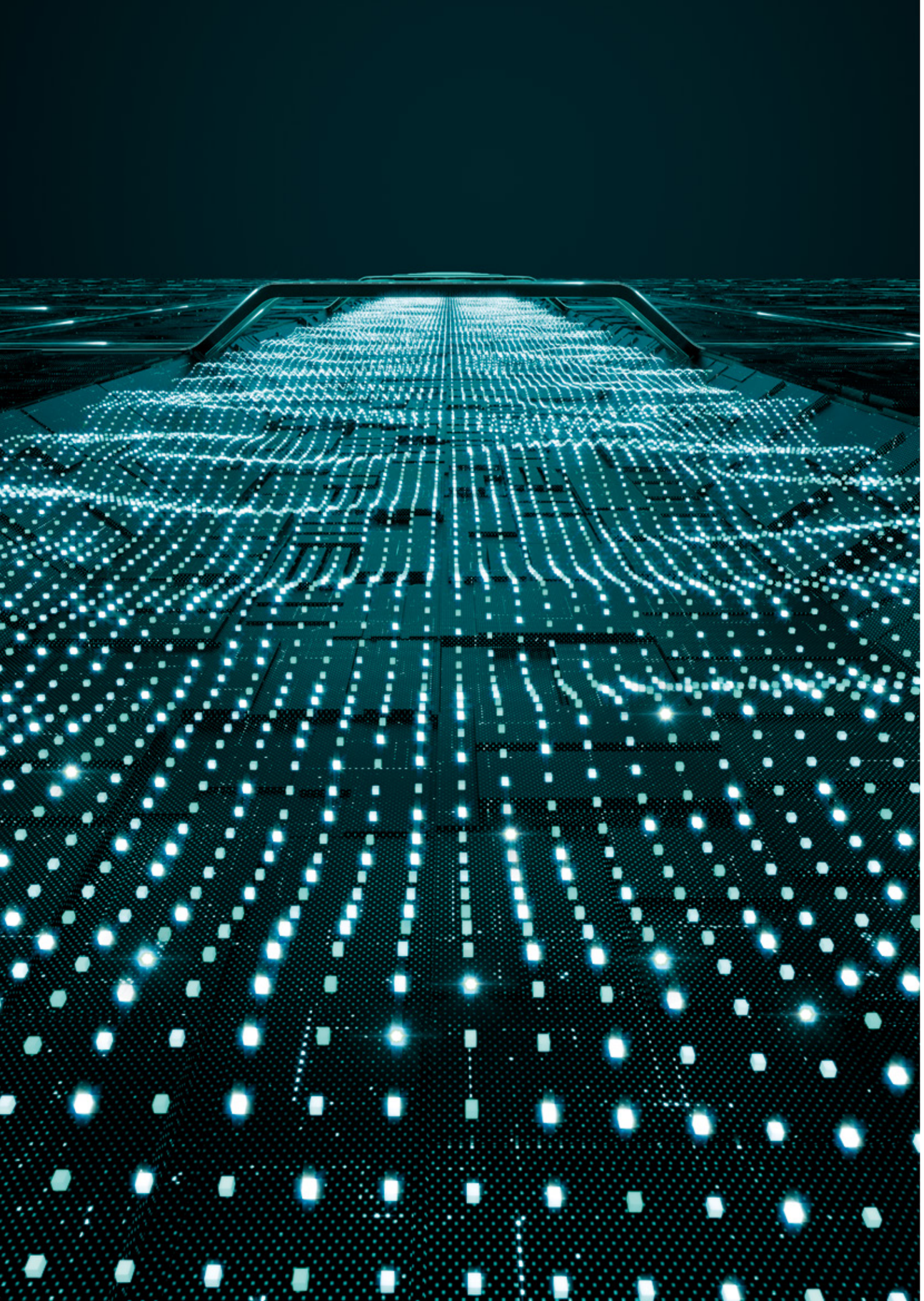
ÇÖZÜME GENEL BAKIŞ

INSPECT

Güvenlik ihlallerini engellemeye, görünürlüğü geliştirmeye ve sorun gidermeye olanak sağlayan, ESET PROTECT platformunun XDR etkinleştirme bileşeni

Progress. Protected.



Kapsamlı Algılama & Yanıt (XDR) Çözümü nedir?

ESET PROTECT platformunun XDR etkinleştirme bileşeni ESET Inspect, kötü amaçlı davranışları ve güvenlik ihlallerini tanımlama, risk değerlendirme, olaya yanıt verme, olayı soruşturma ve ortadan kaldırma amacıyla kullanılan bir araçtır.

