

SST-Havelsan
Siber Savunma Teknolojileri

"Güven Yazıyoruz"

**SİBER GÜVENLİK
ÜRÜNLERİ VE HİZMETLERİ**

YETKİNLİKLERİMİZ

- Türk Standartları Enstitüsü tarafından yetkilendirilmiş “A Seviyesinde Sızma Testi Yapan, Eğitim ve Danışmanlık Veren” ilk firma
- CISSP, GREM, GPEN, GCIH, CEH, GAWN, GPEN, GMOB, GXPN, GCIA, ISO27001LAC, OWASP sertifikasyonlarına sahip personel
- Uluslararası Siber Güvenlik Tatbikatlarına katılım
- Sızma Testi, Zafiyet Denetimi ve Kaynak Kod Analizi hizmeti (150+ proje)
- Siber Güvenlik Teknik Uzmanlık Eğitimi (500+ kişi)
- Siber Güvenlik Farkındalık Eğitimi (5000+ kişi)
- Danışmanlık Hizmeti (50+ proje)
- Çözüm Ortağı (100+ firma)
- Siber Savunma Teknoloji Merkezi (SİSATEM)
- Uçtan Uca Siber Güvenlik Çözümleri



SST-Havelson
Siber Savunma Teknolojileri

SİBER GÜVENLİK ÜRÜNLERİMİZ

HAVELSAN
GÖZCÜ

HAVELSAN
KALKAN

HAVELSAN
BARIYER

iletee

HAVELSAN GÖZCÜ SİBER GÜVENLİK OLAY YÖNETİMİ VE ALARM SİSTEMİ

Siber Güvenlik Olay Yönetimi ve Alarm Sistemi kurumların bilişim altyapısı bileşenlerinin oluşturdukları kayıtların merkezi olarak toplanmasını, ilişkilendirilmesini, sorgulanmasını ve alarm üretilmesini sağlamaktadır.

Toplanan loglar normalize edilip ilişkilendirildikten sonra kullanıcı arayüzü üzerinden canlı akış ekranları ile sistem izleme, alarm üretimi, sorgulama ve raporlama özellikleri ile eksiksiz bir çözüm olarak sunulur.

Teknik Özellikler

- Web Tabanlı Yönetim
- Dağıtık mimari üzerinde yatay ve dikey ölçeklenebilirlik
- Çevrim dışı (offline) güncelleme kapasitesi
- Kolay ve hızlı eklenti (plug-in) desteği
- Analiz ve sorgulama yeteneği
- Kolay Arşivleme
- Rol Tabanlı ve Yapılandırılabilir Raporlama
- 5651 Sayılı Kanun Uyumluluğu

HAVELSAN KALKAN YÜK DENGELİYİCİ VE WEB UYGULAMA GÜVENLİK DUVARI

Yük Dengeleyici ve Web Uygulama Güvenlik Duvarı, web uygulamalarına yönelik saldırıları tespit edip engellemekte ve yüksek ağ trafikleri için yük dengeleme sağlamaktadır.

Teknik Özellikler

- Öğrenme ve imza tabanlı tehdit tespiti
- SSL sonlandırma
- OSI katman 4 ve 7 için yük dengeleme
- Servis durum ve sağlık kontrolleri
- HTTP, DNS, SMTP, IMAP, POP3 desteği
- HTTP önbellekleme
- Yüksek performans
- Bağlantı tekilleştirme, trafik sıkıştırma
- Yedeklilik / Hizmet sürekliliği
- Web tabanlı yönetim

HAVELSAN BARIYER VERİ SIZINTISI VE KAÇAĞI ÖNLEME SİSTEMİ

HAVELSAN BARIYER, kurum dışına izinsiz veri çıkışının önlenmesi, belirlenen engelleme kurallarına uygun olarak bilgi güvenliğinin sağlanması, verinin olması gereken yerde bulunduğu ve doğru kullanıcılar tarafından erişildiğinin denetlenmesi ve kontrol edilmesine imkan sağlayan PARDUS ile uyumlu yerli bir siber güvenlik ürünüdür. HAVELSAN BARIYER, büyük ve küçük Kamu Kurumlarının, diğer sivil kurum ve kuruluşların ve Askeri Kurumların özel güvenlik ihtiyaçlarını sağlayacak düzeyde yüksek performansa sahip olarak geliştirilmiştir.

