PICUS

ÜRÜN BROŞÜRÜ

BÜTÜNCÜL GÜVENLİK DOĞRULAMA PLATFORMU

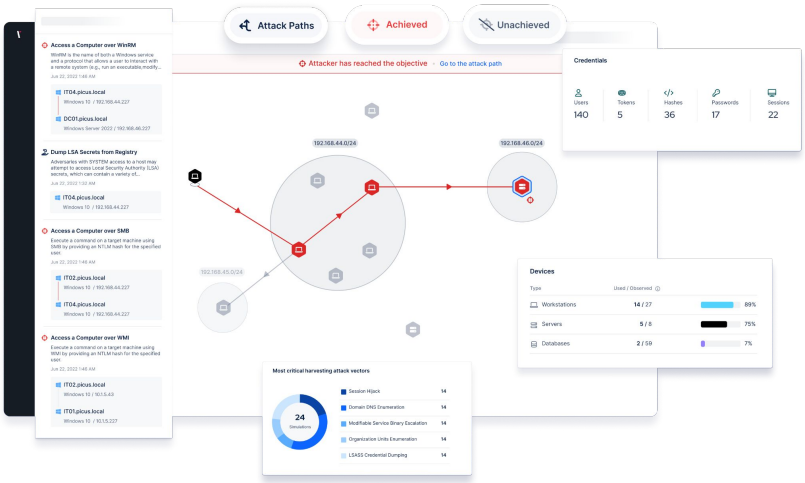
Atak Yolu Doğrulaması

KRİTİK KULLANICILARA VE VARLIKLARA ULAŞAN YOLLARI SAF DIŞI BIRAKARAK SALDIRGANLARIN İLERLEMESİNİ ÖNLEYİN

Siber güvenlik ihlalleri artık operasyonel bir gerçeklik olduğundan, en kötü olasılıklar göz önüne alınarak plan yapmak zorunlu hale gelmiştir. Siber ihlal varsayımı (assume breach) yaklaşımının anahtarı, ağınıza ilk erişimi elde ettikten sonra, sofistike saldırganların daha önce keşfedilmemiş güvenlik açıklarından ve yanlış yapılandırmalardan yararlanarak hedeflerine nasıl ulaşabileceğini anlamaktır.

Picus Atak Yolu Doğrulaması (Attack Path Validation - APV), güvenlik ekiplerinin, kurum içi bir ağa ilk erişimi olan ve güvenlik kontrollerini atlatabilen bir saldırganın kritik sistemleri ve kullanıcı hesaplarını ele geçirmek için atabileceği adımları otomatik olarak keşfetmesini ve görselleştirmesini sağlar.

Picus'un **Akıllı Saldırgan Karar Motoru** tarafından desteklenen bu kullanımı kolay araç, en kısa atak yollarını belirlemek ve gerçek bir risk oluşturduklarını doğrulamak için gerçek dünyadaki saldırgan aksiyonlarını simüle eder.



Windows Aktif Dizinize (AD) giden en kısa yolları keşfedin.

ATAK YOLU DOĞRULAMASI KURUM İÇİ AĞ GÜVENLİĞİNİZİ NASIL GÜÇLENDİRİR?

Kritik varlıklara giden yolları ortaya çıkarır ve doğrular

Picus APV, saldırganların AD'nizi ele geçirmek için kullanabileceği en kısa yolu belirler ve teorik olarak var olanlar değil, istismar edilebilecek gerçek yollar olduklarını doğrulamak için gerçek dünyadaki saldırgan eylemlerini simüle eder.

İç saldırı yüzeyinizin bütünsel bir görünümünü sağlar

Picus APV, tek bir ilk erişim noktasından gerçekleştirilen manuel kırmızı takım çalışmalarından farklı olarak, ağınızın birden çok noktasından simülasyonlar çalıştırmanıza ve haftalar değil dakikalar içinde sonuç almanıza olanak sağlayarak daha geniş bir perspektif sağlar.

Zafiyetleri ve hatalı yapılandırmaları önceliklendirmenize yardımcı olur

Ağınızdaki birden fazla atak yolunun birleştiği varlıkları belirleyin ve en iyi güvenlik etkisini elde etmeniz için bu düğüm noktalarındaki güvenlik açıklarını ve yanlış yapılandırmaları gidermeye öncelik verin.

Aktif Dizin güvenliğini güçlendirir

Bir saldırganın Domain Admin (DA) yetkilerini elde etmesine ve ortamınızdaki tüm kullanıcıların, sistemlerin ve verilerin kontrolünü ele geçirmesine olanak verebilecek zayıflıkları azaltın.

Kırmızı Takım operasyonlarını otomatikleştirir

Ofansif güvenlik testlerini otomatikleştirerek zamandan ve paradan tasarruf edin ve manuel testlerinizin daha iyi çıktı vermesini ve değer sunmasını sağlayın.

Güvenlik kontrollerinizin etkinliğini test eder

Kurumunuzun uç nokta güvenliğinin, yanal hareket ve saldırganlar tarafından kullanılan diğer atlatma tekniklerini tespit edip önleyecek şekilde yapılandırılıp yapılandırılmadığını ölçmek için Picus APV'yi kullanın.

ATAK YOLU NEDİR?

Atak yolu, bir kurumun ağını ihlal eden bir saldırganın hedefine ulaşmak için izleyebileceği rotanın görselleştirilmesidir. Çoğu kurum, takip edilmediği taktirde, siber suçluların kritik varlıkları tehlikeye atmasını kolaylaştırabilecek ve sayısı giderek artan binlerce potansiyel atak yoluna sahiptir.

