Raporlama

İçerikler

Genel Bakış

Bu belge, penetrasyon testi raporlaması için temel kriterleri tanımlamayı amaçlamaktadır. Kendi özelleştirilmiş ve markalı formatınızı kullanmak için çok teşvik edilirken, aşağıdakiler bir rapor içinde gerekli olan öğelerin yüksek düzeyde bir şekilde anlaşılmasını sağlamalıdır. Raporun okuyucuya değer sağlaması için bir yapı.

Rapor Yapısı

Rapor, çeşitli kitlelere yapılan testin amaçlarını, yöntemlerini ve sonuçlarını iletmek için iki (2) ana bölüme ayrılmıştır.

Yönetici Özeti

Bu bölüm, Bazenasyon Testinin özel hedeflerini ve test egzersizinin yüksek seviyeli bulgularını okuyucuya iletecektir. Amaçlanan izleyiciler, güvenlik programının gözetim ve stratejik vizyonundan sorumlu olanların yanı sıra, tanımlanan / doğrulanmış tehditlerden etkilenebilecek örgütün herhangi bir üyesi olacaktır. Yönetici özeti, aşağıdaki bölümlerin tümünü içermemektedir:

Arka plan:

Arka plan bölümü okuyucuya testin genel amacını açıklamalıdır. Risk, karşı önlemler ve test hedefleri ile ilgili olarak belirlenen şartlara ilişkin ayrıntılar, okuyucuyu genel test hedeflerine ve göreceli sonuçlara bağlamak için mevcut olmalıdır.

(Örnek: (MTÜM) Birleşik <Pentester> dahili / dış güvenlik açığı değerlendirmesi ve (lojik alan veya fiziksel konum) bulunan spesifik sistemlerin penetrasyon testi ile görevlendirildi. Bu sistemler (risk sıralaması) olarak tanımlanmıştır ve uygunsuz bir şekilde erişilirse (Mclient) maddi zarara neden olabilecek (veri sınıflandırma düzeyi) verileri içerir. (CLient'in) doğrudan ve dolaylı saldırıya karşı savunma yeteneğini test etmek amacıyla, <Pentester> kapsamlı bir ağ kırılganlık taraması, Güvenlik Açıcılık konformasyonu (<-in-sert saldırı türleri on->) zayıf hizmetlerin sömürülmesi, müşteri tarafı saldırıları, tarayıcı yan saldırıları (etc) Bu değerlendirmenin amacı, (İKLİT) iş-kritik bilgileri güvence altına almak için uygulanan güvenlik kontrollerinin etkinliğini doğrulamaktı. Bu rapor, CLIENT'in güvenlik duruşunu güçlendirmesine yardımcı olmak için değerlendirmeden elde edilen bulguları ve ilgili iyileştirme önerilerini temsil etmektedir.

- Test sırasında hedefler değiştirilirse, tüm değişikliklerin raporun bu bölümünde listelenmesi gerekir. Ek olarak, değişiklik mektubu raporun ekine dahil edilmeli ve bu bölümden bağlantılı olmalıdır.

