Siber Güvenlik Ekosisteminde Kariyer Yolları

Siber güvenlik alanında hala ne iş yapacağına karar vermedin mi? Gel beraber neler yapabileceğimize bakalım. Öncelikle siber güvenlik nedir? Ama önce bu konu hakkında biraz geçmişe gidelim neler biliyoruz biraz inceleyelim. İnsanlar neden siber güvenliğe ihtiyaç duymuş bir düşünelim. Çünkü nasıl ki bir varlığın zayıf noktaları var korunmaya ihtiyacı var bilişim de tamamen öyle. Seneler öncesine de bakarsak ilk siber saldırı 1834'te Fransa'da gerçekleşti. İki hırsız, Fransız Telgraf Sistemi'ni sömürerek finans piyasası bilgilerini çaldı. Kaç senesinde olursak olalım her zaman bir şekilde ihtiyaç duyuluyor. Bu sebeple Siber güvenlik bilişim sektörünün olmazsa olmaz bir bileşenidir. Siber güvenlik cihazların, sistemlerin, bilgisayarların, ağların ve verilerin kötü amaçlı saldırılardan korumak için oluşan bir alandır. Ve bu alanda da bir çok bölüme ayrılıdır. İlk olarak güvenlik analistliğinden başlayalım.

GÜVENLİK ANALİSTİ

Bir siber güvenlik analisti, şirketin donanımını, yazılımını ve ağlarını siber suçlulardan korur. Analistin birincil rolü, şirketin BT altyapısını ayrıntılı olarak anlamak, onu her zaman izlemek ve potansiyel olarak ağı ihlal edebilecek tehditleri değerlendirmektir. BT yi bilmeyenler için bir kuruluşun uygulamaları oluşturmak ve çalıştırmak için ihtiyacı olan şeylere denir. Kısaca özetlersek şirketin bilişim güvenliği onlardan sorumludur. Anlık olayları mevcut tehditleri incelerler.

GÜVENLİK MÜHENDİSİ

Bu bölümümüz ise güvenlik mühendisi bu da analist gibidir fakat günlük değil her zaman olabilecek gelecekte oluşabilecek sorunlara odaklanır. Ve güvenliği kendisi inşa eder. Ne demek isteniyor burada? Yani bir saldırı olmaması için nasıl bir çözüm kurulması gerekiyor? Sorusuna cevap verir ve uygular.

OLAY MÜDAHALE

Olay müdahale ekibi aktif olayın içindeki bir ekiptir. Sonuçta hiçbir şey %100 güvenli değildir. Tamamen güvenli sandığımız şeylere de sızılabilir. Bu sebeple olay müdahale uzmanları saldırı gerçekleştikten sonra neler yapılır ne yapılması gerekiyor gibi sorulara cevap verir. Belli bir adım sırasına göre ilerlerler ardından sistemin değişmesi gerekip gerekmediğini belirtirler. Sonuç olarak bu kişiler kritik müdahalelerde bulunur ve aktif saldırılarda işin içine girerler. Diğerlerinden farkı ise önceden savunmak değil de aktif olan bir şey uzaklaştırmak için çalışırlar.

DİJİTAL ADLİ TIP UZMANI

Bir sonraki bölümümüz ise Dijital Adli Tıp Uzmanı az önce adım adım saldırıların içine girdik şimdi de saldırıdan sonra kim işin içine girer neler olur onu göreceğiz. Bu bölümdeki kişiler çoğunlukla saldırıların arkasındaki siber suçluları tespit etmek için çalışırlar. Mesela bir cinayet şüphelisinin cihazlarından gelen verileri analiz etmek için çalışabilirler. Sonuçta nerde bir suçlu varsa ufak da olsa bir tarafı bilişime her zaman bağlıdır. Bu işteki insanlar delil inceleme, veri toplama, analiz etme gibi işlemler yaparlar. Ardından bu olanları raporlayıp delil olarak mahkemelere sunabilirler. Hüküm vermek onların işi değildir sadece delil hazırlarlar.

