Zafiyet Önceliklendirmeyi Destekleme: Risk Tabanlı Bir Yaklaşım

SafeBreach

OTD BİLİŞİM

İçindekiler Tablosu

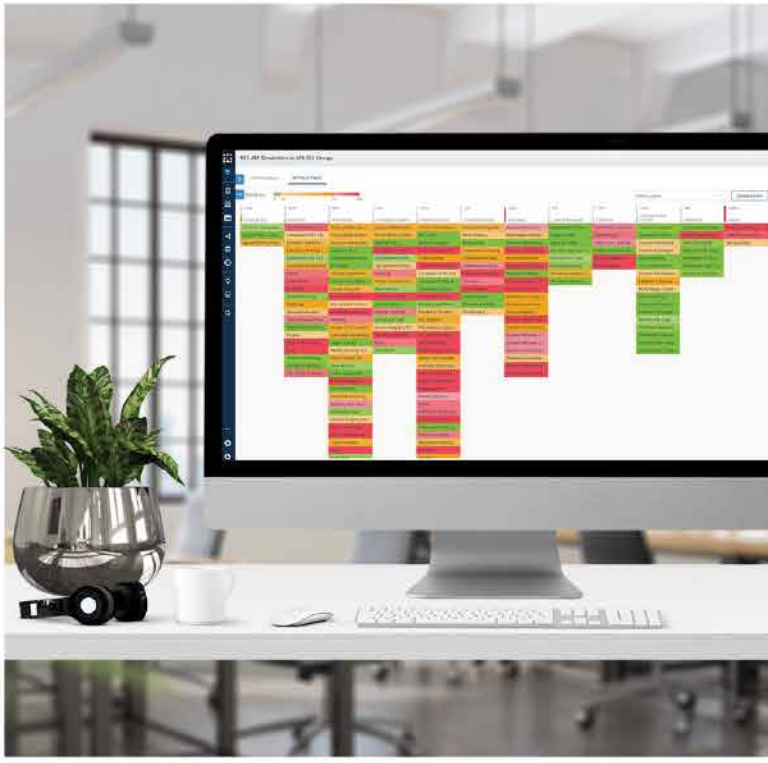
1. Yönetici Özeti	3
2. Geleneksel Zafiyet Problemi Önceliklendirme	4
3. Saldırı İstihbaratı ile Zafiyet Önceliklendirme	5
4. Makine Öğrenimi ve Yapay Zeka ile Zafiyet Önceliklendirme	6
5. Zafiyet Önceliklendirmeye Yönelik Risk Tabanlı Bir Yaklaşım Benimseme	7
6. SafeBreach'in Risk Tabanlı Önceliklendirmeyi Desteklemeye Yönelik Özel Yaklaşımını Kullanma	8
7. Ortam Eklemek için SafeBreach'i Kullanma Özel Bağlam	9
8. SafeBreach Platformunu Kullanarak Kritik Zafiyet Önceliklendirme	10
9. Sonuç	11

SafeBreach

OTD BİLİŞİM

Yönetici Özeti

Zafiyet yönetimi (ZY) dünyasının karşılaştığı en büyük zorluk önceliklendirmedir. ZY ekipleri öncelikle kuruma yönelik yüksek risk teşkil eden zafiyetleri düzeltmeyi amaçlar. Ancak, güvenlik ekibinin ortamında binlerce zafiyet olma ihtimaline rağmen, siber saldırıda bulunanlar yalnızca ağa girmek ve kritik varlıklarınıza erişmek için yalnızca tek bir zafiyete ihtiyaç duyar. VM ekipleri önceliklendirmeyi belirlemek için hangi kriterleri kullanır?
ZY araçları ile entegre olabilen SafeBreach çözümü kurumun mevcut zaafiyetlerinin erişilebilirliği ve kötüye kullanılabilirliği bakımından esas güvenlik duruşunu ortaya çıkarabilir. SafeBreach ortamınızdaki saldırıları sürekli ve güvenli bir şekilde yöneterek hem ağ tabanlı hem de sunucu tabanlı saldırı risklerini hesaplar. Güvenlik ekipleri SafeBreach'in
sezgilerini ZY tarama sonuçlarını birleştirerek potansiyel bir saldırı ile büyük bir erişilebilirlik
ve kötüye kullanılabilirlik riski taşıyan zafiyetlerin giderilmesine öncelik verebilirler. SafeBreach basitçe zafiyet yamalamaya ilişkin tahmin çalışması yürütür.



