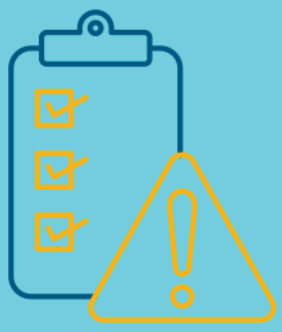
Bir İhlal ve Saldırı Simülasyon Platformunun En Önemli 5 Kritik Özelliği



SafeBreach

OTD BİLİŞİM

İçindekiler

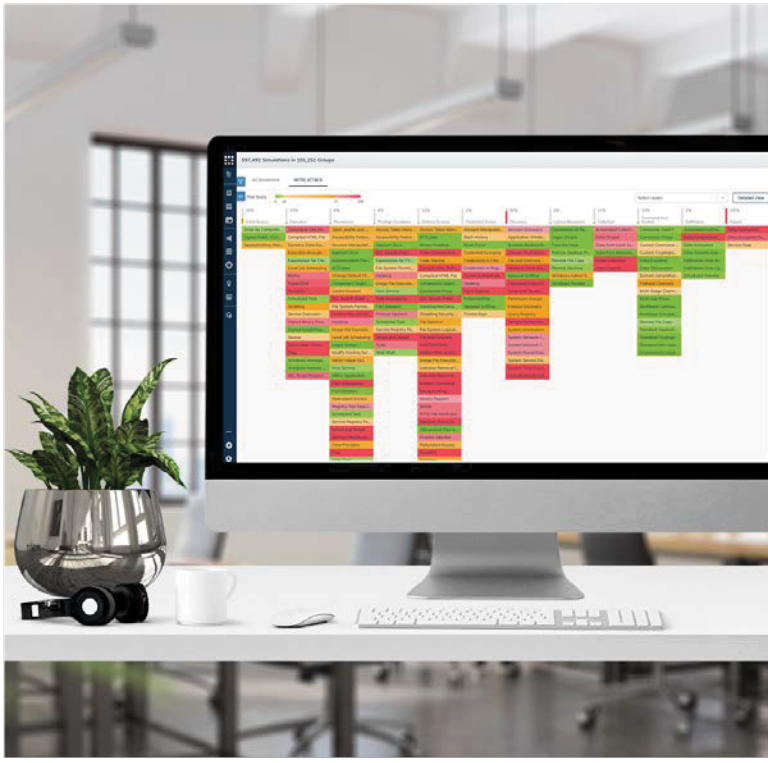
Giriş

Bilinmeyen "Sıfır Gün" tehditleri manşetleri süslese de, aslında, güvenlik ihlallerinin büyük çoğunluğunda, saldırganlar yanlış yapılandırılmış sistemleri veya yazılım veya donanımdaki iyi belgelenmiş güvenlik kusurlarını kullanır.

Modern bir işletmenin BT altyapısı, dinamik ağlardan, bulut altyapısından, düzinelerce yazılım uygulamasından ve binlerce uç nokta cihazından oluşan karmaşık bir mimariden oluşur. Her bir mimari unsurunun kendi güvenlik kontrolleri vardır. bir saldırganın altyapınıza, ağlarınıza, cihazlarınıza ve yazılımınıza girmesi için ihtiyaç duyduğu tek şey basit bir yanlış yapılandırma veya daha az güvenli yapılandırmalara geçiştir.

Pratik açıdan, birden fazla kurumsal güvenlik ekibinin işlerini manuel olarak koordine etmesi ve çakışan tüm sistemler için yapılandırmaları optimize etmesi neredeyse imkansızdır. Farklı ekiplerin kendi yönetim görevleri, yetkileri ve güvenlik endişeleri vardır. Ek olarak, sürekli optimizasyonlar ve manuel testler yapmak, zaten az personele sahip güvenlik ekiplerine ağır bir yük getirir. Bu nedenle güvenlik ekipleri, sürekli olarak ortaya çıkan (ve çoğunlukla kendi kendine uygulanan) güvenlik zayıflıklarını azaltmak için İhlal ve Saldırı Simülasyonu'na (BAS) yöneliyor.

BAS, temel olarak eski Sızma Testi ve Güvenlik Açığı Yönetimi araçlarından farklıdır. Bu yaklaşımların her ikisi de önemli ölçüde manuel rehberlik gerektirir ve aslında güvenlik ekipleriniz için daha fazla iş ve daha fazla parazit yaratır. Buna karşılık, BAS, kapsamlı oyun kitaplarındaki binlerce saldırıyı tamamen otomatik hale getirir ve sürekli olarak bunları simüle eder. BAS, yanlış yapılandırmaları ve güvenlik açıklarını tespit eder; ve en yüksek öncelikli azaltmaları açıkça göstermek için daha da ileri gitmelidir. Bu, güvenlik ekiplerinin daha az kaynakla daha fazlasını başarmasına ve reaktif bir güvenlik duruşundan kuruluşlarına BT altyapısının ve verilerinin güvenli olduğuna ve öyle kalacağına dair çok daha yüksek düzeyde güvence sağlayan proaktif bir güvenlik duruşuna geçmelerini sağlar. Sürekli simülasyonlar, kuruluşun güvenlik duruşunu aşamalı olarak iyileştirmesini sağlar.



Daha fazla güvenlik kontrolü kurumunuzu daha güvenli yapmaz.

Bir BAS Platformundan Ne İstenir?

BAS çözümleri, karmaşık bir kurumsal ortamının büyüklüğüne uymak ve en etkili şekilde kullanılmak için birkaç kritik yeteneğe sahip olmalıdır. Bu belge, bu önemli yeteneklerin neler olduğunu ve en iyi güvenlik sonuçlarının sağlanmasına nasıl katkıda bulunduklarını ve kuruluş için iş riskini nasıl azalttığını açıklar.

İhlal ve Saldırı Simülasyonu

Güvenlik kontrolü doğrulaması için

Simüle eder

Tüm saldırıları simüle etmek veya Tehdit Grupları, Taktikler ve Teknikler temelinde simülasyon yapmak veya tüm saldırıları simüle etmek veya Tehdit Grupları, Taktikler ve Teknikler veya belirli kötü amaçlı yazılım türleri temelinde simülasyon yapmak için belirli kötü amaçlı yazılım tür saldırı yöntemlerini içeren kapsamlı bir saldırı yöntemleri kılavuzu sağlar.

Görselleştirme

Risk puanına, MITRE ATT&CK ısı haritasına ve verilerin nasıl sızdırılabileceğine ilişkin Altyapı görünümüne dayalı olarak güvenlik duruşunuzun resmini çizmek için simülasyonlardan elde edilen veriye dayalı sonuçları sunar.

