IBM Security QRadar Risk Manager
Sürüm 7.2.4

Başlangıç Kılavuzu

Not

Bu belgeyi ve desteklediği ürünü kullanmadan önce şu bilgileri okuyun: “Bildirimler” sayfa 31.

Ürün bilgileri

Bu belge, bu belgenin güncellenmiş sürümü geçersiz kılmadığı sürece, IBM QRadar Security Intelligence Platform V7.2.4 ve sonraki yayın düzeyleri için geçerlidir.

İçindekiler

IBM Security QRadar Risk Manager ürününe giriş

Bu bilgiler, IBM® Security QRadar Risk Manager ile kullanılmak üzere tasarlanmıştır. QRadar Risk Manager, aygıt yapılandırmalarını izlemek, ağ ortamınızdaki değişikliklerin simülasyonunu yapmak ve ağınızdaki riskleri ve güvenlik açıklarını önceliklendirmek için kullanılan bir araçtır.

Hedef kitle

Bu kılavuz, QRadar Risk Manager sistemlerinin ağınıza kurulmasından ve yapılandırılmasından sorumlu olan ağ yöneticileri için tasarlanmıştır.

Teknik belgeler

Tüm çevrilmiş belgeler de dahil, web'deki IBM Security QRadar ürün belgelerini bulmak için http://www.ibm.com/support/knowledgecenter/SS42VS/welcome adresindeki IBM Knowledge Center olanağına erişin.

QRadar ürün kitaplığındaki daha fazla teknik belgelere nasıl erişileceğine ilişkin bilgi için www.ibm.com/support/docview.wss?rs=0&uid=swg21614644 adresindeki Accessing IBM Security Documentation Technical Note başlıklı belgeye bakın.

Müşteri desteği ile iletişim kurma

Müşteri desteği ile iletişim kurma hakkında bilgi için http://www.ibm.com/support/docview.wss?uid=swg21616144 adresindeki Support and Download Technical Note başlıklı belgeye bakın.

İyi güvenlik uygulamaları bildirimi

BT sistemi güvenliği, şirketiniz içinde ve dışında uygunsuz erişimi önleme, algılama ve bu erişime yanıt verme yoluyla sistemlerin ve bilgilerin korunmasını kapsar. Uygunsuz erişim, bilgilerin değiştirilmesi, yok edilmesi, uygunsuz ya da yanlış kullanımıyla sonuçlanabilir veya başkalarına saldırılarda kullanım da dahil, sistemlerinizin hasar görmesi ya da yanlış kullanılmasıyla sonuçlanabilir. Hiçbir BT sistemi ya da ürünü tamamen güvenli olarak değerlendirilmemelidir ve uygunsuz kullanım veya erişimin önlenmesinde tek bir ürün, hizmet ya da güvenlik önlemi tamamen etkili olamaz. IBM sistemleri, ürünleri ve hizmetleri, mutlaka ek işletim yordamlarını içerecek, kapsamlı bir yasal güvenlik yaklaşımının parçası olacak şekilde tasarlanmıştır ve en üst düzeyde etkili olabilmesi için başka sistemleri, ürünleri ya da hizmetleri gerektirebilir. IBM, HERHANGİ BİR SİSTEM, ÜRÜN YA DA HİZMETİN, HERHANGİ BİR TARAFIN ZARARLI YA DA YASA DIŞI EYLEMİNDEN MUAF DEĞİLDİR VEYA ŞİRKETİNİZİ BU TÜR ZARARLI YA DA YASA DIŞI EYLEMLERE KARŞI MUAF TUTMAZ.

Lütfen Dikkat:

Bu Programın kullanımı, çeşitli yasa ya da düzenlemelere tabi olabilir. Gizlilik, veri koruması, istihdam ve elektronik iletişim ve depolama ile ilgili olanlar da bunlara dahildir. IBM Security QRadar yalnızca yasal amaçlarla ve yasal şekilde kullanılabilir. Müşteri, bu Programın geçerli yasalar, düzenlemeler ve ilkelere uygun olduğunu kabul eder ve bunlara karşı tüm sorumluluğu üstlenir. Lisans sahipleri, IBM Security QRadar ürününün yasal kullanımını sağlamak için gerekli izinleri, onayları ya da lisansları alacağını veya aldığını beyan eder.

Bölüm 1. IBM Security QRadar Risk Manager ürününü kullanmaya başlama

IBM Security QRadar Risk Manager ayrı kurulan bir araçtır. Aygıt yapılandırmalarını izlemek, ağ ortamınızdaki değişiklikleri simüle etmek ve ağınızdaki riskleri ve güvenlik açıklarını önceliklendirmek için QRadar Risk Monitor uygulamasını kullanın.

QRadar Risk Manager uygulamasına, IBM Security QRadar SIEM konsolundaki **Risks** (Riskler) sekmesinden erişilir.

QRadar Risk Manager, sistem yöneticisine aşağıdaki görevleri tamamlaması için araçlar sağlayarak QRadar SIEM olanağını geliştirir:

- Risk yönetimini merkezileştirme.
- Ağınızı görüntülemek için bir topoloji kullanma.
- Ağ aygıtlarını yapılandırma ve izleme.
- Ağ aygıtları arasındaki bağlantıları görüntüleme.
- Güvenlik duvarı kuralları arama.
- Tetiklenen kurallar için olay sayısını ve var olan kuralları görüntüleme.
- Ağ aygıtlarınız için aygıtları ve yolları arama.
- Uyumluluğu sağlamak için ağınızı izleme ve denetleme.
- Ağınızda açıklardan yararlanma simülasyonları tanımlama, zamanlama ve çalıştırma.
- Güvenlik açıklarını arama.

Bilgi zekasını artırmak için merkezi risk yönetimi ve uyumluluk birçok dahili ekibin işbirliğini gerektirebilir. Ek Risk Yönetimi aracı içeren yeni nesil bir SIEM olarak, birinci nesil SIEM ürünlerinde gerekli olan adım sayısını azalttık. QRadar SIEM'de yönetilen varlıklar için ağ topolojisi ve risk değerlendirmesi sağlarız.

Değerlendirme sürecinde, sisteminizi, güvenliğinizi, risk analizinizi ve ağ bilgilerini toplama ve ilintilendirme yoluyla birleştirerek ağ ortamınıza yönelik tam görünürlük sağlarsınız. Ortamınıza yönelik, el ile işlemleri ve diğer özel amaçlı ürün teknolojilerini kullanarak elde edemeyeceğiniz görünürlük ve verimlilik sağlayan bir portal da tanımlarsınız.

Bölüm 2. IBM Security QRadar Risk Manager ürününü devreye alma

QRadar Risk Manager aracınız, en son QRadar Risk Manager yazılımıyla birlikte kurulur.

IBM Security QRadar Risk Manager değerlendirme aracını kurmalısınız. Yazılım için etkinleştirme gerekir ve QRadar Risk Manager aracına bir IP adresi atamanız gerekir.

Yazılımınızı etkinleştirme ve bir IP adresi atama konusunda yardıma gereksinim duyarsanız müşteri desteği ile iletişim kurun.

Araç, ağ aygıtlarınızdan bilgileri kabul etmeye hazırdır.

IBM Security QRadar Risk Manager ürününü kullanma hakkında bilgi için bkz. *IBM Security QRadar Risk Manager Kullanıcı Kılavuzu*.

QRadar Risk Manager ürününü ortamınızda devreye almak için aşağıdakileri yapmalısınız:

1. En son IBM Security QRadar SIEM sürümünün kurulu olduğundan emin olun.
2. Tüm ön kurulum gereksinimlerinin karşılandığından emin olun.
3. QRadar Risk Manager aracınızı ayarlayın ve açın.
4. QRadar SIEM konsolunuza QRadar Risk Manager eklentisini kurun.
5. QRadar SIEM ile QRadar Risk Manager aracı arasında iletişim kurun.
6. QRadar Risk Manager kullanıcılarınız için kullanıcı rollerini tanımlayın.

Ürünü kurmadan önce

IBM Security QRadar Risk Manager ürününü kurmadan önce IBM Security QRadar SIEM konsolu için kuruluş işlemini tamamlamanız gerekir. En iyi uygulama olarak, QRadar SIEM ve QRadar Risk Manager ürününü aynı ağ anahtarına kurun.

Aşağıdaki bilgileri gözden geçirmeniz gerekir:

- Güvenlik duvarı kapısı erişimini yapılandırma
- Ağ ayarlarını tanımlama
- QRadar Risk Manager ürünündeki desteklenmeyen özellikler
- Desteklenen web tarayıcıları

IBM Security QRadar Risk Manager değerlendirme aracını kurmadan önce aşağıdakilere sahip olduğunuzdan emin olun:

- iki birimli araç için alan
- monte edilmiş raf rayları ve raflar

İsteğe bağlı olarak, QRadar SIEM konsoluna erişmek için bir USB klavye ve standart VGA monitör isteyebilirsiniz.

Güvenlik duvarlarında kapı erişimini yapılandırma

IBM Security QRadar konsolu ile IBM Security QRadar Risk Manager arasındaki güvenlik duvarları, belirli kapılarda trafiğe izin vermelidir.

QRadar SIEM konsolu ile QRadar Risk Manager arasında bulunan güvenlik duvarlarının aşağıdaki kapılarda trafiğe izin verdiğinden emin olun:

- 443 numaralı kapı (HTTPS)
- 22 numaralı kapı (SSH)
- 37 numaralı kapı UDP (Zaman)

Ağ ayarlarını tanımlama

Kuruluş işlemini başlatmadan önce ağ ayarlarınızla ilgili bilgi toplamanız gerekir.

Ağ ayarlarınız için aşağıdaki bilgileri toplayın:

- Anasistem adı
- IP adresi
- Ağ maskesi adresi
- Alt ağ maskesi
- Varsayılan ağ geçidi adresi
- Birincil Etki Alanı Ad Sistemi (DNS) sunucu adresi
- İkincil DNS sunucusu (isteğe bağlı) adresi
- Ağ Adresi Çevirisi (NAT) e-posta sunucusu adını kullanan ağlar için genel IP adresi
- E-posta sunucusu adı
- Ağ Zaman Protokolü (NTP) sunucusu (yalnızca Konsol) ya da zaman sunucusu adı

QRadar Risk Manager uygulamasında desteklenmeyen özellikler

IBM Security QRadar Risk Manager tarafından desteklenmeyen özelliklerin bilinmesi önemlidir.

