Otomatik Siber Güvenlik Olay Müdahalesi

Hazırlayan:

DUYGU KAÇAR

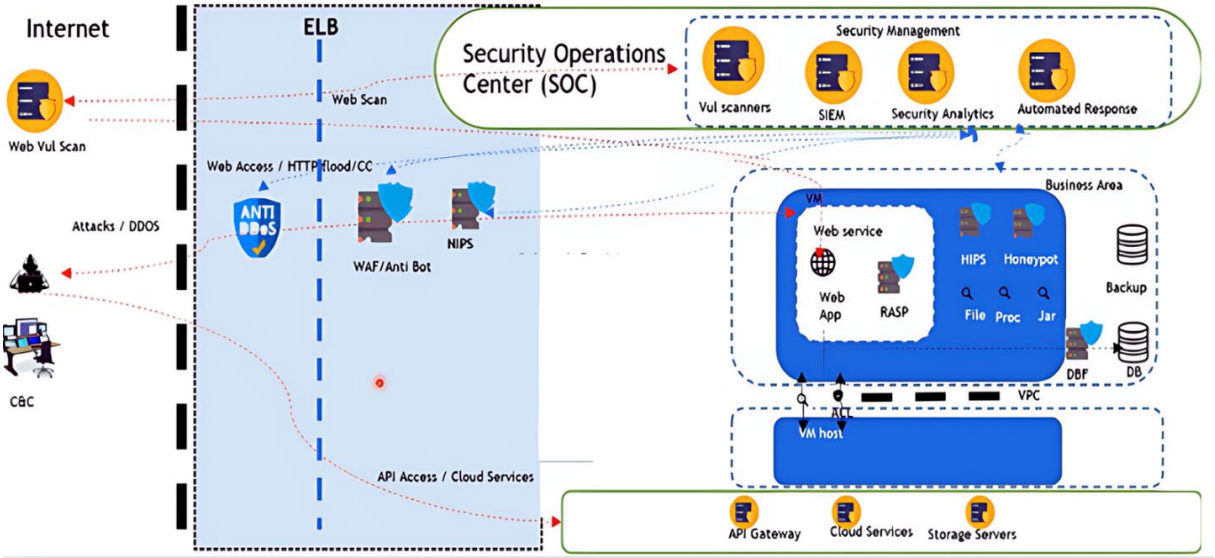
İçindekiler

Giriş

Bu raporumda Otomatik Siber Güvenlik Olay Müdahalesi hakkındaki araştırmalar yazıldı . Bu rapor, siber güvenlik mimarisi, Güvenlik Operasyonları Merkezi (SOC) ve olay müdahalesi konularında kapsamlı bir inceleme sunmayı amaçlamaktadır. Siber tehditlerin artmasıyla birlikte, kurumların bu tehditlere karşı koyma yeteneklerini güçlendirmeleri hayati bir önem taşımaktadır. Bu doğrultuda, NIST siber güvenlik çerçevesi ve olay müdahale stratejileri üzerinde durulacak, otomatik yanıt ve akıllı algılama çözümlerinin etkinliği değerlendirilecektir.

Raporda, olay müdahale çerçevelerinden olay müdahale stratejilerine, tespit ve analiz yöntemlerinden sınırlama ve kurtarma adımlarına kadar geniş bir yelpazede konular ele alınacaktır. Ayrıca, veri ihlali durumlarında izlenecek adımlar ve en iyi siber güvenlik teknikleri üzerinde durulacak, SOAR platformlarının (Güvenlik Orkestrasyonu, Otomasyon ve Müdahale) kullanımı ve özellikleri detaylandırılacaktır. Bu rapor, siber güvenlik alanında çalışan profesyonellere rehberlik etmek ve kurumların güvenlik duruşlarını iyileştirmelerine yardımcı olmak amacıyla hazırlanmıştır.

1. Siber Güvenlik Mimarisi, SOC ve Olay Müdahalesi



Kuruluşlar tarafından güvenlik katmanları genellikle şu şekilde uygulanır:

- **Anti-DDoS** çözümleri DDoS saldırılarını ve web uygulamalarını önlemek için sınır düzeyinde dağıtılır.
- **Güvenlik duvarları** ağ kenarında konuşlandırılır ve ardından ağ izinsiz giriş önleme sistemi(WAF ve NIPS) gelir. Bu sistem, ağ, ana bilgisayar ve uygulama düzeyindeki saldırıları tespit eder ve filtreler.

Ancak bu güvenlik çözümleri her zaman yeterli değildir. İmzalara dayalı olarak uygulama trafiğindeki tehditleri belirlememize yardımcı olurlar, ancak çalışma zamanı tehditleri genellikle göz ardı edilir. Bu nedenle, uygulamanın iç verilerine ilişkin içgörüler elde etmek ve tehditleri çalışma zamanında belirlemek için ek güvenlik denetimlerine ihtiyacınız vardır.

Bunun için dağıtabileceğiniz güvenlik çözümleri şunlardır:

- **Host-based Intrusion Prevention System(HIPS),** ana bilgisayar içindeki kötü amaçlı etkinlikleri tespit etmek ve önlemek için kullanılır. Bu sistem, ana bilgisayar içindeki kötü amaçlı dosyalar, işlemler ve savunmasız dosyaları belirlememize yardımcı olur.
- **Honeypots (bal küpleri)**, saldırgan davranışlarını öğrenmek için dağıtılabilir.
- **Database Firewalls**, veritabanı trafiğini izleyen ve veritabanına özgü saldırıları algılayan uygulama güvenlik duvarlarıdır. Bu sistemler, hassas verilere erişen saldırıları öncelikli olarak tespit eder ve korur.
- **RASP (Runtime Application Self-Protection),** uygulamaların çalışma zamanında kendilerini korumalarını sağlayan bir güvenlik teknolojisidir. Uygulama içinde çalışarak güvenlik tehditlerini algılar, saldırıları önler ve uygulamanın çalışma sürecinde sürekli olarak izleme yapar.

Bulut hizmetlerine bakacak olursak:

- **Bulut hizmetleri**, bulut satıcıları tarafından depolama sunucularıyla barındırılır ve API Gateway aracılığıyla kontrol edilen bulut hizmetlerine erişim sağlanır. Ancak, saldırganlar da bu hizmetleri hedef alır.

Güvenlik kontrollerinin nasıl ve neden dağıtıldığını anladık. Ancak, bunların düzgün çalıştığından nasıl emin olabiliriz? Güvenlik kontrolleri, saldırıları tespit etme ve önleme konusunda ne kadar başarılı? Bunları sürekli olarak nasıl izleyebiliriz? Güvenlik kontrollerinin etkinliğini nasıl kontrol ederiz? Bu saldırılara karşı olaysal tepkimiz nedir?

İşte burada güvenlik operasyonları devreye girer. **Güvenlik operasyonları merkezi (SOC)**, günün her saati siber tehditleri izlemek, önlemek, tespit etmek, araştırmak ve yanıt vermekle sorumludur. **Olay müdahale çerçevesi**, siber tehditleri tespit etmede ve yanıt vermede SOC'nin önemli bir bileşenidir.

2. NIST Siber Güvenlik Çerçevesi- Akıllı Algılama ve Otomatik Yanıt

Bu iki siber güvenlik çerçevesi, akıllı algılama ve otomatik yanıt sunar. Siber güvenliğin bir standardı vardır ve bu bir IST çerçevesidir. İletişime izin veren endüstri standartlarını, yönergelerini ve uygulamalarını sunan bir sonraki temel çerçeve, çeşitli düzeylerde kuruluşlar arasında siber güvenlik faaliyetleri ve hedeflerini destekler. Sonraki temel işlevler, güçlü bir iş temeli oluşturur ve siber güvenlik gereksinimlerini tanımlar.

Siber güvenlik çerçevesinin beş unsuru vardır. Bu Intelligent Detection and Automated Response (IPDR) 'dir. Bu temel beş işlev, kuruluşların siber güvenlik riskini yönetmelerine ve yönetim kararları almalarına yardımcı olur. Beş temel unsur vardır.

Birincisi tanımlamaktır. Tanımlama işlevi, siber güvenlik risklerini anlamaktan strateji geliştirmeye kadar yardımcı olur. Web uygulaması, ana bilgisayar ve ağlardaki güvenlik açıklarını belirleyin, Ve ev sahibinin ne tür risklere maruz kaldığı gibi kurumsal varlıklardaki riski belirleyin, vb. Bu nedenle, riskle ilişkili kritik varlıkları tanımlamanız gerekir. Yani bir site haritası oluşturmamız gerekiyor.

İkinci unsur korumadır. Koruma işlevi, kritik hizmetler için uygun güvenlik önlemlerini tanımlar. Güvenlik önlemlerine ihtiyaç vardır.

Üçüncü unsur algılama işlevidir. Algılama işlevi, siber güvenlik olaylarını tespit etme ve süreci tanımlar. Siber güvenlik olayları için sürekli izleme uygulayın ve güvenlik kontrollerinin yeterliliğini kontrol edin. Bu işlevin bir parçası olarak, uzmanlığa ve ilişkili risklere dayalı imzalar veya kurallar oluşturmanız gerekir.

Dördüncü unsur tepkidir. Tepki işlevi, algılanan siber güvenlik olayı için uygun eylemi gerçekleştirildiğini tanımlar.

Son unsur kurtarmadır. Kurtarma işlevi, dayanıklılık için uygun planları tanımlar ve siber güvenlik olaylarından etkilenen kuruluşları kurtarmayı destekler.

Zamanında otomatik yanıt alabilir ve iz temettülerini arşivleyebiliriz. Ayrıca, organizasyonu geleceğe hazırlamak için güvenlik tatbikatları ve tabletop tatbikatlar yapılabilir. Siber güvenlik stratejisi açısından, etkin tespit kuralları ve imzaları geliştirilerek siber güvenlik olaylarının önlenmesi ve bu olaylardan hızlı kurtulma stratejileri belirlenebilir.

2.1. Olay Müdahale Çerçeveleri

- NIST
- SANS
- CREST

2.1.1. NIST

4 geniş aşamaya ayrılması gerekiyor.

- Hazırlık,
- tespit ve Analiz,
- kontrol altına alma, eradikasyon ve kurtarma,
- olay sonrası.

NIST'e göre, siber güvenlik olay müdahalesi süreci dört geniş aşamaya ayrılır. İlk aşama, 'Hazırlık', potansiyel olaylara yanıt vermek için gerekli planlama ve kaynakların hazırlanmasıyla ilgilidir.

Bu aşamada, olayların tespit edilmesi ve analiz edilmesi için gerekli sistemler ve süreçler belirlenir. İkinci aşama 'Tespit ve Analiz', olası olayların tanımlanması, incelenmesi ve etkilerinin anlaşılması sürecini içerir. Üçüncü aşama 'Kontrol Altına Alma, Eradikasyon ve Kurtarma', siber saldırının yayılmasını durdurmayı, zararı minimize etmeyi ve normal işletme durumuna dönmeyi amaçlar. Son olarak, 'Olay Sonrası' aşaması, olayın nedenlerini ve etkilerini değerlendirir, öğrenilen dersler çıkarılır ve gelecekteki olaylara daha iyi yanıt vermek için iyileştirmeler yapılır.

2.1.2. SANS

Sans, olay müdahale planı için altı adım tanımlar, örneğin.

- Preparation (Hazırlık)
- Identification (Kimlik tespiti)
- Containment (Çevreleme)
- Eradication (Eradikasyon)
- Recovery (Kurtarma)
- Lessons Learned (Öğrenilen Dersler)

SANS, olay müdahale planı için altı adım belirlemektedir. İlk adım 'Hazırlık' ve tanımlama aşamasıdır. Ardından 'Tespit ve Analiz' gelir, bu da genellikle tehdit tespiti ve analiziyle benzerdir. Sonra 'Çevreleme, Eradikasyon ve Kurtarma' adı altında üç aşama birleştirilir; SANS çerçeveleri bunları ayrı aşamalar olarak ele alır. Doğru: 'Olay Sonrası' etkinlikleri, öğrenilen derslerle ilişkilendirilir. Bu, SANS ve NIST' in neredeyse aynı adımları tanımladığını göstermektedir.

