IBM Security QRadar SIEM

Entegre bir araştırmacı raporlama sistemi ile tehdit korumasını ve uygunluğunu güçlendirir

Önemli özellikler

- Günlük yönetimi ve ağ tehdidi koruma teknolojilerini ortak bir veritabanı ve paylaşımlı pano kullanıcı arabirimi ile entegre etme
- Binlerce güvenlik olayını, şüpheli saldırıların yönetilebilir bir listesine indirgeme
- Kötü amaçlı etkinliği algılayıp uzun süreler boyunca izleyerek, diğer güvenlik çözümlerinin genellikle kaçırdığı gelişmiş tehditlerin ortaya çıkarılmasına yardımcı olma
- Gelişmiş yetenekler ile içerideki sahteciliği algılama
- Düzenleme zorunluluklarının ve destek uyumluluğunun aşılmasına yardımcı olma.

Günümüzde ağlar hiç olmadıkları kadar büyük ve karmaşıktır. Bunları kötü amaçlı etkinliklere karşı korumak ise bitmek bilmeyen bir görevdir. Fikri mülkiyetlerini güvence altına almak, müşterilerinin kimliklerini korumak ve iş aksamalarını önlemek isteyen kurumların, günlükleri ve ağ akış verilerini izlemekten fazlasını yapmaları gereklidir; bu etkinlikleri kullanılabilir bir şekilde algılamak için gelişmiş araçlar kullanmaları gerekir. IBM® Security QRadar bilgi güvenliği ve olay yönetimi (SIEM), yılların verdiği bağlamsal kavrayışları kullanarak, kullanılabilir ağ verilerini toplamak, normalleştirmek ve ilişkilendirmek için küçük veya büyük bir kurumun güvenlik operasyon merkezinde bir bağlayıcı çözüm işlevi görebilir. Sonuç olarak ortaya *güvenlik zekası* çıkar.

Bu ürünün temelinde, gerçek zamanlı günlük olayını ve ağ akış verilerini yakalayarak olası saldırganların izini ortaya çıkarmak üzere tasarlanmış yüksek düzeyde ölçeklendirilebilir bir veritabanı bulunmaktadır. QRadar SIEM, her etkinliği kendi ham biçiminde depolayarak ve ardından gerçek tehditleri yanlış algılamalardan ayırt etmeye yardımcı anında bağıntı etkinlikleri gerçekleştirerek, bir ağda dağıtılmış binlerce aygıttaki günlük kaynağı olay verilerini birleştiren kurumsal bir çözümdür. Ayrıca, gerçek zamanlı Katman 4 ağ akış verilerini ve daha da benzersiz olarak Katman 7 uygulama yüklerini derin paket inceleme teknolojisini kullanarak yakalar.

Tüm QRadar ailesi bileşenlerinde paylaşılan sezgisel bir kullanıcı arabirimi, BT personelinin ağ saldırılarını önem derecesine göre hızlı bir şekilde tanımlayıp gidermesine yardımcı olur ve binlerce uyarı ve anormal etkinlik düzenini sıralar ve daha fazla inceleme sağlayacak şekilde *saldırı* sayısını büyük ölçüde azaltır.

Tehdit algılama ve öncelik sırasına koyma için gerçek zamanlı görünürlük sağlama

QRadar SIEM, bütün BT altyapısında bağlamsal ve eyleme geçirilebilir gözetim sağlayarak, genellikle diğer güvenlik çözümlerinin kaçırdığı tehditlerin algılanması ve giderilmesi için kurumlara yardımcı olur. Bu tehditler, uygulamaların uygunsuz kullanımını, içerideki sahteciliği ve milyonlarca etkinliğin 'gürültüsü' içinde kolayca kaybolan gelişmiş 'düşük ve yavaş' tehditleri içerebilir.