QRadar Risk Manager uygulamasında aşağıdaki özellikler desteklenmez:

- Yüksek kullanılabilirlik (HA)
- Dynamic Routing for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) ya da Routing Information Protocol (RIP)
- IPv6
- Bitişik olmayan ağ maskeleri
- Yük dengeli rotalar
- Başvuru eşlemleri
- Saklama ve İletme

Desteklenen web tarayıcıları

IBM Security QRadar ürünlerindeki özelliklerin düzgün şekilde çalışması için desteklenen bir web tarayıcısı kullanmanız gerekir.

QRadar sistemine eriştiğinizde sizden bir kullanıcı adı ve parola istenir. Kullanıcı adı ve parola önceden sistem yöneticisi tarafından yapılandırılmış olmalıdır.

Aşağıdaki tabloda, web tarayıcılarının desteklenen sürümleri listelenmektedir.

Çizelge 1. QRadar ürünleri için desteklenen web tarayıcıları

Web tarayıcısı	Desteklenen sürüm
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32 bitlik Microsoft Internet Explorer, belge kipi ve tarayıcı kipi etkinleştirilmiş şekilde	9.0 10
Google Chrome	IBM Security QRadar V7.2.4 ürünlerinin yayın tarihinden itibaren geçerli sürüm

Internet Explorer'da belge kipini ve tarayıcı kipini etkinleştirme

IBM Security QRadar ürünlerine erişmek için Microsoft Internet Explorer kullanırsanız, tarayıcı kipini ve belge kipini etkinleştirmeniz gerekir.

Yordam

1. Internet Explorer web tarayıcınızda, Developer Tools (Geliştirici Araçları) penceresini açmak için F12 tuşuna basın.
2. **Browser Mode** (Tarayıcı Kipi) seçeneğini tıklatın ve web tarayıcınızın sürümünü seçin.
3. **Document Mode** (Belge Kipi) seçeneğini tıklatın.
   - Internet Explorer V9.0 için **Internet Explorer 9 standards** (Internet Explorer 9 standartları) seçeneğini belirleyin
   - Internet Explorer V8.0 için **Internet Explorer 8 standards** (Internet Explorer 8 standartları) seçeneğini belirleyin

IBM Security QRadar Risk Manager kullanıcı arabirimine erişim

IBM Security QRadar Risk Manager; URL, kullanıcı adı ve parola için varsayılan oturum açma bilgilerini kullanır.

IBM Security QRadar Risk Manager uygulamasına QRadar konsolu aracılığıyla erişirsiniz. IBM Security QRadar konsolunda oturum açtığınızda aşağıdaki tabloda yer alan bilgileri kullanın.

Çizelge 2. QRadar Risk Manager için varsayılan oturum açma bilgileri

Oturum açma bilgileri	Varsayılan
URL	https://<IP adresi>; burada <IP adresi>, QRadar konsolunun IP adresidir.
Kullanıcı adı	admin
Parola	Kuruluş işlemi sırasında QRadar Risk Manager'a atanan parola.
Lisans anahtarı	Varsayılan bir lisans anahtarı, sisteme 5 hafta süreyle erişim sağlar.

QRadar Risk Manager aracını ayarlama

Yönetim arabirimine bağlanmanız ve güç bağlantılarının QRadar Risk Manager aracına bağlandığından emin olmanız gerekir.

Başlamadan önce

Önkoşulları okuyun, anlayın ve alın.

Bu görev hakkında

IBM Security QRadar Risk Manager değerlendirme aracı, iki birimli, raf düzenekli bir sunucudur. Raf rayları ve raflar, değerlendirme ekipmanı ile birlikte sağlanmaz.

QRadar Risk Manager aracı dört ağ arabirimi içerir. Bu değerlendirme için, yönetim arabirimi olarak ETH0 etiketli ağ arabirimini kullanın. Diğer arabirimler izleme arabirimleridir. Tüm arabirimler, QRadar Risk Manager aracının arka panelindedir.

Güç düğmesi ön paneldedir.

Yordam

1. Yönetim ağ arabirimini, ETH0 etiketli kapıya bağlayın.
2. Özel olarak ayrılan güç bağlantılarının aracın arkasına bağlandığından emin olun.
3. İsteğe bağlı. QRadar SIEM konsoluna erişmek için USB klavyesini ve standart bir VGA monitör bağlayın.
4. Araçta bir ön bölme varsa, herhangi bir yandaki tırnaklara bastırarak bölmeyi araçtan çekip çıkarın.
5. Aracı açmak için öndeki güç düğmesine basın.

Sonuçlar

Araç, önyükleme işlemiyle başlar.

QRadar Risk Manager uygulamasını QRadar konsoluna ekleme

IBM Security QRadar Risk Manager uygulamasını yönetilen anasistem olarak IBM Security QRadar konsoluna eklemeniz gerekir.

Başlamadan önce

Sıkıştırmayı etkinleştirmek istiyorsanız, her bir yönetilen anasistem için minimum sürüm QRadar Console 7.1 ya da QRadar Risk Manager 7.1 olmalıdır.

Konsol NAT etkin olduğunda devreye alımınıza NAT etkin olmayan bir yönetilen anasistem eklemek için QRadar konsolunu bir NAT etkin anasisteme değiştirmeniz gerekir. Yönetilen anasistemi devreye alımınıza eklemeden önce konsolu değiştirmeniz gerekir. Daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Yordam

1. Web tarayıcınızı açın.
2. https://<IP Adresi> URL'sini yazın; burada <IP Adresi>, QRadar konsolunun IP adresidir.
3. Kullanıcı adınızı ve parolanızı yazın.
4. **Admin** (Yönetim) sekmesinde **Deployment Editor** (Devreye Alma Düzenleyicisi) seçeneğini tıklatın.
5. Menüden **Actions** (İşlemler) ve **Add a Managed Host** (Yönetilen Anasistem Ekle) seçeneğini belirleyin.
6. **Next** (İleri) seçeneğini tıklatın.
7. Aşağıdaki parametreler için değer girin:

Seçenek	Açıklama
Enter the IP of the server or appliance to add (Eklenecek sunucu ya da aracın IP'sini girin)	QRadar Risk Manager uygulamasının IP adresi.
Enter the root password of the host (Anasistemin kök parolasını girin)	Anasistemin kök parolası.
Confirm the root password of the host (Anasistemin kök parolasını onaylayın)	Parolanızın onayı.
Host is NATed (Anasistem NAT etkindir)	Yönetilen anasistemde NAT'ın etkinleştirilmesi için NAT etkin ağ, statik NAT çevirisini kullanıyor olmalıdır. Daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.
Enable Encryption (Şifrelemeyi Etkinleştir)	Anasistem için bir SSH şifreleme tüneli oluşturur. İki yönetilen anasistem arasında şifrelemeyi etkinleştirmek için her bir yönetilen anasistem, QRadar Console 7.1 ya da QRadar Risk Manager 7.1 uygulamasını çalıştırıyor olmalıdır.
Enable Compression (Sıkıştırmayı Etkinleştir)	İki yönetilen anasistem arasında veri sıkıştırmasını etkinleştirir.

8. Aşağıdaki seçeneklerden birini belirleyin:
   - **Host is NATed** (Anasistem NAT etkindir) onay kutusunu işaretlediyseniz, NAT parametreleri için değer girmeniz gerekir.

Seçenek	Açıklama
Enter public IP of the server or appliance to add (Eklenecek sunucu ya da aracın genel IP'sini girin)	Yönetilen anasistemin genel IP adresi. Yönetilen anasistem, NAT kullanan farklı ağlarda diğer yönetilen anasistemlerle iletişim kurmak için bu IP adresini kullanır.
Select NATed network (NAT etkin ağ seç)	Bu yönetilen anasistemin kullanmasını istediğiniz ağ. Yönetilen anasistem, QRadar konsoluyla aynı alt ağ üzerindeyse, NAT etkin ağın konsolunu seçin. Yönetilen anasistem, QRadar konsoluyla aynı alt ağ üzerindeyse, NAT etkin ağın yönetilen anasistemini seçin.

   - **Host is NATed** (Anasistem NAT etkindir) onay kutusunu işaretlemediyseniz **Next** (İleri) düğmesini tıklatın.
9. **Finish** (Son) düğmesini tıklatın. Bu işlemin tamamlanması birkaç dakika sürebilir. Devreye alımınız değişiklikler içeriyorsa tüm değişiklikleri devreye almanız gerekir.
10. **Deploy** (Devreye Al) seçeneğini tıklatın.

Sonraki adım

Web tarayıcınızın önbelleğini temizleyin ve QRadar konsolunda oturum açın. **Risks** (Riskler) sekmesi şimdi kullanılabilir olur.

İletişim kurma

QRadar Risk Manager'ı kurup yapılandırmadan önce QRadar Risk Manager aracınız ile QRadar SIEM konsolunuz arasında iletişim kurmanız gerekir.

Bu görev hakkında

İletişim kurma işleminin tamamlanması birkaç dakika sürebilir. QRadar Risk Manager aracınızın IP adresini değiştirirseniz ya da QRadar Risk Manager'ı başka bir QRadar SIEM konsoluna bağlamanız gerekirse, QRadar SIEM **Admin** (Yönetim) sekmesinde **Risk Manager Settings** (Risk Manager Ayarları) seçeneğini kullanabilirsiniz.

Yordam

1. Web tarayıcınızı açın ve web tarayıcısı önbelleğini temizleyin.
2. QRadar SIEM'de oturum açın. IP adresi, kullanıcı adı ya da kök parola hakkında bilgi için bkz. IBM Security QRadar Risk Manager kullanıcı arabirimine erişme.
3. **Risks** (Riskler) sekmesini tıklatın.
4. Aşağıdaki parametreler için değerler girin:

Seçenek	Açıklama
IP/Host (IP/Anasistem)	QRadar Risk Manager aracının IP adresi ya da anasistem adı
Root Password (Kök Parola)	QRadar Risk Manager aracının kök parolası

5. **Save** (Kaydet) seçeneğini tıklatın.

