LOG YÖNETİMİ

Log yönetimi; sunucular, güvenlik duvarları ve diğer BT ekipmanları dahil olmak üzere şirketinizin sistemlerinde ve ağlarında meydana gelen tüm olayları ayrıntılandıran dosyalardır. Günümüzde güvenlik noktasında önemi artan konuların başında gelmektedir. Log Yönetimi hem yasal zorunluluklar nedeni ile hem de uluslar arası standartlar tarafından (ISO 27001) önerilmektedir. Eğerki log yönetimi yapabiliyorsak örnek olarak aşağıdaki sorulara cevap verebilme durumumuz vardır.

Belirli zaman aralıklarında kimler oturum açtı?

Sistem yöneticileri takip ediliyor mu?

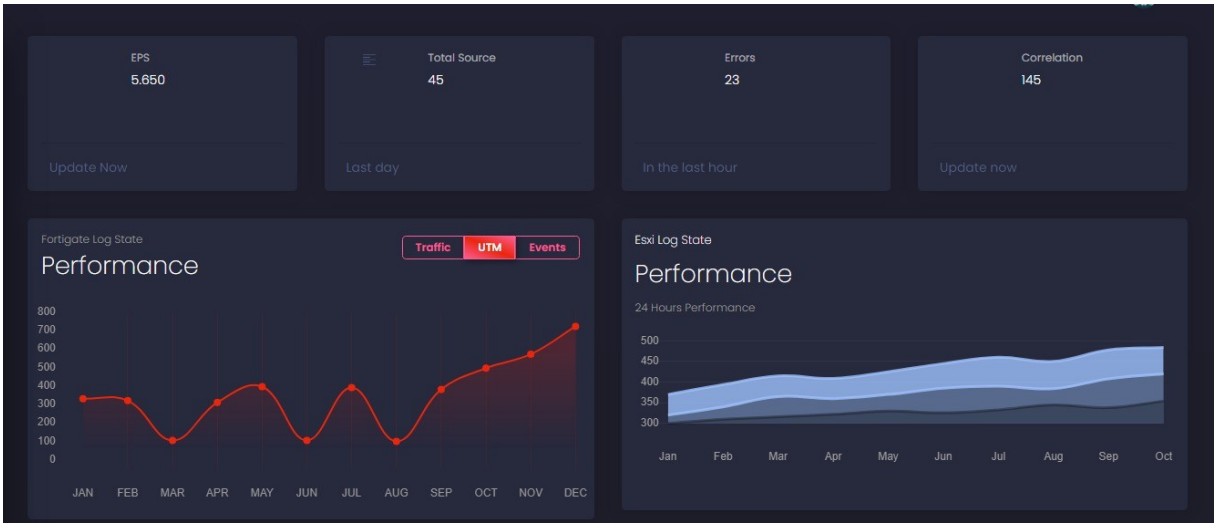
Bilgisayar adı (hostname), IP adresi, MAC adresi değişikliği oldu mu?

Kimler hangi IP adresini aldı?

Kimler hangi saatle VPN bağlantısı kurdu?

