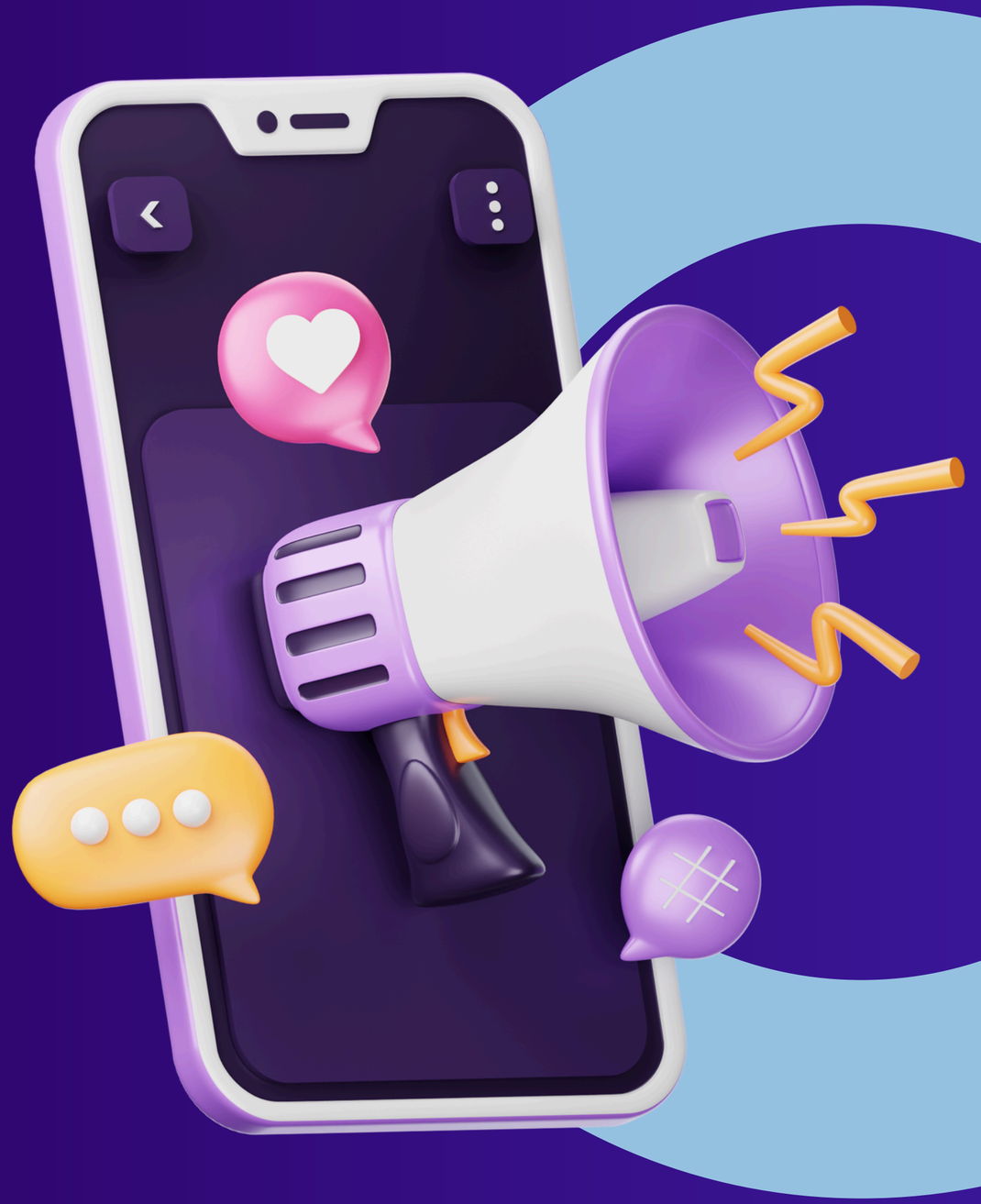
QUEVATECH

ON-PREM* ILE KRIPTOGRAFIK RASTGELELIĞE DAYALI GÜVENLIK

KRIPTOGRAFININ KALBINDE: ÖLÇÜLEBILIR ÖNGÖRÜLEMEZLIK SAĞLIYORUZ.



