yanı sıra dünya çapında çok sayıda başka şirket de HSBC, BankWest ve Ticketmaster gibi bağlantı sorunları yaşadı. Müşteri ilişkilerini etkiledi ve şirket için büyük bir kayıpla sonuçlandı.

# Zararlı Yazılım Analizi

## Kötü Amaçlı Yazılım Türleri

### CASUS YAZILIM

Casus yazılım terimini muhtemelen daha önce duymuşsunuzdur, ancak tam olarak nedir? Rakipleriniz, bunu size karşı kullanmaktan mutluluk duyacaktır. Normalde, bu yazılım bir web sitesinden veya sisteminize yüklediğiniz bazı üçüncü taraf yazılımlardan kurulacaktır. Yaptığı şey, tüm dosyalarınızı, e-postalarınızı, anlık iletilerinizi, takvim davetlerinizi ve sisteminizde sahip olabileceğiniz diğer bilgileri aramaya başlamaktır. Bunları toplar ve sizinle ilgili bir profil oluşturur.

En iyi senaryoda, sadece bilgilerinizi toplar; ancak en kötü durumda, bir web sitesi adı ve kullanıcı adınızı ve şifrenizi yazarsanız, bunları toplayarak saldırgana geri gönderebilir. Hatta, ekranda gördüklerinizin ekran görüntülerini alabilir ve bunları e-posta veya anlık mesaj yoluyla rutin aralıklarla geri gönderebilir.

Dünya çapında her 39 saniyede bir siber saldırı gerçekleşmektedir.

### DONANIM SORUNLARI

Altyapınızın kullandığı donanımın hâlâ lisanslı ve eski olmadığından emin misiniz? Güncelliğini yitirmiş eski sistemlerin bakımı pahalı olabilir. Teknolojinin çok daha hızlı eskimesi dışında, eski bir ev ya da aracın bakımını yapmaktan çok da farkı yoktur.Eski bilgisayar, hard disk vb. kullanıyorsanız, bir gün sisteminiz çökebilir veya üreticiler destek vermeyi bıraktığı için virüs bulaşabilir.Bu nedenle, altyapınızın güncelliğini yitirmesi nedeniyle güvenlik riskleri ve virüslere karşı savunmasız olmadığından emin olmak istersiniz.

# HİZMETLERİMİZ

## Red Team Hizmeti

Mevcut BT ekibinizi eğitiyoruz.

Red Team hizmeti, şirketinize yönelik olası dış saldırılara karşı mevcut güvenlik altyapınızı denetlemek ve güçlendirmek için yapılan bir test sürecidir. Bu sürece dahil olan ekibiniz, olası saldırganları ve sisteminize karşı yapılabilecek çeşitli saldırı yöntemlerini öğrenir. Olası saldırı yöntemlerini gerçek zamanlı olarak uyguladığımız saldırı senaryolarını da gerçekleştirerek bir saldırgan gibi düşünebilme ve saldırılara karşı hazırlıklı olma yeteneğinizi artırıyoruz.

## Blue Team Hizmeti

Saldırıya karşı savunmak.

Şirketinize yönelik olası siber saldırılara karşı hazırlık seviyenizi artırmak, saldırılara zamanında ve yeterli şekilde müdahale edebilmek için iç güvenlik ekibinizi Mavi Takım Hizmeti eğitim sürecine dahil ediyoruz.

Bu nedenle, iç güvenlik ekibiniz, sistemlerinize yönelik gerçek saldırı durumları veya Red Team senaryoları sırasında yeterli düzeyde hazır olacaktır.