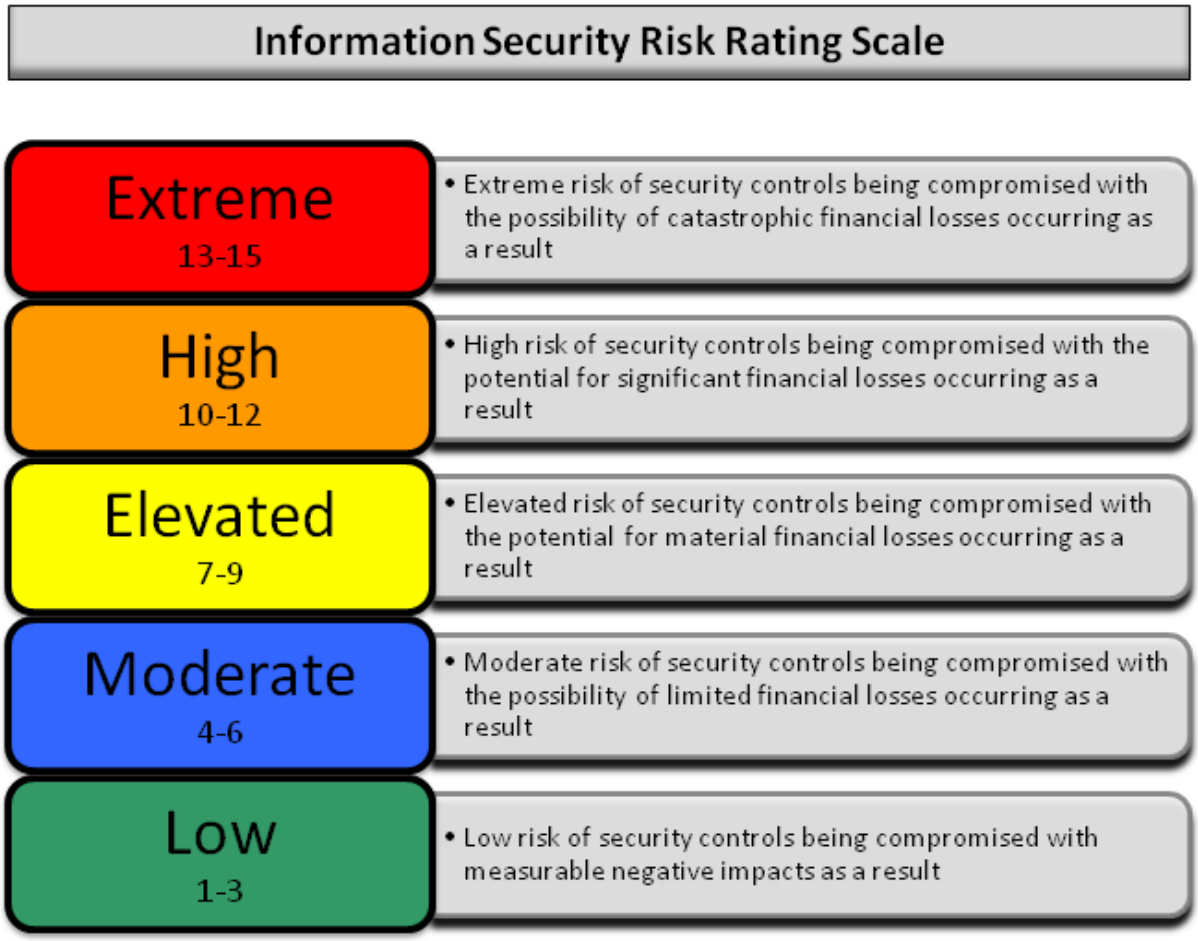
Genel Duruş:

Bu alan, testin genel etkinliğinin ve pentesters'ın ön katılım oturumlarında belirtilen hedeflere ulaşma yeteneğinin bir

anlatısı olacaktır. Sistemik'in kısa bir açıklaması (ex. Sistemik sorun = Etkili Yama Yönetimi Sürecinden Yoksun ve. Belirtisel = MS08-067'yi xyz kutusunda eksik buldum) test süreci boyunca tanımlanan sorunları ve hedef bilgilerine erişim sağlama ve işletmeye potansiyel bir etki belirleme yeteneği.

Risk Sıralaması / Profili:

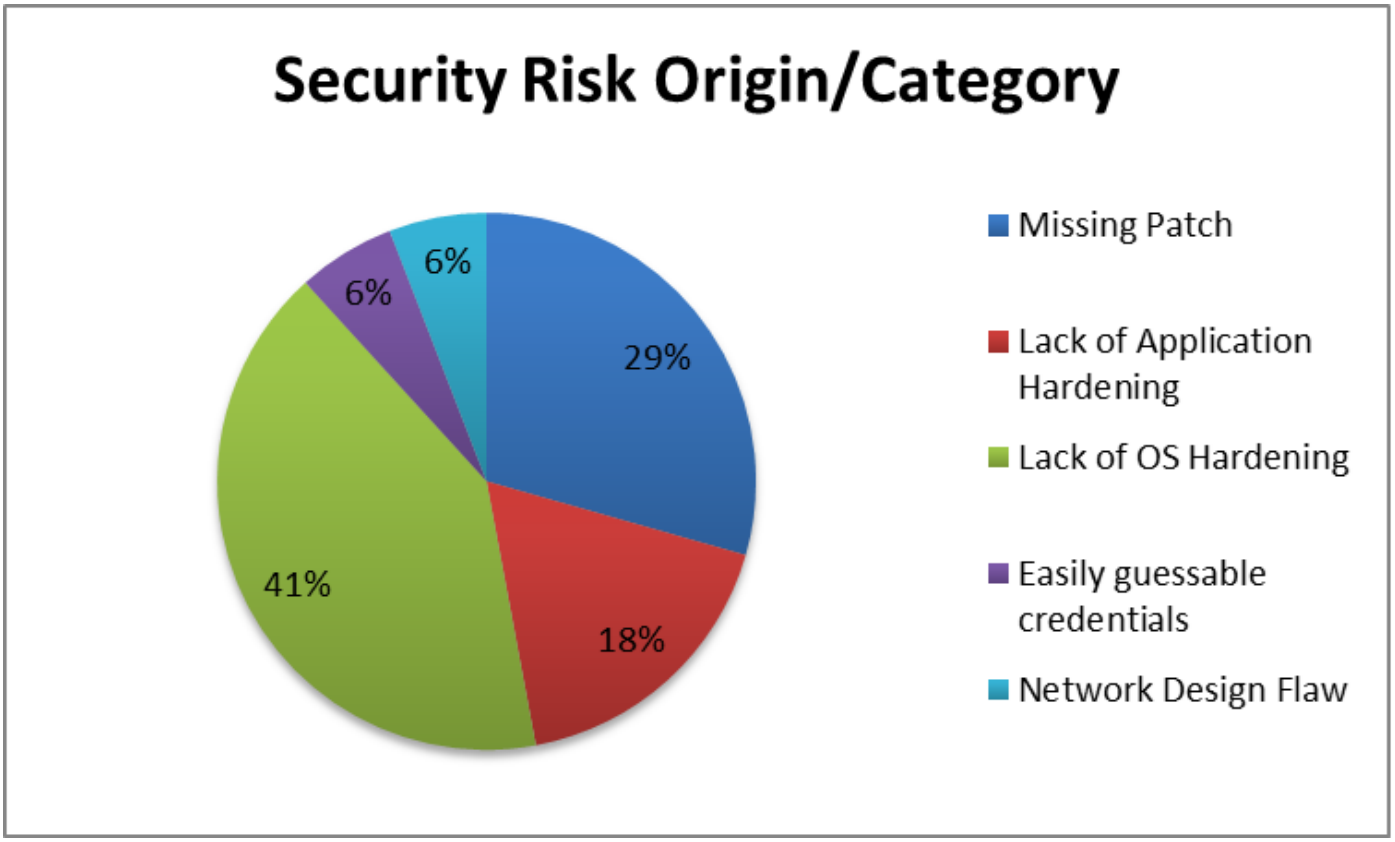
Genel risk sıralaması / profil / skor bu alanda tanımlanacak ve açıklanacaktır. Ön angajman bölümünde Pentester, skor mekanizmasını ve riskin izlenmesi / derecelendirmek için bireysel mekanizmayı tanımlayacaktır. FAIR, DREAD ve diğer özel sıralamalardan çeşitli yöntemler çevresel puanlar halinde birleştirilecek ve tanımlanacaktır.



(İKLİM) için "Genel Risk Puanı" şu anda Yedi (7). Bu derecelendirme, güvenlik kontrollerinin maddi finansal kayıp potansiyeli ile tehlikeye atılmış bir risk anlamına gelir. Danışman, bu risk puanını, yönlendirilmiş saldırının başarısıyla birlikte yüksek bir risk ve birkaç orta risk açığına dayanarak belirledi. Belirlenen en ciddi güvenlik açığı, bir dizi hassas belgeye erişime ve cihazdaki içeriği kontrol etme yeteneğine izin veren kurumsal halka dönük web sitesinde varsayılan şifrelerin varlığıydı. Bu güvenlik açığı, kullanıcı hesaplarının çalınmasına, hassas bilgilerin sızmasına veya tam sistem uzlaşmasına yol açabilir. Birkaç daha az ciddi güvenlik açığı, geçerli hesap kimlik bilgilerinin çalınmasına ve bilgi sızıntısına yol açabilir.

