

HİZMETLER KATALOGU

Siber Güvenlik Çözümleri



**LAST
GUARD**
Cyber Security Technologies



LastGuard ile Tanışın!

LastGuard Bilişim Teknolojileri, uzman ekibiyle kurumlara ve özel sektöre yönelik güvenlik testleri, siber istihbarat çözümleri, danışmanlık hizmetleri, teknik ve farkındalık eğitimleri sunarak siber saldırılara karşı hazırlıklı olmalarını ve siber savunmalarını güçlendirmeyi amaçlamaktadır. Farklı sertifikasyonlar ve standartlar ile donanımlı ekibini her geçen gün güçlendirmektedir.



**TÜRKİYE
SİBER GÜVENLİK
KÜMELENMESİ**



Siber Güvenlik Çözümlerimiz



**SİBER
İSTİHBARAT**



**SOC
HİZMETİ**



**GÜVENLİK
TESTLERİ**



**SİBER GÜVENLİK
EĞİTİMLERİ**



**LAST
GUARD**
Cyber Security Technologies

www.lastguardsecurity.com

info@lastguardsecurity.com

0 850 840 55 22

Akademi Mah. Gürbulut Sk. Konya Teknokent G346 SELÇUKLU/KONYA

Eğitimler



**KURUMSAL BİLGİ
GÜVENLİĞİ EĞİTİMİ**



**ZARARLI YAZILIM
ANALİZİ EĞİTİMİ**



**LINUX SİSTEM
YÖNETİMİ EĞİTİMİ**



**WINDOWS SİSTEM
YÖNETİMİ EĞİTİMİ**



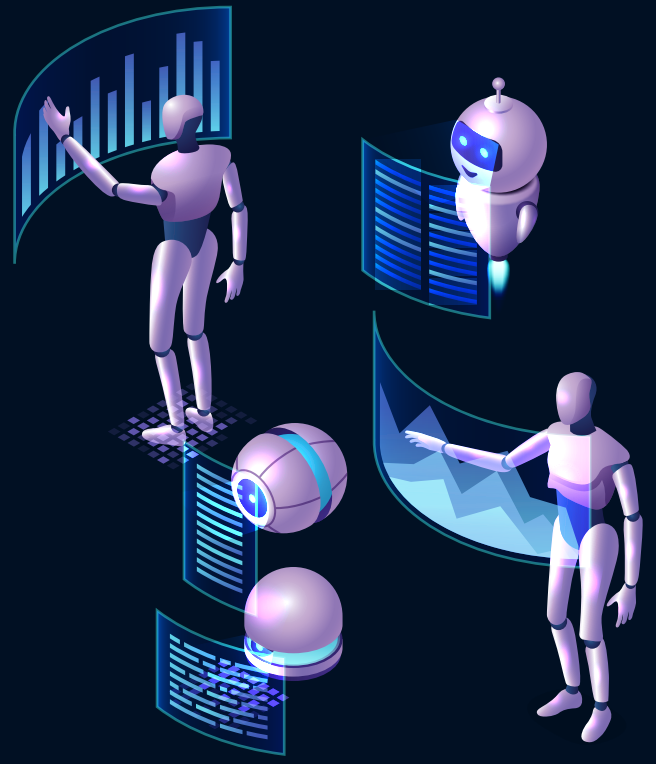
**UYGULAMALI SIZMA
TESTİ EĞİTİMİ**



**WEB UYGULAMA
GÜVENLİĞİ EĞİTİMİ**



**MOBİL UYGULAMA
GÜVENLİĞİ EĞİTİMİ**



**SİBER İSTİHBARAT
EĞİTİMİ**



**İÇ AĞ SIZMA
TESTİ EĞİTİMİ**



**KABLOSUZ AĞ
GÜVENLİĞİ EĞİTİMİ**



**PYTHON
EĞİTİMİ**

Siber İstihbarat Nedir?