Altı adımı anlamak için öncelikle 'Hazırlık' ile başlamamız gerekiyor. Bu aşamada, kurumsal güvenlik politikasının tanımlanması ve güncellenmesi, risk değerlendirmelerinin yapılması ve kritik güvenlik olaylarının belirlenmesi gerekmektedir.

'Tespit' aşaması, anormal davranışları izleme sistemlerinin bir parçası olarak tehdit tespitini içerir. Bir olay tespit edildiğinde, adli kanıtlar toplanır, analiz edilir ve belgelenir.

'Çevreleme' aşamasında saldırı altındaki ağ kesimleri izole edilir ve geçici çözümler uygulanarak sistemlerin yeniden oluşturulması desteklenir.

'Eradikasyon' adımında, kötü amaçlı yazılımların kaldırılması ve saldırının nedenleri belirlenir.

'Kurtarma' aşaması, etkilenen sistemlerin normale dönüşünü sağlar ve sistemin test edilmesini, doğrulanmasını ve izlenmesini içerir.

Son olarak, 'Ders Öğrenme' adımıyla olayın analiz edilmesi, belgelenmesi ve olay müdahale sürecinin iyileştirilmesi sağlanır. Bu aşamaların belgelenmesi, gelecekteki olaylara daha etkili bir şekilde yanıt verilmesine yardımcı olur.

2.1.3. CREST

Siber güvenlik olay müdahale olgunluk değerlendirmesi, kuruluşların siber güvenlik olaylarına nasıl müdahale ettiğini ve bu konudaki yeteneklerini değerlendiren bir süreçtir. Crest, bir olgunluk modeli geliştirerek kuruluşların bu müdahale yeteneklerini ölçmektedir. SOC hizmetleri ve sertifikasyon gereksinimlerini karşılamak için iyileştirmeler ve öneriler sağlar. Crest sertifikası, bir kuruluşun siber güvenlik olaylarına müdahale kabiliyetini gösterir. Uluslararası Akreditasyon ve Belgelendirme Kuruluşu tarafından kabul edilmiştir ve güvenlik alanında bilgi temsil eder ve destekler.

3. Olay Müdahale Stratejisi

Olay müdahalesinin amacı ve nesnel hedefleri şudur:

- Hizmetleri koruyun.
- Güvenlik olaylarından kaynaklanan iş etkisini en aza indirin.
- Olaylardan ders alın ve önleyici tedbirler veya koruma tedbirleri uygulayın.
- Yasal, düzenleyici ve kurumsal ilkeler gibi uyumluluk gereksinimlerini karşılayın.

Siber güvenlik olay müdahale süreci altı aşamada gerçekleşir. İlk olarak, bağlam oluşturulmalıdır; bu, strateji oluşturmadan önce mevcut durumu anlamak anlamına gelir. Politika ve planlama aşamasında, olay yanıtı tanımlanır ve ekip yapısı belirlenir. Olay müdahale sürecinde, olay playbook'u oluşturulur ve standart prosedürler tanımlanır. Playbook ; olaylara gerçek zamanlı olarak yanıt vermek ve çözmek için standart prosedürlerin ve adımların tanımlandığı anlamına gelir. Ayrıca, ekibi gelecekteki olaya hazırlayacak birkaç alıştırma da içerebilir. Olay müdahale standartlarını, politika sürecini ve kontrol listesini tanımlar.

Bu aşamada, siber güvenlik olaylarını tespit ve analiz ettiğimiz siber güvenlik saldırılarını ele alıyoruz. Olay yönetimi ve soruşturması aşamasında, siber güvenlik saldırıları analiz edilir. Müdahale ve iyileştirme aşamasında, adli kanıtlar toplanır ve sistemler normale döndürülür. Son olarak, iyileştirme eylemleri belirlenir ve gelecekteki saldırılara karşı önlemler alınır.

3.1. Olay Müdahale Stratejisi- İş Hızlandırma

- Geliştirilmiş güvenlik.
  - Overall Response Time(Genel Tepki Süresi)
  - Incident Containment(Olay Önleme)
  - Incident Recovery(Olay Kurtarma)
  - Coordination(Koordinasyon)
- Maliyeti düşür.
  - Operation downtime(Çalışma kesintileri)
  - Incident Impact(Olay Etkisi)
  - Sanction(Yaptırım)
  - Threat intel Sharing(Tehdit ıntel Paylaşımı)
- işi hızlandır.
  - Industry Requirement (Endüstri Gereksinimi)
  - Law Requirement (Yasa Gereksinimi)
  - Improve Customer Base (Müşteri Tabanını Geliştirme)
  - Client Requirement (Müşteri Gereksinimi)
  - Business Continuity (İş Sürekliliği)

3.1.1. Gelişmiş Güvenlik

Geliştirilmiş güvenlik, bir organizasyonun siber tehditlere karşı daha hazırlıklı, hızlı ve etkili olmasını sağlar. Bu, güvenlik olayının tespit edilmesinden çözümüne kadar geçen sürenin azaltılması (Genel Tepki Süresi), olayın yayılmasını durdurmak için hızlı müdahale (Olay Önleme), olaydan sonra sistemleri ve hizmetleri normale döndürme süreci (Olay Kurtarma) ve farklı ekipler arasında etkin iş birliği ve iletişim (Koordinasyon) ile sağlanır. Bu bileşenlerdeki iyileştirmeler, organizasyonun genel güvenliğini artırır.

3.1.2. Düşük Maliyet

Operasyonun kapalı kalma süresi ve olayın etkisi otomatik olarak daha az olursa, maliyet minimum düzeyde olacaktır. Ayrıca, olay zamanında ve etkili bir şekilde ele alınırsa cezalar da daha az olacaktır. Başka bir şey de, soruşturmaya yardımcı olan tehdit istihbaratı bilgilerini paylaşarak maliyetin en aza indirilebilmesidir ve tehditlerin tanımlanmasında. Bütün bunlar maliyeti düşürecektir.

3.1.3. İş hızlandırma

Siber saldırıları zamanında ele alabiliriz, böylece hizmetlerin devam etmesine ve iyileştirilmesine yardımcı olur ve iş sürekliliğine katkı sağlar. Bu nedenle, etkili bir olay müdahale stratejisine sahip olmak, iş büyümesini hızlandırmak için çok ama çok önemlidir.

3.2. Olay Müdahale Stratejisi - Ekipler ve Hiyerarşi

Olay Yönetimi ve Müdahale ekibi, risk tanımlama, denetim ekibi, uyumluluk ekibi, SOC ekibi, hizmet ekibi ve BT destek ekibi gibi çeşitli ekiplerle koordinasyon sağlar. Tipik olarak, kuruluşlar aşağıdaki gibi bir hiyerarşi oluşturur:

- L1 takımı
- L2 takımı
- L3 takımı

L1 TAKIMI

Birinci seviye sorumluluk, uyarıları 7/24 ele almak, ön analiz yapmak ve gerekirse bir sonraki seviyeye iletmektir. Daha fazla araştırma ve derin analiz gerektiğinde L1 ekibi durumu L2 ekibine iletir, aksi takdirde kendileri yönetip kapatabilirler. Günlük görevler arasında güvenlik kontrollerini yönetmek ve yapılandırmak bulunur.

L2 TAKIMI

L2 ekibi, uyarı algılama kurallarını düzenli olarak günceller ve optimize eder, böylece gerçek saldırıları tetikler ve normal trafik için yanlış alarmları önler. L2 ekibinin bir başka işlevi de tehdit istihbaratını kullanmaktır. Siber tehdit istihbaratı, işletmelerin tehdit bilgilerini anlamak ve bu bilgileri siber güvenliği önlemek, hazırlamak ve tanımlamak için kullanmalarıdır. Kuruluşlar, sektördeki diğer kuruluşlarla işbirliği yapmalı ve tehditleri tanımlamak ve anlamak için tehdit istihbaratını senkronize etmelidir. L2 ekibinin sorumlulukları arasında kurumsal varlık verilerini toplamak, gözden geçirmek ve kritik kaynakları belirlemek de bulunmaktadır. Ayrıca, L2 ekibi saldırıları engelleme ve iyileştirme sürecinde de rol alır.

L3 TAKIMI

L3 ekibi, L1 ve L2 ekiplerinin desteğe ihtiyaç duyduğu yerlerde daha derin analiz ve soruşturma gerektiren durumları ele alır. Ayrıca, sızma testi yaparak güvenlik açıklarını belirler ve gerekli düzeltmeleri uygular. L3 ekibi, kök neden analizi yaparak iyileştirme eylemleri önerir ve güvenlik çözümü optimizasyonlarını sağlar.

Kuruluşlar, olay müdahale ekiplerini ve hiyerarşiyi bu şekilde oluşturur. Böylece siber güvenlik olayları sistematik ve etkili bir şekilde ele alınabilir ve kuruluşlar, dünyadaki çeşitli ekiplerle koordinasyon sağlayarak bu süreçleri yönetir.

3.3. Olay Müdahale Stratejisi- IR politikası ve planı

Olay müdahale politikasının bir parçası olarak, olay kapsamı, olay önceliklendirmesi ve olay raporlama olmak üzere üç aşama tanımlıyoruz.

1. Olay Kapsamı:

- Olay kapsamı, neyi koruyacağınızı bilmektir. Bu yüzden, kuruluşunuzdaki kritik kaynakları ve potansiyel tehditleri tanımlamalısınız. Örneğin, ödeme hizmetleri gibi kritik varlıklar ve hassas bilgiler (kredi kartı bilgileri, Sosyal Güvenlik bilgileri vb.) korunmalıdır. Taç mücevherlerinizin ve içindeki potansiyel tehditlerin doğru tanımlanması, bu kritik varlıkları korumak için gereklidir.

2. Olay Önceliklendirmesi:

- Kurtarma önceliklerini belirleyin. Sistemlerinizin nasıl çalıştığını belgeleyin ve bu belgeleri güncel tutun. Olay müdahale ekipleri bu belgeleri gözden geçirerek sistemin nasıl çalıştığını ve mimarisini anlayacak, böylece olay müdahalesinde gereken adımları atabileceklerdir.

3.Olay Müdahale Planı:

Olay müdahale politikasını tanımladıktan sonra, olay müdahale planını oluşturmalıyız. Olay müdahale planının bir parçası olarak, üç aşama tanımlıyoruz: olay işleme, soruşturma ve iyileştirme eylemleri.

- **Olay İşleme:** Olay işleme, siber güvenlik saldırılarının nasıl ele alınacağını tanımlar. Siber güvenlik olaylarının nasıl tespit edileceği, analiz edileceği ve adli kanıtların nasıl toplanacağı ile ilgili süreçleri içerir. Ayrıca, enfeksiyonun yayılmasını kontrol altına almak için izolasyon stratejilerini belirler.

- **İletişim Stratejisi:** Ne ve kiminle iletişim kuracağınızı belirleyin. İç ve dış paydaşları tanımlayın. Bu, olay müdahale planının önemli bir parçasıdır.

- **Ders Çıkarma ve İyileştirme Eylemleri:** Olay müdahale sürecinden sonra kök neden analizi yaparak öğrenilecek dersleri belirleyin. Bu, gelecekteki siber güvenlik olaylarına karşı daha hazırlıklı olmanızı sağlar.

Olay müdahale süreci, koordinasyon ve bilgi paylaşımı ile etkin bir şekilde yönetilmelidir. Bu, siber güvenlik siber saldırılarının etkili bir şekilde ele alınmasına yardımcı olacaktır.

3.4. Olay Müdahale Stratejisi- Olay Müdahale Başucu Kitabı(playbook)

Olay yanıtı Playbook'u, siber güvenlik olaylarının ele alınmasında önemli bir bileşendir. Saldırganların her gün gerçekleştirdiği yaygın saldırı senaryoları için ayrıntılı rehberliğe ihtiyacınız vardır. Kimlik avı, kaba kuvvet saldırıları, kötü amaçlı yazılım enfeksiyonları, enjeksiyon saldırıları ve uzaktan kod yürütme gibi saldırılar için olay yanıtı Playbook'larını kullanabiliriz.