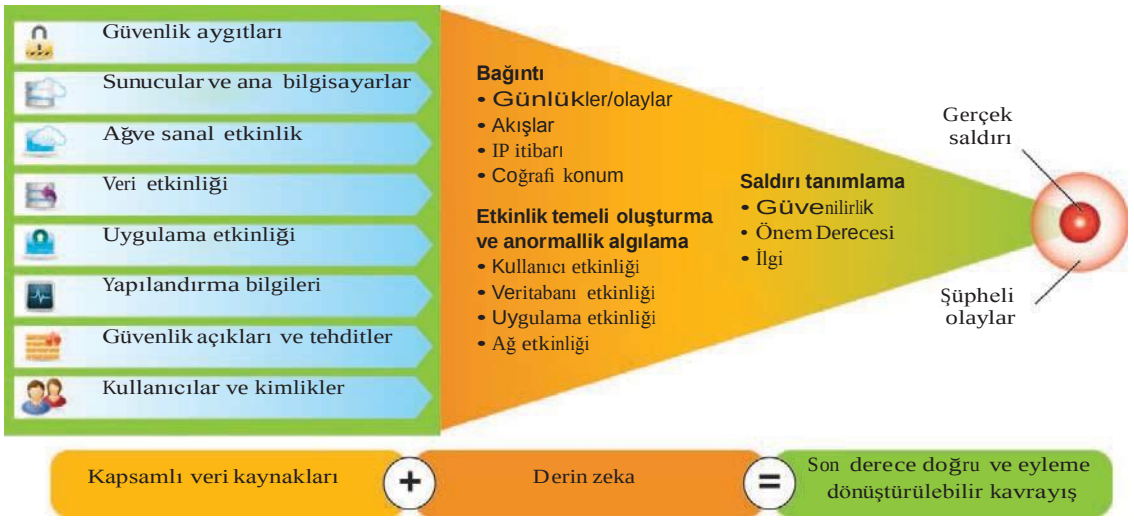
QRadar SIEM şunları içeren bilgileri toplar:

- **Güvenlik olayları:** Güvenlik duvarları, sanal özel ağlar (VPN'ler), saldırı algılama sistemleri, saldırı önleme sistemleri ve daha fazlasındaki olaylar
- **Ağ olayları:** Anahtarlar, yönlendiriciler, sunucular ve daha fazlasındaki olaylar
- **Ağ etkinlik bağlamı:** Ağ ve uygulama trafiğindeki Katman 7 uygulama bağlamı
- **Kullanıcı veya varlık bağlamı:** Kimlik ve erişim yönetimi ürünlerinde ve güvenlik açığı tarayıcılarındaki bağlamsal veriler
- **İşletim sistemi bilgileri:** Ağ varlıkları için satıcı adı ve sürüm numarası özellikleri
- **Uygulama günlükleri:** Kurumsal kaynak planlama (ERP), iş akışı, uygulama veritabanları, yönetim platformları ve daha fazlası.

İncelemeleri eyleme geçirilebilir saldırılara odaklamak için uyarıları azaltma ve öncelik sırasına koyma

Çoğu kurum her gün milyonlarca, hatta milyarlarca olay yaratmaktadır ve bu olay verilerini kısa bir öncelikli saldırılar listesine indirmek oldukça zor olabilir. QRadar SIEM, ağdaki geçerli ana bilgisayarları ve sunucuları (varlıkları) bulmak ve sınıflandırmak için çoğu ağ günlüğü kaynak aygıtlarını otomatik olarak keşfeder, ağ akış verilerini inceler ve uygulamaları, iletişim kurallarını, hizmetleri ve kullandıkları bağlantı noktalarını izler. Bu verileri toplar, depolar ve analiz edip tehdit algılama ve uyumluluk raporlama ve denetlemede kullanmak için gerçek zamanlı olay bağıntısı gerçekleştirir. Milyarlarca olay ve akış bu sayede azaltılır ve iş etkilerine göre az sayıda gerçekleştirilebilir saldırı kalacak şekilde öncelik sırasına konulabilir.

Sonuç olarak, güvenlik profesyonelleri haftalar yerine sadece günler içinde QRadar SIEM kurulumundan değer görmeye başlayabilir; dağıtımlar ise pahalı danışmanlar olmadan gerçekleşebilir. Otomatik keşif özellikleri, yeni şablonları ve filtreleri sayesinde, daha geniş BT operasyonel araçlarıyla olduğu gibi, sisteme ortamınızı öğretmek için aylar harcamazsınız. Mimari, hepsi donanım tabanlı, yalnızca yazılım veya sanal yazılım gereci olarak kullanılabilir olan olay işlemcisi gereçleri, olay toplama gereçleri ve akış işlemcisi gereçlerinin çoklu modellerini kullanmaktadır. Daha küçük kurulumlar, tek bir hepsi bir arada çözümle başlayıp olay ve akış işlemcisi gereçlerini gereken şekilde ekleyerek kolayca konsol dağıtımlarına yükseltilebilir.



QRadar SIEM, önceki ve müşteri tanımlı kuralları kullanıp yönetilebilir bir saldırılar listesine indirgeyerek, çeşitli kaynaklardaki verileri yakalar.