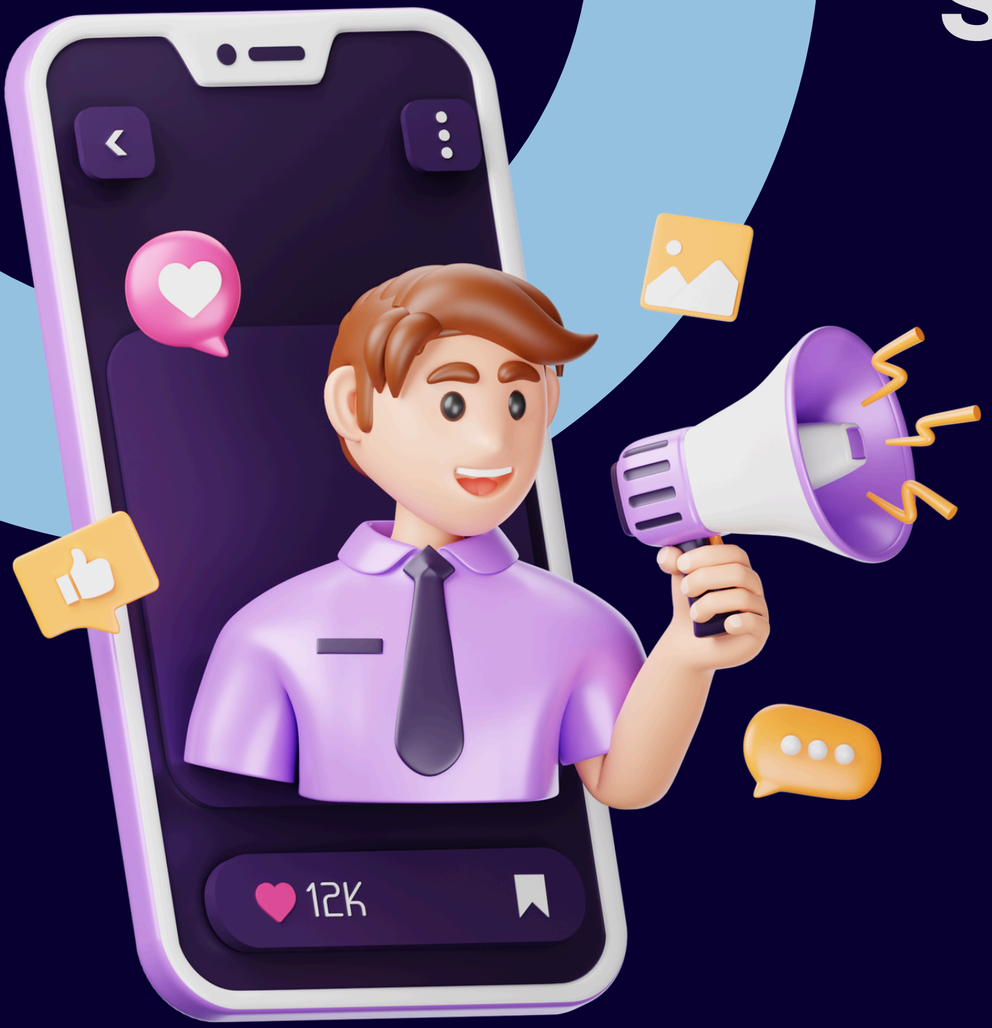
QuevaTech Adına Sunan:
Hasan Yiğit

Email:
hasan@queva.tech

*On-prem : Kurum içi çalışan cihaz, dışa bağlı olmayan cihaz.