Temel olarak, olay yanıtı Playbook'u, gerçek zamanlı olaylara yanıt vermek ve çözmek için standart prosedürleri ve adımları tanımlar. Çalışma kitabı genellikle aşağıdaki bileşenleri içerir:

1. Ön Koşullar:

- Ön koşullar, soruşturmaya başlamadan önce ele alınması gereken belirli gereksinimlerdir. Örneğin, günlüğe kaydetmenin açık olması gibi. Bu adımlar, soruşturmaya başlamadan önce tamamlanmalıdır.

2. İş Akışı:

- İş akışı, soruşturmayı gerçekleştirmek için mantıksal bir akış izlemeyi gerektirir. Bu, saldırı vektörlerini analiz etmeyi, olay belirtilerini değerlendirmeyi, olayın nedenini araştırmayı, olay analizini yapmayı, olayı sınırlamayı, yok etmeyi ve kurtarmayı içerir.

3. Denetim Listesi:

- Olay yanıtı sürecini tamamlamak için gereken görevlerin listesini içeren bir denetim listesine sahip olmak zorunludur. Bu, hiçbir şeyin atlanmamasını sağlar ve ayrıntılı bir denetim listesi, her yönün ele alınmasına yardımcı olur.

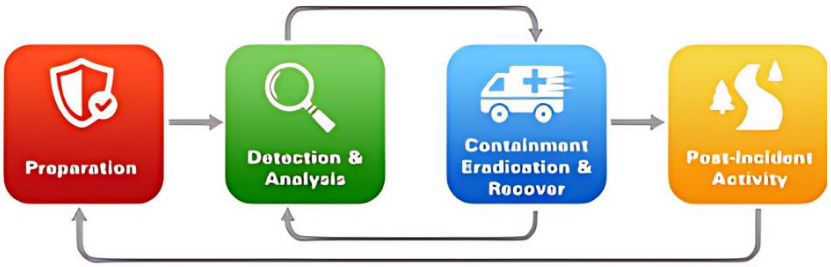
4. Soruşturma Adımları:

- Belirli bir olay araştırması için ayrıntılı adım adım rehberlik sağlar. Her olay farklıdır, bu nedenle her olay için ayrıntılı rehberlik gereklidir. Adli veri toplama ve analizini içerir ve buna göre koruyucu önlemler alınır.

Özetle:

Tipik olaylar için senaryoları önceden hazırlamamız gerekiyor. Müdahale eylemleri dahil. Olay meydana geldiğinde ne yapılması gerektiğini, nelere dikkat edilmesi gerektiğini bilmek önemlidir. Bu senaryolar, olaydan olaya farklılık gösterir ve müdahale eylemleriyle birlikte hazırlanmalıdır.

3.5. Olay Müdahale Stratejisi- Olay Müdahale Yaşam Döngüsü



Bu olay yanıtı doğrusal bir etkinlik değildir.

Doğrusal aktivite, bir olay tespit edildiğinde başlayan ve bir eradikasyon ve kurtarma ile sona eren süreçtir. Aksine, olay müdahalesi, sürekli öğrenme ve iyileştirmenin olduğu döngüsel bir faaliyettir. Örgütün kendini etkili bir şekilde nasıl savunabileceğini bu süreçle anlarız.

Olay Yaşam Döngüsündeki Geri Bildirim Döngüleri:

Her olaydan sonra, olay sırasında neler olduğunu araştırmak ve raporlamak için büyük bir çaba sarf edilir. Bu geri bildirim, önceki aşamalara yapılır ve daha sonra daha iyi bir hazırlık, tespit ve analiz yapılması sağlanır. Gelecekteki olaylara daha iyi hazırlıklı olabilmek için bu çok önemlidir.

Burada, muhafaza ve eradikasyondan algılama ve analize kadar bir geri besleme döngüsü olduğunu görebilirsiniz. Bu, bir saldırının birçok bölümünün tespit aşamasında tam olarak anlaşılmadığı anlamına gelir ve sadece müdahale ve iyileşme aşamasına girdiğinde ortaya çıkar. Bu dersler, ekibin bir dahaki sefere saldırıları etkili bir şekilde algılamasına ve analiz etmesine yardımcı olabilir.

Olay müdahalesi genel olarak dört aşamaya ayrılmıştır. Ancak bu dört aşama, anlamak için daha fazla adıma bölünebilir. Olay müdahalesi daha derinlemesine şu şekilde incelenebilir:

1. Hazırlık:

   - Bu aşamada gerekli olan her şeyin hazır olduğundan emin olunur.

2. Algılama:

   - Saldırıyı tanımlama sürecidir.

3. Önceliklendirme:

   - Bu aşamada, olayı onaylayın, etkiyi değerlendirin ve aciliyet ve ciddiyet düzeyini belirleyin.

4. Muhafaza:

   - Bu aşamada, virüslü ana bilgisayarı veya ağı izole edin.

5. Veri Toplama ve Adli Soruşturma:

   - Bu aşamada detaylı adli soruşturma yapılır.

6. Eradikasyon ve Kurtarma:

   - Bu aşamada tehditler ortadan kaldırılır ve sistemler normal operasyonlara geri döndürülür.

7. Raporlama ve İyileştirme

- Olay sonrası rapor hazırlanır ve ilgili paydaşlarla paylaşılır. Aynı zamanda gelecekte benzer olayların daha etkili bir şekilde yönetilmesi için dersler çıkarılır ve iyileştirme önlemleri alınır

4. Olaya Müdahale – Hazırlık

Hazırlık aşamasının amacı, bir kuruluşun olaylara anında ve etkili bir şekilde yanıt verebilmesini sağlamaktır. Bu aşama, kuruluşu olayları önlemeye ve olayları etkili bir şekilde ele almaya hazırlar. Hazırlık aşamasında dikkat edilmesi gereken kilit noktalar aşağıdaki gibidir:

Araçlar, Kaynaklar ve Organizasyon:

Kuruluşun güvenlik olaylarına yanıt verebilmesi için gerekli araçların (SIEM sistemleri, antivirüs yazılımları, tehdit istihbarat platformları) güncellenmesi, yeterli insan gücü ve finansal kaynakların sağlanması önemlidir. Olay müdahale ekibinin yapılandırılması, rollerin net bir şekilde tanımlanması ve ekipler arasındaki iletişimin sağlanması, hızlı ve etkili müdahale için gereklidir.

Ekip Oluşumu ve Hiyerarşi:

Daha önce tartıştığımız gibi, bir olay müdahale ekibi oluşturmak ve bu ekibin hiyerarşisini belirlemek önemlidir. Herkesin rol ve sorumluluklarını bilmesi gerekir.

Prosedürler ve Planlar:

Olay müdahale planlarının ve prosedürlerinin hazırlanması gerekir. Bu planlar, olay sırasında atılacak adımları ve izlenecek yolları belirler.

Olay Yanıtı Playbook'ları:

Her olay türü için (örneğin, kimlik avı, fidye yazılımı, enjeksiyon saldırıları) detaylı olay yanıtı playbook'ları oluşturulmalıdır. Playbook'lar, önkoşulları, iş akışını, kontrol listelerini ve soruşturma adımlarını içermelidir.

Lojistik:

Lojistik, savaş odası ekipmanları, kırtasiye malzemeleri, dizüstü bilgisayarlar ve adli iş istasyonlarını kapsar.

Savaş Odası:

24/7 çalışabilecek, olayları tartışmak ve strateji oluşturmak için ayrı savaş odaları oluşturulmalıdır.

Dizüstü Bilgisayarlar ve Adli İş İstasyonları:

Soruşturma ve adli analiz için gerekli olan lojistik ekipmanlar sağlanmalıdır.

Ekip Kullanılabilirliği ve Eskalasyon:

Bu konuda eksiksiz bir ekibin mevcut olduğunu bildiğinizden emin olun.

Çağrı Üzerine Destek:

Tam ekip hazır olmalıdır. Gerekirse daha yüksek yönetime ve kritik kaynaklara yükseltilmelidir.

İletişim Bilgileri:

Olay sırasında ulaşılması gereken kişilerin iletişim bilgileri güncel tutulmalıdır.

Bağlantı Noktası Listesi:

Hangi bağlantı noktalarına erişim izni verildiği ve hangi bağlantı noktalarına izin verilmediği belirtilmelidir. Yaygın olarak kullanılan bağlantı noktaları, genellikle doğru şekilde yapılandırılmadığında güvenlik risklerine yol açabilir. Truva atı gibi zararlı yazılımlar, bu tür bağlantı noktalarına erişim sağlayarak sistemlere sızabilirler. Hangi bağlantı noktalarına erişime izin verildiği

ve hangilerine izin verilmediği önemlidir. Yanlış yapılandırmalar bazen geliştiricilerin bağlantı noktalarını açık bırakmalarına neden olabilir. Bu durum, saldırganların bu açık bağlantı noktalarına erişmesine veya kaba kuvvet saldırıları gerçekleştirmesine olanak tanır. Böylece saldırganlar, bu kaynaklara uzaktan erişim elde edebilirler.

Güvenlik Kontrolleri Belgeleri:

Uygulama protokolleri, izinsiz giriş algılama ve virüsten koruma ürünleri hakkında belgeler tutulmalıdır. Bu belgeler, olay müdahale ekibinin neyin izinli, neyin yapılandırıldığını ve hangi kaynakların erişim yetkisine sahip olduğunu anlamalarına yardımcı olur.

Kritik Varlıklar:

Örneğin, veritabanı sunucuları gibi kritik varlıkların listesi tutulmalıdır.

Güncel Temel Bilgiler:

Beklenen ağ, sistem ve uygulama etkinlikleri ve davranışları belgelenmelidir. Normal davranıştan herhangi bir sapma, anormal bir davranış olarak değerlendirilmelidir.

Risk Değerlendirmeleri:

Sistemlerin, uygulamaların ve hizmetlerin periyodik risk değerlendirmeleri yapılmalıdır.

Güvenlik Tatbikatları:

İhlal hazırlığı için güvenlik tatbikatları periyodik olarak yapılmalıdır.

Ana Bilgisayar Güvenliği:

Tüm ana bilgisayarlar, standart yapılandırmalar kullanılarak uygun şekilde sağlamlaştırılmalıdır. En az ayrıcalık ilkesine uyulmalıdır.

Ağ Çevresi Güvenliği:

Ağ çevresi, açıkça izin verilmeyen tüm etkinlikleri reddedecek şekilde yapılandırılmalıdır.

Kötü Amaçlı Yazılım Önleme:

Kötü amaçlı yazılım önleme yazılımları, kuruluş genelinde dağıtılmalıdır.

Kullanıcı Farkındalığı ve Eğitimi:

Kullanıcılar, politika ve prosedürlerden haberdar edilmelidir. Kullanıcı farkındalığı artırılmalıdır.

Olay Azaltma Yazılımı:

Temiz işletim sistemi ve uygulama kurulumlarının görüntülerine erişim sağlanmalıdır.

Bu hazırlık aşamaları, bir kuruluşun gelecekteki olaylara etkili bir şekilde yanıt verebilmesi için kritik öneme sahiptir.

4.1. Güvenlik Tatbikatları

Güvenlik tatbikatı, hazırlık aşamasındaki kilit adımlardan biridir. Bu tatbikatlar, algılama mantığını doğrulamamıza ve işletmelerin olaya hazırlıklı olmalarına yardımcı olur. Saldırıları simüle ettiğimiz, algılama mantığını doğruladığımız ve hangi olaya nasıl yanıt aldığımızı gördüğümüz simüle edilmiş ortamlarda gerçekleştirilir. Eğer herhangi bir güvenlik açığı bulunursa, bu tatbikatlar sayesinde gerekli önlemler alınabilir.

Bazı güvenlik tatbikatları şunlardır:

1.Veri İhlali: Veri sızıntıları durumunda algılama mantığını doğrulamak ve hangi olay yanıtını aldığımızı görmek.

