T.C.
ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ
REKTÖRLÜĞÜ
İdari ve Mali İşler Daire Başkanlığı

Sayı : 19207542-934.01/ 24.06.2020

Konu : Teklife Davet

Sayın :

Kurumumuzun ihtiyacı olan (2) kalem ANTİVİRÜS YAZILIM ALIMI işi satın alınacaktır. İlgilendiğiniz takdirde K.D.V. hariç fiyat teklifinizi en geç 30/06/2020 tarihine kadar göndermenizi, teklifinizde teslimat süresinin de bildirilmesini rica ederim.

Ali KANBER
Satınalma Şube Müdürü

Satınalma tarih ve saati : 30/06/2020 - 10:00
Teklif Başvuru Yeri : Eskişehir Osmangazi Üniversitesi Rektörlüğü İdari ve Mali İşler Daire Başkanlığı Meşelik Kampüsü/ESKİŞEHİR

Teslimat Yeri : Eskişehir Osmangazi Üniversitesi Rektörlüğü Depoları Meşelik Kampüsü-ESKİŞEHİR

Teklif Türü : Teklif Birim Fiyat - İşin tamamı

İhtiyaç Listesi

Sıra No	Malın / İşin Adı	Miktar	Birim	Birim Fiyat	Tutar
1	SUNUCU ANTİVİRÜS YAZILIMI	1	ADET		
2	SON KULLANICI ANTİVİRÜS YAZILIMI	1	ADET		

EK: Teknik şartname

Satınalmanın Yapılacağı Birim: ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ
NOTLAR:
1) Teklif mektupları üzerinde sipariş sonrasında ürünlerin kaç günde teslim edileceği belirtilecektir.
2) Teklif zarfları elden, posta veya faks yolu ile tarafımıza gönderilecektir.
3) Teklif edilen malzemelere ait orijinal katalog var ise teklif mektupları içerisinde getirilmesi gerekmektedir.
4) Şartlı teklifler ve Türk Lirası haricinde verilen fiyatlar değerlendirmeye alınmayacaktır.
5) Teklif edilen ürünlerin marka ve modelleri teklif mektubunda ayrıntılı olarak belirtilecektir.
6) Teklifler KALEM bazında değerlendirilecektir.
7) İSTEKLİLER VERGİ NO/TC NUMARALARINI MUTLAK SURETLE BELİRTECEKLERDİR.

Meşelik Kampüsü ESKİŞEHİR
Telefon: (222) 2393750-5505-5506 Faks: (222)2290056 e-posta: esogusatinalma@ogu.edu.tr Elektronik ağ: www.ogu.edu.tr

19.06.2020

Endpoint Protection Teknik Şartnamesi

Teklif edilecek çözümün, merkezi yönetim modülü ve koruma sağlanacak sistemlere kurulacak olan yazılım ile birlikte iki bileşenden oluşacak olup her iki bileşen aynı üreticinin ürünü olmalıdır.

Teklif, en az 750(yedi yüz elli) kullanıcılı olacaktır.

Teklif edilen çözüme ait lisanslar ile birlikte en az 3 (üç) yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir.

Merkezi Yönetim Modülü

Yönetim Modülü bulut tabanlı olmalı ve web arayüzüne internetin olduğu herhangi bir noktadan tablet, telefon, bilgisayar ile erişim sağlanmalıdır.

Active Directory ile düşük boyutlu bir yazılım kurularak entegre olmalı, kullanıcı ve kullanıcı grubu bilgilerini otomatik olarak belirli periyotlarda, yönetim konsoluna aktarılmalıdır.

Her politika için hazır şablonlar olmalı ve sistem yöneticisi kendi isteğine özel politikalar oluşturabilmelidir. Politikalar kullanıcılara ve cihazlara özel oluşturulabilmelidir.

Rol tabanlı (kullanıcı, yönetici, süper yönetici, yardım masası ve salt okunur) yönetim özelliği bulunacaktır.

Her kullanıcı bilgisayarı için özel bir parola üretilmeli ve bu parola ile yazılımın sistem üzerinden kaldırılması, görev yöneticisinden servisin durdurulması ve kritik bazı servislerin devre dışı bırakılması önlenmelidir.