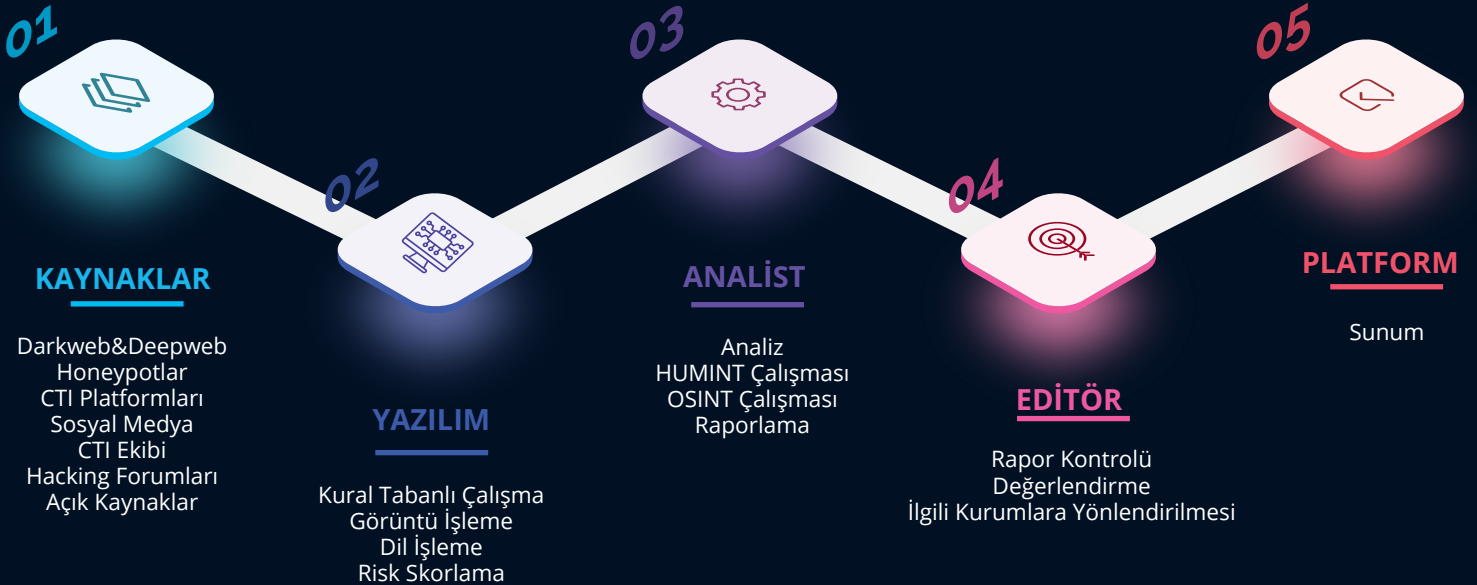
Siber istihbarat hizmeti kapsamında ekibimiz, kurumunuzun veya kuruluşunuzun müşterilerine, kimliğine veya markasına zarar verebilecek olası tüm tehditleri önceden tespit ederek raporlamaktadır. Toplanan verilerin bir süreçten geçirilerek analiz edilmesi sonucu saldırganların amaçları, metotları ya da saldırı türleri tespit edilerek erken önlem alınması, bu sayede kurumunuzun potansiyel saldırılara hazır hale gelmesi amaçlanmaktadır.



Hedef Sektörler

- 01 FİNANS
- 02 E-TİCARET
- 03 TELEKOMÜNİKASYON
- 04 ENERJİ
- 05 SAVUNMA SANAYİ
- 06 KAMU
- 07 ÜNİVERSİTE
- 08 KOLLUK KUVVETLERİ

İstihbarat Süreci



LastGuard CTI Platform

Proaktif Siber Güvenlik Çözümü



Gerçek Zamanlı Koruma



7/24 CTI Ekibi Desteği



Gelişmiş API Desteği



Otomatize Taramalar



Yapay Zeka Desteği



Sınırsız Bildirim Desteği



Modüler Satın Alma

Siber İstihbarat Faydaları

Güvenlik Ekibinizin Verimliliğini Arttırın

Yerel güvenlik ekiplerinizin ihtiyacı olan istihbarat desteğini onlara sağlayarak verimliliklerini en üst düzeye çıkarın.



Veri Kaybını Önleyin

Kurumuza yönelik tehditleri 7/24/365 prensibiyle takip eden bir istihbarat platformuyla veri kaybı olasılığını en aza indirin.