Sonraki adım

Kullanıcı rollerini tanımlayın.

Risk Manager kullanıcı rolünü ekleme

QRadar Risk Manager olanağına erişim sağlamak için Risk Manager kullanıcı rolünü atamanız gerekir.

Bu görev hakkında

Varsayılan değer olarak QRadar SIEM, QRadar Risk Manager'da her şeye erişim sağlayan varsayılan bir yönetici rolü sağlar. Varsayılan yönetici rolü de dahil, yönetici ayrıcalıkları atanan bir kullanıcı kendi hesabını düzenleyemez. Başka bir yönetimle görevli kullanıcı gerekli değişiklikleri yapmalıdır.

Kullanıcı rolleri oluşturma ve yönetme hakkında bilgi için *IBM Security QRadar SIEM Administration Guide* başlıklı yayına bakın.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **System Configuration** (Sistem Yapılandırması) seçeneğini tıklatın.
3. **User Management** (Kullanıcı Yönetimi) bölmesinde **User Roles** (Kullanıcı Rolleri) seçeneğini tıklatın.
4. Sol bölmede, düzenlemek istediğiniz kullanıcı rolünü seçin.
5. **Risk Manager** onay kutusunu seçin.
6. **Save** (Kaydet) seçeneğini tıklatın
7. **Close** (Kapat) seçeneğini tıklatın.
8. **Admin** (Yönetim) sekmesinde **Deploy Changes** (Değişiklikleri Devreye Al) seçeneğini tıklatın.

Bölüm 3. Ağ verilerini toplama

Ağınızdaki aygıtlardan yapılandırma bilgilerini okumak için QRadar Risk Manager uygulamasını yapılandırmanız gerekir.

Ağ aygıtlarınızdan toplanan yapılandırma bilgileri, ağınız için topolojiyi oluşturur ve QRadar Risk Manager uygulamasının ağ yapılandırmanızı anlamasını sağlar.

QRadar Risk Manager'da toplanan veriler, topolojiyi ağ ortamınızla ilgili temel bilgilerle doldurmak için kullanılır.

Veri toplama, üç adımdan oluşan bir işlemdir:

- Ağ aygıtı yapılandırmalarını karşıdan yüklemek için QRadar Risk Manager uygulamasına kimlik bilgilerini sağlayın.
- Configuration Source Management'ta (Yapılandırma Kaynak Yönetimi) bir aygıt listesi oluşturmak için aygıtları keşfedin.
- Aygıt yapılandırmalarını elde etmek ve topolojiyi ağınızla ilgili verilerle doldurmak için aygıt listesini yedekleyin.

Kimlik Bilgileri

QRadar Risk Manager, aygıt yapılandırmalarına erişip aygıt yapılandırmalarını karşıdan yüklemek için kimlik bilgileriyle yapılandırılmalıdır. Kimlik bilgileri, QRadar Risk Manager uygulamasının güvenlik duvarlarına, yönlendiricilere, anahtarlara ya da İzinsiz Giriş Engelleme Sistemi (IPS) aygıtlarına bağlanmasına olanak sağlar.

Sistem yöneticileri, QRadar Risk Manager uygulamasına belirli bir aygıta erişme izni veren aygıt kimlik bilgilerini girmek için **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) olanağını kullanır. QRadar Risk Manager, belirli bir ağ aygıtı için bireysel aygıt kimlik bilgilerini kaydedebilir. Birden çok ağ aygıtı aynı kimlik bilgilerini kullanıyorsa bir gruba kimlik bilgileri atayabilirsiniz. Örneğin, kuruluştaki tüm güvenlik duvarları aynı kullanıcı adı ve parolaya sahipse bir gruba kimlik bilgileri atayabilirsiniz. Kimlik bilgileri, tüm güvenlik duvarları için adres kümeleriyle ilişkilendirilmiştir ve kuruluşunuzdaki tüm güvenlik duvarlarının aygıt yapılandırmalarını yedeklemek için kullanılır.

Not: Belirli bir aygıt için ağ kimlik bilgileri gerekmiyorsa, **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) içinde parametre boş bırakılabilir.

Kimlik bilgilerini yapılandırma

QRadar Risk Manager olanağına aygıtlara erişim yetkisi sağlamak için ağ aygıtlarını yapılandırırsınız.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Plug-ins** (Eklentiler) seçeneğini tıklatın.
3. **Risk Manager** (Risk Yöneticisi) bölmesinde **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) seçeneğini tıklatın.
4. Gezinme menüsünde **Credentials** (Kimlik Bilgileri) seçeneğini tıklatın.
5. **Network Groups** (Ağ Grupları) bölmesinde **Add a new network group** (Yeni bir ağ grubu ekle) seçeneğini tıklatın.

6. Ağ grubu için bir ad yazın ve **OK** (Tamam) düğmesini tıklatın.
7. **Add address** (Adres ekle) alanına aygıtınızın IP adresini yazın ve **Add** (Ekle) seçeneğini tıklatın. Eklemeniz gereken her adres için bu adımı yineleyin.

   Not: Eklediğiniz adreslerin, **Add address** (Adres ekle) kutusunun yanındaki Network address (Ağ adresi) bölümünde görüntülendiğinden emin olun. **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) içinde diğer ağ gruplarında önceden var olan aygıt adreslerini eşlemeyin.
   Bir IP adresi, IP adresleri aralığı, CIDR alt ağı ya da bir joker karakter yazabilirsiniz. Örneğin, joker karakter kullanmak için 10.1.*.* yazın ya da CIDR kullanmak için 10.2.1.0/24 değerini kullanın.
8. **Credentials** (Kimlik Bilgileri) bölmesinde **Add a new credential set** (Yeni bir kimlik bilgileri kümesi ekle) seçeneğini tıklatın.
9. Yeni kimlik bilgileri kümesi için bir ad yazın ve **OK** (Tamam) düğmesini tıklatın.
10. Oluşturduğunuz kimlik bilgileri kümesinin adını seçin ve aşağıdaki parametreler için değerleri yapılandırın:

Seçenek	Açıklama
Username (Kullanıcı Adı)	Bağdaştırıcıda oturum açmak için geçerli bir kullanıcı adı. Bağdaştırıcılarda, rule.C, objects.C, implied_rules.C ve Standard.PF gibi birçok dosyaya erişmek için kullanıcı adı ve parola gerekir.
Password (Parola)	Aygıtın parolası.
Enable Password (Parolayı Etkinleştir)	İkinci düzey kimlik doğrulaması için parolayı yazın. Uzman Kipi için kullanıcı kimlik bilgileri istendiğinde bu parola gereklidir.
SNMP Get Community (SNMP Alma Topluluğu)	İsteğe Bağlı
SNMPv3 Authentication Username (SNMPv3 Kimlik Doğrulama Kullanıcı Adı)	İsteğe bağlı parametre.
SNMPv3 Authentication Password (SNMPv3 Kimlik Doğrulama Parolası)	İsteğe bağlı parametre.
SNMPv3 Privacy Password (SNMPv3 Gizlilik Parolası)	İsteğe bağlı parametre. SNMPv3 yakalamalarının şifresini çözmek için kullanmak istediğiniz protokol.

11. **OK** (Tamam) düğmesini tıklatın.

Aygıtları keşfetme

Keşif işlemi, eklediğiniz kimlik bilgilerini kullanarak topoloji arabirimine ağ aygıtları ekler.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Plug-ins** (Eklentiler) seçeneğini tıklatın.
3. **Risk Manager** (Risk Yöneticisi) bölümünde **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) seçeneğini tıklatın.

4. Gezinme menüsünde **Discover Devices** (Aygıtları Keşfet) seçeneğini tıklatın.
5. Keşfetmek istediğiniz aygıtların konumunu belirtmek için bir IP adresi ya da CIDR aralığı yazın.
6. **Add (+)** (Ekle (+)) simgesini tıklatın.
7. Tanımlanan IP adresinden ya da CIDR aralığından ağdaki aygıtları aramak istiyorsanız, **Crawl the network from the addresses defined above** (Yukarıda tanımlanan adreslerden ağı tara) kutusunu seçin.
8. **Run** (Çalıştır) seçeneğini tıklatın.

Aygıt yapılandırmasını alma

Aygıt yapılandırmasını karşıdan yüklemek için aygıtlarınızı yedeklersiniz; böylece QRadar Risk Manager topolojiye aygıt bilgilerini dahil edebilir.

Başlamadan önce

Aygıt yapılandırmalarını karşıdan yükleyebilmeniz için önce kimlik bilgileri kümelerini yapılandırmanız gerekir.

Bu görev hakkında

Tek bir aygıtı ya da tüm aygıtları yedekleyebilirsiniz.

Jobs (İşler) sekmesinden aygıt yapılandırmalarının otomatik yedeklemelerini zamanlama hakkında bilgi için *IBM Security QRadar Risk Manager User Guide* başlıklı yayına bakın.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Plug-ins** (Eklentiler) seçeneğini tıklatın.
3. **Risk Manager** (Risk Yöneticisi) bölmesinde **Configuration Source Management** (Yapılandırma Kaynak Yönetimi) seçeneğini tıklatın.
4. **Devices** (Aygıtlar) sekmesini tıklatın.
5. Tüm aygıtlara yönelik yapılandırmayı almak için gezinme bölmesinde **Backup All** (Tümünü Yedekle) seçeneğini tıklatın. Devam etmek için **Yes** (Evet) seçeneğini tıklatın.
6. Belirli aygıtlara ilişkin yapılandırmayı almak için tek tek aygıtları seçin. Yedeklenecek birden çok aygıtı seçmek için Ctrl tuşunu basılı tutun. **Backup** (Yedekle) düğmesini tıklatın.

Aygıtları içe aktarma

Virgülle ayrılmış dosya (.CSV) kullanarak Configuration Source Manager'a (Yapılandırma Kaynak Yönetimi) bir bağdaştırıcı listesi ve bunların ağ IP adreslerini eklemek için Device Import (Aygıt İçe Aktar) işlemini kullanın.

Aygıt içe aktarma listesi en fazla 5000 aygıt içerebilir, ancak liste, içe aktarma dosyasındaki ilişkili IP adresi ve her bir bağdaştırıcı için bir satır ve içermelidir.

