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 (Güvenlik Yönetim Sistemi standartları) ve Genel Veri Koruma Kuralı (GDPR) akreditasyonlarını almıştır. Şirketin tüm kalite standartlarını karşıladığı anlamına gelir. Ayrıca Snipsec, yeni Uzak Masaüstü Hizmeti Neptune'u tanıttı. Start-up'ların, işletmelerin ve diğer kuruluşların sanki tek bir ofisteymiş gibi uzaktan çalışmasına yardımcı olan, pazardaki bir yeniliktir.

SİBER GÜVENLİK
NEDEN ÖNEMLİDİR?

Siber güvenlik, ne kadar büyük veya küçük olursa olsun her kuruluş için önemlidir.

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

Siber suçlar artmaya devam ediyor çünkü

UCUZ > HIZLI > YÜKSEK KARLI

Siber suçlar, işletmelere milyonlarca dolarlık zararlar mal olabilir. Ancak bu, sadece finansal maliyetlerle ilgili değildir; aynı zamanda itibarlarına ve iş yapma yeteneklerine zarar verebilir, hatta bazen çalışanların, hastaların, müşterilerin ve diğerlerinin fiziksel güvenliklerini ve sağlıklarını tehlikeye atabilir.

Siber güvenlik, güven oluşturur. Siber güvenlik, müşteriler ve çalışanlar arasındaki güveni etkiler. İnsanlar, bilgilerinin düzgün bir şekilde korunduğunu ve gizli tutulduğunu hissetmediklerinde markaya, ürüne ve hizmetlere olan güvenlerini kaybetmeye başlarlar.

HACKERLAR HER GÜN GELİŞİYOR!

Başarılı bir işletme ancak güvenli ve korumalı olduğunda gelişebilir.

ALANINDA UZMAN EKİBİMİZ, VERİLERİNİZİ İZİNSİZ ERİŞİMLERE VE KÖTÜ NİYETLİ SALDIRILARA KARŞI KORUMAKTA ÜST DÜZEY TECRÜBE VE YETKİNLİĞE SAHİPTİR.

Bilgisayar korsanları artık sadece meraktan hareket etmiyor.

SİBER GÜVENLİK, YETKİN TESPİT VE YÜKSEK KALİTELİ SAVUNMA SAYESİNDE ŞİRKETİNİZE VE ZAMANINIZA MİLYONLAR KAZANDIRIR VE STRESİ AZALTIR.

Ekibimizin üstlendiği de tam olarak budur!

HİZMETLERİMİZ

Güvenlik Test Hizmetleri

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

Kuruluşunuz BT altyapısına ne kadar bağımlı?

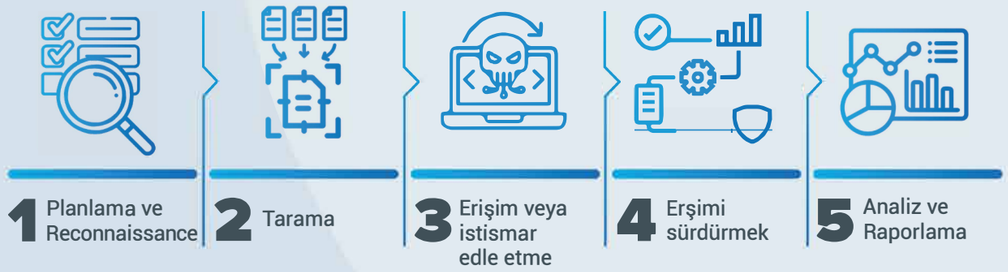
BT altyapınız bir günlüğüne bozulsa maliyeti ne kadar olur?

Bu soruları yanıtlayarak siber uzayda güvenliğin önemini öğreneceksiniz.

