Careers in Cyber

Task 1 Introduction (Giriş)

Siber güvenlik kariyerleri giderek daha fazla talep görmekte ve yüksek maaşlar sunmaktadır. Güvenlik sektöründe saldırgan pentesting'den (makineleri hacklemek ve güvenlik açıklarını raporlamak) savunmacı güvenliğe (siber saldırılara karşı savunma yapmak ve bunları araştırmak) kadar birçok farklı iş vardır.

Neden siber alanda kariyer yapmalısınız?

Yüksek Ücret - güvenlik alanındaki işler yüksek başlangıç maaşlarına sahiptir

Heyecan verici - iş, yasal olarak sistemleri hacklemeyi veya siber saldırılara karşı savunmayı içerebilir

Talep görüyor olun - 3,5 milyondan fazla doldurulmamış siber pozisyon var

Bu oda, çeşitli siber güvenlik rolleri hakkında bilgi sağlayarak siber güvenliğe girmenize yardımcı olur; ayrıca siber becerilerinizi geliştirmeye başlamak için kullanabileceğiniz farklı öğrenme yollarına bağlantı verir.

Siber güvenlikteki farklı rolleri keşfetmeye başlayalım!

cevap gerekmemektedir.

Task 2 Security Analyst (Güvenlik Analisti)

Güvenlik analistleri, şirketi saldırılardan korumak için kuruluşlar genelinde güvenlik önlemleri oluşturmanın ayrılmaz bir parçasıdır. Analistler, mühendislerin önleyici tedbirler geliştirmesi için eyleme geçirilebilir verileri ve önerileri ortaya çıkarmak üzere şirket ağlarını araştırır ve değerlendirir. Bu iş rolü, güvenlik gereksinimlerini ve güvenlik ortamını anlamak için çeşitli paydaşlarla birlikte çalışmayı gerektirir.

Sorumluluklar

Şirket genelinde siber güvenliği analiz etmek için çeşitli paydaşlarla birlikte çalışmak

Ağların güvenliği hakkında sürekli raporlar derlemek, güvenlik sorunlarını ve buna karşılık alınan önlemleri belgelemek Yeni saldırı araçları ve eğilimleri üzerine araştırmaları ve veri güvenliğini korumak için ekipler arasında ihtiyaç duyulan önlemleri
içeren güvenlik planları geliştirin.

Task 3 Security Engineer (Güvenlik Mühendisi)

Siber saldırıları önlemeye yardımcı olmak için güvenlik kontrollerini, ağları ve sistemleri tasarlamak, izlemek ve sürdürmek

Güvenlik mühendisleri, genellikle güvenlik iş gücünün üyelerinden elde edilen tehdit ve güvenlik açığı verilerini kullanarak güvenlik çözümleri geliştirir ve uygular. Güvenlik mühendisleri, web uygulama saldırıları, ağ tehditleri ve gelişen trendler ve taktikler de dahil olmak üzere geniş bir yelpazedeki saldırıları atlatmak için çalışırlar. Nihai hedef, saldırı ve veri kaybı riskini azaltmak için güvenlik önlemlerini korumak ve benimsemektir.

Sorumluluklar

Yazılım genelinde güvenlik önlemlerinin test edilmesi ve taranması

Sistemleri güncellemek ve güvenlik açıklarını azaltmak için ağları ve raporları izleyin

Optimum güvenlik için gereken sistemleri belirleme ve uygulama

Task 4 Incident Responder (Olay Yanıtlayıcısı)

Saldırganların operasyonları devam ederken saldırıları belirler ve hafifletir

Olay müdahale uzmanları güvenlik ihlallerine verimli ve etkili bir şekilde yanıt verir. Sorumluluklar arasında, kuruluşların olaylar sırasında ve sonrasında yürürlüğe koymaları için planlar, politikalar ve protokoller oluşturmak yer alır. Bu genellikle, saldırılar ortaya çıkarken gerçek zamanlı olarak yapılması gereken

değerlendirmeler ve yanıtlarla oldukça baskı altında bir pozisyondur. Olay müdahale ölçümleri MTTD, MTTA ve MTTR'yi içerir - (saldırıları) tespit etme, tanıma ve kurtarma süresi. Amaç hızlı ve etkili bir yanıt elde etmek, finansal durumu korumak ve olumsuz ihlal sonuçlarından kaçınmaktır. Nihayetinde, olay müdahale ekipleri şirketin verilerini, itibarını ve finansal durumunu siber saldırılara karşı korur.

Sorumluluklar

Kapsamlı, eyleme geçirilebilir bir olay müdahale planının geliştirilmesi ve benimsenmesi

Güçlü en iyi güvenlik uygulamalarının sürdürülmesi ve olay müdahale önlemlerinin desteklenmesi

Olay sonrası raporlama ve gelecekteki saldırılara hazırlık, olaylardan çıkarılacak dersler ve uyarlamaların dikkate alınması

Task 5 Digital Forensics Examiner (Dijital Adli Tıp Denetçisi)

Olayları ve suçları araştırmak için dijital adli tıp kullanmaktan sorumludur

Dedektifçilik oynamayı seviyorsanız, bu mükemmel bir iş olabilir. Bir kolluk kuvvetinin parçası olarak çalışıyorsanız, suçları çözmeye yardımcı olmak için kanıt toplamaya ve analiz etmeye odaklanacaksınız: suçluyu suçlamak ve masumları temize çıkarmak. Öte yandan, eğer işiniz bir şirketin ağını savunmaksa, politika ihlalleri gibi olayları analiz etmek için adli tıp becerilerinizi kullanacaksınız.

