OLAY MÜDAHALESININ TEMELI OLARAK OLAY GÜNLÜKLERININ ANALIZI

YASIN KARAMAN, IT BUSINESS MANAGEMENT (BACHELOR PROFESSIONAL), CISSP, CEH

ONUR SAVAŞ, PENETRATION TESTER

1. ARKA PLAN VE UYGULAMA KAPSAMI

1.1 Arka plan

Birkaç yıldır, çeşitli türlerde parasal ve/veya ideolojik amaçlı siber saldırılarda istikrarlı bir artış gözlemlenmektedir. Bu bağlamda özellikle aşağıdaki olay türlerinden bahsetmek gerekir:

- APT kampanyaları (TTP) (Gelişmiş Kalıcı Tehditler)[1],
- DDoS saldırıları (Distributed Denial of Service)[2] yanı sıra
- kasıtlı veri sızdırma veya kazara veri sızıntıları

Bilgisayar tabanlı suçlar ve saldırılardaki genel artış nedeniyle, faillerin etkili ve verimli bir şekilde kovuşturulması veya soruşturulması giderek daha önemli hale gelmektedir. Bu durum hem bilgisayar tabanlı sistemlerin saldırı aracı olarak kullanıldığı (geniş anlamda siber suçlar) hem de sistemlerin kendilerinin saldırı hedefi olduğu (dar anlamda siber suçlar) durumlar için geçerlidir.

Bu bağlamda adli soruşturmaların görevleri, dijital suçların kanıtlanması (örneğin dijital izlerin analiz edilmesi yoluyla), sonuçta ortaya çıkan soruşturmalar ve daha etkili karşı önlemlerin başlatılabilmesi için siber saldırıların ve etkilerinin izlenebilirliğidir.

Mevcut günlük verileri, bir güvenlik olayının analizinde merkezi bir rol oynar. Günlük verileri genellikle kişisel veriler de içerdiğinden, Avusturya Veri Koruma Yasası ve Genel Veri Koruma Yönetmeliği burada da geçerlidir. Bu, diğer şeylerin yanı sıra, hem güvenlikle ilgili verilere veya olası olayların analizine yönelik bir kısıtlama hem de buna karşılık gelen bir kısıtlama gerektirir.

Yetkisiz erişim veya manipülasyondan korumak için günlük verilerine yönelik yedekleme konsepti.

Adli soruşturmanın amacı aşağıdaki sorulara cevap vermektir:

- Ne oldu?
- Nerede oldu bu?
- Ne zaman oldu bu?
- Bu nasıl oldu?

[1] Bunlar, yetkililer, kurumlar veya şirketler gibi kuruluşlara yönelik karmaşık, hedefli ve ayrıntılı saldırılardır.
[2] Ayrıca CSC yayın serisine bakınız: "Dağıtılmış Hizmet Engelleme (DDoS) - Arka plan, önleyici tedbirler ve hafifletme tedbirleri".

Bu soruları yanıtlamak iki farklı yaklaşımla mümkün olabilir:

ÖLÜM SONRASI ANALIZ

Ölüm sonrası analiz, dijital izlerin adli bir kopya üzerinde analiz edildiği, kapatılmış bir sistemin analizidir duplication[3] analiz edilir. Ancak, uçucu veriler genellikle sistem kapatıldığında kaybolduğundan ve bu nedenle analiz edilemediğinden, çalışma zamanında sistemin durumu hakkında ifadeler pek mümkün değildir.

CANLI YANIT ANALIZI

Buna karşılık, canlı yanıt analizleri uçucu ve/veya geçici olarak erişilebilir verilerin incelenmesine olanak tanır.

1.2 Uygulama kapsamı

Bu rehberin kapsamlı bir BT adli tıp ve/veya olay müdahale kılavuzu olması amaçlanmamıştır. Alman Federal Bilgi Güvenliği Ofisi'nin (BSI) BT Adli Tıp Kılavuzları gibi bu amaca yönelik kapsamlı ve kapsamlı belgeler zaten mevcuttur.[2]

Bu eylem önerisinin odak noktası aşağıdaki soruların yanıtlanmasıdır:

- Bir şirkette delillerin olası muhafazasına ilişkin olarak alınması gereken en önemli (asgari) önlemler ve önleyici tedbirler nelerdir?
- Doğru (teknik) davranış nedir ve belirli bir güvenlik olayına yönelik en önemli adımlar ve tepkiler nelerdir?
- Kanıtların korunması için (yetkililer için) hangi ilgili adımlar atılmalı veya tavsiye edilmelidir?
- İlgili makamlarla nasıl iletişime geçiyorsunuz? Ve bunlar hangileri?