2. İkincil Güvenlik Açıkları: Yetkisiz girişler, kötü amaçlı işlemler ve kod enjeksiyonları gibi güvenlik açıklarını tespit etmek. Bu tatbikatlar, ağdaki uygulama ve hizmetlerdeki güvenlik açıklarını belirlememize ve hangi olay yanıtını aldığımızı görmemize yardımcı olur.

3. Uygulama Sertleştirme: Varsayılan kimlik doğrulamasından yararlanarak yetkisiz erişim elde edilmesi durumunda alınacak sertleştirme önlemlerini belirlemek.

Bu tatbikatların bir parçası olarak, açıklardan yararlanma tekniklerini geliştirmeniz ve bu güvenlik açıklarını kullanarak nasıl hafifletme önlemleri alacağınızı belirlemeniz gerekir. Böylece, saldırganların bu güvenlik açıklarını kullanmasını önleyebiliriz.

Güvenlik Tatbikatı Süreci:

Güvenlik tatbikatları, üretim ortamını etkileyebileceğinden ilgili tüm paydaşların bilgilendirilmesi ve onay alınması önemlidir. Üç aşamalı bir süreç vardır:

1. İlgili paydaşlara tatbikat hakkında bilgi verilmesi.

2. Ayrı bir test ortamında tatbikatın yapılması.

3. Tatbikat sonuçlarının raporlanması ve analiz edilmesi.

Tatbikat sonuçları, tatbikat adı, yürütücüsü, gözlemcisi, başlangıç ve bitiş zamanı, sonuçları ve karşılaşılan zorluklar gibi bilgileri içermelidir. Öğrenilen dersler ve iyileştirme alanları belirlenmelidir. Bu süreç, kuruluşların gelecekteki siber güvenlik olaylarına karşı hazırlıklı olmasını sağlar.

Bu tatbikatlar, kuruluşların güvenlik kontrollerinin azalması durumunda bile iş sürekliliğini sağlamalarına yardımcı olur. Siber saldırılar sırasında ana bilgisayarın izole edilmesi gibi önlemleri uygulamak, saldırganların yetkisiz erişimini önlemek için kritik öneme sahiptir. Ayrıca, bağlantı noktası taraması ve ters kabuk gibi saldırı senaryolarına karşı hazırlıklı olmak da önemlidir.

Özetle, güvenlik tatbikatları, olası siber saldırılara karşı hazırlıklı olmanın ve etkili yanıt stratejileri geliştirmenin anahtarıdır.

4.2. Tabletop Egzersizleri

Tabletop egzersizleri nedir ve bize nasıl yardımcı olur? Tabletop egzersizleri, kriz yönetimine hazırlık amacıyla yapılan gayri resmi ve tartışmaya dayalı oturumlardır. Bu egzersizler, ek hafifletme önlemlerini belirlememize ve kriz yönetimi için kuruluşumuzu hazırlamamıza yardımcı olur. Ekip, acil bir durumda rollerini ve müdahalelerini tartışır.

Bazı masa üstü egzersizleri şunlardır:

1. **Hızlı Düzeltme**: Ağ yöneticisinin yamayı test etmeden dağıtması ve kullanıcıların oturum açamamasına neden olması durumunda nasıl başa çıkacağımızı tartışmak. Bu tür durumlara hazırlıklı olmak için kuruluşların oturup bu senaryoları tartışması önemlidir. Farklı kuruluşlar için duyarlı önlemler değişiklik gösterebilir, bu nedenle her kuruluşun kendi stratejisini belirlemesi gerekir.
2. **Kötü Amaçlı Yazılım Bulaşmaları**: Kullanıcının kötü amaçlı yazılımla enfekte olmuş bir SD kartı şirket dizüstü bilgisayarına takması durumunda nasıl başa çıkacağımızı tartışmak. Ekip, bu tür acil durumlara karşı duyarlı önlemler almalı ve stratejiler oluşturmalıdır.
3. **Planlanmamış Saldırılar**: Bir saldırgan grubunun kuruluşunuzu hedef alması durumunda ne yapacağınızı belirlemek. Olay müdahale görevlisi olarak ne yapmanız gerektiğini tartışmak ve planlanmamış saldırılara karşı önlem almak.
4. **Bulut Uzlaşması**: Kuruluşunuzun saldırıya uğramış bir bulut depolama hizmetinde hassas verileri depolaması ve bu durumun potansiyel olarak müşteri bilgilerini açığa çıkarması durumunda nasıl başa çıkacağınızı tartışmak. Ekip, rollerini ve müdahale yöntemlerini belirlemeli ve acil durumlar için uygun stratejiler oluşturmalıdır.

Tabletop egzersizleri sırasında ekip, gayri resmi tartışmalar yaparak stratejiler geliştirir ve uygun duyarlı önlemleri belirler. Bu egzersizler, kriz durumlarında nasıl hareket edileceğine dair bir plan oluşturulmasına yardımcı olur.

Özetle, tabletop egzersizleri kriz yönetimi için hazırlık yapmanın ve uygun stratejiler geliştirmenin anahtarıdır. Ekipler, bu tür acil durumlara karşı hazırlıklı olmalı ve gerektiğinde uygulamak üzere stratejiler oluşturmalıdır.

5. Olay Müdahalesi -Tespit ve Analiz

5.1. Tespit ve Analiz

Bir siber güvenlik olayı gerçekleştiğinde, olayın tespiti ve analizi kritik adımlardır. Bu aşama, olayın gerçekten olup olmadığını belirlemek ve olayın doğasını anlamak amacıyla gerçekleştirilir. Olayın tespiti ve analizinde, saldırı vektörlerinin anlaşılması, olay belirtilerinin incelenmesi ve olayın analiz edilmesi gibi adımlar yer alır.

1. Attack Vectors (Saldırı Vektörleri)

Saldırı vektörleri, saldırganların güvenlik açıklarından yararlanarak ağ veya uygulama hizmetlerine erişim sağladığı yollar veya yöntemlerdir. Örnekler:

- Web Tabanlı Saldırıları:
  - XSS (Cross-Site Scripting):Güvenlik açığı bulunan bir web uygulamasına kötü amaçlı kod enjekte edilmesi.
  - SQL Enjeksiyonu:Veri hırsızlığı için kullanılabilir.
- E-posta Saldırıları:
  - Zararlı yazılım içeren ekler veya kötü amaçlı web sitelerine yönlendiren bağlantılar.

2. Sign of Incident (Olay Belirtileri)

Olay belirtileri, potansiyel olayın habercisi olabilir ve iki kategoriye ayrılır: öncüller ve göstergeler.

- Öncüller: Gelecekte bir olayın meydana gelebileceğinin işaretidir.

- Göstergeler: Bir olayın meydana gelmiş olabileceğinin veya devam ediyor olabileceğinin işaretidir.

3. Source of Precursors (Öncüllerin Kaynağı)

Olay analizinde doğru tespit edilmesi gereken her öncü veya göstergenin değerlendirilmesi önemlidir. Ancak bu, yanlış pozitifler ve büyük hacimli veriler nedeniyle zor olabilir.

- **Ağ ve Sistem Profillemesi:** Normal davranışların anlaşılması, anormal aktivitelerin tespiti için önemlidir.

- **Günlük Saklama Politikası Oluşturma:** Eski günlük girişlerinin analizde kullanılması.

- **Olay Bağıntısı Yapma:** Farklı günlüklerden gelen verilerin ilişkilendirilmesi.

-**İnternet Arama Motorlarını Kullanma:** Olağandışı faaliyetler hakkında bilgi bulma.

-**Paket Dinleyicilerini Kullanma:** Ağ trafiğinin yakalanması ve analiz edilmesi.

- **Veri Filtreleme:** En şüpheli faaliyetlerin araştırılması.

4. Incident Analysis (Olay Analizi)

Olay analizinde, saldırı vektörlerinin anlaşılması, olay belirtilerinin tespiti ve olayın detaylı analizi gibi adımlar kritik öneme sahiptir. Bu süreçler, gelecekte benzer olayların önlenmesi ve hızlı müdahale için gereklidir.

Olay analizini daha etkili hale getirmek için birkaç öneri:

1. **Ağ ve Sistem Profillemesi**
   -Normal davranışları anlamak ve anormal aktiviteleri tespit etmek için ağların ve sistemlerin profillenmesi önemlidir.
2. **Günlük Saklama Politikası**
   -Günlük verilerinin ne kadar süreyle saklanacağını belirlemek için bir günlük saklama politikası oluşturun ve uygulayın.
3. **Olay Bağıntısı**
   -Farklı günlüklerden gelen verileri ilişkilendirerek olayları analiz edin. Bu, belirli bir olayın olup olmadığını doğrulamada kritiktir.
4. **İnternet Arama Motorlarını Kullanma**
   -Olağandışı faaliyetler ve saldırganlar hakkında bilgi edinmek için internet arama motorlarını kullanın.
5. **Paket Dinleyicilerini Kullanma**
   -Ağ trafiğini yakalamak ve analiz etmek için paket dinleyicilerini kullanın. Bu, özellikle olayın ayrıntılı analizinde faydalıdır.
6. **Veri Filtreleme**
   -En şüpheli faaliyetleri araştırmak için verileri filtreleyin. Önemsiz göstergeleri elemek ve yalnızca en önemli göstergeleri incelemek etkili bir stratejidir.
7. **Olay Önceliklendirme**
   -Olayları etkilerine ve kurtarılabilirlik durumlarına göre önceliklendirin. İlk gelene ilk hizmet esasına göre değil, önem derecesine göre işlem yapın.

5. Incident Prioritization (Olay Önceliklendirme)

Olay önceliklendirme, olayların işleme sırasının belirlenmesidir. Olaylar, etkilerine ve kurtarılabilirliklerine göre önceliklendirilmelidir.

6. Incident Notification (Olay Bildirimi)

Olay bildirimi, olay analizinin tamamlanmasının ardından yapılmalıdır. İlgili tüm personelin olay hakkında bilgilendirilmesi ve olay müdahale ekibinin uygun kişilerle iletişim kurması gereklidir.

7. Sonuç

Olay Müdahale Ekibi, olay verilerini korumalı ve erişimi kısıtlamalıdır, çünkü bu veriler genellikle hassas bilgiler içerir. Olay analizi tamamlandıktan sonra harekete geçilmeli ve ardından olay bildirimi yapılmalıdır. Bir olay inceleme raporu hazırlamak önemlidir. Bu raporu, güvenlik olayı araştırma özeti raporunda genel bakış, güvenlik durumu, ekip kurulumu, ekip lideri ve üyeler hakkında bilgiler, ilk saldırı analizi, olay zaman çizelgeleri, saldırı zaman çizelgeleri, acil durum ekibi ve kuruluş acil durum engelleme, saldırı yolu analizi, saldırının kuruluş ağı içinde nasıl ilerlediği, yanal hareketler ve saldırı davranışları, enfeksiyon vektör analizi, güvenlik açığından nasıl yararlanıldığı ve çözüm önerileri, iyileştirme önlemleri, güvenlik duruşu ve çözümdeki boşlukların giderilmesi için alınacak tedbirler gibi bilgileri bir araya getirerek hazırlayabilirsiniz. Bu bilgilerle hazırlanan soruşturma özet raporu, güvenlik olayının kapsamlı bir analizini sunar ve iyileştirme önlemlerini belirlemeye yardımcı olur.

5.2. Olay İnceleme Yöntemleri

Çoğu durumda, güvenlik olaylarını araştırmak için iki yol izlenebilir: gerçek zamanlı analiz ve günlük analizidir.

5.2.1. Gerçek Zamanlı Analiz

Bazı saldırılar, kritik varlıkları hedef alan tehlikeli saldırılar olarak sınıflandırılır ve bu nedenle yüksek riskli uyarılar olarak kabul edilir. Örneğin, kaba kuvvet saldırıları, veri hırsızlığı saldırıları, uzaktan kod yürütme saldırıları ve komut yürütme saldırıları kritik uyarılar olarak değerlendirilebilir. Bu tür uyarılar, olay müdahale ekibinin dikkatine sunulmak üzere e-posta, SMS veya telefon yoluyla alınmalıdır. Bu tür uyarılara hızlı bir şekilde müdahale edilmesi ve dakikalar veya saatler içinde çözülmesi gerekmektedir.