Önceliklendirme

Güvenlik açığı yönetimi çözümlerinden VM taramalarını alın ve kuruluş için nelerin risk altında olabileceğine dayalı olarak yama yönetimine uygun şekilde öncelik vermek için istismar edilebilirliğe dayalı yeni puan belirlemek için simülasyon sonuçlarını ilişkilendirir.

Düzeltme

Güvenlik duruşunu sağlamlaştırmak için güvenlik kontrollerine ve yama yönetimine odaklanma ortak hedefiyle çapraz işlevli ekipleri bir araya getirir.

SafeBreach

OTD BİLİŞİM

1. Saldırı Tekniği ve APT Kapsamı

Otomatik saldırıların hacmi ve şiddeti giderek artarken, saldırganlar bir hedefi ihlal etmeye çalıştıklarında çok sayıda açıktan yararlanmayı dener ve farklı türdeki zayıflıkları test eder. Ek olarak, bilgisayar korsanları genellikle bir kuruluşun hangi güvenlik kontrollerini ve sistemlerini çalıştırdığını tespit edebilir ve saldırılarını bu sistemlerin kör ve zayıf noktalarını eşleştirmek için ayarlayabilir.
Bir BAS platformunun, tüm Gelişmiş Kalıcı Tehditleri (APT'ler) kapsayan saldırı taktikleri, teknikleri ve prosedürleri (TTP'ler) içeren, yararlanabileceği kapsamlı bir çalışma kitabı olmalıdır. Bu çalışma kitabı, MITRE ATT&CK çerçevesinin TTP'lerini içermeli, ancak bunlarla sınırlı olmamalıdır.

Tüm Büyük Saldırı Yüzeylerinin Kapsanması

Kurumsal BT ayak izleri büyük ve karmaşıktır. Çok sayıda ağ çözümünden oluşurlar, tam dizi uç nokta cihazları, Windows ve Linux sunucuları ve Windows ve Mac'in her sürümünü çalıştıran masaüstü ve dizüstü bilgisayarların bu altyapıya dağıtılması muhtemeldir. Karmaşık ve dinamik ortamların güvenlik duruşunu doğrulamak ve izlemek, son derece zorludur ve güvenlik ve operasyon ekipleri için bir yüktür.
Eksiksiz bir BAS platformu, ağ, uç nokta, bulut ve e-posta gibi ana saldırı cephelerini kapsamalıdır. Örneğin, şirket içinde, yerel ve dağıtılmış makinelerde ve bulutta çalıştırdığınız tüm büyük işletim sistemlerini test edecektir. BAS, tüm güvenlik kontrollerini kapsamalıdır çünkü bunlar genellikle yama, güncelleme ve diğer normal BT süreçlerinin bir parçası olarak yanlışlıkla yapılan yanlış yapılandırmalara tabidir.

Kuruluşlar buluta geçerken, bir BAS çözümünün genel ve özel bulut altyapısına (IaaS) yönelik saldırıları simüle etmesi ve IAM, ağ, depolama ve yönetici erişimi dahil olmak üzere kontrol düzlemini ele alması zorunludur. Bulut teknolojisi yığınını yukarı taşımak ve yanal hareket, sistem kötüye kullanımı, ayrıcalık yükseltme ve onaylanmamış süreçleri çalıştırmayı kapsayan veri düzlemini ele almak da çok önemlidir. Artık konteyner tabanlı uygulamalara odaklanan saldırılarla, BAS platformunun özellikle Docker konteynerleri için saldırılara sahip olması önemlidir.

SafeBreach | OTD BİLİŞİM

Yeni Tehditlerde SLA

Bir BAS platformunun, yeni ortaya çıkan tehditleri hızla kapsayacak bir yöntemi olmalıdır. Yeni bir US-CERT uyarısı aracılığıyla yeni bir tehdit belirlenip duyurulduğunda, güvenlik ekipleri buna karşı hızlı bir şekilde test yapabilmeli ve tehdidin hangi güvenlik açıklarından yararlanabileceğini belirleyebilmelidir. Daha spesifik olarak, bilinen tehditleri kapsama konusunda bir BAS platformunun SLA'sını ve yanıt süresi garantilerini kontrol etmelisiniz. Bir BAS tedarikçisinin Ar-Ge ekibi, birkaç gün içinde tespit edilen veya ortaya çıkan herhangi bir US-CERT tehdidini kapsayan kapsamlı bir simülasyon seti gönderebilmelidir. Bu, kuruluşların tehditle ilgili simülasyonlar yayınlanır yayınlanmaz savunmalarını doğrulamasını sağlar. Kuruluşları yeni US-CERT uyarılarına karşı korumak için simülasyon eklemesi bir hafta veya daha uzun süren BAS platformlarına dikkatle bakılmalıdır; bu süre zarfında bilgisayar korsanları, bir kuruluşun altyapısını tehlikeye atmak için yeni yayınlanan uyarıdan yararlanabilir ve işletme ciddi şekilde etkilenebilir.

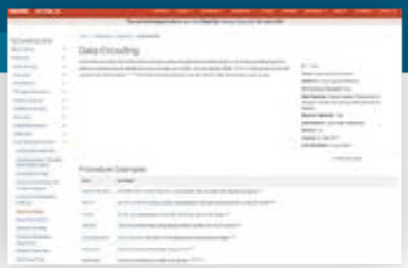
Kapsam Esnekliği

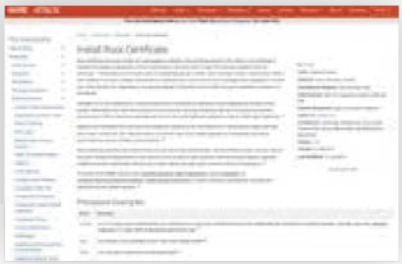
Kuruluşun bilinen tüm saldırılara karşı güvende olmasını sağlaması için BAS'ın geniş bir saldırı kapsamına sahip olması zorunludur. Bir saldırının biliniyor olması, onu bugünün altyapısında geçerli kılmaz. Verimlilik ve sonuçların daha iyi yorumlanması için BAS platformu, günümüzde potansiyel olarak zarar verebilecek saldırı yöntemlerine vurgu yapmalı ve test önceliği vermelidir. Aynı zamanda, BAS platformunun, güvenlik ekiplerinin belirli taktiklere veya tekniklere odaklanmasını sağlamak için esnekliğe ihtiyacı vardır. Örneğin, kuruluş için yüksek önceliğe sahip belirli tehdit gruplarının TTP'lerini test etme becerisine ihtiyaç duyacaklar. Ekip, kuruluştaki tüm simülatörlerde belirli bir tehdit grubuyla ilişkili tüm taktikleri ve teknikleri çalıştırmaya karar verebilir. Yönetici süiti veya yönetim kurulundan "x, y ve z tehditlerine karşı ne kadar güvendeyiz?" sorusu geliyorsa, BAS platformu cevabı hızlı bir şekilde verebilmelidir.