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT- Forensics.pdf?blob=publicationFile&v=1

Bir güvenlik olayı sırasında bir yetkili çağrılırsa, her zaman iki hedef ön plandadır:

1. Tehlike önleme
2. Soruşturmalar

İkinci husus her zaman yetkili makamın savcılığa rapor verme yükümlülüğüyle sonuçlanır.

Bir olaydan sonra temizlik, iç süreçlerin iyileştirilmesi, daha sonraki adımların uygulanması veya önlemlerin uygulanması gibi eylemler ve görevler yetkili makamların görev alanına girmez, ancak şirketin sorumluluğundadır.

2. HAZIRLIKLAR

Aşağıdaki açıklamaların odak noktası, farklı günlük verisi türleri ve ilgili bir analizi mümkün kılacak olasılıklar veya adımlardır.

Erişim haklarına ilişkin olarak log verilerinin korunmasına yönelik artan ihtiyacın sağlanması gibi altyapısal ve organizasyonel hazırlıklar ve kurallar aşağıda ayrıntılı olarak ele **alınmayacaktır.** Bununla birlikte, günlük verilerinin depolanması, aktarılması ve işlenmesine ilişkin koruyucu tedbirlerin doğru bir şekilde uygulanmasının önemine burada işaret edilmelidir.

2.1 Veri toplama

Veri toplama bağlamında, (1) **ağ ve ana bilgisayar tabanlı olay günlükleri ile** (2) **uygulama ve veritabanı olay günlükleri** arasında temel bir ayrım yapılabilir.

AĞ VE ANA BILGISAYAR TABANLI GÜNLÜKLER

Aşağıdaki tabloda, avantaj ve dezavantajları ve önerilen saklama süresine ilişkin bir öneri de dahil olmak üzere günlüğe kaydedilebilecek / kaydedilmesi gereken farklı günlük verileri hakkında bilgi verilmektedir.

Veri türü	Avantajlar	Dezavantajlar	Depolama süresi
Full Packet Capture (PCAP); ağ paketlerinin orijinal tam veya kısmi verilerini içermektedir. Ancak, PCAP verilerinin yakalanması ve saklanması sadece özel durumlarda veya yüksek derecede kritik olan sistemler için gereklidir. Bu verilerin rutin olarak yakalanması ve saklanması önerilmez.	Ağ paketlerinin ve veri trafiğinin derinlemesine analizi, serbestçe kullanılabilen araçlar ve yardımcı programlar sayesinde mümkündür. Ancak, tam veri erişimi sadece şifrelenmemiş iletişimlerde mümkündür.	Toplanan verilerin boyutu, depolama alanı gereksinimleri ve analiz süresi gibi gereksinimler, son derece büyük olabilir. Bunun yanı sıra, analiz sırasında gizlilikle ilgili yasal düzenlemeler gibi hukuki çerçeve koşulları da sorun oluşturabilir.	3 ay veya daha uzun süre
Netflow verileri, ağ iletişiminin içeriğini değil, her ağ bağlantısının meta verilerini içermektedir.	Netflow verileri, ağ trafiğinin içeriğine değil, her ağ bağlantısının meta verilerine dayandığı için, depolama alanı gereksinimleri daha azdır ve analizleri daha hızlıdır. Ayrıca, verilerin gizliliğine ilişkin hukuki sınırlamalar da daha azdır. Netflow verilerinin analizi, ağ trafiği şifreli veya şifresiz olsa da mümkündür.	Netzwerk paketinin içeriği kaydedilmediği için, ayrıntılı analizler yapılamamaktadır.	6 ila 12 ay arası
Log dosyaları, uygulama veya platforma özgü bilgileri (örneğin, proxy günlükleri veya işletim sistemi olay günlükleri) içerir.	SIEM sistemleri, derinlemesine uygulama ve platform özel analizlerini mümkün kılar.	Log verilerini zenginleştirmek ve farklı kaynaklardan birleştirmek ve bağlantılar kurmak için önemli bir çaba gerektirir. Login içerikleri ile ilgili uygulama ve platform özel bağımlılıklar söz konusudur.	6 ila 12 ay arası

Yukarıda bahsedilen günlük veri türleriyle ilgili olarak, "saf" analiz açısından (yetkililer, işlemler vb.) "ne kadar çok ve kapsamlı olay günlüğü verisi toplanırsa o kadar iyidir" ilkesinin geçerli olduğunu belirtmek gerekir. Elbette verimlilik açısından bu günlük toplamanın her zaman geçerli olmaması söz konusu değildir. Depolama alanı veya analiz için insan kaynakları için ek masrafların kabul edilmesi gerekebilir.

