**Incident Handling and Response Overview**

Table of Contents

[Task 1: Explain the differences between an Event and an Incident. 1](#_Toc147878825)

[Task 2: Explain the stages of incident handling contains 1](#_Toc147878826)

[Task 3: Explain the objective of each stage and what the main activities and aims to. 2](#_Toc147878827)

[Task 4: What are the prerequisites for a SOC in the preparation stage for an incident? 4](#_Toc147878828)

[Task 5: Explain the artifacts of an incident. What should it include? 4](#_Toc147878829)

[Task 6: What are the differences between containment and eradication? 5](#_Toc147878830)

[Task 7: Give an example of short-term containment and long-term containment. 5](#_Toc147878831)

[Task 8: Explain the Post-Incident Activity Stage, Why do we have to use this stage? 5](#_Toc147878832)

# **Task 1: Explain the differences between an Event and an Incident.**

Bir event, bir sistem veya ağda gözlemlenebilen herhangi bir oluşumdur. Bir kullanıcının bir dosya paylaşımına bağlanması, bir sunucunun web isteği alması, bir kullanıcının e-posta göndermesi ve bir güvenlik duvarının bir bağlantı girişimini engellemesi gibi durumları içerir. Olumsuz event’ler sistem çökmeleri, paket flood saldırıları, hassas verilere izinsiz erişim ve verileri yok eden zararlı yazılım çalışıtırılması gibi gibi olumsuz sonuçları olan olaylardır.

Incident ise bilgisayar güvenliği politikalarının, kabul edilebilir kullanım politikalarının veya standart güvenlik uygulamalarının ihlali veya bu ihlalin yaklaşan bir tehdidi olarak kabul edilebilir. Incident örneği olarak;

* Bir saldırganın, elinde bulunan bir botnet ile web sunucuna yüksek miktarda bağlantı isteği göndererek çökmesine neden olmasıi
* Kullanıcıları yanıltarak aslında zararlı bir yazılım içeren epostayı açmasını sağlayıp, harici bir sistem ile bağlantı kurmasının sağlanması,
* Bir saldırganın organizasyona ait hassas verileri elde ederek fidye talebinde bulunması gibi olaylar incident olarak sayılabilir.

Incident’leri eventlerden ayırmak son derece önemlidir.

* Incident bir sistemin gizliliğini, bütünlüğünü ve kullanılabilirliğini kasıtlı olarak veya kazara tehdit eden veya olumsuz etkileyen siber faaliyetlerdir ve bunlara uygun kanallar aracılığı ile alarm verilir ve bildirilir.
* Event ise normal davranış veya ortamda meydana gelen değişikliklerdir.

# **Task 2: Explain the stages of incident handling contains**

Olay müdahalesi genel olarak siber güvenlik olaylarına etkili bir şekilde tepki vermek, hafifletmek ve kurtarmak için bir dizi aşamayı içerir. Bu aşamalar, belirli bir olay yanıtı çerçevesinde veya modeline bağlı olarak değişiklik göstermektedir.

Olay müdahalesine ilişkin aşamalar NIST tarafından yayınlanan NIST SP 800-61 Computer Security Incident Handling Guide (<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> ) içeriğinde aşağıdaki şekilde tanımlanmıştır.

1. Hazırlık (Preparation)
2. Tanımlama ve Analiz (Detection and Analysis)
3. Kontrol, Yoketme ve Kurtarma (Containment, Eradication & Recovery)
4. Olay Sonrası Aktiviteler (Post-Incident Activity)

A diagram of a life cycle

Description automatically generated

Öte yandan SANS’ın yayını olan SANS Incident Handler’s Handbook ‘ta (<https://sansorg.egnyte.com/dl/6Btqoa63at>) bir olayın çeşitli aşamalarında izlenecek önemli adımları vurgulayarak daha taktiksel ve prosedürel bir yaklaşım belirlemiştir. Belirtilen kaynakta olay müdahalesine yönelik aşamalar ise aşağıda verilmiştir.

1. Hazırlık (Preparation)
2. Tanımlama (Identification)
3. Kontrol (Containment)
4. Yok Etme (Eradiction)
5. Kurtarma (Recovery)
6. Edinilen Dersler (Lessons Learned)

# **Task 3: Explain the objective of each stage and what the main activities and aims to.**

Bir önceki göreve verilen cevaplardan yola çıkarak SANS’ın Olay müdahale süreçlerinin amaçları ve yapılacak faaliyetler aşağıda çıkarılmıştır.