Saldırıların Gerçekliği ve Geçerliliği

Simüle edilmiş saldırılar, gerçek bir saldırıya mümkün olduğunca yakın olmalıdır. Örneğin, bir saldırının ağ kaydını çalıştırmak, bir üretim veya üretime yakın ortamda çalışan iki canlı, gerçek kuruluş (SafeBreach simülatörleri olan) arasındaki saldırıyı fiilen yürütmekten farklıdır. Aynı şekilde, ortamı ve konfigürasyonları taramak ve bir saldırının potansiyel başarısını belirlemek, saldırıyı fiilen gerçekleştirmek ve sonucu görmekle aynı şey değildir.

SafeBreach, MITRE ATT&CK bilgi tabanına ve çerçevesine aktif olarak yeni teknikler katan tek BAS satıcısıdır. SafeBreach Labs, çerçeveye dört yeni teknik kattı. Orijinal araştırmaya bağlılık, platformun yeteneklerini hızla gelişen güvenlik tehditlerinin önüne geçirmek için bir BAS sağlayıcısı için temel bir gerekliliktir.





"Kızıl (Red) Ekip" Operasyonları

Genişletilebilir bir BAS platformu, kırmızı ekiplerin ölçeklendirmesini ve daha önce mümkün olandan daha geniş test kapsamı oluşturmasını sağlar. Kırmızı ekip, yeni TTP'leri ve saldırı ilerlemelerini daha iyi tahmin etmek için kendi saldırılarını platforma oluşturma veya yükleme yeteneği istiyor. Bu genişletilebilirlik, kırmızı ekibin şunları ele almasına izin verecektir:

• Çeşitli çerçevelerde kapsanamayan kuruluşa özgü riskler

• Yakın zamanda keşfedilen ancak yama sürecinde henüz çözülmemiş yeni riskler

Bu şekilde, BAS çözümü, yeni saldırı kombinasyonları geliştirmek için platformda halihazırda mevcut olan saldırıların yapı taşlarını birleştirebilmelidir. Bu, saldırı geliştirmeye hız ve verimlilik katar. BAS platformu ayrıca yeni saldırılar ekleme, ağ kaydından (PCAP) veya Python gibi programlama dillerinden yararlanma yollarını da desteklemelidir.

Bilinmeyen Tehdit Kapsamı

Bilinen tehditlerin kapsanması yeterli değildir. Açık olmayabilecek bilinmeyen tehditleri ve kalıpları kapsamak için kapsamlı bir BAS platformu, saldırgan davranışları ve genel siber güvenlik taktikleri, teknikleri ve prosedürleri için yeterli kapsama sahip olmalıdır. İdeal olarak, bu kapsam Securityfocus, GitHub ve Reddit gibi iyi bilinen saldırı bilgi kaynaklarından yararlanacaktır. Her kuruluş, hangi bilgi kaynaklarının en önemli olduğunu belirleyebilmeli ve saldırı oyun kitaplarını sürekli güncellemek için bu saldırıları ekleyebilmelidir.

2. Güvenle Çalışın, Doğruluğu Sağlayın ve Akıllıca Ölçeklendirin

Kuruluş genelinde test edilebilecek binlerce saldırı senaryosuna sahip olmak, güvenlik ekiplerine test için zaman sağlar. Kırmızı ekiplerin, organizasyonla ilgili olmayabilecek bazı saldırılar da dahil olmak üzere, artık her saldırıyı oluşturması gerekmiyor.
Otomatik ihlal ve saldırı simülasyonu, sürekli olarak saldırı senaryoları çalıştırarak, insanların yeni yüksek öncelikli saldırılara ve şüpheli güvenlik açıklarına, vahşi doğada görülmeden önce proaktif olarak odaklanmasına olanak tanır. Ayrıca BAS platformunun ağda saldırı simülasyonlarını düzgün bir şekilde çalıştırmak için karmaşık konfigürasyonlar gerektirmemesi de önemlidir, çünkü bu güvenlik ekiplerine yük olabilir ve raporlamayı yavaşlatabilir.

Akıllıca Ölçeklendirme

Akıllıca ve kolayca ölçeklendirmek için, BAS platformunun, saldırı yüzeyindeki belirli noktalara karşı hangi saldırıların gerçekleştirilmesi gerektiğini belirlemesi gerekir. Hangi tür saldırıların çalıştırılacağını, altyapıda nerede çalıştırılacağını ve hangi sıra veya dönüşlerde çalıştırılacağını otomatik olarak belirleyebilmelidir. Örneğin, bir BAS platformu Windows saldırılarını yalnızca Windows makinelerinde, MacOS saldırılarını yalnızca Mac'lerde, Linux saldırılarını yalnızca Linux sunucularında ve Windows Sunucularında yalnızca Windows Sunucularında saldırı gerçekleştirmelidir. Benzer şekilde, BAS platformu, BT varlıklarının bağlamını tanımalı ve örneğin, yalnızca veritabanlarına ve veri altyapısının diğer bölümlerine karşı veri hırsızlığı istismarlarını çalıştırmalıdır. Bu yetenekleri kullanmadaki bu zeka, operasyon ekibini strese sokmadan BAS sisteminin otomatik olarak büyük bir kuruluşa ölçeklenmesine yardımcı olur. Ek olarak, saldırı bir kontrol veya başka bir iyileştirme önlemi ile zincirin daha yukarılarında engellenmiş olsa bile, BAS'ın gelişmiş güvenlik iyileştirme fırsatlarını tespit etmek için tüm öldürme zinciri boyunca saldırı oyun kitaplarını test edebilmesi gerekir.
Büyük bir organizasyonun güvenlik duruşunu doğru bir şekilde test etmek ve ölçmek ve büyük bir organizasyon için ölçek büyütmek için bir BAS platformunun, bilinen saldırıları sürekli ve otomatik olarak simüle etmesi ve saldırı profillerini ve simülasyon parametrelerini yapılandırmak için manuel ayarlama ve etkileşimler gerektirmemesi gerekir.
Örneğin, kapsamlı manuel ayarlama, güvenlik ekibinin dinamik ağ yollarını anlamasını gerektiren zaman alıcı ve karmaşıktır. Manüel olarak ayarlanmış BAS, potansiyel olarak kör noktalar oluşturan insan yanlılığını ortaya çıkarır.