Bununla birlikte, toplanan her bir günlük verisi türü için asgari bir bilgi kümesi belirlenmeli ve en azından tüm sistemlerde uygulanmalıdır, örneğin aşağıdaki sistem olayları, olası bir kötü amaçlı yazılım bulaşması açısından önemleri nedeniyle her zaman işletim sistemi düzeyinde kaydedilmelidir:

- Komut / Powershell Komutları
- Servis / Cronjobs Oluşturma, Başlatma, Durdurma
- Program başlatma, otomatik başlangıç girdileri
- Kullanıcıya özel olaylar (yerel ve ağ kullanıcılarının başarılı/başarısız kimlik doğrulaması, kullanıcı oluşturma, kullanıcı haklarında ve atanan gruplarda değişiklikler)
- Ağ erişimi

Aşağıdaki tablo, bu tür verilerin ağınızda nerelerde toplanabileceğine ve bu toplama noktaları için hangi avantaj ve dezavantajların mevcut olduğuna dair genel bir bakış sunmaktadır.

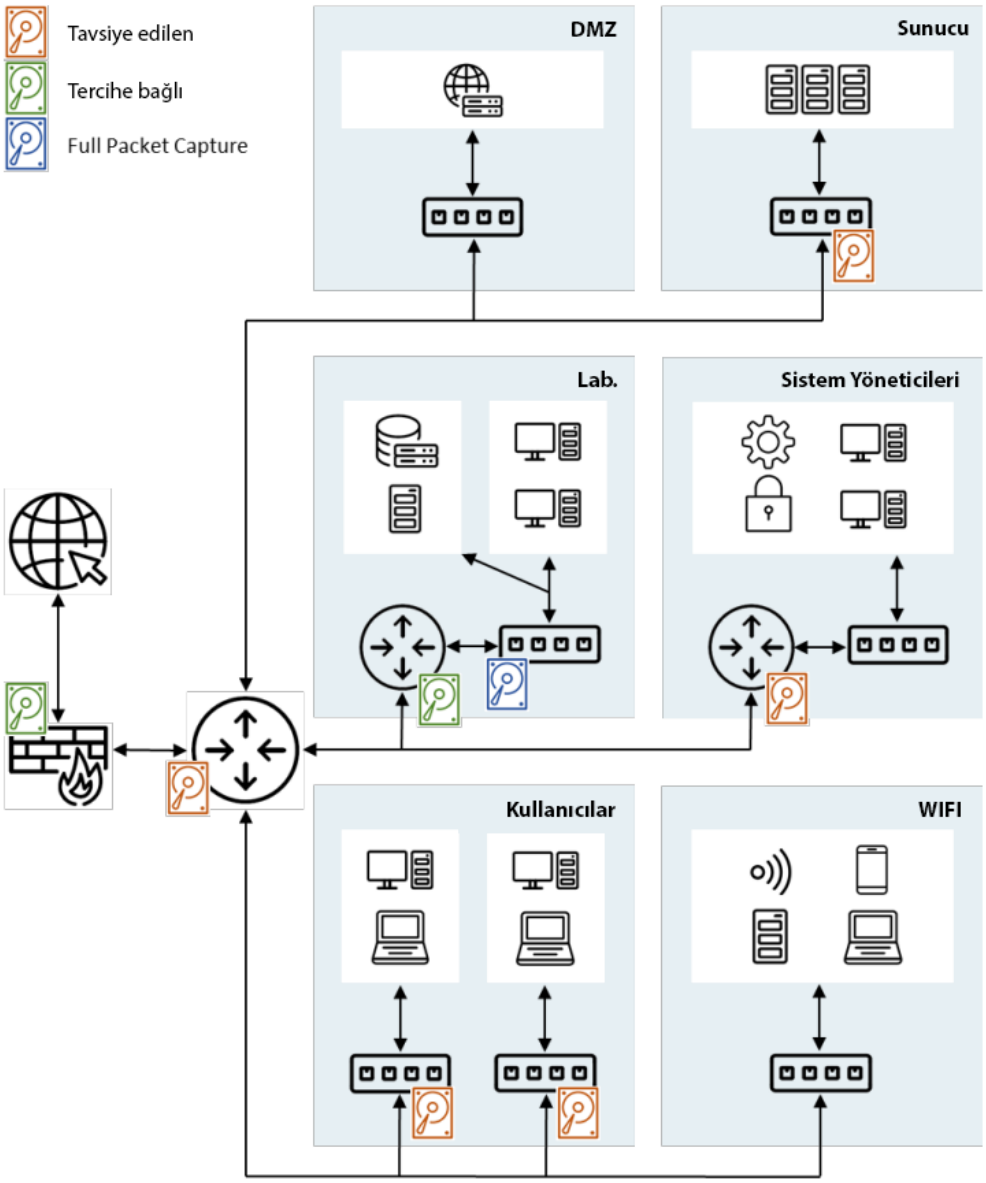
Toplama noktası	Avantajlar	Dezavantajlar
Switch üzerindeki bir Mirrorport sayesinde ağ paketleri kopyalanabilir ve daha sonra PCAP veya Netflow analizleri için başka bir yere gönderilebilir.	Mirrorport oluşturmak için minimum yapılandırma ayarları gereklidir. Switchler hemen hemen tüm ağ topolojilerinde ve ağ katmanlarında kullanılır veya her zaman mevcuttur.	Sınırlı bant genişliği nedeniyle veri kaybı mümkündür.
Yönlendiriciler genellikle NetFlow verilerini dışa aktarma imkanı sunar.	Yaygın ağ topolojilerinde işlevsellik zaten mevcut olduğundan, minimum yapılandırma ayarlamaları gereklidir.	Normalde PCAP mümkün değildir.

