Siber Güvenlik & SOC Mastery

Dijital Kaleleri Savunun

Siber güvenlik bir ürün değil, sürekli evrimleşen bir süreçtir. Vebende Akademi ile bu süreci yönetmeyi, tehdit avcılığından olay müdahalesine kadar uçtan uca uzmanlık kazanın. En iyi savunma, saldırganın bir sonraki adımını bilmektir.

Modern Tehditlere Karşı Mühendislik Yaklaşımı

Problem

Klasik firewall ve antivirüs çözümleri gelişmiş kalıcı tehditlere (APT) karşı yetersiz kalıyor. Geleneksel güvenlik duvarları, modern siber saldırıların sofistike yöntemleri karşısında etkisiz hale geliyor.

Çözüm

Veri odaklı, otomasyon destekli ve analitik tabanlı bir Güvenlik Operasyon Merkezi (SOC) disiplini ile gerçek zamanlı tehdit algılama ve müdahale.

SIEM Teknolojileri

Güvenlik bilgi ve olay yönetimi sistemleri ile log analizi

EDR Çözümleri

Uç nokta tespit ve yanıt teknolojileri ile aktif savunma

SOAR Platformları

Güvenlik orkestrasyon, otomasyon ve yanıt süreçleri

Görünmez Duvarlar Örmek: Network Security & Hardening

Traffic Analysis

Wireshark ve Tcpdump ile paket seviyesinde derin analiz ve anomali tespiti

Firewall & IPS

Yeni nesil güvenlik duvarlarının (NGFW) stratejik konumlandırılması ve konfigürasyonu

VPN & Zero Trust

"Asla güvenme, her zaman doğrula" prensibiyle erişim kontrolü ve kimlik doğrulama

Hands-on Laboratuvar

Şüpheli ağ trafiğinin tespiti, protokol analizi ve gerçek saldırı vektörlerinin firewall üzerinden bloklanması. SYN flood, DDoS ve port scanning saldırılarını anlık tespit edin.

Son Kale: EDR ve Host Hardening

EDR/XDR Teknolojileri

- Şüpheli süreçlerin (Process) gerçek zamanlı takibi
- Dosya hareketlerinin ve registry değişikliklerinin izlenmesi
- Behavioral analysis ile tehdit algılama

OS Hardening Prosedürleri

- Windows ve Linux sunucuların güvenlik sıkılaştırma ayarları
- Least privilege prensibi ile izin yönetimi
- Benchmark ve CIS kontrolleri

Anti-Forensics Savunması

Saldırganların izlerini silme tekniklerine karşı adli bilişim temelleri ve log koruma yöntemleri

Ransomware Tespiti

Fidye yazılımı saldırılarının erken tespiti, izolasyonu ve etkisiz hale getirilmesi

Güvenliğin Beyni: SIEM ve Log Yönetimi

01

Log Collection

Dağıtık sistemlerden tüm güvenlik olaylarının merkezi bir noktada toplanması

02

Correlation Engine

ELK Stack, Splunk veya Azure Sentinel ile logların anlamlandırılması ve ilişkilendirilmesi

03

Alert Generation

False-positive oranı minimize eden optimize kural yazımı ve filtreleme

04

Dashboarding

SOC analistleri için gerçek zamanlı tehdit haritaları ve görsel raporlama

Pratik Senaryo

Kaba kuvvet (Brute-Force) saldırısı için özel bir SIEM kuralı geliştirin. Fail2ban entegrasyonu ile otomatik IP bloklama, anomali tespiti ve risk skorlama mekanizmaları oluşturun.

Saldırgan Gibi Düşünmek: Red Teaming

Ofansif Güvenlik Perspektifi

Saldırganların yöntemlerini anlayarak daha etkili savunma stratejileri geliştirmek için ofansif güvenlik teknikleri.

Vulnerability Assessment

Nessus, OpenVAS ve diğer zafiyet tarama araçlarıyla sistematik açığ tespiti ve risk derecelendirme

Exploitation Teknikleri

Bilinen açıkların nasıl sömürüldüğünü öğrenerek savunma kurgusunu güçlendirmek

Social Engineering

İnsan faktörünü ve phishing saldırılarını simüle ederek farkındalık oluşturma

Lab Çalışması

Güvenli olmayan bir web uygulamasının (OWASP Top 10) zafiyet analizini yapın. SQL injection, XSS ve CSRF saldırılarını test edin ve düzeltme önerileri geliştirin.

Saldırı Anında Kriz Yönetimi

Incident Response ve Digital Forensics

Hazırlık

IR planı, takım rolleri ve iletişim protokolleri

Tespit

Log analizi ve tehdit doğrulama

Kontrol

Saldırının yayılmasını durdurma

Temizleme

Root cause analysis ve kalıcı çözüm

Memory Forensics

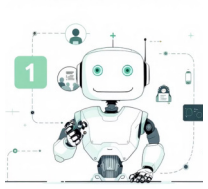
RAM üzerinden zararlı yazılım analizi, process injection tespiti ve malware davranış incelemesi

Root Cause Analysis

Saldırının kök nedenini belirleme, attack chain haritalama ve güvenlik açıklarının tarihsel analizi

Hands-on Simülasyon: Gerçek bir veri sızıntısı (Data Breach) senaryosu sonrası dijital kanıt toplama, volatile ve non-volatile memory analizi ve tam forensik raporlama

Geleceğin SOC Birimi: SOAR ve Python



Playbook Design

Tekrarlayan güvenlik olaylarının otomatik cevaplanması için orchestration playbook'ları oluşturun

API Integration

Farklı güvenlik araçlarını (SIEM, EDR, Firewall) REST API'ler ile birbiriyle entegre edin

Python for Security

Güvenlik görevlerini otomatize eden scriptler yazın ve güvenlik otomasyon ekosistemi inşa edin

Proje Senaryosu

Şüpheli bir IP'nin otomatik olarak tüm firewall'larda bloklanmasını sağlayan bir SOAR playbook'u geliştirin. Threat intelligence feed entegrasyonu, otomatik karar mekanizmaları ve insan onayı iş akışları implement edin.

