IBM Security QRadar SIEM
Sürüm 7.2.4

Başlangıç Kılavuzu

Not

Bu belgeyi ve desteklediği ürünü kullanmadan önce şu bilgileri okuyun: “Bildirimler” sayfa 23.

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

QRadar SIEM ürünüyle çalışmaya başlama - giriş

IBM Security QRadar SIEM Başlangıç Kılavuzu size temel kavramları, kuruluş işlemine genel bakışı ve kullanıcı arabiriminde gerçekleştirdiğiniz temel görevleri tanıtır.

Hedef kitle

Bu bilgiler, ağ güvenliğini araştırmak ve yönetmekten sorumlu olan güvenlik yöneticileri tarafından kullanılmak üzere tasarlanmıştır. Bu kılavuzu kullanmak için, kurumsal ağ altyapınızı ve ağ teknolojilerini bilmeniz gerekir.

Teknik belgeler

Daha fazla teknik belgeye, teknik notlara ve sürüm notlarına nasıl erişileceği hakkında bilgi için bkz. Accessing IBM® Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Müşteri desteği ile iletişim kurma

Müşteri desteği ile iletişim kurma hakkında bilgi için bkz. Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

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. QRadar SIEM - genel bakış

IBM Security QRadar SIEM, durumsal farkındalık ve uyumluluk desteği sağlayan bir ağ güvenliği yönetim platformudur. QRadar SIEM, akış tabanlı ağ bilgisi, güvenlik olayı ilintilendirmesi ve varlık temelli güvenlik açığı değerlendirmesi birleşimini kullanır.

Başlamak için bir temel QRadar SIEM kuruluşunu yapılandırın, olay ve akış verilerini toplayın ve raporlar oluşturun.

Günlük etkinliği

IBM Security QRadar SIEM uygulamasında ağ olaylarını gerçek zamanlı izleyip görüntüleyebilir ya da gelişmiş aramalar gerçekleştirebilirsiniz.

Log Activity (Günlük Etkinliği) sekmesi, güvenlik duvarı ya da yönlendirici aygıtı gibi bir günlük kaynağından kayıtlar gibi olay bilgilerini görüntüler. **Log Activity** (Günlük Etkinliği) sekmesini kullanarak aşağıdaki görevleri gerçekleştirebilirsiniz:

- Olay verilerini araştırma.
- QRadar SIEM uygulamasına gerçek zamanlı olarak gönderilen olay günlüklerini araştırma.
- Olay arama.
- Yapılandırılabilir zaman serisi grafiklerini kullanarak günlük etkinliğini izleme.
- QRadar SIEM uygulamasını ayarlamak için yanlış pozitifleri belirleme.

Ağ etkinliği

IBM Security QRadar SIEM uygulamasında, iki anasistem arasındaki iletişimi araştırabilirsiniz.

Network Activity (Ağ Etkinliği) sekmesi, ağ trafiğinin nasıl iletileceği ve içerik yakalama seçeneği etkinleştirildiyse nelerin iletildiği ile ilgili bilgileri görüntüler. **Network Activity** (Ağ Etkinliği) sekmesini kullanarak aşağıdaki görevleri gerçekleştirebilirsiniz:

- QRadar SIEM uygulamasına gerçek zamanlı olarak gönderilen akışları araştırma.
- Ağ akışlarını arama.
- Yapılandırılabilir zaman serisi grafiklerini kullanarak ağ etkinliğini izleme.

Varlıklar

QRadar SIEM, ağ sunucularınızı ve anasistemlerinizi keşfetmek için pasif akış verilerini ve güvenlik açığı verilerini kullanarak otomatik olarak varlık profilleri oluşturur.

Varlık profilleri, çalıştırılan hizmetler de dahil, ağınızdaki her bir bilinen varlıkla ilgili bilgi sağlar. Varlık profili bilgileri, ilintilendirme amacıyla kullanılır ve yanlış pozitiflerin azaltılmasına yardımcı olur.

Assets (Varlıklar) sekmesini kullanarak aşağıdaki görevleri gerçekleştirebilirsiniz:

- Varlıkları arama.
- Tüm öğrenilen varlıkları görüntüleme.
- Öğrenilen varlıklar için kimlik bilgilerini görüntüleme.
- Yanlış pozitif güvenlik açıklarını ayarlama.

Hücumlar

IBM Security QRadar SIEM ürününde, bir ağ sorununun asıl nedenini belirlemek için hücumları araştırabilirsiniz.

Offenses (Hücumlar) sekmesini kullanarak, ağınızda oluşan tüm hücumları görüntüleyebilir ve aşağıdaki görevleri tamamlayabilirsiniz:

- Ağınızdaki anormallikleri, ağ davranışlarını, kaynak ve hedef IP adreslerini ve hücumları araştırma.
- Birden çok ağdan kaynaklanan olay ve akışları aynı hedef IP adresine ilintilendirme.
- **Offenses** (Hücumlar) sekmesinin çeşitli sayfalarına gidip olay ve akış ayrıntılarını araştırma.
- Bir hücuma neden olan benzersiz olayları belirleme.

Raporlar

IBM Security QRadar SIEM uygulamasında özel raporlar oluşturabilir ya da varsayılan raporları kullanabilirsiniz.

QRadar SIEM, özelleştirebileceğiniz, yeniden markalayabileceğiniz ve QRadar SIEM kullanıcılarına dağıtabileceğiniz varsayılan rapor şablonları sağlar.

Rapor şablonları; uyumluluk, aygıt, yönetici ve ağ raporları gibi rapor tipleri halinde gruplanır. Aşağıdaki görevleri tamamlamak için **Reports** (Raporlar) sekmesini kullanın:

- QRadar SIEM verileri için raporlar oluşturma, dağıtma ve yönetme.
- İşletim ve yönetici kullanımı için özelleştirilmiş raporlar oluşturma.
- Güvenlik ve ağ bilgilerini tek bir raporda birleştirme.
- Önceden kurulu rapor şablonlarını kullanma ya da düzenleme.
- Raporlarınızı özelleştirilmiş logolarla markalaştırma. Markalaştırma, raporların farklı kitlelere dağıtılması için yararlıdır.
- Özel ve varsayılan raporlar oluşturmaya yönelik zamanlama ayarlama.
- Raporları çeşitli biçimlerde yayınlama.

Veri toplama

QRadar SIEM, çeşitli biçimlerde ve çok çeşitli aygıtlardan gelen güvenlik olayları, ağ trafiği ve tarama sonuçları gibi bilgileri kabul eder.

Toplanan veriler üç ana bölüm olarak kategorilere ayrılır: olaylar, akışlar ve güvenlik açığı değerlendirme bilgileri.

Olay verilerini toplama

Olaylar; güvenlik duvarları, yönlendiriciler, sunucular ve izinsiz giriş algılama sistemleri (IDS) ya da izinsiz giriş engelleme sistemleri (IPS) gibi günlük kaynakları tarafından oluşturulur.

Çoğu günlük kaynakları, sistem günlüğü protokolünü kullanarak QRadar SIEM ürününe bilgi gönderir. QRadar SIEM aşağıdaki protokolleri de destekler:

- Basit Ağ Yönetimi Protokolü (SNMP)
- Java™ veritabanı bağlantısı (JDBC)
- Güvenlik Aygıtı Olayı Değişimi (SDEE)

Varsayılan olarak QRadar SIEM, belirli bir zaman çerçevesi içinde belirli sayıda tanımlanabilir günlük alındıktan sonra otomatik olarak günlük kaynaklarını algılar. Günlük kaynakları başarıyla algılandıktan sonra QRadar SIEM, **Admin** (Yönetim) sekmesinde Log Sources (Günlük Kaynakları) penceresine uygun aygıt desteği modülünü (DSM) ekler.

Çoğu DSM'ler yerel günlük gönderme yeteneği içerse de birçok DSM, günlükleri göndermek için fazladan yapılandırma, aracı ya da her ikisini gerektirir. DSM tipleri arasında yapılandırma değişiklik gösterir. DSM'lerin, QRadar SIEM ürününün desteklediği bir biçimde günlükleri gönderecek şekilde yapılandırıldığından emin olmanız gerekir. DSM'leri yapılandırma hakkında daha fazla bilgi için *DSM Configuration Guide* adlı yayına bakın.

Yönlendiriciler ve anahtarlar gibi belirli günlük kaynağı tipleri, QRadar SIEM ürününün günlükleri hızlı şekilde algılaması ve Log Source (Günlük Kaynağı) listesine eklemesi için yeterli günlük göndermez. Bu günlük kaynaklarını el ile ekleyebilirsiniz. Günlük kaynaklarını el ile ekleme hakkında daha fazla bilgi için *Log Sources User Guide* başlıklı yayına bakın.

Toplanan veriler üç ana bölüm olarak kategorilere ayrılır: olaylar, akışlar ve güvenlik açığı değerlendirme (VA) bilgileri.

Akış verilerini toplama

Akışlar, ağ trafiği hakkında bilgi sağlar ve QRadar SIEM ürününe akış günlüğü dosyaları, NetFlow, J-Flow, sFlow ve Packeteer gibi çeşitli biçimlerde gönderilebilir.

Aynı anda birden çok akış biçimini kabul ederek QRadar SIEM, bilgi için tamamen olaylara güvenilmesi durumunda gözden kaçırılabilecek olan tehditleri ve etkinlikleri algılayabilir.

QRadar QFlow Collectors, uygulamanın hangi kapıda çalıştığına bakılmaksızın ağ trafiğinin tam uygulama algılamasını sağlar. Örneğin, Internet Relay Chat (IRC) protokolü 7500/TCP kapısında iletişim kuruyorsa QRadar QFlow Collector, trafiği IRC olarak belirler ve görüşmenin başına ait bir paket yakalaması sağlar. NetFlow ve J-Flow, hangi protokolün kullanıldığına ilişkin herhangi bir bağlam sağlamadan 7500/TCP kapısında trafik olduğunu size bildirir.

Genel ikiz kapı konumları, çekirdek, DMZ, sunucu ve uygulama anahtarlarını içerir; NetFlow, sınır yönlendiricileri ve anahtarlardan ek bilgi sağlar.

QRadar QFlow Collectors varsayılan olarak etkindir ve QRadar SIEM aracında kullanılabilir bir arabirime bağlanması için bir ikiz, aralık ya da musluk gerekir. Akış kapısı, QRadar SIEM aracında ağ arabirimlerinden birine bağlandığında akış analizi otomatik olarak başlar. Varsayılan olarak QRadar SIEM, 2055/UDP kapısında NetFlow trafiği için yönetim arabirimini izler. Gerekirse fazladan NetFlow kapısı atayabilirsiniz.

Güvenlik açığı değerlendirme bilgileri

QRadar SIEM, çeşitli üçüncü taraf tarayıcılardan VA bilgilerini içe aktarabilir.

VA bilgileri, QRadar Risk Manager uygulamasının etkin anasistemleri, açık kapıları ve olası güvenlik açıklarını belirlemesine yardımcı olur.