Çoğu kuruluş, risklerin ve bunların kendileri üzerindeki etkilerinin farkında değildir. Sistemlerinin saldırıya uğramasının çeşitli yollarını hayal edemezler. Riski bildiğiniz zaman, tehdidi en aza indirmek veya önlemek için önlemler alırsınız. Size yardımcı olabileceğimiz şey de tam olarak 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 önce bir hedef belirleyerek sistemi analiz ediyoruz. Ardından, güvenlik açıklarını tarayarak bunların istismar edilebilir olup olmadığını inceliyoruz. İstismar edilebilir bir güvenlik açığı tespit edildiğinde, saldırı gerçekleştirilir. Erişim sağlandıktan sonra, sisteme tekrar erişmek üzere kullanabileceğimiz bir arka kapı bırakmak önemlidir. Pentest sürecinin sonunda müşteriye, sisteminin güvenlik açıkları ve bunların nasıl düzeltileceği hakkında detaylı bir rapor sunulur.

Olay Müdahale Hizmeti SİBER AMBULANS

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

Çalışanlarınız işe geldiğinde birdenbire bilgisayarların çalışmasına izin vermeyen bilinmeyen bir virüs mü ortaya çıktı? Veya ağınızın çalışmasını durduran bir donanım sorunu mu yaşanıyor? Bu tür durumlarla karşılaştığınızda ve anında yardıma ihtiyacınız olduğunda, 7/24 SnipeSec'i arayabilirsiniz. İşletmenizin karşılaştığı sorunları anında çözüyoruz. Veri sızıntısı, hizmet kesintisi, felaket kurtarma ve yedekleme kaynaklarına yönelik saldırılar dahil, çeşitli siber tehditlerle karşı karşıyayız.

Şirketiniz bir siber olayla karşılaştığında, uzman olmayan kişiler tarafından olaya geç müdahale edilmesi veya panikle yanıt verilmesi şirketinize ciddi zararlar verebilir. SnipeSec olarak, uzman ve uzmanlaşmış kişilerden oluşan Olay Müdahale ekiplerimizle (CSIRT), şirketinizin maruz kaldığı her türlü siber olayda kurumsal operasyonlarınızın devamlılığını ve güvenliğini korumak amacıyla Olay Müdahale hizmeti sunuyoruz.

Şirketinizdeki kritik müşteri bilgileriniz, finansal bilgileriniz veya çeşitli plan ve projelerinizin sızmasına neden olabilecek bir veri sızıntısına karşı gerekli tüm önlemleri alıyoruz.

Acil müdahale hizmetimiz 7/24/365 hizmet vermektedir.

HİZMETLERİMİZ

Güvenlik Operasyon Merkezi

Sisteminizin 7/24/365 gözetimi

Ağınızın 7/24/365 izlendiğinden ve herhangi bir olay durumunda anında önlem alındığından emin olmak ister misiniz?
Bu nedenle, işinizin tüm teknik yönleriyle ilgilenen uzak bir BT ekibi olarak SOC hizmeti sunuyoruz. SOC ile, ek çalışan, ekipman, ilave ofis alanı gibi konularda endişelenmenize gerek kalmadan sadece aldığınız hizmet için ödeme yaparsınız.

Küçük ve Orta Ölçekli şirketler, altyapı büyüklüğüne ve kişi sayısına göre basit bir aylık faturalandırma modeli ile Güvenlik Operasyon Merkezi Hizmeti'nden (SOCaaS) hızlı ve verimli bir şekilde yararlanabilir.

Güvenlik Operasyon Merkezi (SOC), şirketinize yönelik iç ve dış tüm siber güvenlik olaylarını tespit etmek, analiz etmek, önlemek ve müdahale etmek amacıyla kurulmuş, güvenlik durumunuzu sürekli izlemenize ve iyileştirmeler yapmanıza yardımcı olan kurum içi merkezi bir yapıdır.