Toplama noktası	Avantajlar	Dezavantajlar
Web proxy'leri, yük dengeleyiciler, DHCP ve DNS sunucuları vb. gibi Katman cihazları ve hatta uç nokta cihazları PCAP, Netflow veya diğer veri ve bilgileri toplamak için değerli kaynaklar olabilir.	Proaktif olarak ve/veya bir olay durumunda adresinden toplanacak, ilişkilendirilecek ve değerlendirilecek ek veri ve bilgiler burada toplanabilir.3.	Günlük verilerini zenginleştirmek ve farklı kaynaklardan toplamak ve ilişkilendirmek için önemli ölçüde daha fazla çaba. Oturum açma içeriğiyle ilgili olarak uygulamaya veya platforma özgü bağımlılıklar.
Bir ağ musluğu, ağ paketlerini çoğaltan ve daha fazla PCAP veya Netflow analizi için ileten özel bir donanım tabanlı cihazdır.	Özellikle ağ verilerinin toplanmasına yönelik uygulama amacı ve dolayısıyla toplama noktaları açısından "en iyi durum" (performans ve güvenilirlik açısından da).	Cihazlar çok pahalı olabilir ve genellikle ağa kurulum için ağ trafiğinde kısa süreli kesintiler gerektirir.

Ağ günlük verileri için uygun toplama noktalarının belirlenmesi, gözetim/izleme ve/veya kanıt toplama amacıyla etkin veri toplanmasını sağlamak için gerekli ilk adımdır.

Bu durum aşağıdaki şekilde örneklendirilmiştir:

[4] Ayrıca bkz. bölüm 2.2



Aşağıdaki en iyi uygulamalar bu tanımlamaya yardımcı olabilir ve takip edilmelidir:

- Kritik verilerin / altyapının tanımlanması
- Şirket çapında bir ağ planının oluşturulması / sürdürülmesi (şema)
- Kullanıcı, veri ve (bağlıysa) internet arasındaki merkezi ve/veya kritik ağ noktalarının tanımlanması, örneğin VLAN'ların birleştirilmesi
- Kritik ve/veya hassas veri işleme ve/veya veri depolama konumlarının tanımlanması, örn: DNS sunucusu, CRM sistemi, sürüm kontrol sistemi vb.
- Düzenleyici ve yasal uygunluk ile ilgili koordinasyon
- NAT/PAT/yük dengeleyiciler vb. tarafından çevrilmeden önce ağ akışlarının depolanması.

UYGULAMA VE VERITABANI GÜNLÜKLERI

Farklı uygulamaların ve veritabanlarının denetim günlükleri, erişim günlükleri, iş akışı günlükleri vb. de olayların izlenebilirliği için çok değerli bilgiler sağlayabilir (örn. veri sızıntısı vb.).

