NESİL
TEKNOLOJİ

METODOLOJİ

BULUT
PENETRASYON TESTİ

BAĞLANTI ÖZETİ

Nesil Teknoloji'nin Bulut Sızma Testi, bulut ortamındaki güvenlik endişelerini belirlemeye yönelik kapsamlı bir yaklaşımdır. Çok çeşitli bulut tabanlı güvenlik açıklarını ortaya çıkarmak için açık kaynak ve özel yöntemler kullanıyorlar. Bu katılım, bulut ortamına yetkili erişim gerektirir ve katılımın amaçlarını ve kapsamını anlamak ve onaylamak için paydaşlarla bir araya gelir. Ekip daha sonra kapsam dahilindeki tüm bulut risklerinin keşfini ve numaralandırılmasını gerçekleştirir ve bulut ortamına erişimi olan birinin tehdidini simüle eder. Bu etkileşimin birincil sonucu, güvenlik ekiplerinizin tüm bulut risklerini anlamasını ve saldırı olasılığına, iş etkisine ve gerekli kaynak tahsisine göre iyileştirmeye öncelik vermesini sağlamaktır.

YÜKSEK DÜZEY SÜREÇ

1

Bilgi Toplama

Ortam ve kimlik bilgileri erişimini alın.

Görevin hedeflerini ve kapsamını doğrulamak için müşteriyle birlikte çalışın.

2

Keşfet ve Listele

Bulut kaynaklarındaki tüm yanlış yapılandırmaları sıralayarak test etmeye ve yapılandırma incelemeleri gerçekleştirmeye başlayın

Hizmet ve uygulama numaralandırmayla birlikte bağlantı noktası taramasını gerçekleştirin.

3

Bulut Sızma Testi

Önceki adımlarda gerçekleştirilen Keşif ve numaralandırma, bulut yükseltme yollarını geçmek, açığa çıkan kimlik bilgilerini aramak ve bulmak, bu kimlik bilgilerine erişimi test etmek, aşırı izin veren ağ erişimini belirlemek, yanlış yapılandırılmış bulutlardan, ağdan yararlanmak için kullanılacaktır.
ve uygulama hizmetleri, terk edilmiş alt alan adlarının belirlenmesi vb.

4

Analiz ve Raporlama

Kritik ve temel güvenlik açıklarını belirleyin ve gerekli iyileştirme çabalarını belirleyin.

Bulguların taslağını çıkarın ve gözden geçirin

Bulgular raporunda üç temel bileşeni sunun: Olasılığın belirlenmesi, Etki analizi, Şiddetin belirlenmesi ve gerekirse bir İyileştirme incelemesi gerçekleştirin.

METODOLOJİ DETAYLARI

AŞAMA 1 : ÖN DEĞERLENDİRME

Projenin zamanında tamamlanmasını ve başarısını garanti etmek için gerekli değerlendirme gereksinimlerinin yerine getirilmesi gerekir.

ÖN DEĞERLENDİRME GEREKSİNİMLERİ	
YAPILANDIRMA İNCELEMESİ İÇİN HESAP	Aşağıdakilere erişmek için: • Bulut ortamına API erişimi • Bulut ortamına Grafik Kullanıcı Arayüzü (GUI) veya Konsol erişimi • Güvenlik Denetimi izinleri Nesil Teknoloji'nin görev yöneticisi, uygun izinlere sahip bir hesabın nasıl oluşturulacağı konusunda özel talimatlar verecektir
SIZMA TESTİNE YÖNELİK HESAPLAR	Sızma testi gerçekleştirmek için değerlendirme ekibinin standart bir kullanıcı hesabına veya ihlal edilmiş bir uygulama/mikro hizmete benzeyen hesap kimlik bilgilerine ihtiyacı vardır. Erişim, sızma testinin hedefleriyle uyumlu olmalıdır. Örneğin erişim bir yazılım geliştiricisinin hesabını taklit edebilir.
ÇEVRE ERİŞİMİ	Değerlendirmeyi gerçekleştirmek için ekibin bulut API'sine ve ilgili tüm hizmetlere ağ erişimi. Bu erişim genellikle aşağıdaki yöntemlerden biriyle sağlanır: • VPN erişimi olan bir istemci dizüstü bilgisayar • Bir Atlama Kutusu • Doğrudan internet erişimi
HEDEFLER	Saha çalışmasına başlamadan önce değerlendirme ekibi Ana görev hedeflerini belirlemek için müşterinin ekibiyle işbirliği yapar. Bu hedefler genellikle şunları içerir: • Ayrıcalıklı kimlik bilgileri veya müşteri verileri gibi yüksek değerli hedeflere ulaşmak • Saldırıyı bulutun kısıtlı alanlarına genişletme