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

SOC hizmeti sırasında danışmanlarımız:

- **Güvenlik açıklarının ve güvenliğin mevcut durumu hakkında rapor verecektir.**
- **Maliyet optimizasyonu için en uygun siber güvenlik mimarisini ve stratejilerini önerir.**
- **Gerekli güvenlik araç setini uygulayacak, özelleştirecek ve destekleyici süreçler oluşturacaktır.**
- **Paket bazında tüm SOC sorumluluklarını üstlenecektir.**
- **Yeni bulgular ve daha fazla iyileştirme fikirleri hakkında düzenli olarak rapor verecektir.**

Güvenlik Operasyon Merkezi

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 bir kullanıcı tanımlanarak hassas bilgilere erişim sağlandığında bu durumdan haberdar olma süreciniz nedir ve bu erişimi nasıl tespit edersiniz?
- Kullanıcıların yetkileri güvenlik riski oluşturacak şekilde değiştirildiğinde veya yükseltildiğinde, bu değişiklikleri nasıl ve ne zaman fark edersiniz? Yetki değişikliklerini izlemek için kullanılan yöntemler nelerdir?
- 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 kritik öneme sahip dosyalara yetkisiz erişim gerçekleştiğinde veya yetkisiz erişim denemesi olduğunda, bu durumu nasıl anlarsınız ve yetkisiz erişimleri önlemek veya tespit etmek için hangi güvenlik önlemleri alınıyor?
- 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, emsallerine göre daha yüksek satış artışı ve dayanıklılıktan yararlandığını biliyor muydunuz? Dijital olarak olgun bir kuruluş, yaptığı her şeyde dijital teknolojiyi ve bununla ilişkili kültürü ve ağları en iyi şekilde kullanan kuruluştur. Dijital olgunluk, bugün var olan dünyaya ve içindeki insanlara uygun hale gelmektir. Dijital Dönüşüm, mevcut süreçlerinizi otomatikleştirerek iyileştirebilir, böylece kârınızı önemli ölçüde artırabilir. Ancak Dijital Dönüşümü uygulamadan önce, şirketinizin şu anda nerede olduğunu ve ne ölçüde iyileştirilmesi gerektiğini bilmek için Dijital Olgunluk Değerlendirmesine ihtiyaç vardır.

Bu hizmetimizin yanı sıra firmanızın teknolojiye ayak uydurmasını ve işletmenizin sınırlarını ülke sınırlarının dışına taşımasını da sağlıyoruz.

Firma profilinizin oluşturulması ve SWOT analizi ile başlayan danışmanlık sürecinde firmanızın tüm yönlerinin belirlenmesi ile dijital dönüşüm süreçlerinizin planlanması ile firmanıza katma değer sağlayacak gerekli tüm stratejileri sizin için oluşturmaktayız.

Danışmanlık hizmetimiz süresince sizlere teknolojik anlamdaki tüm konularda (alım-satım, yatırım, projelendirme, kar-zarar analizi v.b.) danışmanlık hizmeti sağlamakta, firmanız ile teknoloji alanında yapmayı planladığınız tüm yatırımlarınızda sizlere uluslararası bağlantılarımız kapsamında destek vermekteyiz.

Dijital Olgunluk Değerlendirmesi

Dijital olgunluğunuza yatırım yapmak, başarınıza yatırım yapmaktır.

Günümüzde teknolojinin iyileştiremeyeceği neredeyse hiçbir alan kalmadı. Bu nedenle, bir dijital olgunluk değerlendirmesi yapmak ve teknolojiyi işletmenizin en büyük sorunlarını çözmek, çalışanlarınızı motive etmek ve işlerini daha verimli hale getirmek için kullanmak, zaman ve çaba harcamaya değer bir adımdır. Geleceğe açık ve vizyoner bir yaklaşımla, işletmeniz mevcut engellerin üstesinden gelebilir ve böylece sürdürülebilir bir başarı yakalayabilir.

Dijital olgunluk araştırmanızın ardından, dijital olgunluk seviyenizi ölçme ve iyileştirme konusunda rehberlik ve stratejik tavsiyeler alacaksınız. Ayrıca, dijital olgunluk analizinizden elde edilen içgörüleri kullanarak, işletmenize özel bir dijital strateji oluşturmanıza yardımcı olacağız.