Örneğin,

```
<Bağdaştırıcı::Adı 1>,<IP Adresi>
<Bağdaştırıcı::Adı 2>,<IP Adresi>
<Bağdaştırıcı::Adı 3>,<IP Adresi>
```

Burada:

<Bağdaştırıcı::Adı>, üreticiyi ve aygıt adını içerir; örneğin, Cisco::IOS.

<IP Adresi>, aygıtın IP adresini içerir; örneğin, 191.168.1.1.

Çizelge 3. Aygıt içe aktarma örnekleri

Üretici	Adı	Örnek <Bağdaştırıcı::Adı>,<IP Adresi>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

CSV dosyasını içe aktarma

Virgülle ayrılmış değer (CSV) dosyasını kullanarak Configuration Source Management'a (Yapılandırma Kaynak Yönetimi) ana aygıt listesi içe aktarabilirsiniz.

Başlamadan önce

Bir aygıt listesini içe aktarır ve sonra CSV dosyasında bir IP adresi üzerinde değişiklik yaparsanız, Configuration Source Management (Yapılandırma Kaynak Yönetimi) listesinde bir aygıtı yanlışlıkla çoğaltabilirsiniz. Bu nedenle, ana aygıt listenizi yeniden içe aktarmadan önce Configuration Source Management'tan (Yapılandırma Kaynak Yönetimi) bir aygıtı silin.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Plug-ins** (Eklentiler) seçeneğini tıklatın.
3. **Plug-Ins** (Eklentiler) bölmesinde **Device Import** (Aygıt İçe Aktarma) seçeneğini tıklatın.
4. **Browse** (Göz At) seçeneğini tıklatın.
5. CSV dosyanızı bulun, **Open** (Aç) seçeneğini tıklatın.
6. **Import Devices** (Aygıtları İçe Aktar) seçeneğini tıklatın.

Sonuçlar

Bir hata görüntülenirse, hataları düzeltmek için CSV dosyanızı gözden geçirmeniz ve dosyayı yeniden içe aktarmanız gerekir. Aygıt listesi yanlış şekilde yapılandırılırsa ya da aygıt listesi yanlış bilgiler içerirse CSV dosyasının içe aktarılması başarısız olabilir. Örneğin, CSV dosyanızda iki nokta ya da komut eksik olabilir, tek bir hatta birden çok aygıt bulunabilir veya bir bağdaştırıcı adında yazım hatası olabilir.

Aygıt içe aktarma işleminiz durdurulursa, CSV dosyasından aygıtlar Configuration Source Management'a (Yapılandırma Kaynak Yönetimi) eklenmez.

Aygıt içe aktarma ile ilgili sorunları giderme

Aygıtınızı içe aktarmayı denedikten sonra hata iletisi alırsanız bu, CSV dosyasının içe aktarımının başarısız olmasından kaynaklanabilir.

Aygıt listesi yanlış şekilde yapılandırılmışsa, aygıtın içe aktarımı başarısız olabilir. Örneğin, CSV dosyasında iki nokta ya da bir komut eksik olabilir veya tek bir satırda birden çok aygıt bulunabilir.

Ayrıca aygıt listesi yanlış bilgiler içerdiğinde de içe aktarma başarısız olabilir. Örneğin, bir bağdaştırıcı adındaki tipografik bir hata gibi.

Aygıt içe aktarımı durdurulursa, CSV dosyasındaki hiçbir aygıt, Configuration Source Management'a (Yapılandırma Kaynak Yönetimi) eklenmez. İletide, kurulu bağdaştırıcılarınız için geçerli bağdaştırıcı adlarının bir listesi görüntülenir. Bir hata görüntülenirse, hataları düzeltmek için CSV dosyanızı gözden geçirmeniz gerekir. Hatalar düzeltildikten sonra dosyayı yeniden içe aktarabilirsiniz.

Bölüm 4. Denetimleri yönetme

IBM Security QRadar Risk Manager, soruları yanıtlamanıza yardımcı olarak ağ güvenliği ilkelerinin ve uyumluluk gereksinimlerinin değerlendirilmesini kolaylaştırır.

Uyumluluk denetimi, güvenlik yöneticileri için gerekli ve karmaşık bir görevdir. QRadar Risk Manager, aşağıdaki soruları yanıtlamanıza yardımcı olur:

- Ağ aygıtlarım nasıl yapılandırıldı?
- Ağ kaynaklarım nasıl iletişim kuruyor?
- Ağımın güvenlik açıkları nerelerdedir?

Kullanım senaryosu: Yapılandırma denetimi

Denetim uyumluluğu için ve yapılandırma yedeklemelerini zamanlamak için QRadar Risk Manager tarafından yakalanan ağ aygıtlarının yapılandırma bilgilerini kullanabilirsiniz.

Yapılandırma yedeklemeleri, denetim uyumluluğunuz için aygıt değişikliklerinin kaydedilmesine yönelik merkezi ve otomatik bir yöntem sağlar. Yapılandırma yedeklemeleri, yapılandırma değişikliklerini arşivler ve bir geçmiş başvurusu sağlar; bir geçmiş kaydını yakalayabilir ve bir yapılandırmayı başka bir ağ aygıtıyla karşılaştırabilirsiniz.

QRadar Risk Manager ürününde yapılandırma denetimi size şu seçenekleri sağlar:

- Ağ aygıtı yapılandırmalarınızın geçmiş kaydı.
- Yapılandırmaları karşılaştırdığınızda aygıt değişikliklerini görüntüleyen normalleştirilmiş bir görünüm.
- Aygıtınızdaki kuralları aramaya yönelik bir araç.

Aygıtlarınız için yapılandırma bilgileri, Configuration Source Management'ta (Yapılandırma Kaynak Yönetimi) aygıt yedeklemelerinden toplanır. QRadar Risk Manager, aygıt listenizi her yedeklediğinde, bir geçmiş başvurusu sağlamak için aygıt yapılandırmanızın bir kopyasını arşivler. Configuration Source Management'ı (Yapılandırma Kaynak Yönetimi) ne kadar sık zamanlarsanız, karşılaştırma ve geçmiş başvurusu için o kadar çok yapılandırma kaydınız olur.

Aygıt yapılandırması geçmişini görüntüleme

Ağ aygıtının yapılandırma geçmişini görüntüleyebilirsiniz.

Bu görev hakkında

Yedeklenen ağ aygıtları için geçmiş bilgilerini görüntüleyebilirsiniz. Bu bilgilere, **Configuration Monitor** (Yapılandırma İzleyicisi) sayfasında **History** (Geçmiş) bölmesinden erişilebilir. Geçmiş bölmesi, bir ağ aygıtı yapılandırmasıyla ilgili bilgileri ve Configuration Source Management (Yapılandırma Kaynak Yönetimi) kullanılarak aygıt yapılandırmasının en son yedeklendiği tarihi sağlar.

Yapılandırma, QRadar Risk Manager'da ağ aygıtınız için saklanan dosyaların tipini görüntüler. Genel yapılandırma tipleri:

- Ağ aygıtınızla ilgili bilgileri içeren XML veri dosyaları olan **Standard-Element-Document** (Standart Öğe Belgesi) (SED). Tek tek SED dosyaları, işlenmemiş XML biçiminde görüntülenir. Bir SED başka bir SED dosyasıyla karşılaştırılırsa görünüm, kural farklılıklarını görüntülemek için normalleştirilir.

- Belirli ağ aygıtları tarafından sağlanan yapılandırma dosyaları olan **Config** (Yapılandırma). Bu dosyalar, aygıt üreticisine bağlıdır. Yapılandırma dosyası, yapılandırma dosyası çift tıklatılarak görüntülenebilir.

Not: Aygıtınıza bağlı olarak başka birçok yapılandırma dosyası görüntülenebilir. Bu dosyalar çift tıklatıldığında içerikler düz metin olarak görüntülenir. Düz metin görünümü, web tarayıcısı penceresinden bulma (Ctrl +f), yapıştırma (Ctrl+v) ve kopyalama (Ctrl+C) işlevlerini destekler.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Configuration Monitor** (Yapılandırma İzleyicisi) seçeneğini tıklatın.
3. Ayrıntılı aygıt bilgilerini görüntülemek için bir yapılandırmayı çift tıklatın.
4. **History** (Geçmiş) seçeneğini tıklatın.
5. **History** (Geçmiş) bölmesinde bir yapılandırma seçin.
6. **View Selected** (Seçileni Görüntüle) seçeneğini tıklatın.

Tek bir aygıt için aygıt yapılandırmalarını karşılaştırma

Tek bir aygıt için aygıt yapılandırmalarını karşılaştırabilirsiniz.

Bu görev hakkında

Karşılaştırdığınız dosyalar Standart Öğe Belgeleri (SED) ise, yapılandırma dosyaları arasındaki kural farklılıklarını görüntüleyebilirsiniz.

Normal yapılandırmaları karşılaştırdığınızda metnin rengi aşağıdaki kuralları belirtir:

- Yeşil noktalı anahat, aygıta eklenen bir kuralı ya da yapılandırmayı belirtir.
- Kırmızı kısa çizgili anahat, aygıttan silinen bir kuralı ya da yapılandırmayı belirtir.
- Sarı düz çizgi, aygıtta değiştirilen bir kuralı ya da yapılandırmayı belirtir.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Configuration Monitor** (Yapılandırma İzleyicisi) seçeneğini tıklatın.
3. Ayrıntılı yapılandırma bilgilerini görüntülemek için herhangi bir aygıtı çift tıklatın.
4. Bu aygıtın geçmişini görüntülemek için **History** (Geçmiş) seçeneğini tıklatın.
5. Birincil yapılandırma seçin.
6. Ctrl tuşuna basın ve karşılaştırma için ikinci bir yapılandırma seçin.
7. **History** (Geçmiş) bölmesinde **Compare Selected** (Seçileni Karşılaştır) seçeneğini tıklatın.
8. İsteğe bağlı. İşlenmemiş yapılandırma farklılıklarını görüntülemek için **View Raw Comparison** (İşlenmemiş Karşılaştırmayı Görüntüle) seçeneğini tıklatın. Karşılaştırma bir yapılandırma dosyası ya da başka bir yedekleme tipi içinse, işlenmemiş karşılaştırma görüntülenir.