QUEVATECH

SORUN ALANI



Zayıf rastgelelik

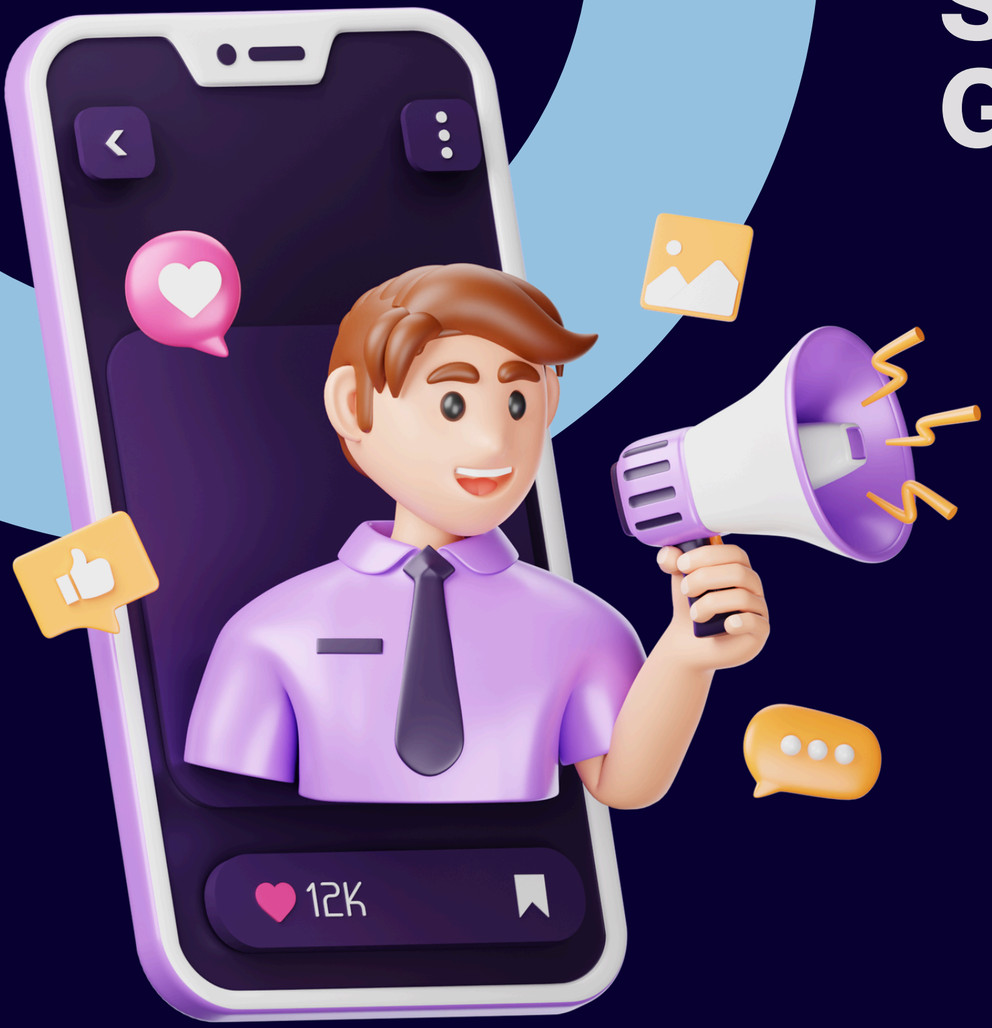
Zayıf Rastsal Sayı Üreteci RNG

Zayıf anahtar

Zincirleme risk ile sonuçlanır

Sonuç sessiz açık kapıdır.

QUEVATECH



SORUN ALANI GERÇEK ÖRNEKLER

- Debian OpenSSL (2006–2008) – **Tahmin edilebilir anahtarlar** https://nvd.nist.gov/vuln/detail/cve-2008-0166
- Juniper NetScreen (2012–2015) – **VPN trafiğinin sessizce çözülmesi** CVE-2015-7755 https://hovav.net/ucsd/dist/juniper.pdf
- RSA BSAFE varsayılanı (2007–2013) – **Şüpheli RNG'nin yaygınlaştırılması** https://www.securityweek.com/nist-pulls-dualecdrbg-algorithm-random-number-generator-recommendations/
- Android SecureRandom hatası (2013) – **Bitcoin cüzdanlarının boşaltılması**
- YubiKey FIPS serisi (2019) – **İlk kullanımda düşük entropi**

QUEVATECH

ÇÖZÜM ÖZETİ

NEDEN ÖNEMLI?