Marka İtibarınızı Koruyun

Anlık bildirimlerle markanıza yönelik yapılan saldırılardan marka itibarınız zedelenmeden haberdar olun ve önlem alın.



Envanter Yönetiminizi Kolaylaştırın

Dijital envanterinizi tüm yönleriyle takip ederek farkında olmadığınız saldırı yüzeylerinizi profesyonel çözümlerle yönetin.

Güvenlik Maliyetinizi Düşürün

Düşük false positive oranıyla, yüksek kaliteli istihbarata en uygun fiyata erişerek güvenlik bütçenizi en verimli şekilde kullanın.



Saldırı Yüzey Alanınızı Yönetin

Saldırı yüzey alanınızı hızlı ve güvenilir bir şekilde yöneterek dijital riskleri en aza indirin.



Envanter Yönetimi

İlgili kurumun domain, subdomain, web sayfaları, mail adresleri, açık servisler, DNS kayıtları, web teknolojileri, servisler ve diğer detayları rutin olarak denetlenir.

 **Domain Takibi**

 **Web Teknolojileri**

 **Sosyal Medya Takibi**

 **Anahtar Kelimeler**

 **Mail Takibi**

 **IP Adresi Takibi**



IoC Takibi

Dış kaynaklardan ve kendi tuzak sunucularımızdan gelen saldırgan verileri sürekli olarak ürüne eklenir.

 **Karaliste IP**

 **Phishing Domain**

 **Karaliste Hash**

 **Zararlı URL**



Tehdit Monitörleme

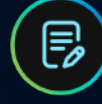
Farklı kaynaklardan elde edilen bilgiler, envanter bölümüyle de ilişkilendirilerek kuruma raporlanır.



Leak Data



Darkweb & Deepweb Takibi



Zafiyet Analizi



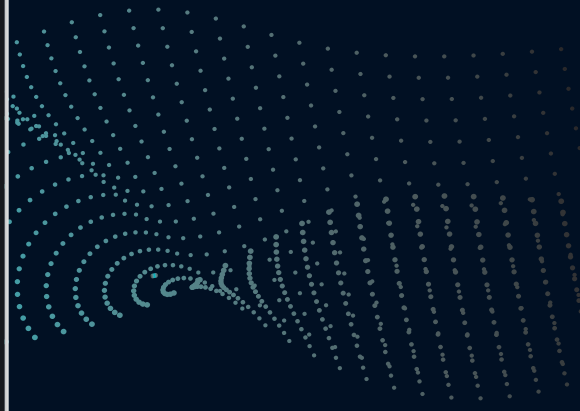
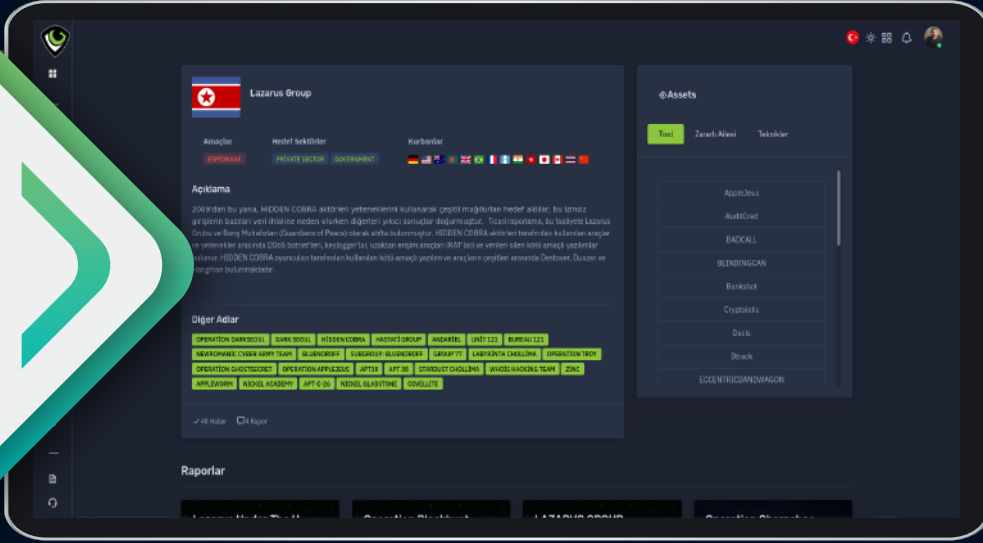
APT Grupları Analizi



Malware Analizi



Siber Güvenlik Haberleri



Kolluk Kuvvetleri

Darkweb&Deepweb başta olmak üzere farklı kaynaklardan elde edilen bilgilerle tüm suçlara yönelik yapılan çalışmalar raporlanır.