5.2.2. Günlük Analizi

Diğer bir araştırma yöntemi ise günlük analizidir. Uyarıların çoğu düşük öncelikli uyarılardır ve bu nedenle tüm yüksek öncelikli uyarılar çözümlendikten sonra tek tek ele alınmaları gerekir. Tabii ki, kaynaklar daha düşükse, düşük öncelikli uyarılar da zamanında ele alınabilir ve bunların gerçek bir etkisi olup olmadığına bakılabilir.

5.3. Otomatik Güvenlik Olay Analizi platformu

Güvenlik olayı analizi, gerçek zamanlı analiz, günlük analiz ve saldırgan analizini kapsar. Platform, dış tehdit istihbaratı ile senkronize çalışarak kural yönetimi sağlar.

5.3.1.Gerçek Zamanlı Analiz

Gerçek zamanlı analiz, saldırıların anında tespit edilip analiz edilmesini sağlar. Kritik uyarılar, olay müdahale ekibinin hızlı bir şekilde müdahale etmesini gerektirir.

5.3.2. Günlük Analizi

Günlük analiz, düşük öncelikli uyarıların değerlendirilmesini içerir. Yüksek öncelikli uyarılar çözüldükten sonra, bu uyarılar da incelenir ve gerektiğinde müdahale edilir.

5.3.3. Saldırgan Analizi

Saldırgan analizi, saldırganın niyetini ve davranışını belirlemeyi amaçlar. Kaynak izleme ve dış tehdit istihbaratı ile senkronize edilerek saldırganın tehdit tanımlaması yapılır.

5.3.4. Dış Tehdit İstihbaratı Senkronizasyonu

Dış tehdit istihbaratı, siber saldırılarda zararlı olayları azaltmak için kullanılır. Bu istihbarat, alan izleme, açık kaynak istihbaratı, sosyal medya, derin ve karanlık ağlardan elde edilir. Kuruluşlar, tehdit verilerini toplar ve SIEM aracı ile kullanımı kolay bir gösterge panosuna dönüştürür.

5.3.5. Uyarı Kuralı Yönetimi

Uyarı kuralı yönetimi, sürekli uyarı algılama kurallarının oluşturulması, güncellenmesi ve izlenmesini içerir. Kurallar, tehditleri daha az hatalı pozitif sonuçla algılayacak şekilde sürekli olarak değerlendirilir.

5.3.6. Otomatik Alarm Analiz Platformu

Otomatik alarm analiz platformu, güvenlik kontrollerinden ve olay yönetim sistemlerinden bilgi alarak bu bilgileri derinlemesine savunma sistemine entegre eder. Bu, uyarı analizini ve olay yanıtını otomatikleştirir ve güvenlik kontrollerinde uygun sınırlama veya izolasyon önlemlerini alır.

6. Olay Müdahalesi - Sınırlama, Eradikasyon, Kurtarma

6.1. Müdahale ve Kurtarma

Olay veya saldırı doğrulandıktan sonra, durumu idare etmek için adımlar atmamız gerekiyor. Bu adımlar çevreleme, eradikasyon ve kurtarma işlemlerini kapsar.

Çevreleme stratejisi, olayın veya saldırının yayılmasını önlemek için hızlı harekete geçmeyi amaçlar. Ağı ve tehdidi kontrol altına alarak, sistemi normale döndürürüz.

Sınırlama ile kastedilen güvenlik olayını tespit ettikten ve analiz ettikten sonra, saldırganın veya saldırganın daha fazla kaynağa erişmesini veya daha fazla hasar vermesini engellemek önemlidir.

Güvenlik olayı müdahale prosedürümüzün birincil amacı, müşteriler üzerindeki etkiyi sınırlamak ve verileri, sistemleri, uygulamaları ve hizmetleri korumaktır. Bu nedenle, sınırlama stratejisi geliştirilir ve doğru çözüm üretilir.

Çevreleme stratejileri, her olay türüne göre farklılık gösterebilir. Örneğin, e-posta kaynaklı kötü amaçlı yazılım bulaşmasını kontrol altına alma stratejisi ile DOS saldırısını kontrol altına alma stratejisi farklı olabilir.

Bazı durumlarda, saldırganı bir izole alanına yönlendirme gibi stratejiler de kullanılabilir. Bu, saldırganın izlenmesini sağlar ve adli kanıt toplamak için fırsat sunar.

Çevreleme stratejisi gecikirse, saldırgan ağdaki diğer sistemlere zarar verebilir. Bazı saldırılar, çevrelendiklerinde ek zararlar verebilirler. Örneğin, kompromize uğramış bir ana makine, olay elemanı saldırıyı ağdan kesmeye çalıştığında, sonraki pingle sonuçsuz kalabilir.

Saldırgan, ağdan kesilse bile, ana makinedeki verilerin tümünü geçersiz kılabilir veya şifreleyebilir.

Bu nedenle, çevrelemeden hemen sonra, ek adli kanıt toplama ve analiz ile eradikasyon işlemine geçmeliyiz. Tüm kötü amaçlı işlemleri veya dosyaları silmeli ve sistemleri kurtarma süreciyle yeniden inşa etmeliyiz.

Her ne kadar bir olay sırasında kanıt toplamanın temel nedeni olayı çözmek olsa da hukuki süreçlerde de gerekli olabilir. Bu durumlarda, tüm kanıtların, kompromize uğramış sistemlerin ve arşivlerin açıkça belgelenmesi önemlidir.

Olay elemanı, saldırganı izlemek için gerekli olsa da genellikle çevreleme, eradikasyon ve kurtarma süreçlerine odaklanmalıdır. Saldırganın izini sürmek zaman alıcı ve boşa giden bir süreç olabilir, bu yüzden saldırgan kaynağını doğrulayarak izlemek daha güvenilir bir yoldur.

Eradikasyon ve kurtarma işlemleri, bir olay çevrelenip kontrol altına alındıktan sonra yapılır. Eradikasyon, olayın bileşenlerini ortadan kaldırmak için gereklidir. Örneğin, kötü amaçlı yazılımları silmek ve ihlal edilmiş kullanıcı hesaplarını devre dışı bırakmak gibi adımları içerir.

Kurtarma sürecinde, sistemleri normale döndürmek ve sistemlerin normal işleyişini onaylamak için işlemler yapılır. Kurtarma, temiz yedeklerden sistemi geri yükleme, sistemleri sıfırdan yeniden inşa etme, kompromize uğramış dosyaları temiz sürümlerle değiştirme, yamaları kurma, şifreleri değiştirme ve ağ parametrelerini sıkılaştırma gibi adımları içerebilir.

6.2. Adli Analiz (Forensic Analysis)

Adli inceleme, ihlalin tam anlamıyla anlaşılmasını, saldırının giderilmesini ve tekrarlanmasının önlenmesini sağlar. Bu süreç dikkatlice yürütülmelidir ve gerektiğinde delillerin mahkemede kabul edilebilir olmasını sağlamak için en iyi uygulamalar izlenmelidir.

6.2.1. Ağ Düzeyinde Adli İnceleme:

- Güvenlik duvarı günlükleri, ağ trafiği akışları, IPS günlükleri, ana bilgisayar günlükleri ve SIEM uyarıları incelenir.

- Güvenlik olayının ne zaman başladığını, kimin başlattığını, yapılan eylemlerin sırasını ve işletmeye etkilerini belirlemek önemlidir.

- Güvenlik duvarı günlükleri, ağdaki gelen ve giden tüm olayları izlemeye yardımcı olur.

- Ağ trafiği analizi, anormallikleri tespit etmek ve hedeflenen cihazları belirlemek için kullanılır.

- Uygulama günlükleri, saldırı türleri hakkında değerli ağ tehdit bilgileri sağlar.

- Bellek, CPU, disk, disk alanı veya maksimum sayıda saldırı aktif oturumunun aşırı kullanımı.

6.2.2. Sistem Düzeyinde Tehdit Analizi:

- Hangi sistem bileşenlerinin korunması gerektiğini ve hangi güvenlik risklerine karşı korunmaları gerektiğini belirlemek önemlidir.

- Varlıkların (sunucular, ağ cihazları, yazılımlar, uygulamalar, veri tabanları) belirlenmesi ve olay günlüklerinin analiz edilmesi gereklidir.

- Zayıf yazılım sürümleri, yetkisiz erişim girişimleri, veri dışarı sızdırma ve uzaktan kod yürütme gibi tehditler değerlendirilir.

6.2.3. Kullanıcı ve Uygulama Düzeyinde Tehdit Analizi:

- Uygulama içeriğinin, çalışma zamanı gecikmelerinin, uygulama güvenliği günlüklerinin ve yapılandırma dosyalarının incelenmesi saldırının kökenini izlemeye yardımcı olur.

- Modern uygulamalar genellikle birden fazla sunucu, veri merkezi ve bulut sağlayıcısı üzerinde dağıtılır ve büyük veri tabanları ile desteklenir.

6.2.4. Zararlı Yazılım Analizi:

Zararlı yazılım analizi Statik Zararlı yazılım Analizi , Dinamik Zararlı Yazılım Analizi ve Hibrit Zararlı Yazılım Analizi olarak 3 e ayrılır.

Statik Kötü Amaçlı Yazılım Analizi:

Bu tür analiz, dosyaları kötü niyet belirtileri açısından inceler. Gerçekten çalışan kötü amaçlı yazılım koduna ihtiyaç duymaz. Tanımlanan dosya adları, karma değerleri, IP adresleri, etki alanları, dosya başlıkları gibi göstergelerle çalışır. Çalışma zamanında gözlemlenen kötü amaçlı davranışlar bu analizle algılanamaz.

Dinamik Zararlı Yazılım Analizi:

Dinamik zararlı yazılım analizinde, şüpheli kötü amaçlı kodlar güvenli bir ortam olan bir sandbox'ta çalıştırılır. Sandbox, sistem veya ağa bulaşma riski olmadan kötü amaçlı dosyaların çalıştırılmasına yardımcı olur. İdeal olarak hem statik hem de dinamik kötü amaçlı yazılım analizinin birleştirilmesi, her iki yaklaşımın da en iyi özelliklerini sunar.

Hibrit Zararlı Yazılım Analizi:

Hibrit Zararlı Yazılım Analizi, zararlı yazılımların tespiti ve analizinde hem statik hem de dinamik analiz yöntemlerinin birleştirildiği bir yaklaşımdır. Statik analiz, zararlı yazılımın kodunun incelenmesi ve zararlı davranışların tespit edilmesi için kullanılırken, dinamik analiz, zararlı yazılımın bir sanal ortamda çalıştırılarak davranışlarının gözlemlenmesini içerir. Bu hibrit yaklaşım, daha kapsamlı ve etkili bir analiz sağlar, çünkü hem kodun içeriği hem de çalışma zamanı davranışları değerlendirilir.

6.2.4. Tehdit İstihbaratı:

Tehdit istihbaratı, genellikle güvenlik açıkları ve saldırı göstergeleri gibi bilgilerdir. Bu bilgiler, tehditlerin belirlenmesine ve anormal saldırı davranışlarının tanımlanmasına yardımcı olur. Saldırının arkasındaki niyeti açığa çıkarır ve belirli tehdit türleriyle ilişkilendirilebilir.

Linux ve Windows Arasındaki Farklar:

Linux'ta kayıt defteri bulunmaması, adli inceleme sürecinde farklı yaklaşımları gerektirir. Linux sistemlerinde dağınık kaynaklardan bilgi toplamak önemlidir. Dosya silindiğinde meta veriler sıfırlanabilir.