Organizasyonunuz, zamanla ve teknolojiyle uyumlu bir şekilde sürekli dönüşmezse, uzun vadede sürdürülebilirliği sıkıntıya girecektir.

HİZMETLERİMİZ

Zararlı Yazılım Analizi

KÖTÜ AMAÇLI DOSYALARIN KONTROLÜ

Günümüzde işletmenizin performansını bozabilecek 20'den fazla kötü amaçlı yazılım türü vardır. Hepsinin ortak bir yanı var - hepsinin şirketlere milyonlar kaybettirmesi. Dünyanın dört bir yanındaki bilgisayar korsanları, küçük, orta ölçekli ve büyük işletmeleri hedef alarak muazzam miktarda kâr elde ediyor. Eskiden insanlar doğrudan mağazanızdan hırsızlık yapabilirdi, bu nedenle her binada hırsızlardan korunmak veya kimliklerini öğrenerek onları cezalandırmak için gözetleme kameraları vardır. Bununla birlikte, dijital bir ağ üzerinden hırsızlık yapmak, mağazadan bazı öğeleri çalmaktan daha az çaba gerektirir, daha ucuz ve daha karlıdır.

Bu nedenle, dünya çapında çeşitli türlerde karmaşık kötü amaçlı yazılımlar icat eden binlerce bilgisayar korsanı var. Herkesi hedefliyorlar çünkü günümüzde internet ülke, dil veya diğer özelliklerle sınırlı değil. Kuruluşlar, ağlarına virüs bulaştığının farkında bile olmayabilir. Ve hiç beklemedikleri bir anda, kurum için değerli olan her şeyi alt üst ederek, performansını duraksatıyor.

Kötü Amaçlı Yazılım Analizi hizmeti ile şirketinizi veya tüm bilgi işlem altyapınızı bulaştıran ve şirketinizin sistemlerine koruma sağlayan kötü amaçlı yazılım türevleri (kötü amaçlı yazılım, fidye yazılımı, dropper, casus yazılım vb.) için derinlemesine analiz ve temizleme hizmeti verilir.