> **Daha fazla güvenlik kontrolü kurumunuzu daha güvenli yapmaz.**

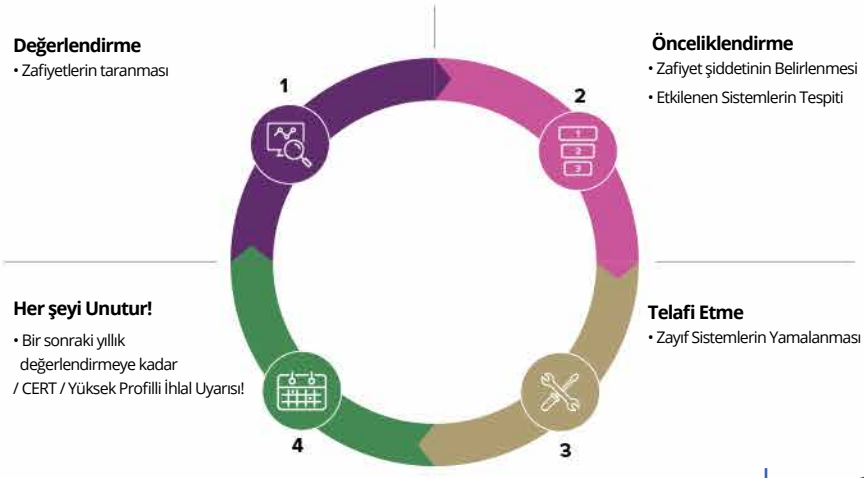
Geleneksel Zafiyet Önceliklendirme Problemi

ZY araçları ekiplerin hangi sistemlerin yamalanması gerektiğini belirlemelerine yardımcı olur, ancak hangi yamanın kurumun güvenlik duruşu üzerinde en büyük etkiyi yaratacağını belirlemeye yardımcı olamaz.
Zafiyet yama önceliklendirme başarılı ZY çalışmaları için önemlidir. VY araçları zafiyetleri tespit eder, ancak gerçek saldırı maruziyetine dair sezgiler ve en önemlisi hafifletme ve giderme çalışmalarını uygun şekilde önceliklendirmek için gereken kuruma özel bağlam bakımından yeterli değildir.
Ağ veya sistem zafiyetini tespit etmek için gereken görünürlüğe sahip olmayan güvenlik ekipleri yalnızca ZY araçlarına göre hareket ederek güvenlik duruşunu büyük ölçüde etkileyebilirler. Örneğin,
bir zafiyet "kritik" olarak işaretlenebilir, ancak erişilemeyen bir yerde bulunabilir. Bu zafiyet dış bir düşmanca erişilebilir olan başka bir "kritik" zafiyet kadar yüksek öncelikli olarak değerlendirilmemelidir. Ayrıca, yanlış yapılandırılan güvenlik kontrolleri düşmanların kurumun en değerli varlıklarına ulaşmasına fırsat verebilir.
Günümüzün birçok ZY ekibinin gerçeği kurumun farklı araçları ve ürünleri içerisinde birçok zafiyet bulunmasıdır. Ekipler bu zayıflıkların tamamını çözemez. Dolayısıyla, herhangi bir yama önceliklendirme çalışması kurumun risk maruziyetini ve toleransını yansıtmalıdır.
Mevcut zafiyet önceliklendirme yaklaşımlarında aşağıdakiler dahil olmak üzere birçok eksiklik bulunmaktadır:

• Ağırlıkla yalnızca zafiyet şiddetine ilişkin verilere odaklanır, bu da birçok zafiyetin kritik olarak sınıflandırılmasına sebep olur.
• Toplantı uygunluk gerekliliklerine odaklanır, bu da ZY araçları ile "şiddetli" olarak işaretlenemeyecek kötüye kullanıma müsait zafiyetler için potansiyel ön önceliklendirme yapılmasına neden olur.
• "Büyük resmin" görülememesine sebep olur. Ekiplerin kuruma etki eden mevcut bağlamı sınırlıdır. Örneğin, zafiyetler "hafif" olarak sınıflandırılabilir, ancak kurumun çok değerli varlıklarına kolaylıkla erişim fırsatı veren kritik yerlerde bulunur.
• Ağırlıkla statik, anlık zekaya odaklanır, bu da geriye dönük zekanın yanlış önceliklendirme yapmasına sebep olabilir.
• Reaktiftir, yani ekipler daha büyük bir risk oluşturabilecek diğer kritik zafiyetlerden önce yama için öne çıkan zafiyetleri önceliklendirme eğilimdedir.
Geleneksel zafiyet önceliklendirme iş akışları aşağıdaki adımları içerir:
1. Durum değerlendirmesi - ortamın zafiyetlere yönelik taranması.
2. Zafiyet önceliklendirme - zafiyetin şiddeti (CVSS puanları) ve etkilenen sistemlere dayanarak önceliklendirme.
3. Telafi etme - zayıf sistemlerin yamalanması.

Ekipler daha sonra bir sonraki yıllık değerlendirmeye veya bir sonraki CERT veya yüksek profilli ihlal uyarısına kadar bu çalışmaları unutma eğilimindedir.

Geleneksel Zafiyet Önceliklendirme İş Akışı



SafeBreach

OTD BİLİŞİM

Saldırı İstihbaratı ile Zafiyet Önceliklendirme

Kaçırılmış bir kritik zafiyet kuruma ciddi zararlar verme potansiyeline sahiptir. Ancak güvenlik ekiplerinin ele alması gereken büyük zafiyet hacimleri olması nedeniyle, atasözünde de söylendiği gibi samanlıkta iğne aramak oldukça zor bir iştir.

Tüm güvenlik kontrolleri ve yapılandırmaları da dahil olmak üzere saldırı yüzeyinin tamamında görünürlüğe sahip olmak kritik zafiyetlerin tespiti ve önceliklendirilmesinde atılacak ilk gerekli adımdır.

