

**Gremlin Kaos Aracının**

**Fizibilite Raporu**

190541003 - Beyza Barın

|  |  |
| --- | --- |
| **İÇİNDEKİLER** | **SAYFA NUMARASI** |
| 1.Giriş | 2 |
| 2.Gremlin | 3 |
| 3.Pazar Araştırması | 4 |
| 4.Teknik Değerlendirme | 5 |
| 5.Sonuç | 5 |
| 6.Swot (Güçlü Zayiıf Fırsat Tehdit) | 5 |
| 7.Kaynaklar | 6 |

**1. GİRİŞ**

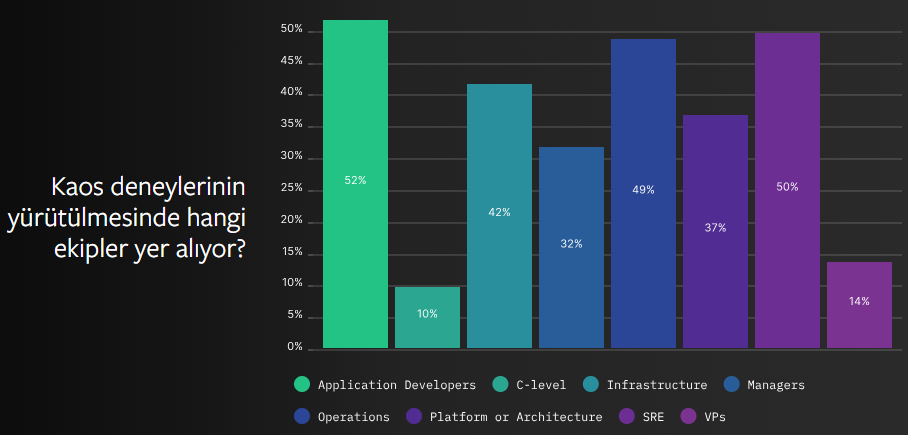
Bu rapor, Gremlin Kaos aracının bir organizasyon veya proje için kullanılabilirliğini ve uygulanabilirliğini değerlendirmeyi amaçlamaktadır. Gremlin, sistemlerin dayanıklılığını test etmek ve olası hataları öngörmek için kullanılan bir kaos mühendisliği platformudur. Bu raporda, kaos mühendisliği hakkında bilgilere ve Gremlin aracı hakkında pazar araştırması, teknik değerlendirme, mali analiz ve risklerin neler olduğu verilecektir.

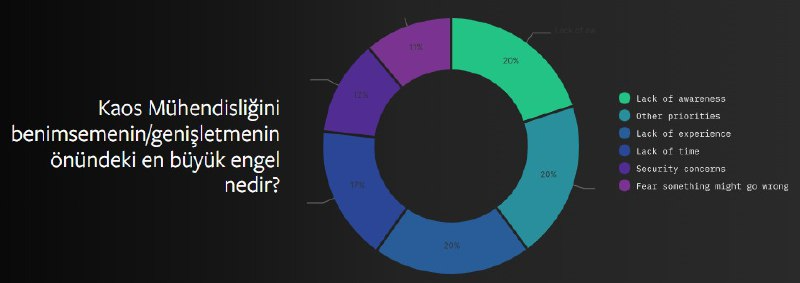
**Kaos Mühendisliği Nedir?**

Kaos mühendisliği, dağıtılmış yazılımın rastgele kesintiler karşısında dayanıklılığını doğrulamak için kasıtlı olarak başarısızlık ve hatalı senaryolar sunan bir test yöntemidir.

"Dünyanın dört bir yanındaki mühendislik ekipleri, sistemlerine kasıtlı olarak zarar vermek, etkiyi izlemek ve arızaları müşteri deneyimlerini olumsuz etkilemeden önce düzeltmek için Kaos Mühendisliği'ni kullanıyor. Bunu yaparken MTTD ve MTTR'yi azaltırken maliyetli kesintilerin önüne geçiyor, ekiplerini bilinmeyene hazırlıyor ve müşteri deneyimini koruyorlar. Aslında Gartner, 2023 yılına kadar Kaos Mühendisliği uygulamalarını kullanan kuruluşların %80'inin SRE girişimlerinin bir parçası olarak ortalama çözüm sürelerini (MTTR) %90 oranında azaltacağını öngörüyor. Aynı paralellikleri ilk Kaos Mühendisliği Durumu Raporunda da görüyoruz: en iyi performansı gösteren Kaos Mühendisliği ekipleri, bir saatten daha kısa bir MTTR ile dört dokuzlu kullanılabilirlikle övünüyor."