Teknik Özellikler

- Uç nokta ve sunucuda keşif
- Gelişmiş Parmakizi
- İçerik bazlı koruma
- Harici medya kontrolü
- Web tabanlı yönetim
- Yatay ve dikey ölçeklenebilirlik



iletee GÜVENLİ HABERLEŞME PLATFORMU

HAVELSAN günümüzde önemi gitgide artan mobil platformlardaki iletişim ve veri saklama ihtiyaçlarının güvenli ve güvenilir bir şekilde karşılanması için iletee çözümünü geliştirmektedir. iletee güvenilirlik boyutunu ise kullanmış olduğu Güvenilir İşletim Ortamı teknolojisi aracılığı ile gerçekleştirmektedir.

Teknik Özellikler

- Güvenilir İşletim Ortamı teknolojisini (TEE) kullanarak işletim sistemi seviyesinden kaynaklanan zafiyetleri önleme
- Mevcut iletişim uygulamasına güvenilirlik katmanı ekleyerek güvenliği artırması
- Uçtan uca şifreleme ve kimlik doğrulama teknolojisi
- Güvenli / Güvenilir
 - Anlık mesajlaşma
 - Grup mesajlaşması
 - Sesli görüşme
 - Konum paylaşma
 - Ses, video, fotoğraf, kişi bilgileri paylaşımı
- Güvenilir Kullanıcı Arayüzü
- Dizin Sistemi (LDAP) Entegrasyonu

SİBER GÜVENLİK OPERASYON MERKEZİ SİSATEM'DE VERİLEN HİZMETLER



SİSATEM ÖNCESİ RİSK VE TEHDİTLER

- Takip edilemeyen güvenlik ihlalleri
- Sosyal mühendislik saldırıları
- Fidyeye yazılımları ve kötücül yazılımlarla erişilemez hale gelen sistemler