Kredi Kartı Dolandırıcılığı



Sahtecilik Suçları



Narkotik Suçları



Terör Suçları



Coin Takibi



Kaçakçılık Suçları



Güvenlik Testleri

İÇ AĞ SIZMA TESTİ

Kurumun iç ağındaki bulunan bilişim sistemlerinin, iç ağa bağlanmış bir saldırgan bakış açısıyla güvenlik testlerinin gerçekleştirilmesidir.



DIŞ AĞ SIZMA TESTİ

Kurumunuzun envanterinde bulunan dışarıya açık her türlü bilişim sisteminin (Web uygulamaları, FTP, API, mobil uygulama vb.) bir saldırgan bakış açısıyla test edilmesidir.



KABLOSUZ AĞ SIZMA TESTİ

Ekibimiz, kurumunuzda bulunan wi-fi bağlantılarındaki güvenlik açıklarını tespit etmekte ve çözüm önerileriyle birlikte raporlamaktadır.



Güvenlik Testleri

SOSYAL MÜHENDİSLİK TESTİ



Bu testler sonucunda kurumunuz personellerinin sosyal mühendislik alanındaki farkındalığı belirlenerek bu farkındalığın artırılması için gerekli çalışmalar yapılmaktadır.

MOBİL UYGULAMA SIZMA TESTİ



Mobil pentestte uygulamanın kullandığı API'lar, teknolojiler ve kaynak kod üzerinde güvenlik arařtırmalarının belli bir sistemikte yapılmasıdır.

WEB UYGULAMA SIZMA TESTİ



Web uygulamalarına yönelik zafiyetlerin OWASP vb. standartlara göre test edilmesi ve raporlanmasıdır.



Security Operations Center (SOC) Hizmeti

- Güvenlik Analizi**
Güvenlik verileri toplanır, izinsiz girişler, tehditler ve davranışsal anomali tespitleri için kullanılır.
- Yetkisiz Erisim Tespiti**
Kötü amaçlı yazılımlar, rootkitler şüpheli işlemleri tespit eder. Ağ anomalileri, gizli dosyalar ve anormal işlemleri algılar.
- Log Analizi**
İşletim sistemi ve uygulama günlüklerini okur, kural tabanlı analizler yapar. Güvenlik ihlallerinde bildirimde bulunur.
- Dosya Analizi**
Dosya izinlerini, sahiplikleri ve diğer detayları belirler. Ekleme, silme, düzenleme işlemlerini takip eder.
- Zafiyet Tespiti**
Güvenlik verileri toplanır, izinsiz girişler, tehditler ve davranışsal anomali tespitleri için kullanılır.
- Konfigürasyon Kontrolleri**
Sistem sıkılaştırma süreci için uygulama ve işletim sistemindeki yapılandırma- larınızı periyodik olarak tarar.
- Olay Müdahalesi**
Komut ve sistem sorgularını uzaktan çalıştırmak, loC belirlemek ve adli bilişim süreçleri için kullanılabilir.
- Bulut Güvenliği**
Amazon AWS, Google Cloud ve diğer bulut sağlayıcılardan veri alır ve zayıflıkları tespit eder.
- Regülasyonlar**
PCI DSS, GDPR, KVKK, NIST 800-53 SOC2 ve HIPAA gibi regülasyonlara uyumluluk süreci için raporlar sunar.
- Konteyner Güvenliği**
Docker sunucularının davranışlarını izler, tehditler, güvenlik açıkları ve anomalileri tespit eder.