SIEM ürünleri ile entegre olabilmeli ve entegrasyon yönetim konsolundan temin edilen API token ile yapılmalıdır.

Yönetim Konsolu üzerinde yapılan aksiyonların Audit Log'larına belirli zaman aralıkları seçilerek erişilebilmeli ve 90 günlük zaman diliminde bu log'lar çekilebilmeli, CSV/PDF formatlarında indirilebilmelidir.

Çeşitli kategorilerde yer alan internet sitelerine erişimleri sınırlandırabilmek amacıyla web filtreleme politikaları oluşturulabilmeli, sistem yöneticisinin istediğine özel url, ip adresi, domain bilgisine göre tanımlar eklenebilmelidir.

Uygulama kontrolü için çeşitli kategorilerde uygulamaları, üretici yönetim konsolunda bir liste halinde sunmalı ve sistem yöneticisi bu listeden dilediği uygulamayı seçip, kullanıcı bilgisayarında çalıştırılmasını önleyebilmelidir.

Veri Sızıntısını önlemek amacıyla belirli dosya türüne, adına yada dosyanın içerisinde geçen anahtar kelimelere göre kurallar oluşturulabilmeli ve kritik verilerin harici çıkarılabilir medya, tarayıcı , Skype, Skype for Businees, Outlook, Outlook Express, Thunderbird, Microsoft Lync gibi uygulamalar üzerinden sızdırılması durumunda ya tamamen bloklanmalı yada kullanıcının inisiyatifine bırakılmalıdır. Bu işlemlerin log'u tutulmalıdır.

Cihaz kontrolü politikalarında, harici çıkarılabilir medya, Wireless, MTP/PTP, Bluetooth gibi donanımların kontrolü sağlanmalıdır. Model ya da Cihaz ID'sine göre istisnalar oluşturulabilmelidir.

Yönetim konsolunda, makinalara kurulan ajan yazılımların güncelleme işlemleri belirli zaman aralıklarında durdurulabilmeli ya da sistem yöneticisi tarafından kontrollü yapılabilmelidir.

Ufuk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen

Gelişmiş tehditlerin kurum ağında diğer cihazlara yayılmasını önlemek amacıyla üreticinin, güvenlik duvarı ürünü ile entegre çalışabilmelidir ve tehditleri otomatikleştirilmiş olay çözümleme yöntemi ile bertaraf edebilmelidir.

Raporlama Özellikleri

Grafiksel olarak belirli zaman aralıklarında cihaz, web, dlp, uygulama kontrolü ve diğer modüllerin raporları oluşturulmalıdır. CSV, PDF formatında ulaşılabilmeli, yazıcıdan çıktı alınabilmelidir.

Agent(Ajan) yüklü olan bilgisayarda bir olay meydana geldiğinde, otomatik olarak sistem yöneticisine detayları içeren bir e-posta gönderilmelidir. Olay detayları, farklı seviyelerde(düşük, orta ve bilgi) yönetim konsolunda sınıflandırılmalıdır.

Belirli kategorilerde zamanlanmış raporlar oluşturulabilmelidir.

Koruma Ajanı Modülü

Bulut tabanlı yönetim yazılımı ile HTTPS 443 portu üzerinden güvenli bir şekilde iletişime geçmelidir.

Windows 7, 8, 8.1, 10, Mac OS X 10.11, 10.12, 10.13, 10.14 desteğine sahip olacaktır.

Sisteme erişim sağlayan zararlı bir uygulama, komuta edildiği bir sunucuya bağlanması durumunda trafik analiz edilmeli ve bir anomali tespit edilmesi durumunda bu uygulamanın trafiği sonlandırılmalıdır.

Virüs'lerin, antivirüs yazılımını durdurmasını önleyen, aynı zamanda yazılımın servislerini ve kaldırma işlemini denetleyen bir yapılandırma olmalıdır. Bu sayede kullanıcılar kritik servisleri devre dışı bırakmamalıdır.

Ajan, kurulu olduğu bilgisayarda herhangi bir dosya açıldığında veya çalıştırıldığında, değişiklik yapıldığında güvenliği sağlamak amacıyla hızlıca taramalıdır.