Forensic analysis	Files/Commands to be verified
Hidden Executables on file system	find / -name ".*" -exec file -p '{}' \; | grep ELF
Hidden Directories and Files	find / -type d -name ".*"
Immutable Files and Directories (Often Suspicious)	lsattr / -R 2> /dev/null | grep "\----i"
User Login History	/var/log/wtmp
Useful authentication data	/var/log/auth.log , /var/log/secure, /var/log/audit/audit.log, **/var/log/btmp**
Check persistence mechanism	Service start-up scripts /etc/inittab, /etc/init.d, /etc/rc.d /etc/init.conf, /etc/init (Upstart) /etc/cron* /var/spool/cron/*
Additional files to analyze	/etc/sudoers, /etc/passwd, /var/log/daemon.log, /var/log/syslog

Bu komutlar linux sisteminde arananları ararken yardımcı olacak.

Önemli Dosyaların İncelenmesi:

Adli inceleme sürecinde, kullanıcı oturum geçmişi, kimlik doğrulama verileri, değişmez dosyalar ve sistem çağrılarını içeren günlük dosyaları özellikle önemlidir. Bu dosyalar, şüpheli etkinliklerin tespit edilmesine ve saldırı zaman çizelgesinin yeniden oluşturulmasına yardımcı olabilir.

Analiz Edilecek Diğer Dosyalar:

Ek olarak, sudoers dosyaları, şifre dosyaları, sistem günlükleri ve arka plan programlarının oluşturduğu günlük dosyaları da incelenmelidir. Bu dosyalar, şüpheli aktivitelerin tespit edilmesinde ve saldırıya karşı önlem alınmasında önemlidir.

6.3. Eradikasyon ve Temizleme

Soruşturma ve adli analiz tamamlandıktan sonra, eradikasyon aşamasına başlayabilirsiniz. Bu aşamada, olayla ilgili tüm bileşenleri kaldırmanız gerekir. Saldırgan tarafından bırakılan tüm yapıtları, kötü amaçlı kod verilerini vb. tespit edip temizleyin ve her açığı veya güvenlik açığını kapatın. Bu, bilgisayar korsanı tarafından izinsiz giriş için kullanılan tüm yöntemleri içermelidir.

Temizleme İşlemine Başlamadan Önce

- Olayın tam resmini çizmeden temizleme işlemine başlamayın.
- Olayın kök nedenini belirleyin.
- Tüm sistemleri kontrol ederek aynı güvenlik açığının başka yerlerde de mevcut olup olmadığını tespit edin.
- Ortadan kaldırma işlemi mümkün olduğunca hızlı yapılmalıdır. Düşmana yanıt vermesi için zaman tanımamalısınız.

Eradikasyon Yöntemleri

Kötü niyetli ayak izlerini ortadan kaldırmak için aşağıdaki senaryoları uygulayabilirsiniz:

1. **Virüs ve Casus Yazılım Tarayıcısı Çalıştırma**:
    - Kötü amaçlı dosyaları ve hizmetleri kaldırmak için tarama yapın.
2. **İmzaların Güncellenmesi**:
    - HIPS, güvenlik duvarı, NIPS, antivirüs ve diğer güvenlik kontrollerindeki imzaları güncelleyin.
3. **Kötü Amaçlı Yazılım Dosyalarının Silinmesi**:
    - Kötü amaçlı yazılım dosyalarını silin.
4. **Kullanıcı Hesaplarının Devre Dışı Bırakılması**:
    - İhlal edilen kullanıcı hesaplarını devre dışı bırakın.
    - Parolaları değiştirin.
5. **Yararlanılan Güvenlik Açıklarının Azaltılması**:
    - Tüm güvenlik açıklarını tespit edip ortadan kaldırın.
6. **Güvenlik Açıklarının Belirlenmesi ve Giderilmesi**:
    - Sistem genelinde güvenlik açıklarını belirleyin ve düzeltin.

7. **Dış Paydaşların Bilgilendirilmesi**:
    - Gerekirse müşterileri ve medyayı bilgilendirin.

Ek Senaryolar

Eradikasyon işlemi sırasında keşfedebileceğiniz ek senaryolar da mevcuttur. Bu senaryoları tamamen ortadan kaldırmak için uygulayın.

Bilgilendirme ve Raporlama

- Liderliği ve üst yönetimi eradikasyon ve temizleme sonuçları hakkında bilgilendirin.
- Gerekirse dış paydaşları, müşterileri ve medyayı bilgilendirin.

Bu, burada listelediğim önemli senaryolardan bazılarıdır ve diğer senaryoları da keşfetmek suretiyle tamamen ortadan kaldırma işlemi gerçekleştirin.

6.4. Düzeltme

Bu, sistemlerin geri yüklenmesi ve normal operasyonlara dönüş anlamına gelir. Benzer olayların önlenmesi için ağdaki tüm makinelerdeki güvenlik açıklarını düzeltmenizi öneririm.

Ağ Düzeyinde Düzeltme

- Acil tehditlerin önlenmesi: IP adreslerinin, bağlantı noktalarının, alan adlarının ve e-postaların engellenmesi. Güvenlik kontrol imzalarını güncelleyin (güvenlik duvarı, IPS, antivirüs ve SIM imzaları).

Sistem Düzeyinde Düzeltme

- Tehditlerin giderilmesi: Virüslü uygulamaların, eklentilerin ve kütüphanelerin kaldırılması. Güvenlik açığı değerlendirmesi yoluyla bulunan sorunları düzeltin.

Kullanıcı Düzeyinde Düzeltme

- Farkındalık oturumları: Bireylere ve gruplara yönelik tehdit farkındalığı oturumları düzenleyin. Kuruluşlardaki kullanıcıların güvenlik konusunda bilinçlenmesini sağlayın.

Kötü Amaçlı Yazılım Düzeltmesi

- Güvenlik denetimlerinin güncellenmesi: Antivirüs ve kötü amaçlı yazılımdan koruma imzalarını güncelleyin. Ağ IPS ve host-based intrusion prevention sistemlerinde gerekli güncellemeleri yapın.
- Kötü amaçlı yapıtların temizlenmesi: Güvenliği ihlal edilmiş dosyaları temiz bir sürümle değiştirin.

Geri Yükleme Yöntemleri

Siber güvenlik olayından sonra geri yükleme için farklı yollar vardır. Hepsinin farklı etkileri, kurtarma süresi, maliyet ve veri kaybı potansiyeli vardır:

1. Yedekten geri yükleme:
    - Uygun maliyetlidir. İyi bir yedeğiniz varsa mümkündür.

2. Sistemlerin yeniden inşası:
    - Zaman açısından verimli değildir. Çok maliyetli ve veri kaybı olasılığı vardır. Ancak bu prosedür %100 etkilidir ve saldırganın tamamen ortadan kaldırıldığından emin olunur.

Önerilen Düzeltme Adımları

1. Virüs/Casus Yazılım Tarayıcısını Çalıştırma
2. İmzaları Güncelleme
3. Kötü Amaçlı Yazılım Dosyalarını Silme
4. Kullanıcı Hesaplarını Devre Dışı Bırakma
5. Parolaları Değiştirme
6. Yararlanılan Güvenlik Açıklarını Azaltma
7. Güvenlik Açıklarını Belirleme ve Giderme
8. Dış Paydaşları Bilgilendirme

Yukarıda belirtilen adımları uygulayarak sistemlerinizi güvenli hale getirebilir ve benzer olayların tekrar yaşanmasını önleyebilirsiniz.

7. Olay Sonrası Raporlama ve İyileştirme

Olay Raporlaması

Olay raporlaması kapsamında şunları kapsarız ve bunlar gelecekteki olayların ele alınmasına nasıl yardımcı olur:

1. **Olay Dokümantasyonu:** Olay ayrıntıları, tetikleyici nedenler, eşleştirme kuralları, bulgular, zaman çizelgeleri (ne zaman başladığı, ne zaman bittiği), soruşturmanın sonucu ve diğerleri.
2. **Kanıt Toplama:** Tehdit aktörleri hakkında ayrıntılı bilgi toplama, saldırı vektörleri, saldırganların yüklerine sistem yanıtı. Saldırgan yüzeyi, bilgisayar korsanlarının saldırı vektörlerini kullanarak güvenlik açıklarından yararlandığı ve yetkisiz erişim elde ettiği anlamına gelir.
3. **Kök Neden Analizi:** Olay tetikleyicilerinin ve bir olaya yol açan güvenlik açıklarının nedenlerini belirleyin ve belgeleyin.
4. **Azaltma Önlemleri:** İyileştirme noktalarını belgeleyin.

Olay Raporu İletişimi

Rapor hazır olduğunda, ilgili tüm paydaşlara (iç ve dış yönetim, kolluk kuvvetleri, düzenleyiciler, satıcılar ve müşteriler) olay raporunu iletmek önemlidir. Tüm bilgileri belgeleyin ve ileride başvurmak üzere arşivleyin.

Olay Yanıtı İyileştirme Eylemleri

Olay soruşturması, azaltma önlemleri ve raporlaması tamamlandıktan sonra, bu tür olayların tekrarlanmasını önlemek için iyileştirme noktaları belirleyin. İncelemeniz gereken birkaç önemli nokta:

1. **Olay Sonrası Vaka Paylaşımı:** Olay sonrası, ilgili tüm paydaşlarla paylaşın ve açıklayın. Organizasyondaki herkesin bunun farkında olmasını sağlayın.
2. **İyi Uygulamalar ve Öğrenmelerin Paylaşımı:** Güvenlik kontrolleri ve işlem hazırlığı, güvenliğin, kontrollerin ve hazırlığın verimliliğini ve etkinliğini değerlendirin.
3. **Takip:** Gerekirse, güvenlik denetimlerini yeniden yapılandırın ve imzaları güncelleyin.
4. **Eğilim Analizi:** Olay analizinin tarihinden ve geçmiş olaylardan öğrenin. Gelecekte benzer bir olay meydana gelirse, aynı yaklaşımı uygulayın.
5. **Otomatik Olay Yanıtı:** Otomatik sınırlama ve düzeltme. Otomatik sınırlama uygulamaları ile saldırganı sistem veya ağı daha fazla tehlikeye atmaktan otomatik olarak engelleyin.
6. **Yanal Hareket Analizi:** Saldırganın ağda nasıl hareket ettiğini ve tüm makineleri güvenlik açıkları için değerlendirin. Saldırganların ayak izinin ağdan tamamen kaldırıldığından emin olun.
7. **R ve R Süreç İyileştirme:** Temel öğrenmelere dayalı olarak süreçleri optimize edin. Bu, sürekli bir süreçtir ve olay müdahalesini iyileştirir. Düşmanı kısa sürede alt etmeliyiz.

8. Veri İhlali - Veri İhlali Sonrası Nasıl Yanıt Verilir

8.1. Veri İhlali Nedir?

Veri ihlali, kötü niyetli içeriden veya harici saldırganların gizli veya hassas verilere yetkisiz erişim elde ettiği bir güvenlik olayıdır. Örneğin, bir sosyal medya sitesinin 300 milyon kullanıcı hesabının açığa çıkması veri ihlali olarak adlandırılır.

8.2. Veri İhlali Sonrası Yapılması Gerekenler

Veri ihlalinin sonuçlarını hafifletmek ve olayın nedenlerini araştırmak için belirli adımlar atılmalıdır. Bir veri ihlali sonrası ele almada bize rehberlik edecek uygun bir veri ihlali müdahale planına sahip olmalıyız. İşletmenizin bir veri ihlali yaşadığını öğrendikten sonra yapmanız gereken dört temel eylem vardır:

1. Soruşturma:
   - İhlalin nedenini bulmak.
   - Tehdit vektörlerini belirlemek.
   - Yararlanılan güvenlik açıklarını analiz etmek.
   - Tehdit aktörlerini tanımlamak.

2. Çevreleme:
   - Hasarı en aza indirmek ve güvenlik açıklarını kapatmak.
   - Saldırının daha fazla yayılmasını önlemek için ilk müdahale.

3. Düzeltme:
   - Gelecekte benzer olayların tekrarlanmaması için kalıcı çözümler uygulamak.

4. Bildirim:
   - İlgili paydaşlara ve etkilenen kişilere bilgi vermek.
   - İhlalin başladığı yerin izolasyonu ve güvenlik önlemlerinin artırılması.