Saldırıda kötüye kullanılan zafiyetlere ilişkin bir perspektif sağladığı için saldırı istihbaratı zafiyet önceliklendirme çalışmalarını güçlendirir. Güvenlik ekiplerine zafiyetlerin kötüye kullanılma ihtimalinin olduğu sınırlı bir bağlam tanıyan bu istihbarat zafiyet önceliklendirmeyi belli bir dereceye kadar geliştirme potansiyeline sahiptir. Ancak, bu istihbarat zafiyetin kurumun güvenlik duruşu üzerindeki etkisi bakımından en çok ihtiyaç duyulan bağlama sahip değildir. Güvenlik ekiplerinin karşı karşıya olduğu dağ kadar büyük bir zafiyet listesi olduğundan, bu bağlam eksikliği genellikle zafiyet önceliklendirme çalışmalarında hatalara sebep olabilir.

Saldırı istihbaratı saldırı düzenine, devam eden saldırılara ve kötüye kullanılan zafiyetlere ilişkin içgörüler sağlayabilir. Ancak, bu istihbarat çok hızlı bir şekilde eskiyebilir. SaldırıİstihbaratI genellikle güvenlik ekiplerinin zafiyetleri önceliklendirmesine yardımcı olmak için anlık bağlam sağlar, ancak bu her zaman yeterli olmayabilir.

Saldırı istihbaratı ile desteklenen zafiyet önceliklendirme iş akışları aşağıdaki adımları içerir:

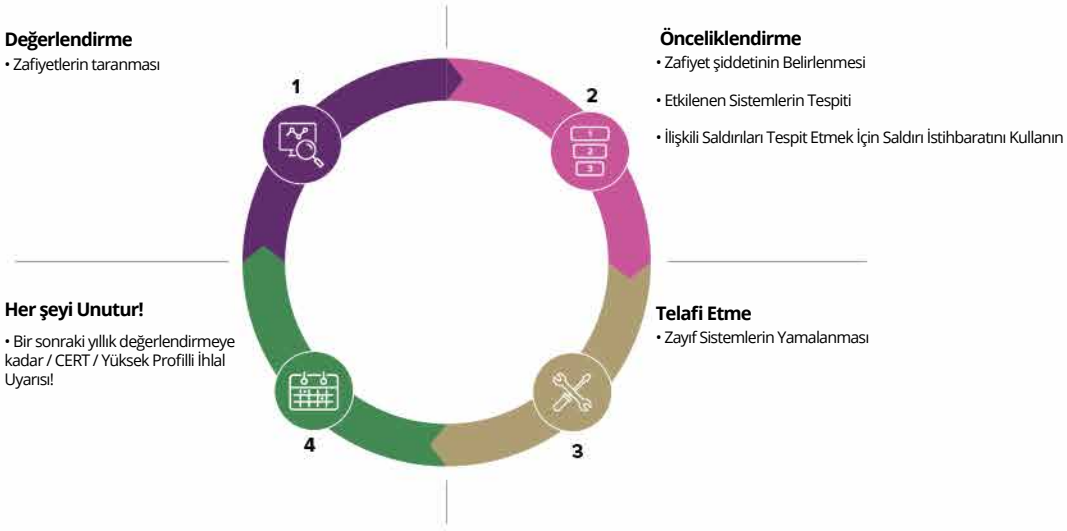
1. Durum değerlendirmesi - ortamın zafiyetlere yönelik taranması.

2. Zafiyet önceliklendirme - telafi edici kontrollere bakılmaksızın zafiyetin şiddetine, etkilenen sistemlere ve bu zafiyetler ile ilişkili saldılara dayanır.

3. Telafi etme - zayıf sistemlerin yamalanması.

Ekipler daha sonra bir sonraki yıllık değerlendirmeye veya bir sonraki CERT veya yüksek profilli ihlal uyarısına kadar bu çalışmaları unutma eğilimindedir.

Saldırı İstihbaratı Güçlü Zafiyet Önceliklendirme İş Akışı



SafeBreach

OTD BİLİŞİM

Makine Öğrenimi ve Yapay Zeka ile Zafiyet Önceliklendirme

Ekiplerin zafiyet güçlendirme ile bazı problemlerin üstesinden gelmesine, yani en kritik zafiyetleri belirlemek adına büyük hacimli olanlara odaklanmalarına yardımcı olmak için, ZY araçlarının satıcıları makine öğrenimi algoritmalarını kullanmaya başlamışlardır. Makine öğrenimi ile araçlar ekiplerin ilk yamalanması gereken yüksek öncelikli zafiyetleri tespit etmesine yardımcı olur.

Bu yaklaşık algoritmaların temizlenmesi ve kötü kullanıma oldukça müsait olan zafiyetin uyarı işaretlerinin tespit edilmesi için kullanılabilecek büyük miktardaki geçmiş zafiyet verileri mevcut olduğunda anlam kazanır.