Farklı aygıtlar için aygıt yapılandırmalarını karşılaştırma

Farklı aygıtlar için iki yapılandırmayı karşılaştırabilirsiniz.

Bu görev hakkında

Karşılaştırdığınız dosyalar Standart Öğe Belgeleri (SED) ise, yapılandırma dosyaları arasındaki kural farklılıklarını görüntüleyebilirsiniz.

Normal yapılandırmaları karşılaştırdığınızda metnin rengi aşağıdaki kuralları belirtir:

- Yeşil noktalı anahat, aygıta eklenen bir kuralı ya da yapılandırmayı belirtir.
- Kırmızı kısa çizgili anahat, aygıttan silinen bir kuralı ya da yapılandırmayı belirtir.
- Sarı düz çizgi, aygıtta değiştirilen bir kuralı ya da yapılandırmayı belirtir.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Configuration Monitor** (Yapılandırma İzleyicisi) seçeneğini tıklatın.
3. Ayrıntılı yapılandırma bilgilerini görüntülemek için herhangi bir aygıtı çift tıklatın.
4. Bu aygıtın geçmişini görüntülemek için **History** (Geçmiş) seçeneğini tıklatın.
5. Birincil yapılandırma seçin.
6. **Mark for Comparison** (Karşılaştırma için İşaretle) seçeneğini tıklatın.
7. Aygıt listesine geri dönmek için gezinme menüsünden **All Devices** (Tüm Aygıtlar) seçeneğini belirleyin.
8. Karşılaştırılacak aygıtı çift tıklatın ve **History** (Geçmiş) öğesini tıklatın.
9. İşaretli yapılandırma ile karşılaştırılacak başka bir yapılandırma yedeklemesi seçin.
10. **Compare with Marked** (İşaretli Olanla Karşılaştır) seçeneğini tıklatın.
11. İsteğe bağlı. İşlenmemiş yapılandırma farklılıklarını görüntülemek için **View Raw Comparison** (İşlenmemiş Karşılaştırmayı Görüntüle) seçeneğini tıklatın. Karşılaştırma bir yapılandırma dosyası ya da başka bir yedekleme tipi içinse, işlenmemiş karşılaştırma görüntülenir.

Kullanım senaryosu: Topolojideki ağ yollarını görüntüleme

QRadar Risk Manager uygulamasındaki topoloji, ağ aygıtlarınızın grafiksel bir gösterimini sunar.

Topoloji yolu araması, ağ aygıtlarınızın nasıl iletişim kurduğunu ve iletişim kurmak için kullandıkları ağ yolunu belirleyebilir. Yol araması, QRadar Risk Manager uygulamasının, kapılar, protokoller ve kurallar ile birlikte bir kaynak ile hedef arasındaki yolu görüntülemesine olanak sağlar.

Aygıtların nasıl iletişim kurduğunu görüntüleyebilirsiniz; bu, güvenli ya da sınırlı erişim varlıklarında önemlidir.

Temel özellikler arasında şunlar yer alır:

- Ağınızdaki aygıtlar arasındaki iletişimleri görüntüleme yeteneği.
- Ağ aygıtlarına yönelik topolojiyi aramak için süzgeçler kullanma.
- Aygıt kurallarını ve yapılandırmayı görüntülemek için hızlı erişim.
- Bir yol aramasından oluşturulan olayları görüntüleme yeteneği.

Topolojide arama yapma

Topolojide arama yaparak aygıt iletişimini görüntüleyebilirsiniz.

Bu görev hakkında

Topoloji modelini süzgeçten geçirmek için bir yol araması kullanılır. Yol araması, yapılandırılan protokol ve yol kullanılarak iletişim kurmasına izin verilen hedef IP adreslerini ya da CIDR aralıklarını içeren kaynak IP adreslerini veya CIDR aralıklarını ve alt ağları içeren tüm ağ alt ağlarını içerir. Arama, var olan topoloji modelinizi inceler ve kaynak ile hedef arasındaki iletişim yolunda bulunan aygıtları ve ayrıntılı bağlantı bilgilerini içerir.

Topolojiniz bir İzinsiz Giriş Engelleme Sistemi (IPS) içeriyorsa aramaya süzgeç uygulamak için güvenlik açıklarını kullanabilirsiniz. Daha fazla bilgi için *IBM Security QRadar Risk Manager User Guide* başlıklı yayına bakın.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Topology** (Topoloji) seçeneğini tıklatın.
3. **Search** (Arama) liste kutusundan **New Search** (Yeni Arama) seçeneğini belirleyin.
4. **Search Criteria** (Arama Ölçütleri) bölmesinde **Path** (Yol) seçeneğini belirleyin.
5. **Source IP/CIDR** (Kaynak IP/CIDR) alanına, topoloji modeline süzgeç uygulamak istediğiniz IP adresini ya da CIDR aralığını yazın. Birden çok girişi virgül kullanarak ayırın.
6. **Destination IP/CIDR** (Hedef IP/CIDR) alanına, topoloji modeline süzgeç uygulamak için kullanmak istediğiniz hedef IP adresini ya da CIDR aralığını yazın. Birden çok girişi virgül kullanarak ayırın.
7. İsteğe bağlı. **Protocol** (Protokol) listesinden, topoloji modeline süzgeç uygulamak için kullanmak istediğiniz protokolü seçin.
8. İsteğe bağlı. **Destination Port** (Hedef Kapı) alanına, topoloji modelini süzgeçten geçirmek istediğiniz hedef kapıyı yazın. Birden çok kapıyı virgül kullanarak ayırın.
9. **OK** (Tamam) seçeneğini tıklatın.
10. Bağlantıyla ilgili ayrıntıları görüntülemek için farenizi bir bağlantı hattının üzerine getirin. Arama, kurallar içeren bir aygıta bağlanırsa, iletişim kutusunda bir aygıt kuralları bağlantısı görüntülenir.

Kullanım senaryosu: Bir hücumun saldırı yolunu görselleştirme

QRadar Risk Manager uygulamasındaki hücumlar, bir ağ koşulu ya da olay ile ilgili size uyarı vermek için sistem tarafından oluşturulan olaylardır.

Saldırı yolu görselleştirmesi, topoloji aramalarıyla hücumları ilişkilendirir. Bu görselleştirme, güvenlik işletmenlerinin hücum ayrıntısını ve ağınız üzerinden hücumun aldığı yolu görüntülemesine olanak sağlar. Saldırı yolu size bir görsel temsil sağlar. Görsel temsil, bir hücumun ağ üzerinden yol almasını sağlamak için iletişim kuran ağınızdaki varlıkları size gösterir. Bu veriler, hücumları izlediğinizi kanıtlamak için denetleme sırasında kritik önem taşır, ancak hücumun ağınızda kritik bir varlığa yönelik alternatif bir yolunun olmadığını da kanıtlar.

Görselleştirme için temel özellikler:

- QRadar SIEM'deki var olan kural ve hücum sisteminden yararlanır.
- Hücumun kaynağı ile hedefi arasındaki tüm aygıtlar için görsel bir yol görüntüler.
- Hücuma izin veren kurallara ve aygıt yapılandırmalarına hızlı erişim.

Hücumun saldırı yolunu görüntüleme

Hücumun saldırı yolunu görüntüleyebilirsiniz. Saldırı yolu, kaynağı, hedefi ve ilişkili aygıtları gösterir.

Yordam

1. **Offenses** (Hücumlar) sekmesini tıklatın.
2. Gezinme menüsünde **All Offenses** (Tüm Hücumlar) seçeneğini tıklatın. **All Offenses** (Tüm Hücumlar) sayfası, ağınızdaki hücumların bir listesini görüntüler. Hücumlar, en yüksek büyüklükte olan en başta olacak şekilde listelenir.
3. Hücum özetini açmak için bir hücumu çift tıklatın.
4. **Offenses** (Hücumlar) araç çubuğunda **View Attack Path** (Saldırı Yolunu Görüntüle) seçeneğini tıklatın.

Bölüm 5. Kullanım senaryosu: İlkeleri izleme

İlke denetimi ve değişiklik denetimi, sistem yöneticilerinin ve güvenlik uzmanlarının kritik iş varlıkları arasında erişimi ve iletişimleri denetlemesine olanak sağlayan temel işlemlerdir.

İlke izleme ölçütleri, aşağıdaki senaryolar için varlıkların ve iletişimlerin izlenmesini içerebilir:

- Ağım, PCI Bölüm 1 denetimleri için riskli yapılandırmalar içeren varlıklar barındırıyor mu?
- Varlıklarım, PCI Bölüm 10 denetimleri için riskli protokolleri kullanan iletişimlere izin veriyor mu?
- Bir ilke değişikliği, ağımda ihlale neden olduğunda bunu nasıl bilirim?
- Güçlendirilmiş ya da yüksek riskli varlıklar için güvenlik açıklarını nasıl görüntülerim?
- Ağımdaki güvenlik açıkları ve İnternet erişimi içeren varlıkları nasıl görüntülerim?

Risk göstergelerini temel alan testler tanımlamak ve sonra belirli sonuçlar, ihlaller, protokoller ya da güvenlik açıklarına yönelik olarak sorguya süzgeç uygulamak için test sonuçlarını kısıtlayın.

IBM Security QRadar Risk Manager, PCI kategorisine göre gruplanmış birçok Policy Monitor sorusu içerir. Örneğin, PCI 1, PCI 6 ve PCI 10 soruları. Ağ güvenliği riskini ortaya çıkarmak üzere kurallar ve varlıklar ya da aygıtlar için sorular oluşturulabilir. Bir varlık ya da aygıt/kural ile ilgili bir soru Policy Monitor'a gönderildikten sonra döndürülen sonuçlar risk düzeyini belirtir. Varlıklardan döndürülen sonuçları onaylayabilir ya da sistemin onaylanmayan sonuçlara nasıl yanıt vermesini istediğinizi tanımlayabilirsiniz.