8.1. Veri İhlali Olay Müdahale Süreci

Bir veri ihlaliyle başa çıkmak için adım adım izlenmesi gereken 10 adım:

1. Olayın Kabulü:
   - İhlalin gerçekleştiğini kabul etmek ve soruşturmayı başlatmak.
   - Operasyonlar, yönetim ve servis ekipleriyle koordinasyon sağlamak.

2. İlk Analiz:

- Anormallikler ve olası arka kapılar için sistem ve uygulama günlüklerini analiz etmek.
- İlk analiz sonrası saldırı kanallarını engellemek.

3. Acil Durum Engelleme:

- Saldırı kaynağını engellemek ve doğrulamak.
- İlk iletişimleri başlatmak ve doğru raporlamayı sağlamak.

4. Adli Olay İncelemesi:

- Adli kanıt toplamak (ana bilgisayar günlükleri, uygulama günlükleri, şüpheli dosyalar, şüpheli işlemler vb.).
- Adli kanıt toplama iki şekilde yapılabilir: manuel olarak veya otomatik işlem yoluyla.

5. Adli Veri Analizi:

- İşletim sistemi günlükleri, işlem günlükleri, erişim günlükleri, ağ günlükleri ve ağ trafiği akışlarını analiz etmek.
- Deneme yanılma saldırıları veya başarısız oturum açma girişimleri için kimlik doğrulama günlüklerini kontrol etmek.

6. Yanal Hareket Analizi

- Saldırganın ağda nasıl hareket ettiğini ve tüm makineleri güvenlik açıkları için değerlendirmek.
- Yanal hareket analizi ile saldırgan ayak izlerini kontrol etmek.

7.Hedef Risk Değerlendirmesi:

- Ana bilgisayarda bulunan güvenlik açıkları için sonuçları taramak ve analiz etmek.
- Nmap kullanarak açık bağlantı noktası taraması gerçekleştirmek.

8.Saldırı Kaynağı İzleme:

- Saldırganları, geçmiş geçmişi, niyetleri, amaçları ve hedefleri kontrol etmek.
- Gelecekteki herhangi bir saldırının olup olmadığını öğrenmek.

9. Uzlaşma İzlerinin Kaldırılması:

- Dosyaları ve izleri silerek uzlaşma izlerini kaldırmak.

- Gidenleri içerir, saldırgan hala devam ediyorsa şüpheli dosyaları sonlandırmak.

10. Rapor Hazırlığı:

- Rapor hazırlamak ve öğrenilen dersleri, iyileştirme eylemlerini ve neyin doğru neyin yanlış gittiğini ele almak.

- Adli kanıtları arşivlemek ve politika gereği belirli bir süre saklamak.

Bu adımlar, veri ihlali durumunda kuruluşların uygun şekilde yanıt vermesini ve benzer olayların gelecekte önlenmesini sağlar.

8.2. Veri İhlallerini Önlemek için En İyi Siber Güvenlik Teknikleri

1. Siber Güvenlik Eğitimi ve Farkındalık

- Çalışanlara düzenli olarak siber güvenlik eğitimleri sağlanmalıdır. Geçmiş olaylar ve güncel tehditler hakkında bilgi verilmelidir.

2. Risk Değerlendirmesi

- Tüm değerli varlıkların belirlenmesi ve risklerin önceliklendirilmesi gerekmektedir.

3. Güvenlik Açığı Yönetimi

- Yazılım güncellemeleri ve yama yönetimi düzenli olarak yapılmalıdır.

4. En Az Ayrıcalık İlkesi

- Kısıtlı erişim ilkeleri uygulanmalıdır, böylece kullanıcıların sadece gereksinim duydukları kaynaklara erişimleri olur.

5. İki Faktörlü Kimlik Doğrulama

- Hassas sistemlere erişim için kullanılmalıdır.

6. Güvenli Parola Politikaları

- Güçlü parolaların zorunlu kılınması ve düzenli olarak değiştirilmesi gerekmektedir.

7. İş Sürekliliği ve Olay Müdahale Planı

- Sistemlerin hızlı bir şekilde kurtarılabilmesi için planlar oluşturulmalıdır.

8. Periyodik Güvenlik İncelemeleri

- Yazılım ve ağlarda düzenli olarak güvenlik incelemeleri yapılmalıdır.

9. Veri Yedekleme

- Tüm hassas verilerin düzenli olarak yedeklenmesi gerekmektedir.

10. Veri Şifreleme

- Aktarılan ve depolanan verilerin güçlü şifreleme algoritmaları ile korunması önemlidir.

11. Güvenli Kodlama Uygulamaları

- Yazılım geliştirme sürecinde güvenli kodlama standartlarına uyulmalıdır.

12. Güçlü Girdi Doğrulaması

- Kullanıcı girişlerinin güvenliğinin sağlanması için güçlü girdi doğrulama yöntemleri kullanılmalıdır.

9. Otomatik Olay Yanıtı

9.1. Güvenlik Orkestrasyonu Otomasyonu ve Müdahalesi

Karmaşık tehdit senaryoları göz önüne alındığında, günümüzde kuruluşlar çok fazla uyarı alıyor. Ancak bu uyarıların hangilerinin gerçek tehdit olduğundan emin olmak ve yanlış pozitifleri azaltmak önemlidir. Çok fazla uyarıyla nasıl başa çıkılacağı konusu ise kritik bir meseledir. Manuel araştırma yaklaşımıyla bu kadar çok uyarıya odaklanmak zor olabilir, bu yüzden otomatik olay müdahalesi çözümleri önem kazanmaktadır.

9.1.1. Otomatik Olay Müdahalesi Nedir?

Otomatik olay müdahalesi, güvenlik, orkestrasyon, otomasyon ve yanıt (SOAR) kavramını içerir. Bu çözümler, çeşitli kaynaklardan (örneğin, güvenlik duvarları, IPS'ler, ağ cihazları) büyük miktarda güvenlik verisi toplar ve bunları birleştirir. Bu veriler daha sonra analiz edilir ve otomatik yanıtlar oluşturularak güvenlik olaylarına müdahale edilir.

9.1.2. SIM ve SOAR Arasındaki Fark

SIM (Güvenlik Bilgi ve Olay Yönetimi) pasif bir araçken, SOAR aktif bir çözümdür. SOAR, uyarıları analiz eder, güvenlik kontrollerini doğrular, olayları proaktif olarak çözer ve gerektiğinde otomatik eylemler gerçekleştirir.

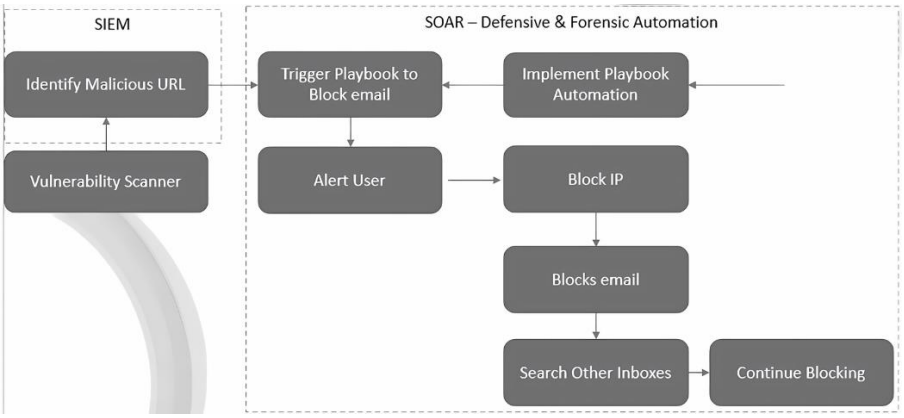
9.1.3. SOAR Platformunun Özellikleri

SOAR platformları yapay zeka ve makine öğrenimi kullanarak uyarıları analiz eder, ek içgörüler sağlar, önerilerde bulunur ve yanıtları otomatikleştirir. Bu platformlar ayrıca önceden tanımlanmış otomatik eylem kümeleri olan playbook'lar sunar. Bu playbook'lar, belirli tehditlere yanıt vermek için kullanılır ve olay algılama ve tepki sürelerini iyileştirmeye yardımcı olur.

9.1.4. Ölçeklenebilirlik ve Verimlilik

SOAR platformları, manuel işlemlerin zorluklarıyla başa çıkmak için ölçeklenebilirlik sağlar. Bu şekilde güvenlik operasyonları daha verimli hale gelir ve düşük seviyeli tehditlerin otomatikleştirilmesiyle maliyetler düşürülür.

9.2. SOAR - Kimlik Avı Saldırısı

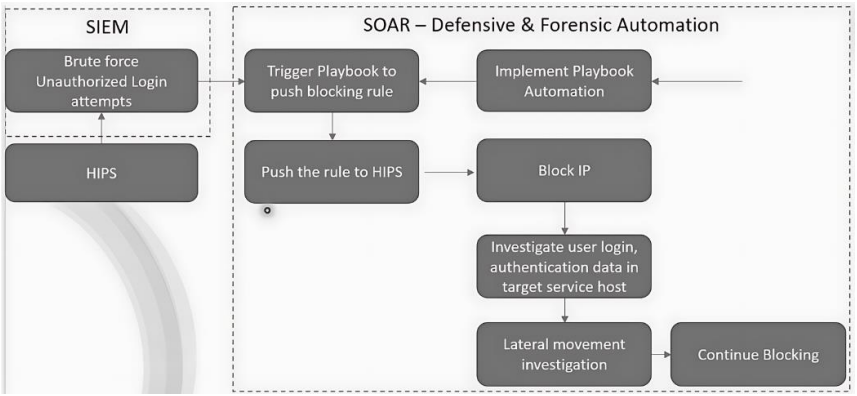


Otomatik olay yanıtı, özellikle kimlik avı saldırıları gibi hızlı yanıt gerektiren tehditlere karşı etkili bir şekilde mücadele etmek için kritik bir rol oynar. İşte bu süreci daha detaylı olarak açıklayalım:

1. **Teşhis ve Algılama**: İlk olarak, SIM platformu (Güvenlik Bilgi ve Olay Yönetimi) üzerinde çalışan güvenlik açığı tarayıcıları veya diğer güvenlik kontrol araçları, potansiyel bir kimlik avı saldırısını tespit eder. Bu, genellikle e-posta üzerinden gelen şüpheli bir içerik veya belirli IP adresleriyle ilişkilendirilen aktiviteler olabilir.
2. **Uyarı ve Tetikleme**: SIM platformu, tespit edilen bu olayı doğrular ve belirli bir playbook'i tetikler. Playbook, olaya yanıt olarak uygulanacak adımların önceden tanımlanmış bir setidir.
3. **Otomatik Müdahale**: Playbook tetiklendiğinde, otomatik müdahale süreci başlar. Örneğin, kimlik avı girişimini hedef alan bir playbook, saldırgan IP adresini otomatik olarak engelleyebilir. Aynı zamanda, kullanıcıları potansiyel tehlikeden haberdar etmek için uyarılar gönderebilir ve bu e-postayı alan diğer kullanıcı gelen kutularını tarayarak benzer saldırılara karşı koruma sağlayabilir.
4. **Yanıt ve Engelleme**: Güvenlik çözümü, olayı analiz ederken, IPS (Saldırı Önleme Sistemi) gibi kaynakları otomatik olarak yöneterek saldırıya yanıt verir. Bu, saldırganın hızlı bir şekilde engellenmesini ve saldırının yayılmasının önlenmesini sağlar.
5. **Süreç İyileştirmesi ve Öğrenme**: Her olay yanıtı süreci, platformun performansını artırmak için değerlendirilir ve gerekirse playbook'ler güncellenir. Bu süreç, gelecekteki benzer tehditlere daha iyi hazırlanmayı sağlar.

Bu şekilde, otomatik olay yanıtı çözümleri, kimlik avı gibi hızlı hareket etme gerektiren tehditlere karşı etkili bir şekilde mücadele etmeye yardımcı olur. Bu süreç, insan müdahalesi gerektirmeyen hızlı ve koordineli bir tepki sağlar, böylece organizasyonların güvenlik risklerini minimize etmesine yardımcı olur.