Ancak, bu yaklaşım kullanılan algoritmaların zafiyetleri en güncel saldırı istihbaratı da dahil olmak üzere o an mevcut olan bilgilere dayanarak uygun ve doğru bir şekilde önceliklendirmesini sağlamak için birçok ön personel müdahalesi gerektirir.

Bu yaklaşım esasen güvenlik kontrollerin etkinliği ve önemli varlıkların dışarıdan erişilebilirliği de dahil olmak üzere kurumun ortam bağlamı bakımından yetersizdir. Ek olarak bu makine öğrenimi algoritmaları belli bir zafiyetin kötüye kullanılabilirliğini tahmin etme niyetinde olan olsalılık modellerine

bağlıdır. Ancak, bu araçlar ortam bağlamı açısından yetersiz olduğundan,

Güvenlik ekiplerinin önemli hususları kaçırmasına veya hemen yamalamaya gerek duymayabilecek zafiyetleri yamalamada zaman ve çalışma kaybı yaşamasına sebebiyet vererek potansiyel olarak yanlış negatiflere veya yanlış pozitiflere ortam hazırlayabilir.

Makine öğrenimi ile desteklenen zafiyet önceliklendirme iş akışları aşağıdaki adımları içerir:

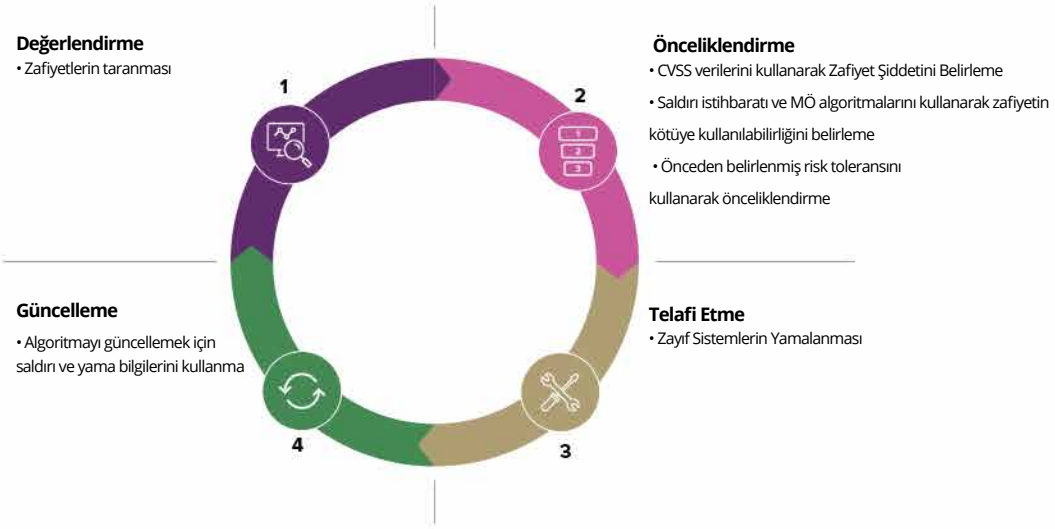
1. Durum değerlendirmesi - ortamın zafiyetlere yönelik taranması.