QRadar Risk Manager, ağınızdaki hücumların büyüklüğünü derecelendirmek için VA bilgilerini kullanır.

VA tarayıcı tipine bağlı olarak QRadar Risk Manager, tarayıcı sunucusundan tarama sonuçlarını içe aktarabilir ya da uzaktan bir tarama başlatabilir.

QRadar SIEM kuralları

Kurallar, bir testin tüm koşulları karşılanırsa olaylar, akışlar ya da hücumlar üzerinde testler gerçekleştirir, kural bir yanıt oluşturur.

QRadar SIEM; çok sayıda güvenlik duvarı engellemeleri, birden çok başarısız oturum açma girişimi ve olası botnet etkinliği gibi çok çeşitli etkinlikleri algılayan kuralları içerir. Kurallar hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Aşağıdaki liste iki kural kategorisini açıklar:

- Özel kurallar, ağınızdaki olağan dışı etkinliği algılamak için olaylar, akışlar ve hücumlar üzerinde testler gerçekleştirir.
- Anormallik algılama kuralları, olağan dışı trafik kalıplarının ne zaman oluştuğunu algılamak için kayıtlı akış ya da olay aramalarının sonuçları üzerinde testler gerçekleştirir.

Önemli: Yönetici dışı erişime sahip bir kullanıcı, erişebildiği ağ alanları için kurallar oluşturabilir. Kuralları yönetmek için uygun rol izinlerine sahip olmanız gerekir. Kullanıcı rolü izinleri hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Desteklenen web tarayıcıları

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

QRadar sistemine eriştiğinizde sizden bir kullanıcı adı ve parola istenir. Kullanıcı adı ve parola, sistem yöneticisi tarafından önceden 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
Belge kipi ve tarayıcı kipi etkinleştirilmiş şekilde 32 bitlik Microsoft Internet Explorer	9.0 10
Google Chrome	IBM Security QRadar V7.2.4 ürünlerinin yayın tarihinden itibaren geçerli sürüm

Bölüm 2. QRadar SIEM devreye alımını başlatma

IBM Security QRadar SIEM temel yeteneklerini değerlendirebilmeniz için önce bir yönetici QRadar SIEM olanağını devreye almalıdır.

QRadar SIEM olanağını devreye almak için yöneticiler aşağıdaki görevleri gerçekleştirmelidir:

- QRadar SIEM aracını kurma.
- QRadar SIEM kuruluşunuzu yapılandırma.
- Olay, akış ve güvenlik açığı değerlendirmesi (VA) verilerini toplama.
- QRadar SIEM kuruluşunuzu ayarlama.

QRadar SIEM aracını kurma

Sistem yöneticileri, kullanıcı arabirimine erişimi etkinleştirmek için QRadar SIEM aracını kurmalıdır.

Başlamadan önce

QRadar SIEM değerlendirme aracını kurmadan önce aşağıdakilere sahip olduğunuzdan emin olun:

- İki birimli araç için alan.
- Raf rayları ve raflar (monte edilmiş).
- İsteğe bağlıdır. Konsol erişimi için USB klavye ve standart VGA monitör.

Yordam

1. Yönetim ağ arabirimini Ethernet 1 etiketli kapıya bağlayın.
2. Özel olarak ayrılan güç bağlantılarını, aracın arkasına takın.
3. Konsol erişimine ihtiyacınız olursa, USB klavyeyi ve standart VGA monitörü bağlayın.
4. Araçta bir ön panel varsa. Herhangi bir taraftaki tırnaklara bastırarak paneli çıkarın ve paneli araçtan çekip çıkarın.
5. Aracı açın.

QRadar SIEM aracı

QRadar SIEM değerlendirme aracı, iki birimli raf düzenekli bir sunucudur. Raf rayları ve raflar, değerlendirme ekipmanı ile birlikte sağlanmaz.

QRadar SIEM aracı, dört ağ arabirimi içerir. Bu değerlendirme için, yönetim arabirimi olarak Ethernet 1 etiketli olan arabirimi kullanın.

Akış toplama için kalan üç izleme arabirimini kullanabilirsiniz. QRadar QFlow Collector, tam ağ uygulama analizi sağlar ve her bir görüşmenin başında paket yakalama işlemleri gerçekleştirebilir. QRadar SIEM aracına bağlı olarak, bir aralık kapısı ya da musluğu, Ethernet 1 dışında bir arabirime bağlandığında otomatik olarak başlar. QRadar SIEM içinde QRadar QFlow Collector bileşenini etkinleştirmek için fazladan adımlar gerekebilir.

Daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Sınırlama: QRadar SIEM değerlendirme aracı, akış analizi için 50 Mbps sınıra sahiptir. Akış toplama için izleme arabirimlerinde toplama trafiğinin 50 Mbps'yi aşmadığından emin olun.

QRadar SIEM yapılandırması

QRadar SIEM uygulamasını yapılandırarak ağ sıradüzeninizi gözden geçirebilir ve otomatik güncellemeleri özelleştirebilirsiniz.

Yordam

1. QRadar ürün kullanıcı arabirimine erişmek için kullandığınız tüm masaüstü sistemlerinde aşağıdaki uygulamaların kurulu olduğundan emin olun:
   - Java Runtime Environment (JRE) sürüm 1.7 ya da IBM 64-bit Runtime Environment for Java V7.0
   - Adobe Flash sürüm 10.x
2. Desteklenen bir web tarayıcısı kullandığınızdan emin olun. Bkz. “Desteklenen web tarayıcıları” sayfa 4.
3. Internet Explorer kullanıyorsanız belge kipini ve tarayıcı kipini etkinleştirin.
   a. Internet Explorer web tarayıcınızda, Developer Tools (Geliştirici Araçları) penceresini açmak için F12 tuşuna basın.
   b. **Browser Mode** (Tarayıcı Kipi) öğesini tıklatın ve web tarayıcınızın sürümünü seçin.
   c. **Document Mode** (Belge Kipi) öğesini tıklatın ve **Internet Explorer 7.0 Standards** (Internet Explorer 7.0 Standartları) seçeneğini belirleyin.
4. Şu URL'yi yazarak QRadar SIEM kullanıcı arabiriminde oturum açın:

   https://<IP Adresi>

   Burada <IP Adresi>, QRadar SIEM Console olanağının IP adresidir.

Ağ sıradüzeni

İş işlevine göre düzenlenen ağınızın farklı alanlarını görüntüleyebilir, tehdit ve ilke bilgilerini iş değeri riskine göre önceliklendirebilirsiniz.

QRadar SIEM aşağıdaki görevleri gerçekleştirmek için ağ sıradüzenini kullanır:

- Ağ trafiğini anlama ve ağ etkinliğini görüntüleme.
- Pazarlama, DMZ ya da VoIP gibi ağınızdaki belirli mantıksal grupları veya hizmetleri izleme.
- Trafiği izleme ve grup içinde her bir grup ve anasistemin davranış profilini çıkarma.
- Yerel ve uzak anasistemleri belirleme ve tanımlama.

Değerlendirme amacıyla, önceden tanımlanmış mantıksal grupları içeren bir ağ sıradüzeni dahil edilmiştir. Ağ sıradüzeninin doğru ve tam olup olmadığını gözden geçirin. Ortamınız, önceden yapılandırılan ağ sıradüzeninde görüntülenmeyen ağ aralıkları içeriyorsa bunları el ile eklemeniz gerekir.

Ağ sıradüzeninizde tanımlanan nesnelerin ortamınızda fiziksel olarak bulunması gerekmez. Altyapınıza ait olan tüm mantıksal ağ aralıkları bir ağ nesnesi olarak tanımlanmalıdır.

Not: Sisteminiz tamamlanmış bir ağ sıradüzeni içermiyorsa, ortamınıza özgü bir sıradüzen oluşturmak için **Admin** (Yönetim) sekmesini kullanın.

Daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Ağ sıradüzeninizi gözden geçirme

Ağ sıradüzeninizi gözden geçirebilirsiniz.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme bölmesinde **System Configuration** (Sistem Yapılandırması) öğesini tıklatın.
3. **Network Hierarchy** (Ağ Sıradüzeni) simgesini tıklatın.
4. **Manage Group:Top** (Grubu Yönet:Üst) listesinde **Regulatory_Compliance_Servers** (Yasal_Uyumluluk_Sunucuları) seçeneğini tıklatın.

   Ağ sıradüzeniniz bir yasal uyumluluk sunucusu bileşeni içermiyorsa, bu yordamın geri kalanında Posta bileşeninizi kullanabilirsiniz.
5. **Edit this object** (Bu nesneyi düzenle) simgesini tıklatın.
6. Uyumluluk sunucuları eklemek için:
   a. **IP/CIDR(s)** (IP/CIDR(ler)) alanına uyumluluk sunucularınızın IP adresini ya da CIDR aralığını yazın.
   b. **Add** (Ekle) düğmesini tıklatın.
   c. Tüm uyumluluk sunucuları için yineleyin.
   d. **Save** (Kaydet) seçeneğini tıklatın.
   e. Düzenlemek istediğiniz diğer ağlar için bu işlemi yineleyin.
7. **Admin** (Yönetim) sekme menüsünde **Deploy Changes** (Değişiklikleri Devreye Al) seçeneğini tıklatın.

   En son ağ güvenliği bilgileri ile yapılandırma dosyalarınızı otomatik olarak ya da el ile güncelleyebilirsiniz. QRadar SIEM, ağ veri akışlarının kullanışlı nitelendirmelerini sağlamak üzere sistem yapılandırma dosyalarını kullanır.

Otomatik güncellemeler

QRadar SIEM konsolu, güncellemeleri almak için İnternet'e bağlı olmalıdır. Konsolunuz İnternet'e bağlı değilse bir dahili güncelleme sunucusunu yapılandırmanız gerekir.

Otomatik güncelleme sunucusunu ayarlama hakkında bilgi için bkz. *IBM Security QRadar SIEM Users Guide*.

QRadar SIEM uygulamasını kullanarak, var olan yapılandırma dosyalarınızı değiştirebilir ya da güncellenmiş dosyaları var olan dosyalarla bütünleştirebilirsiniz.

Yazılım güncellemeleri aşağıdaki web sitesinden yüklenebilir:

http://www.ibm.com/support/fixcentral/

Güncelleme dosyaları aşağıdaki güncellemeleri içerebilir:

- Yapılandırma dosyası değişiklikleri, güvenlik açığı, QID eşlemesi ve güvenlik tehdidi bilgileri güncellemelerini içeren yapılandırma güncellemeleri.
- Protokol güncellemeleri, tarayıcı değişiklikleri ve ayrıştırma sorunlarına yönelik düzeltmeleri içeren DSM güncellemeleri.
- Güncellenmiş JAR dosyaları gibi öğeleri içeren ana güncellemeler.
- Ek çevrimiçi yardım içeriği ya da güncellenmiş komut dosyaları gibi öğeleri içeren ikincil güncellemeler.

