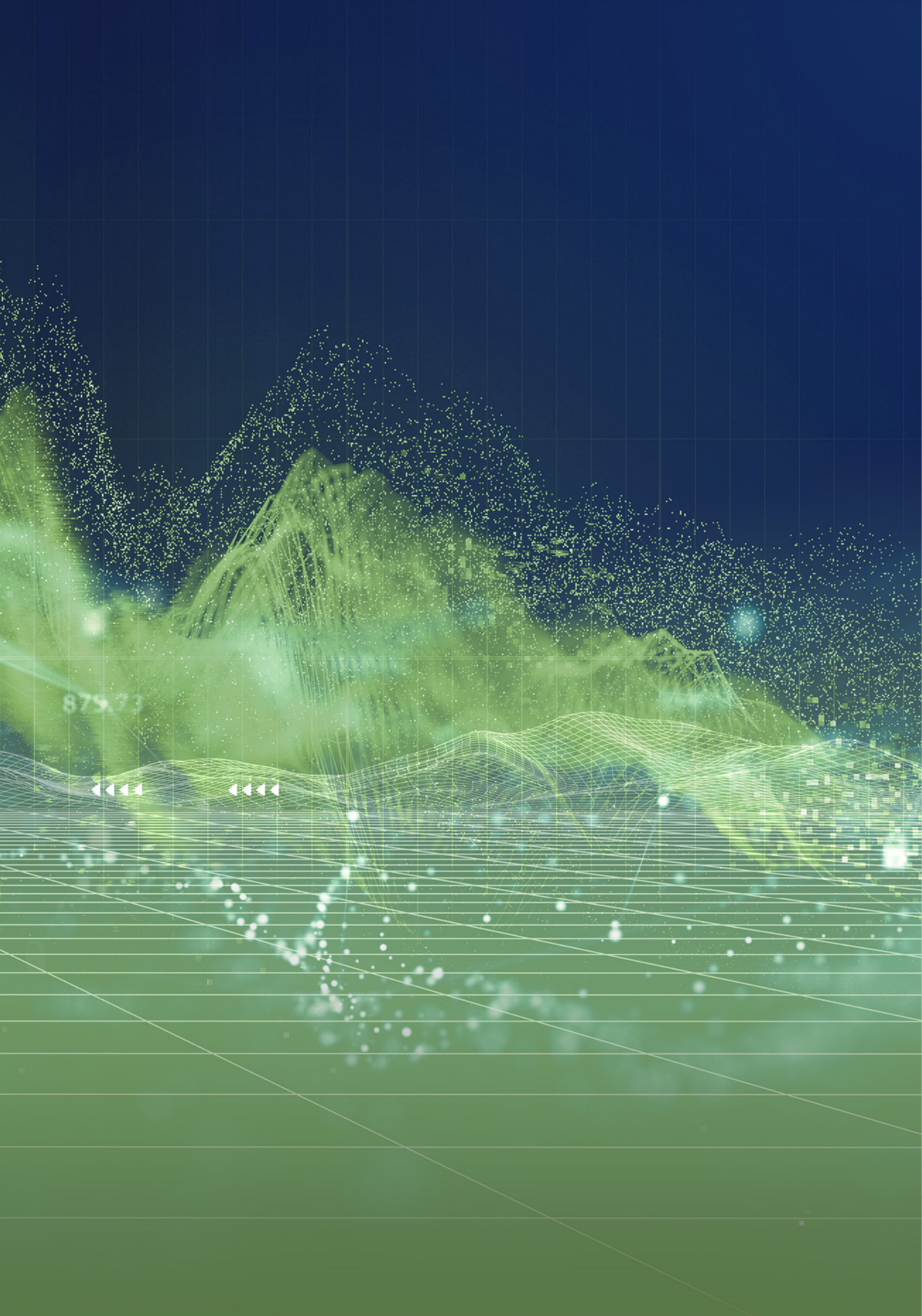
SİBER GÜVENLİK

STM



STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş.