Bu tür günlük verilerinin varlığı veya kalitesi elbette büyük ölçüde uygulamanın veya veritabanının kendi uygulamasına ve yapılandırmasına bağlıdır. Bu nedenle, tüm farklı uygulama ve veritabanlarının ayrıntılı bir listesini vermek bu (ve muhtemelen diğer) eylem önerilerinin kapsamını aşacaktır. Ancak, ağ uygulamalarının uygulama günlükleri bu bağlamda özellikle bilgilendiricidir, bu nedenle burada bazı pratik ipuçları özetlenmiştir:

Bir "http proxy "nin günlükleri (ve zorunlu kullanımı) web sayfalarına erişimin izlenmesi için çok önemlidir. Buradaki ilgili bilgi şudur:

- hedef URL,
- istek türü,
- kaynak IP,
- yanıt kodu,
- paket boyutu,
- yönlendiren ve
- zaman damgaları.

Özellikle kaynak IP ile, söz konusu istemcinin açıkça tanımlanabilmesi sağlanmalıdır (örneğin NAT veya DHCP kullanılırken ilgili günlükler aracılığıyla).

DNS günlükleri hangi etki alanının hangi istemci tarafından çözümlendiği hakkında bilgi sağlar. Bu, örneğin C2 alan adlarının tanımlanmasına yardımcı olur. İşlemeyi ve analizi kolaylaştırmak için pasif bir DNS veritabanı kullanmak faydalıdır. NXDOMAIN isteklerinin de günlüğe kaydedilmesi tavsiye edilir.

2.2 Veri analizi

Toplanan verileri önceki bölümde açıklandığı şekilde işlemek ve analiz etmek için aşağıdaki iş akışı kullanılabilir.

Daha ileri soruşturmalarla ilgili olarak, yetkililerin (veya bir iç güvenlik ekibinin) gerekirse 3. ve 4. adımları gerçekleştirmesini sağlamak için özellikle 1. ve 2. adımlar şirket tarafından gereklidir.

Ayrıca, somut bir güvenlik olayı durumunda, örneğin başka kanıt nesneleri.
Örneğin, bellek ve sabit diskler daha ileri analizler için çok değerli olabilir.

Adım	Hedef
1. Toplam	Analize hazırlık olarak, toplanan günlük verileri ilişkilendirilir ve toplanır (en iyi durumda, bu amaç için halihazırda uygulanmış bir analiz platformunun yardımıyla).
2. Odaklanma	Analizi belirli göstergeler (IP adresleri, bağlantı noktaları, protokoller, zaman/uzaklık, etki alanları, ana bilgisayar adları, vb.) açısından bir veya daha fazla alt veri kümesine odaklayabilmek için tüm veri havuzunun azaltılması veya filtrelenmesi.
3. Analiz	Bir önceki adımda odaklanılan veri havuzunun analizi, şüpheli olay ve ağın normal davranışı hakkında mevcut bilgilerle birleştirilerek, örneğin olağandışı ağ trafiği, protokol kullanımı veya sistem olayları.
4. Gösterge üretme (IOC'ler)	DNS etkinliği, kötü amaçlı yazılım örnekleri, sertifikalar, komuta ve kontrol ağ trafiği gibi daha sonra aynı veya benzer bir olayın göstergeleri olarak hizmet edebilecek kalıpları ve/veya bilgileri bulmak.
5. Göstergelerin kullanımı (IOC'ler)	Bir önceki adımda bulunan yeni göstergeleri tüm veri havuzunda arayarak olası başka olayları burada da tespit edin ve/veya daha sonra sürekli izleme için kendi ağınızın işleyişinde arayın.

Diğerlerinin yanı sıra, aşağıdaki metrikler (örnek olarak verilmiştir) analiz edilecek verilerdeki veya ağın çalışması sırasında devam eden izlemedeki anormallikleri tespit etmek için kullanılabilir:

Metrikler / Konum	DNS	Firewall	HTTP proxy	HTTP	NetFlow	NSM	Pasif DNS
En Çok İletişim Kurulan IP Adresleri					X		
HTTP Kullanıcı Aracısı			X	X		X	
En çok sorgulanan DNS alanları	X					X	X
HTTP gönderi boyutları			X	X		X	
Yeni tanınan/kayıtlı alan adları	X					X	X
Olağandışı bağlantı noktası ve protokol kullanımı					X		
(Periyodik) Trafik Hacmi					X		

2.3 Personel

Önceki bölümlerde açıklanan tüm önlemler, görevler veya adımlar büyük ölçüde nitelikli ve mevcut personele bağlıdır.

Bu, hem hazırlık önlemleri hem de bir olay durumunda faaliyetler açısından kendi personeli veya hizmet sağlayıcılar tarafından yapılabilir.