Olaya tepki verenlerin, ağdaki ve bağlı cihazlardaki tüm etkinlikleri izlemesine ve değerlendirmesine olanak sağlar. Ayrıca gerekli durumlarda sorunun otomatik olarak anında ortadan kaldırılmasına yardımcı olur. ESET, 800'ü aşan ve sayısı sürekli artan algılama kuralıyla kapsamlı tehdit avlama sağlar.

Neden **Kapsamlı Algılama & Yanıt?**

VERİ İHLALLERİ

Şirketler veri ihlalini tespit etmenin yanı sıra bu veri ihlaline müdahale edip bunu ortadan kaldırmalıdır. Bunun son derece net bir şekilde ve iş sürekliliğini kesintiye uğratmadan yapılması gerekir. Çoğu şirket, bu şekilde kapsamlı bir soruşturmaya karşı hazırlıklı değildir ve dışarıdan bir satıcıdan yardım alır. Günümüzde kuruluşlar, ortaya çıkan tehditlerin, şirketi riske atan çalışan davranışlarının ve istenmeyen uygulamaların şirket menfaatlerini ve itibarını riske atmadığından emin olmak için bilgisayarındaki görünürlüğü artırmaya ihtiyaç duyuyor.

Veri ihlallerinin en sık gerçekleştiği sektörler genellikle finans, perakende, sağlık ve kamu hizmeti gibi değerli verilerin bulunduğu sektörlerdir. Ancak, bilgisayar korsanlarının az çaba harcayarak gelir edebileceği diğer sektörler de risk altındadır.

GELİŞMİŞ SÜREKLİ TEHDİTLER (APT) VE HEDEFE YÖNELİK SALDIRILAR

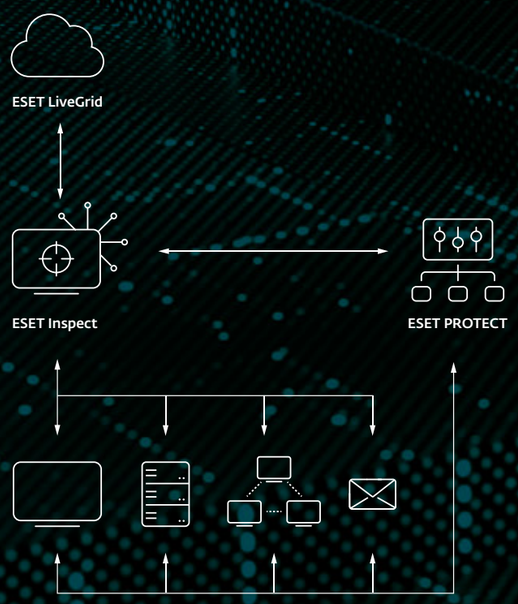
XDR sistemleri, genellikle Tehdit Avlama yoluyla APT'leri ve hedefe yönelik saldırıları tespit etmek, olayı yanıtlama süresini azaltmak ve proaktif olarak gelecek saldırıları engellemek amacıyla kullanılır. Günümüzde birçok şirket günlerce veya belki de aylarca fark edilmeden ağda bekleyen en yeni saldırılara karşı hazırlıklı olmadığından, özellikle APT'leri gün yüzüne çıkarmak şirketler için çok önemlidir.

Güvenlik ekiplerine tamamen açık olan **benzersiz davranış ve itibar tabanlı algılama**, ve bu sayede güvenlik ekiplerine LiveGrid'teki 100 milyondan fazla uç noktadan toplanan gerçek zamanlı besleme sağlar.

ARTTIRILMIŞ KURULUŞ GÖRÜNÜRLÜĞÜ

Kurumsal şirketler için iç tehditler ve kimlik avı hırsızlığı saldırıları başlıca sorundur. Şirketlerde kimlik avı saldırılarında hedef alınabilecek çok fazla çalışan olduğu için genellikle bu tür saldırılar tercih edilir. Tek bir çalışanın bile kandırılması, tüm şirkete sızmak için yeterlidir. Çok sayıda çalışan olduğunda bunlardan birinin şirketin çıkarlarına aleyhine çalışması olasılığı da arttığından, iç tehditler de büyük şirketlerin karşılaştığı tehditlerden biridir.