STM, T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) ve Türk Silahlı Kuvvetleri'ne; proje yönetimi, sistem mühendisliği ve danışmanlık hizmetleri sağlamak amacıyla 1991 yılında kuruldu.

Ana hissedarı SSB olan şirketin, yüzde 63'ü mühendis kadrosunda olmak üzere 850'yi aşkın nitelikli çalışanı bulunmaktadır.

Türkiye'nin önde gelen savunma sanayii firmalarından biri olan STM; askeri deniz platformları, taktik mini İHA sistemleri, siber güvenlik ve bilişim hizmetleri, komuta-kontrol projeleri, uydu teknolojileri, askeri havacılık, radar ve elektronik harp, tedarik ve danışmanlık alanlarında lider bir Türk savunma sanayii şirketidir.

Türk savunma sanayinin milli projelerinde görevler üstlenen STM; NATO ve 30'dan fazla ülkede iş birlikleri, ihracat ve iş geliştirme faaliyetleri yürütmektedir.

Türkiye'nin ilk milli korvet projesinde (MİLGEM) ana alt yüklenici olan STM, Türkiye'nin ilk milli fırkateyni TCG İSTANBUL (F-515)'un da detay tasarımcısı ve ana yüklenicisidir.

Türk Donanması'nın denizaltı modernizasyon ve inşaa süreçlerinde önemli görevler üstlenen STM, Türkiye'nin ilk denizaltı modernizasyon ihracatı olan Pakistan AGOSTA 90B Projesine de imza atmıştır.

Türkiye'nin ilk milli vurucu İHA Sistemi KARGU'yu geliştiren STM, Türkiye'nin ilk Siber Füzyon Merkezini 2016 yılında faaliyete geçirmiştir.

Dünya genelindeki tüm NATO karargâhları arasında istihbarat paylaşımının sağlandığı INTEL-FS2 Projesini geliştiren STM, Türkiye'nin NATO'daki en büyük yazılım ihracatlarından birisini başarıyla sürdürmektedir.

STM, Türkiye'nin savunma sanayii ihtiyaçları öncelikli olmak üzere sahip olduğu teknoloji tabanlı faaliyetleri; kamu ve özel sektör ihtiyaçlarına yönelik çeşitlendirmektedir.

STM'nin Genel Müdürlüğü Ankara'da bulunmakta ve İstanbul, Gölcük, Pakistan ve Ankara'da 9 ayrı yerleşkede faaliyetlerini sürdürmektedir.

STM, dünyanın en büyük 100 savunma sanayii şirketinin yer aldığı "Defense News Top 100" listesinde, 3 kez yer almayı başarmıştır.

SİBER GÜVENLİK

STM SİBER GÜVENLİK YETENEKLERİ

- Siber Tehdit İstihbaratı
- Siber Durumsal Farkındalık
- Siber Risk Yönetimi ve Değerlendirme
- Siber Bilgi Paylaşım ve Uyarı Sistemleri
- Siber Karar ve Süreç Destek Sistemleri
- Akıllı ve Otonom Siber Güvenlik Altyapıları
- Sızma (Pen-Test) Testi Hizmetleri
- Siber Tatbikat ve Hazırlık Altyapıları
- Siber Savunma Birlikte Çalışabilirlik
- Siber Olay/Veri Görselleştirme Altyapıları

SİBER GÜVENLİK FAALİYET ALANLARI

- Siber Füzyon Merkezi Hizmetleri
- Araştırma ve Ürün Geliştirme
- Projeler
- STM Akademi Eğitimleri
- Siber Güvenlik Raporları
- Bayrağı Yakala/Capture The Flag (CTF) Yarışmaları

STM AKADEMİ

Teorik ve Pratik Eğitimler

- STM Akademi'de verilen eğitimler teorik ve pratik unsurları içermektedir.