Kaydedilen günlük verilerinin işlenmesinin yanı sıra bir SIEM sisteminin bakımı ve yapılandırılması için personel kaynakları (Almanya'daki orta ölçekli bir şirket temel alınarak) 12x5 operasyonunda 3 ila 4 tam zamanlı çalışana karşılık gelmektedir. Ancak bu durum, saldırıların mesai saatleri dışında hiç tespit edilememesi ya da yalnızca ertesi gün tespit edilebilmesi gibi yüksek bir riski beraberinde getirmektedir. Böyle bir sistemin 7x24 çalışması için yaklaşık 7 ila 8 çalışanı hesaba katmak gerekir.

Bu değerlendirmeler, geçmişte meydana gelen siber saldırıların (özellikle DDoS ve tahrifatlar) analiz sonuçlarına da dayanmalıdır; bu analizler, ilgili fail gruplarının bu tür saldırılar için genellikle Cuma akşamlarını, hafta sonlarını, tatil dönemlerini veya resmi tatillerin arifesini kullandığını göstermektedir. Yeni saldırı senaryolarıyla başa çıkabilmek için ilgili kişilerin düzenli olarak eğitilmesi gerektiği de unutulmamalıdır. Ayrıca, belirli tehditlere hızlı ve doğru bir şekilde tepki verebilmek için ideal olarak bir olay müdahale planı oluşturulmalı ve uygulanmalıdır.

3. BIR OLAY OLMASI HALINDE

Yetkililerin bakış açısından ve daha ileri soruşturmalar açısından, aynı zamanda saldırının izlenebilirliği ve sonuçta ortaya çıkan karşı önlemler için, aşağıdaki günlük verileri siber saldırının türüne bağlı olarak gerekli veya avantajlıdır.

Günlük Verileri / SiberSaldırı	APT	Veri sızıntısı	DDoS	Arka Kapı	Fidye Yazılımı	Oltalama	Web uygulaması
Güvenlik Duvarı	X	X	X				
HTTP proxy	X	X		X	X		
HTTP sunucusu			X				X
NetFlow	X	X	X	X	X		X
NSM[10]	X	X		X	X		
Pasif DNS	X	X		X	X	X	
DDoS Koruması			X				
Ana bilgisayarda olay günlüğü	X	X		X	X	X	
Özel, getirilen cihazlar (BYOD)	X	X					
Posta sunucusu	X	X			X	X	
Uygulama/veritabanı sunucusu		X	X				X

Saldırı türüne bağlı olarak güvence altına alınması gereken diğer kanıt nesneleri arasında şunlar yer almaktadır

- Çalışma belleği
- Sabit diskler
- Sanal makineler
- Gömülü Cihazlar / Aletler
- Ağ sürücüleri
- Uygulama verileri
- Yedekleme
- Bulut hizmetlerindeki veriler
- Mobil cihazlar
- E-posta geçmişleri

Bir saldırı veya olay durumunda, aşağıdaki iki alt bölüm, hiçbir koşulda yapılmaması gereken veya teknik olarak mümkün olduğu ölçüde her durumda yapılması gereken eylemlere genel bir bakış sunmaktadır.

3.1 Hiçbir durumda

Bir saldırı veya olay durumunda, aşağıdaki eylemler hiçbir koşulda gerçekleştirilmemelidir:

Ne değil?	Neden değil?
Virüs bulaşmış ana bilgisayarın / bilgisayarın zamanından önce kapatılması veya kapatılması .Bunun bir benzeri de sanal makinelerin kapatılmasıdır.	• Önemli veri ve bilgiler bilgisayarın RAM'inde (Rastgele Erişim Belleği) kaybolabilir.
Herkes tarafından erişilebilen Virus Total gibi halka açık platformlarda, kötü amaçlı yazılım örneklerinin bağımsız anlık analizleri yapılması.	• Kötü amaçlı yazılım üreticilerinin, kötü amaçlı yazılımlarının analizi için yüklenmiş olduğu platformlarda "dinleme" yapabileceklerini ve kendi programlarının analiz edildiğini tespit edebileceklerini varsaymak gerekmektedir. • Bunun sonucunda, saldırgan saldırıyı sonlandırabilir, izleri yok edebilir vb.
Sistemin yeniden kurulması, yedeklerin geri yüklenmesi ve günlük işlere dönülmesi gibi basit bir çözüm, bazen kaynak eksikliği veya kamuya açıklanma korkusu gibi nedenlerle daha kapsamlı bir analiz görmezden gelinir veya tedavisi ciddi şekilde geciktirilir. Ancak saldırgan sıklıkla dahili ağda yayılır ve diğer ana bilgisayarlara enfekte olur veya sistemde alternatif erişim yolları bulur. Potansiyel bir saldırganın kendi ağınızda neden olabileceği zarar genellikle küçümsenir. Ayrıca saldırı vektörünün kesin analizi ve açığın kapatılması olmadan, aynı veya benzer bir saldırı her zaman tekrar gerçekleştirilebilir.	• Bazı durumlarda, kaynak eksikliği veya halka açık bilgi haline gelme korkusu nedeniyle daha derinlemesine bir analiz göz ardı edilir veya tedavisi ciddi şekilde geciktirilir. • Saldırgan sık sık iç ağda yayılır ve diğer ana bilgisayarları enfekte eder veya sisteme alternatif erişim yolları sağlar. • Potansiyel bir saldırganın kendi ağında neden olabileceği zarar genellikle küçümsenir. • Giriş vektörünün tam olarak analiz edilmeden ve açığın kapatılmadan aynı veya benzer bir saldırı her zaman tekrar gerçekleştirilebilir.