XDR sistemleri, kuruluşlar için gerekli olan tüm cihazlardaki sorunları görmek, anlamak, engellemek ve ortadan kaldırmak için gereken arttırılmış görünürlüğü sağlar. ESET Inspect, kendilerini Word dosyaları gibi iyi huylu belgelerin bir parçası gibi gösteren kötü amaçlı komut dosyalarını hızlı bir şekilde tespit edip durdurabilir.



Günümüzde kuruluşlar, **ortaya çıkan tehditlerin, şirketi riske atan çalışan davranışlarının** ve **istenmeyen uygulamaların** şirket menfaatlerini ve itibarını riske atmadığından emin olmak için bilgisayarındaki görünürlüğü artırmaya ihtiyaç duyuyor.

ESET farkı

EKSİKSİZ ENGELLEME, ALGILAMA VE YANIT

Ağınızdaki tüm güvenlik sorunlarının hızlı bir şekilde analiz edilmesini ve bu sorunların ortadan kaldırılmasını sağlar. Her bir katmanı ESET Inspect'e veri yollayan ESET'in çok katmanlı güvenliği, gerçek zamanlı olarak çok büyük miktarda veriyi analiz eder, bu sayede tüm tehditleri algılar.

GÜVENLİĞE ÖNCELİK VEREN BİR SATICININ SUNDUĞU ÇÖZÜM

ESET, 30 yılı aşkın bir süredir siber tehditlerle savaşıyor. Bilimi temel alan bir şirket olarak makine öğrenimi, bulut teknolojisi ve şimdi de XDR gibi son teknoloji gelişmeler sunuyor.

ONARMAK YERİNE ÖNLEMEYİ AMAÇLAR

ESET'in XDR yaklaşımı, birçok ödül kazanan önleme ürünleriyle yakın ilişki içerisindedir. Yüksek nitelikli algılama teknolojisi geliştirmeye yönelik kararlılığı sayesinde ESET önleme teknolojisi dünyada liderdir.

AYRINTILI AĞ GÖRÜNÜRLÜĞÜ

Şeffaf algılama kuralları (ESET 800'den fazla kurala sahiptir ve bu sayı sürekli artar), gelişmiş ihlal göstergeleri (IoC) ve arama özelliği, ağınızı Derinlemesine Yürütülebilir Gözden Geçirme özelliği sayesinde şüpheli her şeyi tanımlayabilirsiniz.

HEMEN BAŞLAMAYA HAZIR

ESET'in çözümleri hemen kullanıma hazırdır ve deneyimli tehdit avcılarının ayrıntılı düzenlemelerine olanak sağlayacak kadar güçlüdür.

ESNEK DAĞITIM

Güvenlik çözümünüzü nasıl dağıtacağınıza kadar verebilirsiniz: ESET Inspect, şirket içerisinde kendi sunucularınız çalışabilir veya bulut tabanlı kurulum yoluyla yürütülebilir. Bu sayede kendi sahip olma maliyeti hedeflerinize ve donanım kapasitenize göre kurulumu ayarlayabilirsiniz.

MITRE ATT&CK™

ESET Inspect, algılamalarını tek bir tıkla size en karmaşık tehditler hakkında bile kapsamlı bilgi sağlayan MITRE Düşman Taktikler, Teknikler ve Ortak Bilgi (ATT&CK™) çerçevesine dayanarak yapar.

İTİBAR SİSTEMİ

Kapsamlı filtreleme sayesinde, güvenlik mühendisleri sağlam ESET itibar sistemini kullanarak bilinen tüm iyi uygulamaları tanımlayabilir. ESET sistemi, güvenlik ekiplerinin yanlış teşhisler yerine bilinmeyen ve büyük olasılıkla kötü amaçlı dosyalara zamanlarını ayırmalarını sağlamak üzere yüz milyonlarca iyi huylu belgeden oluşan bir veri tabanına sahiptir.

OTOMASYON VE ÖZELLEŞTİRME

ESET Inspect'i ihtiyaç duyduğunuz ayrıntı ve otomasyon seviyesine göre kolaylıkla ayarlayın. İlk kurulum sırasında ve önceden ayarlanmış kullanıcı profillerinin yardımıyla, istediğiniz etkileşim seviyesini, depolanacak veri türünü ve miktarını seçin. Daha sonra Öğrenme Modunun kuruluşunuzun ortamının haritasını çıkarmasını ve gerekli yerlerde yanlış teşhislerin hariç tutulmasıyla ilgili öneride bulunmasını sağlayın.