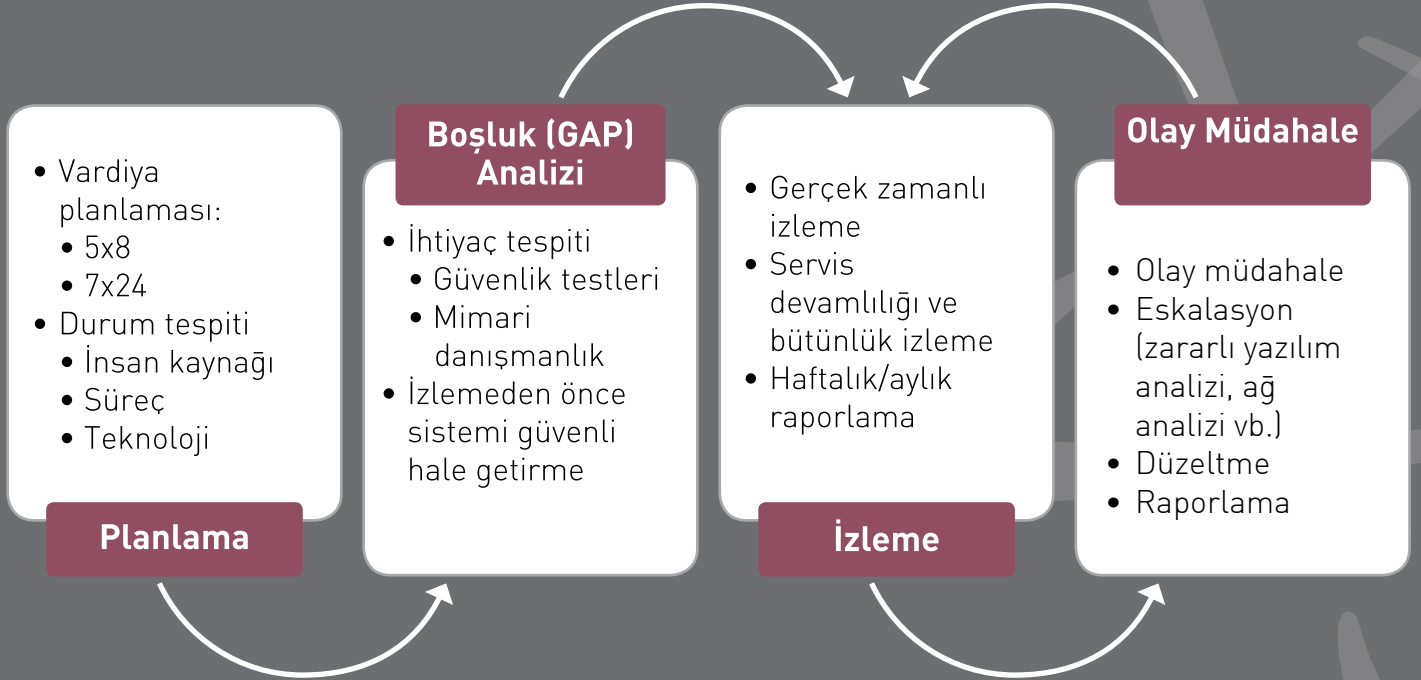
SİSATEM



SİSATEM SONRASI KAZANIMLAR

- Siber güvenlik olaylarının izlenmesi
- Kullanıcı ve cihaz bazlı olay raporları
- Proaktif koruma ve siber tehdit istihbarat raporlarını hazırlama
- Olay müdahale

SİSATEM HİZMETLERİ



SİSATEM HİZMETLERİ

Gerçek Zamanlı İzleme

- Siber Tehdit Tespiti
- Kritik varlıkların izlenmesi
- Kritik sistem olaylarının toplanarak analiz edilmesi
- SIEM korelasyon kurallarının yazılarak büyük veri analitiği algoritmaları ile anomali tespiti yapılması
- Siber tehditlerin raporlanması

Servis Devamlılığı ve Bütünlük İzleme

Olay Müdahale ve Raporlama

- Siber olay takip
- Haftalık/aylık kullanıcı ve cihaz bazlı olay raporlama

Zararlı Yazılım Analizi ve Ağ Analizi

- Statik analiz
- Dinamik analiz
- Repütasyon kontrolü

Düzeltilme ve Sıkılaştırma Önerileri

- Mimari yapılandırma önerileri
- Güvenlik cihazı konfigürasyon önerileri
- Politika, prosedür ve en iyi kullanım

ANALİZ VE TEST HİZMETLERİ



ZAFİYET DENETİMİ

Zafiyet denetimi hizmeti, zafiyetlerin taranmasını, raporlanmasını ve risk haritalarının oluşturulmasını sağlar.

Zafiyet Denetimi Hizmetleri, kurumlardaki bilişim altyapılarında oluşan güvenlik açıklıklarını, saldırganlar bu açıklardan faydalanmadan önce tespit ederek gerekli önlemlerin alınmasını sağlamaktadır.

Kapsam

- Kurum ağında tarama
- Varlık değişiklik tespiti
- Varlık zafiyeti tarama, raporlama
- Risk haritası
- Güvenlik açığı eylem planı

Hedef

Güvenlik zafiyetlerinin tespiti

ANALİZ VE TEST HİZMETLERİ

SIZMA TESTİ

Ülkemizde Türk Standartları Enstitüsü'nün verdiği ağ, sistem altyapısı, ürün (web) uygulamaları ve veri tabanlarını kapsayan Sızma Testi Hizmeti Veren Firma Yeterlilik Belgesi'ni en üst seviyede (A Tipi) alan ilk firma konumunda bulunmaktayız.

Zafiyetlerin tespiti, yerinde gerçekleştirilen çeşitli sızma testi araçlarıyla alanında uzman personeller ile sağlanmaktadır.

Sızma testi hizmetleri sayesinde güvenlik zafiyetleri ortaya çıkmakta ve bu zafiyetlerin giderilmesine yönelik öneriler sunulmaktadır.

Kapsam

- Sızma testleri
- Web uygulamalarına yönelik sızma testleri
- Kablosuz ağlara yönelik sızma testleri
- Zafiyet denetimi
- Kaynak kod analizi
- Dağıtık servis dışı bırakma (DDoS) testi
- Sosyal mühendislik testleri
- Doğrulama testi

Hedef

- Zayıflıkların tespiti
- Açıklıkların giderilmesine yönelik öneriler

UYGULAMA/KAYNAK KOD GÜVENLİK ANALİZİ

Yazılımların güvenlik zafiyetleri; siber güvenlik ekibimizdeki tecrübeli ve nitelikli teknik altyapıya sahip personel kaynağı ile analiz edilebilmektedir. Bunun için statik/dinamik kaynak kod analizi araçları, girdi-çıkı denetimi, imza tabanlı tarama ve davranışsal anomali tespiti vb. birçok yöntem ve teknik kullanılmaktadır.