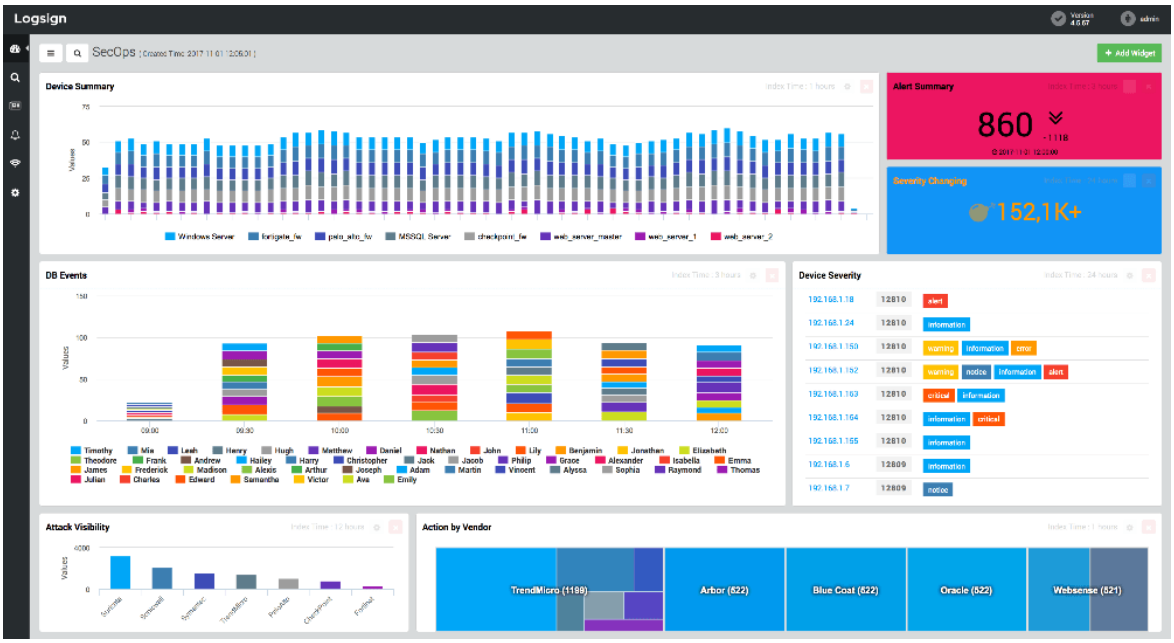
P2P program kullanan var mı?

Domain admin hesabına kullanıcı eklendi mi? Vb.



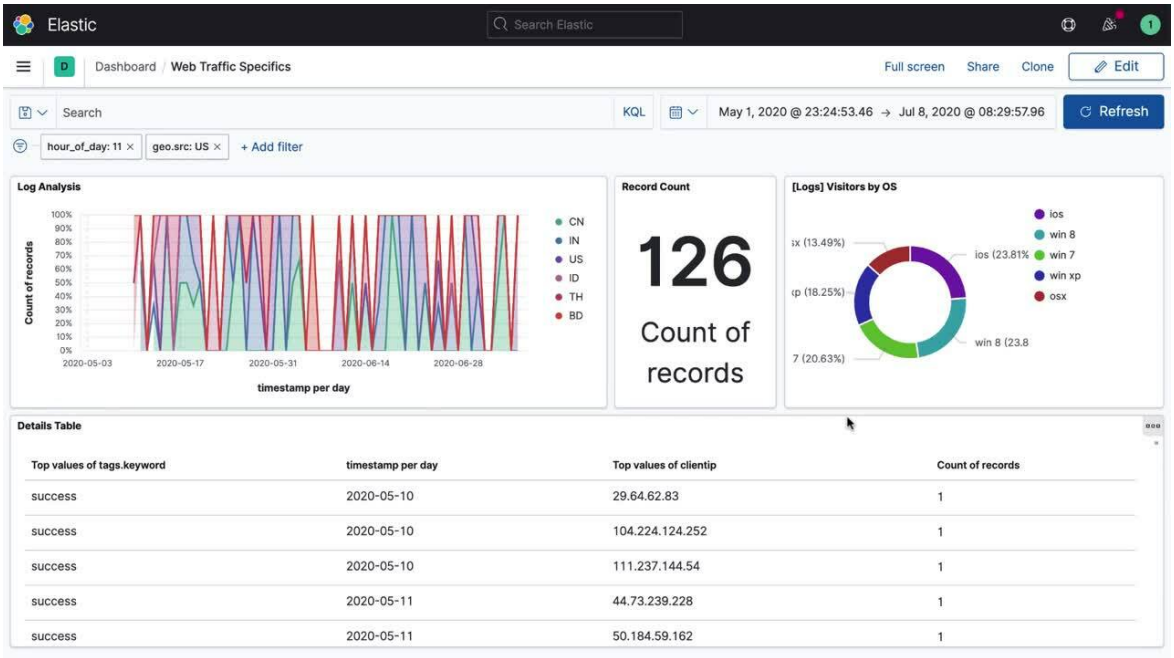
LOGSIGN

Belirlenen bir network üzerinde raporlamayı arzu ettiğiniz faaliyetlere ait logların yönetilebildiği ileri seviye SIEM güvenlik çözümüdür.