3.2 Her durumda

Bir saldırı veya olay durumunda, her halükarda aşağıdaki önlemler alınmalıdır:

Neyi?	Neden?
İç ağda enfekte olan ana bilgisayarların / bilgisayarların izolasyonu.	• "Lateral Movement" (Yanal Hareket) olarak adlandırılan, ağınızın diğer kısımlarının daha da enfekte olması veya ele geçirilmesi durumunu önlemek için.

Neyi?	Neden?
Mümkünse, C&C[13] bağlantılarını kesmeden ancak yavaşlatarak, band genişliğini azaltın.	• Saldırgan / kötü amaçlı yazılım hala dışarıya doğru bir bağlantı görüyor. Band genişliği kısıtlaması çeşitli nedenlerden dolayı yapılabilir, bu nedenle saldırganın şüphelenmesi ve fark edilmesi daha az olasıdır. • Kısıtlama yoluyla büyük ölçekli veri sızdırma engellenebilir. • Saldırganın / kötü amaçlı yazılımın faaliyetlerinin genellikle çok açıklayıcı olan sürekli bir analizi mümkündür.
Analizlere başlamadan önce **sistem durumunun yedeklenmesi.**	• Sistem üzerindeki analizler, çalışma belleğindeki veya veri taşıyıcıları üzerindeki ayrılmamış alanlardaki ilgili eserler gibi verileri istemeden yok edebilir / gizleyebilir. • Ancak, bu veriler daha derin bir adli analizde değerli olabilir. • Saldırgan tespit edildiğini anlarsa, izini kaybettirme fırsatı verilmemelidir.
Analizi kolaylaştırmak için ek loglama ayrıntılarının etkinleştirilmesi.	• Bu, sistem ortamındaki tüm seviyeleri (işletim sistemi, ağ ve uygulamaya özel günlük kaydı) etkiler. • Günlük olaylarının ayrıntı düzeyi büyük ölçüde analizin amacına bağlıdır. Aşağıdaki günlük bilgileri düşünülebilir: ✓ Kullanıcı girişleri ✓ Kullanıcı yönetimi ✓ Veri erişimi ✓ Ayrıcalıklı kullanıcı eylemleri ✓ Süreç takibi ✓ Sistem olayları ✓ Ağ bağlantıları • Kapsamlı bir resim elde etmek için hem hatalar hem de başarılı olaylar kaydedilmelidir. • Ek günlük bilgilerinin etkinleştirilmesinin bellek tüketimini önemli ölçüde artırdığına dikkat etmek önemlidir.

Kritik güvenlik açıklarının kapatılması, örneğin yazılım bileşenlerinin güncellenmesi.	• Daha fazla yayılma olasılığını en aza indirmek için.
Sistem günlük bilgilerinin yedeklenmesi.	• Belgelendirme amaçları için ve gerektiğinde cezai işlemler için.
Sistem analizi görüntüsü.	• Mümkünse, analiz için etkilenen gerçek sistemde mümkün olduğunca az işlem yapılması önerilir ve mümkün olduğunda standart bir formatta bir kopya oluşturulması önerilir.(VM Snapshot veya disk imajı ve geçici belleğin yedeklenmesi).

Neyi?	Neden?
Alınan tüm önlemlerin ve eylemlerin **belgelendirilmesi**	• Elde edilen sonuçların takibi için güvenilir bir kayıt tutulması gerekmektedir. Bu, olayın nasıl ele alındığının, hangi önlemlerin alındığının ve sonuçlarının kaydedilmesi ile sağlanır. Bu, olayın tüm aşamalarının belgelenmesi ve gerektiğinde doğru bir şekilde açıklanabilmesi için son derece önemlidir.