Daha etkili tehdit yönetimi için temel sorulara cevap verme

Güvenlik ekiplerinizin, potansiyel tehditlerini tamamen anlaması için temel soruları yanıtlaması gerekir: Kim saldırıyor? Saldırıya uğrayan ne? İşe olan etkisi ne? Nerede inceleme yapayım? QRadar SIEM önemli olayları ve tehditleri izleyerek, destek verisinin ve ilgili bilgilerin bir geçmişini oluşturur. Saldırı hedefleri, zaman noktası, varlık değeri, güvenlik açığı durumu, saldırıda bulunan kullanıcıların kimlikleri, saldırgan profilleri, etkin tehditler ve önceki saldırıların kayıtları gibi ayrıntıların tümü, güvenlik ekiplerine gerçekleştirmeleri gereken zekayı sağlar.

Analiz ve adli olaylar için olay ve akış verilerinin gerçek zamanlı, konum tabanlı ve geçmişe yönelik aramasını yapmak, etkinlik değerlendirme ve olay çözümleme becerisini büyük ölçüde arttırabilir. Kullanımı kolay panolar, zaman serili görünümler, ayrıntılı arama, paket düzeyinde içerik görünürlüğü ve binlerce ön tanımlı arama ile birlikte kullanıcılar anormallikleri ve en üst seviyedeki etkinlik katılımcılarını özetlemek ve tanımlamak için verileri hızlı bir şekilde toplayabilir. Ayrıca, geniş, coğrafi olarak dağıtılmış ortamlarda birleşik arama gerçekleştirebilirler.

Uygulama görünürlüğü elde etme ve anormallik algılama

QRadar SIEM, uygulamaları, sunucuları ve ağ alanlarını etkileyen davranış değişikliklerini belirlemek için çeşitli anormallik algılama yeteneklerini destekler. Örneğin QRadar SIEM, bir uygulamanın veya bulut tabanlı hizmetin kapalı zamanlarını veya yoğun kullanımını veya geçmiş, hareketli ortalama profilleri ve dönemlik kullanım düzenleriyle tutarlı olmayan ağ etkinlik düzenlerini algılayabilir. QRadar SIEM, bu günlük ve haftalık kullanım profillerinin fark edilmesini öğrenerek, BT personelinin anlamlı sapmaları hızlı bir şekilde tanımlamasına yardımcı olur.

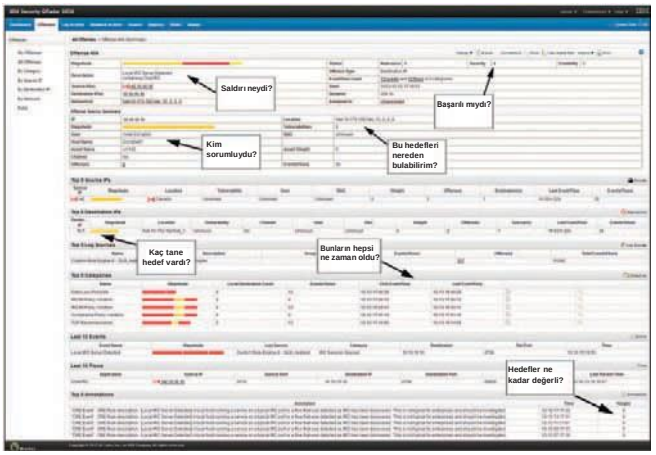
QRadar SIEM merkezi veritabanı ise günlük kaynağı olaylarını ve ağ akış trafiğini birlikte depolayarak, aynı IP kaynağından yayılan çift yönlü ağ akışı etkinliği ile ayrı etkinliklerin ilişkilendirilmesine yardımcı olur. Ayrıca, depolama tüketimini azaltmaya ve lisans gereksinimlerini korumaya yardımcı olmak için, ağ akışı trafiğini ve kayıt operasyonlarını çok kısa sürede tek bir veritabanı girişi olarak gruplandırabilir.

Uygulama trafiğini Katman 7'de algıma becerisi ile QRadar SIEM, bir kurumun ağ ilkesi, tehdit ve genel ağ etkinliği izlemesine doğru analiz ve görüş sağlamasına olanak tanır. Bir IBM Security QRadar QFlow veya VFlow Collector gerecinin eklenmesiyle QRadar SIEM, ağ dahilindeki ERP, veritabanları, Skype, IP üzerinden ses (VoIP) ve sosyal medya uygulamalarının kullanımını izleyebilir. Bu, kimin neyi kullandığı, içerik aktarımı için analiz ve uyarılara ilişkin kavrayışı ve uygun olmayan veri transferleri ile aşırı kullanım düzenlerini ortaya çıkarmak için diğer ağ ve günlük etkinliği ile ilişkilendirmeyi içerir. QRadar SIEM çok sayıda anormallik ve davranışsal algılama kurallarıyla birlikte gelirken, güvenlik ekipleri de, zaman serileri verilerine karşı anormallik algılama sağlayan filtreleme yeteneği üzerinden kendi kurallarını oluşturabilirler.