Kapsam

- Yazılımların güvenlik zafiyetlerin analizi
- Statik/dinamik kaynak kod analizi
- Girdi-çıkı denetimi
- İmza tabanlı tarama ve davranışsal anomali tespiti
- Henüz geliştirme aşamasında olan uygulamalar için Güvenli Yazılım Geliştirme Yaşam Döngüsünün (S-SDLC) tesis edilmesini sağlayacak metotlar

Hedef

Uygulamalarca işlenen ve saklanan kurumsal hassas verinin korunması

BİLİŞİM SİSTEMLERİ GÜVENLİK DENETİMİ

Bir bilgi sisteminin varlıkları güvence altına alıp almadığı, veri bütünlüğünü sağlayıp sağlamadığı, kurumsal amaçlara etkin biçimde ulaşıp ulaşmadığı ve kaynakları verimli bir şekilde kullanıp kullanmadığını belirlemek amacıyla yapılan kanıt toplama ve değerlendirme sürecini kapsayan Bilişim Sistemleri Güvenlik Denetimi, HAVELSAN'ın teknik uzmanlığı ve bu alanda özgün olarak oluşturduğu kontrol listeleri ve denetim metodolojisi ile gerçekleştirilmektedir.

Kapsam

- Bilgi toplama ve değerlendirme
- Kontrol listeleri
- Özgün denetim metodolojisi
- Risk Derecelendirme ve Değerlendirme Raporları

Hedef

- Veri bütünlüğü
- Kaynak optimizasyonu
- Risk önlemlerinin planlanması

DANIŞMANLIK HİZMETLERİ

SİBER GÜVENLİK MİMARİSİ DANIŞMANLIĞI

Günümüzün karmaşık ve entegre çalışan bilgi teknolojileri ortamında güçlü bir siber savunma, ancak güçlü bir güvenlik mimarisi ile sağlanabilir. Siber Güvenlik Tasarım ve Uygulama ekibi kurumların bilgi teknolojileri altyapılarındaki güvenlik gereksinimlerini analiz ederek güvenlik ihtiyaçlarının karşılanmasına yönelik olarak;

- Mevcut Durum ve Boşluk Analizi
- Risk Analizi ve Değerlendirmesi
- Veri, Uygulama, Altyapı ve Süreç Gereksinimlerinin Belirlenmesi
- Siber Güvenlik Mimari Tasarımı ve Uygulaması
- Fark Analizi ve Raporlama

süreç adımlarının uygulandığı güvenlik mimarisi danışmanlığı ve entegrasyonu projelerini gerçekleştirebilmektedir.

Mimari Danışmanlık Kapsamı

- Keşif
- Boşluk Analizi
- Tasarım önerileri

Altyapının Kurulması Kapsamı

- Tasarlanan mimarinin uygulanması
- Eğitimler

DANIŐMANLIK HİZMETLERİ

BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ DANIŐMANLIĐI

HAVELSAN tarafından sunulan Bilgi GüvenliĐi Yönetim Sistemi (BGYS) danıŐmanlık hizmetleri, aŐaĐıda belirtilen ana proje safhalarını kapsamaktadır.

1. Ön Analiz ve Kapsam Belirleme
2. BGYS Planlama ve Kapsam Belirleme
3. BGYS Envanter Belirleme ve Sınıflandırma
4. BGYS Risk Analizi ve DeĐerlendirmesi
5. Sızma Testi ve Güvenlik Denetimleri
6. BGYS Dokümantasyon
7. BGYS EĐitim ve Uygulamaya GeçiŐ

HAVELSAN Bilgi GüvenliĐi Yönetim Sistemi kurulum ve iŐletim süreçlerinin her aŐamasında kurumlar tarafından ihtiyaç duyulan danıŐmanlık, eĐitim ve test hizmetlerini saĐlamakta, kurumlara BGYS alanında anahtar teslim çözümler sunmaktadır.