# Snipesec

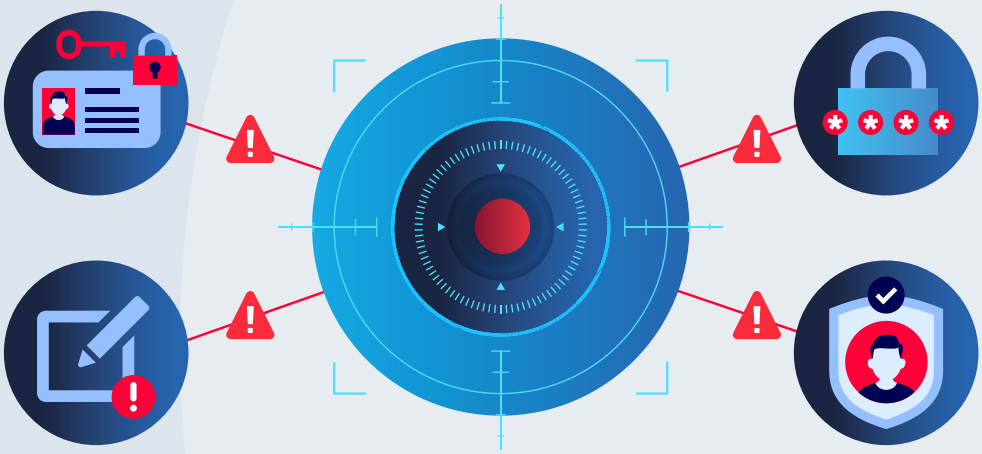
CYBER SECURITY AGENCY

DETECT DEFEND SECURE

# ÜRÜNLERİMİZ

## Siber Poligon

Snipesec'in sunmuş olduğu Siber Poligon hizmeti, gerçek bir atış poligonundan ilham alınarak tasarlanmıştır ve siber güvenlik ekiplerinin saldırı ve savunma becerilerini geliştirme odaklı bir platformdur. Bu platform, kamu ve özel sektör kurumlarına yönelik olarak, siber araçları etkin bir şekilde kullanma kapasitelerini artırma ve bu sayede siber güvenlik alanında nitelikli uzman yetersizliğini giderme imkanı sağlar.



Siber Poligon içerisinde, ekipler gerçekçi ve kontrol edilebilir bir ortamda çeşitli siber saldırı senaryolarıyla karşı karşıya gelir. Örneğin, katılımcılar fidye yazılımı saldırıları veya gelişmiş kalıcı tehditler (APT) gibi senaryolar üzerinde çalışarak, bu tehditleri tespit etme, analiz etme ve müdahale etme becerilerini geliştirirler. Eğitimler, Snipesec uzmanları tarafından rehberlik edilen simülasyonlar ve gerçek zamanlı tatbikatlar şeklinde gerçekleştirilir. Katılımcılar, bu süreçte teorik bilgilerini pratik uygulamalarla pekiştirirken, siber olaylara müdahalede bulunabilecek yetkinlik düzeyine ulaşırlar.

Snipesec, Siber Poligon hizmeti ile kurumların kendi iç siber güvenlik kapasitelerini güçlendirerek, ulusal ve uluslararası düzeyde siber tehditlere karşı daha dirençli hale gelmelerine katkıda bulunmayı hedeflemektedir.

# Jüpiter

Jüpiter Bulut Yedekleme Servisi, verilerinizi güvenli bir şekilde yedeklemenizi ve korumanızı sağlayarak işletmeler ve bireysel kullanıcılar için yüksek güvenlikli ve maliyet-etkin bir çözüm sunar.

Otomatik yedekleme süreçleri sayesinde, verilerinizin kaybolma riski ortadan kaldırılır ve hızlı bir şekilde geri yüklenebilir. Jüpiter, depolama alanınızı ihtiyacınıza göre ölçeklendirerek işletmelerin büyüme ve küçülme süreçlerine uygun esneklik sağlar.

Verilerinizi her türlü tehditten koruyan Jüpiter, hem yetkisiz erişimlere karşı hem de doğal afetler gibi olası tehlikelere karşı güçlü bir güvenlik önlemi sunar. Bulut ortamında yedekleme yaparak, verilerinizi fiziksel alanlardan bağımsız şekilde güvence altına alırsınız. Ayrıca, yedekleme işlemleri otomatikleştirildiği için manuel müdahale gereksiz hale gelir, bu da operasyonel verimliliği artırır.