Genel Bulgular:

Genel bulgular, penetrasyon testi sırasında temel ve istatistiksel bir formatta bulunan sorunların bir özetini sağlayacaktır. Test edilen hedeflerin grafik temsilleri, test sonuçları, süreçler, saldırı senaryoları, başarı oranları ve ön katılım toplantısında tanımlanan diğer trend metrikler mevcut olmalıdır. Ayrıca, sorunların nedeni okunması kolay bir formatta sunulmalıdır. (ex. Sömürülen sorunların temel nedenini gösteren bir grafik)



Ön katılım egzersizi içinde tanımlanırsa, bu alan aynı zamanda karşı önlemlerin çevre içindeki etkinliğini gösteren metrikleri de içermelidir. (örneğin. x saldırıları koştuk ve IPS engellendi. Diğer karşı önlemler de benzer tasarım metriklerine ve etkinliğine sahip olmalıdır.)

Öneri Özeti:

Raporun öneri bölümü, okuyucuya belirlenen riskleri ve önerilen çözüm yolunu uygulamak için gereken genel çaba düzeyini çözmek için gereken görevleri yüksek düzeyde anlamalıdır. Bu bölüm, takip eden yol haritasının sırasına öncelik vermek için kullanılan ağırlık mekanizmalarını da tanımlayacaktır.

Stratejik Yol Haritası:

Yol haritaları, bulunan güvensiz maddelerin iyileştirilmesi için öncelikli bir plan içermelidir ve iş hedeflerine / potansiyel etki seviyesine karşı tartılmalıdır. Bu bölüm, PTES-Tehdit modelleme bölümünde oluşturulan tehdit matrisinin yanı sıra belirlenen hedeflere doğrudan eşlenmeli. Önceden tanımlanmış zaman / nesnel tabanlı hedeflere ayrılarak, bu bölüm çeşitli artışlarla takip etmek için bir eylem yolu oluşturacaktır. Örnek:

Completed at the time of this assessment
Tasks
Identify internal security point of contact • Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion. • Secure appropriate funding for initial program review and 3rd party assessment
Identify Current Security State of security • This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

One (1) to Three (3) Months
Tasks
Create Remediation Strategy • Leverage results found within the Penetration Test to create a full remediation strategy • This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.
Create Information Security Council/Task Force • To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team. • The council should consist of Management of each individual business unit • ....
Begin Security Project planning • Assign Executive owners of security for CLIENT • **...**
Prioritize Remediation Events • Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified. • Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk. • Start process with server patching to gain quick increases in environment security.
Patch Services • **Specific things to be fixed/how...** • **...**
Harden Servers • ... • ...

Three (3) to Twelve (12) Months
Tasks
Security Self Assessment Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a** : found at http://csrc.nist.gov/publications/PubsDrafts.html. Another approach would be to run the **Microsoft Security Assessment Tool** : found at http://www.microsoft.com/technet/security/tools/msat/default.mspx
Twelve (12) Months+
Tasks
Perform 3rd Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen). • Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks • Identify the root cause of compliance gaps • Identify strategy for using the output of the assessment to facilitate a security baseline Begin remediation planning/budgeting

Teknik Rapor

Bu bölüm, okuyucuya testin teknik ayrıntılarını ve angajman öncesi egzersiz içinde önemli başarı göstergeleri olarak kabul edilen tüm yönleri / bileşenleri iletir. Teknik rapor bölümü, testin kapsamını, bilgilerini, saldırı yolunu, etkisini ve iyileştirme önerilerini ayrıntılı olarak açıklayacaktır.

Giriş:

Teknik raporun giriş bölümünün ilk envanteri olması amaçlanmıştır:

- Hem Müşteri hem de Penetrasyon Test Ekibinden teste katılan personel
- İletişim bilgileri
- Teste dahil olan varlıklar
- Testin Amaçları
- Test Kapsamı
- Testin Mukaveyti
- Yaklaşım

- Tehdit / Sınıf Yapısı

Bu bölüm, testte yer alan özel kaynaklar ve testin genel teknik kapsamı için bir referans olmalıdır.