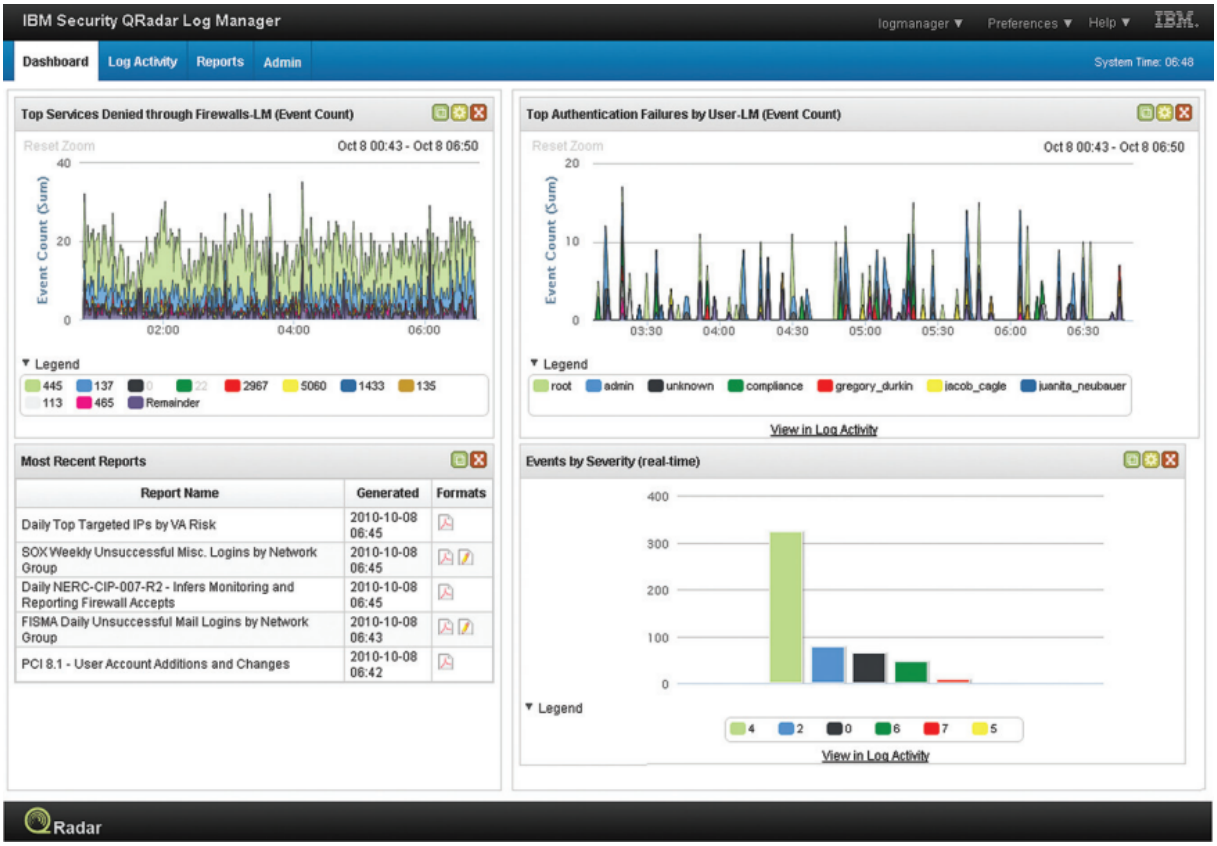
ELK

ELK (ElasticSearch, LogStash, Kibana) açık kaynak kodlu 3 ürünün bir araya gelerek oluşturduğu bir koleksiyondur. ELK büyük veriler içerisinde arama, analiz ve görselleştirme işlemleri gerçekleştirmek için kullanılır.



IBM QRADAR

IBM QRadar Log Manager, QRadar Sense Analytics motorunu kullanarak kuruluşların kendilerini tehditlere, saldırılara ve güvenlik ihlallerine karşı korumasına yardımcı olmak için Ağ güvenliği log olaylarını toplar, analiz eder, depolar ve bunlarla ilgili raporlama yapar. Sense Analytics, aygıtlardaki, sunuculardaki, işletim sistemlerindeki, uygulamalardaki, uç noktalardaki işlenmemiş olayları, eyleme dönüştürülebilir istihbarat verilerine dönüştürür.