Kolton Andrus CEO, Gremlin





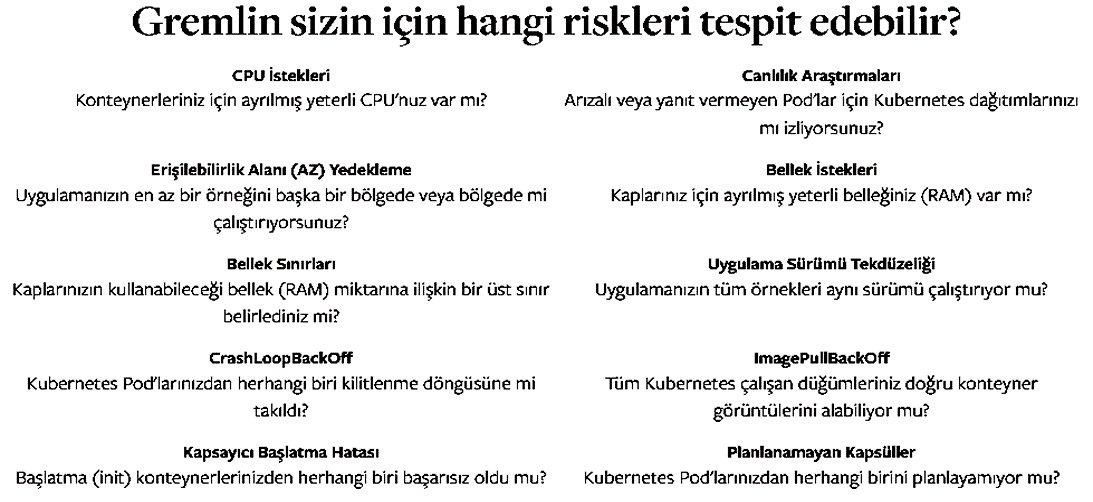
**2. GREMLİN**

Gremlin, web tabanlı güvenilirliği artırmak için tasarlanmış ilk barındırılan kaos mühendisliği platformudur. Hizmet olarak yazılım (SaaS) olarak sunulan Gremlin, birden fazla saldırı türünü kullanarak sistem dayanıklılığını test edebiliyor. Kullanıcılar, hangi saldırı türünün en iyi sonuçları sağlayacağını belirlemek için sistem girdileri sağlar. Kapsamlı altyapı değerlendirmelerini kolaylaştırmak amacıyla testler birbirleriyle bağlantılı olarak yapılabilir.

**Ana Özellikler**

* Arızaların hassas ve kontrollü bir şekilde kontrol edilmesi
* Çok düzeyli sistem saldırılarını içeren özel senaryolar
* Bellek sızıntıları, gecikme enjeksiyonları, disk dolumları ve daha fazlası için test süreci
* GameDay özelliği
* Önceden tanımlanmış testlere dayalı güvenilirlik puanı
* Maliyet
* Gremlin'in fiyatlandırması yıllar içinde, bir ekibin ihtiyaç duyduğu test sıklığını desteklemek için temsilci başına fiyatlandırmadan hedef başına saldırılara kadar dalgalandı.

**Gremlin Sizin Için Hangi Riskleri Tespit Edebilr?**



**Maliyet**

Gremlin'in fiyatlandırması yıllar içinde, bir ekibin ihtiyaç duyduğu test sıklığını desteklemek için temsilci başına fiyatlandırmadan hedef başına saldırılara kadar dalgalandı.