9.3. SOAR - Kaba Kuvvet Saldırısı



1. Teşhis ve Algılama: İlk olarak, SIM (Güvenlik Bilgi ve Olay Yönetimi) platformu veya başka bir güvenlik kontrol sistemi, kaba kuvvet saldırısını tespit eder. Bu saldırılar genellikle büyük hacimli isteklerle ve belirli bir zaman dilimi içinde yoğun aktivite ile karakterizedir.

2. Playbook Tetikleme: SIM platformu, kaba kuvvet saldırısı tespit edildiğinde ilgili playbook'i tetikler. Playbook, bu tür saldırılara karşı alınacak adımları otomatikleştiren bir dizi komut dosyasından oluşur.

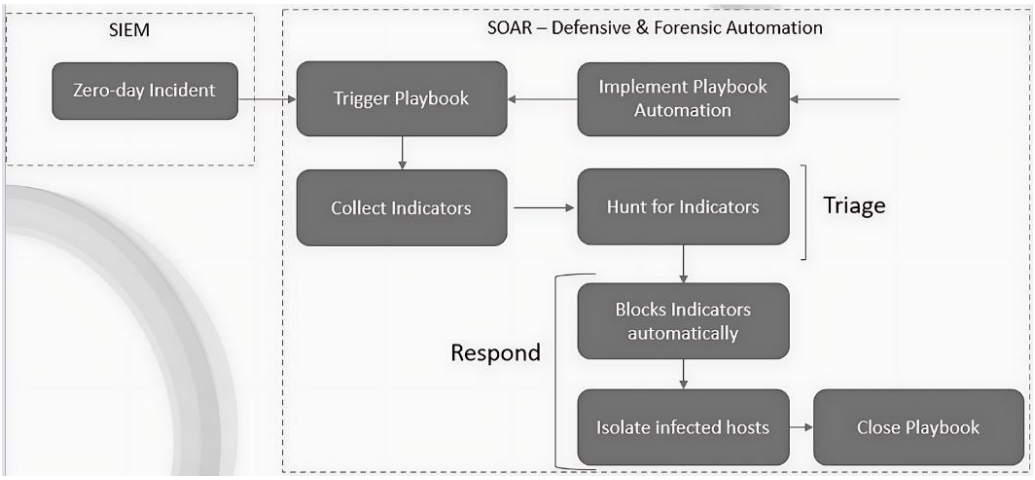
3. Otomatik Engelleme ve Yanıt: Playbook tetiklendiğinde, ilk olarak saldırganın IP adresi veya kaynağı otomatik olarak engellenebilir. Bu, saldırının hızla durdurulmasını sağlar ve ağ kaynaklarının korunmasına yardımcı olur.

4. Takip Eylemleri ve Yanal Hareket Analizi: Otomatik yanıt süreci, sadece saldırının anında durdurulmasını değil, aynı zamanda saldırganın etkisiz hale getirilmesi için takip eylemlerini de içerir. Örneğin, saldırganın erişim sağlamaya çalıştığı diğer sistemlere yönelik yanal hareket analizi yapılabilir ve bu sistemlerdeki kullanıcı hesapları incelenebilir. Eğer saldırganın başka sistemlere geçiş yapmaya çalıştığı tespit edilirse, bu hesapları da otomatik olarak engellemek mümkündür.

5. Süreç İyileştirmesi: Her saldırı olayı, platformun performansını artırmak için değerlendirilir ve playbook'ler sürekli olarak güncellenir. Bu sayede, gelecekteki kaba kuvvet saldırılarına karşı daha etkili ve hızlı bir yanıt sağlanabilir.

Otomatik olay yanıtı, kaba kuvvet saldırıları gibi hızlı ve geniş kapsamlı tehditlere karşı organizasyonların savunmasını güçlendirir. Bu tür saldırılar genellikle manuel müdahale ile etkili bir şekilde ele alınamayacak kadar hızlı gerçekleşirken, otomatikleştirilmiş yanıt süreçleri sayesinde saldırının etkileri minimize edilebilir ve ağın genel güvenliği sağlanabilir.

9.4. SOAR - Sıfır Gün(zero day) Güvenlik Açığı Saldırıları



Zero day tehditleri, siber güvenlik açıkları hakkında satıcıların bilgisi olmadan keşfedilen ve bu nedenle savunma önlemleri alınmadan önce saldırganlar tarafından sömürülen zafiyetlerdir. Bu tür saldırılar, organizasyonlar üzerinde ciddi ve potansiyel olarak yıkıcı etkilere sahip olabilir. Otomatik olay müdahalesi, sıfır gün tehditlerine hızlı ve etkili bir şekilde yanıt vermek için nasıl yardımcı olabilir?

1. Erken Teşhis ve Algılama: Otomatik olay müdahale sistemleri, genellikle SIEM (Güvenlik Bilgi ve Olay Yönetimi) ve SOAR (Güvenlik Otomasyonu, Orkestrasyon ve Yanıt) çözümleriyle entegre edilmiştir. zero day tehditleri tespit edildiğinde, bu sistemler hızla uyarı verir ve ilgili playbook'leri tetikler.

2. IOC Keşfi ve Analiz: Playbook, saldırının göstergelerini (IOC'ler) toplar ve analiz eder. Bu, kötü niyetli faaliyetleri izlemek için uç nokta günlüklerini, ağ güvenlik duvarı günlüklerini ve diğer güvenlik kaynaklarını sorgular.

3. Hızlı Yanıt ve Engelleme: Otomatik yanıt süreci, saldırının etkisini hızla sınırlamak için gereken adımları otomatik olarak gerçekleştirir. Bu, enfekte olmuş sistemleri izole etmek, saldırganın hareket alanını kısıtlamak ve saldırının yayılmasını önlemek gibi işlemleri içerir.

4. Güvenlik Denetimlerinin Güçlendirilmesi: Saldırıdan elde edilen bilgiler, güvenlik denetimlerini güçlendirmek ve gelecekte benzer saldırıları önlemek için kullanılır. Bu süreç, savunma mekanizmalarını sürekli olarak iyileştirmeye yönlendirir.

5. Olayların İncelenmesi ve Geri Bildirim: Her sıfır gün saldırısından sonra, olayların incelenmesi ve playbook'lerin gözden geçirilmesi önemlidir. Bu, gelecekteki saldırılara daha iyi hazırlanmak için öğrenme ve gelişim sürecini besler.

Otomatik olay müdahalesi, zero day tehditlerine karşı hızlı ve etkili bir yanıt sağlayarak organizasyonların zarar görmesini önler ve güvenlik açıklarının kötüye kullanılmasını engeller. Bu sayede, siber güvenlik savunmaları güçlendirilir ve organizasyonlar daha dirençli hale gelir.

10. Özet ve Sonuç

10.1. TOOLS R&R

Tool name	Open source /commercial	Description
Volatility	opensource	Insight into runtime system activity,dynamic memory forensic analysis
AVML	opensource	Memory forensics, insights into runtime system activity
Foremost	opensource	Used to recover/restore file, its forensic tool
Sleuthkit	opensource	Analyze disk images and recover files from the disk image
Ddrescue	opensource	Data recovery tool, recover complete disk system of file and folders
Xtrabackup	opensource	Perform hot backup of MySQL data while the system is running
mysqldump	opensource	MySQL data backup tool and restoration, perform logical backup
Rkhunter	opensource	Unix-based tool that scans for rootkits, backdoors and possible local exploits
iptables	opensource	Used to block intranet compromised/attacker host to prevent lateral movement

10.2. TOOLS - Threat Intelligence

Tool name	Open source /commercial	Description
Ipvoid	Free to use	Oneline ip addr verification
URLScan	Free to use	Online sandbox to validate suspicious urls
PortChecker	Free to use	Online portal for open port verification
VirusTotal	Free to use	Analyze suspicious files, domains, files, Ips and URLs
OSINT framework	Free to use	Collection of online tools to verify various IOCs
MxToolbox	Free to use	Online super tool to verify various IOCs
NetworkAppers	Free to use	Online collection of tools for various network verification
Cuckoo sandbox	Free to use	Online sandbox to verify suspicious malicious files

10.3. TOOLS - Pen Testing & OS hardening

Tool name	category	Description
Metasploit framework	Pen testing	Ruby based, it enables to write,test, and execute exploit code
Lynis	OS hardening	Health scan of systems, compliance testing

10.4. Taahhüt kuralları

Bağlılık kuralları kapsamında dikkate almanız gereken bazı kurallar listelenmiştir. Olay araştırması sırasında dikkat etmeniz gerekenler şunlardır:

1. Saldırgan Grubu ile İletişim Kurmayın: Saldırganlarla iletişim kurmaktan kaçının. Aksi takdirde, bu etkileşim sayesinde sistemlerimize kolayca sızabilirler.

2. Saldırganın Ağına Bağlanmayın: Kuruluşunuzdan saldırganın ağına bağlanmayın. Aksi halde, bağlantımız kritik bilgileri açığa çıkarabilir.

3. Adli Kanıtları Arşivleyin: Adli kanıtlar her zaman gereklidir. Bazen yasal işlemler için gerekebilir veya gelecekteki olay müdahalelerinde bu kanıtlara başvurabilirsiniz. Bu nedenle, adli kanıtları arşivlemek çok önemlidir.

4. Dış Ekiplerle Koordinasyon: İç, dış ve yönetim ekipleriyle her zaman koordinasyon halinde olun. Bazı kararlar, özellikle sınırlama, yok etme ve kurtarma aşamalarında çok kritiktir ve bazen yasal konular da işin içine girebilir. Bu yüzden yönetim ve dış ekiplerle koordinasyon önemlidir.

5. Olay Detaylarının Gizliliği: Tüm olay detayları gizli tutulmalı ve bu bilgilere sınırlı erişim sağlanmalıdır. Olay bilgisi çok hassastır ve korunmalıdır.

10.5. Kritik Noktalar

Gerçek bir olayı ele alırken dikkat etmeniz gereken bazı kritik noktalar şunlardır:

1. Ayrı Adli Uygulama Kopyası Tutun

Adli soruşturma yaptığınızda, adli kanıtları toplamalı ve ayrı bir sunucuda arşivlemelisiniz. Adli bir kopya olmadan aynı sunucuya yeniden yükleme yapmamalısınız. Bu çok önemlidir, aksi takdirde adli kanıtları kaybedebilirsiniz.

2. Sunucuyu Kapatmadan veya İnternet'ten Kesmeden Önce Düşünün

Sunucuyu kapatmadan veya internet bağlantısını kesmeden önce dikkatlice düşünmelisiniz. İlk analizden hemen sonra bu adımı atarsanız, önemli kanıtları kaybedebilirsiniz ve altyapınızın ne ölçüde tehlikeye atıldığını bilemezsiniz. Saldırganla iletişim kurmayı durdurmak, komuta ve kontrol bağlantısını kesmek anlamına gelebilir ve bu da siber suçluyu uyarabilir. Bu adımı atmadan önce gerekli olup olmadığını tekrar düşünmelisiniz.

3. Temiz Bir Yedekleme ile Geri Yükleyin

Yedeklemenin temiz bir kopya olduğundan emin olmadığınız sürece sisteminizi yedekten geri yüklemeyin. Çoğu zaman, gelişmiş kalıcı tehditler (APT'ler) uzun süre fark edilmeden ağınıza bulaşabilir ve yedekleme enfeksiyona eğilimlidir. Virüslü bir yedeklemenin yüklenmesi, enfeksiyonu yeniden oluşturabilir.

Bu kritik noktaları gerçek olayları ele alırken aklınızda bulundurmanızı ve en iyi uygulamaları takip etmenizi öneririm.

10.6. Sonuç

- Mevcut Olay Sürecini Gözden Geçirin
- Olay Ekibini Kurun
- Olay Müdahale Sürecini Tanımlayın
- Olay Müdahale Kontrol Listesini Tanımlayın
- Mevcut ve Geçmiş Olayları Belgeleyin
- NIST Olay Yönetim Metodolojisini Takip Edin
- Olay Müdahale Playbook'u Oluşturun
- Güvenlik Tatbikatları
- Algılama Kuralları Optimizasyonu
- Sürekli İyileştirme