2. Zafiyet önceliklendirme - zafiyetin şiddetine ve algoritmaya göre sıralı zafiyet ihtimaline dayanır.

3. Telafi etme - zayıf sistemlerin yamalanması.

4. Gelecek kullanımlar için algoritmaları güncelleme.

Makine Öğrenme Destekli Zafiyet Önceliklendirme İş Akışı



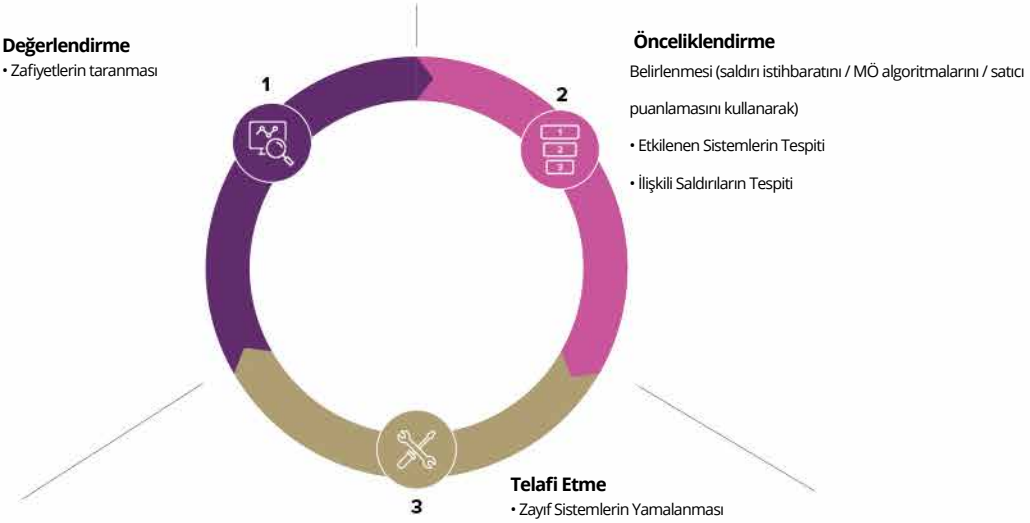
SafeBreach

OTD BİLİŞİM

Zafiyet Önceliklendirmeye Yönelik Risk Tabanlı Bir Yaklaşım Kullanma

Zafiyet o zafiyeti kötüye kullanan saldırı ve bu saldırının kurum üzerinde bıraktığı etki kadar kötüdür. Zafiyetler ZY program etkinliğini arttırmak için riske dayanarak sınıflandırılmalı/önceliklendirilmelidir. Kurum riskini göz önünde bulundurmayan ekipler kullanılması daha zor olan "yüksek öncelikli" zafiyetten potansiyel olarak daha fazla hasara sebep olabilen kolaylıkla kötüye kullanmaya müsait "düşük öncelikli" zafiyeti göz ardı edebilirler. Risk tabanlı zafiyet yönetimi (RBVM) bu sınırlandırmaları ele almayı amaçlayan bir yaklaşımdır.
RBVM kurumun spesifik ortamı ve güvenlik duruşu üzerinde teşkil edeceği riskin düzeyine dayanarak zafiyetleri sınıflandırma ve önceliklendirme sürecidir. RBVM spesifik kurum risklerini sistemlerdeki zayıflıklar ve kötüye kullanımlarla eşleyerek geleneksel ZY yaklaşımını geliştirir. Bu da güvenlik ekiplerinin kötüye kullanım açısından en yüksek riski taşıyan zayıflıklara odaklanmasına olanak verir. Zafiyet önceliklendirmeye yönelik risk tabanlı bir yaklaşım kullanmak güvenlik ekiplerinin:
1. Mevcut saldırıların spesifik kurum ve güvenlik duruşlarını nasıl etkileyebileceğini belirlemesine,
2. Kurum etkisine dayanarak zafiyetlerin giderilmesi konusuna öncelik vermenin yollarını bulmasına olanak sağlar.
Ancak, bu yaklaşım mevcut güvenlik altyapısını ve uygulanmakta olan kontrolleri ve sundukları koruma düzeyini göz önünde bulundurmaz. Saldırı düzenleri değiştikçe güvenlik kontrolleri de güncellenir. Dolayısıyla, mevcut güvenlik kontrolü ile korunmayan şiddetli bir zafiyet korunmayan zafiyet üzerinden önceliklendirilmemelidir. Zafiyet önceliklendirmede RBVM kullanmanın en büyük eksikliklerinden biri budur. Eksiksiz ve etkin olmak için, RBVM'nin kurumun güvenlik kontrollerini ve korumalarını ve kurum genelindeki genel saldırı yüzeyini göz önünde bulundurması gerekir.
Aşağıdaki şemada genel RBVM iş akışına dair bir çizim yer almaktadır.

Genel Risk Tabanlı Zafiyet Önceliklendirme İş Akışı



Geleneksel yaklaşımlar ile karşılaştırıldığında, RBVM aşağıdaki faydaları sunar:

1. Kurumun risk toleransına göre zafiyet önceliklendirme sağlar.

2. Güvenlik ekiplerinin spesifik kurum risklerini mevcut saldırı düzeni ile eşleştirmesine yardımcı olur.

3. Mevcut iş ihtiyaçlarına dayanarak devamlı risk önceliklendirme sağlayarak uygunluğun ötesine geçer.

4. Güvenlik ekiplerinin yamalama ve telafi etme kontrolleri arasında bilgi sahibi olarak karar almalarına olanak tanır.

5. Ekipleri proaktif bir yaklaşım benimseme konusunda destekler.

SafeBreach

OTD BİLİŞİM

Risk Tabanlı Önceliklendirmeyi Desteklemek için SafeBreach'in Özel Perspektifini Kullanma

Yukarıda bahsedildiği üzere, RBVM önceliklendirme yaklaşımının en büyük dezavantajı kurumun güvenlik kontrolleri ve sürekli değişen konfigürasyonlara ilişkin bağlam eksikliğidir. SafeBreach'teki ekip müşterilerimizin spesifik güvenlik kontrolleri ve ortamlarına ilişkin bağlamsal bir görünürlük kazanmalarının kritik önemini bilmektedir. Bu görünürlük güvenlik ekiplerinin hangi zafiyetlerin kurum üzerinde en büyük riski taşıdığını anlamalarının sağlanması bakımından önemlidir.

Güvenlik ekipleri kurumun güvenlik duruşu ve zafiyet yönetimi ile ilgili ortak bir yaklaşım bulunmadığını unutmamalıdır. Saldırgana kurumun en önemli varlıklarına doğrudan erişim fırsatı veren düşük öncelikli zafiyet otomatik olarak bir güvenlik ekibi için yüksek öncelikli hale gelmelidir. Saldırganın elindeki avantajı azaltmak ve kurumun varlıklarını güvenlik altına almak için, ekiplerin
saldırganların niyetini (saldırı) ve spesifik kurum risklerine
karşı mevcut savunma sistemlerini (zafiyet) kullanma kabiliyetlerini tespit etmek önemlidir.

