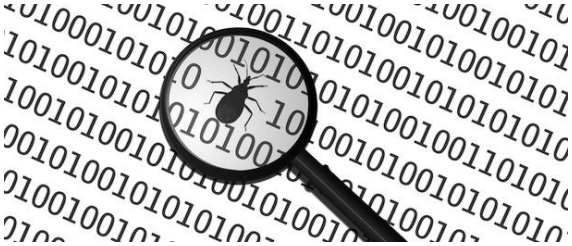
SIGNALSEC
BEYOND INTELLIGENCE



Zafiyet ve Exploit Araştırma Eğitimi

Eğitim Tanımı
Bu eğitim, güvenlik açıklarının nasıl bulunduğunu, günlük iş hayatında kullanılan exploitlerin arka planını, güvenlik endüstrisinin mutfağın merak eden bilgi güvenliği çalışanları içindir. Eğitim güvenlik açıkları bulma yöntemlerini kapsayan pratik bir eğitimdir. Eğitim boyunca kaynak kodu olmayan uygulamalarda güvenlik açığı (0day) arama yöntemleri ve bu açıklar için exploit geliştirme yöntemleri anlatılacaktır.

Eğitim esnasında gerçek senaryolar üzerinden gidilip, katılımcılar ile birlikte SCADA uygulamalarını da kapsayan çeşitli yazılımlarda zafiyetler tespit edilecektir. Tespit edilen zafiyetler için katılımcılar ile gizlilik anlaşması yapılacaktır.

Eğitimin Katkısı
Katılımcılar eğitimin sonunda, günlük iş hayatlarında kullandıkları otomatize araçların, exploitlerin ve exploitation araçlarının temelini, bu araçların nasıl geliştirildiğini ve nasıl zero-day açık bulacaklarını öğrenmiş olacaklardır.

Hedef Kitle
Bilgi Güvenliği Çalışanları, Network / Sistem Uzmanları, Yazılım Geliştiriciler, Kamu Güvenliği Çalışanları

Eğitim İçeriği

[+]Kavramsal Bilgiler
*Exploit nedir?
*Remote, Local, Client-Side ve Server-Side Exploitler
*Zeroday Exploitler
*Exploit Paylaşım Portalları

[+]Zafiyet ve Exploit Ekonomisi
*Marketler (Etik ve Underground)

[+]Programlama Dilleri
*C
*Perl
*Python

[+]Teknik Bilgiler

+İşletim Sistemi
*Process
*Memory
*Dosya formatı

+x86 mimarisi
*İşlemci
*Stack
*Registers
*Assembly

+ Alet Çantası
*Debuggers (windbg , ImmunityDebugger, gdb)
*Disassembler (IDA Pro)

+Vulnerability Research ve Exploiting
*Açık türleri
*Buffer Overflow (Stack, Heap)
*Signedness Errors
*Static Reverse Engineering
*Dynamic Reverse Engineering
*Fuzzing
*Server-side Açık Keşfetme
*Client-Side Açık Keşfetme
*Exploit Geliştirme

SIGNALSEC Bilgi Güvenlik Danışmanlık Yazılım ve Teknoloji Hiz. Tic. Ltd. Şti.
bir bilgi güvenliği ve AR-GE şirketidir. SignalSEC, Türkiye'de eksikliği hissedilen bilgi güvenliği dallarında araştırmalar yapmak ve hizmet vermek amacıyla kurulmuştur.

Temel hedefi zafiyet araştırmaları (vulnerability research) olan SignalSEC, müşterilerine efektif , ar-ge tabanlı ve ileri seviye bilgi güvenliği hizmetleri sunmaktadır. SignalSEC uluslararası bilgi güvenliği camiasında en aktif Türk bilişim şirketidir. SignalSEC araştırmacıları düzenli olarak uluslar arası bilgi güvenliği ve hacker konferanslarına konuşmacı olarak katılmaktadır ve desteklemektedir.

Ayrıca şirketin aralarında Adobe, IBM, Microsoft, Novell gibi firmaların bulunduğu birçok popüler yazılımda keşfettiği , yayınladığı onlarca kritik güvenlik bildirisi bulunmaktadır.

Telefon: +90 232 433 0DAY
Email: info@signalsec.com
Web: www.signalsec.com