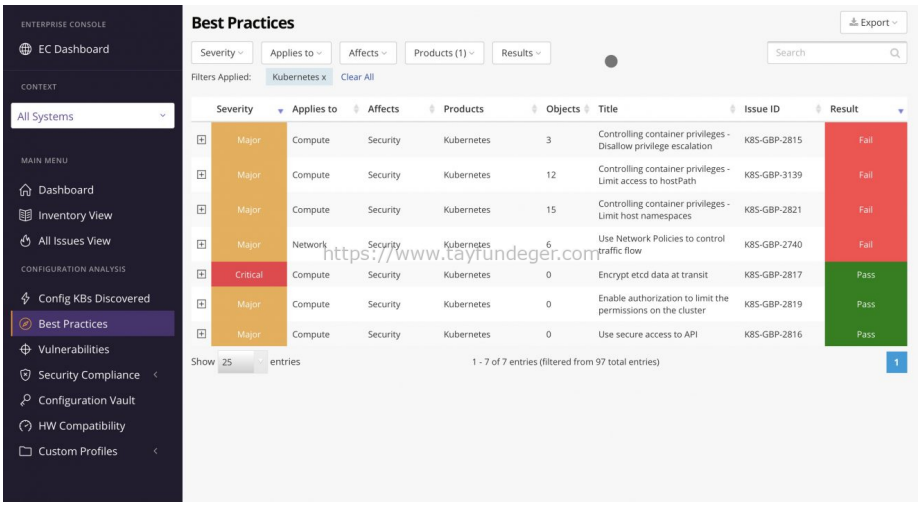
Runecast Kubernetes Ortamınızı Nasıl Analiz Eder?

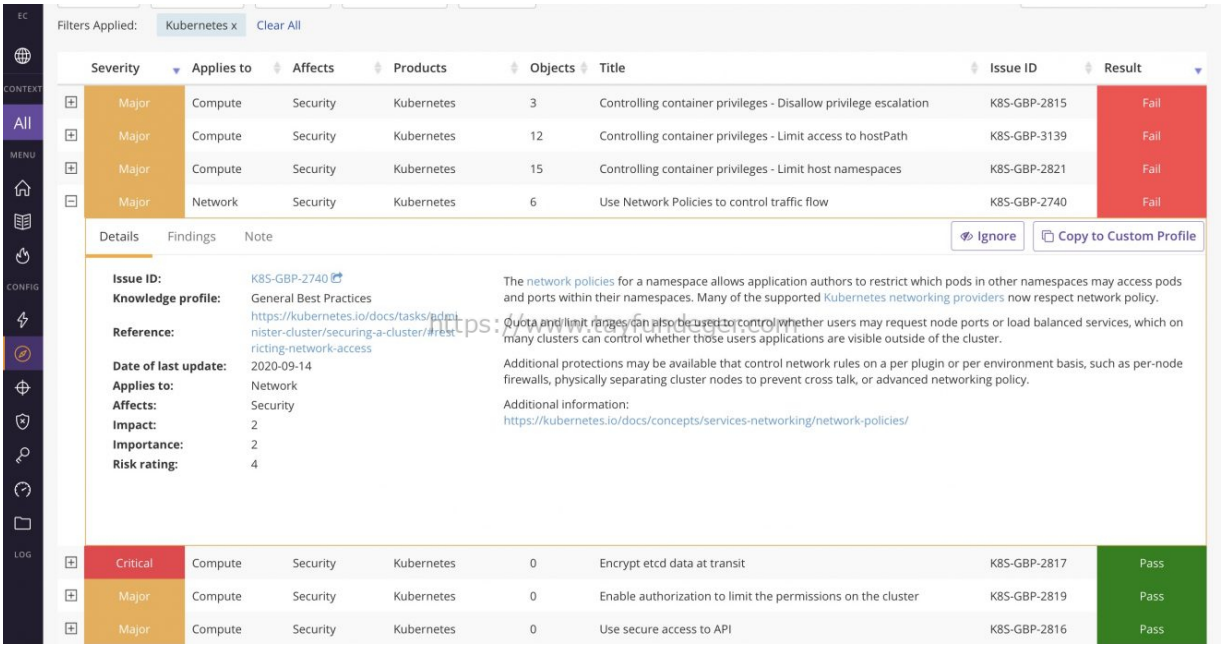
Kubernetes'i en basit hali ile anlatacak olursak, container üzerinde çalışan **mikroservis** tabanlı uygulamaların orkestrasyon işlemini gerçekleştiriyor. Yani sizin arka tarafta kullandığınız angular js'de uygulamanız olabilir ve arka tarafta mysql database'iniz olabilir. Kubernetes sayesinde database instance sayısını arttırabilir ve bunları orkestrasyon işlemini sağlayabilirsiniz. **Kubernetes**, **container** ortamındaki otomasyonu, orkestrasyonu sağlarken sunucunun dolaylı olarak network trafiğinide optimize edebiliyor. Yani şöyle düşünün, kubernetes otomasyon ve orkestrasyon işlemlerini yaparken burada load balancing, storage yönetimi, kaynak yönetimi gibi işleride yönetiyor. Bir container'in nasıl ve nerede devreye girmesi gerektiğini yönetiyor.