Kullanım örnekleri

Derinlemesine Tehdit Algılama – Fidye Yazılımı

Günümüzde fidye yazılımları ağda fark edilmeden, sessiz bir şekilde mümkün olduğunca çok sayıda ağ uç noktası arasında yayılmaya çalışıyor. Önceki imajlara geri dönüldüğünde bile fidye yazılımının yürütülmesinin hemen engellenmemesi için makine yedeklemelerine sızıyor.

ESET Inspect aracısı, ESET uç nokta güvenlik çözümlerinin işlevlerini genişletir ve ağınızda halihazırda mevcut olabilecek fidye yazılımları proaktif olarak algılamanıza olanak tanır. Tipik bir fidye yazılımı senaryosunda kullanıcı, ekinde bir belge bulunan bir e-posta alır. Kullanıcı Word belgesini açtığında makroları çalıştırması istenir. Kullanıcı makroları çalıştırdığında, sisteme bir yürütülebilir dosya düşer ve eşlenmiş sürücüler de dahil olmak üzere mümkün olan her şeyi şifrelemeye başlar.

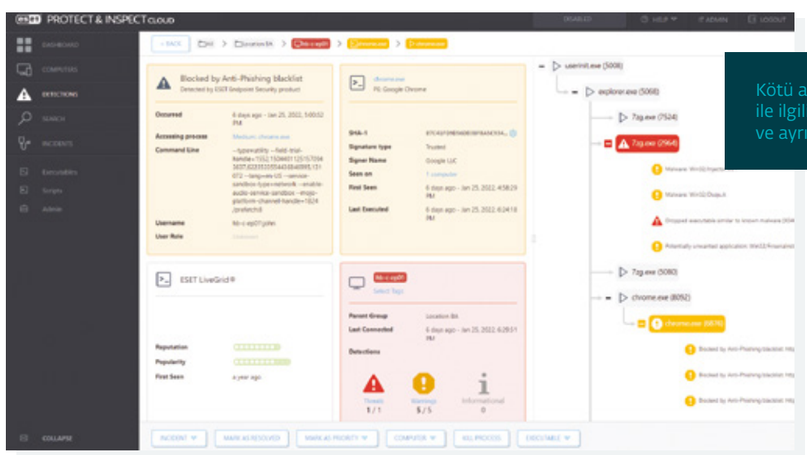
ESET Inspect sayesinde güvenlik ekibiniz bu tür davranışlarla ilgili uyarıları görebilir ve birkaç tıkla neyin etkilendiğini, belirli bir yürütülebilir dosyanın, komut dosyasının veya eylemin nerede ve ne zaman gerçekleştirildiğini görebilir ve bunun nedenini temeline kadar analiz edebilirsiniz.

KULLANIM ÖRNEĞİ

Bir şirket, ağda fidye yazılımı benzeri bir davranış görüldüğünde derhal bilgilendirilmenin yanı sıra fidye yazılımını proaktif olarak tespit etmek için ek araçlar istiyor.

ÇÖZÜM

- ✓ Geçici klasörlerden yürütülürken uygulamaları algılamak için kurallar girin.
- ✓ Ek komut dosyaları veya yürütülebilir dosyalar yürüttüklerinde Office dosyalarını (Word, Excel, PowerPoint) algılamak için kurallar girin.
- ✓ Bir cihazda en yaygın fidye yazılımı uzantılarından herhangi birinin görülmesi durumunda uyarıda bulunun.
- ✓ Aynı konsolda ESET Endpoint Security Solutions'dan Fidye Yazılımı Kalkanı uyarılarını görüntüleyin.



Kötü amaçlı kod davranışı ile ilgili işlem ağacı ve ayrıntılı bilgi

Davranış Algılama ve Sıkça Hata Yapanlar

Güvenlik açısından en zayıf nokta genellikle, herhangi bir kötü niyeti olmasa bile, klavyenin başında oturan bir kişidir.

ESET Inspect, tetiklenen benzersiz alarmların sayısına göre bilgisayarları sıralayarak bu olası zayıf öğeleri kolaylıkla tanımlar. Bir kullanıcının birden fazla alarmı tetiklemesi etkinliklerinin doğrulanması gerektiğinin açık bir göstergesidir.

KULLANIM ÖRNEĞİ

Kötü amaçlı yazılım söz konusu olduğunda ağınızda tekrar tekrar hata yapan kullanıcılar var. Aynı kullanıcılara sürekli virüs bulaşıyor. Bunun nedeni riskli davranışlar mı? Yoksa bu kişiler diğer kullanıcılardan daha fazla mı hedef alınıyor?

