



 MALTEGO

Paterva Maltego XL



MALTEGO NEDİR?

Maltego, gerçek zamanlı veri madenciliği ve bilgi toplamanın yanı sıra bu bilgilerin düğüm tabanlı bir grafikte temsilini, söz konusu bilgiler arasında kalıplar ve çoklu sıra bağlantıları oluşturan, grafiksel bağlantı analizleri için kapsamlı bir araçtır.

Maltego ile, dağınık kaynaklardan verileri kolayca çıkarabilir, eşleşen bilgileri tek bir grafikte otomatik olarak birleştirebilir ve veri ortamınızı keşfetmek için görsel olarak haritalayabilirsiniz.

Maltego, Dönüşümleri kullanarak çeşitli kaynaklardan gelen verileri ve işlevleri kolayca bağlama yeteneği sunar. Dönüştürme Merkezi aracılığıyla 30'dan fazla veri ortağından, çeşitli genel kaynaklardan (OSINT) ve kendi verilerinizden gelen verileri bağlayabilirsiniz.



NE İÇİN KULLANABİLİRİM?

Maltego, güvenlikle ilgili tüm çalışmaların bilgi toplama aşaması için kullanılabilir. Size zaman kazandıracak ve daha doğru ve daha akıllı çalışmanıza olanak sağlayacaktır.

Maltego size çok daha güçlü bir arama sağlayarak daha akıllı sonuçlar verir. "Gizli" bilgilere erişim başarınızı belirlerse, Maltego bunları keşfetmenize yardımcı olabilir.

Maltego, aranan öğeler arasındaki bağlantıları görsel olarak sunarak düşünme sürecinize yardımcı olur.

Maltego'nun odak noktası, internette açık kaynak bilgiler arasındaki gerçek dünya ilişkilerini analiz etmektir. Bu, İnternet altyapısının yanı sıra ona sahip olan kişi ve kuruluş hakkında bilgi bulmayı da içerir.





Maltego XL'nin özellikleri nelerdir?

- Tek bir grafik üzerinde 1.000.000 varlığa kadar bağlantı analizi gerçekleştirme yeteneği.
- Dönüşüm başına 64.000'e kadar sonuç döndürme yeteneği.
- Varlıkları otomatik olarak gruplandırarak toplama düğümlerini içerir, ortak özellikleri görmeye ve aradığınız temel ilişkileri bulmanıza olanak tanır.
- Tek bir oturumda birden çok analistle grafikleri gerçek zamanlı olarak paylaşma becerisini içerir.
- Grafik dışı aktarma seçenekleri şunları içerir:
 - Resimler - jpg, bmp ve png
 - PDF.
 - Tablo biçimleri - csv, xlx ve xlsx
 - GraphML.
 - Varlık listeleri
- Grafik içi aktarma seçenekleri şunları içerir:
 - Tablo biçimleri - csv, xls ve xlsx
 - Kopyala ve yapıştır.



Tüm verilerinize tek bir kullanıcı arayüzünden erişin.

Splunk, ServiceNow, ELK, vb. gibi dahili verileri entegre edin.

Araştırmalarınızı, beslemesi zor OSINT verileriyle bir düğmeye tıklayarak kolayca zenginleştirin.

CrowdStrike, Recorded Future, Flashpoint ve daha fazlası gibi Threat Intel Feed sağlayıcılarını entegre edin.



Verilerinizi hızlı bir şekilde analiz edin.

SIEM uyarılarından ilgili verileri hızla belirleyin ve bunları araştırmanızla ilgili verilerle zenginleştirin.

Bir SIEM uyarısının yanlış pozitif olup olmadığını veya Maltego'nun güçlü görselleştirme yeteneklerinde gerçek bir tehdit olup olmadığını hızla değerlendirin.

Maltego Sistemini kullanarak tekrar eden araştırmaları otomatikleştirin.



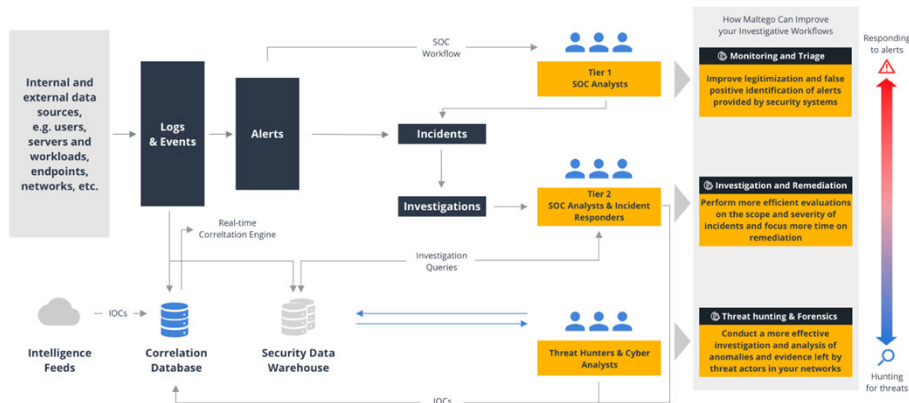
Ekibinizle işbirliği yapın.

Canlı grafik paylaşımı yoluyla ekiplerinizle kolayca işbirliği yapın.

Kuruluşunuz içinde anlaşılması kolay bir tehde genel bakış ve inceleme raporu paylaşın.

Yeni öngörülerini SIEM'inize veya çağrı sisteminize aktararak mevcut iş akışlarıyla kolayca entegre edin.

Araştırma İş Akışlarınızı Optimize Edin



Ankara: Ümit Mah. 4281 Sok. Kafkas Sitesi No:6 06810 Ümitköy/ÇANKAYA

İstanbul: Esentepe Mah. Kelebek Sk. No:2 Marmara Kule Kat:10 D:79 34870 KARTAL



+90 (312) 219 56 16

+90 (216) 771 07 97