Policy Monitor aşağıdaki temel özellikleri sağlar:

- İş akışına yardımcı olması için önceden tanımlı Policy Monitor soruları.
- Kullanıcıların iletişim kurmak için yasaklanan protokolleri kullanıp kullanmadığını belirleme.
- Belirli ağlar üzerindeki kullanıcıların yasaklanan ağlar ya da varlıklarla iletişim kurup kuramayacağını değerlendirme.
- Güvenlik duvarı kurallarının kurumsal ilkeyi karşılayıp karşılamadığını değerlendirme.
- Sistem yöneticilerine saldırı ya da uyarılar oluşturan ilkeleri sürekli izleme.
- Aygıt yapılandırması sonucunda hangi sistemlerin güvenliğinin aşılabileceğini değerlendirerek güvenlik açıklarını önceliklendirme.
- Uyumluluk sorunlarının belirlenmesine yardımcı olma.

Kullanım senaryosu: Şüpheli yapılandırmalar içeren varlıkları değerlendirme

Kuruluşlar, varlıklar ile ağlar arasında izin verilen riskleri ve iletişimleri tanımlamak için kurumsal güvenlik ilkelerini kullanır. Uyumluluk ve kurumsal ilke ihlalleri konusunda yardımcı olmak için kuruluşlar Policy Monitor uygulamasını kullanarak bilinmiyor olabilecek riskleri değerlendirir ve izler.

PCI uyumluluğu, kart sahibinin verilerini içeren aygıtları belirlemenizi, ardından hassas verileri içeren varlıkları korumak için şema oluşturmanızı, iletişimleri doğrulamanızı ve güvenlik duvarı yapılandırmalarını izlemenizi gerektirir. Policy Monitor, bu gereksinimlerin hızlı şekilde karşılanmasına yönelik yöntemler sunar ve sistem yöneticilerinin kurumsal

ilkelere uymasını sağlar. Yaygın risk azaltma yöntemleri arasında, güvenli olmayan protokollerle iletişim kuran varlıkların belirlenmesi ve izlenmesi yer alır. Bunlar, FTP ya da telnet bağlantılarına izin veren yönlendiriciler, güvenlik duvarları veya anahtarlar gibi protokollerdir. Topolojinizdeki riskli yapılandırmalar içeren varlıkları belirlemek için Policy Monitor uygulamasını kullanın.

PCI bölüm 1 soruları aşağıdaki ölçütleri içerebilir:

- Yasaklanan protokollere izin veren varlıklar.
- Riskli protokollere izin veren varlıklar.
- Ağ üzerinde ilke dışı uygulamalara izin veren varlıklar.
- Korumalı varlıklar içeren ağlara yönelik ilke dışı uygulamalara izin veren varlıklar.

Riskli protokollere izin veren aygıtları değerlendirme

Riskli protokollere izin veren aygıtları değerlendirmek için Policy Monitor'ı kullanın.

Bu görev hakkında

QRadar Risk Manager, bir soruyu değerlendirir ve topolojinizde test sorusuyla eşleşen varlıkların sonuçlarını görüntüler. Ağınızdaki güvenlik uzmanları, sistem yöneticileri ya da denetleyiciler, belirli varlıklar için riskli olmayan iletişimleri onaylayabilir. Davranış için hücumlar da oluşturabilir.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Policy Monitor** (İlke İzleyici) seçeneğini tıklatın.
3. Group (Grup) liste kutusundan **PCI 1** seçeneğini belirleyin.
4. **Assess any devices (i.e. firewalls) that allow risky protocols (i.e telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ** (İnternet'ten DMZ'ye riskli protokollere (örn. telnet ve FTP trafiği - sırayla 21 ve 23 numaralı kapı) izin veren aygıtları (örn. güvenlik duvarları) değerlendirme) test sorusunu seçin.
5. **Submit Question** (Soru Gönder) seçeneğini tıklatın.

Kullanım senaryosu: Şüpheli iletişim içeren varlıkları değerlendirme

Ağ varlıklarına erişimi izleyerek, günlüğe kaydederek ve görüntüleyerek PCI bölüm 10 uyumluluğunu belirlemek için Policy Monitor uygulamasını kullanın.

QRadar Risk Manager, topolojideki şaibeli ya da riskli iletişimlere izin veren varlıkları belirleyerek PCI bölüm 10 uyumluluğunun tanımlanmasına yardımcı olabilir. QRadar Risk Manager, gerçek iletişimler veya olası iletişimler için bu varlıkları inceleyebilir. Gerçek iletişimler, iletişim kurmak için soru ölçütlerinizi kullanan varlıkları görüntüler. Olası iletişimler, iletişim kurmak için soru ölçütlerinizi kullanabilecek varlıkları görüntüler.

PCI bölüm 10 soruları aşağıdaki ölçütleri içerebilir:

- Dahili ağlara gelen sorulara izin veren varlıklar.
- Güvenilir olmayan konumlardan güvenilir konumlara iletişim kuran varlıklar.
- VPN'den güvenilir konumlara iletişim kuran varlıklar.
- Güvenilir bir konumda şifrelenmemiş ilke dışı protokollere izin veren varlıklar.

İletişime izin veren varlıkları bulma

İnternet'ten iletişime izin veren varlıkları bulabilirsiniz.

Bu görev hakkında

QRadar Risk Manager, soruyu değerlendirir ve İnternet'ten gelen iletişimlere izin veren dahili varlıkların sonuçlarını görüntüler. Ağınızdaki denetleyiciler, güvenlik uzmanları ya da sistem yöneticileri, güvenli olarak değerlendirilmeyen ya da müşteri verileri içeren varlıklara iletişimleri onaylayabilir. Daha fazla olay oluşturuldukça, bu tip riskli iletişimleri izlemek için QRadar SIEM'de hücumlar oluşturabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Policy Monitor** (İlke İzleyici) seçeneğini tıklatın.
3. Group (Grup) liste kutusundan **PCI 10** seçeneğini belirleyin.
4. **Assess any inbound connections from the internet to anywhere on the internal network** (İnternet'ten dahili ağdaki herhangi bir yere gelen bağlantıları değerlendirin) test sorusunu seçin.
5. **Submit Question** (Soru Gönder) seçeneğini tıklatın.

Kullanım senaryosu: İhlaller için ilkeleri izleme

QRadar Risk Manager, Policy Monitor'da herhangi bir önceden tanımlı veya kullanıcı tarafından oluşturulan soruyu sürekli izleyebilir. QRadar Risk Manager'da olaylar oluşturmak için izleme kipini kullanabilirsiniz.

İzlenecek bir soru seçtiğinizde, QRadar Risk Manager, bir varlık ya da kural değişikliğinin onaylanmayan bir sonuç oluşturup oluşturmayacağını belirlemek için bu soruyu topolojinize karşı analiz eder. QRadar Risk Manager onaylanmayan bir sonuç algılarsa, tanımladığınız ilkede bir sapma hakkında size uyarı vermek için bir saldırı oluşturulabilir. İzleme kipinde QRadar Risk Manager aynı anda 10 sorunun sonucunu izleyebilir.

Soru izleme size aşağıdaki temel özellikleri sağlar:

- Onaylanmayan sonuçlar için saatlik kural ya da varlık değişikliklerini izleme.
- Onaylanmayan sonuçları kategorilere ayırmak için yüksek ve düşük düzeyli olay kategorilerinizi kullanma.
- Onaylanmayan sonuçlarda saldırılar, e-postalar, sistem günlüğü iletileri ya da gösterge panosu bildirimleri oluşturma.
- QRadar SIEM'de olay izlemeyi, ilintilendirmeyi, olay raporlamasını, özel kuralları ve gösterge panolarını kullanma.

Soru yapılandırma

İzlenecek bir soru yapılandırmak için Policy Monitor (İlke İzleyici) olanağını kullanabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Policy Monitor** (İlke İzleyici) seçeneğini tıklatın.
3. İzlemek istediğiniz soruyu seçin.
4. **Monitor** (İzleyici) seçeneğini tıklatın.
5. Sorunuzu izlemek için gerekli gördüğünüz seçenekleri yapılandırın.
6. **Save Monitor** (İzleyiciyi Kaydet) seçeneğini tıklatın.

Sonuçlar

Soru için izleme etkinleştirilir ve izleme ölçütleriniz temel alınarak olaylar ya da hücumlar oluşturulur.

Kullanım senaryosu: Riskleri önceliklendirmek için güvenlik açıklarını kullanma

Ortaya çıkan güvenlik açıkları, ağ varlıkları için önemli bir risk unsurudur.

QRadar Risk Manager, Policy Monitor'daki varlık bilgilerinden ve güvenlik açığı bilgilerinden yararlanır. Bu bilgiler, varlıklarınızın SQL ekleme, gizli alanlar ve tıklatma hilesi gibi giriş tipi saldırılara açık olup olmadığını belirlemek için kullanılır.

Varlıklarınızda algılanan güvenlik açıkları, varlıklarınızın ağ konumuna ya da güvenlik açığı olan başka bir aygıta bağlantısına göre önceliklendirilebilir.

Güvenlik açığı varlık soruları aşağıdaki ölçütleri içerebilir:

- Belirli bir tarihten sonra bildirilen yeni güvenlik açıklarını içeren varlıklar.
- Belirli güvenlik açıkları ya da CVSS puanı içeren varlıklar.
- Giriş manipülasyonu, hizmet reddi, OSVDB doğrulaması gibi belirli bir güvenlik açığı sınıflandırmasına sahip varlıklar.

Güvenlik açıkları içeren varlıkları bulma

Güvenlik açıkları içeren varlıkları bulabilirsiniz.

Bu görev hakkında

QRadar Risk Manager, bir soruyu değerlendirir ve güvenlik açıkları içeren varlıkların sonuçlarını görüntüler. Güvenlik uzmanları, yöneticiler ya da denetleyiciler, ağınızda bilinen SQL ekleme güvenliği açıkları içeren varlıkları belirleyebilir. Korumalı bir ağa bağlı varlıklara hızla yama uygulayabilirler. Daha fazla olay oluşturuldukça, SQL ekleme güvenliği açıklarını içeren varlıkları izlemek için QRadar SIEM'de olaylar ya da hücumlar oluşturabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Policy Monitor** (İlke İzleyici) seçeneğini tıklatın.
3. **Group** (Grup) listesinden **Vulnerability** (Güvenlik Açığı) seçeneğini belirleyin.
4. **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)** (Belirli yerel ağlarda SQL ekleme güvenliği açıkları içeren varlıkları (örn. korumalı sunucu ağı) değerlendir) test sorusunu seçin.
5. **Submit Question** (Soru Gönder) seçeneğini tıklatın.