Jüpiter Bulut Yedekleme Servisi, uygun maliyetlerle yüksek güvenlikli yedekleme imkanı sunar.

Veri merkezi ve yedekleme cihazı maliyetlerini azaltarak işletmelerin ve bireylerin bütçelerine dost bir çözüm ortaya koyar.

**Uzman ekibimiz, yedekleme süreci boyunca 7/24 destek sağlayarak her zaman yanınızda olacaktır.**

# ÜRÜNLERİMİZ

## Neptün (Sanal Masaüstü Servisi)

Artık fiziksel bir ofis kiralamanıza gerek yok!


Kaydolun ve web sitemize giriş yapın

Size uygun paketi seçin

Ödeme yöntemini seçin ve ödeyin

Kimlik bilgilerinizi e-posta ile alın

Herhangi bir cihazdan herhangi bir yerden, herhangi bir zamanda uzaktan bağlanın

Bağlantınız sunucularımızdan geçer ve Yeni Nesil Siber Güvenlik Duvarımız tarafından korunur

Eşsiz anonimlik sistemimizle izlenmeden web'de gezinebilirsiniz

Şirketiniz için bir ofise sahip olmak harika! Tüm çalışanlarınız sabah ofise gelir ve sinerji içinde çalışırlar. Ama bir an için ofise ne kadar ödediğinizi düşünelim. Kirasını mı, fiyatını mı düşündünüz? Peki ya bir ofisin tam olarak çalışması için ihtiyaç duyduğu diğer şeyler? Mobilya, bilgisayar, telefon, yiyecek içecek, internet ve en önemlisi elektrik. Ancak, bir ofisiniz olmalı! Aslında hayır. Pandemi bize, istikrarlı bir internet bağlantımız olduğu sürece herhangi bir şirketin faaliyetlerine devam edebileceğini gösterdi. Artık herkes çevrimiçi çalışmaya alıştı. Ancak bu iş iyi organize edilmedi çünkü işletmeler çok hızlı uyum sağlamak zorundaydı ve ayrıntılı, organize bir çevrimiçi ofis yoktu.

Eh, pandemi bitti ama birçok şirket uzaktan çalışmanın mümkün olduğunu ve daha uygun maliyetli olduğunu fark etti. Bu yüzden size Neptün adlı eşsiz bir ürün sunuyoruz. İşletmeniz için sanal bir ofistir. Çalışanlarınız aynı ofisteymiş gibi online çalışabilirler. Herkesin tek bir ağa bağlı olduğu sanal bir ortamdır ve uzaktan çalışmanın daha verimli bir yoludur. Neptune, uzaktaki personeliniz için fiziksel iş yerinizi dijital bir ofise dönüştürür.

## Kendi dijital ofisinizi oluşturun ve uzaktan çalışmaya izin verin.

Neptune, işletmelerin BT altyapısı yatırım maliyetlerini azaltmak, bakım onarım yüklerini ortadan kaldırmak, yüksek performanslı ve esnek bir çalışma ortamı sağlamak için tasarlanmış güvenli bir uzak masaüstü hizmeti (VDI) altyapısıdır. Çalışanlarınız Neptune'ü her yerden kullanabilir.

Sanal Masaüstü Hizmeti (VDI), şirketler için bilgi işlem yatırımları maliyetlerini en aza indirgemek ve bu hizmetleri yönetirken çoğu kuruluşun karşılaştığı teknik zorluklar ve verimsizlikleri gidermek amacıyla oluşturulmuş bir hizmettir. Ayrıca, Uzak Masaüstü Hizmetlerini (RDS) destekler niteliktedir.

Bu hizmet, ofis çalışanlarının ötesinde eğitim kurumları ve kuruluşlarında da yatırım, bakım-onarım maliyetlerini düşürmek, eğitim-öğretim faaliyetlerinde kullanılan uygulama laboratuvar altyapıları için kaliteli hizmet sunulabilmesi amacıyla yaygın bir şekilde kullanılan bir hizmettir.