Runecast ile birlikte Kubernetes'i ilk olarak 4.5 sürümünde duymaya başladık. Kubernetes altyapılarını tasarlarken cluster ve workload'ları güvence altına almak gerekir. Burada bir orkestrasyon işlemi yapıldığı için çok fazla değişken olacaktır. Bu süreç oldukça dikkat gerektiren süreçler olduğu için eğer 3 party bir üründen faydalanmıyorsanız bazı standartları gözden kaçırmanı oldukça olasıdır. Runecast sayesinde Kubernetes uygulamaları ve Center for Internet Security (CIS) uyumluluk standartları otomaitk olarak kontrol edilir ve olumsuz bir durum var ise bu size raporlanır.

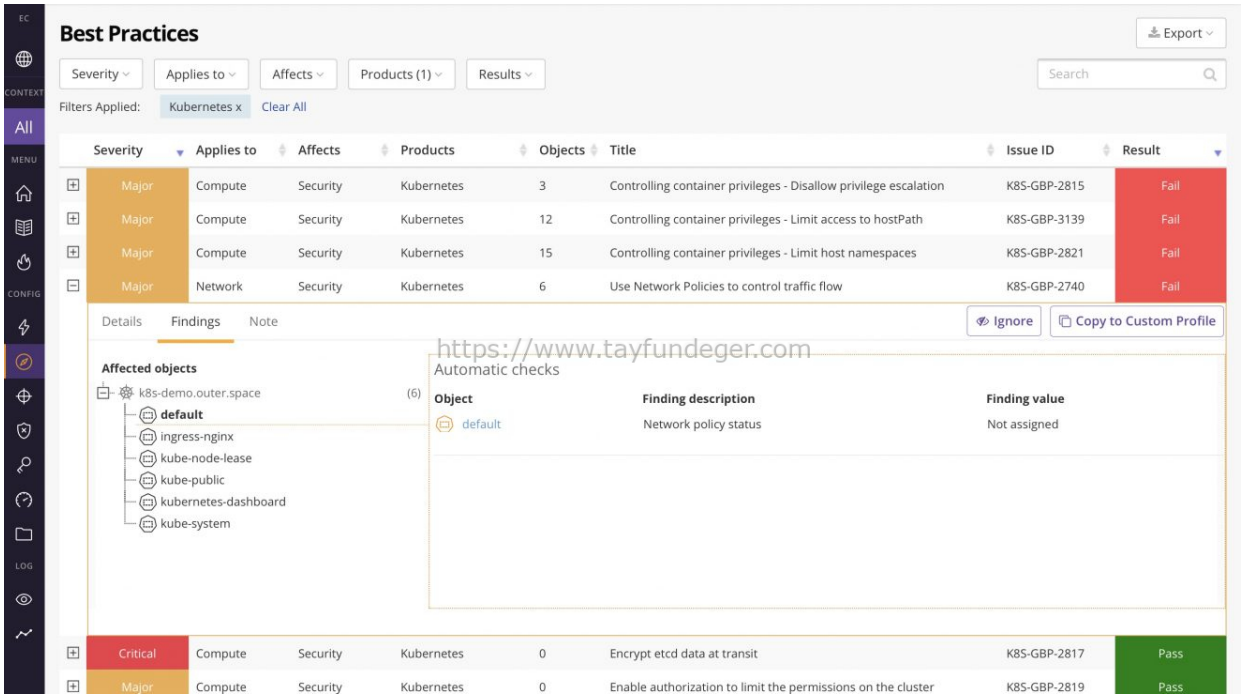
Runecast sayesinde sanallaştırma ortamlarını proaktif olarak izlerken aynı zamanda Kubernetes altyapılarınıda proaktif olarak izleyebiliyoruz. Kubernetes Best Practices 'lerine göre kritik sorunların ve düzeltilmesi gereken adımlarını Runecast üzerinde kolayca görebiliriz. Ayrıca mimarinizde oluşan güvenlik açıklarınıda basit bir şekilde görebilirsiniz.