ZARARLI YAZILIM

Zararlı yazılım, kullanıcıların programlanabilme özelliğine sahip cihazlarına, web sitelerine veya ağlarına zarar veren veya yetkisiz erişim sağlayan herhangi bir yazılımdır. Siber suçlular genellikle bunu, mali kazanç içi kurbanlardan veri elde ederek baskı yapmak üzere kullanır. 9 adet türü vardır;

Virüs: Bulaştığı bilgisayarda dosyaları silme, sabit diski boşaltma ve verileri bozma gibi kötü amaçlı faaliyetler gerçekleştiren programlardır.

Solucan (Worm): Kendini bir ağda çoğaltmak ve diğer bilgisayarlara yaymak için tasarlanmış bir tür kötü amaçlı yazılımdır.

Truva Atı (Trojan): Meşru bir program kılığına girmiş ancak yüklendikten sonra kötü amaçlı etkinlik gerçekleştiren zararlı yazılım çeşididir.

Casus Yazılım (Spyware): Virüs bulaşmış bilgisayardan bilgi çalan ve bunları uzak bir konumdaki kötü amaçlı kişilere gönderen yazılımlardır.

Keylogger: Klavyede yaptığınız her tıklamayı izleyen, kaydeden ve kötü amaçlı kişilere gönderen bir tür casus yazılımdır.

Fidye Yazılımı (Ransomware): Bilgisayarınızdaki dosyaları şifreleyerek erişilemez hale getiren bir kötü amaçlı yazılımdır.

Reklam Yazılımı (Adware): İnternete bağlandığında reklamları görüntülemek için kullanıcının izni olmadan yüklenen yazılımlardır.

Tarayıcı Korsanları: Sayfaların içeriğini değiştirmek, sizi başka konumlara yönlendirmek veya diğer kötü amaçlı işlemleri gerçekleştirmek için tarayıcınızın davranışını değiştiren bir kötü amaçlı yazılım türüdür.

Rootkit: Virüs bulaşmış bir cihaza yönetim erişimi sağlayan ve onu farklı cihaz ve yazılımlara zarar vermek için kullanan kötü amaçlı yazılımdır.

ANOMALY DETECTION

Anomaly Detection, en basit anlamıyla bir veride beklenmedik durumların veya kalıpların bulunmasını sağlayan bir tekniktir. Bu beklenmedik durumlara literatürde outliers (aykırı değerler), exceptions (istisnai durumlar) veya anomaliler denilmektedir. Anomali tespiti, izinsiz giriş tespiti, dolandırıcılık tespiti, arıza tespiti, sistem sağlığının izlenmesi, sensör ağlarında olay tespiti, ekosistem bozukluklarının tespiti ve makine görüsü kullanarak görüntülerde kusur tespiti gibi çeşitli alanlarda uygulanabilmektedir. 3 adet tipi bulunmaktadır;

Point Anomalies: Bireysel bir veri örneği eğer diğer normal verilerden uzaktaysa bu bir anomali veridir. Burada bu anomali tespitine point Anomali denmesinin sebebi anomali tespitinin belli bir niteliğe (attribute) bağlı olmasıdır.

Contextual Anomalies: Belirli bir verimiz bazı durumlarda anomaliye işaret ederken diğer durumlarda normal bir veriye işaret ediyorsa, yani özel bir bağlamda(specific context) anomali davranış sergiliyorsa bu context anomaliye bir örnektir.

Collective Anomalies: Birbiriyle ilişkili olan veriler tüm verisetinde anomali davranış oluşturuyorsa bu bir collective anomaliye örnektir. Burada ilişkili olan bazı veriler bir araya geldiğinde anomali oluşturabilirken, bu veriler bireysel olarak verisetinde anomali davranış göstermiyor olabilir.

Anomali Tespiti için teknikler ise;

Makine Öğrenmesi Temelli Anomali Tespiti
K-Nearest Neighbour ve Density Based Algoritmaları
Kümeleme Tabanlı Algoritmalar
İstatiksel Metodlarla Anomali Tespiti
şeklindedir.