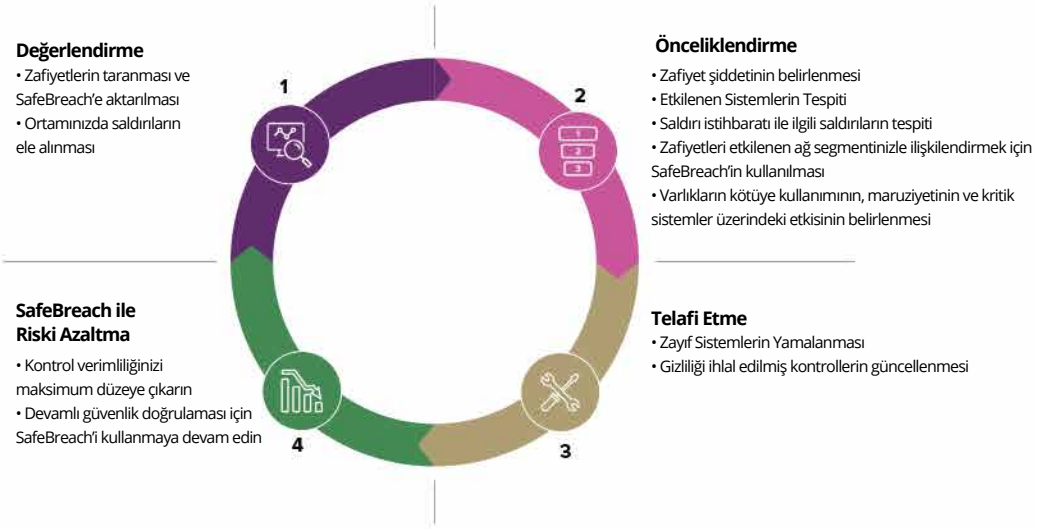
RBVM kurumun spesifik ortamı ve güvenlik duruşu üzerinde teşkil edeceği riskin düzeyine dayanarak zafiyetleri sınıflandırma ve önceliklendirme sürecidir. RBVM spesifik kurum risklerini sistemlerdeki zayıflıklar ve kötüye kullanımlarla eşleyerek geleneksel ZY yaklaşımını geliştirir. Bu da

SafeBreach varlıkların kötüye kullanılabilirliğini ve erişilebilirliğini belirlemek için gerçek saldırılara karşı kurumun güvenlik kontrollerini güvenli ve sürekli olarak doğrulayabilir. Güvenlik ekipleri devamlı olarak güvenlik kontrollerini doğrulayarak ve kritik varlıklara dışarıdan erişilebirlik ile kurum üzerinde teşkil ettiği riski eşleyerek akıllı önceliklendirme kararları alması için ihtiyaç duydukları bağlamı elde edebilirler.

SafeBreach güvenlik ekiplerinin güvenlik duruşlarını etkin bir şekilde yönetmelerine olanak tanır. Bunu aşağıdaki eylemleri gerçekleştirerek yapar:

1. Zafiyete ilişkin genel saldırı yüzeyinin belirlenmesi
2. Zafiyetin genel erişilebilirliğinin belirlenmesi
3. Zafiyetin kurumun kritik varlıkları üzerindeki etkisinin değerlendirilmesi
4. Zafiyetin kötüye kullanım riskini göz önünde bulundurarak düşmanların kurumlarına potansiyel erişiminin belirlenmesi