Otomatik güncelleme ayarlarını yapılandırma

QRadar SIEM güncellemelerinin sıklığını, güncelleme tiplerini, sunucu yapılandırmasını ve yedekleme ayarlarını özelleştirebilirsiniz.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme bölmesinde **System Configuration** (Sistem Yapılandırması) öğesini tıklatın.
3. **Auto Update** (Otomatik Güncelle) simgesini tıklatın.
4. Gezinme bölmesinde **Change Settings** (Ayarları Değiştir) öğesini tıklatın.
5. **Auto Update Schedule** (Otomatik Güncelleme Zamanlaması) bölmesinde varsayılan parametreleri kabul edin.
6. **Update Types** (Güncelleme Tipleri) bölmesinde aşağıdaki parametreleri yapılandırın:
   a. **Configuration Updates** (Yapılandırma Güncellemeleri) liste kutusunda **Auto Update** seçeneğini belirleyin.
   b. Aşağıdaki parametreler için varsayılan değerleri kabul edin:
      - DSM, Tarayıcı, Protokol Güncellemeleri.
      - Ana Güncellemeler.
      - İkincil Güncellemeler.
7. **Auto Deploy** (Otomatik Devreye Al) onay kutusunun işaretini kaldırın.

   Varsayılan olarak onay kutusu seçilir. Onay kutusu seçilmezse, güncellemeler kaldırıldıktan sonra değişiklikleri devreye almanız gerektiğini belirtmek için **Dashboard** (Gösterge Panosu) sekmesinde bir sistem bildirimi görüntülenir.
8. **Advanced** (Gelişmiş) sekmesini tıklatın.
9. **Server Configuration** (Sunucu Yapılandırması) bölmesinde varsayılan parametreleri kabul edin.
10. **Other Settings** (Diğer Ayarlar) bölmesinde varsayılan parametreleri kabul edin.
11. **Save** (Kaydet) seçeneğini tıklatın ve Updates (Güncellemeler) penceresini kapatın.
12. Araç çubuğunda **Deploy Changes** (Değişiklikleri Devreye Al) öğesini tıklatın.

Olayları toplama

Olayları toplayarak, QRadar SIEM olanağına gerçek zamanlı gönderilen günlükleri araştırabilirsiniz.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme bölmesinde **Data Sources** (Veri Kaynakları) öğesini tıklatın.
3. **Log Sources** (Günlük Kaynakları) simgesini tıklatın.
4. Günlük kaynakları listesini gözden geçirin ve günlük kaynağı üzerinde gerekli değişiklikleri yapın.

   Günlük kaynaklarını yapılandırma hakkında bilgi için bkz. *Günlük Kaynakları Kullanıcı Kılavuzu*.
5. Log Sources (Günlük Kaynakları) penceresini kapatın.
6. **Admin** (Yönetim) sekme menüsünde **Deploy Changes** (Değişiklikleri Devreye Al) seçeneğini tıklatın.

Akışları toplama

Akışları toplayarak anasistemler arasındaki ağ iletişimi oturumlarını araştırabilirsiniz.

Anahtarlar ve yönlendiriciler gibi üçüncü taraf ağ aygıtlarında akışların nasıl etkinleştirileceği hakkında daha fazla bilgi için satıcı belgelerinize bakın.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Data Sources > Flows** (Veri Kaynakları - Akışlar) seçeneklerini tıklatın.
3. **Flow Sources** (Akış Kaynakları) simgesini tıklatın.
4. Akış kaynakları listesini gözden geçirin ve akış kaynakları üzerinde gerekli değişiklikleri yapın.

   Akış kaynaklarını yapılandırma hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.
5. Flow Sources (Akış Kaynakları) penceresini kapatın.
6. **Admin** (Yönetim) sekme menüsünde **Deploy Changes** (Değişiklikleri Devreye Al) seçeneğini tıklatın.

Güvenlik açığı değerlendirme bilgilerini içe aktarma

Güvenlik açığı değerlendirme (VA) bilgilerini içe aktararak etkin anasistemleri, açık kapıları ve olası güvenlik açıklarını belirleyebilirsiniz.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme menüsünde **Data Sources > Vulnerability** (Veri Kaynakları - Güvenlik Açığı) seçeneklerini tıklatın.
3. **VA Scanners** (VA Tarayıcıları) simgesini tıklatın.
4. Araç çubuğunda **Add** (Ekle) öğesini tıklatın.
5. Parametre değerlerini girin.

   Parametreler, eklemek istediğiniz tarayıcı tipine bağlıdır. Daha fazla bilgi için bkz. *Güvenlik Açığı Değerlendirme Yapılandırma Kılavuzu*.

   Önemli: CIDR Aralığı, hangi ağların QRadar SIEM tarama sonuçlarında bütünleştirileceğini belirtir. Örneğin, 192.168.0.0/16 ağına karşı bir tarama yürütmek istiyorsanız ve CIDR aralığı olarak 192.168.1.0/24 değerini belirtmek istiyorsanız yalnızca 192.168.1.0/24 aralığındaki sonuçlar bütünleştirilir.
6. **Save** (Kaydet) seçeneğini tıklatın.
7. **Admin** (Yönetim) sekme menüsünde **Deploy Changes** (Değişiklikleri Devreye Al) seçeneğini tıklatın.
8. **Schedule VA Scanners** (VA Tarayıcılarını Zamanla) simgesini tıklatın.
9. **Add** (Ekle) düğmesini tıklatın.
10. Taramanın ne sıklıkla oluşmasını istediğinize ilişkin ölçütleri belirtin.

    Tarama tipine bağlı olarak bu, QRadar SIEM uygulamasının tarama sonuçlarını ne sıklıkla içe aktardığını ve yeni bir tarama başlattığını içerir. Tarama sonuçlarına dahil edilecek kapıları da belirtmeniz gerekir.
11. **Save** (Kaydet) seçeneğini tıklatın.

QRadar SIEM uygulamasını ayarlama

QRadar SIEM uygulamasını ortamınızın gereksinimlerini karşılayacak şekilde ayarlayabilirsiniz.

QRadar SIEM uygulamasını ayarlamadan önce, ağınızdaki sunucuları algılamak, olay ve akışları saklamak ve var olan kuralları temel alan hücumlar oluşturmak üzere QRadar SIEM uygulamasını etkinleştirmek için bir gün bekleyin.

Sistem yöneticileri aşağıdaki ayarlama görevlerini gerçekleştirebilir:

- **Log Activity** (Günlük Etkinliği) ve **Network Activity** (Ağ Etkinliği) **Quick Filter** (Hızlı Süzgeç) özelliğinde bir yük dizinini etkinleştirerek olay ve akış yükü aramalarını iyileştirme.
- Otomatik olarak ya da el ile sunucuları yapı taşlarına ekleyerek daha hızlı başlangıç devreye alımı ve daha kolay ayarlama sağlama.
- Özel kurallar ve anormallik algılama kuralları oluşturarak ya da değiştirerek olay, akış ve hücum koşullarına yönelik yanıtlar yapılandırma.
- Ağdaki her bir anasistemin, en güncel kuralları, keşfedilen sunucuları ve ağ sıradüzenini temel alan hücumlar oluşturduğundan emin olma.

Bilgi yükü dizini oluşturma

Olay ve akış yüklerini aramak için **Log Activity** (Günlük Etkinliği) ve **Network Activity** (Ağ Etkinliği) sekmelerinde bulunan **Quick Filter** (Hızlı Süzgeç) işlevini kullanın.

Quick Filter (Hızlı Süzgeç) öğesini iyileştirmek için bir yük dizini **Quick Filter** (Hızlı Süzgeç) özelliğini etkinleştirebilirsiniz.

Yük dizini oluşturma seçeneği etkinleştirildiğinde sistem performansı düşebilir. **Quick Filter** (Hızlı Süzgeç) özelliğinde yük dizini oluşturmayı etkinleştirdikten sonra dizin istatistiklerini izleyin.

Dizin yönetimi ve istatistikler hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Bilgi yükü dizini oluşturmayı etkinleştirme

Log Activity (Günlük Etkinliği) ve **Network Activity** (Ağ Etkinliği) **Quick Filter** (Hızlı Süzgeç) özelliğinde bilgi yükü dizinini etkinleştirerek olay ve akış bilgi yükü aramalarını iyileştirebilirsiniz.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.
2. Gezinme bölmesinde **System Configuration** (Sistem Yapılandırması) öğesini tıklatın.
3. **Index Management** (Dizin Yönetimi) simgesini tıklatın.
4. **Quick Search** (Hızlı Arama) alanına **Quick Filter** (Hızlı Süzgeç) yazın.
5. Dizin oluşturmak istediğiniz **Quick Filter** (Hızlı Süzgeç) özelliğini tıklatın.
6. **Enable Index** (Dizini Etkinleştir) öğesini tıklatın.
7. **Save** (Kaydet) seçeneğini tıklatın.
8. **OK** (Tamam) düğmesini tıklatın.
9. İsteğe bağlı: Bilgi yükü dizinini devre dışı bırakmak için aşağıdaki seçeneklerden birini seçin:
   - **Disable Index** (Dizini Devre Dışı Bırak) seçeneğini tıklatın.
   - Bir özelliği sağ tıklatın ve menüden **Disable Index** (Dizini Devre Dışı Bırak) seçeneğini belirleyin.

Sonraki adım

Index Management (Dizin Yönetimi) penceresinde görüntülenen parametreler hakkında ayrıntılı bilgiler için bkz. *IBM Security QRadar SIEM Administration Guide*.

Sunucular ve yapı taşları

QRadar SIEM, ağınızdaki sunucuları otomatik olarak keşfedip sınıflandırarak daha hızlı başlangıç devreye alımı ve ağ değişiklikleri oluştuğunda daha kolay ayarlama sağlar.

Sunucu tipine uygun kuralların uygulandığından emin olmak için tek tek aygıtları ya da aygıtların tüm adres aralıklarını ekleyebilirsiniz. Benzersiz protokollere uymayan sunucu tiplerini, ilgili Anasistem Tanımı Yapı Taşı'na el ile girebilirsiniz. Örneğin, yapı taşlarına aşağıdaki sunucu tipleri eklendiğinde daha fazla yalancı pozitif ayarlama gereksinimi azalır:

- **BB:HostDefinition: Network Management Servers** yapı taşına ağ yönetimi sunucularını ekleyin.
- **BB:HostDefinition: Proxy Servers** yapı taşına yetkili sunucuları ekleyin.
- **BB:HostDefinition: Virus Definition and Other Update Servers** yapı taşına virüs ve Windows güncelleme sunucularını ekleyin.
- **BB-HostDefinition: VA Scanner Source IP** yapı taşına VA Tarayıcılarını ekleyin.