PRE-ASSESSMENT REQUIREMENTS

HEDEFLER	• Müşterinin tespit yeteneklerini değerlendirmek için veri çalmak • Belirli düzeyde erişim ve ayrıcalıklar elde etme simüle edilmiş bir saldırgan olarak.
KAPSAM	Değerlendirmeyi yürütmek için ekibin bir listeye ihtiyacı var kapsam dahilindeki bulut ortamları: • AWS hesapları • GCP projeleri • Azure abonelikleri
GEREKLİ ÖZEN	Değerlendirme boyunca Nesil Teknoloji, özellikle otomatik tarama, manuel doğrulama veya sızma testleri sırasında ağ kullanılabilirliğindeki kesintileri azaltmaya çalışır. Testten önce değerlendirme ekibi, müşteriyle çevresel istikrara yönelik riskler hakkında konuşacak ve herhangi bir aksaklığın fark edilmesi durumunda üst kademeye iletme sürecini oluşturacaktır.
YETKİLİ	Saha çalışmasına başlamadan önce, ürünün herhangi bir kısmı veya ilgili kaynaklar üçüncü taraf bir sistemde bulunuyorsa, üçüncü taraf sistem ana bilgisayarından test için yazılı izin alınmalıdır.

	Nesil Teknoloji	Müşteri
• Güvenlik Ekibi ve İşletmeyi Tanımlayın ve Onlarla Tanışın Paydaşlar	✓	✓
• Yapılandırma İncelemesi için Hesapların Hazırlanması		✓
• Sızma Testi için Hesap Hazırlama		✓
• Kimlik Bilgilerini ve Ortam Erişimini Sağlama		✓

• Hedefleri ve Kapsamı Belirleyin	✓	✓

AŞAMA 2:

BİLGİ TOPLAMA VE OTOMATİK TEST

Bu aşamada değerlendirme grubu, bulut uygulamasına ilişkin bilgileri toplamak ve incelemek için hem otomatik araçları hem de manuel yöntemleri kullanarak yerinde çalışmaya başlar.

ÖN DEĞERLENDİRME GEREKSİNİMLERİ	
YAPILANDIRMA SAYISI	Değerlendirme grubu, aşağıdaki yapılandırma ayrıntılarını elde etmek için hem açık kaynaklı hem de özel araçları kullanır: • Hizmet yapılandırma bilgileri • Kimlik Ve erişim yönetmek (IAM) yapılandırma verileri • Veri grupları gibi kaynak düzeyinde erişim kontrolleri • Kimlik bilgileri Ve diğer gizli veri riskleri takım daha sonra istihdam ediyor. Bu bilgiler aşağıdaki görevleri gerçekleştirmek için kullanılır: Olası güvenlik yanlış yapılandırmalarını • tespit etme • Bulut ayrıcalık yükseltme yollarını listeleme • Ortamın saldırı yüzeyini çizin.
AĞ KEŞFİ	Değerlendirme grubu, bulut ağındaki bir konumdan hedef ağdaki etkin ana bilgisayarları bulmak için aşağıdaki eylemleri gerçekleştirir: • Bulut Kaynak Sayımı - Açıkta kalan hizmet uç noktalarını bulmak için bulut API'sini kullanın • Ortak TCP Bağlantı Noktası Taraması - Daha önce bağlantılı olan alt ağlara odaklanarak belirli TCP bağlantı noktalarını bulmak için bağlantı noktası taramasını gerçekleştirin tanınan ana bilgisayar adları ve etki alanları.