ÇÖZÜM

- ✓ Sorunla karşılaşan kullanıcıları ve cihazları kolaylıkla görüntüleyin.
- ✓ Virüsün neden bulaştığını bulmak üzere hızlıca bir kök neden analizi yapın.
- ✓ E-posta, web ve USB cihazları gibi bulaşmanın nedeni olan vektörleri ortadan kaldırın.

Tehdit Avlama ve Engelleme

ESET Inspect'i diğerlerinden ayıran güçlü yönü "samanlıkta iğne bulmaya" yarayan tehdit avlama becerisidir.

Dosya popülerliğine veya itibarına, dijital imzaya, davranışa ve bağlamsal bilgilere göre sıralanan verilere filtreler uygulayarak, herhangi bir kötü amaçlı etkinlik kolayca belirlenebilir ve araştırılabilir. Birden çok filtrenin ayarlanması sayesinde otomatik tehdit avlama görevlerine izin verilir ve algılama eşiği şirkete özel ortama göre ayarlanabilir.

Kötü amaçlı tüm etkinlikler kolayca tanımlanabilir ve araştırılır.

KULLANIM ÖRNEĞİ

Erken uyarı sisteminiz veya güvenlik operasyon merkeziniz (SOC) yeni bir tehdit uyarısında bulunuyor: Sonraki adımlarınız nelerdir?

ÇÖZÜM

- ✓ Yaklaşan veya yeni tehditlerle ilgili verileri almak için erken uyarı sisteminden yararlanın.
- ✓ Yeni bir tehdidin varlığıyla ilgili tüm bilgisayarları araştırın.
- ✓ Tehdidin uyarıdan önce de mevcut olması ihtimaline karşı, sızıntı olup olmadığını görmek için tüm bilgisayarları araştırın.
- ✓ Tehdidin bir ağa sızmasını veya bir kuruluşta yürütülmesini önlemek üzere tehdidi engelleyin.

Ağ Görünürlüğü

ESET Inspect bir açık mimari çözümdür. Güvenlik ekibi, kuruluşun belirli ortamına saldırı tekniklerine göre algılama kurallarını ayarlayabilir.

ESET Inspect, açık mimari sayesinde torrent uygulamaları, bulut depolamalar, Tor tarayıcı, kendi sunucularını başlatma ve istenmeyen diğer yazılımlar gibi belirli yazılımları kullanmayla ilgili kuruluş politikası ihlallerini algılamak üzere yapılandırma esnekliğine de sahiptir.

KULLANIM ÖRNEĞİ

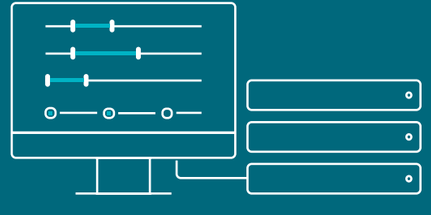
Bazı şirketler, kullanıcıların sistemlerde yürüttüğü uygulamalar konusunda endişelenir. Geleneksel olarak kurulan uygulamaların yanı sıra aslında kurulum gerçekleştirilmeyen taşınabilir uygulamalar konusunda endişelenmelisiniz. Bu uygulamaları nasıl kontrol edebilirsiniz?

ÇÖZÜM

- ✓ Cihazlara kurulan tüm uygulamaları kolaylıkla görüntüleyin ve filtreleyin.
- ✓ Cihazlardaki tüm komut dosyalarını görüntüleyin ve filtreleyin.
- ✓ Yetkilendirilmemiş komut dosyalarının veya uygulamaların yürütülmesini kolaylıkla engelleyin.
- ✓ Yetkilendirilmemiş uygulamalar ve otomatik kurulumlar hakkında kullanıcıları bilgilendirerek bunları kaldırın.

Geleneksel olarak kurulan uygulamaların yanı sıra aslında kurulum gerçekleştirilmeyen taşınabilir uygulamalar konusunda endişelenmelisiniz. Bu uygulamaları nasıl kontrol edebilirsiniz?

Güvenlik ekibi, kuruluşun belirli ortamına saldırı tekniklerine göre **algılama kurallarını ayarlayabilir**.



Bağlama Göre Soruşturma ve Ortadan Kaldırma

Bir etkinliğin "kötü amaçlı" olup olmaması bağlama göre değişir.