Server Discovery (Sunucu Keşfi) işlevi, ağınızdaki birçok sunucu tipini keşfetmek için varlık profili veritabanını kullanır. Server Discovery (Sunucu Keşfi) işlevi, otomatik olarak keşfedilen sunucuları listeler ve yapı taşlarına hangi sunucuları dahil etmek istediğinizi seçebilirsiniz.

Sunucuları keşfetme hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*.

Yapı taşlarını kullanarak, belirli kural testlerini diğer kurallarda yeniden kullanabilirsiniz. QRadar SIEM uygulamasını ayarlamak ve fazladan ilintilendirme kurallarını etkinleştirmek için yapı taşlarını kullanarak yanlış pozitif sayısını azaltabilirsiniz.

Yapı taşlarına otomatik olarak sunucuları ekleme

Yapı taşlarına otomatik olarak sunucuları ekleyebilirsiniz.

Yordam

1. **Assets** (Varlıklar) sekmesini tıklatın.
2. Gezinme bölmesinde **Server Discovery** (Sunucu Keşfi) öğesini tıklatın.
3. **Server Type** (Sunucu Tipi) listesinde, keşfetmek istediğiniz sunucu tipini seçin.

   Kalan parametreleri varsayılan olarak bırakın.
4. **Discover Servers** (Sunucuları Keşfet) seçeneğini tıklatın.
5. Matching Servers (Eşleşen Sunucular) bölmesinde, sunucu rolüne atamak istediğiniz tüm sunucuların onay kutusunu seçin.
6. **Approve Selected Servers** (Seçilen Sunucuları Onaylar) seçeneğini tıklatın.

   Unutmayın: DNS çözümleme bilgilerini görüntülemek için herhangi bir IP adresini sağ tıklatabilirsiniz.

Yapı taşlarına el ile sunucuları ekleme

Bir sunucu otomatik olarak algılanmazsa sunucuyu karşılık gelen Anasistem Tanımı Yapı Taşına el ile ekleyebilirsiniz.

Yordam

1. **Offenses** (Hücumlar) sekmesini tıklatın.
2. Gezinme bölmesinde **Rules** (Kurallar) öğesini tıklatın.
3. **Display** (Görüntü) listesinde **Building Blocks** (Yapı Taşları) seçeneğini belirleyin.
4. **Group** (Grup) listesinde **Host Definitions** (Anasistem Tanımları) seçeneğini belirleyin.

   Yapı taşının adı, sunucu tipine karşılık gelir. Örneğin, **BB:HostDefinition: Proxy Servers**, ortamınızdaki tüm yetkili sunucular için geçerli olur.
5. Bir anasistemi ya da ağı el ile eklemek için, ortamınız için uygun olan karşılık gelen anasistem tanımı Yapı Taşını çift tıklatın.
6. **Building Block** (Yapı Taşı) alanında, **when either the source or destination IP is one of the following** (kaynak ya da hedef IP şunlardan biri olduğunda) sözcük grubundan sonraki altı çizili değeri tıklatın.
7. **Enter an IP address or CIDR** (Bir IP adresi ya da CIDR girin) alanına, yapı taşına atamak istediğiniz anasistem adları veya IP adresi aralıklarını yazın.
8. **Add** (Ekle) düğmesini tıklatın.
9. **Submit** (Gönder) düğmesini tıklatın.
10. **Finish** (Son) düğmesini tıklatın.
11. Eklemek istediğiniz her sunucu tipi için bu adımları yineleyin.

Kuralları yapılandırma

Log Activity (Günlük Etkinliği), **Network Activity** (Ağ Etkinliği) ve **Offenses** (Hücumlar) sekmesinden kuralları ya da yapı taşlarını yapılandırabilirsiniz.

Yordam

1. **Offenses** (Hücumlar) sekmesini tıklatın.
2. Araştırmak istediğiniz hücumu çift tıklatın.
3. **Display > Rules** (Görüntü - Kurallar) seçeneklerini tıklatın.
4. Bir kuralı çift tıklatın.

   Kuralları daha fazla ayarlayabilirsiniz. Kuralları ayarlama hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Administration Guide*
5. Rules (Kurallar) sihirbazını kapatın.
6. Rules (Kurallar) sayfasında **Actions** (İşlemler) seçeneğini tıklatın.
7. İsteğe bağlı: Hücum saklama süresi dolduktan sonra hücumun veritabanından kaldırılmasını önlemek istiyorsanız **Protect Offense** (Hücumu Koru) seçeneğini belirleyin.
8. İsteğe bağlı: Hücumu bir QRadar SIEM kullanıcısına atamak istiyorsanız **Assign** (Ata) seçeneğini belirleyin.

İlgili kavramlar:

"QRadar SIEM kuralları" sayfa 4
Kurallar, bir testin tüm koşulları karşılanırsa olaylar, akışlar ya da hücumlar üzerinde testler gerçekleştirir, kural bir yanıt oluşturur.

SIM modelini temizleme

Her bir anasistemin, en geçerli kuralları, keşfedilen sunucuları ve ağ sıradüzenini temel alan hücumlar oluşturduğundan emin olmak için SIEM modelini temizleyin.

Yordam

1. **Admin** (Yönetim) sekmesini tıklatın.

2. Araç çubuğunda **Advanced > Clean SIM Model** (Gelişmiş - SIM Modelini Temizle) seçeneklerini belirleyin.
3. Gerekli seçeneği tıklatın:

   Hücumları etkin değil olarak ayarlamak için Soft Clean (Geçici Temizle) seçeneğini tıklatın.

   Tüm hücumları kapatmak için isteğe bağlı Deactivate all offenses (Tüm hücumların etkinliğini kaldır) seçeneği ile Soft Clean (Geçici Temizle) seçeneğini tıklatın.

   Tüm girdileri silmek için Hard Clean (Kalıcı Temizle) seçeneğini tıklatın.
4. **Are you sure you want to reset the data model?** (Veri modelini sıfırlamak istediğinizden emin misiniz?) seçeneğini tıklatın.
5. **Proceed** (Devam Et) seçeneğini tıklatın.
6. SIM sıfırlama işlemi tamamlandıktan sonra tarayıcınızı yenileyin.

Sonuçlar

SIM modelini temizlediğinizde tüm var olan hücumlar kapatılır. SIM modelinin temizlenmesi, var olan olayları ve akışları etkilemez.

Bölüm 3. QRadar SIEM uygulamasında çalışmaya başlama

IBM Security QRadar SIEM uygulamasında çalışmaya başlamak için olayları, akışları ve varlıkları arama hakkında bilgi edinin. Ayrıca hücumların nasıl araştırılacağını ve raporların nasıl oluşturulacağını da öğrenin.

Örneğin, **Log Activity** (Günlük Etkinliği) ve **Network Activity** (Ağ Etkinliği) sekmelerinde varsayılan kayıtlı aramaları kullanarak bilgi arayabilirsiniz. Kendi özel aramalarınızı da oluşturup kaydedebilirsiniz.

Sistem yöneticileri aşağıdaki görevleri gerçekleştirebilir:

- Sonuçlar kümesindeki arama ölçütleriyle eşleşen görüntüleme olaylarını ve belirli ölçütleri kullanarak olay verilerini arama. Olay verilerinin sütunlarını seçme, düzenleme ve gruplama.
- Akış verilerini görsel olarak gerçek zamanlı izleme ve araştırma veya görüntülenen akışları süzgeçten geçirmek için gelişmiş aramalar gerçekleştirme. Hangi trafiğinin nasıl iletileceğini belirlemek için akış bilgilerini görüntüleme.
- Tüm öğrenilen varlıkları görüntüleme ya da ortamınızdaki belirli varlıkları arama.
- Ağınızdaki anormallikleri, ağ davranışlarını, kaynak ve hedef IP adreslerini ve hücumları araştırma.
- Varsayılan ya da özel raporları düzenleme, oluşturma, zamanlama ve dağıtma.

Olayları arama

Son 6 saat içinde alınan QRadar SIEM tüm kimlik doğrulama olaylarını arayabilirsiniz.

Yordam

1. **Log Activity** (Günlük Etkinliği) sekmesini tıklatın.
2. Araç çubuğunda **Search > New Search** (Arama - Yeni Arama) seçeneklerini belirleyin.
3. Time Range (Zaman Aralığı) bölmesinde, olay araması için zaman aralığını tanımlayın:
   a. **Recent** (Son) seçeneğini tıklatın.
   b. **Recent** (Son) listesinde **Last 6 Hours** (Son 6 Saat) seçeneğini belirleyin.
4. Search Parameters (Arama Parametreleri) bölmesinde arama parametrelerini tanımlayın:
   a. Birinci listede **Category** (Kategori) seçeneğini belirleyin.
   b. İkinci listede **Equals** (Eşittir) seçeneğini belirleyin.
   c. **High Level Category** (Yüksek Düzey Kategori) listesinde **Authentication** (Kimlik Doğrulaması) seçeneğini belirleyin.
   d. **Low Level Category** (Düşük Düzey Kategori) listesinde varsayılan **Any** (Herhangi Biri) değerini kabul edin.
   e. **Add Filter** (Süzgeç Ekle) seçeneğini tıklatın.
5. Column Definition (Sütun Tanımı) bölmesinde, **Display** (Görüntü) listesinde **Event Name** (Olay Adı) seçeneğini belirleyin.
6. **Search** (Ara) seçeneğini tıklatın.

Olay arama ölçütlerini kaydetme

Gelecekte kullanmak üzere belirtilen olay arama ölçütlerini kaydedebilirsiniz.

Yordam

1. **Log Activity** (Günlük Etkinliği) sekmesini tıklatın.
2. Araç çubuğunda **Save Criteria** (Ölçütleri Kaydet) seçeneğini tıklatın.
3. **Search Name** (Arama Adı) alanına **Example Search 1** (Örnek Arama 1) yazın.
4. Timespan options (Zaman aralığı seçenekleri) bölmesinde **Recent** (Son) öğesini tıklatın.
5. **Recent** (Son) listesinde **Last 6 Hours** (Son 6 Saat) seçeneğini belirleyin.
6. **Include in my Quick Searches** (Hızlı Aramalarıma Dahil Et) seçeneğini tıklatın.
7. **Include in my Dashboard** (Gösterge Panoma Dahil Et) seçeneğini tıklatın.

   Include in my Dashboard (Gösterge Panoma Dahil Et) görüntülenmezse, Column Definition (Sütun Tanımı) bölmesinde **Event Name** (Olay Adı) seçeneğini belirlediğinizi doğrulamak için **Search > Edit Search** (Arama - Aramayı Düzenle) seçeneklerini tıklatın.
8. **OK** (Tamam) düğmesini tıklatın.

Sonraki adım

Zaman serisi grafiğini yapılandırın. Daha fazla bilgi için bkz. “Zaman serisi grafiğini yapılandırma”.

Zaman serisi grafiğini yapılandırma

Belirli bir zaman aralığı aramasıyla eşleştirilen kayıtları temsil eden etkileşimli zaman serisi grafiklerini görüntüleyebilirsiniz.

