Proje Hakkında

- Tarihçesi
- MISP Nedir?

Tarihçesi

Christophe Vandeplas Tehdit Göstergeleri (IOCs), e-posta veya pdf belgeleri ile paylaşılıyor ve otomatik makineler tarafından ayrıştırılamıyor olmasından fazlasıyla rahatsız olmuştur. Bu nedenle Haziran 2011 civarında, CakePHP ile denemeler yapmaya başladı ve fikrinin bir kanıtını ortaya koymuştur. Bu projeye CyDefSIG: Siber Savunma İmzaları adını verdi.

Temmuz 2011'in ortalarında, kişisel projesini Belçika Savunmasındaki iş yerinde sunmuştur ve geri bildirim oldukça olumlu olmuştur. Belçika Savunmasının CyDefSIG'i resmi olarak kullanmaya başlamasıyla birlikte 2011'in ortalarından itibaren CyDefSIG'e erişim verilmiştir. Bu noktada, Christophe, evde çalışmaya devam ederken iş saatlerinde CyDefSIG'e biraz zaman ayırmasına izin verilmiştir.

Bir noktada NATO bu projeden haberdar olmuştur. Ocak 2012'de projeyi daha detaylı olarak tanıtmak için ilk sunum yapılmıştır. NATO, pazarda sunulan diğer ürünlere göre CyDefSIG'in açıklığını bir avantaj olarak görmüştür. Böylece Andrzej Dereszowski, NATO tarafından ilk kısmi zamanlı geliştirici olmuştur.

Birkaç ay sonra NATO, kodu iyileştirmek ve daha fazla özellik eklemek için tam zamanlı bir geliştiriciyi işe almıştır. Geliştirme süreci o tarihten itibaren başlamıştır. Birçok kişisel projede olduğu gibi lisans henüz açıkça yazılmamıştı, proje kamuoyuna Affero GPL lisansı altında yayınlanacağına karar verilmiştir. Bu kaynak kod mümkün olan en çok insanla paylaşmak ve herhangi bir zarardan korumak içindi.

Ocak 2013'te Andras Iklody, MISP'in başlıca tam zamanlı geliştiricisi olmuştu. Günümüzde, Andras Iklody MISP projesinin baş geliştiricisi ve CIRCL'de çalışıyor.

MISP projesi genişledikçe, artık sadece kötü amaçlı yazılım göstergelerini değil, aynı zamanda sahtekarlık veya güvenlik açığı bilgilerini de kapsıyor. Adı artık MISP Threat Sharing olarak değişti. MISP şimdi bir topluluk projesi, bir grup gönüllü tarafından yönetilmektedir.

MISP Nedir?

MISP, hedeflenen saldırılara, tehdit istihbaratına, mali dolandırıcılık bilgilerine ve güvenlik açığı bilgilerine ilişkin Tehdit Göstergelerini (IOC'ler) paylaşmak, depolamak ve ilişkilendirmek için bir tehdit istihbarat platformudur. Bu platform, sadece siber güvenlik göstergelerini ve kötü amaçlı yazılım analizini depolamak ve paylaşmakla kalmaz, aynı zamanda saldırıları, sahtekarlıkları veya tehditleri tespit etmek ve önlemek için IOC'leri ve bilgileri kullanır.

MISP, organizasyonların karşılaştığı tehditler ve güvenlik açıkları hakkında bir bilgi deposu olarak hizmet eder. Bilgi tutarlı bir yapıya kavuşturulduğunda, aranabilir hale gelir ve güvenlik analistlerinin bilgileri farklı zamanlarda ilişkilendirmesi daha kolay olur. Otomatik olarak benzer bilgileri ilişkilendirir ve bilgileri tutarlı bir formatta depolayarak, kuruluşlar arasında bilgi paylaşımını kolaylaştırır.

Ayrıca, MISP iş ortaklarından, analistlerden, araçlardan ve yayınlardan bilgi toplayan bir araçtır. Bu araç, verileri ilişkilendirir, zenginleştirir ve ekiplerin, toplulukların işbirliği yapmasını sağlar. Bu şekilde, otomatik koruyucu araçları ve analiz araçlarını besleyerek etkili bir şekilde tehditleri tespit etmeye ve önlemeye yardımcı olur.