AWS Config

- AWS hesaplarınız içindeki AWS kaynaklarının yapılandırmalarının detaylı görünümlerini sunan bir hizmettir.
- Bu hizmetin güzel yanı, uzun vadeli dayanıklı depolama için S3 kovalarına teslim edilen normalize edilmiş veri sunmasıdır.
- Yaptığı şey, geçmiş dönemlere ait kaynaklarınızın yapılandırma geçmişini içeren şeyler gibi, kaynaklarınıza yapılan değişiklikleri kaydetmek adına bir yapılandırma kayıt zaman çizelgesi sağlamaktır.
- Kaynaklarınızdaki yapılandırma değişikliklerini adeta bir kayıt olarak kaydeden bir sistemdir.
- Herhangi bir kaynağınızın değişikliklerini önleme amacında değildir. Yalnızca bildirimler ve bu değişikliklerin kaydedilmesi içindir.
- Kaynaklarınızın detaylı görünümlerini sağlayarak farklı yapılandırma hatalarını kolayca algılamanıza ve bildirim göndermenize olanak tanır. Bu oldukça detaylı hale gelebilir.
- Amazon EC2 güvenlik gruplarına değişiklik yapma gibi değişiklikleri yakalamak ve sonradan denetlemek için AWS Config kullanabilir. Bu çok güçlü bir araçtır.
- Config etkinliklerini Amazon EventBridge'e veya hatta AWS Lambda'ya göndererek neredeyse gerçek zamanlı olay işleme için olanak tanır. Bu bildirimler, otomatik düzeltme iş yüklerinizi tetikleyebilir. Yani bir güvenlik gruplarına bir değişiklik yapılıyorsa, bu değişikliği tarayan ve değişmiş olabilecek portları düzelten bir Lambda tetikleyicisi kullanabilirsiniz. Şimdi son senaryo ve konsept burada SNS entegrasyonudur.

AWS Trusted Advisor

- Hesabınızı en iyi uygulamalar için incelenen bir hizmettir. Bu, endüstri ve müşteri tarafından belirlenen en iyi uygulamaları kullanır.
- Yaptığı şey, bir hesap düzeyinde çalışıyor ortamlarımızı denetliyor ve ardından bu konuştuğumuz en iyi uygulamalara dayalı olarak gerekli gördüğü yerlerde önerilerde bulunuyor.

Amazon GuardDuty

- GuardDuty, sürekli güvenlik izleme sunan bir hizmettir ve birden çok veri kaynağından, CloudTrail gibi hatta DNS günlüklerinden gelen verileri işleme olanağı tanır.
- Tehdit istihbarat akışları ve makine öğrenimini kullanarak potansiyel kötü niyetli ve istenmeyen eylem desenlerini tespit etmek ve uyarı vermek için akıllı tespit imkanı sunar.
- Bazı örnek bulgular arasında artırılmış ayrıcalıklar, açığa çıkarılmış kimlik bilgileri ve kötü niyetli IP adresleri aracılığıyla API'lerle ve hizmetlerle etkileşimler bulunmaktadır.
- Yaptığı şey, bulgular üretir ve bulgular üretilir ve ardından raporlanır ve bunlar hesaplarınız ve uygulama ortamlarınızın iç görülerini sağlar.
- Bu hizmet ayrıca EventBridge ile kolayca entegre olabilir, böylece otomatikleştirebilirsiniz. Ve buradaki son şey, GuardDuty'yi kuruluşlarda kullanabilir ve bunu yapmanız kesinlikle önerilir.
- Bir sonraki şeyimiz bastırma kuralı. Bunlar, belirli bulgulardaki belirli özellik kombinasyonlarını belirtmenizi sağlayan kurallardır, ki bu mantıklıdır. Bu kurallar aracılığıyla bulguları bastırıyorsunuz.
- Ayrıca güvenilen IP adresleri listesine sahip olabilirsiniz. Bu, GuardDuty'nin hiçbir zaman bulgu oluşturmaktan kaçınacağı güvenilen IP adreslerinin bir listesidir.
- Oluşturulan herhangi bir bulgu, EventBridge otomasyonları içinde kullanabileceğimiz bir olay üretebilir. Bu, lambda'ları tetikleme, SNS konularını tetikleme vb. gibi şeyleri içerir.
- Yani temelde AWS hesaplarımıza entegre edilmiş bir sızma algılama sistemidir. Bu, sınav için bilmeniz gereken bir şeydir. Engelleyici değil, sadece algılar. Ayrıca entegrasyonlarla ilgili bir şeyi de not etmek önemlidir. GuardDuty'yi, Security Hub, Amazon Detective veya EventBridge gibi şeylerle karşılaştırabilir

ve bu, güvenlik verilerini toplamamıza, güvenlik durumlarımızı değerlendirmemize ve ardından olayları ve bulguları incelemek için verileri kaydetmemize olanak tanır.

Amazon Inspector

- Inspector, otomatik değerlendirmeler ve zayıflıklar taramaları sunan yönetilen bir güvenlik hizmetidir.
- Bu, güvenliğimizi ve uyumluluğumuzu artırmamıza yardımcı olacak.
- Yaptığı şey, bulgular üretir ve bu bulgular, listeler aracılığıyla size bildirilen detaylı raporlardır.

AWS Artifact

- Farklı AWS güvenlik ve uyumluluk belgelerinizi indirmek için merkezi bir kaynak sağlayan bir hizmettir.
- Bu hizmet, farklı uyumluluk gereksinimlerine ait farklı belgeleri denetçilere ve düzenleyicilere sunmanıza olanak tanır.
- Ayrıca hizmet, resmi belgelerin yanı sıra, mevcut AWS mimarilerinizi ve uygulamalarınızı güvence altına almak için belgeleri kullanmanız için kılavuzlar sağlar.

Amazon Detective

- Olayları çözmenize yardımcı olan bir dedektif servisidir, bu olayların kök nedenini anlamak için güvenlikle ilgili olayları araştırmanıza yardımcı olur.
- Detective, GuardDuty, VPC Flow Logs ve CloudTrail yönetim olayları gibi AWS hizmetlerinizden otomatik olarak günlükleri toplar ve güvenlik verilerinizin birleşik bir görünümünü ve görsel temsilini oluşturmak için bunları kullanır.
- Amazon Detective, bu görevi güvenlik ekibinizin daha hızlı ve verimli güvenlik soruşturmalarını kolaylaştırmak için istatistiksel analiz, veri madenciliği ve ilgili güvenlik bilgileri veri setlerini oluşturmak ve bağlamak için graf teorisi kullanarak gerçekleştirir.
- Amazon Detective'ı kullanmaya başlamak için, yönetim konsolunda etkinleştirilmesi ve hizmeti başlatmadan önce Amazon GuardDuty'nin etkinleştirilmiş olması gerekmektedir.