Kullanıcı Soruları ve Cevapları

- Lider tehdit istihbaratı analisti olarak, BİT altyapılarına ve kuruluşlarına yönelik saldırıları önleyebilmek için tehditleri yakalamaya odaklanan bir ekibe liderlik etmek istiyorum.
  - Canlı Kontrol Panelini kullanarak ekiplerin gerçek zamanlı olarak neler yaptığını izleyin.
- Bir tehdit analisti olarak, kötü amaçlı yazılımlara nasıl karşı koyacağımı bilmek için kötü amaçlı yazılımları araştırmak, analiz etmek ve tersine mühendislik yapmak istiyorum.
  - **"Event"lere Dosya ve Kötü Amaçlı Yazılım Örnekleri Ekleyin ve İndirin:**
    - MISP panelinizden ilgili etkinliğe gidin.
    - Dosyalar sekmesine gidin ve istediğiniz kötü amaçlı yazılım örneklerini ekleyin.
    - Eğer mevcutsa, kötü amaçlı yazılım örneklerini indirin ve analiz için yerel araştırma ortamlarınıza aktarın.
  - **Kötü Amaçlı Yazılım Olaylarında Karma ve İlgili Bilgileri Arayın:**
    - MISP panelinizden arama aracını kullanarak kötü amaçlı yazılım olaylarındaki karmaları, IP'leri, etki alanlarını ve URL'leri arayın.
    - Bu aramaları gerçekleştirerek, belirli bir kötü amaçlı yazılımın veya tehdidin yaygınlığını ve etkisini değerlendirin.
  - **Kötü Amaçlı Yazılım Örnekleri Karma ve İlgili Bilgileri Ekleyin:**
    - Kötü amaçlı yazılım olaylarınıza kötü amaçlı yazılım örnekleri karmalarını ekleyin.
    - Bu karmaları ekleyerek, benzer kötü amaçlı yazılım örneklerinin izlenmesini ve analiz edilmesini sağlayın.
  - **Korelasyon Grafiği ve Genişletme Modülleri ile Gözlemlenebilirleri İnceliyin:**
    - MISP panelinizde korelasyon grafiklerini kullanarak, gözlemlenebilirler arasındaki ilişkileri analiz edin.
    - Genişletme modüllerini kullanarak, IoC'lerin doğruluğunu kontrol edin ve yanlış pozitifleri ele.
  - **MISP Dışındaki Veri Kaynaklarını Sorgulayarak Kötü Amaçlı Yazılım Olaylarını Zenginleştirin:**
    - MISP panelinizde bulunan modüller aracılığıyla, MISP dışındaki veri kaynaklarını sorgulayarak kötü amaçlı yazılım olaylarını zenginleştirin.
    - Bu sayede, kötü amaçlı yazılım olayları hakkında daha fazla detay ve context elde edin.
  - **Dinamik Kötü Amaçlı Yazılım Analizi Korelasyonları Gerçekleştirin:**
    - İlgili analiz araçlarına (örneğin, VirusTotal, VMRay) kötü amaçlı yazılım örneklerini göndererek, dinamik analiz sonuçlarını alın.
    - Bu sonuçları MISP panelinizdeki kötü amaçlı yazılım olaylarıyla ilişkilendirerek, daha kapsamlı bir tehdit analizi yapın.