Davranışsal tarama(behaviour scan) özelliği olacaktır. Aynı zamanda, antivirüs taraması esnasında üreticinin istihbarat ağ'ından son güncel tehditler sorgulanmalıdır.

Arşivli olan dosyaların içerisi taranabilmelidir.

Makinalara Ajan kurulumlarında ve sonraki zamanlarda çeşitli komponentlerin imza güncellemesini yapabilmesi için kurum içerisindeki bir veya birden fazla sunucuya "Update Cache" rolü atanabilmeli. Band genişliği kullanımını en aza indirgemek için tüm makinalar bulut ortamında ki sunucudan önce güncelleme dosyalarını içerdeki bir sunucudan çekebilmelidir. Eğer Update Cache sunucusuna erişim sağlayamazsa, bulut tabanlı sunucudan güncellemelerini otomatik olarak almalıdır.

Tarama işlemleri için farklı seviyelerde dosya, dizin, proses için istisna(exclusion) özelliği olmalıdır.

Ajan, çeşitli kurulum yöntemlerini desteklemelidir. Manuel, Group Policy, 3.parti araçlar(System Center Configuration Manager, vs.) ve e-mail yöntemlerini desteklemelidir.

Boot CD ve Boot USB oluşturulabilecek ve bilgisayar taraması yapılabilecektir. Virüs, trojan ve diğer zararlı yazılımların tespiti için alternatif olarak çeşitli araçlar(virus removal tool, source of infection tool) sunmalıdır.

Şüpheli bir dosya tespit edildiğinde, bu dosya karantina bölgesine alınmalı ve sistem yöneticisinin inisiyatifine göre SHA-256, sertifika yada yol bilgisine göre yönetim konsolunda, uygulamaya izin verilebilmelidir.

Ufuk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen

Kullanıcıların zararlı içerik-kod barındıran internet sitelerine erişimlerini engellemeli ve dosya indirme esnasında dosyanın repütasyon kontrolünü sağlamalıdır.

Ajan kurulumlarında proxy desteği sağlanmalıdır.

Güncelleme ve yönetim trafiği birbirinden (gerektiğinde) ayrı yönetilebilmelidir. Internet erişimi olmayan makinelerde yönetim trafiği, internet erişimi olan sunucuya rol ataması yapılarak gerçekleştirilebilmelidir.

Yeni Nesil Uç nokta koruma yazılımı

Önerilen çözüm, imzasız yeni nesil bir koruma sunmalı ve ileri seviyedeki zararlı yazılımları temizleyebilmelidir.

Dosya sistemi düzeyinde izleme sağlamalı ve dosyaları değiştirmeye çalışan makineleri ve prosesleri sürekli olarak gözetmelidir.

Fidyecilik amaçlı kullanılan zararlı uygulamalar tarafından hedeflenen kritik çalışma dosyalarının korumasını sağlamalı,şifreleme esnasında durdurulmalı ve dosyalarda oluşabilecek bir şifreleme işleminde, varsayılan güvenli durumuna geri döndürmelidir.

Hem yerel hem de uzak paylaşım dosyalarının toplu şifrelemesini engellemelidir.

Belirtilen çözüm diğer antivirus ürünleri ile birlikte uyumlu çalışabilmelidir.

Bir bulaşma olduğunda, nereden kaynaklandığını ve nasıl yayıldığını ayrıntılı olarak, kök neden analizi yaparak raporlamalıdır. Kök neden analizi, söz konusu saldırı hakkında ve gelecekte bunların nasıl önleneceği hakkında adli (forensic) rapor hazırlayabilmeli, Process Tehdit Zinciri görselleştirme yapabilmelidir.

Yazılımlarda oluşabilecek bir açıklıklardan faydalanan suistimal yazılımlarına (exploitler) karşı tekniklerini inceleyen imzasız bir koruma sağlamalıdır.

Sıfırıncı gün (Patient-Zero / Zero-Day) koruması sağlamalı ve RAM'lere yerleşebilen "Memory-Resident Ataklarını" bloklayabilmelidir.

Kurulum gerektirmeyen zararlı yazılım temizleme aracına sahip olmalıdır.