Ağ yöneticilerinin bilgisayarlarında gerçekleştirilen etkinlikler, finans bölümündeki bilgisayarda gerçekleştirilenlerden oldukça farklıdır. Bilgisayarları doğru bir şekilde gruplayarak güvenlik ekipleri, kullanıcının bu makinede belli bir etkinliği gerçekleştirmeye yetkili olup olmadığını kolay bir şekilde tanımlayabilir. ESET PROTECT uç nokta gruplarının ve ESET Inspect kurallarını senkronizasyonu, bağlamsal bilgilerle ilgili önemli sonuçlar sağlar.

KULLANIM ÖRNEĞİ

Veri, bağlamsal açıdan bakıldığında değerlidir. Doğru kararlar için uyarıların ne olduğunu, hangi cihazlarda gerçekleştiğini ve hangi kullanıcıların bu uyarılar tetiklediğini bilmelisiniz.

ÇÖZÜM

- ✓ Aktif Dizin'e, otomatik gruplamalara veya manuel gruplamalara göre tüm bilgisayarları tanımlayın ve sıralayın.
- ✓ Bilgisayar gruplamalarına bağlı olarak uygulamalara veya komut dosyalarına izin verin veya bunları engelleyin.
- ✓ Kullanıcıya bağlı olarak uygulamalara veya komut dosyalarına izin verin veya bunları engelleyin.
- ✓ Yalnızca belli gruplardan bildirimleri alın.

Kolay Kurulum ve Kolay Tepki – Güvenlik Ekibine Gerek Yoktur

Bir şirketin bu işle ilgilenen güvenlik ekipleri olmasına rağmen, tetiklenen tüm alarmlar karşısında atılacak adımları hızlı bir önceliklendirmek ve uygulamak kolay değildir.

Bu nedenle, tetiklenen her alarmla ilgili olarak bu alarmın ortadan kaldırılması için önerilen adımlar bulunur. ESET Inspect bir tehdit algıladığında, hızlı bir şekilde yanıt işlevi sunar. Belli dosyalar hızla engellenebilir, süreçler sonlandırılabilir ve karantina altında alınabilir, seçili makineler izole edilebilir veya uzaktan kapatılabilir.

KULLANIM ÖRNEĞİ

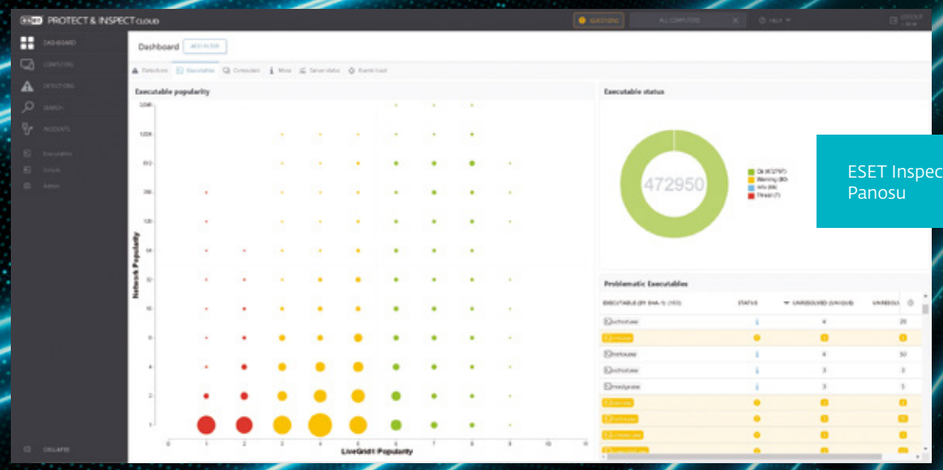
Tüm şirketlerde bu işe ayrılan güvenlik ekipleri bulunmayabilir; gelişmiş algılama kurallarını belirlemek ve uygulamak zor olabilir.

ÇÖZÜM

- ✓ 300'den fazla önceden yapılandırılmış kural.
- ✓ Cihazları engellemek, sonlandırmak veya karantinaya almak için yalnızca tek bir düğmeye tıklayarak kolayca tepki verin.
- ✓ Önerilen ortadan kaldırma ve sonra yapılacak adımlar, alarmlara dahil edilmiştir.
- ✓ uralları kolay bir şekilde ayarlamak veya oluşturmak üzere kurallar XML dili yoluyla düzenlenebilir.

Bir etkinliğin “kötü amaçlı” olup olmaması bağlama göre değişir. ESET PROTECT uç nokta gruplarının ve ESET Inspect kurallarını senkronizasyonu, bağlamsal bilgilerle ilgili önemli sonuçlar sağlar.

Tetiklenen her alarmla ilgili olarak bu alarmın ortadan kaldırılması için önerilen adımlar bulunur.