Siber Güvenlikte Global Bir Oyuncu Olmak

Kariyer Tasarımı ve Sertifikasyon Rehberliği

CEH & Security+

Temel siber güvenlik sertifikasyonları için kapsamlı hazırlık

CySA+

SOC analistleri için log analizi ve tehdit tespiti uzmanlığı

OSCP

Penetration testing ve ethical hacking'in gold standard'ı

Soft Skills Geliştirme

- Teknik bulguları yönetime raporlama
- Stakeholder iletişim becerileri
- Incident response koordinasyonu

Global Fırsatlar

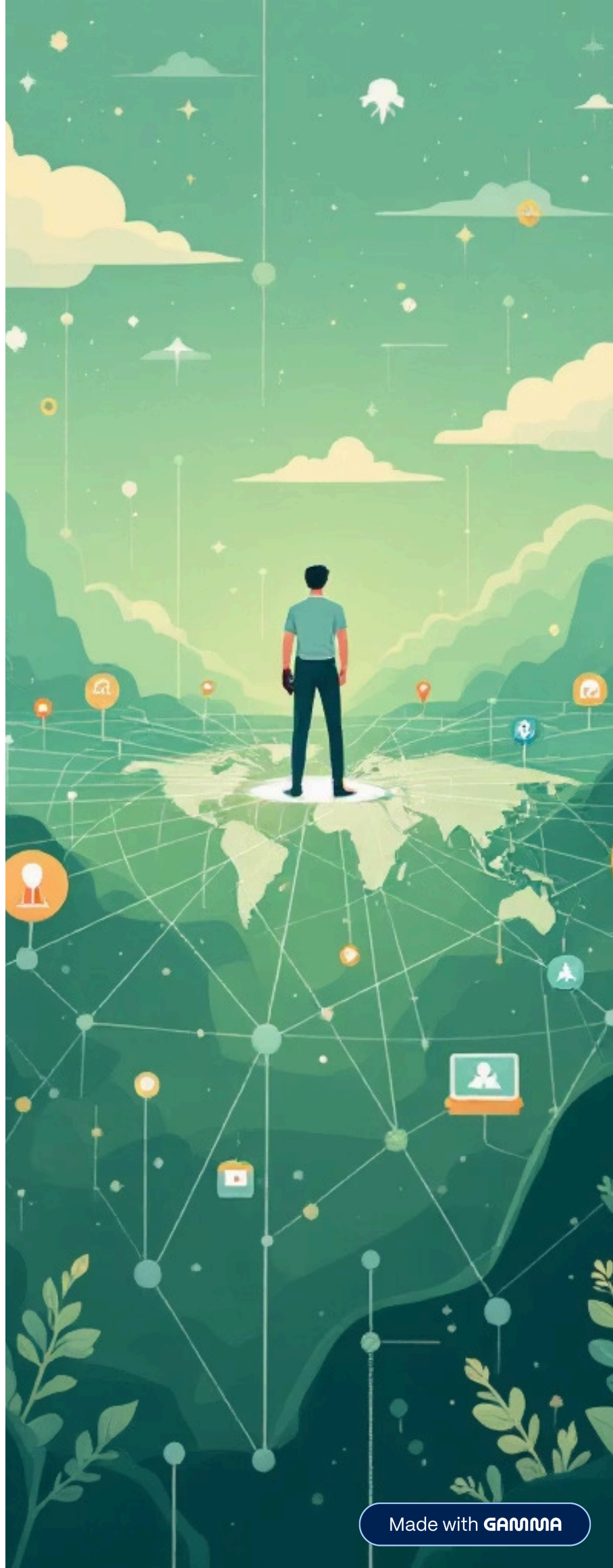
- Körfez, Avrupa ve ABD pazarları
- SOC Analisti pozisyonları
- Güvenlik Mühendisi rolleri

Mentorluk Programı

Teknik ve kariyer desteği, CV danışmanlığı ve mülakat hazırlıkları ile yolculuğunuzda yanınızdayız

Topluluk Ağı

Siber güvenlik profesyonelleri ile network kurun, knowledge sharing ve mentorship fırsatlarından yararlanın



Tam Kapsamlı Yetkinlik

Altyapıdan koda, operasyondan otomasyona kadar uçtan uca siber savunma becerileri

Pratik Odaklı Öğrenme

Sektör lideri araçlarla gerçek saldırı simülasyonları ve hands-on laboratuvar çalışmaları

Kariyer Destek Sistemi

Sertifikasyon hazırlık, mentorluk ve global iş fırsatları ile birlikte yolculuğunuzda yanınızdayız

> "Dijital Dünyayı Daha Güvenli Bir Yer Yapmak İçin Buradayız"

Hemen Başvur

Daha Fazla Bilgi