Risk Tabanlı Zafiyet Safebreach ile Yönetim



SafeBreach

OTD BİLİŞİM

Ortama Göre Bağlam Eklemek için SafeBreach'i Kullanma

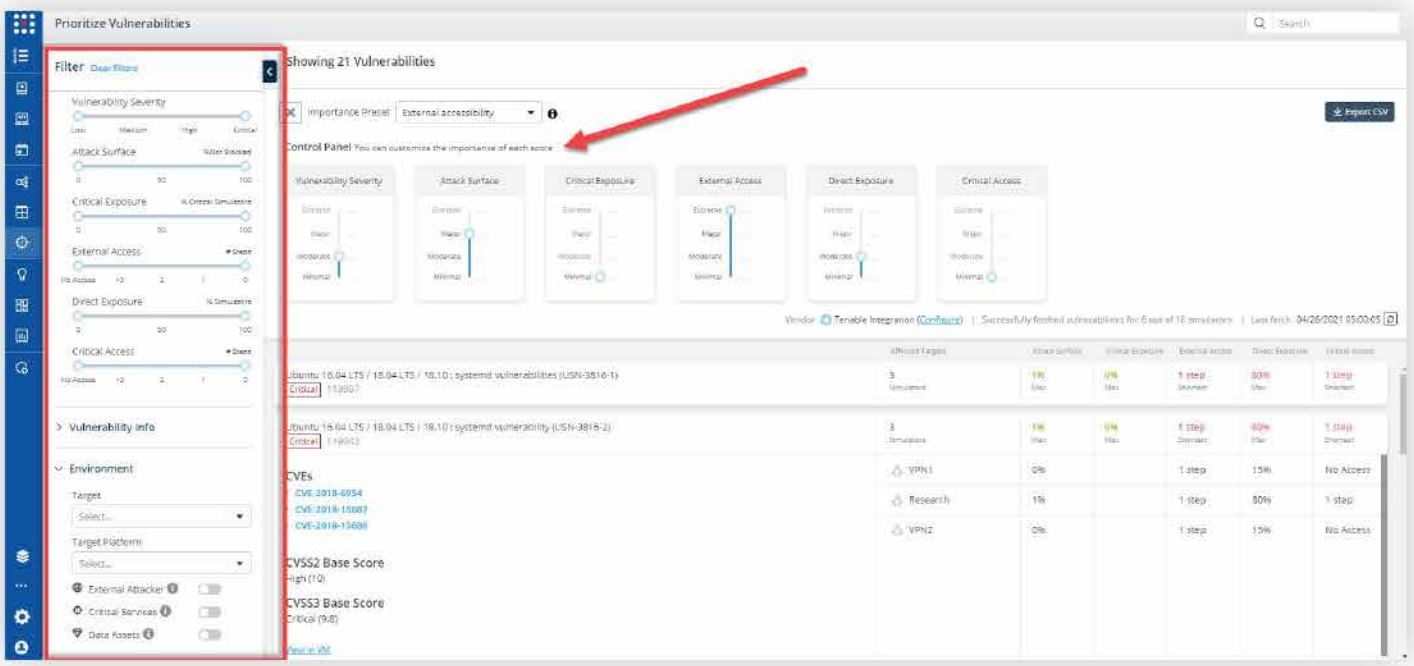
SafeBreach'in ZY araçlarıyla entegrasyonu erişilebilirlik ve kötüye kullanılabilirlik bakımından kurumun ortamına ilişkin esas duruşuna ışık tutar. Kurum ortamındaki saldırıları devamlı ve güvenli olarak ele alan SafeBreach hem ağ hem de sunucu saldırılarının riskini hesaplar. ZY ekipleri SafeBreach'in bağlamsal sezgilerini zafiyet tarama sonuçları ile birleştirerek potansiyel bir düşman tarafından kötüye kullanım bakımından büyük bir risk taşıyan yerlerde zafiyet giderme sürecine odaklanabilirler. SafeBreach ekiplerin ortamlarının doğrulanmış ve esas kabiliyetlerine dayanarak kötüye kullanım ihtimali de dahil olmak üzere eklenen bağlam ile önceliklendirme doğruluğu sağlayan bir risk tabanlı yaklaşım benimsemelerini sağlar. Bu şekilde, güvenlik ekipleri kurumlarında zafiyetlerin sebebiyet verdiği risklere ilişkin gerçekçi bir görünürlüğe sahip olabilirler. Bu da ekiplerin büyük problemler yaratacak saldırılara ve zafiyetlere odaklanmasına ve uygun bir müdahalede bulunmasına olanak sağlar. SafeBreach güvenlik ekiplerinin:

- Güvenlik kontrol verimliliği ve tümü SafeBreach'in saldırı simülasyonları ile doğrulanan en önemli maruziyete dayanarak bağlam ile zafiyetleri önceliklendirmesini,
- Kurumlarının değişen güvenlik gerekliliklerini karşılamak için önceliklendirmeyi özelleştirmesini,
- Farklı ekipler arasında önceliklendirme kriterlerini ve verilerini paylaşmasını,
- Saldırılara karşı etkinliğe ilişkin gerçek zamanlı bağlamsal sezgi oluşturmak adına güvenlik kontrollerini ve yapılandırmalarını sürekli olarak doğrulamasını,
- Zafiyetleri yamalama veya telafi için güvenlik kontrollerini güncelleştirme ile ilgili bilgilendirilmiş olarak karar vermesini,
- Kurumlarının güvenlik duruşunu ve güvenlik harcamalarını optimum düzeye çıkarmak için karar alıcıların ihtiyaç duyduğu görünürlüğü ve zekayı sunmasını,
- Yamalama öncesi ve sonrası da dahil olmak üzere maksimum koruma düzeyleri sağlamak adına savunma sistemlerini sürekli olarak test etmesini sağlayarak RBVM'yi güçlendirir.

SafeBreach | OTD BİLİŞİM

SafeBreach Platformunu Kullanarak Kritik Zafiyetleri Önceliklendirme

SafeBreach platformu Qualys, Rapid7, Tenable ve daha birçok satıcıdan alınanlar da dahil olmak üzere birçok pazar lideri ZY aracı ile entegre olabilir. Bu entegrasyonlar ile, SafeBreach ZY aracının tespit ettiği zafiyetleri içe aktarabilir. Ortamınızdaki saldırıları güvenli bir şekilde ele alan
SafeBreach, güvenlik ekiplerinin en kritik riskleri ve bu risklerin giderilmesi için atılması gereken adımları tespit etmesine olanak sağlar.
Bu çözüm potansiyel bir saldırı ömrünün tüm aşamalarını test ederek binlerce saldırıyı güvenli bir şekilde ele alır.
SafeBreach, güvenlik ekiplerinin kurumlarına yönelik spesifik risklere dayanarak zafiyetleri önceliklendirmeye ilişkin akıllı ve veri güdümlü bir yöntem oluşturmasını sağlar. Güvenlik ekipleri yama yönetim çalışmalarını saldırganların kullanımı bakımından en büyük riski taşıyan belli yerlere odaklayabilir. SafeBreach ayrıca ekiplerin kritik zafiyetlerin ortadan kaldırılmasını sağlamak için düzeltme çalışmalarından sonra güvenlik kontrollerini yeniden doğrulamasına olanak tanır. SafeBreach yalnızca bilinen zafiyetler ve saldırılar hakkında jenerik veriler sağlamak yerine ekiplerin en kritik zafiyetlerinin nerede bulunduğunu tespit etmesine yardımcı olur.
SafeBreach, kullanıcılarının kurumları üzerinde en büyük risk teşkil eden zafiyetleri tespit etme, sınıflandırma ve önceliklendirme çalışmalarını basit hale getiren sezgisel, kullanımı kolay bir arayüz sunar.
SafeBreach etkilenen hedeflere yapılan saldırıların sonuçlarına dayanarak SafeBreach risk puanları ile zafiyet verilerini otomatik olarak çoğaltır.