ESET Inspect Panosu

Çözüm özellikleri

OLAY YÖNETİM SİSTEMİ

İlgili kullanıcı eylemleriyle birlikte olası kötü amaçlı olayları bir zaman çizelgesinde görüntülemek için algılamalar, bilgisayarlar, yürütülebilir dosyalar veya süreçler gibi nesneleri mantıksal birimler halinde gruplayın. ESET Inspect, bir olayın öncelik sıralaması, soruşturma ve çözüm aşamalarında büyük ölçüde yardımcı olabilecek tüm ilgili olayları ve nesneleri olaya tepki verenlere otomatik olarak sunar.

CANLI YANIT SEÇENEKLERİ

ESET Inspect, bir uç noktayı yeniden başlatma ve kapatma, uç noktaları ağın geri kalanından izole etme, isteğe bağlı tarama yapma, çalışan herhangi bir işlemi sonlandırma ve karma değerine dayalı olarak herhangi bir uygulamayı engelleme gibi tek tıkla kolayca erişilebilen yanıt eylemleri sunar. Ayrıca Terminal adı verilen ESET Inspect'in canlı yanıt seçeneği ile güvenlik profesyonelleri, PowerShell'deki tüm soruşturma ve ortadan kaldırma seçeneklerinden yararlanabilir.

KÖK NEDEN ANALİZİ

Potansiyel olarak kötü niyetli olaylar zincirinin kök neden analizini ve tam süreç ağacını kolayca görüntüleyin, istenen ayrıntı düzeyine kadar inin ve hem iyi niyetli hem de kötü amaçlı nedenlerle ilgili kötü amaçlı yazılım uzmanlarımız tarafından sağlanan zengin içerikli bağlama ve açıklamalara dayalı olarak bilinçli kararlar verin.

HERKESE AÇIK API

ESET Inspect; SIEM, SOAR, etiketleme araçları ve diğer birçok araç gibi etkili entegrasyona izin vermek üzere algılamalara erişmenin ve bunları dışa aktarmanın yanı sıra bu algılamaların ortadan kaldırılmasını sağlayan Herkese Açık bir REST API'ye sahiptir.

TEHDİT AVLAMA

Güçlü sorgu tabanlı IOC aramasını kullanın ve dosya popülerliği, itibar, dijital imza, davranış veya diğer bağlamsal bilgilere göre sıralamak için ham verilere filtreler uygulayın. Birden çok filtrenin ayarlanması; APT'leri ve hedefe yönelik saldırıları algılama, durdurma yeteneği de dahil olmak üzere otomatik ve kolay bir şekilde tehdit avlamaya ve olaylara yanıt vermeye olanak tanır.

GÜVENLİ VE SORUNSUZ UZAKTAN ERİŞİM

Olaya yanıt verme ve güvenlik hizmetleri, olaya yanıt verenin konsola bağlantısı ve uç noktalar arasındaki bağlantının kolaylıkla erişilebilir olması sayesinde sorunsuz bir şekilde yerine getirilebilir. Bağlantı, üçüncü taraf araçlarına gerek duymadan, en üst seviyede güvenlik önlemlerinin uygulanmasıyla gerçek zamanlı hıza yakın bir şekilde gerçekleşir.

TEK TIKLA İZOLASYON

Kötü amaçlı yazılımın yanal hareketini hızlı bir şekilde durdurmak üzere ağ erişim politikaları tanımlayın. ESET Inspect arayüzünde yalnızca tek bir tıkla, ihlale uğrayan cihazı ağdan izole edin. Ayrıca, cihazları müdahale durumundan kolayca çıkarın.

ANOMALİ VE DAVRANIŞ ALGILAMA

Yürütülebilir bir dosya tarafından gerçekleştirilen eylemleri kontrol edin ve yürütülen süreçlerin güvenli veya şüpheli olup olmadığını hızlı bir şekilde değerlendirmek için ESET'in LiveGrid® İtibar sistemini kullanın. Basit kötü amaçlı yazılımlar veya imza algılamaları yerine davranışla tetiklenecek biçimde yazılan belli kurallarla kullanıcıyla ilgili anormal olayları izlemek mümkündür. Bilgisayarların kullanıcıya veya bölüme göre gruplandırılması sayesinde güvenlik ekipleri, kullanıcının belirli bir eylemi gerçekleştirip gerçekleştirmeyeceğini belirleyebilir.