BGYS Danışmanlığı Kapsamı

- ISO 27001 sertifikasyon süreci için danışmanlığın sağlanması
- Departmanlar ve işleyişlerin derinlemesine incelenmesi
- İç tetkikler
- Eğitimler

BGYS Uygulanma Kapsamı

- ISO 27001 sertifikasyon süreci için teknik desteğin sağlanması
- Güvenlik strateji ve prosedürlerinin hazırlanması



EĞİTİMLERİMİZ

HAVELSAN, başta havacılık ve elektronik harp gibi alanlar olmak üzere sahip olduğu simülasyon ve kurumsal eğitim sunma tecrübesini, siber güvenlik alanında uzman personelinin birikimiyle birleştirerek bu alanda farkındalık eğitiminden detaylı teknik eğitimlere kadar birçok konu ve kapsamda eğitim verebilmektedir.



Siber Güvenlik Teknik Eğitimleri

- Güvenli Yazılım Geliştirme
- Kaynak Kod Analizi
- Ağ Analizi
- Kötücül Yazılım Analizi
- Mobil Güvenlik
- Tehdit Analiz
- SOME Kurulum
- Siber Olay Analiz ve Müdahale



Özelleştirilmiş Siber Güvenlik Eğitimleri



Kırmızı Takım / Mavi Takım Tatbikatı



Siber Güvenlik; Farkındalık Eğitimleri

Kariyer Yolu

Seviye

Temel

Eğitim Yolu	Eğitim Kodu	Eğitim İsmi
HVL-SEC	001	Siber Güvenlik Farkındalık Eğitimi
HVL-SEC	101	Siber Güvenlik Temelleri
HVL-SEC	110	Yöneticiler İçin Siber Güvenlik Semineri
HVL-SEC	201	Siber Saldırı ve Savunmaya Giriş
HVL-SEC	203	Temel Seviye Siber Olay Yönetimi ve Müdahale
HVL-SEC	205	Ağ Güvenliği Temelleri
HVL-SEC	207	İşletim Sistemleri Güvenlik Sıkılaştırma



EĞİTİMLERİMİZ

Kariyer Yolu



Eğitim Yolu	Eğitim Kodu	Eğitim ismi
HVL-SEC	301	Ağ Zafiyet Taraması ve Sızma Testi
HVL-SEC	302	Web Uygulama Zafiyet Taraması ve Sızma Testi
HVL-SEC	303	Kötücül Yazılım Analizi Temelleri
HVL-SEC	305	Adli Bilişim
HVL-SEC	308	Mobil Güvenlik
HVL-SSD	501	Güvenli Yazılım Geliştirme Temelleri
HVL-SIEM	121	HAVELSAN GÖZCÜ – SIEM Yönetimi
HVL-WAF	122	HAVELSAN KALKAN – Web Uygulama Güvenlik Duvarı Yönetimi



Kariyer Yolu

Seviye

Uzman

Eğitim Yolu	Eğitim Kodu	Eğitim ismi
HVL-SEC	309	Endüstriyel Kontrol Sistemleri Güvenliği
HVL-SEC	310	Bilişim Sistemleri Güvenlik Denetimi
HVL-SEC	401	İleri Seviye Ağ Sızma Testi ve Zafiyet Denetimi
HVL-SEC	402	İleri Seviye Web Uygulama Saldırıları ve Korunma
HVL-SEC	403	Kırmızı Takım Eğitimi
HVL-SEC	405	Siber Tehdit İstihbaratı





**SİSATEM (Siber Güvenlik
Operasyon Merkezi)
Hizmetleri**



**Analiz ve Test
Hizmetleri**



**Siber Güvenlik
Ürünleri**



**Danışmanlık
Hizmetleri**



**Siber Güvenlik
Akademisi**



HAVELSAN Mustafa Kemal Mahallesi 2120 Cad. No: 39, 06510, Çankaya/Ankara

T. 0.312.219 57 87 (35 HAT PBX) F. 0.312.219 57 97

E. siber@havelsan.com.tr www.havelsan.com.tr

[@HAVELSANResmi](https://twitter.com/HAVELSANResmi) [in](https://www.linkedin.com/company/havelsan) HAVELSAN

www.sisatem.com.tr



HAVELSAN Türk Silahlı Kuvvetlerini Güçlendirme
Vakfı'nın bir kuruluşudur.