SafeBreach Platformunda Zafiyet Önceliklendirme

Güvenlik ekipleri SafeBreach risk puanlarına, satıcı tarafından verilen şiddet puanlarına ve hedef ortamlara dayanarak zafiyetleri kolaylıkla filtreleyebilmektedir. Güvenlik ekipleri zafiyetleri daralttıktan sonra spesifik risk toleranslarına ve gereksinimlerine dayanarak ve daha hızlı bir yama yönetimi sağlayarak önceliklendirme yapabilmektedir. Güvenlik ekipleri SafeBreach'te yer alan varsayılan önceliklendirme kriterlerini kullanabilir veya zafiyetlere ilişkin özel önceliklendirme yapabilirler. Zafiyetler aşağıdaki kriterler kullanılarak özelleştirilebilir:

- Dışarıdan erişilebilirlik—Bu ön ayar güvenlik ekiplerinin dış saldırganlarca nasıl kolaylıkla erişime açık olabileceğine dayanarak zafiyetleri önceliklendirmesine olanak tanır. Sadece birkaç adım ile kolaylıkla erişilebilecek ağ çevresindeki her varlık öncelikle yamalanmak için tespit edilebilir.
- Yakın maruziyet—Bu ön ayar güvenlik ekiplerinin zayıf önemli varlıkların etrafındaki korunmasız hedeflere dayanarak önceliklendirme yapmasını sağlar. Korunmasız çevre hedeflerin sayısı ne kadar fazla olursa, kritik varlıklara yönelik risk de o kadar yüksek olur.
- Kritik hedef yakınlığı—Bu ön ayar güvenlik ekiplerinin kurumlarının önemli varlıklarına yönelik doğrudan saldırı yolları sunan varlıkların zafiyetlerine dayanarak önceliklendirme yapmasını sağlar.
- Özel Önceliklendirme—Önceden ayarlanan önceliklendirmelerin hiçbiri kurumun risk toleransına uygun değilse, güvenlik ekipleri kendilerine için önemli hususlara göre önceliklendirmeyi özelleştirebilirler. Bu hususlar:

- Zafiyetin şiddeti
- Zafiyetin kötüye kullanıma maruz kalma ihtimali
- Zafiyetin kritik varlıklarınız içerisindeki yaygınlık durumu
- Zafiyetin dış bir saldırgan tarafından kötüye kullanılma ihtimali
- Zafiyetin içeriden kötüye kullanılma ihtimali
- Zafiyetin kötüye kullanımı sonrasında kritik varlıklarınızın zarar görme ihtimali

Güvenlik ekiplerinin kuruma yönelik risk düzeyine dayanarak zafiyet yamalamayı önceliklendirmesini sağlayan SafeBreach platformu, güvenlik ekiplerine ayrıca proaktif, dinamik ve uyarlanabilir güvenlik duruşu yaratma ve kuruma ise iş devamlılığını sağlarken birçok farklı saldırının karşısında durma fırsatı tanır. Ayrıca, önceliklendirilen zafiyetlerin raporları görüntülenebilir ve diğer risk ve önceliklendirme verileriyle birleştirilebilecekleri dış sistemlere aktarılabilir. SafeBreach entegrasyonu tamamen otomatiktir ve platformun birçok lider ZY aracı ve bu araçların API'siyle etkileşimde olmasını sağlar.

Sonuç

ZY ekipleri SafeBreach'ten alınan güvenlik kontrol doğrulama verilerini ZY araçları ve CISO'lardan alınan verilerle birleştirerek ihtiyaç duydukları resmin tamamını elde edebilirler. Bu birleşim kurumun asıl –ve şu anki– güvenlik yapılandırması ve duruşuna dayanan RBVM'ye olanak sağlar. En önemlisi, güvenlik ekiplerinin ilgili zamanda gerçekten önemli olan hususa odaklanmasına yardımcı olur. Bu da kurumun koruma stratejisi ve genel güvenlik duruşunda büyük bir fark yaratabilir.

Bugün bir Demo Programlayın

otd.salesgrp@onlineteknikdestek.com

www.onlineteknikdestek.com

SafeBreach

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

OTD BİLİŞİM