Yordam

1. Grafik başlık çubuğunda **Configure** (Yapılandır) simgesini tıklatın.
2. **Value to Graph** (Grafiği Oluşturulacak Değer) listesinde **Destination IP (Unique Count)** (Hedef IP (Benzersiz Sayı)) seçeneğini belirleyin.
3. **Chart Type** (Grafik Tipi) listesinde **Time Series** (Zaman Serisi) seçeneğini belirleyin.
4. **Capture Time Series Data** (Zaman Serisi Verilerini Yakala) öğesini tıklatın.
5. **Save** (Kaydet) seçeneğini tıklatın.
6. **Update Details** (Ayrıntıları Güncelle) seçeneğini tıklatın.
7. Arama sonuçlarınızı süzgeçten geçirin:
   a. Süzgeçten geçirmek istediğiniz olayı sağ tıklatın.
   b. **Filter on Event Name is <Olay Adı>** seçeneğini tıklatın.
8. Kullanıcı adına göre gruplanan olay listesini görüntülemek için **Display** (Görüntü) listesinden **Username** (Kullanıcı Adı) seçeneğini belirleyin.
9. Aramanızın **Dashboard** (Gösterge Panosu) sekmesinde görünür olduğunu doğrulayın:
   a. **Dashboard** (Gösterge Panosu) sekmesini tıklatın.
   b. **New Dashboard** (Yeni Gösterge Panosu) simgesini tıklatın.
   c. **Name** (Ad) alanına **Example Custom Dashboard** (Örnek Özel Gösterge Panosu) yazın.
   d. **OK** (Tamam) düğmesini tıklatın.
   e. **Add Item** (Öğe Ekle) listesinde **Log Activity > Event Searches > Example Search 1** (Günlük Etkinliği - Olay Aramaları - Örnek Arama 1) seçeneklerini belirleyin.

Sonuçlar

Kayıtlı olay aramanızdaki sonuçlar, Gösterge Panosunda görüntülenir.

Akışları arama

Gerçek zamanlı olarak akış verilerini arayabilir, izleyebilir ve araştırabilirsiniz.

Ayrıca görüntülenen akışları süzgeçten geçirmek için gelişmiş aramalar da gerçekleştirebilirsiniz. Hangi ağ trafiğinin nasıl iletileceğini belirlemek için akış bilgilerini görüntüleyin.

Yordam

1. **Network Activity** (Ağ Etkinliği) sekmesini tıklatın.
2. Araç çubuğunda **Search > New Search** (Arama - Yeni Arama) seçeneklerini tıklatın.
3. Time Range (Zaman Aralığı) bölmesinde akış arama zaman aralığını tanımlayın:
   a. **Recent** (Son) seçeneğini tıklatın.
   b. **Recent** (Son) listesinde **Last 6 Hours** (Son 6 Saat) seçeneğini belirleyin.
4. Search Parameters (Arama Parametreleri) bölmesinde arama ölçütlerinizi tanımlayın:
   a. Birinci listede **Flow Direction** (Akış Yönü) seçeneğini belirleyin.
   b. İkinci listede **Equals** (Eşittir) seçeneğini belirleyin.
   c. Üçüncü listede **R2L** seçeneğini belirleyin.
   d. **Add Filter** (Süzgeç Ekle) seçeneğini tıklatın.
5. **Display** (Görüntü) listesinde Column Definition (Sütun Tanımı) bölmesinde **Application** (Uygulama) seçeneğini belirleyin.
6. **Search** (Ara) seçeneğini tıklatın.

Sonuçlar

Son 6 saatte uzaktan yerele (R2L) akış yönüne sahip tüm akışlar görüntülenir ve **Application Name** (Uygulama Adı) alanına göre sıralanır.

Akış arama ölçütlerini kaydetme

Gelecekte kullanım için belirtilen akış arama ölçütlerini kaydedebilirsiniz.

Yordam

1. **Network Activity** (Ağ Etkinliği) sekmesi araç çubuğunda **Save Criteria** (Ölçütleri Kaydet) seçeneğini tıklatın.
2. **Search Name** (Arama Adı) alanına **Example Search 2** (Örnek Arama 2) yazın.
3. **Recent** (Son) listesinde **Last 6 Hours** (Son 6 Saat) seçeneğini belirleyin.
4. **Include in my Dashboard** (Gösterge Panosuna Dahil Et) ve **Include in my Quick Searches** (Hızlı Aramalara Dahil Et) seçeneğini tıklatın.
5. **OK** (Tamam) düğmesini tıklatın.

Sonraki adım

Gösterge panosu öğesi oluşturun. Daha fazla bilgi için bkz. “Gösterge panosu öğesi oluşturma”.

Gösterge panosu öğesi oluşturma

Kayıtlı akış arama ölçütlerini kullanarak bir gösterge panosu öğesi oluşturabilirsiniz.

Yordam

1. **Network Activity** (Ağ Etkinliği) araç çubuğunda **Quick Searches > Example Search 2** (Hızlı Aramalar - Örnek Arama 2) seçeneklerini belirleyin.
2. Aramanızın Gösterge Panosuna dahil edildiğini doğrulayın:
   a. **Dashboard** (Gösterge Panosu) sekmesini tıklatın.
   b. **Show Dashboard** (Gösterge Panosunu Göster) listesinde **Example Custom Dashboard** (Örnek Özel Gösterge Panosu) seçeneğini belirleyin.
   c. **Add Item** (Öğe Ekle) listesinde **Flow Searches > Example Search 2** (Akış Aramaları - Örnek Arama 2) seçeneklerini belirleyin.
3. Gösterge panosu grafiğinizi yapılandırın:
   a. **Settings** (Ayarlar) simgesini tıklatın.
   b. Yapılandırma seçeneklerini kullanarak, grafiği oluşturulan değeri, kaç tane nesnenin görüntüleneceğini, grafik tipini ya da grafikte görüntülenen zaman aralığını değiştirin.
4. Şu anda grafikte görüntülenen akışları araştırmak için **View in Network Activity** (Ağ Etkinliğinde Görüntüle) seçeneğini tıklatın.

Sonuçlar

Network Activity (Ağ Etkinliği) sayfası, zaman serisi grafiğinizin parametreleriyle eşleşen sonuçları görüntüler. Zaman serisi grafikleri hakkında daha fazla bilgi için bkz. *IBM Security QRadar SIEM Users Guide*.

Varlıkları arama

Assets (Varlıklar) sekmesine eriştiğinizde Asset (Varlık) sayfası, ağınızdaki tüm keşfedilen varlıklarla doldurulmuş şekilde görüntülenir. Bu listeyi daraltmak için arama parametrelerini yalnızca araştırmak istediğiniz varlık profillerini görüntüleyecek şekilde yapılandırabilirsiniz.

Bu görev hakkında

Anasistem profillerini, varlıkları ve kimlik bilgilerini aramak için arama özelliğini kullanın. Kimlik bilgileri; ağınızdaki MAC adresleri, kullanıcı oturum açmaları ve DNS bilgileri gibi daha fazla ayrıntı sağlar.

Örneğin:

Yordam

1. **Assets** (Varlıklar) sekmesini tıklatın.
2. Gezinme bölmesinde **Asset Profiles** (Varlık Profilleri) öğesini tıklatın.
3. Araç çubuğunda **Search > New Search** (Arama - Yeni Arama) seçeneklerini tıklatın.
4. Bir kayıtlı aramayı yüklemek istiyorsanız aşağıdaki adımları gerçekleştirin:
   a. İsteğe bağlı: **Group** (Grup) listesinde, **Available Saved Searches** (Kullanılabilir Kayıtlı Aramalar) listesinde görüntülemek istediğiniz varlık arama grubunu seçin.
   b. Aşağıdaki seçeneklerden birini belirleyin:
      - **Type Saved Search or Select from List** (Kayıtlı Arama Yazın ya da Listeden Seçin) alanına, yüklemek istediğiniz aramanın adını yazın.
      - **Available Saved Searches** (Kullanılabilir Kayıtlı Aramalar) listesinde, yüklemek istediğiniz kayıtlı aramayı seçin.
   c. **Load** (Yükle) seçeneğini tıklatın.
5. Search Parameters (Arama Parametreleri) bölmesinde arama ölçütlerinizi tanımlayın:

a. Birinci listede, aramak istediğiniz varlık parametresini seçin. Örneğin, **Hostname** (Anasistem Adı), **Vulnerability Risk Classification** (Güvenlik Açığı Risk Sınıflandırması) ya da **Technical Owner** (Teknik Sahip).
b. İkinci listede, aramak için kullanmak istediğiniz değiştiriciyi seçin.
c. **Entry** (Girdi) alanına, arama parametrenizle ilgili belirli bilgileri yazın.
d. **Add Filter** (Süzgeç Ekle) seçeneğini tıklatın.
e. Arama ölçütlerine eklemek istediğiniz her süzgeç için bu adımları yineleyin.

6. **Search** (Ara) seçeneğini tıklatın.

Örnek

CVE-2010-000 CVE tanıtıcısının etkin olarak açıklarından yararlanıldığına ilişkin bir bildirim alırsınız. Devreye alımınızdaki anasistemlerin bu açığa maruz kalıp kalmadığını belirlemek için aşağıdaki adımları uygulayın:

1. Arama parametreleri listesinden **Vulnerability External Reference** (Güvenlik Açığı Harici Başvurusu) seçeneğini belirleyin.
2. **CVE** seçeneğini belirleyin.
3. Belirli CVE tanıtıcısına karşı güvenlik açığı olan tüm anasistemlerin listesini görüntülemek için 2010-000 yazın.

Daha fazla bilgi için Açık Kaynak Güvenlik Açığı Veritabanı web sitesine (*http://osvdb.org/*) ve Ulusal Güvenlik Açığı Veritabanına (*http://nvd.nist.gov/*) bakın.

Hücum araştırmaları

Offenses (Hücumlar) sekmesini kullanarak, ağınızdaki anormallikleri, ağ davranışlarını, kaynak ve hedef IP adreslerini ve hücumları araştırabilirsiniz.

QRadar SIEM, aynı hücumda birden çok ağda ve sonuç olarak aynı ağ olayında bulunan hedef IP adresleri ile olay ve akışları ilintilendirebilir. Bu, ağınızdaki her bir hücumu etkili şekilde araştırmanızı sağlar.

Hücumları görüntüleme

Ağınızdaki her bir hücumu araştırabilirsiniz.

Örneğin, ağınızdaki anormallikleri, ağ davranışlarını, kaynak ve hedef IP adreslerini ve hücumları araştırabilirsiniz.

Yordam

1. **Offenses** (Hücumlar) sekmesini tıklatın.
2. Araştırmak istediğiniz hücumu çift tıklatın.
3. Araç çubuğunda **Display > Destinations** (Görüntü - Hedefler) seçeneklerini belirleyin.