Servis ve Uygulamaları Etkilemeden Üretim Devam Ederken Çalıştırma

Bir BAS platformunun kurumsal güvenlik duruşu hakkında doğru bir şekilde rapor vermesi için, yansıtılmış bir üretim ortamında değil, gerçek bir üretim ortamında çalışması gerekir. Simülasyonları bir laboratuvarda çalıştırmak veya üretimden atmosfer sağlamak, gerçek bir kurumsal ağın tüm hareketli parçalarını etkin bir şekilde test etmeye imkan vermez. "Üretimde" çalışan simülasyonlar ile "üretim uygulamalarına karşı çalışan" simülasyonları birbirinden ayırmak önemlidir. Simülatörler, üretim ağını geçerek üretime kurulmalı ve kuruluştaki tüm uç noktaları (Windows masaüstü işletim sistemleri, Windows Sunucu İşletim Sistemleri, Linux Sunucu İşletim Sistemleri, Mac İşletim Sistemleri) ve bunların güvenlik ayarlarını temsil etmeli ve bunlar üzerinde çalışmalıdır.

Simülasyonlar Canlı Uygulamaları veya Hizmetleri Etkilememelidir

Saldırı yöntemlerinin simülatörden simülatöre, ağ üzerinden ve uç noktalarda çalışması gerekir, ancak üretim uygulamalarına ve hizmetlerine karşı çalıştırılmamalıdır. Canlı üretim uygulamalarıyla etkileşime giren simülasyonları çalıştırmak, BT güvenliği ve DevOps ekipleri üzerinde kesinti süresine, gelir kaybına ve aşırı yüklere neden olma riskini beraberinde getirecektir.

Bir BAS platformu herhangi bir üretim hizmetini durdurur veya yavaşlatırsa, büyük olasılıkla muhalefetle karşılaşacaktır. Aslında, bir kuruluştaki haydut unsurlar, hizmet sunumunu herhangi bir şekilde etkiliyorsa, aktif olarak BAS platformunu yıkmaya veya kapatmaya çalışabilir. Bu, platformun simüle edilmiş saldırılar gerçekleştirirken gerçek canlı prodüksiyon sistemleriyle hiçbir etkileşim olmamasını sağlaması gerektiği anlamına gelir.

Tüm BAS İşlemleri Geri Alınabilir niteliktedir

Başka bir deyişle, platform çerçevesi, BAS etkinliğinin bir parçası olarak gerçekleştirilen herhangi bir işlemin tamamen tersine çevrilebilir olmasını ve programlı olarak geri alınmasının kolay olmasını sağlamalıdır. Bu, bir üretim ortamında saldırıların güvenli bir şekilde yürütülmesini sağlar.

3. Kullanım Kolaylığı ve Ekosisteme Entegrasyon

Son birkaç yıl içinde birçok kuruluş, siber saldırılara karşı savunmak için çok sayıda güvenlik çözümü satın almaya odaklandı. Bunlara arasında ağ araçları, uç nokta çözümleri, güvenli ağ geçitleri, DLP, SIEM, SOAR ve Güvenlik Açığı Yönetimleri bulunmaktadır. Çoğu güvenlik ekibi, işlerine önemli ölçüde karmaşıklık katan "araç artışından" sıkıntı çeker. İronik bir şekilde, araçların yayılması/ artması, tehditlere karşı koruma sağlamak için 70 ila 100 güvenlik kontrolünü yerinde kullanmanın ve yapılandırmanın karmaşıklığı ve bunların birlikte nasıl çalıştıklarına dair doğru farkındalığı sağlama zorluğu nedeniyle güvenliği korumak gerçekten zor hale geldi.

Herhangi bir güvenlik aracı, yanlış yapılandırılırsa veya diğer sistemlere düzgün şekilde entegre edilmezse işe yaramaz olabilir. Bu nedenle, herhangi bir yeni çözüm, doğru bir şekilde kabul edilebilmesi ve yararlanılabilmesi için karmaşıklığı artırmamalı, azaltmalıdır.

Bir BAS platformunun kullanımı kolay olmalı ve ayrıca bir kuruluşun kullandığı diğer güvenlik araçlarının ve kontrollerinin kullanım kolaylığını ölçülebilir şekilde artırmalıdır.

Başlangıç olarak, etkili bir BAS, sızma, ana bilgisayarlardan yararlanma, yanal hareket etme ve verileri sızdırma amaçlı saldırıları simüle ederek her bir çözüm için her güvenlik kontrolünü test edecektir. Bu BAS süreci, tüm kontrollerde tek test noktası olarak hizmet eder ve sızma testi sistemlerinin manuel olarak doğrulanması veya ayarlanması gibi hantal süreci basitleştirir. İkinci olarak, etkili bir BAS, mevcut iş akışlarına sorunsuz bir şekilde uymalı ve etkin bir şekilde entegre edilmesi ve düzgün çalışması için ek ayrı iş akışları veya önemli profesyonel hizmetler gerektirmemelidir.

Bu entegrasyon yeteneğinin temel unsurlarından bazıları şunlardır:

Güvenlik Olaylarının Otomatik Analizi - Teknoloji Entegrasyonları

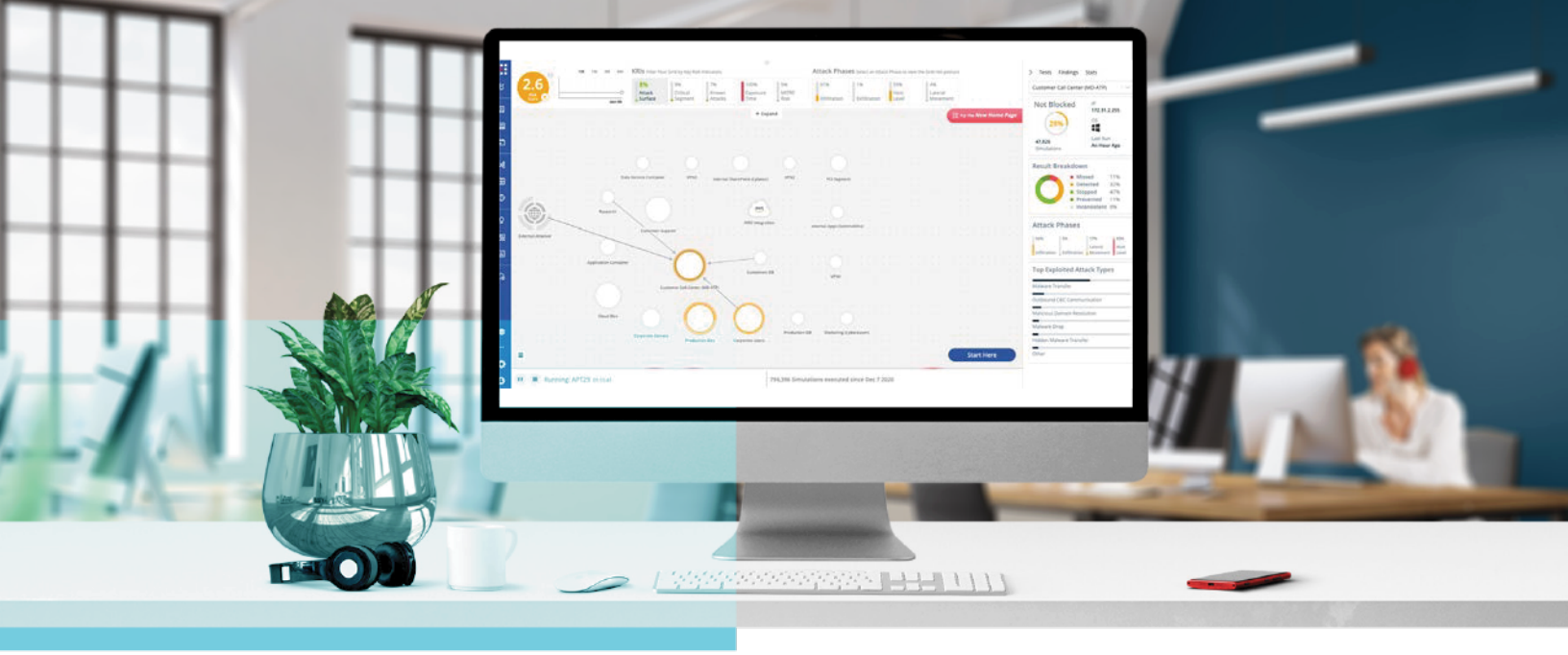
Güvenlik ekosisteminin her bir saldırı türüne nasıl tepki verdiğini anlamak, güvenlik duruşunu iyileştirmenin anahtarıdır. BAS platformları, güvenlik olaylarını simüle edilmiş saldırılarla otomatik olarak ilişkilendirmek için uç nokta, ağ ve SIEM çözümleriyle entegre olmalıdır.

Bu, güvenlik ekibine önemli olayları analiz etme ve arama ve boşlukları tanıma konusunda önemli ölçüde zaman kazandırır. Etkili entegrasyon, BAS platformunun, simüle edilmiş bir saldırının güvenlik ekosistemi tarafından önlenip engellenmediğini, tespit edilip edilmediğini veya tamamen kaçırıldığını otomatik olarak belirlemesini sağlar

Otomatikleştirilmiş İş Akışları ve Süreçlerle Entegrasyon

BAS, otomatik ihlal düzeltmesi yapmak için SOAR, SIEM ve biletleme çözümleriyle sıkı iş akışı entegrasyonlarına sahip olmalıdır. İş akışı sistemleriyle entegrasyonlar, sorunların azaltılması ve düzeltilmesi için gerekli olan ek bilgi toplama, yapılandırma değişiklikleri ve analist onaylarına yönelik süreçleri başlatmak için kullanılabilir. Zamanla, bu iki yönlü iş akışı entegrasyonları, güvenlik ekibinin BAS tarafından keşfedilen sorunları hızlı ve etkili bir şekilde azaltma yeteneğini geliştirerek güvenlik duruşunu iyileştirir ve ihlal riskini azaltır.

Özetlemek gerekirse, güvenlik ekiplerinin zamanlarını nasıl harcadıklarına ilişkin bir analiz, testin manuel olarak değiştirilmesine daha az zaman harcandığını ve BAS aracını entegre etmek için çok az veya hiç ekstra zaman harcanmadığını göstermelidir. Aksi takdirde, BAS platformu biraz ters etki yapabilir.



Risk Puanlaması ve Açıkların Önceliklendirilmesi

BAS'ı uygulamak, kuruluşta yüz binlerce saldırı yürütmek anlamına gelir. Ekiplerin, BAS simülasyonları tarafından oluşturulan çok sayıda uyarıyı (her biri keşfedilen bir güvenlik açığını bildiren) analiz etmesini ve buna göre hareket etmesini beklemek gerçekçi değildir. Ölçeklenebilir bir BAS platformu, güvenlik ve altyapı ekiplerinin iş riskine dayalı güvenlik duruşunu iyileştirmek için daha yüksek bir düzeyde bütünsel olarak çalışabilmesi için bireysel sonuçları soyutlama ve azaltma eylemlerini otomatik olarak çıkarma yeteneğine sahip olmalıdır.

BAS çözümleri, bir kuruluşun genel güvenlik duruşunu anlamasına yardımcı olmak için kritik verileri bir araya getirmelidir. BAS, kapsamlı verilerle yönlendirilen bir risk derecelendirme yaklaşımı uygulayarak farklı güvenlik ekiplerini de bir araya getirebilir. Bu yeteneği genel olarak yararlı kılmak için, aşağıdakiler gibi belirli tüketici sınıfı özellikleri içerecektir:

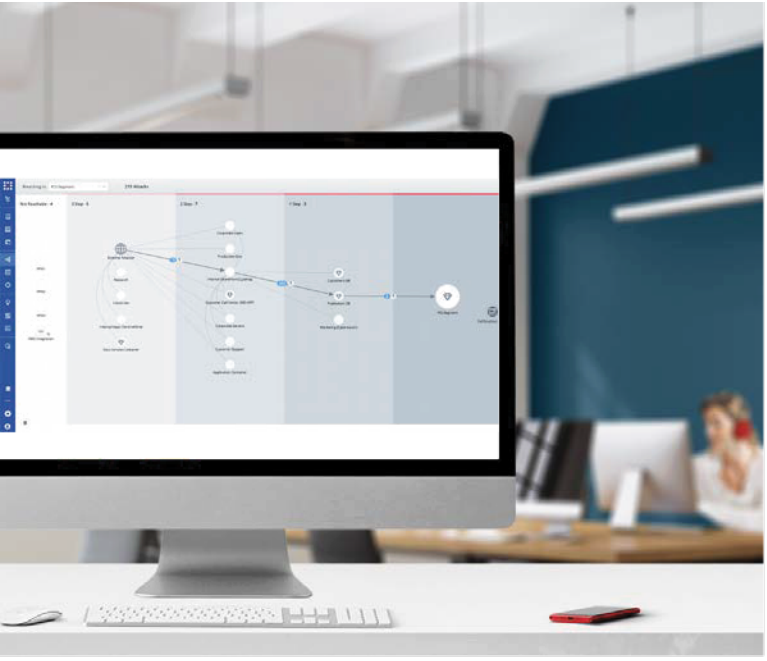
- Yönetici raporları ve otomatik raporlama
- Kontrol panelleri
- Isı haritası ve görselleştirme araçları