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

Zararlı Yazılım Analizi

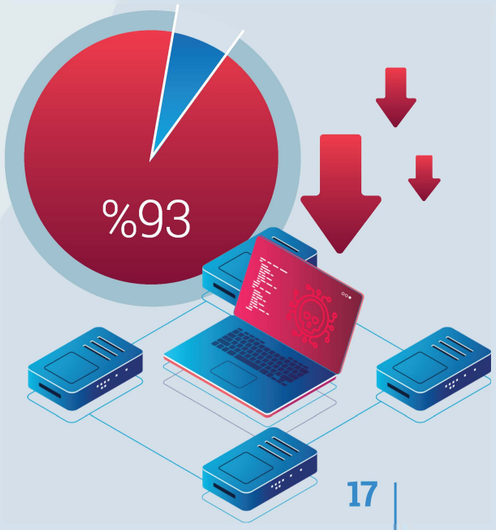
Kötü Amaçlı Yazılım Türleri

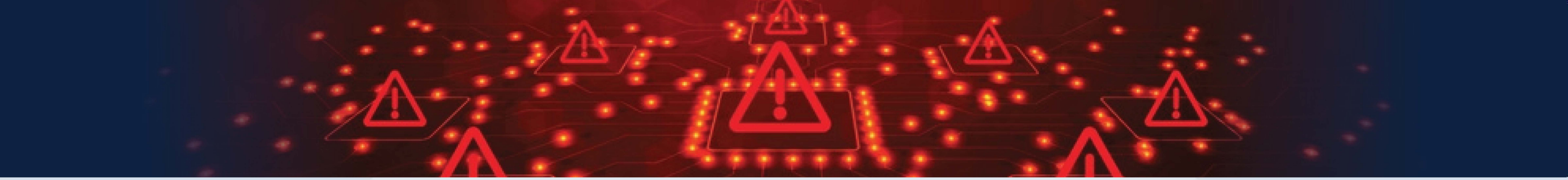
FİDYE YAZILIMI

İşletmeniz bilgisayarlara ve bilgisayarlardaki verilere ne kadar bağlı? Ya sahip olduğunuz tüm ağlar bir günlüğüne çalışmayı durdurursa? İşletmeniz bir günde ne kadar para kaybeder? Peki ya haftalar? Bilgisayar korsanlarının şu anda hesapladığı şey bu. Hesaplamalardan sonra,sisteminize girerler, dosyalarınızı şifrelerler veya şifrenizi değiştirirler veya siz ödeme yapana kadar sisteminizi tutmak için başka bir şey yaparlar. Bir gün ofisinize giriyorsunuz, bilgisayarınızı açıyorsunuz ve şöyle bir şey görüyorsunuz, "Bilgisayarınız kilitlendi. 10.000$ ceza ödemeniz gerekiyor ve bu bağlantıyı kullanarak Bitcoin ile ödeyebiliyorsunuz. geri erişim. Bana ödeme yaparsan, sana gizli kilit açma kodunu vereceğim ve sonra onu küçük beyaz kutuya koyup tamam'a basabilirsin". Ve çoğu zaman, ödeme yapsanız bile, anahtara tekrar erişmenize izin vermezler. En iyi durumda, yaparlar. En kötü durumda, şimdi paranızı aldılar ve karşılığında gösterecek hiçbir şeyiniz yok. Ransomware çok acı verici olabilir. Saldırganlar işletmeleri daha da yoksullaştırıyor. Fidye saldırılarında büyük paralar var, yılda yüz milyonlarca dolar, hatta belki milyarlarca dolar ve bilgisayar korsanları çok daha zengin oluyor. Dünyanın en iyi siber suçluları, St. Petersburg'daki veya dünyanın diğer şehirlerindeki bazı genç adamlar gibi ayda bir milyon dolar kazanıyorlar. Ve küçükten büyüğe her türden işletmeyi hedefliyorlar.

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, farkında olmadan bilgisayarınıza bulaşabilir. Örneğin, işiniz için gerekli bir web sitesinden bir program indirmeye çalıştığınızda, kurulum dosyasının içinde kötü amaçlı kodlar gizli olabilir. Programı çalıştırdığınız anda bu kodların bilgisayarınıza yüklenmesine izin vermiş olursunuz ve virüs sisteminize yerleşir. Bu aşamadan sonra virüs, çoğalmaya ve yayılmaya çalışacaktır ve bunu sizin bir kullanıcı eyleminiz sayesinde gerçekleştirecektir. Örnekte olduğu gibi, programı yüklemeniz virüsün çalışmasına ve zararlı eylemlere başlamasına, örneğin uygulamaların çökmesine, neden olabilir. Bu da virüsün ağınıza yayılmasına zemin hazırlar. Farklı karmaşıklık seviyelerine sahip çeşitli virüs türleri bulunur. Antivirüs sağlayıcılarımız her geçen gün virüslerin nasıl çalıştığını anlamada ve onları durdurmada daha da gelişmektedir. Ancak, virüs üreticileri, şifrelenmiş virüsler gibi antivirüs programlarının tespitini zorlaştıran yöntemler geliştiriyor. Bu da sürekli bir mücadele olarak, kötü niyetli kişiler yeni yöntemler buldukça, güvenlik uzmanlarının da savunma mekanizmalarını iyileştirmesini gerektiriyor.

