Bir SIEM Çözümüne Neden İhtiyacım Var?

Kurumların ve kuruluşların SIEM çözümlerinden beklentilerini belirleyen faktörleri analiz etmek gerekmektedir. Kurum ve kuruluşlar tarafından tercih edilen SIEM çözümlerinin uygulama aşamasında neden başarısızlığa doğru gittiğinin sonuçlarını belirlemek önemlidir.

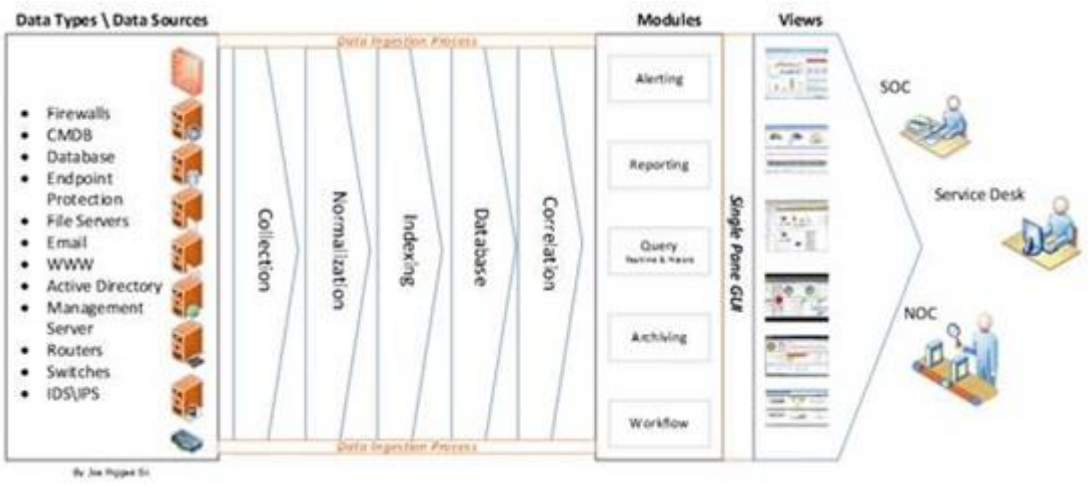
Kurum ve kuruluşların neden SIEM çözümlerini tercih ettikleri ve tercih edilen SIEM çözümünden beklentilerinin başlıca şu şekildedir;

- Uyumluluk süreçleri (HIPAA , SOX, PII, NERC , COBIT 5, FISMA , PCI vb.)
- ISO 27000, ISO 27001, ISO27002 ve ISO 27003 gibi süreçlerin takibi ve devamlılığı
- Log kayıtlarının toplanması ve saklanması
- Log kayıtlarının izlenmesi ve oluşan olaylara yanıt süreleri
- Vaka yönetimlerinin yapılması ve oluşan olaylara ilişkin kayıtların açılması
- Güvenlik politikalarının uygulaması ve uygulanan politikaların ihlalleri

SIEM çözümlerinin 5651 yasasına ilişkin gerekliklere cevap vermesi beklenmektedir. Bununla beraber kurum ve kuruluşların hassas verilerini korumakla kalmayıp aynı zamanda uyumluluk süreçlerinin gereksinimlerini yerine getirmek için SIEM çözümlerini tercih etmektedir.

Başarısız denetimler bilgi ve maddi kayıpların yanında yetişmiş personel kayıpları ve kurumların iş düzenlerinin bozulması gibi sonuçlara yol açabilmektedir.

Başarılı bir şekilde uygulanan SIEM projeleri ile bunların önüne geçilebilmek mümkündür.



SIEM Çözümünden Beklentiler Nelerdir?

SIEM çözümleri tak kullan şeklinde nitelendirdiğimiz bir kavram değildir. SIEM çözümlerinin kurumalara uygulanmasından sonra, uygulanan çözümü gerekli veri kaynakları ile besleyerek ve güvenlik kuralları prosedürlerini sisteme entegre edip uygulayarak beklentileri karşılayabilmektedir.

SIEM çözümleri iş ve süreç odaklı olmalıdır. Önemli olayları fark etmeli ve bununla ilgili süreç yöneticilerine uyarılar göndererek, aksiyon almalarını istemelidir.

ITIL süreçleri göz önüne alındığında başlangıç noktasının başlamak olmadığını SIEM entegrasyonlarını ile başlangıç süreçlerine katkıda bulunarak süreçlerin olgunlaşmasını sağlar.