Daha güçlü bir tohum, daha güçlü şifreleme anahtarları demektir. Bu da kişisel verilerinizden ulusal siber güvenliğe kadar her şeyi korur. Altyapınıza eklediğiniz, görünmez bir emniyet kemeri gibidir; güvenliği sessizce ve sürekli olarak artırır.

NEREDE KULLANILIR?

- **Şifreleme ve Güvenlik:** OpenSSL ve PKCS#11 gibi standartları kullanan tüm sistemlerde.
- **Ağ Güvenliği:** VPN'ler ve SSL/TLS sertifikaları.
- **Donanım Güvenliği:** HSM'ler (Donanımsal Güvenlik Modülleri)
- **İşletim Sistemleri:** İşletim sistemlerinin kendi rastgele sayı üreteçleri (RNG).
- **Kurumsal Süreçler:** CA (Sertifika Yetkilisi) ve SOC (Güvenlik Operasyon Merkezi) süreçleri.

QUEVATECH

ÇÖZÜM ÖZETİ

ÖZET NOTUMUZ

Sistemlerin şifreleme için kullandığı rastgelelik kalitesini artırarak, dijital altyapının genel güvenliğini yükseltiriz. **Basitçe, daha iyi bir başlangıç (tohum), daha sağlam bir sonuç ve süreçler demektir.**

NASIL ÇALIŞIR?

- **Kaynak:** Sistemin entropi kaynaklarından (örneğin, donanım gürültüsü) veri toplar.
- **Yapay Zeka (AI) ile Koşullandırma:** Toplanan ham veriyi, Yapay Zeka algoritmaları kullanarak işler ve kalitesini artırır.
- **Bayt Akışı Üretimi:** Bu işlem sonucunda, standart testlerden geçen yüksek kaliteli bir rastgele bayt akışı elde edilir.
- **Kullanım:** Bu güçlü tohum, daha sonra VPN oturumları, sertifika anahtarları veya diğer şifreleme amaçlı rastgele verilerin üretiminde kullanılır.

QUEVATECH

ENTEGRE EDİLEBİLİR ENTROPİ CİHAZI

NE ÖNERİYORUZ?
Kurum içinde çalışan bir rastgelelik cihazı ve bunun kalitesini ölçen test yazılımı sağlıyoruz.

NEDEN ÖNEMLI?
Kurumunun RNG/anahtar kalitesini nesnel biçimde arttırır. Oluşturur ve dağıtırsınız.

QUEVATECH

ENTROPİ PROXY YARDIMCI YAZILIMI

NE SÖYLÜYORUZ?

Sunucuların ve uygulamaların anahtar/oturum üretimine TRNG karışımı enjekte ederiz.

NEDEN ÖNEMLI?

Günlük operasyonun içinde otomatik çalışır; insan hatasını azaltır, zayıf RNG kullanımını engeller.

NASIL ÇALIŞIR?

Api veya soket düzeyinde bir aracı servis; mevcut sistemlere hafif entegrasyon. Açık kaynak yazılım.

NEREDE KULLANILIR?

Kurumsal sunucular, VPN, kimlik sağlayıcılar, imzalama servisleri.

Operasyonun ortasına, görünmez ve hafif bir emniyet kemeri takıyoruz.

QUEVATECH

ANAHTAR KİOSKU GİZLİ PAYLAŞIM GÖREV DEVRİ GÜVENLİĞİ

İnsan süreçleri kırılgandır; diğer yöntemler güvenilir değildir;
bu modül onları prosedüre bağlar.

NE SÖYLÜYORUZ?

Görev değişimlerinde tek-kullanımlık, izlenebilir anahtar üretimi ve parçalara bölünmüş sırrın güvenle saklanması/kurtarılması.

NEDEN ÖNEMLI?

Personel değişimi gibi durumlarda erişim sürekliliği ve denetlenebilirlik korunur.
Kiosk güvenli anahtar üretir; Shamir yöntemiyle sırrı parçalara ayırır; yetkili bir araya gelmeden sır açılmaz.

NEREDE KULLANILIR?

Yer kritik erişimleri, CA törenleri, yüksek yetkili hesaplar.