   Hedefte güvenlik açığı olup olmadığını ya da hedefin şüpheli davranış sergileyip sergilemediğini belirlemek için her bir hedefi araştırabilirsiniz.
4. Araç çubuğunda **Events** (Olaylar) öğesini tıklatın.

Sonuçlar

List of Events (Olaylar Listesi) penceresi, hücumla ilişkili tüm olayları görüntüler. Olayları arayabilir, sıralayabilir ve süzgeçten geçirebilirsiniz.

Örnek: PCI rapor şablonlarını etkinleştirme

Reports (Raporlar) sekmesini kullanarak rapor şablonlarını etkinleştirebilir, devre dışı bırakabilir ve düzenleyebilirsiniz.

Bu başlangıç görevinde, Payment Card Industry (PCI) rapor şablonlarını etkinleştirirsiniz.

Yordam

1. **Reports** (Raporlar) sekmesini tıklatın.
2. **Hide Inactive Reports** (Etkin Olmayan Raporları Gizle) onay kutusunun işaretini kaldırın.
3. **Group** (Grup) listesinde **Compliance > PCI** (Uyumluluk - PCI) seçeneklerini belirleyin.
4. Listedeki tüm rapor şablonlarını seçin:
   a. Listedeki birinci raporu tıklatın.
   b. Listedeki son raporu tıklatırken Üst Karakter tuşunu basılı tutarak tüm rapor şablonlarını seçin.
5. **Actions** (İşlemler) listesinde **Toggle Scheduling** (Zamanlamayı Aç/Kapat) seçeneğini belirleyin.
6. Oluşturulan raporlara erişin:
   a. **Generated Reports** (Oluşturulan Raporlar) sütunundaki listeden, görüntülemek istediğiniz raporun zaman damgasını seçin.
   b. **Format** (Biçim) sütununda, görüntülemek istediğiniz rapor biçiminin simgesini tıklatın.

Örnek: Kayıtlı arama temelinde bir özel rapor oluşturma

Bir arama içe aktararak ya da özel ölçütler oluşturarak rapor oluşturabilirsiniz.

Bu görev hakkında

Bu başlangıç görevinde, “Olayları arama” sayfa 15 içinde oluşturduğunuz olay ve akış aramaları temelinde bir rapor oluşturursunuz.

Yordam

1. **Reports** (Raporlar) sekmesini tıklatın.
2. **Actions** (İşlemler) listesinde **Create** (Oluştur) seçeneğini belirleyin.
3. **Next** (İleri) seçeneğini tıklatın.
4. Rapor zamanlamasını yapılandırın.
   a. **Daily** (Günlük) seçeneğini belirleyin.
   b. **Monday, Tuesday, Wednesday, Thursday, and Friday** (Pazartesi, Salı, Çarşamba, Perşembe ve Cuma) seçeneklerini belirleyin.
   c. Listeleri kullanarak **8:00** ve **AM** seçeneğini belirleyin.
   d. **Yes - Manually generate report** (Evet - El ile rapor oluştur) seçeneğinin belirlendiğinden emin olun.
   e. **Next** (İleri) seçeneğini tıklatın.
5. Rapor düzenini yapılandırın:
   a. **Orientation** (Yön) listesinde **Landscape** (Yatay) seçeneğini belirleyin.
   b. İki grafik kapsayıcısı içeren düzeni seçin.
   c. **Next** (İleri) seçeneğini tıklatın.
6. **Report Title** (Rapor Başlığı) alanına **Sample Report** (Örnek Rapor) yazın.

7. Üst grafik kapsayıcısını yapılandırın:
   a. **Chart Type** (Grafik Tipi) listesinde **Events/Logs** (Olaylar/Günlükler) seçeneğini belirleyin.
   b. **Chart Title** (Grafik Başlığı) alanına **Sample Event Search** (Örnek Olay Araması) yazın.
   c. **Limit Events/Logs To Top** (Başa Koyulacak Olayları/Günlükleri Sınırla) listesinde **10** değerini seçin.
   d. **Graph Type** (Grafik Tipi) listesinde **Stacked Bar** (Yığın Çubuk) seçeneğini belirleyin.
   e. **All data from the previous (24 hours)** (Öncekilerdeki tüm veriler (24 saat)) seçeneğini tıklatın.
   f. **Base this event report on** (Bu olay raporu için şunu temel al:) listesinde **Example Search 1** (Örnek Arama 1) seçeneğini belirleyin.

      Örnek Arama 1 kayıtlı aramasındaki ayarlar kullanılarak kalan parametreler otomatik olarak doldurulur.
   g. **Save Container Details** (Kapsayısı Ayrıntılarını Kaydet) seçeneğini tıklatın.
8. Alt grafik kapsayıcısını yapılandır:
   a. **Chart Type** (Grafik Tipi) listesinde **Flows** (Akışlar) seçeneğini belirleyin.
   b. **Chart Title** (Grafik Başlığı) alanına **Sample Flow Search** (Örnek Akış Araması) yazın.
   c. **Limit Flows To Top** (Başa Koyulacak Akışları Sınırla) listesinde **10** değerini seçin.
   d. **Graph Type** (Grafik Tipi) listesinde **Stacked Bar** (Yığın Çubuk) seçeneğini belirleyin.
   e. **All data from the previous 24 hours** (Önceki 24 saatteki tüm veriler) seçeneğini tıklatın.
   f. **Available Saved Searches** (Kullanılabilir Kayıtlı Aramalar) listesinde **Example Search 2** (Örnek Arama 2) seçeneğini belirleyin.

      Örnek Arama 2 kayıtlı aramasındaki ayarlar kullanılarak kalan parametreler otomatik olarak doldurulur.
   g. **Save Container Details** (Kapsayısı Ayrıntılarını Kaydet) seçeneğini tıklatın.
9. **Next** (İleri) seçeneğini tıklatın.
10. **Next** (İleri) seçeneğini tıklatın.
11. Rapor biçimini seçin:
    a. **PDF and HTML** (PDF ve HTML) onay kutularını tıklatın.
    b. **Next** (İleri) seçeneğini tıklatın.
12. Rapor dağıtım kanallarını seçin:
    a. **Report Console** (Rapor Konsolu) seçeneğini tıklatın.
    b. **Email** (E-posta) seçeneğini tıklatın.
    c. **Enter the report destination email address(es)** (Rapor hedefi e-posta adreslerini girin) alanına e-posta adresinizi yazın.
    d. **Include Report as attachment** (Raporu ek olarak dahil et) seçeneğini tıklatın.
    e. **Next** (İleri) seçeneğini tıklatın.
13. Son Report (Rapor) sihirbazı ayrıntılarını doldurun:
    a. **Report Description** (Rapor Tanımı) alanına şablonun bir tanımını yazın.
    b. **Yes - Run this report when the wizard is complete** (Evet - Sihirbaz tamamlandığında bu raporu çalıştır) seçeneğini tıklatın.
    c. **Finish** (Son) düğmesini tıklatın.

14. **Generated Reports** (Oluşturulan Raporlar) sütununda liste kutusunu kullanarak raporunuzun zaman damgasını seçin.

Bildirimler

Bu yayındaki bilgiler, ABD'de kullanıma sunulan ürün ve hizmetlere ilişkindir.

IBM bu belgede sözü edilen ürün, hizmet ya da özellikleri diğer ülkelerde kullanıma sunmayabilir. IBM müşteri temsilcisinden ya da çözüm ortağından, bulunduğunuz yerde kullanıma sunulan ürün ve hizmetler hakkında bilgi edinebilirsiniz. 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 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. Lisans sorularınız için aşağıdaki adresten IBM'e yazılı olarak başvurabilirsiniz:

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

Çift bayt karakter takımı (DBCS) bilgilerine ilişkin lisans sorguları için, ülkenizdeki IBM Fikri Mülkiyet Departmanı ile bağlantıya geçin ya da sorgularınızı yazılı olarak aşağıdaki adrese gönderin:

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

Aşağıdaki paragraf, ilgili hükümlerin yerel yasalarıyla bağdaşmadığı ülkeler 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 devletler, belirli işlemlerde açık veya zımni garanti feragatnamesine izin vermez, bu nedenle bu bildirim sizin için geçerli olmayabilir.

Bu bilgilerde teknik yanlışlıklar ya da yazım hataları olabilir. Buradaki bilgiler düzenli aralıklarla güncellenir ve belgenin yeni basımlarına eklenir. IBM, önceden bildirimde bulunmaksızın, bu yayında açıklanan ürünler ve/veya programlar üzerinde iyileştirmeler ve/veya değişiklikler yapabilir.

Bu belgede sahibi IBM olmayan web sitelerine yapılan göndermeler kullanıcıya kolaylık sağlamak içindir ve bu web sitelerinin onaylanması anlamına gelmez. Bu Web sitelerindeki malzemeler, bu IBM ürününe ilişkin malzemelerin bir parçası değildir ve bu Web sitelerini kullanma sorumluluğu kullanıcıya 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 koşullara tabidir ve bazı durumlarda bedelli olarak edinilebilir.

Bu belgede açıklanan lisanslı program ve bu program için kullanabileceğiniz tüm lisanslı malzemeler IBM tarafından, IBM Müşteri Sözleşmesi, IBM Uluslararası Program Lisansı Sözleşmesi ya da taraflar arasında yapılan herhangi bir eşdeğer sözleşmeye göre sağlanmaktadır.

Bu yazının içinde geçen bütün performans verileri denetlenmiş bir ortamda belirlenmiştir. Bu nedenle, başka işletim ortamlarında çok farklı sonuçlar alınabilir. Bazı ölçümler, geliştirme düzeyindeki sistemlerde yapılmıştır ve bu ölçümlerin, yaygın olarak kullanılan sistemlerle aynı olacağına ilişkin herhangi bir garanti yoktur. Ayrıca, bazı ölçümler bilinen veriler kullanılarak tahmin edilmiş olabilir. Gerçek sonuçlar değişiklik gösterebilir. Bu belgeyi okuyan kullanıcıların, kendi ortamlarına ilişkin uygulanabilir verileri doğrulamaları gerekir.

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 yeteneklerine ilişkin sorular, bu ürünleri sağlayan firmalara 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, IBM'in önerdiği güncel perakende satış fiyatlarıdır ve duyuruda bulunulmaksızın değiştirilebilir. Bayi fiyatları değişiklik gösterebilir.

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. Tüm bu adlar kurgusal olup kullanılan ad ve adreslerin gerçek bir kuruluşla olan benzerliği tamamen tesadüftür.

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

Ticari markalar

IBM, IBM logosu ve ibm.com, International Business Machines Corporation'ın ABD'de ve/veya diğer ülkelerdeki ticari markaları ya da tescilli ticari markalarıdır. Bu ve diğer IBM ticari markalı terimler, bu bilgilerde ilk geçtikleri yerde bir ticari marka sembolüyle (® ya da ™) işaretlenmişse, bu semboller bu bilgilerin yayınlandığı sırada IBM'in sahip olduğu, ABD'de kayıtlı ticari markaları ya da ortak hukuk ticari markalarını gösterir. 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).