**Gremlin'i Kullanmalı Mıyım?**

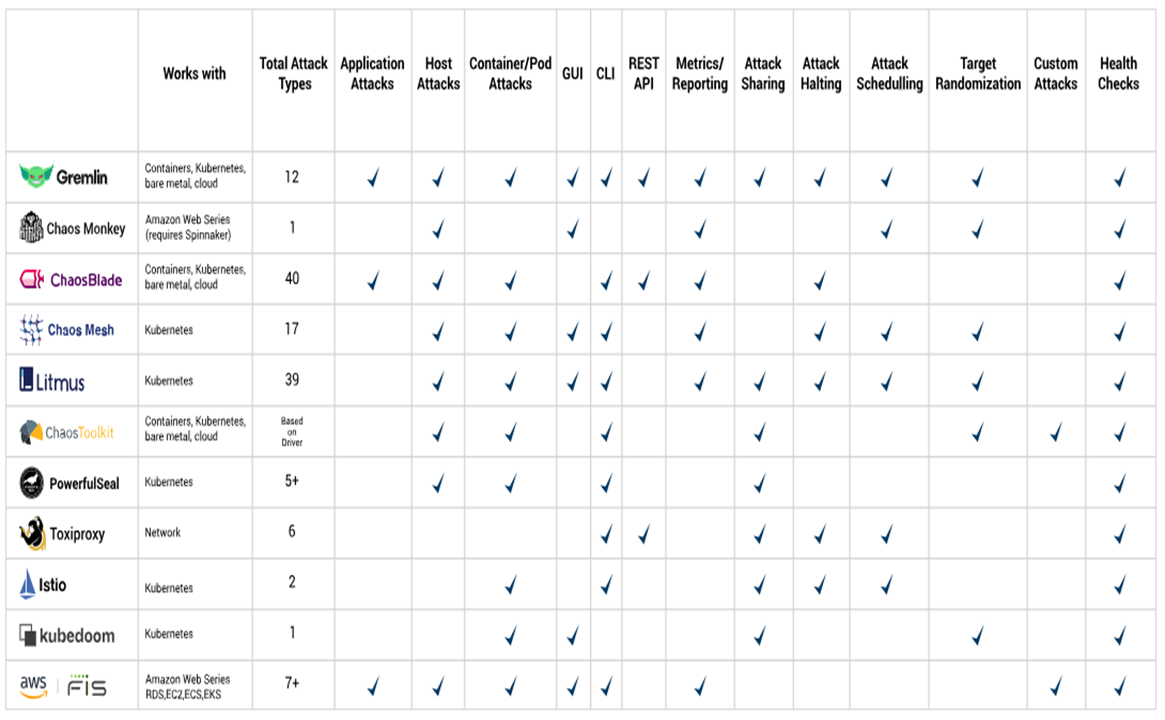
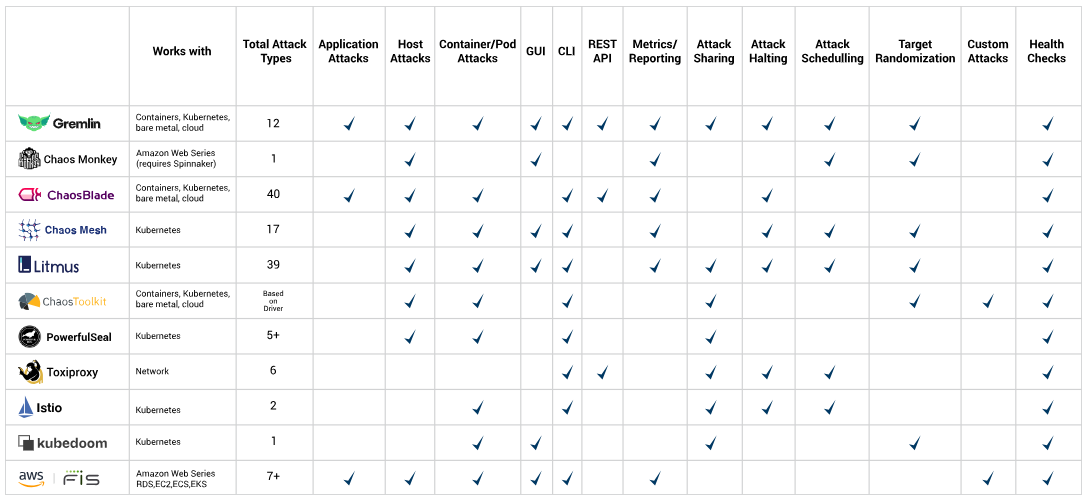
Dünyanın ilk yönetilen kurumsal kaos mühendisliği teknolojisi olan Gremlin, kullanıcılara düzinelerce saldırı vektörü başlatma, saldırıları durdurma ve geri alma ve sistem güvenilirliğini artırma yeteneği sağlar. Sürdürülebilir ve güvenilir bir internet yaratma misyonuyla tasarlanan Gremlin, gelir kaybını ve olumsuz sistematik etkileri en aza indirmek için yazılım zayıflıklarını tespit ediyor.

**3. PAZAR ARAŞTIRMASI**

Popüler kaos araçları aşağıdaki tabloda karşılaştırılmıştır.

**Araçlar =** Gremlin, Chaos Monkey, Chaos Blade, Chaos Mesh, Litmus, Chaos Toolkit, Powerful Seal, Toxipoxy, Istio, Kubedoom, Aws Fis

**Özellikler =**Toplam Saldırı Türleri, Uygulama Saldırılarıları, Ana Bilgisayar Saldırıları, Konteyner/Pod Saldırıları, GUI, CLI'si, REST API'si, Metrikler/Raporlama, Saldırı Paylaşımı, Saldırı Durdurma, Saldırı Planlama, Hedef Rastgeleleştirme, Özel Saldırılar, Sağlık kontrolleri



**4. TEKNİK DEĞERLENDİRME:**

**1. Kullanım Kolaylığı:** Gremlin, kullanıcı dostu bir arayüze sahip olmalı ve hizmet kesintilerini belirlemek ve uygulamak için kullanıcı dostu araçlar sunmalıdır. Arayüzün sezgisel olması, kullanıcıların kolayca kaos deneyleri oluşturmasını sağlar.