Sorumluluklar

Yasal prosedürlere uyarak dijital kanıt toplama

Davayla ilgili cevapları bulmak için dijital kanıtları analiz etme

Bulgularınızı belgeleyin ve vaka hakkında rapor hazırlayın

Task 6 Malware Analyst (Kötü Amaçlı Yazılım Analisti)

Nasıl çalıştıkları ve ne yaptıkları hakkında daha fazla bilgi edinmek için tüm kötü amaçlı yazılım türlerini analiz eder

Bir kötü amaçlı yazılım analistinin işi, şüpheli programları analiz etmeyi, ne yaptıklarını keşfetmeyi ve bulguları hakkında raporlar yazmayı içerir. Temel görevleri derlenmiş programları makine dilinden, genellikle düşük seviyeli bir dilde, okunabilir koda dönüştürmek olduğu için kötü amaçlı yazılım analistine bazen tersine mühendis de denir. Bu iş, kötü amaçlı yazılım analistinin özellikle assembly dili ve C dili gibi düşük seviyeli dillerde güçlü bir programlama geçmişine sahip olmasını gerektirir. Nihai hedef, kötü amaçlı bir programın gerçekleştirdiği tüm faaliyetler hakkında bilgi edinmek, nasıl tespit edileceğini bulmak ve raporlamaktır.

Sorumluluklar

Tersine mühendislik gerektiren kötü amaçlı programların statik analizini gerçekleştirme Kontrollü bir ortamda faaliyetlerini gözlemleyerek kötü amaçlı yazılım örneklerinin dinamik analizini gerçekleştirmeTüm bulguları belgeleyin ve raporlayın

Task 7 Penetration Tester (Sızma Test Cihazı)

Teknoloji ürünlerinin güvenlik açıklarına karşı test edilmesinden sorumludur

Sızma testinin pentesting ve ethical hacking olarak adlandırıldığını görebilirsiniz. Bir sızma test uzmanının görevi, bir şirketteki sistemlerin ve yazılımların güvenliğini test etmektir - bu, sistemli hackleme yoluyla kusurları ve güvenlik açıklarını ortaya çıkarma girişimleriyle elde edilir. Sızma testi uzmanları her bir durumdaki riski değerlendirmek için bu açıklardan yararlanır. Şirket daha sonra bu bilgileri kullanarak gerçek bir siber saldırıyı önlemek için sorunları düzeltebilir.

Sorumluluklar

Bilgisayar sistemleri, ağlar ve web tabanlı uygulamalar üzerinde testler gerçekleştirme

Güvenlik değerlendirmeleri, denetimleri gerçekleştirin ve politikaları analiz edin

Saldırıların önlenmesi için eylemler önererek içgörüleri değerlendirin ve raporlayın

Task 8 Red Teamer (Red Teamer)

Düşman rolünü oynar, bir kuruluşa saldırır ve düşman perspektifinden geri bildirim sağlar

Kırmızı ekip çalışanları, daha hedefe yönelik bir iş rolü ile sızma test uzmanlarına benzerlik gösterir. Sızma test uzmanları, siber savunmayı iyi durumda tutmak için sistemlerdeki birçok güvenlik açığını ortaya çıkarmaya çalışırken, kırmızı ekip uzmanları şirketin tespit ve müdahale yeteneklerini test etmek için görevlendirilir. Bu iş rolü, siber suçluların eylemlerini taklit etmeyi, kötü niyetli saldırıları taklit etmeyi, erişimi korumayı ve tespit edilmekten kaçınmayı gerektirir. Kırmızı ekip değerlendirmeleri bir aya kadar sürebilir ve genellikle şirket dışından bir ekip tarafından gerçekleştirilir. Genellikle olgun güvenlik programlarına sahip kuruluşlar için en uygun olanlardır.

Sorumluluklar

İstismar edilebilir güvenlik açıklarını ortaya çıkarmak, erişimi sürdürmek ve tespit edilmekten kaçınmak için bir tehdit aktörünün rolünü taklit edin

Kuruluşların güvenlik kontrollerini, tehdit istihbaratını ve olay müdahale prosedürlerini değerlendirin

Şirketlerin gerçek dünyadaki örneklerden kaçınması için eyleme geçirilebilir verilerle içgörüleri değerlendirin ve raporlayın

Task 9 Quiz

Bu oda size siber güvenlik alanındaki farklı kariyerler hakkında genel bir bakış sağladı. Siber güvenlik alanında hayalinizdeki işi bulmak için çevrimiçi eğitimden yararlanabileceğinizi unutmayın. Hangi siber güvenlik rolünün size en uygun olduğunu öğrenmek için sağ taraftaki "Siteyi Görüntüle" düğmesine tıklayarak erişebileceğiniz eğlenceli testimizi deneyin.