HİZMET VE UYGULAMA SAYIMI	Hedef ağdaki etkin ana bilgisayarlar bulunduğunda, grup, aşağıdaki teknikleri uygulayarak çalışan ağ hizmetlerini listelemeye çalışır: • Ayrıntılı Bağlantı Noktası Taramaları - Bilinen bağlantı noktalarında ve canlı ana bilgisayarlarda TCP/UDP bağlantı noktası taraması gerçekleştirin • Hizmet ve Uygulama Numaralandırma - Deneme Çalışan ağ hizmetlerini ve uygulamalarını belirlemek ve incelemek.

	Nesil Teknoloji	Müşteri
• Yapılandırma Bilgilerini Toplayın	✓	
• Kimlik ve Erişim Yönetimine (IAM) ilişkin Yapılandırma Verilerini Toplayın	✓	
• Kaynak Düzeyindeki Erişim Kontrollerini (ör. Veri Grupları) keşfedin	✓	
• Kimlik Bilgilerini ve Diğer Gizli Verileri Açığa Çıkarın	✓	
• Olası Güvenlik Yanlış Yapılandırmalarını Belirleyin	✓	
• Bulut Ayrıcalığı Yükseltme Yollarını Numaralandırın	✓	
• Saldırı Yüzeyi Haritalaması	✓	
• Açığa Çıkan Uç Noktaları Belirleyerek Bulut Kaynaklarını Numaralandırın	✓	
• Hedefleme için Belirli Bağlantı Noktalarını Belirleme TCP Bağlantı Noktası Taraması	✓	
• Bilinen Bağlantı Noktalarına ve Canlı Ana Bilgisayarlara Karşı TCP/UDP Taramaları Gerçekleştirin	✓	
• Hizmet ve Uygulamaları Parmak İzine Göre Numaralandırma	✓	
Ağ Hizmetlerini ve Uygulamalarını Çalıştırma		

AŞAMA 3: PENETRASYON TESTİ

Yapılandırma incelemesini tamamladıktan sonra değerlendirme grubu, bulut uygulamasındaki güvenlik açıklarını tespit etmek ve bunlardan yararlanmak için aşağıdaki eylemleri gerçekleştirir.

PRE-ASSESSMENT REQUIREMENTS

CLOUD PENETRATION TESTING

Değerlendirme grubu, kapsam dahilindeki sistemlere ve kimlik bilgilerine sızmayı, yatay hareket etmeyi ve hedef ortamda ayrıcalıkları artırmayı amaçlar. Bu amaçla aşağıdaki eylemleri gerçekleştirir:

- **Bulut Ayrıcalık Yükseltme Yollarını Geçiş Yapmak**
- **Açıkta Olan Gizli Bilgiler ve Kimlik Bilgilerini Aramak**
- **Belirlenen Kimlik Bilgilerinin Erişilebilirliğini Doğrulamak**
- **Aşırı İzin Verilen Ağ Erişim Kontrollerini Belirlemek**
- **Yanlış Yapılandırılmış Bulut Hizmetlerinden Faydalanmak**
- **Zayıf Ağ Servisleri ve Uygulamalarını Kötüye Kullanmak**
- **Kullanılmayan Alt Alan Adlarını Bulmak**

	Nesil	Müşteri
Bulut Ayrıcalığını Yükseltme Yollarını Geçin	✓	
Açığa Çıkan Sırları ve Kimlik Bilgilerini Avlayın	✓	
Tanımlanan Kimlik Bilgisi Erişimini Test Edin	✓	
Aşırı İzin Veren Ağ Erişim Kontrollerini Belirleyin	✓	
Yanlış Yapılandırılmış Bulut Hizmetlerinden Yararlanma	✓	
Savunmasız Ağ Hizmetlerinden ve Uygulamalarından Yararlanma	✓	
Terk Edilmiş Alt Alan Adlarını Tanımlayın	✓	

AŞAMA 4: ANALİZ & RAPORLAMA

Nesil Teknoloji raporları, değerlendirme hedefleri, yüksek etkili bulgular ve tavsiyeler de dahil olmak üzere, katılımın yönetici özetini sağlar. Her sonuç bir güvenlik açığı tanımını, çoğaltma adımlarını ve özel tavsiyeleri içerir. Değerlendirme ekibi her bulgunun iş riskini değerlendirir.