Siber Güvenlik Temel Farkındalık

- Bilgi güvenliği farkındalığının yetersiz olduğu bilinmektedir.
- Güncel saldırı yöntemleri ve önlemleri hakkında teorik ve pratik eğitimler verilmektedir.

Siber Güvenlik Uzmanı Eğitimleri

- Siber güvenlik konusunda çalışan personelin eğitim seviyesinin ortaya çıkan yeni saldırı teknikleri ve yöntemlerini de kapsayacak şekilde güncel tutulması gerekmektedir.

İleri Seviye Siber Güvenlik Eğitimleri

- Geniş yelpazedeki birçok konunun yanı sıra, derinlemesine belirli konuların araştırılması ve eğitimine yönelik programlar hazırlanmıştır.

Siber Güvenlik Yönetici Eğitimleri

- STM Akademi'de yöneticiler için stratejik seviyede siber güvenlik eğitimleri verilmektedir.

Siber Laboratuvar

- Zararlı yazılım analizi, tehdit analizi ve sızma testi,
- Dayanıklı ağ sistem mühendisliği,
- Yüksek performans bilgi işleme ve veri analitiği,
- Tersine mühendislik, zafiyet ve açıklık belirleme vb.

STM AKADEMİ SİBER GÜVENLİK EĞİTİMLERİ

- Saldırı Tespit ve Kayıt Yönetimi Eğitimi
- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi
- Uygulamalı Web Sızma Testi
- Siber Güvenlik ve Risk Değerlendirme
- Merkezi Güvenlik İzleme ve Olay Yönetimi
- Zararlı Yazılım Analizi Eğitimi
- Temel Açık Kaynak İstihbarat - OSINT ve Siber Tehdit İstihbaratı
- Web Uygulama Güvenliği Eğitimi
- Güvenli Yapılandırma Denetimi
- Yöneticiler İçin Bilgi Güvenliği
- İş Sürekliliği ve Felaketten Kurtarma
- Sosyal Mühendislik Saldırı ve Korunma Yöntemleri
- ISO 27001 Uygulama Eğitimi
- Etik Bilgisayar Korsanı Eğitimi
- Uygulamalı Büyük Veri Bilimsel Eğitimi
- Uygulamalı Büyük Veri Mühendislik Eğitimi

STM SİBER GÜVENLİK RAPORLARI

- Üçer aylık dönemlerde yayımlanan "Türkiye Siber Tehdit Durum Raporu" yaşanan siber olaylar konusunda genel bilgi sunmaktadır ve ülkemizde siber güvenlik farklılığının gelişmesine katkı ve destek sağlamaktadır.
- Raporlar, siber tehdit değerlendirmesi ile öngörüler ışığında hazırlanan muhtemel siber saldırı bilgilerini de içermektedir.

BAYRAĞI YAKALA ETKİNLİĞİ, CAPTURE THE FLAG (CTF)

- STM liderliginde kamu, özel sektör ve üniversitelerin tek çatı altında birleştirilmesi ve siber güvenlik alanında bilgi paylaşım ağının oluşturulması hedeflenmiştir.
- 2015 yılından beri her yıl düzenlenen ve gelecek yıllarda da devam edecek olan etkinlik, bu alanda Türkiye'deki en uzun soluklu ve en yüksek katılımlı çalışmasıdır.

SİBER FÜZYON MERKEZİ

Kritik teknoloji ve bilgi varlıklarını koruyan proaktif ve önleyici faaliyetleri içeren **Siber Füzyon Merkezi (SFM)**; Siber Tehdit İstihbarat Merkezi, Siber Operasyon Merkezi ve Zararlı Yazılım Analiz Laboratuvarı (Z-Lab) olmak üzere bütünleşik ve entegre 3 ana merkezden oluşmaktadır.