Saldırganların ağ içinde yararlanabilecekleri yaygın riskler arasında yanlış yapılandırmalar, gereğinden fazla verilen kullanıcı yetkileri, zayıf parolalar, yetersiz ağ segmentasyonu ve erişim kontrolleri ile yama uygulanmamış güvenlik açıkları bulunur.

PICUS, ATAK YOLLARINI YÖNETMEYE NASIL YARDIMCI OLUR?

Picus Atak Yolu Doğrulaması, saldırganların bir Windows Etki Alanı Yöneticisi yetkilerini ele geçirmesini sağlayabilecek görünmeyen, izlenemeyen ve yönetilmeyen atak yollarını keşfederek ve engellemeye yardımcı olarak iç ağ güvenliğini güçlendirir.

Diğer çözümlerin aksine Picus APV, önceliklendirilmesi zor olan binlerce teorik yolu ortaya çıkararak güvenlik ekiplerini bunaltmaz. Bunun yerine, en kısa yolu keşfetmek ve bu yolun gerçek bir risk oluşturduğunu doğrulamak için gerçek bir saldırganın aksiyonlarını simüle eder.

PICUS AKILLI SALDIRGAN KARAR MOTORU

Picus APV ürününün merkezinde, Akıllı Saldırgan Karar Motoru (Intelligent Adversary Decision Engine) bulunur. Bu motor, ortamınızda keşif ve tarama yaparak, hedefe mümkün olan en verimli ve en sessiz atak yoluyla nasıl ulaşılabileceğine karar verir.

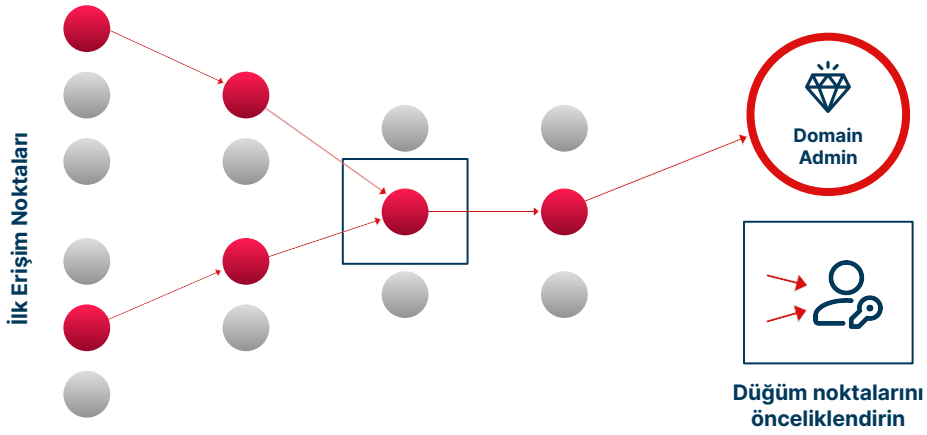
Picus APV tarafından simüle edilebilen gerçek ataklar şunları içerir:

- ✓ **Credential harvesting**
- ✓ **Password cracking**
- ✓ **Data Gathering**
- ✓ **Lateral movement**
- ✓ **Pivoting**
- ✓ **Privilege escalation**
- ✓ **Masquerading**
- ✓ **Relay**
- ✓ **Vulnerability exploitation**
- ✓ **Kerberoasting**

DOĞRU ALANLARDAKİ İYİLEŞTİRMELERE ODAKLANIN

Picus APV, manuel kırmızı takım alıştırmalarından daha bütünsel bir görünüm sağlamak için birden çok ilk erişim noktasından test yapmayı hızlı ve kolay hale getirir.

Güvenlik etkisini en üst düzeye çıkarmak için, birden çok yolun birleştiği varlıklar olan "düğüm noktalarını" belirlemek için test sonuçlarını karşılaştırın ve bu noktalardaki güvenlik açıklarını ve yanlış yapılandırmaları azaltmaya öncelik verin.



TEMEL ÖZELLİKLER

✓ **Otomatik atak yolu haritası çıkarma**
Yüksek riskli atak yollarını görünür kılın ve bunları düzeltmek için hızla harekete geçin.

✓ **Akıllı Saldırgan Karar Motoru**
Atlatma taktiklerine karşı güvenliğinizi test ederek gerçekçi bir görünüm elde edin.

✓ **Gerçek atak aksiyonları kütüphanesi**
Picus Labs tarafından geliştirilen en son siber atak tekniklerini kullanarak atak yollarını tespit edin ve doğrulayın.

✓ **Özelleştirilebilir test seçenekleri**
Test kapsamını ve aksiyonlarını tanımlayarak simülasyonları gereksinimlerinize göre uyarlayın.

✓ **Tamamen ajansız kurulum**
Simülasyon başlatmak için bir İlk Erişim Noktasında PowerShell betiğini veya yürütülebilir bir dosyayı çalıştırın.

> Sızma testi ve diğer bazı değerlendirme uygulamalarını her zaman kullanmamıza rağmen, hiçbiri olası saldırı senaryolarına karşı güvenlik duruşumuzu kapsamlı bir şekilde anlamamız için gereken derinliği ve genişliği vermedi. Picus platformu bir oyun değiştirici oldu.
>
> BT Güvenliği Ürün Müdürü
> ING Bank

Gartner peerinsights™
4.9 / 5*
*Ortalama puan (Ekim 2022)

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022
CYBERTECH100 2022 The World's Most Innovative CyberTech Companies for Financial Services
GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022
AICPA SOC 2 Type II

www.picussecurity.com

picussecurity