

YAZILIM VE HAZIRLIK

Olay Müdahale Hazırlığı

Bir güvenlik olayı yaşandığında ne yapılacağını, kimin sorumlu olduğunu ve kiminle nasıl iletişim kurulacağını önceden planlamanıza, etkiyi en aza indirmenize destek oluyoruz.



6

kapsam alanı

5

adımlı yöntem

6

teslim edilen çıktı

// NEDEN ÖNEMLİ?

Neden önemli?

Olay anında karar vermek için en kötü zamandır.



Hazır bir plan, net roller ve denenmiş senaryolar; tespitten toparlanmaya kadar geçen süreyi ve olayın maliyetini önemli ölçüde azaltır.

// KİMLER İÇİN?

Bu hizmet kimler için uygun?



Daha önce yazılı müdahale planı olmayan kuruluşlar



SOC/SIEM kuran veya kurmayı planlayan ekipler



ISO 27001 ve ISO 22301 çalışması yapanlar



Üst yönetimiyle olay senaryolarını denemek isteyenler

// KAPSAM

Neleri kapsıyor?



Olay müdahale planı

Rolleri, yetkileri, iletişim zincirini ve karar noktalarını tanımlarız.



Sınıflandırma ve eskalasyon

Olayların önem derecesini ve kime ne zaman bildirileceğini belirleriz.



Senaryo bazlı oyun kitapları

Fidye yazılımı, hesap ele geçirme ve veri sızıntısı gibi senaryolar için adım adım rehberler hazırlarız.



Masa başı tatbikatlar

Yönetim ve teknik ekiplerle gerçekçi senaryo tatbikatları yaparız.



Kanıt koruma ve iletişim

Kanıtların korunmasını, iç ve dış iletişimi ve KVKK ihlal bildirimini planlarız.



Olay sonrası inceleme

Olay sonrası değerlendirme ve iyileştirme sürecini kurgularız.

Saldırgan gibi düşünür, savunmacı gibi inşa ederiz.

// ÇALIŞMA YÖNTEMİ

Nasıl ilerliyoruz?

1

Mevcut durum ve riskler

Mevcut planlarınızı, ekibinizi ve en olası senaryoları değerlendiririz.

2

Plan ve rollerin tanımlanması

Müdahale planını, sorumlulukları ve iletişim akışını yazarız.

3

Oyun kitaplarının hazırlanması

Öncelikli senaryolar için uygulanabilir adımlar geliştiririz.

4

Tatbikat

Planı masa başı tatbikatlarla sınar, eksikleri tespit ederiz.

5

İyileştirme

Bulgulara göre planları günceller, düzenli gözden geçirme takvimi oluştururuz.

// ÇIKTILAR

Neler teslim ediyoruz?

- ✓ Olay müdahale planı ve prosedürleri
- ✓ Sınıflandırma ve eskalasyon matrisi
- ✓ Tatbikat raporu ve iyileştirme önerileri

- ✓ Rol ve iletişim matrisi
- ✓ Senaryo bazlı oyun kitapları
- ✓ Olay sonrası inceleme şablonu

// GÖRSEL ANLATIM

Konuya özel görseller

Olay müdahalesinde roller ve aşamalar

Kim, hangi aşamada, ne yapar? Hazırlık aşamasında netleştirilen bu akış kriz anında zaman kazandırır.

**Roller önceden belli**

Kriz anında yetki ve görev tartışması zaman kaybettirir.

Yalnızca teknik değil

Hukuk, iletişim ve yönetim de müdahalenin parçasıdır.

Sonrası da önemli

Kök neden analizi ve dersler bir sonraki olayı önler.

Hazırlık aşamasının çıktıları

Olay olmadan önce hazırlanan bu parçalar müdahale süresini belirler.

**Plan ve playbook**

Yaygın senaryolar için adım adım hazır prosedürler.

Delil korunur

Log ve delil toplama hem analiz hem hukuki süreç için gereklidir.

Tatbikatla sınanır

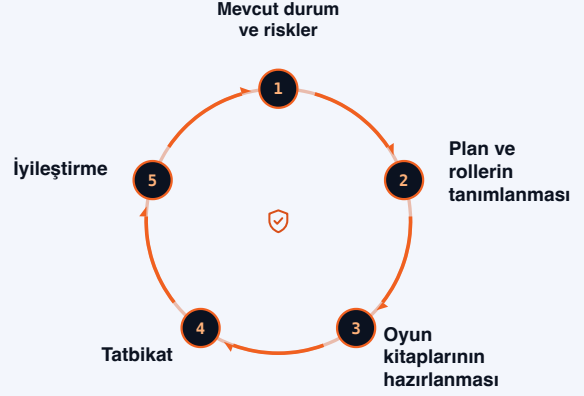
Masabaşı tatbikat plandaki boşlukları olay yaşanmadan gösterir.

// GÖRSEL ÖZET

Hizmete genel bakış

KAPSAM HARİTASI

UYGULAMA DÖNGÜMÜZ



// TEK ÇATI ALTINDA

Diğer hizmetlerimiz

- | | | |
|--------------------------------------|------------------------------------|--------------------------------------|
| ISO 27001 Danışmanlığı | ISO 22301 Danışmanlığı | ISO 14298 Danışmanlığı |
| KVKK Uyum Danışmanlığı | Siber Güvenlik Danışmanlığı | Risk Yönetimi Danışmanlığı |
| Sızma Testi | Düzenli Zafiyet Tarama ve Yönetimi | DoS, DDoS Testleri ve Koruma Hizmeti |
| SOC / SIEM Kurulumu | Endpoint Security İzleme Hizmeti | Güvenli Yazılım Geliştirme |
| Bilgi Güvenliği Farkındalık Programı | | |

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com

Hizmet sayfası ve bilgi formu
için QR kodu okutun