Kullanım senaryosu: Varlık güvenlik açıklarını bölgeye ya da ağ iletişimlerine göre önceliklendirme

Korumalı varlıklarla aynı ağda olan güvenlik açıklarına sahip sistemler daha yüksek veri kaybı riski altındadır.

Bölgeye ya da ağa göre varlıklardaki güvenlik açıklarının algılanması, ağınızdaki açıkların oluşmadan engellenmesi için temel önlemdir. PCI bölüm 6.1 ve 6.2, güvenlik açığı yaması

yayın düzeyinden sonra bir ay içinde sistemleri gözden geçirip sistemlere yama uygulamanızı şart koşar. QRadar Risk Manager, yama uygulama işlemini otomatikleştirme ve önceliklendirme konusunda yardımcı olur. Varlıklarınızda güvenlik açıkları algılandıkça, bunları ağ konumuna ya da saldırıya açık olan başka bir aygıta bağlantıya göre önceliklendirebilirsiniz. Şüpheli bölgelere ya da dahili ilkenizin izin verdiğinden daha yüksek CVSS puanına sahip varlıklara bağlanabilen güvenli ağlar için önceliklendirme önemlidir.

Güvenlik açığı olan varlık soruları aşağıdaki ölçütleri içerebilir:

- Şüpheli coğrafi bölgelerle iletişim kuran ve korumalı varlıklar içeren, istemci tarafı güvenlik açığı içeren varlıklar.
- Belirli bir ağda hizmet reddi güvenlik açıklarını içeren varlıklar.
- Belirli bir ağda posta güvenlik açıklarını içeren varlıklar.
- Güvenlik açıkları ve belirli bir CVSS (Common Vulnerability Scoring System; Genel Güvenlik Açığı Puanlama Sistemi) puanına sahip varlıklar.

Ağ üzerindeki güvenlik açığı içeren varlıkları bulma

Belirli bir ağ üzerindeki güvenlik açığı içeren varlıkları bulabilirsiniz.

Bu görev hakkında

QRadar Risk Manager, soruyu değerlendirir ve sonuçları, işletim sistemine özgü güvenlik açığı içeren belirli konumda görüntüler. Ağınızın denetleyicileri, güvenlik uzmanları ya da sistem yöneticileri, güvenli olarak değerlendirilmeyen ya da müşteri verileri içeren varlıklara iletişimleri onaylayabilir. Daha fazla olay oluşturuldukça, bu tip riskli iletişimleri izlemek için hücumlar oluşturabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Policy Monitor** (İlke İzleyici) seçeneğini tıklatın.
3. **Group** (Grup) liste kutusundan **Vulnerability** (Güvenlik Açığı) seçeneğini belirleyin.
4. **Assess assets with OS specific vulnerabilities on a specific localnet(s)** (Belirli yerel ağlarda işletim sistemine özgü güvenlik açığı içeren varlıkları değerlendirme) test sorusunu seçin.
5. **Submit Question** (Soru Gönder) seçeneğini tıklatın.

Bölüm 6. Simülasyonlar için kullanım senaryoları

Kullanım senaryosu: Ağ varlıklarında saldırıların simülasyonunu yapma

Çeşitli kaynaklardan güvenlik açıkları için ağınızı test etmek üzere bir simülasyon kullanabilirsiniz.

Ağınızdaki aygıt yapılandırmalarını denetlemek için saldırı simülasyonlarını kullanabilirsiniz.

Simülasyonlar aşağıdaki temel özellikleri sağlar:

- Simülasyonlar, bir saldırının ağınıza karşı uygulayabileceği teorik yol permütasyonlarını görüntüler.
- Simülasyonlar, saldırıların diğer varlıklara uzanmak için ağ aygıtlarınız üzerinden nasıl yayılabileceğini görüntüler.
- Simülasyonlar, güvenlik açığı olan siteleri algılamak için izlemeye olanak sağlar.

Simülasyon oluşturma

SSH protokolünde bir ağ saldırısı için simülasyon oluşturabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Simulation > Simulations** (Simülasyon - Simülasyonlar) seçeneklerini belirleyin.
3. **Actions** (İşlemler) listesinden **New** (Yeni) seçeneğini belirleyin.
4. Simülasyon için bir ad yazın.
5. **Current Topology** (Geçerli Topoloji) seçeneğini belirleyin.
6. **Use Connection Data** (Bağlantı Verilerini Kullan) onay kutusunu seçin.
7. **Where do you want the simulation to begin** (Simülasyonun nereden başlamasını istiyorsunuz?) listesinden, simülasyon için bir başlangıç noktası seçin.
8. Simülasyon saldırısını ekleyin, **Attack targets one of the following open ports using protocols** (Saldırı protokolleri kullanarak şu açık kapılardan birini hedefler).
9. Bu simülasyon için **open ports** (açık kapılar) seçeneğini tıklatın ve 22 numaralı kapıyı ekleyin.
10. **protocols** (protokoller) öğesini tıklatın ve **TCP** seçeneğini belirleyin. SSH, TCP kullanır.
11. **OK** (Tamam) düğmesini tıklatın.
12. **Save Simulation** (Simülasyonu Kaydet) seçeneğini tıklatın.
13. **Actions** (İşlemler) listesinden **Run Simulation** (Simülasyonu Çalıştır) seçeneğini belirleyin. Sonuçlar sütunu, simülasyonun çalıştırıldığı tarihin ve sonuçları görüntülemeye yönelik bir bağlantının yer aldığı bir listeyi içerir.
14. **View Results** (Sonuçları Görüntüle) seçeneğini tıklatın.

Sonuçlar

Sonuçlarda, SSH güvenlik açıklarını içeren varlıkların bir listesi görüntülenerek ağ yöneticilerinin izin verilen ya da ağınızda beklenen SSH bağlantılarını onaylamasına olanak sağlar. Olaylar ya da hücumlar için onaylanmayan iletişimler izlenebilir.

Görüntülenen sonuçlar, ağ yöneticilerinize ya da güvenlik uzmanlarınıza, saldırının ağınızda kullanabileceği bağlantıların ve saldırı yolunun görsel bir gösterimini sunar. Örneğin, birinci adım, simülasyondan etkilenen doğrudan bağlı varlıkların bir listesini sağlar. İkinci adım, simülasyonunuzdaki birinci düzey varlıklarla iletişim kurabilen ağınızdaki varlıkları listeler.

Saldırıda sağlanan bilgiler, olası binlerce saldırı senaryosuna karşı ağınızı test etmenize ve güçlendirmenize olanak verir.

Kullanım senaryosu: Ağ yapılandırması değişiklikleri riskini simüle etme

Var olan ağınızı temel alarak sanal ağ modelleri tanımlamak için bir topoloji modeli kullanabilirsiniz. Birleştirilebilen ve yapılandırılabilen bir dizi değişikliği temel alan bir ağ modeli oluşturabilirsiniz.

Simülasyonu kullanarak yapılandırma değişikliklerinin ağınız üzerindeki etkisini belirlemek için bir topoloji modeli kullanabilirsiniz.

Topoloji modelleri aşağıdaki temel işlevselliği sağlar:

- Ağ değişikliklerini test etmek için sanal topolojiler oluşturma.
- Sanal ağlara karşı saldırıların simülasyonunu yapma.
- Test yoluyla, korunan varlıklar için riskleri ve güvenlik açıklarını azaltma.
- Sanal ağ kesimleri, varlıklarınızın ya da ağınızın hassas kısımlarını sınırlamanıza ve test etmenize olanak sağlar.

Bir ağ yapılandırması değişikliğinin simülasyonunu yapmak için:

1. Bir topoloji modeli oluşturun.
2. Topoloji modeline karşı bir saldırı simülasyonu gerçekleştirin.

Topoloji modeli oluşturma

Ağ değişikliklerini test etmek ve saldırıların simülasyonunu yapmak için bir topoloji modeli oluşturabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde, **Simulations** > **Topology Models** (Simülasyonlar - Topoloji Modelleri) seçeneklerini tıklatın.
3. **Actions** (İşlemler) listesinden **New** (Yeni) seçeneğini belirleyin.
4. Model için bir ad yazın.
5. Topolojiye uygulamak istediğiniz değişiklikleri seçin.
6. **Configure model as follows** (Modeli şu şekilde yapılandırın) bölmesine eklenen testleri yapılandırın.
7. **Save Model** (Modeli Kaydet) seçeneğini tıklatın.

Sonraki adım

Yeni topoloji modeliniz için bir simülasyon oluşturun.

Saldırıların simülasyonunu yapma

Kapılarda ve protokollerde saldırı simülasyonu yapabilirsiniz.

Yordam

1. **Risks** (Riskler) sekmesini tıklatın.
2. Gezinme menüsünde **Simulation > Simulations** (Simülasyon - Simülasyonlar) seçeneklerini belirleyin.
3. **Actions** (İşlemler) liste kutusundan **New** (Yeni) seçeneğini belirleyin.
4. Simülasyon için bir ad yazın.
5. Oluşturduğunuz bir topoloji modelini seçin.
6. **Where do you want the simulation to begin** (Simülasyonun nereden başlamasını istiyorsunuz?) listesinden, simülasyon için bir başlangıç noktası seçin.
7. Simülasyon saldırısını ekleyin, **Attack targets one of the following open ports using protocols** (Saldırı protokolleri kullanarak şu açık kapılardan birini hedefler).
8. Bu simülasyon için **open ports** (açık kapılar) seçeneğini tıklatın ve 22 numaralı kapıyı ekleyin.
9. **protocols** (protokoller) öğesini tıklatın ve TCP öğesini seçin. SSH, TCP kullanır.
10. **OK** (Tamam) seçeneğini tıklatın.
11. **Save Simulation** (Simülasyonu Kaydet) seçeneğini tıklatın.
12. **Actions** (İşlemler) listesinden **Run Simulation** (Simülasyonu Çalıştır) seçeneğini belirleyin. Sonuçlar sütunu, simülasyonun çalıştırıldığı tarihin ve sonuçları görüntüleme bağlantısının yer aldığı bir liste kutusunu içerir.
13. **View Results** (Sonuçları Görüntüle) seçeneğini tıklatın.