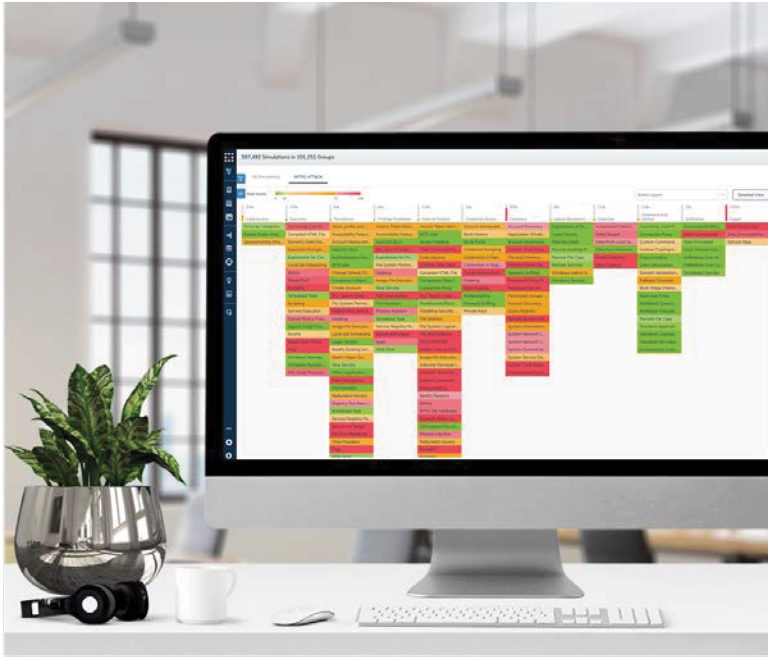
Bunlar, kullanıcıların BAS simülasyon bulgularını ve önerilen sonraki adımları kolayca özümsemelerine ve anlamalarına yardımcı olur. Daha spesifik olarak, bu risk ve önceliklendirme yeteneği aşağıdaki bileşenleri içermelidir:

Kilit Risk Göstergeleri

Risk göstergeleri, kuruluşunuzun ilerlemesini izlemenize, güvenlik duruşunuzun gerçekten geliştiğini doğrulamanıza ve zaman içindeki eğilimleri anlamanıza yardımcı olur. İzlenen risk göstergesi türleri, kuruluşunuzun en çok neye önem verdiğini yansıtmalıdır. Örneğin, genel saldırı yüzeyi, savunmalardan geçen saldırı girişimlerinin yüzdesi olarak ölçülür Başka bir gösterge, engellenen MITRE çerçeve saldırılarının yüzdesi olarak ölçülen saldırılara karşı savunmanın başarı oranı olabilir. Bir kuruluş, kritik bölümlerine karşı riskleri hesaplamak veya finansal işlemleri içeren veya finansal verileri ve PII'yi depolayan hizmetlerin risk değerini yükseltmek isteyebilir. Bir BAS, seçmeyi, kalibre etmeyi ve ardından bu göstergelere karşı ölçüm yapmayı kolaylaştırmalıdır. Ek olarak, bir BAS, aşağıdakileri izlemek için bir ihlalin keşfedilmesinden çözülene kadar maruz kalma süresini ve ayrıca düzeltmenin başarı oranını hesaplayabilmelidir:

- Bir güvenlik ekibinin verimliliği ve yanıt verebilirliği
- Güvenlik duruşunu iyileştirmenin etkinliği





MITRE ATT&CK Isı Haritası

MITRE ATT&CK çerçevesi, siber güvenlik için ortak bir dil oluşturur. ATT&CK gezgininden yararlanmak, bir BAS platformunun harita maruziyetlerinin ısı haritasını çıkarmasına olanak tanır ve bu son derece görsel yaklaşım, ortak iyileştirme hedeflerini takip etmek için ekipleri hızla bir araya getirir. Kuruluşu hedefleyen tüm saldırılara veya belirli tehdit gruplarına veya tekniklere dayalı simülasyon oldukça faydalıdır. Simülasyon sonuçlarının ısı haritası, ekipleri hızlı bir şekilde maruz kalma alanlarına odaklar.

Bir MITRE ATT&CK Isı Haritasına dahil edildiğinde simülasyon sonuçları, test edilen tüm saldırıların güvenlik durumu hakkında genel bir fikir vermelidir. Isı haritası, ekiplere hangi simülasyonların engellendiğine veya tespit edildiğine ve düzeltme seçeneklerine ilişkin ayrıntılı bir görünüm için belirli saldırı tekniklerini derinlemesine inceleyen testler seçmesinde yardımcı olur.

Saldırı Yollarının Haritalanması

Ekiplerin farklı azaltma görevlerini uygun şekilde önceliklendirmesine yardımcı olmak için, saldırıların dışarıdan bir varlığa nasıl ulaşabileceğini görselleştirmek değerlidir. Öldürme zincirinin (kill-chain) bir haritası veya diyagramı, bilgi güvenliği ekibinin zincirin en verimli şekilde nasıl kırılacağını görmesine yardımcı olur. Zengin görselleştirme yeteneği, güvenlik ekiplerinin kuruluşlarının tüm saldırı yüzeyini anlamasına ve değerlendirmesine yardımcı olur. Bu özellikle, bir ekip altyapının farklı kısımlarını yakınlaştırıp uzaklaştırabiliyorsa veya sonuçları temel niteliklere göre filtreleyebiliyorsa etkilidir. Görselleştirme, ekiplerin BAS tarafından tanımlanan en yüksek tehdit içeren güvenlik risklerinin ölüm zincirlerini görmelerini ve analiz etmelerini sağlayarak önceliklendirmeye yardımcı olur. Görselleştirme, örneğin, aşağıdaki hususlarda yardım sağlar:

1. Sızma veya sızma için harici saldırgandan hedef segmente giden bir yol olup olmadığına bakın.
2. Hedef segmentin diğer segmentlerden ne kadar açık olduğunu belirleyin
3. Birçok saldırı yoluna izin veren darboğaz segmentleri veya bağlantıları tespit edin.

Görselleştirmeler ayrıca, ilk sızma yöntemleri, ana bilgisayar tavizleri, yanal hareketler ve yayılmadan sızma, tecrit (fidye yazılımı) veya yok etme (silme saldırıları) bir saldırıya dahil edilen tüm serileri veya adımları gösterebilir.

