Splunk Nedir ?

Splunk, büyük veri analizi ve log yönetimi için kullanılan bir yazılımdır. Yapılandırılmış ve yapılandırılmamış verileri gerçek zamanlı olarak toplar, indeksler, analiz eder ve anlamlı raporlar oluşturur. Özellikle BT güvenliği, sistem izleme ve iş zekası alanlarında kullanılır.

Splunk Ne İçin Kullanılır?

1. **Log Yönetimi ve Analizi:**
   - Sunucular, ağ cihazları, güvenlik duvarları gibi sistemlerden gelen logları toplayıp analiz eder.
   - Logların kolayca aranmasını ve raporlanmasını sağlar.
2. **Güvenlik Bilgi ve Olay Yönetimi (SIEM):**
   - Siber saldırıları tespit etmek için kullanılır.
   - Anormal aktiviteleri izleyerek güvenlik tehditlerine karşı uyarılar üretir.
3. **Gerçek Zamanlı İzleme ve Uyarılar:**
   - Sistem performansını sürekli takip eder.
   - Ağ trafiğini, uygulama hatalarını ve sistem durumlarını izleyerek anlık uyarılar oluşturur.
4. **İş Zekası ve Veri Analitiği:**
   - Büyük verileri analiz ederek iş süreçlerini iyileştirmek için kullanılabilir.
   - Kullanıcı davranışlarını analiz ederek stratejik kararlar alınmasını sağlar.
5. **Uygulama ve Altyapı Performans Yönetimi:**
   - Web ve mobil uygulamaların performansını ölçerek hataları tespit eder.
   - Veri merkezleri, bulut ortamları ve sanal makineler üzerindeki işlemleri analiz eder.

Splunk, özellikle büyük ölçekli sistemlerde merkezi log yönetimi ve analiz yapmak isteyen şirketler tarafından tercih edilir. Eğer log analizi veya sistem izleme ile ilgili bir ihtiyacın varsa, Splunk iyi bir seçenek olabilir. Kullanımına dair daha fazla detay istiyor musun?

Videolu Eğitim İçeriği Mağlesef Yok ☹