Zararlı Yazılım Analizi

Kötü Amaçlı Yazılım Türleri

TRUVA ATI

Bu kötü amaçlı yazılım türüne geçmeden önce, kısa bir tarih dersiyle başlayalım. Binlerce yıl öncesine, Yunanistan ile Truva arasında süren savaşa dönelim. Yaklaşık 10 yıl süren bu savaşın ardından, Yunanlılar kuşatmadan yorulup yeni bir strateji denemeye karar verdiler. Büyük bir tahta at inşa ettiler ve bunu barış teklifi olarak Troya şehrine sundular. Ancak bu zararsız görünen hediye, aslında Yunan askerleriyle doluydu. At, şehrin içine alındıktan sonra gece boyunca içindeki askerler dışarı çıkarak şehrin kapılarını Yunan ordusuna açtı ve Truva şehri yerle bir edildi. İşte bu, bir Truva atının ilk örneğiydi. Günümüzde, bilgisayarlarda kullanılan Truva atları (Trojanlar) da benzer şekilde çalışır. Bir yazılım, size yararlı bir işlev sunacağını söyler, ancak gizlice kötü amaçlı bir işlevi de yerine getirir.

Örneğin, çocukluğumuzda çok popüler olan Tetris oyununu ele alalım. Herkes bu oyuna sahip olmak istiyordu ve arkadaşlar birbirine oyun disklerini verirdi. Ancak bir kişi, oyunun içine bir Truva atı yerleştirdi. Siz oyunu bilgisayarınıza yükleyip oynamaya başladığınızda, perde arkasında kötü amaçlı bir yazılım çalışır ve sizin sisteminizle başka bir kişi arasında bir bağlantı kurarak makinenizi uzaktan kontrol etmelerine olanak tanırdı. Bu, kritik verilerinizin çalınmasına, dosyalarınızın silinmesine ya da sisteminizin işleyişinin ciddi şekilde kesintiye uğramasına neden olabilirdi.

Başarınızı güvence altına almak için gizliliğinizi koruyoruz.

Zararlı Yazılım Analizi

Kötü Amaçlı Yazılım Türleri

KÖTÜ AMAÇLI SPAM

Emotet, öncelikle e-posta spam'ı (malspam) yoluyla yayılan bir saldırıdır. Amazon'dan, bankanızdan meşru bir e-posta kılığına girmiş bir e-posta veya bir bağlantıya tıklamanızı veya bir eki indirmenizi söyleyen tanıdığınız birinden bir not alabilirsiniz. Bunun meşru bir e-posta olduğunu düşünerek, bunu yapmaktan çekinmeyeceksiniz. Özellikle, bu e-posta tanıdığınız birinden geliyorsa. İlk enfeksiyon bu şekilde yapılır.

Daha sonra bağlı sistemlere üç ana yoldan yayılmaya çalışacaktır. Öncelikle, şimdi bu sefer kişilerinize erişecek ve sizden gelmiş gibi görünen bir kimlik avı e- postası gönderecek. Ardından, ağınızdaki diğer sistemlere (evdeki veya kuruluşunuzdaki diğer bilgisayarlar olabilir) yayılmak için bilinen yazılım güvenlik açıklarını kullanmaya çalışacaktır. Son olarak, şifreyi kırarak tüm bilgileri almaya çalışacaktır.

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

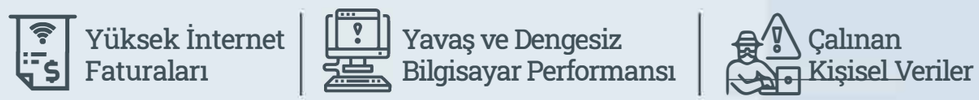
Zararlı Yazılım Analizi

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:



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, 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 ve bunların hepsini toplar ve üzerinizde bir profil oluşturur. en iyi senaryo. En kötü durumda, bir web sitesi adını ve kullanıcı adınızı ve şifrenizi yazarsanız, bunu toplayabilir ve saldırgana geri gönderebilir. Hatta ekranda gördüklerinizin ekran görüntülerini alma ve bunları e-posta veya anlık mesaj yoluyla rutin aralıklarla geri gönderme özelliğine de sahiptir.

Dünya çapında her 39 saniyede bir siber saldırı gerçekleşmektedir.