- Lider tehdit istihbaratı analisti olarak, güvenlik duruşunu geliştirebilmek için tehdit verilerini, eyleme dönüştürülebilir tehdit istihbaratına dönüştürmek istiyorum.
  - Dış kaynaklardan veri alımı yapın
  - "Feed"leri ekleyin
  - "Event"leri ve "Attribute"leri etiketler, taksonomiler ve galaksiler kullanarak bağlamlandırın.
- Tehdit Analisti olarak, tehdit bilgilerini üçüncü taraflarla paylaşmak istiyorum, böylece ortak bir durum farkındalığı kazanabiliriz.
  - MISP örneğinde farklı dağıtım modellerini kurun
  - Olayları ve öznitelikleri örnekler arasında senkronize edin
  - Bir kuruluşun paylaşım politikasını karşılamak için filtreleme işlevlerini kullanın
  - Bilgileri, pentest bilgilerini, kötü amaçlı yazılım örneklerini, zafiyetleri içeride ve dışarıda paylaşın
- Tehdit Analisti olarak, tehditleri izlemek ve canlı verilere erişmek istiyorum, böylece ciddi bir hasara neden olmadan tehditleri yönetebilirim.
  - Göstergelerin listelerini içe aktarın ve IoC'lerin "Feed"lerde mevcut olup olmadığını kontrol edin.
  - Widget'ları kullanarak istatistikleri ve gözlemleri izleyin
  - Canlı verileri ve istatistikleri MISP Dashboard aracılığıyla bir veya daha fazla MISP örneğinden gösterin
- Tehdit Analisti olarak, çeşitli kaynaklardan gelen göstergeleri toplamak ve karşılaştırmak istiyorum, böylece çeşitli tehditler arasındaki bağlantıları kurabilirim.
  - Topluluklara katılın ve "Feed"lere abone olun
  - "Event"leri ekleyin ve belirli "Feed"lere "Event"ler atayın
  - MISP'in otomatik korelasyon motorunu kullanarak göstergeleri karşılaştırın
  - MISP'te mevcut olan "Feed"leri analiz edin
  - Korelasyon grafiğini kullanarak "Event"leri ve "Attribute"leri bağlayın
  - Modülleri kullanarak "Attribute"ler üzerinde daha fazla bilgi edinin
  - Galaksileri kullanarak "Event"leri kötü amaçlı yazılımlar, tehdit aktörleri vb. ile ilişkilendirin (örneğin ATT&CK)
- Tehdit Analisti olarak, yeni tehditleri araştırırken sorgular yapabilmek için tehdit verilerinin yapılandırılmış bir veritabanına sahip olmak istiyorum.
  - Bilgileri STIX formatında yapılandırılmış bir formatta depolayın
  - Serbest metin içe aktarma aracını kullanarak yapılandırılmamış raporları içe aktarın
  - MISP'i güvenlik ve sahtekarlık tehdit istihbaratı için merkezi bir merkez olarak kullanın. OSINT ve ticari beslemelerden göstergeleri bir araya getirerek tehdit istihbaratını merkezileştirin
  - "False-Positive"leri ve kopyaları kaldırın
  - Gözlemler tarafından puanlanan göstergeleri değerlendirin
  - Üçüncü taraflardan tehdit istihbaratı veya "Feed"lerini içe aktarın. "Feed"leri oluşturmak için veri deposunun filtrelenmiş alt kümelerini oluşturun
  - Değerlendirme için doğrudan "Feed"leme verilerini önizleyin ve karşılaştırın
- Tehdit Analisti olarak, ham tehdit verilerini zenginleştirerek ve bağlamsallaştırarak harekete geçirilebilir istihbarat üretebilmek istiyorum.
  - Taksonomileri kullanarak saldırgan TTP'lerini anlayın
  - Galaksileri ve taksonomileri kullanarak riskleri ve olayları kategorize edin
  - Etiket koleksiyonlarını kullanarak bilgileri hızlı bir şekilde sınıflandırın

    - Gözlem kaynakları hakkında bilgilerle gözlemleri bağlamsallaştırın
    - IDS'lerin dışa aktarımını etiketlerle zenginleştirin
    - Gözlemleri gözlemleme bilgilerini kullanarak bozulma ve göstergeleri puanlayın
    - MISP'in daha zengin veri yapısı kullanarak karmaşık senaryoları tanımlayın ve görselleştirin
    - MISP nesneleri (object) kullanarak "Attribute"lerin gelişmiş kombinasyonlarını sağlayın
- Tehdit Analisti olarak, tehditleri araştırarak bilgisayar sistemlerini saldırılardan korumak istiyorum.
    - MISP topluluklarından ilgili verileri bulun. Birden çok kaynaktan gelen yeni MISP olaylarını ve uyarıları önizleyin, örneğin e-posta raporları, CTI sağlayıcıları ve SIEM'ler
    - Belirli bir IOC içeren olaylar için bir MISP örneğine sorgu yapın. Diğer MISP olayları, öznitelikler, nesneler, etiketler ve galaksilere göz atın
    - "Event"ler oluşturun, IoC'ler ekleyin ve etiketler kullanarak bağlamsallaştırın
    - Bir olayı bileşenlerine, nesnelerine, etiketlerine, galaksilere ve/veya ilgili "Event"lere dönüştürün
    - Galaksiler ve ilgili "Event"ler aracılığıyla daha fazla ayrıntıya göz atın
    - Kullanılan Cytomic Orion API gibi araçlardan belirli MISP göstergelerinin gözlemlendiğini kontrol etmek için sorgular yapın ve ardından bunları MISP olaylarına eklemek için görme ayrıntılarını içe aktarın
    - Kullanıcılar, betikler ve IDS'ler tarafından toplanan Gözlemlerden tehditleri önceliklendirin.
    - Kullanıcılar, betikler ve IDS'ler tarafından bildirilen Gözlemler kullanılarak göstergeleri bozulma/sona erme durumlarına göre sona erdirin

---

Revision #3
Created 9 April 2024 12:05:41 by İlayda Durlanık
Updated 9 April 2024 22:13:01 by İlayda Durlanık