QUEVATECH

MİMARİ VE GÜVEN SINIRLARI

VERILERINIZ KURUMUNUZDA KALIR:

Sistemimiz tamamen kurum içi (on-prem) çalışır. Bu sayede hassas verileriniz kurumunuzun fiziksel ve sanal sınırlarını asla terk etmez. Tüm denetim kayıtları imzalı ve zincirleme yapıda saklanır.

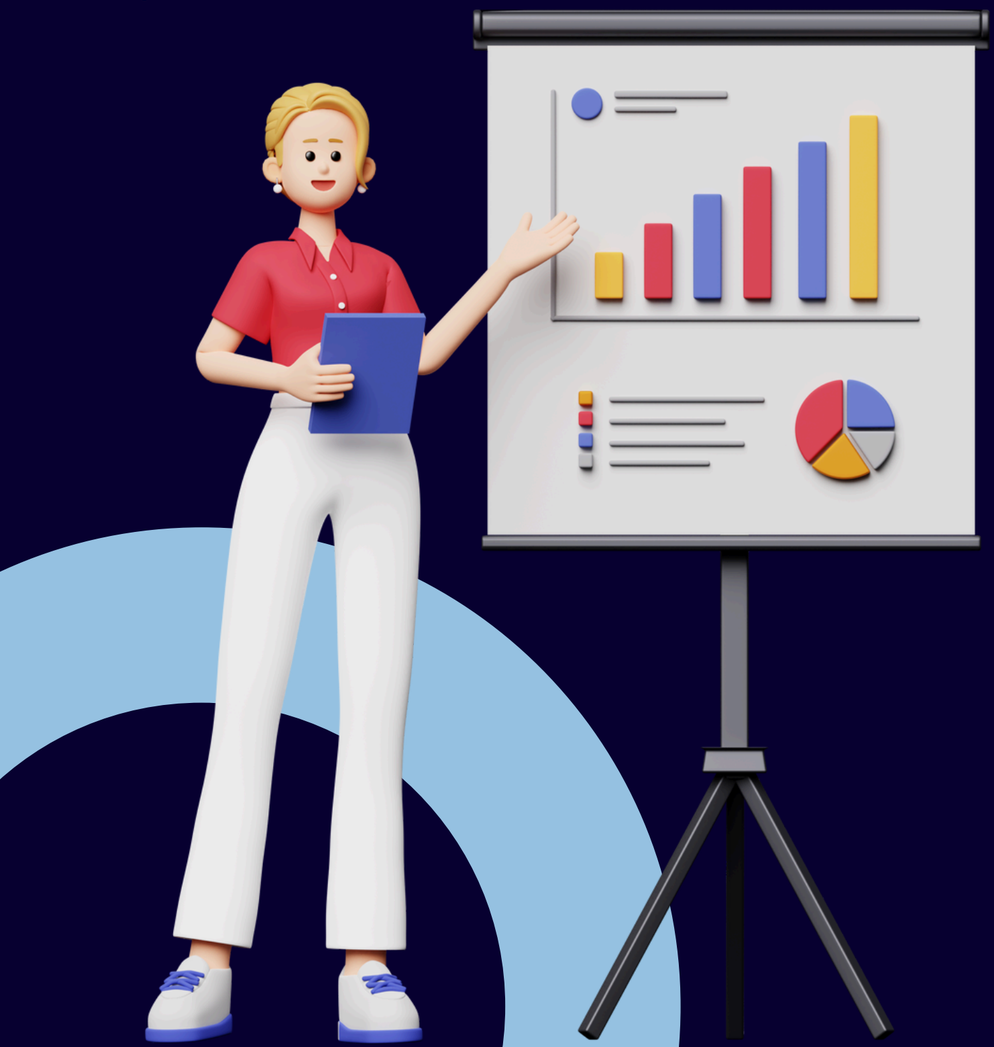
DIŞA BAĞIMLILIK YOK :

Cloudflare'in doğal gürültü kaynaklarından ilham alması gibi, kendi iç kaynaklarımızdan besleniriz. Yan kanal saldırılarına karşı özel önlemler alınmıştır ve yapay zeka modellerimiz bilinen arka kapılardan arındırılmıştır.