Uç nokta bilgisayarları üzerinde performansa etkisi minimal olmalıdır.

Komuta ve control (Command & Control) merkezlerine giden trafiği tespit edebilmelidir.

Suistimal yazılımı önleme (exploit prevention) ve tarayıcı suistimal yazılımı önleme (browser exploit prevention) özelliklerine sahip olmalıdır.

Bulut tabanlı yönetim konsolu olmalı, kolay kurulum ve politika yönetimi sunmalıdır.

Office uygulamaları yada diğer kurumsal uygumalar false positive tespiti durumunda istisna kuralları oluşturulabilmeli ve uygulamaların çalışma süreçleri etkilenmemelidir.

Önerilen çözümün üreticisi uç nokta korunmasında Gartner'da en az 5 yıl liderler bölümünde olmalıdır.

Yeni nesil güvenlik çözümü, derin ögrenme modeli kullanarak tehdit dünyasında yer alan çok sayıda bilinen/bilinmeyen zararlı yazılımlara karşı kısa sürelerde tespit, koruma ve önleme yetenekleri sağlamalıdır.

Ufuk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen

18.06.2020

Server Protection Teknik Şartnamesi

Teklif edilecek çözümün, merkezi yönetim modülü ve koruma sağlanacak sistemlere kurulacak olan ajan ile birlikte iki bileşenden oluşacak olup her iki bileşen aynı üreticinin ürünü olmalıdır.

Teklif, en az 25 (yirmi beş) sunucu sayısına göre olacaktır.

Teklif edilen çözüme ait lisanslar ile birlikte en az 3 (üç) yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir.

Merkezi Yönetim Modülü

Yönetim Modülü bulut tabanlı olmalı ve web arayüzü üzerinden herhangi bir cihaz (tablet, telefon, bilgisayar) ile yönetim arabirimine erişim sağlanmalıdır.

Active Directory ile entegre olmalı ve kullanıcı/grup/cihaz bilgilerini otomatik olarak düşük boyutlu bir yazılım üzerinden belirli periyotlarda, yönetim modülüne aktarılmalıdır.

Her politika için hazır şablonlar olmalı ve sistem yöneticisi kendi isteğine özel politikalar oluşturabilmelidir.

Rol tabanlı (kullanıcı, yönetici, süper yönetici, yardım masası ve salt okunur) yönetim özelliği bulunmalıdır.

Her sunucu için özel bir parola üretilmeli ve bu parola ile yazılımın sistem üzerinden kaldırılması ve kritik bazı servislerin devre dışı bırakılması önlenmelidir.

SIEM ürünleri ile entegre olabilmesi için bir yönetim modülü üzerinden bir API Token üretilebilmelidir.

Yönetim Modülü üzerinde yapılan aksiyonların Audit Log'larına belirli zaman aralıkları seçilerek erişilebilmeli ve 90 günlük zaman diliminde bu log'lar çekilebilmeli, CSV/PDF formatlarında indirilebilmelidir.

Çeşitli kategorilerde yer alan internet sitelerine erişimleri sınırlandırabilmek amacıyla web filtreleme politikaları oluşturulabilmeli, sistem yöneticisinin istediğine özel url, ip adresi bilgisi eklenebilmelidir.

Uygulama kontrolü için çeşitli kategorilerde uygulama listesi sunulmalı ve sistem yöneticisi listeden istenilen uygulamanın sunucuda çalıştırılmasını önleyebilmelidir.

Veri Sızıntısını önlemek amacıyla belirli dosya türlerine göre yada dosyanın içerisinde geçen anahtar kelimelere göre kurallar oluşturulabilmeli ve kritik verilerin harici çıkarılabilir medya, Tarayıcı , Skype, Outlook, Outlook Express gibi uygulamalar üzerinden sızdırılması durumunda ya tamamen bloklanmalı yada kullanıcının inisiyatifine bırakılmalıdır. Bu işlemlerin log'u tutulmalıdır.

Ek güvenlik gereksinimleri yada PCI-DSS uyumluluğunu sağlamak amacıyla, sunucularda kayıt defteri alanları, kritik windows sistem dosyalarının bulunduğu alanlarındaki değişikler izlenmelidir. Bu işlemin haricinde kullanıcı dosya, dizin ve kayıt defteri tanımlaması yapabilmelidir. Bu alanlarda yapılan değişiklikler raporlanabilmelidir.