Bildirimler

Bu bilgiler, ABD'de kullanıma sunulan ürünler ve hizmetler için geliştirilmiştir.

IBM bu belgede sözü edilen ürün, hizmet ya da özellikleri diğer ülkelerde kullanıma sunmayabilir. Şu anda bölgenizde kullanılabilir olan ürünler ve hizmetlerle ilgili bilgiler için yerel IBM temsilcinizle görüşün. IBM ürünlerine, programlarına ya da hizmetlerine yapılan göndermeler yalnızca o IBM ürününün, programının ya da hizmetinin kullanılabileceğini göstermez. Aynı işlevi gören ve IBM'in fikri mülkiyet haklarına zarar vermeyen herhangi bir ürün, program ya da hizmet de kullanılabilir. Ancak IBM dışı kaynaklardan sağlanan ürün, program ya da hizmetlerle gerçekleştirilen işlemlerin değerlendirilmesi ve doğrulanması kullanıcının sorumluluğundadır.

IBM'in, bu belgedeki konularla ilgili patentleri ya da patent başvuruları olabilir. Bu belgenin size verilmiş olması, patentlerin izinsiz kullanım hakkının da verildiği anlamına gelmez. Lisansla ilgili sorularınızı aşağıdaki adrese yazabilirsiniz:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 ABD

Çift baytlı karakter kümesi (DBCS) bilgileriyle ilgili lisans sorgularınız için ülkenizde bulunan IBM Fikri Mülkiyet Bölümü'ne başvurun ya da sorgularınızı, yazılı olarak şu adrese gönderin:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japonya

İzleyen paragraf, bu tür kayıt ve koşulların, yasalarıyla bağdaşmadığı ülkeler ya da bölgeler için geçerli değildir:

IBM BU YAYINI, OLDUĞU GİBİ, HİÇBİR KONUDA AÇIK YA DA ÖRTÜK GARANTİ VERMEKSİZİN SAĞLAMAKTADIR; TİCARİ KULLANIMA UYGUNLUK AÇISINDAN HER TÜRLÜ GARANTİ VE BELİRLİ BİR AMACA UYGUNLUK İDDİASI AÇIKÇA REDDEDİLİR. Bazı ülkeler (ya da bölgeler) belirli işlemlerde açık ya da zımni garantilerin reddedilmesine izin vermezler; bu nedenle, bu açıklama sizin için geçerli olmayabilir.

Bu yayın teknik yanlışlar ya da yazım hataları içerebilir. Buradaki bilgiler düzenli aralıklarla güncellenir ve yayının yeni basımlarına eklenir. IBM, bu yayında açıklanan ürün(ler) ve/ya da program(lar) üzerinde herhangi bir zamanda geliştirmeler ve/ya da değişiklikler yapabilir.

Bu belgede sahibi IBM olmayan web sitelerine yapılan göndermeler kullanıcıya kolaylık sağlamak içindir ve bu web sitelerinin onaylanması anlamına gelmez. Bu web sitelerinin içerdiği malzeme, bu IBM ürününe ilişkin malzemenin bir parçası değildir ve bu tür web sitelerinin kullanılmasının sorumluluğu size aittir.

IBM, sağladığınız bilgilerden uygun bulduklarını, size herhangi bir sorumluluk yüklemeden kullanabilir ya da dağıtabilir.

Bu programın lisans sahipleri (i) bağımsız olarak yaratılan programlarla diğer programlar arasında (bu program da içinde olmak üzere) bilgi değiş tokuşunu ve (ii) değiş tokuş edilen bilginin karşılıklı kullanımını etkinleştirmek amacıyla bilgi edinmek için aşağıdaki adrese başvurmalıdırlar:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451 ABD

Bu tür bilgiler, ilgili kayıt ve koşullar altında ve bazı durumlarda bedelli olarak edinilebilir.

Bu belgede açıklanan lisanslı program ve bu programla birlikte kullanılabilecek tüm lisanslı malzemeler, IBM Müşteri Sözleşmesi, IBM Uluslararası Program Lisans Sözleşmesi ya da eşdeğer herhangi bir sözleşmenin koşulları kapsamında IBM tarafından sağlanır.

Burada belirtilen başarım verileri denetimli bir ortamda elde edilmiştir. Bu nedenle, başka işletim ortamlarında çok farklı sonuçlar alınabilir. Bazı ölçümler, geliştirme düzeyindeki sistemlerde yapılmış olabilir ve bu ölçümlerin, kullanımınıza sunulan sistemlerde aynı olacağı konusunda herhangi bir garanti verilemez. Bununla birlikte, bazı ölçümler de verilere dayalı tahmin yoluyla hesaplanmıştır. Gerçek sonuçlar değişiklilik gösterebilir. Bu belgenin kullanıcıları kendi ortamları için geçerli verileri kendileri doğrulamalıdırlar.

IBM dışı ürünlerle ilgili bilgiler, bu ürünleri sağlayan firmalardan, bu firmaların yayın ve belgelerinden ve genel kullanıma açık diğer kaynaklardan alınmıştır. IBM bu ürünleri sınamamıştır ve IBM dışı ürünlerle ilgili başarım, uyumluluk gibi iddiaları doğrulayamaz. IBM dışı ürünlerin yetenekleriyle ilgili sorular, bu ürünlerin sağlayıcılarına yöneltilmelidir.

IBM'in gelecekteki yönelim ve kararlarına ilişkin tüm bildirimler değişebilir ve herhangi bir duyuruda bulunulmadan bunlardan vazgeçilebilir; bu yönelim ve kararlar yalnızca amaç ve hedefleri gösterir.

Gösterilen tüm IBM fiyatları önerilen perakende satış fiyatlarıdır, günceldir ve bildirimde bulunulmaksızın değiştirilebilir. Yetkili bayi fiyatları farklı olabilir.

Bu belge, günlük iş ortamında kullanılan veri ve raporlara ilişkin örnekler içerir. Örneklerin olabildiğince açıklayıcı olması amacıyla kişi, şirket, marka ve ürün adları belirtilmiş olabilir. Bu adların tümü gerçek dışıdır ve gerçek iş ortamında kullanılan ad ve adreslerle olabilecek herhangi bir benzerlik tümüyle rastlantıdır.

Bu belgenin elektronik kopyasına bakıyorsanız, fotoğraflar ve renkli resimler görünmeyebilir.

Ticari Markalar

IBM, IBM logosu ve ibm.com, International Business Machines Corporation (IBM) firmasının ABD'de ve/ya da diğer ülkelerdeki ticari markaları ya da tescilli ticari markalarıdır. Bunlar ve IBM'in ticari markasını taşıyan diğer terimler, bu belgede geçtikleri ilk yerde ticari marka simgesiyle (® ya da ™) gösteriliyorsa, bu simgeler bu bilgilerin yayınlandığı sırada IBM'in sahibi olduğu, ABD'de tescilli ya da özel hukuka tabi ticari markaları belirtir. Bu ticari markalar başka ülkelerde tescilli veya genel hukuk ticari markası da olabilir. IBM ticari markalarının güncel listesini Web üzerinde şu adreste bulabilirsiniz: Telif hakkı ve ticari marka bilgileri (www.ibm.com/legal/copytrade.shtml).

Microsoft, Windows, Windows NT ve Windows logosu, Microsoft Corporation firmasının ABD'de ve/ya da diğer ülkelerdeki ticari markalarıdır.

Diğer şirket, ürün ve hizmet adları, diğer firmalara ait ticari marka ya da hizmet markaları olabilir.

Gizlilik ilkesiyle ilgili önemli noktalar

Hizmet olarak yazılım çözümleri de dahil olmak üzere IBM Yazılım ürünleri ("Yazılım Ürünleri"), ürün kullanımı bilgilerini toplamak, son kullanıcı deneyiminin geliştirilmesine yardımcı olmak ve son kullanıcıyla etkileşimleri veya diğer amaçlar için etkileşimleri uyarlamak için tanımlama bilgilerini ya da diğer teknolojileri kullanabilir. Yazılım Ürünleri çoğu durumda kimlik bilgilerini toplamaz. Yazılım Ürünlerimiz'den bazıları kimlik bilgileri toplamanızı sağlamaya yardımcı olabilir. Bu Yazılım Ürünü kişisel olarak tanımlanabilir bilgileri toplamak için tanımlama bilgileri kullanıyorsa, bu ürünün tanımlama bilgileri kullanımıyla ilgili birtakım bilgiler aşağıda sağlanmıştır.

Devreye alınan yapılandırmalara bağlı olarak bu Yazılım Ürünü, oturum yönetimi ve kimlik doğrulama amacıyla her bir kullanıcının oturum tanıtıcısını toplayan oturum tanımlama bilgilerini kullanabilir. Bu tanımlama bilgileri devre dışı bırakılabilir, ancak bunlar devre dışı bırakıldığında etkinleştirdikleri işlevsellik de ortadan kaldırılır.

Bu Yazılım Ürünü için devreye alınan yapılandırmalar, müşteri olarak size tanımlama bilgileri ve diğer teknolojiler aracılığıyla son kullanıcıların kişisel bilgilerini toplama olanağı sağlıyorsa, bildirme ve rıza zorunluluğu da içinde olmak üzere, veri toplanmasıyla ilgili yasalar için hukuki görüş almanız gerekmektedir.

Tanımlama bilgileri de dahil, bu amaçla kullanılan çeşitli teknolojiler hakkında daha fazla bilgi için http://www.ibm.com/privacy adresindeki IBM'in Gizlilik İlkesi'ne ve http://www.ibm.com/privacy/details adresindeki IBM'in Çevrimiçi Gizlilik Bildirimi'ne, http://www.ibm.com/software/info/product-privacy adresindeki "Cookies, Web Beacons and Other Technologies" ve "IBM Software Products and Software-as-a-Service Privacy Statement" başlıklı bölümlere bakabilirsiniz.

Dizin

Sayısallar

A

B

Ç

D

G

H

I

İ

K

M

N

O

Ö

P

Q

R

S

Ş

T

U

V

W

Y