OPRERASYON GÜVENLIĞI

Sistemin temelinde, dışa bağımlılığı ortadan kaldıran çoklu kaynak yapısı yatar. Bu sayede hiçbir bileşen tek başına tüm ürünü kıramaz. Operasyonel güvenliğimizi ise sürekli model güncellemeleri ve düzenli bakımlarla en üst düzeyde tutarız.

QUEVATECH



KANITLAR: GÜVEN DEĞİL, ÖLÇÜLEBILIR SONUÇLAR

BIZ "INANIN" DEMIYORUZ, KANITLIYORUZ.

Sistemimizin güvenilirliği, bilimsel araştırmalar ve somut testlerle desteklenir. Bu yaklaşımımız, şeffaflık ve güven inşa etmenin temelidir.

- **Bilimsel Doğrulama:** Çalışma prensiplerimizi ve yöntemlerimizi bilim dünyasına açıkça sunuyoruz. Ayrıntılı makalemize **arxiv.org/abs/2507.00145** adresinden ulaşabilirsiniz.
- **Üstün Performans:** Ürettiğimiz rastgele veri, standart CPU'ların rastgelelik çıktısından %2-3 daha iyi performans gösterir. Bu sonuçlar, NIST SP 800-22 testleri gibi uluslararası kabul görmüş yöntemlerle 100 x 1Mb boyutundaki veri setleri üzerinde elde edilmiştir (bkz. Tablo 2).
- **Yüksek Entropi:** Rastgele bayt akışımız, 8 bitin 7.94'ü kadar yüksek bir minimum entropi değeriyle neredeyse mükemmel bir rastgelelik sunar.
- **Şeffaflık ve Denetim:** Elde ettiğimiz veriler, ticari olmayan tüm denetimlere açıktır. Her iddiamızın arkasında somut bir metot ve rapor vardır. Bu raporlar, karar alma süreçlerinizde kullanabileceğiniz güvenilir dosyalardır.

Özetle, rastgelelik kalitemiz yalnızca bir iddia değil, ölçülebilir ve kanıtlanabilir bir gerçektir.

QUEVATECH

NEDEN KENDINIZ GELIŞTIRMEMELISINIZ?

KURUM IÇINDE SIFIRDAN BIR KRIPTO ALTYAPISI KURMAK, SADECE BIR YAZILIM PROJESI DEĞILDIR; YÜKSEK MALIYETLI, ÇOK DISIPLINLI VE UZUN SOLUKLU BIR SÜREÇTIR.