DONANIM SORUNLARI

Altyapınızın kullandığı donanımın hala lisanslı olduğundan ve eski olmadığından emin misiniz? Güncelliğini yitirmiş eski sistemlerin bakımı pahalı olabilir. Teknolojinin çok daha hızlı eskimesi dışında, çok eski bir ev veya aracın bakımını yapmaktan çok da farklı değil. Eski bilgisayar, harddisk vb. kullanıyorsanız bir gün sisteminiz çökebilir veya üreticiler destek vermeyi bıraktığı için virüs bulaşabilir. Bu nedenle, altyapınızın güncelliğini yitirmiş olması nedeniyle güvenlik risklerine ve virüslere karşı savunmasız olmadığından emin olmak istersiniz.

HİZMETLERİMİZ

Yayından Kaldırma Hizmeti

İtibarınızı koruyun.

"Take Down", pazar payınızı ve şirketinizin itibarını kaybetmeniz için şirketinizin markasına ve pazar payına zarar veren çevrimiçi yayınlanan içeriklere karşı yasal çerçevede ve size yardımcı olan ve yol gösteren bir hukuk danışmanlığı hizmetidir.

Şirketinizin marka itibarını tehdit eden, müşterilerinizi kaybetmenize ve dolayısıyla ticari faaliyetlerinizin azalmasına neden olabilecek çevrimiçi içeriklerin kaldırılmasını gerekli yasal düzenlemelere uygun olarak gerçekleştiriyoruz.

Hizmet verdiğiniz alandaki hizmet koşullarınızı ihlal eden çeşitli içerikler, sosyal medya içerikleri, profiller, çevrimiçi hesaplar veya web sayfaları, Take Down hizmeti ile yasal olarak kapatılır ve yayından kaldırılır.

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.

HİZMETLERİMİZ

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

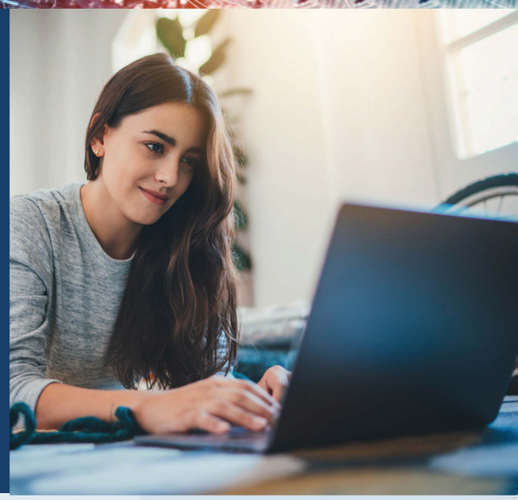
Eşsiz anonimlik sistemimizle izlenmeden web'de gezinebilirsiniz

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 İşlem yatırım maliyetlerini en aza indirgemek ve bu servisleri yönetirken çoğu kuruluşun karşılaştığı teknik zorlukları ve verimsizlikleri gidermek için oluşturulmuş ve Uzak Masaüstü Hizmetlerini (RDS) destekler nitelikte bir hizmettir.

Bu hizmet, ofis çalışanlarının ötesinde eğitim kurum ve kuruluşlarında da yatırım, bakım-onarım maliyetlerinin düşürülmesi, eğitim-öğretim faaliyetlerinde kullanılan uygulama laboratuar altyapıları için kaliteli hizmet sunulabilmesi maksadı ile yaygınca 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