Komuta ve Kontrol[13]

4. UYGULAMA IÇIN PRATIK TAVSIYELER

4.1 Konsept ve Konfigürasyon

Merkezi günlük platformları, ağ cihazları, uygulamalar ve sunucuların veya istemcilerin işletim sistemleri gibi çok çeşitli veri kaynaklarından gelebilen günlük verilerini analiz etmek için en son teknoloji olarak kabul edilir. Sadece ihtiyaç duyulduğunda farklı veri kaynaklarını ve formatlarını birleştirmeye başlamak genellikle analizi önemli ölçüde geciktirir. Aynı zamanda, günlük verileri saldırganlar tarafından manipüle edilmeye veya yetkisiz kişilerin erişimine karşı, ayrı sistemlere dağıtılmalarına kıyasla daha iyi korunabilir. Bu aynı zamanda hem güvenlik olaylarının (izleri) hem de hataların araştırılması açısından tüm sistemin aktif olarak izlenmesini sağlar veya kolaylaştırır.

Veri toplamak, görselleştirmek ve analiz etmek için hem ücretsiz hem de ücretli yazılım çözümleri bulunmaktadır. Kullanılacak teknolojiye karar verirken, edinim maliyetlerine ek olarak aşağıdaki hususlar da göz önünde bulundurulmalıdır:

- Personel eğitimi için maliyetler
- Maliyetlerin kaydedilen veri miktarına bağımlılığı
- Kaydedilen veriler için seçim kriterlerini ayarlama maliyetleri
- Günlük verilerini (hem gizli şirket içi verileri hem de kişisel verileri içerebilir) üçüncü taraflara veya bulut sağlayıcılarına aktarırken yasal koruma.

Farklı kaynaklardan gelen verilerin pratik analizi ve korelasyonu için, tek tip şirket zaman verilerinin kullanılması yararlıdır. Bu, (dahili veya harici) zaman sunucularının kullanımının yanı sıra tek tip bir zaman diliminin kullanılmasını veya kullanılan zaman diliminin etiketlenmesini içerir. Ayrıca, merkezi bir günlük veri analizi durumunda bile herhangi bir zamanda kesin veri kaynaklarını belirleyebilmek (veya bunlara göre filtreleyebilmek) için toplama sırasında verilerin uygun şekilde etiketlenmesi tavsiye edilir.

4.2 Hızlı Kazananlar

Bilinen IOC'ler veya anomali tespiti ile ilgili kapsamlı veri toplama, korelasyon ve analize ek olarak, mevcut bir tehlikeye işaret edebilecek ve daha fazla araştırılması gereken şüpheli davranışları tespit etmek için bazı hızlı kazanımlar da vardır.

Aşağıdaki durumlar dikkat çekici olabilir:

- Harici bir web sunucusuna, istemcinin sunucudan aldığından daha fazla veri yüklenir (yükleme/indirme oranı).
- Gelen ve giden e-postalar:
  - Hangi eklentiler dışarıdan kendi şirket ağına geliyor?
  - E-posta ile gönderilen dikkat çekici miktarda veri var mı?
  - Şirket içi politikaya aykırı olmasına rağmen bilinen ücretsiz e-posta sağlayıcılarına gönderilen/alınan e-postalar var mı?
  - E-postalar otomatik olarak (örneğin bir kural aracılığıyla) harici adreslere iletiliyor mu?
  - IP tabanlı URL'lerle iletişim (örneğin https://194.12.X.X adresine erişimler gibi) kötü amaçlı yazılımlara işaret edebilir, çünkü bu normal işlemlerde nadiren gerçekleşir.
- Olağandışı bağlantı noktaları ile iletişim
  - Hangi eklentiler dışarıdan kendi şirket ağına geliyor?
  - HTTP(S) trafiği 80 ve 443 numaralı bağlantı noktalarından başka bağlantı noktalarından da geçiyor mu?
  - Yönlendiricisiz POST istekleri: Yönlendiricinin olmaması doğrudan bir sayfa görünümünü gösterebilir.
- İş istasyonları arasında doğrudan iletişim.
- Powershell veya Windows Scripting Host gibi belirli programların çağrılması.
- Kayıt defteri anahtarlarında, program klasöründeki dosyalarda, hizmetlerde, görevlerde, eklentilerde "ilginç" sapmalar meydana geliyor mu?

Burada kısmen Windows Powershell ile çeşitli sorgular gerçekleştirilebilir (örneğin, tarayıcı eklentilerinin veya Outlook'taki kuralların listelenmesi).