SIEM projelerinin başarılı olarak sonuçlanması için ihtiyaç duyulan adımlar aşağıdaki gibidir:

- Gereksinimlerin Tespiti, Kapsam Belirleme ve Proje Yönetimi
- Log Kaynaklarının Belirlenmesi
- Kaynaklardan Alınacak Logların Detay ve İçeriğinin Belirlenmesi
- Log Anlamlandırma, Etiketleme ve Seviyelendirme Çalışması
- Gelişmiş Korelasyon Kurallarının Oluşturulması
- Siber Saldırı Simülasyon ve SOME Tatbikat Çalışması
- Gerçek Zamanlı “Security Monitoring Dashboard” Tasarımı

ScopVision Nedir?

ScopVISION, firmaların bilgi sistemlerinde ve bilişim ağlarında, çeşitli sistemlerin ürettiği olay kayıtlarının toplanarak merkezileştirilmesi ve olay araştırmalarında kullanılabilmesi amacıyla tasarlanmıştır. ScopVISION, son kullanıcı bilgisayarlarını, sunucuları, uygulamaları ve veri tabanlarında oluşan olayları izlemek için merkezi bir analiz platformu sağlar. ScopVISION kullanılarak bilgi sistemleri üzerindeki güvenlik riskleri anlık olarak tespit edilir.

ScopVISION’ın, toplanan veri üzerinden çalışan korelasyon yeteneği sayesinde, sürekli yapılması gereken incelemeler otomatikleştirilerek, tanımlanan durumlar oluştuğunda uyarılar üretilir ve ilgili kişiler bilgilendirilir. Bu sayede sistem üzerinde meydana gelebilecek olası olaylar önceden tanımlanarak tespit edilir ve gerekli müdahale yapılmasına olanak sunar.

ScopVision Neden Farklıdır?

- ScopVISION, tasarımında kullanılan Elasticsearch Veri Tabanı sayesinde büyük veri üzerinde hızlı arama ve analiz yapılmasına olanak sağlar.
- ScopVISION, üzerinde toplanan verinin büyüklüğünden bağımsız olarak gerçek zamanlı ve geçmişe dönük korelasyon olanakları sunar.
- ScopVISION, veri kaçaklarının araştırılması için güçlü Adli Analiz yeteneklerine sahiptir.
- ScopVISION, basitliğin ön planda tutulmuş ara yüzü ile kullanıcılarına hızlı ve kolay operasyon imkânı sunar.
- ScopVISION, sunucu ya da bilgisayarda uzaktan ajansız ya da yerel uygulama kurulumu ile çalışabilir.

- ScopVISION, ihtiyaçlara göre kurulum sonrası yeniden ölçeklenebilir, yatayda büyüme yeteneği ile sadece sunucu ekleyerek ihtiyaç duyulan performans seviyelerine çıkartılabilir.
- **Yerli ve Milli ürün** olan ScopVISION'ın operasyonel maliyeti düşüktür. Bilgisayar sistemlerinde günlük log toplama, USB / Yazıcı hareketlerinin takibi ve korelasyon gibi özellikler için birden fazla ürünün kullanılması gerekir. ScopVISION, bu özellikleri tek sistem altında uygun maliyetle sunar.

ScopVision Kullanımı Sonrası Kazanımlar;

- Sistem üzerinde çalışan uygulamaların ağ bağlantılarını takip ederek raporlar ve bu sayede istihbarat yazılımlarının keşfedilmesini kolaylaştırır.
- Sistem üzerinde çalışan uygulamaların dosya hareketlerini takip ederek raporlar ve bu sayede fidye zararlıları gibi uygulamaların keşfedilmesini kolaylaştırır.
- Bilgisayarların USB bağlantıları ve yazıcılar ile ilgili tüm hareketlerini, sistem donanım değişikliklerini ve tüm log kayıtlarını izler.
- Bilgisayar sistemleri içinde bilgi kaçağına yol açabilecek güvenilmeyen programları izler.
- Coğrafi konum desteği sayesinde uygulamaların bağlantı açtığı ülkeleri raporlar.
- Toplanan bilgiler ihtiyaç planlamasının daha iyi yapılmasını ve bu sayede organizasyon ağı içerisindeki bilgi akışının görünür hale gelmesini sağlar.