HİZMETLERİMİZ

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

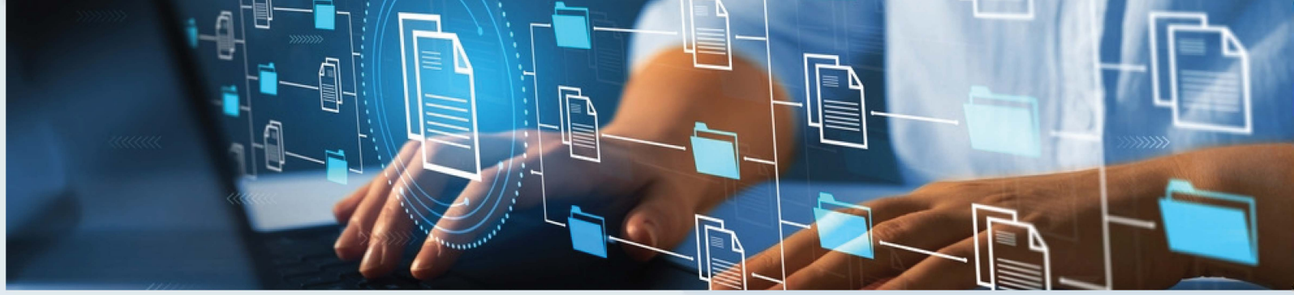
Neptün, sizleri tüm donanımsal arıza ve bakım-onarım maliyetlerinden uzak tutar. Neptün sayesinde gelişmekte olan bilişim dünyasında donanım güncellemesi veya bakım-onarım işlemlerini düşünmenize gerek kalmaz, Neptün altyapısında tüm donanım güncellemeleri ve bakım-onarım faaliyetleri tarafımızca yapılmaktadır. 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.) ayni lab ortamına bağlanma imkanına sahip olur.

ANONİM VPN BAĞLANTISI

Neptune offers a secure VPN connection in line with your anonymity request for your internet connection on the machines within the virtual network you want to create belonging to your company. You can choose the type of VPN connection you want for your employees among the VPN options offered upon your request, and you can use them safely and uninterruptedly on virtual machines belonging to all your employees Neptune network.



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 kullanmakta olduğu tüm sanal makinelerin dinamik yedekleme işlemlerini* talebiniz doğrultusunda (günlük,haftalık,aylık.v.s) ve belirttiğiniz zaman aralıklarında dinamik şekilde gerçekleştirir. Yedekleme işlemlerinin gerçekleştiği esnada çalışanlarınızın kullandığı sistemlerin performansı etkilenmez ve hiçbir veri ve iş kaybına uğramaksızın çalışmaya devam eder.

TEMEL YAZILIM KURULUMU

Neptün, talep ettiğiniz işletim sistemine sahip sanal makineler içerisinde ihtiyacınız olan tüm temel yazılımları* sizlere hazır şekilde sunmaktadır. Talep edeceğiniz tüm ek yazılımlar lisanslı şekilde sanal masaüstü Neptün makineniz içerisine kurulmaktadır. Bu da sizlerin 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 Neptune'u tanıttı. 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.
- Snipesec, büyük ölçekli şirketlerin yanı sıra küçük ölçekli şirketlerle İşletmenizin 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

Sonuçlar elde etmeyi hedefliyoruz
ve her müşteri bizim için en iyi durum olmalıdır.

Günümüzde işletmenizi dijitalleştirmemek basitçe gelişmemek anlamına gelir. Misyonumuz, işletmelerin dijital bir dünyada büyümelerine ve güvenliklerini ve emniyetlerini sağlamalarına yardımcı olmaktır. 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 dondurup herhangi bir kar kaybetmelerini göze alamayız. Bu nedenle yılın hangi günü ve hangi saati olursa olsun her zaman tetikteyiz.

FROG PEST CONTROL
OSCAR GROUP
OSCAR PARK HOTEL
OSCAR RENT A CAR
OSCAR PETROL
Bellapais Monastery Village
WEN AJANS
VUNI PALACE HOTEL CASINO • SPA • CONVENTION
STM ENGINEERING | TECHNOLOGY | CONSULTANCY
OSCAR MOTORS OSCAR GROUP OF COMPANIES
OSCAR GROUP
NTL NORTHERN TRAVEL
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI EGM

ÇÖZÜM ORTAKLARI

COMODO SSL CERTIFICATE
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, Turkey

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