OLASILIK BELİRLEME	Her bir güvenlik açığı için değerlendirme grubu, aşağıdakileri dikkate alarak bu güvenlik açığından yararlanma olasılığını değerlendirir: • Tehdit Kaynağı Motivasyonu ve Yeteneği • Güvenlik Açığının Özellikleri • Kontrollerin Varlığı ve Etkinliği
ETKİ ANALİZİ	Değerlendirme grubu, her bir güvenlik açığının başarılı bir şekilde kullanılmasının kuruluş ve müşterileri üzerindeki sonuçlarını gizlilik, bütünlük ve kullanılabilirlik açısından inceler ve değerlendirir.
ŞİDDET BELİRTİSİ	Nesil Teknoloji, kötüye kullanımın olasılığını ve etkisini değerlendirmek için dahili uzmanlığı ve OWASP ve CVSS gibi yaygın olarak kullanılan derecelendirme metodolojilerini kullanarak önem dereceleri atar. Grup, genel ciddiyeti kritik, yüksek, orta veya düşük olarak sınıflandırmak için bu faktörleri dikkate alıyor. Her bir bulgunun ciddiyeti, diğer sonuçların ciddiyetinden ayrı olarak belirlenir.

	Nesil	Müşteri
• Olasılık Belirleme	✓	
• Etki Analizi	✓	
• Şiddetin Belirlenmesi	✓	

AŞAMA 5: İYİLEŞTİRME İNCELEMESİ (İSTEĞE BAĞLI)

Talep üzerine değerlendirme grubu, müşteri güvenlik açıklarının giderildiğini onayladıktan sonra belirlenen güvenlik açıklarının taramasını ve testini tekrarlar.

Aşama 1: Ön Değerlendirme Gereksinimleri	Nesil Teknoloji	Müşteri
• Sorumlulukların Tanımlanması	✓	✓
• Güvenlik Ekibi ve İş Paydaşlarını Belirleyin ve Onlarla Tanışın		✓
• Yapılandırma için Hesapların Hazırlanması		✓
• Sızma Testi için Hesapların Hazırlanması		✓
• Provizyon Kimlik Bilgileri ve Ortam Erişimi	✓	✓
• Hedefleri ve Kapsamının Belirlenmesi		
Aşama 2: Bilgi Toplama ve Otomatik Test		
• Yapılandırma Bilgilerini Toplayın	✓	
• Kimlik ve Erişim Yönetimine (IAM) ilişkin Yapılandırma Verilerini Toplayın	✓	
• Kaynak Düzeyindeki Erişim Kontrollerini (yani Veri Gruplarını) keşfedin	✓	
• Kimlik Bilgilerini ve Diğer Gizli Verileri Açığa Çıkarın	✓	
• Olası Güvenlik Yanlış Yapılandırmalarını Belirleyin	✓	
• Bulut Ayrıcalığı Yükseltme Yollarını Numaralandırın	✓	
• Saldırı Yüzeyi Haritalaması	✓	
• Açığa Çıkan Uç Noktaları Belirleyerek Bulut Kaynaklarını Numaralandırın	✓	
• Hedefleme için Belirli Bağlantı Noktalarını Belirleme TCP Bağlantı Noktası Taraması	✓	
• Bilinen Bağlantı Noktalarına ve Canlı Ana Bilgisayarlara Karşı TCP/UDP Taramaları Gerçekleştirin	✓	
• Parmak İzi Çalıştırma Ağı Hizmetleri ve Uygulamalarına Hizmet ve Uygulamaları Numaralandırma	✓	

Aşama 3: Bulut Sızma Testi		
• Bulut Ayrıcalığını Yükseltme Yollarını Geçin	✓	
• Açığa Çıkan Gizli Bilgileri ve Kimlik Bilgilerini Yakalayın Tanımlanan Kimlik	✓	
• Bilgisi Erişimini Test Edin	✓	
• Aşırı İzin Veren Ağ Erişim Kontrollerini Belirleyin Yanlış Yapılandırılmış Bulut Hizmetlerini Suistimal Edin	✓	
• Savunmasız Ağ Hizmetlerinden ve Uygulamalarından Yararlanmak Terk Edilmiş Alt Alan Adlarını Belirlemek	✓	
Aşama 4: Analiz ve Raporlama		
• Olasılık Belirleme	✓	
• Etki Analizi Şiddetinin Belirlenmesi	✓	✓