ETİKETLEME

Bilgisayarlar, alarmlar, hariç tutmalar, görevler, yürütülebilir dosyalar, süreçler ve komut dizinleri gibi nesnelerin hızlı filtrelenmesi için etiketler atayın veya etiketleri kaldırın. Etiketler kullanıcılarla paylaşılabilir ve oluşturulduktan sonra saniyeler içerisinde atanabilir.

İHLAL DURUMUNDA BİRÇOK GÖSTERGE

Karma değer, kayıt defteri düzenlemeleri, dosya düzenlemeleri ve ağ bağlantıları dahil olmak üzere 30'dan fazla farklı göstergeye dayalı modülleri görüntüleyin ve engelleyin.

AÇIK MİMARİ VE ENTEGRASYON

ESET Inspect, güvenlik ekipleri için tamamen şeffaf olan, benzersiz davranış ve itibar tabanlı algılama sunar. Tüm kurallar, SIEM entegrasyonları dahil belli şirket ortamlarının ihtiyaçlarını karşılamak üzere ince ayar yapmaya veya kolayca oluşturmaya olanak sağlamak için XML ile kolaylıkla düzenlenebilir.

ŞİRKET POLİTİKASI İHLALİ ALGILAMA

Kuruluşunuzun ağındaki herhangi bir bilgisayarda kötü amaçlı modüllerin yürütülmesini engelleyin. ESET Inspect, açık mimarisi sayesinde torrent uygulamaları, bulut depolama, Tor tarama veya diğer istenmeyen yazılımlar gibi belirli yazılımların kullanımı için geçerli olan politikaların ihlallerini algılamak üzere esnekliğe sahiptir.

KARMAŞIK PUANLAMA

Olaylara bir önem değeri atayan ve yöneticilerin olası olaylar için daha yüksek olasılığa sahip bilgisayarları hızlı bir şekilde tanımlamasına olanak tanıyan bir puanlama işleviyle alarmları öncelik derecesine göre sıralayın.

YEREL VERİ TOPLAMA

Yürütme süresi, dosyayı yürüten kullanıcı, bekleme süresi ve saldırıya uğrayan cihazlar dahil olmak üzere yeni yürütülen bir modül hakkında kapsamlı verileri görüntüleyin. Hassas veri sızıntısını önlemek için tüm veriler yerel olarak depolanır.

ESET hakkında

ESET® dünya çapında 30 yılı aşkın bir süredir işletmeler ve tüketiciler için sektör lideri BT güvenliği yazılımları ve hizmetleri geliştiriyor, ayrıca siber güvenlik tehditlerine kapsamlı ve çok katmanlı koruma sağlar.

ESET kötü amaçlı yazılımı önlemek, algılama ve kötü amaçlı yazılıma tepki vermek üzere makine öğreniminde ve bulut teknolojilerinde öncüdür. ESET, dünya genelinde bilimsel araştırmayı ve gelişmeyi destekleyen özel bir şirkettir.

SAYILARLA ESET

1 milyar+
küresel kullanıcı

400 bin+
kurumsal müşteri

200+
ülke ve bölge

13
küresel AR&GE merkezi

MÜŞTERİLERİMİZDEN BAZILARI

MITSUBISHI MOTORS
Drive your Ambition

9.000'den fazla uç nokta 2017'den beri ESET tarafından korunuyor

Allianz Suisse

4.000'den fazla posta kutusu 2016'dan beri ESET tarafından korunuyor

Canon
Canon Marketing Japan Group

32.000'den fazla uç nokta 2016'dan beri ESET tarafından korunuyor

T · ·

2 milyon müşteri tabanı 2008'den beri ISP güvenlik ortağı

YÜKSEK SEKTÖR STANDARTLARINA BAĞLILIK

AV comparatives APPROVED Business Security DEC 2021

ESET, 2021 Aralık'ta AV - Comparatives tarafından düzenlenen Kurumsal Güvenlik Testi'nde ONAYLI Kurumsal Güvenlik Ürünü ödülüne layık görüldü.

G2 Leader WINTER 2022

ESET, sürekli olarak küresel G2 kullanıcı yorumu platformunda en yüksek sıralarda yer alıyor ve çözümleri dünya genelinde tüketiciler tarafından takdir görüyor.

FORRESTER®

ESET çözümleri, "The Forrester Tech Tide(TM): Sıfır Güven Tehdit Algılama ve Yanıt, 2021 ikinci çeyrek" dahil olmak üzere önde gelen analiz firmaları tarafından sürekli örnek satıcı olarak gösteriliyor.

Digital Security
Progress. Protected.