Cihaz kontrolü politikalarında, harici çıkarılabilir medya, wireless, MTP/PTP, Bluetooth gibi donanımların kontrolü sağlanmalıdır. Model ya da Cihaz ID'sine göre istisnalar oluşturulabilmelidir.

Yönetim konsolundan politikalar sunucu seviyesinde oluşturulabilmelidir.

Ufuk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen

Lockdown politikası ile makinada çalıştırılabilir uygulamaların parmak izi alındıktan sonra herhangi çalıştırılabilir dosyanın sunucu da çalıştırılması önlenebilmeli, bir uygulama çalıştırılmak istediğinde yol(path) bilgisi Lockdown politikalarına yazılarak aksiyon alınabilmelidir.

Gelişmiş tehditlerin kurum ağında yayılmasını önlemek amacıyla üreticinin, güvenlik duvarı ürünü ile entegre çalışabilmelidir.

Raporlama Özellikleri

Grafiksel olarak belirli zaman aralıklarında cihaz, web, dlp, uygulama kontrolü ve diğer modüllerin raporları oluşturulmalıdır. CSV, PDF formatında ulaşılabilmeli, yazıcıdan çıktı alınabilmelidir.

Koruma yazılımı yükle olan sunucu da bir olay meydana geldiğinde, otomatik olarak sistem yöneticisine detayları içeren bir e-posta gönderilmelidir. Olay detayları, farklı seviyelerde (düşük, orta ve bilgi) yönetim konsolunda sınıflandırılmalıdır.

Belirli kategorilerde zamanlanmış raporlar oluşturulabilmelidir.

Koruma Ajanı Modülü

Bulut tabanlı yönetim yazılımı ile HTTPs 443 portu üzerinden güvenli bir şekilde iletişime geçmelidir.

Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016 (32 yada 64 bit), 2019, Ubuntu 16/18 LTS, SUSE 12/15, Red Hat Enterprise Linux 6/78, Oracle Linux 6/7, Debian 9/10, CentOS 6/7/8, Amazon Linux, Amazon Linux 2 desteğine sahip olacaktır.

Sisteme erişim sağlayan bir uygulama zararlı bir internet trafiği meydana getirmesi halinde, komut edildiği sunucu ile bağlantı sağlaması durumunda zararlı trafik tespit edilebilmeli.

Virüs'lerin antivirüs yazılımını durdurmasını önleyen, aynı zamanda yazılımın servislerini ve kaldırma işlemini denetleyen bir yapılandırma olmalıdır. Bu sayede kullanıcılar kritik servisleri devre dışı bırakmamalıdır.

Ajan, kurulu olduğu sunucu da herhangi bir dosya açıldığında veya çalıştırıldığında, değişiklik yapıldığında güvenliği sağlamak amacıyla hızlıca taranmalıdır.

Davranışsal Tarama(behaviour scan) özelliği olacaktır. Davranışsal tarama(behaviour scan) özelliği olacaktır. Aynı zamanda, antivirüs taraması esnasında üreticinin istihbarat ağ'ından son güncel tehditler sorgulanmalıdır.

Makinalara Ajan kurulumlarında ve sonraki zamanlarda çeşitli komponentlerin imza güncellemesini yapabilmesi için kurum içerisindeki bir veya birden fazla sunucuya "Update Cache" rolü atanabilmeli. Band genişliği kullanımını en aza indirgemek için tüm makinalar bulut ortamında ki sunucudan önce güncelleme dosyalarını içerdeki bir sunucudan çekebilmelidir. Eğer Update Cache sunucusuna erişim sağlayamazsa, bulut tabanlı sunucudan güncellemelerini otomatik olarak almalıdır.

Tarama işlemleri için farklı seviyelerde dosya, dizin, proses için istisna(exclusion) özelliği olmalıdır.

Ajan, çeşitli kurulum yöntemlerini desteklemelidir. Manuel, Group Policy, 3.parti araçlar(System Center Configuration Manager, vs.) ve e-mail yöntemlerini desteklemelidir.