### BU HİZMETİ KİMLER KULLANABİLİR?

Neptün, teknoloji alanında faaliyet gösteren işletmelerin dışında kalan birçok küçük ve orta büyüklükteki işletmeler için de kullanım kolaylığı ve maliyeti bakımından birçok avantajlar sağlaması sebebi ile tercih edilmektedir. Bunların içerisinde başlıca olarak;

- Eğitim-öğretim kurumları (dershane, kolej, lise ve üniversiteler)
- Oteller ve casinolar
- Muhasebe ofisleri
- Eczaneler
- Süpermaketler
- Benzin istasyonları
- Seyahat acenteleri
- Yapı Marketler

# ÜRÜNLERİMİZ

## Neptün (Sanal Masaüstü Servisi)

### NEDEN NEPTÜN?

#### YÜKSEK PERFORMANS

Neptün, çalışanlarınıza ve sizlere son teknoloji yüksek kalitede donanım ve yazılımlara sahip olan yüksek performans sanal masaüstü makine paketlerini sunmaktadır. Bu sağlanan sanal makineler için tercih edebileceğiniz farklı ve yüksek hızda internet bandı, depolama alanı, işlemci ve hafıza seçenekleri mevcuttur. Neptün sisteminde, size özel hazırlanan kapalı ağ içerisine dahil olan çalışan sayınızın artışından Neptün ağ performansınız, kullandığı yük dengeleme sistemleri sayesinde hiçbir şekilde etkilenmez..

#### DÜŞÜK MALİYET

Neptün, sizleri tüm donanımsal arıza ve bakım-onarım maliyetlerinden uzak tutar. Neptün sayesinde gelişmekte olan bilişim dünyasında donanım güncellemesi veya bakım-onarım işlemlerini düşünmenize gerek kalmaz, Neptün altyapısında tüm donanım güncellemeleri ve bakım-onarım faaliyetleri tarafımızca yapılmaktadır. Bu durum işletmenize çok düşük yatırım maliyetleri ile yüksek performanslı bilgisayarlar kullanma avantajını sağlar.

#### GÜVENLİ KAPALI AĞ

Neptün, şirketinizin ihtiyaç duyduğu bilgi işlem iş yükü oranında yüksek performanslı ve düşük maliyetli sanal makineler oluşturarak tüm şirket çalışanlarınızın güvenli kapalı ağ içerisinde esnek ve güvenli bir çalışma ortamına kesintisiz şekilde 7/24 uzaktan erişebilmesine olanak sağlar. Neptün içerisinde oluşturulan bu kapalı ağ sayesinde tüm çalışanlarınız fiziksel olarak ayni ofiste çalışır gibi (dosya paylaşımı v.b.) aynı lab ortamına bağlanma imkanına sahip olur.

#### ANONİM VPN BAĞLANTISI

Neptune, şirketinize ait oluşturmak istediğiniz sanal ağ içerisindeki makinelerde internet bağlantınız için anonimlik talebiniz doğrultusunda güvenli bir VPN bağlantısı sunar. Talebiniz üzerine sunulan VPN seçenekleri arasından çalışanlarınız için istediğiniz VPN bağlantı türünü seçebilir, tüm çalışanlarınızın Neptune ağınıza ait sanal makinelerde güvenli ve kesintisiz bir şekilde kullanabilirsiniz.

## KESİNTİSİZ BAĞLANTI

Neptün, güçlü ve yedekli iletişim altyapısı sayesinde sanal makinelerinize kesintisiz bağlantı olanağı sunar. Neptün Sanal makinenize 7/24/365 herhangi bir kesinti olmadan sorunsuz bir şekilde dilediğiniz noktadan Neptün'e ait bağlantı programı ile bağlanabilirsiniz. Neptün altyapısında bulunan fiziksel sistem bağlantı hatları yedeklidir ve Neptün altyapısında gerçekleştirilecek her türlü bakım/onarım/güncelleme işlemleri sizlerin bilgisi dahilinde yapılır ve tüm işlemler sistemde kesinti yapılmadan gerçekleştirilir.