Son derece sezgisel bir tek konsollu güvenlik çözümünü yönetme

QRadar SIEM, işleve göre rol tabanlı erişim ve gerçek zamanlı analize, olay yönetimine ve raporlamaya erişim için küresel görünüm sunan merkezi bir kullanıcı arabirimi sağlayarak, bir kurumun güvenlik operasyonları için sağlam bir temel sunar. Güvenlik, ağ etkinliği, uygulama etkinliği, sistem izleme ve uyumluluk dahil olmak üzere beş adet varsayılan gösterge panosu vardır ve kullanıcılar kendi çalışma alanlarını oluşturup özelleştirebilmektedirler.

Bu panolar, bir saldırının başlangıcını gösterebilen uyarı etkinliğindeki ani değişikliklerin algılanmasını kolaylaştırır. Bir grafik tıklatıldığında, güvenlik ekiplerinin vurgulanan etkinlikleri veya şüpheli bir saldırıyla ilgili ağ akışlarını hızla araştırmasını sağlayan bir ayrıntılandırma yeteneğini başlatılır. Ayrıca, belirli roller, aygıtlar, uyumluluk düzenlemeleri ve dikey endüstriler ile ilgili binlerce şablon sayesinde, rapor oluşturma işlemi hızlanır.



QRadar SIEM, her şüpheli saldırının arkasında büyük miktarda adli ayrıntının yanı sıra, var olan kuralları ayarlamak veya yanlış algılamaları azaltmak için yenilerini ekleme becerisi de sunmaktadır.

Tehdit korumasını sanal ortamlara genişletme

Sanal sunucularda güvenlik açıkları açısından fiziksel sunucular kadar şüpheli olduğu için, sanal veri merkezinde bulunan uygulamaların ve verilerin korunması için kapsamlı güvenlik zekası çözümleri uygun önlemleri de içermelidir.

BT profesyonelleri QRadar VFlow Collector gereçlerini kullanarak sanal ağlarındaki büyük miktardaki iş uygulama etkinlikleri için artırılmış görünürlük elde eder ve güvenlik izleme, uygulama katmanı davranışı analizi ve anormallik algılama için bu uygulamaları daha iyi tanımlayabilirler. Operatörler, daha derin güvenlik ve adli ilkeler için uygulama içeriğini de yakalayabilir.

Uyumluluğu yönetmek için ayrıntılı veri erişimi ve kullanıcı etkinliği raporları oluşturma

QRadar SIEM, bir kurumun yasal zorunlulukları karşılama ve uyumluluğu rapor etmedeki başarısı için önemli olan şeffaflık, güvenilirlik ve ölçülebilirlik öğelerini sağlar. Çözümün gözetim beslemelerini ilişkilendirme ve entegre etme becerisi, denetçiler için BT riskleri üzerine daha fazla tam metrik raporlamasını sağlamanın yanında, endüstri uyumluluk gereksinimlerinin karşılanmasına yönelik binlerce rapor ve kural şablonu da sağlar.

Kurumlar, otomatik güncellemeler üzerinden yeni tanımları, düzenlemeleri ve en iyi uygulamaları eklemek için QRadar SIEM'in genişletilebilirliği ile uyumluluk odaklı BT güvenliği gereksinimlerine etkili olarak yanıt verebilir. Ayrıca, tüm ağ varlıklarının profilleri iş fonksiyonuna göre gruplandırılabilir – örneğin, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) uyumluluk denetimlerine tabi olan sunucular.

Çözümün önceden oluşturulmuş gösterge panoları, raporları ve kural şablonları şu düzenlemeler ve kontrol çerçeveleri için tasarlanmıştır: CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG ve daha fazlası.

Yüksek kullanılabilirlik ve olağanüstü durum kurtarma yetenekleri ekleme

Yüksek kullanılabilirlik ve olağanüstü durum kurtarma yetenekleri gerçekleştirmek için, QRadar cihaz ailesinin tüm üyeleri ile benzer ikinci sistemler eşlenebilir. Olay işlemcisi cihazlarından, akış işlemcisi cihazlarına ve hepsi bir arada ve konsol SIEM cihazlarına kadar, kullanıcılar gereken yer ve zamanda güç ve koruma ekleyerek sürekli operasyonu sağlayabilir.

İş dayanıklılığı arayan kurumlar için QRadar yüksek kullanılabilirlik çözümleri, sistemler arasında entegre otomatik yük devretme ve tam disk senkronizasyonu sunar. Bu çözümler mimari olarak şık bir şekilde tak ve çalıştır cihaz üzerinden kolayca dağıtılabilir ve başka herhangi bir üçüncü taraf arıza yönetimi ürününe gerek kalmaz.