Bilgi toplama:

İstihbarat toplama ve bilgi değerlendirmesi iyi bir penetrasyon testinin temelleridir. Test cihazı çevre hakkında ne kadar bilgi sahibi olursa, testin sonuçları o kadar iyi olur. Bu bölümde, TIP'in İstihbarat toplama aşamasının uygulanması yoluyla mevcut kamu ve özel bilgilerin kapsamını göstermek için bir dizi öğe yazılmalıdır. En azından, belirlenen sonuçlar 4 temel kategoride sunulmalıdır:

Pasif Zeka:

İstihbarat, IP / Altyapı ile ilgili bilgiler için DNS, Google çukurlaştırma gibi dolaylı analizlerden toplandı. Bu bölüm, herhangi bir trafiği doğrudan varlıklara göndermeden MÜŞİSTÜR ortamındaki teknolojiyi profillemek için kullanılan tekniklere odaklanacaktır.

Aktif Zeka:

Bu bölüm, altyapı haritalama, liman taraması ve mimari değerlendirme ve diğer ayak baskı faaliyetleri gibi görevlerin yöntemlerini ve sonuçlarını gösterecektir. Bu bölüm, trafiğin mal varlığına gönderilmesiyle MÜŞİYON ortamındaki teknolojiyi profillemek için kullanılan tekniklere odaklanacak.

Kurumsal Zeka:

Kuruluşun yapısı, iş birimleri, pazar payı, dikey ve diğer kurumsal işlevler hakkındaki bilgiler hem iş sürecine hem de test edilen daha önce tespit edilen fiziksel varlıklara eşleştirilmelidir.

Personel Zekası:

İstihbarat toplama aşamasında bulunan ve kullanıcıları MÜŞİMENT teşkilatına haritalandıran tüm bilgiler. Bu bölüm, kamu / özel çalışan depoları, posta depoları, seks çizelgeleri ve çalışan / şirketin bağlantısına yol açan diğer öğeler gibi istihbarat toplamak için kullanılan teknikleri göstermelidir.

Güvenlik Açığı Değerlendirmesi:

Güvenlik açığı değerlendirmesi, bir TESTte bulunan POTANSIYEL güvenlik açıklarını ve her tehdidin tehdit sınıflandırmasını belirleme eylemidir. Bu bölümde, kırılganlığın kanıtlanmasının / sınıflandırılmasının yanı sıra kırılganlığı tanımlamak için kullanılan yöntemlerin bir tanımı mevcut olmalıdır. Buna ek olarak, bu bölüm şunları içermelidir:

- Güvenlik Açığı Sınıflandırma Seviyeleri
- Teknik Güvenlik Açıkları
  - OSI Katmanlı Vulns
  - Tarayıcı Bulundu
  - Manuel olarak tanımlandı
  - Genel Maruziyet
- Mantıksal Güvenlik Açıkları
  - NON OSI Vuln
  - Kolon türü
  - Nasıl / Nerede bulunur
  - Maruziyet
- Sonuçların Özeti

Sömürü / Güvenlik Açığı Doğrulama:

Sömürü veya Güvenlik Açığı onayı, hedef varlığa belirli bir erişim düzeyi elde etmek için önceki bölümlerde tanımlanan güvenlik açıklarını tetikleme eylemidir. Bu bölüm, tanımlanan güvenlik açığını ve aşağıdakileri doğrulamak için atılan tüm adımları ayrıntılı olarak gözden geçirmelidir:

- Sömürü Zaman Çizelgesi
- Sömürülme için seçilen hedefler
- Sömürü Faaliyetleri
  - Yönetilen Saldırı
    - Hedef ev sahipleri sömürülen
    - Hedef ev sahipleri istismar edilebiliyor
      - Bireysel Ev Sahibi Bilgileri
      - Yapılan saldırılar
      - Saldırılar Başarılı
      - Erişim seviyesi / Tırmandırma yolu
      - Düzeltme
        - Vuln bölüm referansına bağlantı
        - Ek Azaltma tekniği
        - Kontrol önerisini telafi etmek
- Dolaylı Saldırı
  - Phishing
    - Saldırının zaman çizelgesi/ayrıntıları
    - Hedefler belirlendi
    - Başarı/yaylık oranı
    - Verilen erişim seviyesi
  - Müşteri tarafı
    - Saldırının zaman çizelgesi/ayrıntıları
    - Hedefler belirlendi
    - Başarı/yaylık oranı
    - Verilen erişim seviyesi
  - Tarayıcı tarafı
    - Saldırının zaman çizelgesi/ayrıntıları
    - Hedefler belirlendi
    - Başarı/yaylık oranı
    - Verilen erişim seviyesi