Hazırlık Aşaması:

-Amaç : Etkili olay yanıtı için temel oluşturmak.

-Faaliyetler:

\* Olay müdahale politikası ve planı oluşturulması.

\* Olay müdahale ekibi için roller ve sorumlulukların tanımlanması.

\* Eğitim ve farkındalık programlarının düzenlenmesi.

\* Olay tespiti ve yanıt için gerekli araçlarn ve teknolojilerin hazırlanması.

\* Organizasyon dışı kuruluşlarla iletişim kanalarının ve koordinasyonun kurulması.

Tanımlama Aşaması:

* Amaç: Güvenlik olayının gerçekleştiğini tanımlamak ve doğrulamak.
* Faaliyetler :

\* Anormal veya şüpheli faaliyetleri izlemek için izleme sistemlerinin kullanılması.

\* Logların ve diğer ver kaynaklarının analiz edilerek potansiyel incidentlerın tanımlanması.

\* Bir incident’ın neyi içerdiğini tanımlamak için kriterlerin belirlenmesi

Kontrol Aşaması:

* Amaç: Olayın yayılmasını engellemek veya daha fazla zarar vermesini önlemek.
* Faaliyetler:

\* Etkilenen sistemlerin veya ağların izole edilmesi.

\* Ele geçirilmiş veya tehlikedeki kullanıcı hesabı veya servislerin devre dışı bırakılması.

\* Geçici çözümler ve yamaların uygulanması.

Yok Etme Aşaması:

* Amaç: Olayın köken nedenini belirlemek ve ortadan kaldırmak.
* Faaliyetler:

\* Saldırının kökeni ve yöntemlerini anlamak için kapsamlı soruşturma yapılması.

\* Olayın tekrarlanmasını önlemek için kalıcı düzeltmeler geliştirilmesi ve uygulanması.

\* Zararlı yazılımların veya izinsiz erişim noktalarının kaldırılması.

Kurtarma Aşaması:

* Amaç: Etkilenen sistemleri normal işlemlere geri döndürmek.
* Faaliyetler:

\* Uygulamanan düzeltmelerin etkinliğinin doğrulanması.

\* Yedeklerden veri ve yapılandırmaların geri yüklenmesi.

\* Sistemlerin herhangi bir kalıntı tehlikesi açısından izlenmesi.

Edinilen Dersler Aşaması:

* Amaç: Olay yanıtı sürecini analiz ederek gelecekteki yanıtları iyileştirmek.
* Faaliyetler:

\* Olay sonrası bir değerlendirme yaparak güçlü ve zayıf yönlerin belirlenmesi.

\* Öğrenilen derslerek dayanarak olay müdahale süreçlerinin güncellenmesi.

\* Olay müdahale ekibi ve genel olarak organizasyon ile bilgi ve deneyim paylaşımı.

NIST’in olay müdahale süreçlerinin amaçları ve icra ediecek faaliyetleri aşağıda çıkarılmıştır.

Hazırlık Aşaması:

* Amaç: Organizasyonun güvenlik olaylarına etkili bir şekilde yanıt verme ve kurtarma için hazırlıklı olmasını sağlamak. Bir olay müdahale yeteneği oluşturmak ve sürdürmek.
* Faaliyetler:

\* Olay müdahale politikası ve planını geliştirme ve uygulama.

\* Olay müdahale ekibi için farkındalık ve eğitim programları düzenleme.

\* Olay müdahale ekibini kurma ve rolleri ile sorumlulukları tanımlama.

\* Olay müdahale yeteneği oluşturma ve uygulama.

Tespit ve Analiz Aşaması:

* Amaç: Incidentleri hızlı bir şekilde tanımlamak ve etkili yanıt ve kurtarma sağlamak. Olayları zamanında tespit etmek ve etkilerini anlamak.
* Faaliyetler:

\* İzleme ve tespit sistemlerini uygulama.

\* Olayları analiz ederek kapsam ve etkilerini belirleme.

\* Adli verileri toplama ve analiz etme.

\* Bilgi paylaşımı ve harici kuruluşlarla iş birliği yapma.

Kontrol, Yok Etme ve Kurtarma Aşaması:

* Amaç: Zararı en aza indirmek, işlemleri geri yüklemek ve olayın tekrarını önlemek. Olayın etkilerini sınırlamak, kök nedeni ortadan kaldırmak ve normal işlemleri geri yüklemek.
* Faaliyetler:

\* Olayı yayılmasını önlemek için kontrol etme.