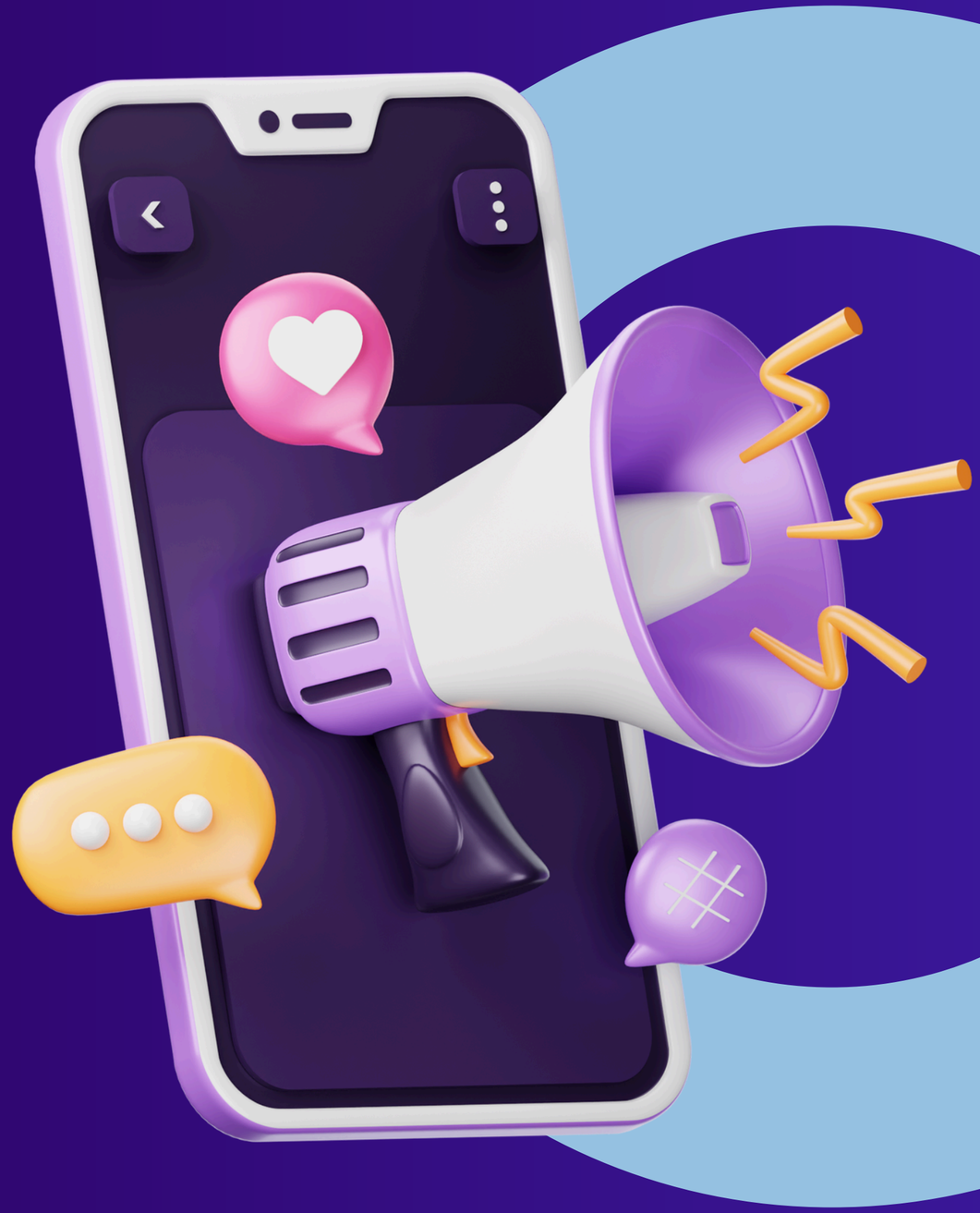
Bu, hem zamanınızı hem de değerli kaynaklarınızı asıl işinizden uzaklaştırır.

- **Geniş Uzmanlık Alanları:** Kriptografi, fiziksel entropi mühendisliği, güvenlik testleri ve yasal mevzuat gibi birçok farklı uzmanlık alanını aynı anda ve sürekli olarak bir araya getirmeniz gerekir. Bu, tek bir ekiple yönetilmesi oldukça zordur.
- **Gizli Maliyetler:** Dışarıdan görünmeyen maliyetler oldukça fazladır. Projenin Ar-Ge aşaması için 6-9 ay süren, 8-10 kişilik bir ekibin çalışması, test laboratuvarları, otomasyon sistemleri ve kapsamlı denetim dokümantasyonu gerekir. Buna bir de yıllık bakım ve güncelleme döngülerini ekleyin.
- **Zaman ve Fırsat Kaybı:** Bu süreçler, kurumsallaşmış kurumların asıl operasyonel görevlerinden kaynak ayırmalarına neden olur. Karar alma ve sistemin yaygınlaştırılması aylar sürebilir, bu da sizi rakiplerinizin gerisine düşürür.

QUEVATECH

BUGÜN, GELECEĞE CESURCA BAKTIĞINIZ VE RİSK ALMAK YERİNE GÜVENLİĞE YATIRIM YAPTIĞINIZ İÇİN TEŞEKKÜR EDERIZ.

İLK CIHAZI DEVREYE ALMA TARIHIMIZI BUGÜN NETLEŞTIRELIM. 45 GÜN SONRA, VAATLERIMIZIN SOMUT BIR KANIT DOSYASINDA YER ALDIĞINI GÖRECEKSINIZ. GÜVENLIĞI KONUŞMAKTAN, KANITLAMAYA GEÇELIM.



Email (her şey için):
hasan@queva.tech

Website:
www.queva.tech