## DİNAMİK YEDEKLEME

Neptün, çalışanlarınızın kullandığı tüm sanal makinelerin dinamik yedekleme işlemlerini talebiniz doğrultusunda (günlük, haftalık, aylık, vb.) ve belirttiğiniz zaman aralıklarında dinamik bir şekilde gerçekleştirir. Yedekleme işlemleri sırasında çalışanlarınızın kullandığı sistemlerin performansı etkilenmez ve hiçbir veri veya iş kaybı yaşanmadan çalışmalarına devam eder.

## TEMEL YAZILIM KURULUMU

Neptün, talep ettiğiniz işletim sistemine sahip sanal makineler içerisinde ihtiyaç duyduğunuz tüm temel yazılımları sizlere hazır şekilde sunmaktadır. Talep edeceğiniz tüm ek yazılımlar lisanslı bir şekilde sanal masaüstü Neptün makinenize kurulmaktadır. Bu da yazılım temini, lisanslaması veya kurulumu gibi iş yüklerinden kurtulmanıza yardımcı olur.

## GDPR UYUMLU GÜVENLİ SİSTEM

Neptün sistemi, GDPR (Global Data Protection Rule) uyumlu bir altyapıya sahiptir. Neptün sistem altyapısı, güncel siber saldırılara karşı proaktif güvenlik teknolojileri ve alanında uzman profesyonel ekibi ile sanal makinelerinizin güvenliğini sağlamaktadır. Sanal makinelerinizde barındırdığınız tüm verileriniz GDPR kapsamında koruma altındadır.

## KENDİ CİHAZINI GETİR

Çalışanlar, işlerini yapmaları için gerekli uygulamaları içeren güvenli masaüstü oturumlarına bağlanmak için kişisel cihazlarını kullanabilir.

## KOLAY YÖNETİM

Neptün sayesinde çalışanlarınızın kullandığı sanal makinelerde dilediğiniz donanımsal veya yazılımsal güncelleme veya değişiklik işlemlerini teknik bilgi sahibi olmanıza gerek duymadan Neptün kullanıcı hesabınıza ait yönetim panelinizden kolayca yapabilirsiniz.

# EĞİTİMLERİMİZ

SnipeSec, siber güvenlik dalında hazırladığı çeşitli eğitim ve kurslar vasıtası ile halkı bilişim ve siber güvenlik konusunda bilinçlendirmeyi ve daha güvenli ve bilinçli bir bilişim toplumu oluşmasına katkıda bulunmayı hedeflemektedir.

## TEMEL EĞİTİMLER

Bilişim kanunları ve yönetmelikleri, ağ, güvenlik, kriptoloji, işletim sistemleri gibi çeşitli alanlarda temel eğitimler veriyoruz.

## VERİ TABANI EĞİTİMİ

Veri tabanı eğitimleri, NoSQL ve Oracle gibi veritabanları hakkında yetkin bilgi vermek için tasarlanmıştır.

## GÜVENLİK EĞİTİMLERİ

Bu eğitimler, güvenlik hakkında derinlemesine bilgi edinmenize yardımcı olacaktır. Sızma testi, siber saldırıların analizi ve daha fazlası gibi siber güvenliğin tüm yönlerini kapsar.

## WEB EĞİTİMLERİ

Web eğitimler, FrontEnd ve BackEnd, API ile çalışma, Web güvenliği ve bir Web geliştiricisi olmak veya becerilerinizi geliştirmek için bilmeniz gereken her şeyi içerir.

## SANALLAŞTIRMA

Günümüzde sanal gerçeklik giderek daha popüler hale geliyor. Bu nedenle genel olarak Kubernetes, Yedekleme ve Sanallaştırma eğitimleri veriyoruz.

## MOBİL EĞİTİMLER

Bu eğitimler, IOS, Android'de mobil uygulama geliştirme ve güvenliği gibi bir mobil uygulama geliştiricisi olmak için gerekli tüm bilgileri içerir.