\* Olayın kök nedenini ortadan kaldırma.

\* Etkilenen sistemleri ve verileri kurtarma.

\* Gelecekteki olayları önlemek için düzeltici önlemleri uygulama.

Olay Sonrası Aktiviteler Aşaması:

* Amaç: Gerçekleşen olaylardan elde edilen bilgilerle olay müdahale süreçlerini, yeteneklerini ve genel güvenlik durumunu iyileştirmek. Olayları belgelemek ve sürekli iyileştirmek için öğrenmek.
* Faaliyetler:

\* Olay ayrıntıları, yanıt eylemleri ve öğrenilen dersleri belgeleme.

\* Olay sonrası bir değerlendirme ve analiz yapma.

\* Olay müdahale planlarını ve yeteneklerini öğrenilen derslere dayanarak güncelleme.

# **Task 4: What are the prerequisites for a SOC in the preparation stage for an incident?**

# **Task 5: Explain the artifacts of an incident. What should it include?**

Organizasyonların olay müdahale süreçleri boyunca göz önünde bulundurmaları gereken çeşitli artifactler bulunmaktadır. Bu artifactler güvenlik olaylarını anlama, yanıtlama ve öğrenme açısından kritik olan bilgi ve belgelerdir. Temel olarak olması gereken artifactler ve içerikleri aşağıda sunulmuştur.

1. Olay Kaydı:

- Olayla ilgili temek bilgiler, olay kimliği, tarih,saat ve ilk değerlendirme

- Olayı yöneten ve ilgili tarafların iletişim bilgileri

- Olayın kısa açıklaması ve etkisi

2. Muhafaza Zinciri:

- Delilin muhafaza ve işlenmesine dair belgeler

- Delili elinde bulunduran kişilerin adları

- Delil transferlerinin zaman damgaları ve detayları

3. Delil Kayıtları:

- Toplanan tüm delillerle ilgili detaylı kayıtlar

- Her bir delilin kaynağı yeri ve bağlamı hakkında bilgiler

- Muhafaza ve işleme ayrıntıları

4. Tanık Beyanları:

- Olayı gözlemleyen kişilerin beyanları

- Tanıkların ne gözlemlediği veya yaşadığına dair açıklamalar

- Tanıkların iletişim bilgileri

5. Adli Veri:

- Etkilenen sistemler üzerinde yapılan adli analiz sonuçları.

- Zararlı yazılımlar, izinsiz erişim izinleri veya diğer anormalliklere dair bilgiler.

- Detaylı adli raporlar.

6. Uyarılar ve Bildirimler:

- Olay sırasında tetiklenen uyarıların kopyaları

- Olay müdahel ekipleri, yönetim veya diğer paydaşlara gönderilen bildirimler

- Uyarıların meydana geldiği zaman damgaları veya detayları

7. İletişim Kayıtları:

- Olay sırasında gerçekleşen iletişim kayıtları.

- Olayla ilgili e-posta alışverişleri, sohbet kayıtları veya diğer iletişim biçimleri.

- Alınan kararlar ve yapılan eylemler hakkında bilgiler.

8. Olay Analizi Raporları:

- Olayın, kök nedenlerin ve etkilerin detaylı analizi.

- Olaydan öğrenilen dersler ve iyileştirmeler için öneriler.

- Organizasyonun bilgi tabanına katkıda bulunabilecek bilgiler.

9. Hukuki Belgeler:

- Olayın hukuki yönleriyle ilgili belgeler.

- Herhangi bir arama kararı, mahkeme kararı veya hukuki anlaşmalar.

- Olay sonrası bildirim yükümlülüklerine ilişkin belgeler.

10. Olay Sonrası İnceleme:

- Olay sonrası inceleme sürecine dair belgeler.

- İncelenen bulgular, güçlü yönler ve iyileştirme alanlarından elde edilen sonuçlar.

- İnceleme temelinde olay yanıt planlarının ve süreçlerinin güncellenmesi.

Belirtilen artifactler olay müdahale yaşam döngüsünde belirli bir amaca hizmet eder ve olayın ayrıntılı anlaşılmasına ve çözüm bulunması için katkıda bulunur.

# **Task 6: What are the differences between containment and eradication?**

# **Task 7: Give an example of short-term containment and long-term containment.**

# **Task 8: Explain the Post-Incident Activity Stage, Why do we have to use this stage?**