Endpoint Security Agent



ORACLE®
Solaris



Lisans Ücreti Yok

Açık kaynak yazılım çözümleri sayesinde lisans ücreti gerekmiyor.



EPS Limiti Yok

EPS, sunucunuzun gücü ile doğru orantılıdır ve daima arttırılabilir.



Personel Gideri Yok

Kurumunuzda analist istihdam etmeden de operasyonel süreçler devam eder.



Ömür Boyu Kullanım

SOC hizmeti sonlandığında bile SIEM ürünü kurum envanterinde yerini korumaktadır.



Diğer Hizmetler

Siber güvenlik alanında farklı alanlarda uzman ekibimiz ile danışmanlık hizmetleri, network ve güvenlik çözümleri sunmaktayız. Teknik ekibimizden 7/24 destek alabilirsiniz.

LOG ANALİZİ

Log yönetimi, anlık olarak gerçekleşen saldırının delillerini veya olası bir saldırının göstergelerini elde etmeye olanak sağlamaktadır. Saldırı sonrası sistemin zayıflıkları hakkında bilgi edilmesi açısından da büyük önem taşımaktadır. Log analizi hizmeti kapsamında, kurumunuza ait ağların ve cihazların tespiti, kurumunuza en uygun log sisteminin belirlenmesi, log sisteminin kurulumu ve log yönetimi gereksinimleri ekibimiz tarafından giderilmektedir.

WAF YÖNETİMİ

Kurumun web uygulamalarına özel olarak tercih edilen WAF hizmeti seçilir. Kurumun talepleri doğrultusunda güvenlik kuralları hazırlanır ve WAF konfigürasyonları uygulanır.

FİREWALL YÖNETİMİ

Tehditlerin büyük çoğunluğu network(bilgisayar ağı) temellidir ve Güvenlik Duvarları bu tehditleri durdurmada kilit rol oynar. Güvenlik Duvarları yazılımsal ve donanımsal olabilir ve bu güvenlik ürünleri tak çalıştır mantığı ile çalışmamaktadır. Bir güvenlik uzmanının gerekli ayarlamaları yaptıktan sonra kullanabileceğiniz bir üründür. Hizmetlerimiz kurumların Güvenlik altyapısına ve yaklaşımlarına göre farklılık göstermektedir.

SWITCH&ROUTER KONFIGURASYONU

Hangi networklerin birbirleri ile haberleşeceği ve bu haberleşme altyapısının hangi protokoller üzerinden gerçekleşeceği gibi durumlar için şirketimizin hizmetleri bulunmaktadır. Network'ün ölçütüne ve bilgisayar ağı yapısına göre en uygun protokol seçilir ve istenilen bilgisayar ağları arasında yalıtım sağlanır. Kurumun isteği doğrultusunda istenilen protokol altyapısına uygun şekilde konfigürasyon yapılabilmektedir.

SİSTEM SIKILAŞTIRMA

Sistem sıkılaştırma hizmeti, işletim sistemleri, ağ altyapısı ve yazılımlardaki potansiyel zafiyetleri ve tehdit oluşturan unsurları ortadan kaldırarak güvenlik risklerini minimuma indirmeyi hedeflemektedir. Kullanıcı yetkilendirmeleri, kullanılmayan servisler ve araçlar, erişim yetkileri, güvenlik politikaları ve bilinen zafiyetler ele alınarak eksiklikler giderilir.

HONEYPOT ÇÖZÜMLERİ

Honeypotlar, saldırganların ilgisini üzerine çekmek için kontrollü olarak zafiyet bırakılan cihazlardır. Ağ içerisinde doğru noktalara konumlandırılarak gerçek cihazlardan önce bu cihazlara saldırılması sağlanır. Honeypotlardan elde edilen verilerle saldırganın tekniklerinin yanı sıra dijital parmak izine dair de veriler elde edilir. Diğer yandan saldırgan honeypotlarla zaman kaybederken olay müdahalesi için zaman kazanılır ve gerçek sistemlere erişmeden önce önlem alınır.



**LAST
GUARD**
Cyber Security Technologies

www.lastguardsecurity.com

info@lastguardsecurity.com

0 850 840 55 22

Akademi Mah. Gürbulut Sk. Konya Teknokent G346