# Snipesec Neden İşiniz İçin En İyi Siber Güvenlik Şirketidir?

- Snipesec, Türkiye, Kıbrıs ve Estonya'da başarıyla faaliyet gösteren ve müşterilerine yüksek kaliteli hizmetler sunan şubeleri bulunan uluslararası bir kuruluştur.
- Snipesec, BT sektöründe yüksek kaliteli hizmetler sunan 10 yılı aşkın deneyime sahiptir.
- Snipsec, yeni Uzak Masaüstü Hizmeti Neptün 'ü kullanıma sundu . Start-up'ların, işletmelerin ve diğer kuruluşların sanki tek bir ofisteymiş gibi uzaktan çalışmalarına yardımcı olan, pazardaki bir yeniliktir.
- Snipsec, ISO 9001:2015 (Kalite Yönetim Sistemi standartları), ISO 27001:2013 (Güvenlik Yönetim Sistemi standartları) ve Genel Veri Koruma Kuralı (GDPR) akreditasyonuna sahiptir. Şirketin tüm kalite standartlarını karşıladığı anlamına gelir.
- Yeni iş parçacığı türlerinden haberdar olmak ve yeni siber güvenlik yöntemlerini öğrenmek için tüm çalışanlar sürekli eğitimden geçmektedir.
- Snipesec ile çalışırken, yürütülen tüm operasyonlar hakkında bilgilendirilebilmeniz için size haftalık ve aylık raporlar sunulacaktır.
- Snipsec, büyük ölçekli şirketlerin yanı sıra küçük ölçekli şirketlerle de işletmenizin bağımsız ihtiyaçlarını karşılayacak karşılık gelen hizmetleri bulacaksınız.
- Yukarıda listelenen hizmetleri sağlamak için yalnızca meşru şirketlerle çalışıyoruz. Hiçbir koşulda etik dışı işlemler yapmayız.
- Şirketin tüm çalışanları, zorlukları seven ve sonuçlara odaklı, yüksek eğitimli sertifikalı profesyonellerdir.

# REFERANSLAR

## Sonuçları şekillendiriyoruz ve her müşteri bizim için bir önceliktir.

Günümüzde işletmenizi dijitalleştirmemek, basitçe gelişmemek anlamına gelir. Misyonumuz, işletmelerin dijital dünyada büyümelerine yardımcı olmak, güvenliklerini ve emniyetlerini sağlamaktır. Her müşteri, bireysel olarak yaklaştığımız benzersiz bir durumdur; ancak her birine aynı ilgiyi gösteriyoruz.

**Bizim için en önemli olan, her türlü olaya anında müdahale edebilmektir.**
Herhangi bir yerde, herhangi bir zamanda bir olay olduğunda anında aksiyon alıyoruz, çünkü sistemde bir arızanın olduğu her dakikanın şirket için bir kayıp anlamına geldiğinin bilincindeyiz.

Müşterilerimizin teknik sorunlar nedeniyle işlevlerini durdurup herhangi bir kar kaybı yaşamalarını göze alamayız.

Bu nedenle yılın hangi günü ve hangi saati olursa olsun her zaman tetikteyiz.