Veri koruması ve kurtarması arayan kurumlar için QRadar olağanüstü durum kurtarma çözümleri, canlı verileri (örn. akışlar ve olaylar), birinci bir QRadar sisteminde ayrı bir tesiste bulunan ikincil bir paralel sisteme iletir.

Güvenlik açıkları için profil oluşturma

IBM Security QRadar Risk Manager, ağın en savunmasız varlıklarını tanımlayarak QRadar SIEM'i tamamlar. Bu sistemler potansiyel olarak tehdit oluşturacak etkinliklerle katıldıklarına hemen uyarı oluştururlar. Örneğin, kurumlar yamalanmamış uygulamalar, aygıtlar ve sistemler için ağlarını tarayabilir, hangilerinin Internet'e bağlı olduğunu belirleyebilir ve her bir uygulamanın düzeltilmesini risk profiline göre özelleştirir. Daha fazla bilgi için lütfen bkz.QRadar Risk Manager veri sayfası.

Ağ olaylarını ve akışlarını yakalamak için kapsamlı aygıt desteği alma

Kurumsal ağlarda dağıtılan önde gelen satıcıların 450'den fazla ürünü için destek ile birlikte QRadar SIEM ağ çözümler güvenlik çözümleri, sunucular, ana bilgisayarlar, işletim sistemleri ve uygulamalar dahil olmak üzere geniş bir sistem yelpazesinde toplama, analiz ve ilişkilendirme sağlar. Ayrıca, QRadar SIEM, IBM ve diğer pek çok satıcının özel uygulamaları ve yeni sistemleri desteklemek için kolayca genişletilebilir.

Neden IBM?

IBM, dünyanın en geniş güvenlik araştırma, geliştirme ve sağlama kurumlarından birini işletmektedir. IBM çözümleri güvenlik açıklarını azaltmaları ve stratejik girişimlerinin başarısına daha fazla odaklanmaları için kurumları güçlendirir.

Ek bilgi için

IBM Security QRadar SIEM'in kurumunuzun tehdit yönetimini ve uyumluluk zorluklarını nasıl çözebileceği hakkında daha fazla bilgi almak için IBM temsilciniz veya IBM İş Ortağınız ile iletişime geçin veya şu adresi ziyaret edin: **ibm.com**/security.

IBM Security çözümleri hakkında

IBM Security, kurumsal güvenlik ürünleri ve hizmetleri için en gelişmiş ve entegre portföylerden birini sunar. Dünyaca ünlü IBM X-Force araştırma ve geliştirme tarafından desteklenen portföy, kimlik ve erişim yönetimi, veritabanı güvenliği, uygulama geliştirme, risk yönetimi, uç nokta yönetimi, ağ güvenliği ve daha fazlası için çözümler sunarak, kurumların çalışanlarını, altyapılarını, verilerini ve uygulamalarını bir bütün olarak korumalarına yardımcı olmak için güvenlik zekası sağlamaktadır. Bu çözümler, kurumların etkili olarak risk yönetimi gerçekleştirmelerini ve mobil, bulut, sosyal medya ve diğer kurumsal iş mimarileri için entegre güvenlik uygulamalarını sağlar. IBM, dünyanın en geniş güvenlik araştırma, geliştirme ve sağlama kurumlarını işletmektedir ve 130'dan fazla ülkede günlük 13 milyar güvenlik olayını izlemenin yanında ve 3.000'den fazla güvenlik patentine sahiptir.

IBM Global Financing (IGF) ayrıca işletmenizin gerek duyduğu yazılım ürünlerini mümkün olduğunca uygun maliyetli ve stratejik yollardan elde etmenize yardımcı olur. Krediye uygun müşterilerimizle birlikte çalışarak işletme ve gelişim hedeflerine uyan, verimli maliyet yönetimi sağlayan ve toplam sahip olma maliyetini (TCO) düşüren finans çözümleri geliştiriyoruz. IGF ile önemli BT yatırımlarınız için kaynak yaratın ve işletmenizi daha da ileri taşıyın. Daha fazla bilgi için **ibm.com**/financing/uk/ adresini ziyaret edin.

www.platinbilisim.com.tr.

IBM Türk Limited Şirketi
Büyükdere Caddesi
Yapı Kredi Plaza
B Blok
Levent
İstanbul 34330
Türkiye

IBM ana sayfasına **ibm.com**/tr adresinden erişebilirsiniz

Lütfen geri dönüşüme tabi tutun