Post Exploitation:

Tüm testlerdeki en kritik öğelerden biri, test edilen MÜŞİFT içi üzerindeki DÜZELsel etki ile bağlantıdır. Yukarıdaki bölümler, kırılganlığın teknik doğasını ve kusurdan başarılı bir şekilde yararlanma yeteneğini aktarırken, Post Exploitation bölümü sömürü yeteneğini gerçek riske bağlamalıdır. Bu alanda aşağıdaki öğeler ekran görüntülerinin kullanımı, zengin içerik alımı ve gerçek dünya ayrıcalıklı kullanıcı erişimi örnekleri ile kanıtlanmalıdır:

- Ayrıcalık Tırmanma yolu
  - kullanılan teknik
- Müşteri tarafından tanımlanan Kritik Bilgilerin Satın Alınması
- Bilginin değeri

- Temel iş sistemlerine erişim
- Uyumluluk korumalı veri setlerine erişim
- Ek Bilgiler / Sistemlere Erişildi
- Kalıcılık yeteneği
- Sürkilik yeteneği
- Karşı tedbir etkinliği

  Bu bölüm, sistemlerde kapsamda bulunan karşı önlemlerin etkinliğini kapsamalıdır. Hem aktif (proaktif) hem de pasif (reaktif) karşı önlemlerle ilgili bölümlerin yanı sıra test aşamasında tetiklenen herhangi bir olay müdahalesi etkinliği hakkında ayrıntılı bilgi içermelidir. Değerlendirme faaliyetlerine direnmede etkili olan karşı önlemlerin bir listesi, CLIENT'in gelecekteki izinsiz giriş girişimlerini ele almak için algılama sistemlerini ve süreçlerini daha iyi ayarlamasına yardımcı olacaktır.

  - Algılama Kabiliyeti
    - FW / WAF/IDS/IPS
    - İnsan
    - DLP
    - Log
  - Yanıt ve etkinlik

Risk/maruz:

İşletmeye doğrudan etki, güvenlik açığı, sömürü ve sonrası sömürü bölümlerinde mevcut olan kanıtlarla nitelendirildiğinde, risk miktarı yapılabilir. Bu bölümde yukarıdaki sonuçlar risk değerleri, bilgi kritikliği, kurumsal değerleme ve ön katılım bölümünden türetilmiş iş etkisi ile birleştirilir. Bu, MÜŞTERİ'ye test boyunca bulunan güvenlik açıklarını tanımlama, görselleştirme ve para kazanma ve CLIENTS iş hedeflerine karşı çözümlerini etkili bir şekilde ağırlaştırma olanağı verecektir. Bu bölüm aşağıdaki alt bölümlerde iş riskini kapsayacaktır:

- Olay sıklığını değerlendirin
  - olası olay sıklığı
  - Teclay tehdidi kabiliyeti (3'ten - tehdit modellemesi)
  - Tahmin kontrol gücü (6)
  - Bileşik kırılganlık (5)
  - Gerekli beceri seviyesi
  - Erişim seviyesi gerekli
- Olay başına tahmin kaybı büyüklüğü
  - Birincil kayıp
  - İkincil kayıp
  - Risk kökü neden analizini tanımlamak
    - Kök Neden asla bir yama değildir
    - Başarısız Süreçleri Belirleyin
- Türetme Riski
  - Tehdit
  - Savunmasızlık
  - Kaplama

Sonuç:

Teste genel bakış. Bu bölümün genel testin yankılarının yanı sıra CLIENT güvenlik duruşunun büyümesini desteklediği öne sürülmektedir. Güvenlik programında ilerlemeyi ve gelecekte bir test / güvenlik faaliyeti rejimine

olanak sağlamak için destek ve rehberlikle olumlu bir notla sona ermelidir.