Boot CD ve Boot USB oluşturulabilecek ve bilgisayar taraması yapılabilecektir. Virüs, trojan ve diğer zararlı yazılımların tespiti için alternatif olarak çeşitli araçlar(virus removal tool, source of infection tool) sunmalıdır.

Uluk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen

Şüpheli bir dosya tespit edildiğinde, bu dosya karantina bölgesine alınmalı ve sistem yöneticisinin inisiyatifine göre SHA-256, sertifika yada yol bilgisine göre yönetim konsolunda, uygulamaya izin verilebilmelidir.

Kullanıcıların zararlı içerik-kod barındıran internet sitelerine erişimlerini engellemeli ve dosya indirme esnasında dosyanın repütasyon kontrolünü sağlamalıdır.

Ajan kurulumlarında proxy desteği sağlanmalıdır.

Güncelleme ve yönetim trafiği birbirinden (gerektiğinde) ayrı yönetilebilmelidir. Internet erişimi olmayan makinelerde yönetim trafiği, internet erişimi olan sunucuya rol ataması yapılarak gerçekleştirilebilmelidir.

Yeni Nesil Uç nokta koruma yazılımı

Önerilen çözüm, imzasız yeni nesil bir koruma sunmalı ve ileri seviyedeki zararlı yazılımları temizleyebilmelidir.

Dosya sistemi düzeyinde izleme sağlamalı ve dosyaları değiştirmeye çalışan makineleri ve prosesleri sürekli olarak gözetmelidir.

Fidyecilik amaçlı kullanılan zararlı uygulamalar tarafından hedeflenen kritik çalışma dosyalarının korumasını sağlamalı,şifreleme esnasında durdurulmalı ve dosyalarda oluşabilecek bir şifreleme işleminde, varsayılan güvenli durumuna geri döndürmelidir.

Hem yerel hem de uzak paylaşım dosyalarının toplu şifrelemesini engellemelidir.

Bir bulaşma olduğunda, nereden kaynaklandığını ve nasıl yayılımlandığını ayrıntılı olarak, kök neden analizi yaparak raporlamalıdır. Kök neden analizi, söz konusu saldırı hakkında ve gelecekte bunların nasıl önleneceği hakkında adli (forensic) rapor hazırlayabilmeli, Process Tehdit Zinciri görselleştirme yapabilmelidir.

Yazılımlarda oluşabilecek bir açıklıklardan faydalanan suistimal yazılımlarına (exploitler) karşı tekniklerini inceleyen imzasız bir koruma sağlamalıdır.

Sıfırıncı gün (Patient-Zero / Zero-Day) koruması sağlamalı ve RAM'lere yerleşebilen "Memory-Resident Ataklarını" bloklayabilmelidir.

Kurulum gerektirmeyen zararlı yazılım temizleme aracına sahip olmalıdır.

Uç nokta bilgisayarları üzerinde performansa etkisi minimal olmalıdır.

Komuta ve control (Command & Control) merkezlerine giden trafiği tespit edebilmelidir.

Suistimal yazılımı önleme (exploit prevention) ve tarayıcı suistimal yazılımı önleme (browser exploit prevention) özelliklerine sahip olmalıdır.

Bulut tabanlı yönetim konsolu olmalı, kolay kurulum ve politika yönetimi sunmalıdır.

Office uygulamaları yada diğer kurumsal uygumalar false positive tespiti durumunda istisna kuralları oluşturulabilmeli ve uygulamaların çalışma süreçleri etkilenmemelidir.

Önerilen çözümün üreticisi uç nokta korunmasında Gartner'da en az 5 yıl liderler bölümünde olmalıdır.

Yeni nesil güvenlik çözümü, derin ögrenme modeli kullanarak tehdit dünyasında yer alan çok sayıda bilinen/bilinmeyen zararlı yazılımlara karşı kısa sürelerde tespit, koruma ve önleme yetenekleri sağlamalıdır.

Ufuk SALTAN
Ağ ve Sistem Uzmanı

Mehmet KOÇ
Bilgisayar Mühendisi

Çiğdem KARAYEMİŞ
Teknisyen