**2. Esneklik ve Özelleştirme:** Gremlin, farklı senaryoları simüle etmek için esnek yapılandırma seçenekleri sunmalıdır. Kullanıcılar, hizmet kesintilerinin türünü, süresini ve etkilediği kaynakları özelleştirebilmelidir.

**3. Platform Uyumluluğu:** Gremlin, farklı bulut sağlayıcıları ve altyapı ortamlarıyla uyumlu olmalıdır. Bu, kullanıcıların farklı sistemlerde ve çevrelerde kaos deneyleri yapmasını sağlar.

**4. Güvenilirlik ve Performans:** Gremlin, hizmet kesintilerini simüle etme sürecinde güvenilir olmalı ve sistem performansını olumsuz etkilememelidir. Ayrıca, kaos deneyleri sırasında sağlanan verilerin doğruluğu ve güvenilirliği de önemlidir.

**5. Topluluk Desteği ve Belgeleme:** Gremlin'in kullanıcılar için kapsamlı belgelendirmeye ve destekleyici bir topluluğa sahip olması önemlidir. Bu, kullanıcıların sorunlarını çözmelerine ve en iyi uygulamaları paylaşmalarına yardımcı olur.

**5. SONUÇ:**

Gremlin, kullanıcı dostu arayüzü, esnek yapılandırma seçenekleri ve çeşitli platformlarla uyumluluğuyla dikkat çeken bir kaos mühendisliği aracıdır. Kullanıcılar, Gremlin'i kullanarak çeşitli hizmet kesintilerini simüle edebilir ve sistemlerinin dayanıklılığını test edebilirler. Bununla birlikte, Gremlin'in bazı özelliklerinin daha fazla belgelendirilmesi ve topluluk desteğinin daha da geliştirilmesi gerekebilir. Genel olarak, Gremlin, dağıtılmış sistemlerin güvenilirliği üzerinde olumlu bir etki sağlayabilecek güçlü bir kaos mühendisliği aracıdır.

**6. SWOT ANALİZİ**

**Güçlü Yanlar (Strengths):**

* Gremlin, sistemlerde hataları öngörmek ve dayanıklılığı artırmak için etkili bir araçtır.
* Kolay kullanımı ve kullanıcı dostu arayüzü, Gremlin'in geniş bir kullanıcı tabanına ulaşmasını sağlar.
* Gremlin, farklı platformlara (örneğin, bulut tabanlı altyapılar, mikro hizmetler) entegre olabilme yeteneğine sahiptir.
* Kullanımı kolay kullanıcı arayüzü, yerleşik ekiplere çeşitli saldırılar ve testler yapılmasına olanak tanır
* Manuel entegrasyonlar oluşturmak için API desteği
* Güvenilirliği çeşitli farklı faktörlere dayalı olarak değerlendirir

**Zayıf Yanlar (Weaknesses):**

* Gremlin'in fiyatlandırma modeli, küçük ölçekli organizasyonlar için maliyetli olabilir.
* Bazı kullanıcılar, Gremlin'in karmaşık ayarlarının ve senaryolarının anlaşılması gerektiğini belirtmiştir.
* Gremlin'in bazı özellikleri, belirli altyapılar veya sistemlerle uyumsuz olabilir.
* Yazılım özelleştirilemez
* Deney JSON dosyalarını yazılım teslim hattına entegre etme zorluğu
* Minimum raporlama yetenekleri

**Fırsatlar (Opportunities):**

* Gremlin, sürekli gelişen bir alandaki pazarda yeni müşteriler kazanma potansiyeline sahiptir.
* Gremlin'in yeni entegrasyonlar ve özellikler eklenerek hizmet yelpazesi genişletilebilir.
* Kurumsal güvenlik ve bütünlük taleplerinin artması, Gremlin gibi dayanıklılık testi araçlarına olan talebi artırabilir.

**Tehditler (Threats):**

* Pazardaki rekabetin artması, Gremlin'in pazar payını azaltabilir.
* Gremlin'in kullanımının düşük olduğu durumlarda, organizasyonlar dayanıklılık testi araçlarına yeterli bütçe ayırmayabilir.
* Teknolojik gelişmeler ve güvenlik risklerindeki değişiklikler, Gremlin'in uyum sağlamak zorunda olduğu sürekli bir ortam oluşturabilir.

**KAYNAKLAR**

<https://www.gremlin.com/>

<https://www.infoq.com/news/2021/02/chaos-engineering-2021-report/>

<https://www.harness.io/blog/chaos-engineering-tools>

<https://www.royalcyber.com/blog/devops/chaos-engineering-tools/>

<https://medium.com/google-cloud/gremlin-chaos-engineering-on-google-cloud-2568f9fc70c9>