# ÇÖZÜM ORTAKLARI

COMODO SSLCERTIFICATE

eset

Microsoft Solutions Partner

RUCKUS COMMSCOPE REGISTERED SOLUTION PROVIDER

veeam

# AKREDİTASYONLAR

Snipesec
CYBER SECURITY AGENCY

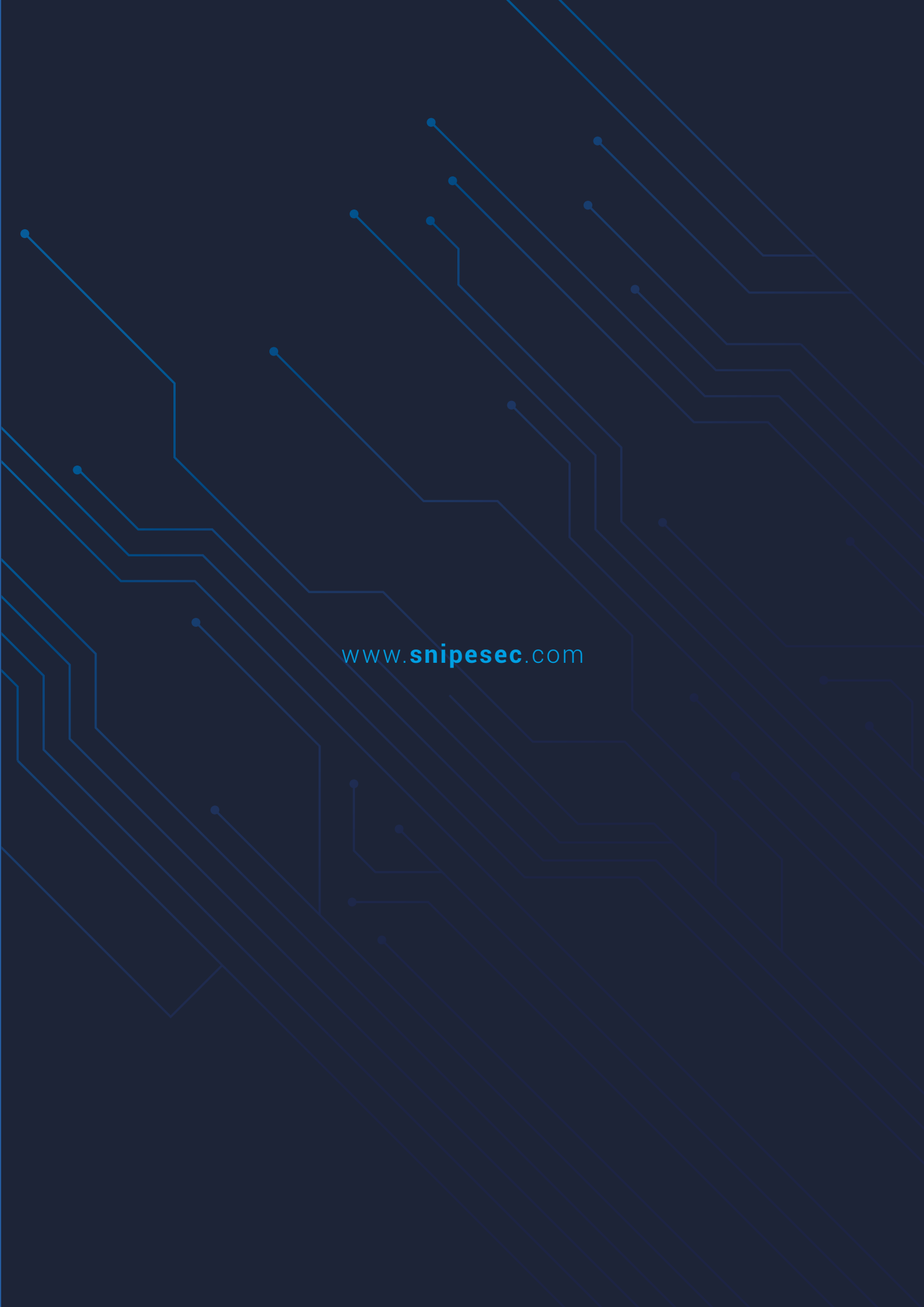
Kuzey Kıbrıs'ın ilk ve tek
**Akredite Bilişim ve Siber Güvenlik Şirketi**

ISO 9001:2015 Kalite Yönetim Sistemi

ISO 27001:2013 Bilgi Güvenliği

TSE-HYB

TF-CSIRT Trusted Introducer


www.snipesec.com

Snipesec
CYBER SECURITY AGENCY

DETECT DEFEND SECURE

**TÜRKİYE OFİS**
Eti Mahallesi Gazi Mustafa Kemal Bulvarı No 94/8 Çankaya, Ankara, Türkiye

**KIBRIS OFİS**
Şht. Mehmet Bayram Yaşar Sokak No:3/A , Yenişehir, Lefkoşa, Kuzey Kıbrıs.

info@snipesec.com | +90 (850) 303 27 04

www.snipesec.com