KÖTÜ AMAÇLI YAZILIM ANALİSTİ

Ve sonraki bölümümüze geçelim. Kötü Amaçlı Yazılım Analistliğinde bir kötü amaçlı yazılım var ise örnek veriyorum virüsler, worm, Trojan gibi bir çok zararlı yazılımları öngörüp sistem için en iyisi ne ise tüm bilgilerini kullanıp engellemeye çalışırlar. Öncelikle sistemi analiz ederler ardından belgelerler sonrasında bir strateji oluşturarak yazılımı izlemeye alırlar. Herhangi bir problemde ya da problem oluşturabilecek bir olayda müdahale ederler. Bir ekip olarak çalışırlar.

PENETRASYON TEST UZMANLARI

Ve diğer bölümümüze bakalım. Penetrasyon test uzmanları, güvenlik açıklarını çeşitli araçlarla ve tekniklerle tespit eden kişilerdir. Bu araçlar arasında port tarama, güvenlik açığı taraması, parola kırma , sosyal mühendislik , sql enjeksiyonu , xss , csrf , ssrf gibi bilindik açıklar yer alır. Bu testlerin amacı gerçek korsanlar gibi düşünüp acaba bunu yaparsam sızabilir miyim sorusuna cevap aramaktır. Eğer cevap evet ise bunu bildirmektir. Görevleri arasında sistemi düzeltmek yoktur. Şöyle düşünelim kendi şirketimize bir siyah şapkalı saldırdı nerelerden girebilir bilmemiz gerekiyor. Gerçekten saldırmak yerine bu işi simüle edebilecek kişiler bulurlar bu kişilerde onlardır.

KIRMIZI TAKIM VE MAVİ TAKIM

Şimdi sonraki bölümümüze geçelim. Kırmızı takım ve mavi takım bu ikisini birlikte ele aldım. Çünkü birbirleriyle bağlantılı konular. İlk kırmızı takımı inceleyelim. Amaçları saldırı operasyonlarını ele almak ve kuruluşların saldırı halinde nasıl performans göstereceğini test etmektir. Pentesterdan farkı ise kırmızı takım sistemin genelinde direnci ölçer fakat pentesterlar belli bir sistemdeki açıkları ölçerler. Ve kırmızı takım bilindik değil de gerçek bir sızma simülasyonu gibi hareket ederler. Şimdi de mavi takıma geçelim kırmızı takımın tam aksine bir saldırı yapıldığında nasıl tedbirler alınması gerekir bunu araştırırlar. Yani kısaca kırmızı takım saldırı yapıyorken mavi takım savunmadan sorumludur. Peki siz hangi taraftasınız?

SERTİFİKA VE KARİYER GELİŞİMİ

Şimdi sizlerin de merak ettiği gibi bu bölümlerde nasıl bilgi sahibi olunur neler yapılması gerekir onu görelim. (https://pauljerimy.com/security-certification-roadmap) Attığım linkte hangi bölüm için hangi sertifika gerekli ilk olarak merakınız nereye yakın bulup o konu hakkında sertifika bazlı olsun kişisel gelişmelere başlanması gerekiyor. bu ulaştığım bilgileri sizde merak ediyorsanız en sonda tüm linkleri atacağım.

https://www-wgu-edu.translate.goog/career-guide/information-technology/cybersecurity-analyst-career.html?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc (Siber güvenlik analistliği)

https://www-sentinelone-com.translate.goog/cybersecurity-101/cloud-security/offensive-security/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc&_x_tr_hist=true (saldırı güvenliği)

https://www-wgu-edu.translate.goog/career-guide/information-technology/malware-analyst-career.html?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=wa (kötü amaçlı yazılım)

https://www-ibm-com.translate.goog/think/topics/digital-forensics?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc (dijital adli bilişim)

https://www-monroeu-edu.translate.goog/news/cybersecurity-history-hacking-data-breaches?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc (siber güvenlik tarihi)

https://www-proofpoint-com.translate.goog/us/threat-reference/incident-response?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc (olay müdahale uzmanı)