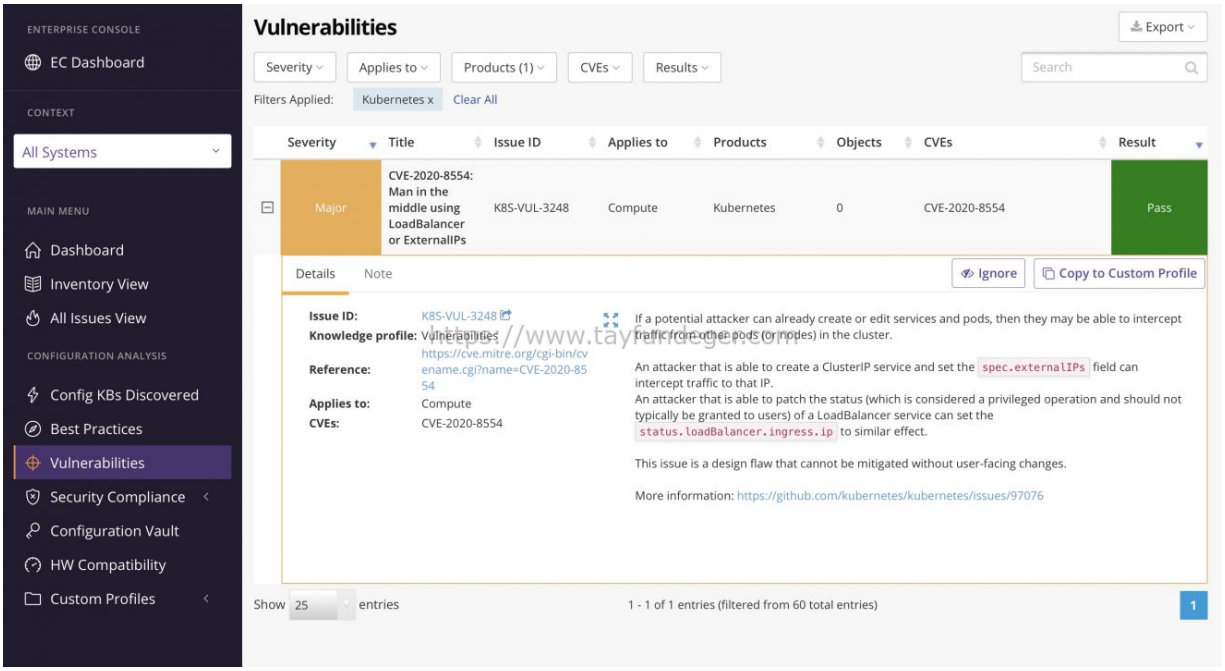
Runecast kullanıyorsanız Kubernetes altyapınızı basit bir şekilde kontrol edebileceğinizi söylemiştim. Runecast'a login olduktan sonra Best Practices bölümüne giriş yapıyoruz. Burada Products bölümünde yer alan Kubernetes seçeneğini seçerek Kubernetes ile ilgili Best Practices'lere aykırı olan bulguları karşımıza getiriyoruz.



Runecast Kubernetes Ortamınızı Nasıl Analiz Eder? Kubernetes kullanıyorsanız network tarafında yapacağınız izolasyonlara dikkat etmeniz gerekmektedir. Yukarıdaki örnekte Kubernetes objelerinde bir network policy'nin kullanılmadığı belirtiliyor. Ancak Kubernetes Best Practices'lerinde bunun kullanılması gerektiği belirtiliyor. Trafik akışını IP adresi veya port düzeyinde (OSI katmanı 3 veya 4) kontrol etmek istiyorsanız cluster'ınızda belirli uygulamalar için Kubernetes NetworkPolicies kullanmayı düşünebilirsiniz. Container mimarilerinde bu genellikle atlanan veya gözardı edilen bir konudur. Ancak bir saldırı veya atak durumunda bunların ne kadar önemli olduğunun farkına varırız.