Yönetici Raporları

Yönetici raporları, günlük operasyonların önceliklendirilmesini etkilemese de, ekiplerin güvenlik eylemlerine öncelik verme ve güvenlik varlıklarını tahsis etme stratejilerini iletmesine yardımcı olur.
Bir BAS çözümünde yönetici raporlarının istenen özellikleri:

- Kuruluşun güvenlik duruşunun net bir resmini iletmek
- Belirli Tehdit Grubu TTP'lerine karşı güvenlik duruşunu detaylandırmak
- Yapılandırma veya stratejide değişiklik yapılmasına yardımcı olmak
- Bütçe için destek talepleri
- Gerçek eğilimleri ve faaliyetleri gösterecek kadar kapsamlı olmalı
- Otomatik ve zaman içindeki ilerlemeyi (veya ilerleme eksikliğini) izleyebilmeli

Zengin görselleştirme yeteneği, güvenlik ekiplerinin kuruluşlarının tüm saldırı yüzeyini anlamasına ve değerlendirmesine yardımcı olur.

SafeBreach | OTD BİLİŞİM

4. Azaltma Faaliyetlerinin Önceliklendirilmesi

Bir BAS platformu, bilinen TTP'ler genelinde tüm güvenlik çözümlerinizin ve kontrollerinizin etkinliğini test etmek için sürekli olarak yüz binlerce ihlal yöntemini çalıştıracağından, bu, hafifletme için birçok uyarı ve öneri oluşturur. Olayları uygun güvenlik kontrolleriyle otomatik olarak ilişkilendirmek için uç nokta, ağ ve SIEM çözümleriyle entegrasyon esastır. Risk puanları, ısı haritaları ve ağ maruz kalma haritaları gibi özellikler, güvenlik ekiplerinin ve liderlerinin iyileştirme için odaklanılacak alanları görmesine ve miktarını belirlemesine yardımcı olur.
İyi tasarlanmış bir BAS platformu, güvenlik açıklarını tek tek düzeltmekten daha verimli olan bütünsel iyileştirme eylemleri sağlamak için tüm simülasyonlardan elde edilen sonuçları toplayacaktır. Tehditler ağ, web, uç nokta ve e-posta gibi kategorilere göre gruplandırılmalıdır. Bu, güvenlik, BT, ağ, uç nokta ve risk ekiplerinin çabalarını bütünsel bir iyileştirme planında koordine etmeyi daha uygun hale getirir.

Güvenlik ve altyapı ekiplerinin önce en kritik güvenlik açıklarını düzeltmesine yardımcı olmak için BAS çözümü, iş riskine göre sıralanmış bir yığın halinde önerilen azaltma eylemlerine öncelik vermelidir. Bu, hem BAS tarafından hem de BAS'ın tanımladığı güvenlik açıklarının genel kritikliğine ilişkin bağlamsal bilgileri alan bir önceliklendirme motoru tarafından yönlendirilir. Sıralama ayrıca, daha yüksek öncelikli varlıkları açıkça belirlemek için kuruluş tarafından tanımlanan iş mantığına da bağlıdır.
BAS platformu, tüm ekibin iş riskine dayalı güvenlik duruşunu iyileştirmek için en yüksek öncelikli iyileştirmelere odaklanabileceği en öncelikli birleşik çalışma alanı veya gösterge panosu oluşturmalıdır.
Önceliklendirme, küçük güvenlik değişikliklerini son derece önemli hale getirebilecek iş riskine dayanmalıdır. Örneğin, bir NextGen güvenlik duvarında bir kuralı güncellemek, bir işletmenin en değerli BT varlıklarını korumada büyük bir etkiye sahip olabilir. Buna karşılık, çokça duyurulan uç nokta saldırılarına karşı iyileştirme, aslında işin riskini azaltmak için çok az şey yapabilir.

Güvenlik Açığı Yönetim Çözümleri ile Entegrasyon

Daha gelişmiş BAS çözümleri, belirli BAS simülasyonlarına dayalı olarak organizasyonun tüm fiili sömürülebilir zayıflıklarının ölçümünü sağlamak için güvenlik açığı yönetimi tarama sonuçlarına içgörü sağlar

Problem

Güvenlik açığı yönetimi çözümleri, hangi cihazların belirli yamaların uygulanması gerektiğini belirlemek için bir kuruluştaki cihazları tarar. Güvenlik ve BT ekipleri, yüksek hacimli yama isteklerine ayak uyduramamaktadır. Ayrıca, güvenlik açığı yönetimi çözümlerinden gelen yama azaltma öncelik listesi, şu anda yürürlükte olan güvenlik kontrolleri göz önüne alındığında, hangi güvenlik açıklarından gerçekten yararlanılabileceğini dikkate almaz.İyi tasarlanmış bir BAS platformu, güvenlik açıklarını tek tek düzeltmekten daha verimli olan bütünsel iyileştirme eylemleri sağlamak için tüm simülasyonlardan elde edilen sonuçları toplayacaktır. Tehditler ağ, web, uç nokta ve e-posta gibi kategorilere göre gruplandırılmalıdır. Bu, güvenlik, BT, ağ, uç nokta ve risk ekiplerinin çabalarını bütünsel bir iyileştirme planında koordine etmeyi daha uygun hale getirir.

Çözüm

BAS çözümü, organizasyona yönelik olası riskleri ve riskleri anlamak için öldürme zinciri (kill chain) boyunca çeşitli saldırı türlerini simüle eder. VM ile entegrasyon, BAS çözümünün güvenlik açığı yama verilerini almasına ve ihlal ve saldırı sonuçlarıyla ilişkilendirmesine olanak tanır.

Sonuç

BAS çözümü, iş riskini azaltmaya odaklanan özelleştirilmiş bir yama yönetimi öncelik listesi tanımlar.

Örneğin, bir BAS çözümü, tam öldürme zincirini test etmek için truva atlarının e-posta, ağ ve uç nokta çözümlerine yönelik saldırı davranışlarını simüle edecektir. Bazı simülasyonlarda, saldırılar ağ tarafında engellenecektir; ve böylece öldürme zinciri boyunca daha fazla var olan güvenlik açıklarına asla ulaşamayacaklar. Ancak diğer simülasyonlarda, saldırının güvenlik kontrolleri tarafından engellenmemesi muhtemeldir ve bu, kuruluşa truva atının hangi güvenlik açıklarından yararlanabileceği ve öldürme zinciri boyunca devam edebileceği konusunda fikir verir.
Güvenlik açığı yönetimi ve BAS sonuçlarının konsolidasyonu, kuruluşun iş riski açısından güvenlik açıklarının sonuçlarını anlamasına ve kuruluş için yama yönetiminin en etkili önceliğini tanımlamasına yardımcı olur.

