Proje Hakkında

- TheHive Nedir?
- TheHive Tarihçesi

TheHive Nedir?

TheHive, güvenlik olaylarının yönetimine ve analizine yardımcı olmak için tasarlanmış açık kaynaklı ve ücretsiz bir Güvenlik Olayı Müdahale Platformudur (SIRP). SOC'ler, CSIRT'ler, CERT'ler, hızla araştırılması ve harekete geçilmesi gereken güvenlik olaylarıyla ilgilenen tüm bilgi güvenliği uygulayıcılarının hayatını kolaylaştırmak için tasarlanmıştır. Güvenlik analistleri, Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT'ler) ve Güvenlik Operasyon Merkezleri (SOC'ler) için geliştirilen TheHive, tehdit avcıları ve olaylara müdahale edenlerin güvenlik olaylarını verimli ve etkili bir şekilde araştırmaları ve çözmeleri için kapsamlı bir çözüm sunar.

Özelleştirilebilir gösterge tabloları, yerleşik gözlemlenebilir veriler, MISP ve Cortex gibi popüler tehdit istihbaratı araçlarıyla entegrasyon dahil olmak üzere zengin özellikleriyle TheHive, güvenlik uzmanlarının, güvenlik olaylarını etkili ve verimli bir şekilde önceliklendirmesine, analiz etmesine ve bunlara yanıt vermesine olanak tanır. TheHive, Cortex, güvenlik analistleri ve araştırmacılar gözlemlenebilir ögeyi kolaylıkla analiz edebilir.

TheHive Tarihçesi

StrangeBee adındaki şirket, 2019 yılından bu yana TheHive projesini üstlenmiş ve Cortex ekosisteminin geliştirilmesi, sürdürülmesi, desteklenmesi ve dağıtılması gibi önemli görevleri üstlenmiştir. Şirketin kurucularını destekleyen güçlü bir ekip bulunmaktadır. Bu ekipte projenin hayata geçmesine yardımcı olan Nabil Adouani ,Thomas Franco ,Jérôme Leonard gibi önemli isimler liderlik etmiştir.

TheHive, 2013 yılında Fransız Bilgi Güvenliği Ajansı (ANSSI) tarafından başlatılan ve ilk sürümü açık kaynak kodlu bir olay müdahale platformu olarak geliştirilen bir projedir. 2014 yılında ilk resmi sürümünü (v1.0) yayınlayan TheHive, o zamandan beri birçok yeni özellik ve geliştirmeyle güncellenmiştir. Bu süre zarfında, geliştirme ekibi, proje yöneticileri ve topluluk katkılarıyla TheHive'ın sürekli iyileştirilmesine katkıda bulunmuştur.

2022 yılında, TheHive lisansı ticari bir lisansa dönüşmüştür. Bu dönüşüm, TheHive'ın olgunlaşmasını sağlamış ve özellikle şirketlerin karşılaştığı güvenlik zorluklarına daha etkin bir şekilde yanıt verebilme kabiliyetini artırmıştır. Ticari lisansın getirdiği avantajlar, kullanıcılar için daha güçlü ve kapsamlı bir deneyim sunmayı amaçlamaktadır. Proje yönetimi ve geliştirme ekibi, kurucuları destekleyen TheHive'ın başarısını sağlamaktadır.