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.

Revision #5
Created 6 April 2024 20:41:48 by İlayda Durlanık
Updated 7 April 2024 18:19:47 by İlayda Durlanık