5. Değerleme Zamanı

Esnek Yerleştirme Seçenekleri

Esnek dağıtım seçeneklerine sahip olmak, CISO'ların ve CIO'ların mevcut altyapı ayak izlerini etkin bir şekilde güvence altına almalarını sağlar. Ayrıca, güvenlik duruşlarını altyapılarının devam eden evrimine uyacak şekilde uyarlamalarına da olanak tanır.
Bir BAS çözümüne hem SaaS hem de şirket içi sistem olarak erişilebilir olmalıdır. Şu anda, düzenlenmiş ortamların çoğu (finansal hizmetler, sağlık hizmetleri, devlet) şirket içi dağıtım gerektirmektedir. Ayrıca, kurumsal kullanıma hazır bir BAS, Windows, Linux ve MacOS dahil olmak üzere çeşitli işletim sistemlerinin simülatörlerine yerleşebilmelidir. Yine bir BAS platformu, Amazon Web Services, Microsoft Azure, Google Compute Platform ve diğerleri dahil olmak üzere büyük bulut ortamlarında da konuşlandırılabilir olmalıdır. Gerçekte, çoğu büyük kuruluş artık, barındırılan altyapıyı, özel bulutu ve genel bulutlara yayan hibrit bir altyapıya sahiptir. Bir BAS çözümü, bu gelişen hibrit mimarileri barındırmalıdır.

Yerleşim Kolaylığı ve Hızı

Simülatörler ve BAS platformları ne kadar hızlı ve kolay bir şekilde konuşlandırılabilir? Yerleşim için standart zaman çizelgesi hakkında soru sorarken, tahminlerin BAS platformu üretimini hazır hale getirmek için gereken test ve ayar süresini de içerdiğini doğrulayın. Yapılandırmalar, paneller ve rapor şablonları için ne kadar özelleştirme gerektiğini belirleyin. Saldırı simülatörü yapılandırmaları için, ağınızı ve uç noktalarınızı kapsayan saldırıları ayarlamak için gereken belirli adımları görmeyi isteyin. Bu karmaşıksa ve birçok adım gerektiriyorsa, BAS aracı önemli ölçüde bir devreye alma süresi gerektirecektir ve önemli ölçüde gizli bir karmaşıklık içerebilecektir. Ekibinizin platformda yetkin hale gelmesi için ne kadar eğitim gerektiğini öğrenin. Uzun kullanıma sunma süresi talep etmesi, yalnızca güvenlik duruşundaki iyileştirmeleri geciktirir.

Rol Tabanlı Giriş

BAS, yöneticilerden mavi ve kırmızı ekiplere kadar bir kuruluştaki birden fazla ekip tarafından kullanılacağından ve kullanılması gerektiğinden, BAS platformu rol tabanlı görevlendirmeleri desteklemelidir. Yöneticiler raporları ve gösterge tablolarını görüntüleyebilmeli, mavi ekipler ise çeşitli simülasyonları yapılandırabilir ve yürütebilir olmalıdır. Yalnız Kırmızı ekiplerin, yeni ve özel ihlal yöntemleri oluşturma becerisi olacaktır.

Sonuç

Esnek dağıtım seçeneklerine sahip olmak, CISO'ların ve CIO'ların mevcut altyapı ayak izlerini etkin bir şekilde güvence altına almalarını sağlar. Ayrıca, güvenlik duruşlarını altyapılarının devam eden evrimine uyacak şekilde uyarlamalarına da olanak tanır.

- SafeBreach ve Cybereason ortaklığı, kuruluşların Cybereason platformunun doğru şekilde konuşlandırıldığını ve optimum şekilde yapılandırıldığını doğrulamasını sağlayarak en son tehditlere karşı koruma sağlar.
- SafeBreach simülasyonları, olayla ilgili tüm verileri Cybereason'dan otomatik olarak çeker. İlişkili veriler, Cybereason platformunda daha fazla araştırma için hızlı bir bağlantı ile simülasyon sonuçlarına yerleştirilir.
- Güvenlik operasyon ekiplerinin güvenlik tehditlerine karşı daha hazırlıklı olmalarını sağlar.
- Saldırıları önlemek, tespit etmek ve bunlara yanıt vermek için gereken gerçek yaşam olay süresini azaltır.
- Cybereason'ın güvenlik kontrollerini optimize ederek genel saldırı yüzeyini küçültür.
- Geniş bir mevcut çerçeve kapsamı ve bilinen saldırı türleri ve TTP'lerin mümkün olan en geniş kapsamı
- En son tehdit ortamına ayak uydurmak için net bir süreç ve bunu gerçekleştirmek için araştırma kaynakları
- Güvenlik kontrollerini başlatacak ancak üretim ortamlarını asla etkilemeyecek güvenli kötü amaçlı yazılım örnekleri
- Geniş, çeşitli uç nokta kapsamı sağlar (Windows sunucusu, Linux, Windows masaüstü ve dizüstü bilgisayarlar, Mac)

Kompleks konfigürasyonlarla güvenlik ekiplerinin aşırı yüklenmesini önlemek ve olası önyargı oluşturmak için simülasyonlarını tüm kuruluş genelinde otomatik ve akıllı bir şekilde ölçeklendirme yeteneği

- SOC'ye aşırı uyarıları önlemek için simülasyon günlüklerinin uygun güvenlik çözümüyle otomatik ilişkilendirilmesi
- Simülasyon sonuçlarını sunan ve güvenlik ekibinin riskleri hızlı bir şekilde anlamasını ve içgörüleri geniş ekiplerle paylaşmasını sağlayan net ve özlü grafikler, diyagramlar ve ısı haritaları
- "İyileştirme felcini" önlemek için doğru önceliklendirme yetenekleri Ağ, web, uç nokta ve e-posta düzeltmesine konsolide ve hedefli azaltma verileri
- Başlıca uç nokta, ağ, SOAR ve SIEM platformlarıyla kolayca entegrasyon

Kritik yeteneklerden ve entegrasyonlardan yoksun bir BAS çözümüyeterince açıklık sağlanmamasına neden olabilir, değerli personel zamanını ve diğer kaynakları tüketebilir ve hatta üretim servislerini engelleyebilir. Öte yandan, tam özellikli, iyi entegre edilmiş bir BAS platformu, saldırı yüzeyinin daha iyi analizi ve düzeltilmesi yoluyla güvenlik duruşunu önemli ölçüde iyileştirir. Böyle bir çözüm, bilgi güvenliği ekiplerinin daha fazla insan eklemeden ve daha fazla güvenlik aracı satın almadan daha etkili olmalarını sağlayarak birkaç ay içinde kendini amorte edebilir.

Savunmanızı test etmek için TTP'leri simüle edin

Maruz kalmaları veriye dayalı sonuçlarla görselleştirin

Sömürülebilir güvenlik açıklarına öncelik verin

İşletmenizi savunmak için bütünsel çözüm

SafeBreach

OTD BİLİŞİM

Bugün bir Demo Programlayın

otd.salesgrp@onlineteknikdestek.com

www.onlineteknikdestek.com

SafeBreach

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

OTD BİLİŞİM