Java ve tüm Java tabanlı ticari markalar ve logolar, Sun Microsystems, Inc.'ın ABD ve/veya diğer ülkelerdeki ticari markaları ya da tescilli ticari markalarıdır.

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, başka şirketlerin ticari markaları 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 size bir müşteri olarak tanımlama bilgilerini ve diğer teknolojileri kullanarak son kullanıcıların kimlik bilgilerini toplama yeteneği sağlıyorsa, bildirme ve rıza gereklilikleri de içinde olmak üzere bu tür verilerin toplanmasına ilişkin yasalar konusunda 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.

Sözlük

Bu sözlük, IBM Security QRadar SIEM yazılım ve ürünlerine ilişkin terim ve tanımları sağlar.

Bu sözlükte aşağıdaki çapraz referanslar kullanılmıştır:

- *Bkz.* sizi tercih edilmeyen bir terimden tercih edilen bir terime veya bir kısaltmadan tam yazılmış bir ifadeye yönlendirir.
- *Ayrıca bkz.* sizi ilgili veya karşıt bir terime yönlendirir.

Diğer terimler ve tanımlar için bkz. IBM Terminolojisi web sitesi (yeni pencerede açılır).

A

Açık Kaynak Güvenlik Açığı Veritabanı (OSVDB)
Ağ güvenliği topluluğu için ağ güvenliği topluluğu tarafından oluşturulan, ağ güvenliği güvenlik açıklarıyla ilgili teknik bilgi sağlayan bir açık kaynak veritabanı.

açık sistemler bağlantısı (OSI)
Bilgi alışverişi için Uluslararası Standartlar Örgütü (ISO) standartlarına uygun şekilde açık sistemler bağlantısı.

Adres Çözümleme Protokolü (ARP)
Bir IP adresini, yerel ağ üzerindeki bir ağ bağdaştırıcısı adresine dinamik olarak eşleyen bir protokol.

Ağ Adresi Çevirisi (NAT)
Güvenlik duvarında, güvenli İnternet Protokolü (IP) adreslerinin dış kayıtlı adreslere dönüştürülmesi. Bu, dış ağlarla iletişim sağlar, ancak güvenlik duvarının içinde kullanılan IP adreslerini maskeler.

ağ ağırlığı
Ağın önemini belirten, her bir ağa uygulanan sayısal değer. Ağ ağırlığı kullanıcı tarafından tanımlanır.

ağ geçidi
Farklı ağ mimarilerine sahip ağları ya da sistemleri bağlamak için kullanılan aygıt ya da program.

ağ katmanı
OSI mimarisinde, öngörülebilir hizmet kalitesine sahip açık sistemler arasında bir yol oluşturmak için hizmet sağlayan katman.

ağ nesnesi
Ağ sıradüzeninin bir bileşeni.

ağ sıradüzeni
Ağ nesnelerinin sıradüzensel toplamı olan bir kapsayıcı tipi.

akış Görüşme sırasında bir bağlantı üzerinden iletilen tek bir veri iletimi.

akış günlüğü
Akış kayıtları toplaması.

akış kaynakları
Akışın yakalandığı kaynak. Akış, yönetilen bir anasisteme kurulan donanımdan geldiğinde dahili olarak sınıflandırılır ya da akış bir akış toplayıcısından gönderildiğinde harici olarak sınıflandırılır.

alt ağ Bkz. alt ağ.

alt ağ Daha küçük, birbirinden bağımsız ancak yine de birbiriyle bağlantılı alt gruplara ayrılmış ağ.

alt ağ maskesi
İnternet alt ağı için, bir IP adresinin anasistem bölümündeki alt ağ adresi bitlerini tanımlamak için kullanılan 32 bit maske.

alt arama
Tamamlanan arama sonuçları kümesi içinde bir arama sorgusunun gerçekleştirilmesini sağlayan işlev.

anahtar dosyası
Bilgisayar güvenliğinde, genel anahtarları, özel anahtarları, güvenilir kökleri ve sertifikaları içeren dosya.

anasistem bağlamı
Her bir bileşenin beklendiği gibi çalıştığından emin olmak için bileşenleri izleyen bir hizmet.

anormallik
Ağın beklenen davranışından sapma.

ARP Bkz. Adres Çözümleme Protokolü.

ARP Yeniden Yönlendirme
Anasisteme, ağ üzerinde bir sorun olduğunu bildirmeye ilişkin bir ARP yöntemi.

ASN Bkz. otonom sistem numarası.

Aygıt Desteği Modülü (DSM)
Birden çok günlük kaynağından alınan olayları ayrıştırıp çıktı olarak görüntülenebilen standart bir sınıflama biçimine dönüştüren yapılandırma dosyası.

ayrıştırma sırası
Kullanıcının, ortak bir IP adresi ya da anasistem adını paylaşan günlük kaynakları için önem sırasını tanımlayabildiği bir günlük kaynağı tanımı.

B

Basit Ağ Yönetimi Protokolü (SNMP)
Karmaşık ağlardaki sistemlerin ve aygıtların izlenmesine ilişkin protokoller bütünü. Yönetilen aygıtlara ilişkin bilgiler Yönetim Bilgi Tabanında (MIB) tanımlanır ve depolanır.

başvuru eşlemi
Bir anahtarın bir değere (örneğin, bir kullanıcı adının bir genel tanıtıcıya) doğrudan eşlenmesine ilişkin veri kaydı.

başvuru kümesi
Bir ağ üzerindeki olay ya da akışlardan türetilen tekli öğelerin listesi. Örneğin, IP adreslerinin bir listesi ya da kullanıcı adlarının listesi.

başvuru tablosu
Tip atanmış olan veri kaydının diğer anahtarlara eşlendiği ve sonra tek bir değere eşlendiği bir tablo.

birikeç Bir işlem işleneninin saklanabildiği ve sonradan o işlemin sonucuyla değiştirilebildiği bir kayıt.

birincil HA anasistemi
HA kümesine bağlı ana bilgisayar.

birleştirme aralığı
Olayların paketlenme aralığı. Olay paketleme 10'ar saniyelik aralıklarla oluşur ve o anda birleşen olaylarla eşleşmeyen ilk olaydan başlar. Birleştirme aralığı içinde ilk üç eşleşen olay paketlenir ve olay işleyicisine gönderilir.

büyüklük
Belirli bir hücumun göreli önemini belirten bir ölçü. Büyüklük; ilgi, önem düzeyi ve güvenilirlikten hesaplanan ağırlıklı bir değerdir.

C

canlı tarama
Oturum adına göre tarama sonuçlarından rapor verileri oluşturan bir güvenlik açığı taraması.

CIDR Bkz. Sınıfsız Etki Alanı İçi Yönlendirme.

CVSS Bkz. Genel Güvenlik Açığı Puanlama Sistemi.

D

davranış
Sonuçları da dahil olmak üzere bir işlem ya da olayın gözlemlenebilir etkileri.

DHCP Bkz. Dinamik Anasistem Yapılandırması Protokolü.

Dinamik Anasistem Yapılandırması Protokolü (DHCP)
Yapılandırma bilgilerini merkezi olarak yönetmek için kullanılan bir protokol. Örneğin, DHCP otomatik olarak bir ağ üzerindeki bilgisayarlara IP adresleri atar.

dış tarama aracı
Ağ üzerindeki varlıklar hakkında güvenlik açığı bilgilerini toplamak için ağa bağlı olan bir makine.

DNS Bkz. Etki Alanı Adı Sistemi.

DSM Bkz. Aygıt Desteği Modülü.

E

eşlemlerin başvuru eşlemi
Birçok değere eşlenmiş iki anahtarın veri kaydı. Örneğin, bir uygulamanın toplam baytlarının bir kaynak IP'sine eşlenmesi.

Etki Alanı Adı Sistemi (DNS)
Etki alanlarını IP adresleriyle eşleştiren dağıtılmış veritabanı sistemi.

etkin sistem
Yüksek kullanılabilirlik (HA) kümesinde, tüm hizmetleri çalışmakta olan sistem.

F

FQDN Bkz. tam etki alanı adı.

FQNN Bkz. tam ağ adı.

G

Genel Güvenlik Açığı Puanlama Sistemi (CVSS)
Güvenlik açığı önem derecesinin ölçüldüğü bir puanlama sistemi.

günlük kaynağı
Bir olay günlüğünün kaynağı olan güvenlik ekipmanı ya da ağ ekipmanı.

günlük kaynağı uzantısı
Olay yükündeki olayları tanımlamak ve kategorilere ayırmak için gerekli tüm düzenli ifade desenlerini içeren bir XML dosyası.

güvenilirlik
Bir olay ya da hücumun doğruluğunu belirlemek için kullanılan, 0-10 arasında bir sayısal derecelendirme. Birden çok kaynak aynı olayı ya da hücumu bildirdikçe güvenilirlik artar.

güvenilirlik deposu dosyası
Güvenilir bir varlık için genel anahtarları içeren bir anahtar veritabanı dosyası.

güvenlik açığı
İşletim sistemi, sistem yazılımı ya da uygulama yazılımı bileşenindeki bir güvenlik açığı.

H

HA Bkz. yüksek kullanılabilirlik.

hakim Ağ trafiğini ve güvenlik olaylarını, tanımlanmış özel kurallara karşı analiz eden dahili bir bileşen.

HA kümesi
Bir birincil sunucu ve bir ikincil sunucudan oluşan yüksek kullanılabilirlikli yapılandırma.

HMAC
Bkz. Hash-Based Message Authentication Code (Karma Tabanlı İleti Kimlik Doğrulama Kodu.

HMAC
Şifreli karma işlevi ve gizli anahtarı kullanan bir şifreleme kodu.

hücum İzlenen bir koşula yanıt olarak oluşturulan bir olay ya da gönderilen bir ileti. Örneğin, hücum, bir ilkenin ihlal edilip edilmediğine ya da ağın saldırı altında olup olmadığına ilişkin bilgiler sağlar.

I/İ

ICMP Bkz. Internet Control Message Protocol.

içerik yakalama
Yapılandırılabilir bir yük miktarını yakalayıp verileri bir akış günlüğünde saklayan işlem.

IDS Bkz. izinsiz giriş algılama sistemi.

ihlal Kurumsal ilkeyi atlayan ya da kurumsal ilkeye uymayan bir hareket.

ikincil HA anasistemi
HA kümesine bağlı yedek bilgisayar. İkincil HA anasistemi, birincil HA anasisteminin başarısız olması durumunda birincil HA anasisteminin sorumluluğunu üstlenir.

İletim Denetimi Protokolü (TCP)
İnternet'te ve ağlar arası protokol için Internet Engineering Task Force (IETF) standartlarını izleyen herhangi bir ağda kullanılan bir protokol. TCP, paket anahtarlamalı iletişim ağlarında ve bu ağların birbirine bağlı sistemlerinde anasistemden anasisteme güvenilir protokol sağlar. Ayrıca bkz. İnternet Protokolü.

iletme hedefi
Günlük ve akış kaynaklarından işlenmemiş ve normalleştirilmiş verileri alan bir ya da daha fazla satıcı sistemi.

ilgi Ağ üzerindeki bir olay, kategori ya da hücumun göreli etkisinin ölçümü.