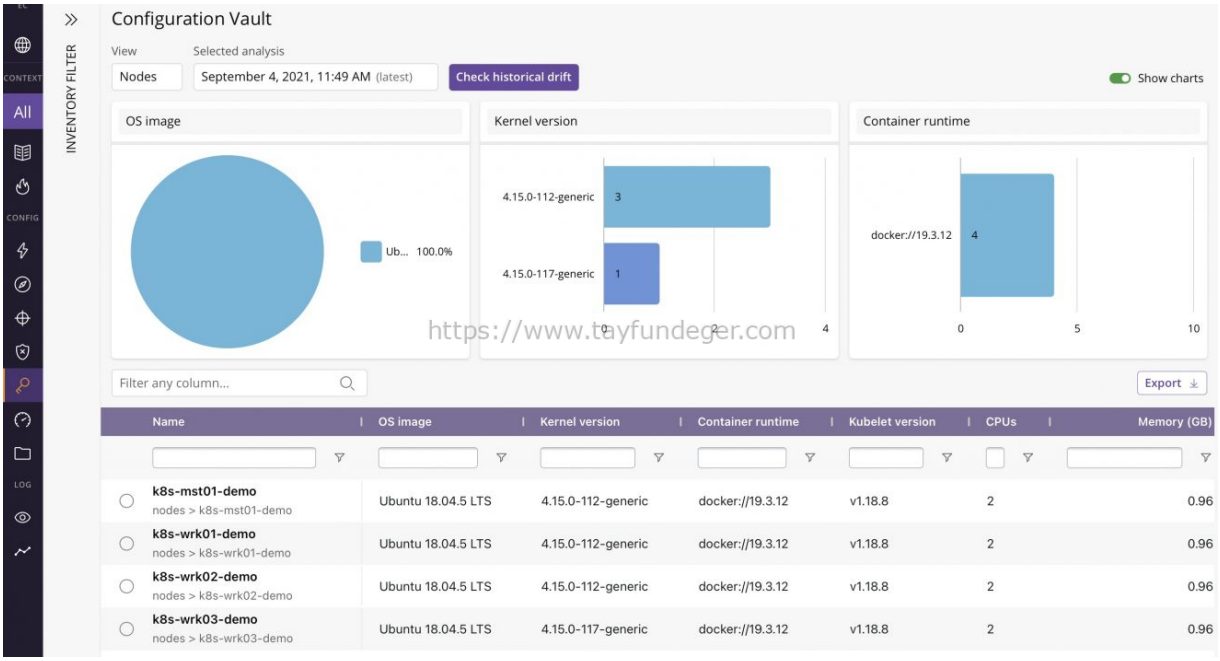


Ayrıca Best Practices'e aykırı olan bu durumun cluster'da mı yoksa node'lar arasında mı olduğunu ayırca Findings bölümünden görebilirsiniz. Yani bunun güzel yanı aslında komple node ve cluster'lara kadar taramalar yapıp bunların özelinde uyumsuzlukları çıkartıyor.



Vulnerabilities bölümünde güvenlik açıklarını görebilirsiniz. Runecast birden fazla ürünü kontrol ettiği için yukarıda yer alan Products bölümünden Kubernetes'i seçmeniz gerekiyor. Kubernetes'i seçtiğimizde, Kubernetes ortamındaki güvenlik zaafiyetlerini görebilirsiniz. Yukarıdaki örnekte, CVE-2020-8554 'un güvenlik zaafiyetini görebilirsiniz. Kubernetes kullanan kişiler bilir bu güvenlik zaafiyeti ilk çıktığında çok konuşulmuştu. Çünkü bu açık sayesinde cluster'da yeni pod'lar oluşturabilir ve gelen trafiği izleyebilirsiniz.

Gördüğünüz gibi oldukça ciddi bir güvenlik zaafiyeti ancak Runecast kullanıyorsanız Kubernetes altyapınızda bulunan güvenlik zaafiyetlerini ayrıca düşünmenize gerek kalmıyor. Çünkü Runecast, Kubernetes'in güvenliği için CIS Benchmark'ı kapsayarak node düzeyinde ve cluster düzeyinde otomatik Kubernetes analizleri sunar. Runecast Analyzer , CIS 1.6.0'a karşı kontrollerin kapsamı ile CIS Benchmarks ile güvenlik uyumluluğunuzu proaktif olarak denetler . Ayrıca güvenlik açığı eşlemesi sağlar.



Kubernetes bulunan ortamlarda Configuration Vault özelliğini kullanabilirsiniz. Bu özellik sayesinde konfigurasyon farklılıklarını görebilir ve buna göre müdahalelerde bulunabilirsiniz. Yukarıdaki örnekte node'lar arasında bulunan kernel version farklılığını görebilirsiniz. Ayrıca burada CPU, Memory, Kubelet version, Pod sayısı, OS Image gibi değerleride görebilirsiniz. İlerleyen versiyonlarda muhtemelen Configuration Vault bölümünde daha fazla veri ile karşılaşırız diye düşünüyorum.

Kendi altyapınızda güvenli bir şekilde çalışan Runecast Analyzer, hem bulutta hem de şirket içinde neler olup bittiğine ilişkin öngörülerle Kubernetes altyapınız için güvenlik uyumluluğu kontrollerini otomatikleştirir. Bu durum altyapıya proaktif yaklaşmanızı ve her zaman kontrol altında tutmanıza olanak sağlar.

Runecast Vmware Analyzer – Türkiye Distribütör firması “OTD Bilişim” satış ekibi otd.salesgrp@onlineteknikdestek.com ile iletişime geçebilirsiniz.