Internet Control Message Protocol (ICMP)
Kaynak anasistemle iletişim kurmak için, örneğin bir veri birimindeki bir hatayı bildirmek için, ağ geçidi tarafından kullanılan bir internet protokolü.

İnternet hizmeti sağlayıcısı (ISP)
İnternet'e erişilmesini sağlayan bir kuruluş.

İnternet Protokolü (IP)
Verileri, bir ağ ya da birbirine bağlı ağlar üzerinden yönlendiren bir protokol. Bu protokol, yüksek protokol katmanları ile fiziksel ağ arasında aracı görevi görür. Ayrıca bkz. İletim Denetimi Protokolü.

IP Bkz. İnternet Protokolü.

IP çok noktaya yayın
Tek bir çok noktaya yayın grubunu oluşturan sistemler kümesi bir İnternet Protokolü (IP) veri biriminin iletimi.

IPS Bkz. izinsiz giriş engelleme sistemi.

ISP Bkz. İnternet hizmeti sağlayıcısı.

istemci Bir sunucudan hizmet isteyen yazılım programı ya da bilgisayar.

izinsiz giriş algılama sistemi IDS)
Bir ağ ya da anasistemin parçası olan izlenen kaynaklardaki girişimleri veya başarılı saldırıları algılayan yazılım.

izinsiz giriş engelleme sistemi (IPS)
Zararlı olabilecek etkinliği reddetme girişiminde bulunan bir sistem. Reddetme

mekanizmaları arasında süzgeçten geçirme, izleme ya da hız sınırlarını ayarlama yer alabilir.

K

keşif (recon)
Ağ kaynaklarının kimliğiyle ilgili bilgilerin toplanma yöntemi. Daha sonra bir önem düzeyi atanan ağ kaynağı olaylarının listesini derlemek için ağ taraması ve diğer teknikler kullanılır.

kimlik Bir kişi, kuruluş, yer ya da öğeyi temsil eden bir veri kaynağındaki öznitelikler toplaması.

kimlik bilgileri
Bir kullanıcıya veya işleme belirli erişim izinleri veren bir bilgi kümesi.

konsol Bir işletmenin, sistemin işleyişini denetleyip gözleyebileceği görüntü istasyonu.

kural Bilgisayar sistemlerinin ilişkileri tanımlamasını ve otomatik yanıtları uygun şekilde çalıştırmasını sağlayan bir koşullu deyimler kümesi.

kümelerin başvuru eşlemi
Birden çok değere eşlenmiş bir anahtarın veri kaydı. Örneğin, ayrıcalıklı kullanıcı listesinin bir anasisteme eşlenmesi.

küme sanal IP adresi
Birincil ya da ikincil anasistem ve HA kümesi arasında paylaşılan bir IP adresi.

L

LAN Bkz. yerel ağ.

LDAP Bkz. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
X.500 modelini destekleyen dizinlere erişim sağlamak için TCP/IP kullanan ve daha karmaşık olan X.500 Directory Access Protocol (DAP) kadar kaynak gerektirmeyen açık protokol. Örneğin, bir İnternet ya da intranette kişi, kuruluş ve diğer kaynakları bulmak için LDAP kullanılabilir.

L2L Bkz. Yerelden Yerele.

L2R Bkz. Yerelden Uzağa.

N

NAT Bkz. Ağ Adresi Çevirisi.

NetFlow
Ağ trafiği akış verilerini izleyen bir Cisco ağ protokolü. NetFlow verileri; istemci ve sunucu bilgilerini, hangi kapıların kullanıldığını ve bir ağa bağlı yönlendiriciler ve anahtarlar üzerinden iletilen paket ve bayt sayısını içerir. Veriler, veri analizinin gerçekleştiği NetFlow toplayıcılarına gönderilir.

O/Ö

OSI Bkz. açık sistemler bağlantısı.

OSVDB
Bkz. Açık Kaynak Güvenlik Açığı Veritabanı.

otonom sistem numarası (ASN)
TCP/IP'de, IP adresleri atayan aynı merkezi yetkili tarafından otonom sisteme atanan bir numara. Otonom sistem numarası, otomatik yönlendirme algoritmalarının otonom sistemleri ayırt etmesini mümkün kılar.

önem düzeyi
Bir kaynağın bir hedefte oluşturduğu göreli tehdidin ölçümü.

P

protokol
Bir iletişim ağındaki iki ya da daha çok aygıt veya sistem arasında verilerin iletişimini ve aktarımını denetleyen kurallar bütünü.

Q

QID Eşlemi
Her bir benzersiz olayı tanımlayan ve olayın nasıl ilintilendirileceğini ve düzenleneceğini belirlemek için olayları düşük düzeyli ve yüksek düzeyli kategorilere eşleyen bir sınıflama.

R

rapor Sorgu yönetiminde, bir sorgunun çalıştırılıp sorguya bir form uygulanması sonucunda elde edilen biçimlendirilmiş veriler.

rapor aralığı
Sonunda olay işleyicisinin tüm yakalanan olayı ve akış verilerini konsola göndermesi gerektiği yapılandırılabilir bir zaman aralığı.

recon Bkz. keşif.

R2L Bkz. Uzaktan Yerele.

R2R Bkz. Uzaktan Uzağa.

S/Ş

Sınıfsız Etki Alanı İçi Yönlendirme (CIDR)
Sınıf C İnternet Protokolü (IP) adreslerini ekleme yöntemi. Adresler müşterilerin kullanımı için İnternet Hizmet Sağlayıcılarına (ISP) verilir. CIDR adresleri, yönlendirme çizelgelerinin boyutunu küçültür ve kuruluşlarda daha çok IP adresini kullanılabilir kılar.

sistem görünümü
Bir sistemi oluşturan birincil ve yönetilen anasistemlerin görsel temsili.

site dışı hedef
Bir olay toplayıcıdan olay ya da veri akışı alan birincil sitenin dışındaki bir aygıt.

site dışı kaynak
Bir olay toplayıcıya normalleştirilmiş veriler ileten birincil sitenin dışındaki bir aygıt.

SNMP Bkz. Basit Ağ Yönetimi Protokolü.

SOAP Merkeziliği kaldırılmış, dağıtılmış bir ortamda bilgi alışverişine yönelik hafif bir XML tabanlı protokol. Bilgileri sorgulayıp döndürmek ve İnternet'te hizmetleri çağırmak için SOAP kullanılabilir.

şifreleme
Bilgisayar güvenliğinde, özgün verilerin alınamadığı ya da yalnızca şifre çözme işlemiyle alınabildiği şekilde verileri anlaşılmaz bir biçime dönüştürme işlemi.

T

tam ağ adı (FQNN)
Ağ sıradüzeninde, tüm departmanları içeren bir nesnenin adı. Tam ağ adına örnek: CompanyA.Department.Marketing.

tam etki alanı adı (FQDN)
İnternet iletişiminde etki alanı adının alt adlarının tümünü içeren anasistem adı. Tam etki alanı adına örnek: rchland.vnet.ibm.com.

tarayıcı
Web uygulamalarındaki yazılım güvenlik açıklarını arayan otomatik bir güvenlik programı.

TCP Bkz. İletim Denetimi Protokolü.

U/Ü

uç nokta
Bir ortamdaki API ya da hizmetin adresi. API bir uç noktayı açığa çıkarır ve aynı anda diğer hizmetlerin uç noktalarını çağırır.

uygulama imzası
Paket yükünün araştırılmasından türetilen ve sonra belirli bir uygulamayı tanımlamak için kullanılan benzersiz bir özellik kümesi.

Uzaktan Uzağa (R2R)
Bir uzak ağdan başka bir uzak ağa gerçekleştirilen dış trafik.

Uzaktan Yerele (R2L)
Bir uzak ağdan yerel ağa gerçekleştirilen dış trafik.

üst akış
Depolama kısıtlamalarını azaltarak işleme kapasitesini artırmak için benzer özelliklere sahip birden çok akıştan oluşan tek bir akış.

V

varlık Bir işletim ortamında devreye alınması tasarlanan ya da devreye alınan yönetilebilir bir nesne.

veri noktası
Bir metriğin, bir zaman noktasındaki hesaplanan değeri.

veritabanı yaprak nesnesi
Bir veritabanı sıradüzenindeki uçbirim nesnesi ya da düğümü.

W

whois sunucusu
Etki alanı adları ve IP adresi ayırmaları gibi kayıtlı İnternet kaynakları hakkında bilgi almak için kullanılan bir sunucu.

Y

yanlış pozitif
Pozitif olarak sınıflandırılan (sitenin güvenlik açığı olduğunu belirten), ancak gerçekte kullanıcının negatif olduğuna (güvenlik açığı olmadığına) karar verdiği bir test sonucu.

yaprak
Ağaç yapısında alt öğesi olmayan bir girdi ya da düğüm.

yedek sistem
Etkin sistem başarısız olduğunda otomatik olarak etkinleşen sistem. Disk eşleme etkinleştirilirse, etkin sistemden verileri eşler.

yenileme zamanlayıcısı
Geçerli ağ etkinliği verilerini güncelleyen zamanlanmış aralıklarda otomatik olarak ya da el ile tetiklenen bir dahili aygıt.

yerel ağ (LAN)
Tek bir bina ya da yerleşke gibi sınırlı bir alandaki birkaç aygıtı bağlayan ve daha büyük bir ağa bağlanabilen ağ.

Yerelden Uzağa (L2R)
Bir yerel ağdan başka bir uzak ağa gerçekleştirilen dahili trafikle ilgili.

Yerelden Yerele (L2L)
Bir yerel ağdan başka bir yerel ağa gerçekleştirilen dahili trafikle ilgili.

yinelenen akış
Farklı akış kaynaklarından alınan aynı veri iletiminin birden çok eşgörünümü.

yönetici paylaşımı
Yönetici ayrıcalıklarına sahip olmayan kullanıcılardan gizlenen bir ağ kaynağı. Yönetici paylaşımları, yöneticilere bir ağ sistemindeki tüm kaynaklara erişme yetkisi sağlar.

yönlendirme kuralı
Olay verileri tarafından ölçütleri karşılandığında, bir koşul toplamının ve sonraki yönlendirmenin gerçekleştirildiği bir koşul.

yüksek kullanılabilirlik (HA)
İş yüklerinin kümedeki kalan düğümlere yeniden dağıtılabilmesi için düğüm ya da yardımcı program hataları oluştuğunda yeniden yapılandırılan bir kümelenmiş sistemle ilgili.

yük verileri
Üstbilgi ve yönetici bilgileri dışında bir IP akışında bulunan uygulama verileri.

Dizin