STM SİBER FÜZYON MERKEZİ (SFM)

- Geleneksel siber güvenlik işlevselliklerini, yeni yeteneklerle birleştirerek tek ve entegre siber güvenlik yaklaşımı
- Siber tehdit istihbaratının güvenlik ve teknolojik ve müdahaleleri ile entegre eden çok yönlü yaklaşım
- Bu entegrasyon ile kritik teknoloji ve bilgi varlıklarını koruyan proaktif eylemleri yönlendirme
- İş, insan, süreç ve teknolojinin bütünleşmesi

STM SFM HİZMETLERİ

- Siber Operasyon Merkezi Hizmetleri
- Dinamik Risk Yönetimi
- Olay Müdahale
- Siber Tehdit İstihbaratı
- Zararlı Yazılım ve Sistem Analizi
- Trafik Analizi ve İzleme

Siber Operasyon Merkezi (SOM)

- SOC Kurulum ve İşletme Danışmanlığı
- 7/24 Güvenlik İzleme Hizmeti
- SIEM İyileştirme ve Optimizasyon Danışmanlığı
- Use Case Danışmanlığı
- Olay Müdahale Hizmeti
- Tehdit Avcılığı Hizmeti

Siber Tehdit İstihbaratı Merkezi (STIM)

- Atak Yüzey Analizi
- Açık Kaynak Tehdit İstihbaratı Analizi
- Siber Tehdit İstihbaratı Platformu
- Dark/Deep Web Analizi
- Tehdit Aktörü Analizi
- Müşteriye Özel Hazırlanmış Tehdit Raporları

STM SİBER OPERASYON MERKEZİ

Siber Operasyon Merkezi'nde; siber olayların tespiti için altyapı tesis edilmesi, güvenlik politikalarının uygulanması ve izlenmesinden başlayan, olay inceleme ve yerinde olay müdahalesini kapsayan hizmetler verilmektedir. Kurumların ihtiyaçlarına binaen bu hizmetlerin bir veya birkaçı kuruma özel plan dahilinde verilmektedir.

OLAY İLİŞKİLENDİRME (KORELASYON) HİZMETİ

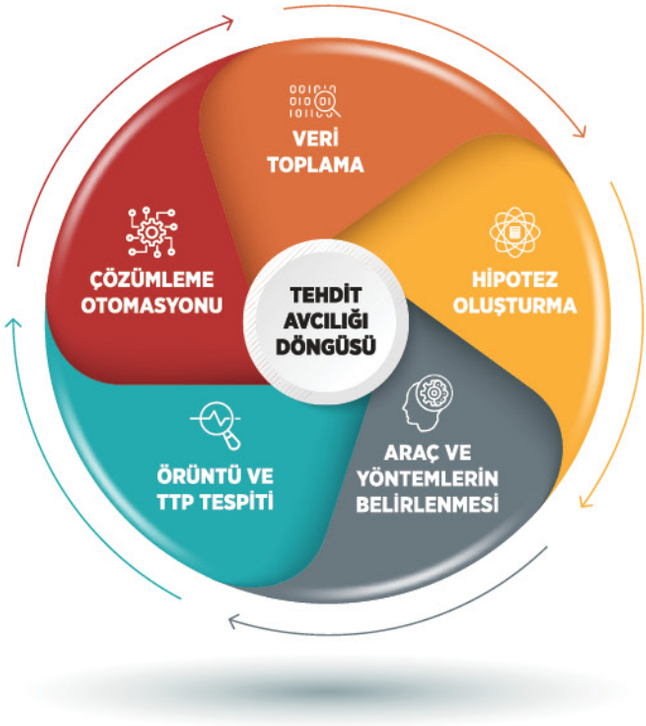
Olay kaynakları ve SIEM çözümünün yetenekleri doğrultusunda kayıtların ilişkilendirilmesi ve sonuçlar çıkarılması için ihtiyaç duyulan korelasyon kuralları belirlenir ve sisteme tanımlanır. Tanımlı kurallar neticesinde oluşan alarmlar incelenerek güvenlik ihlallerinin nedenleri detaylı şekilde araştırılır.

SIEM İZLEME HİZMETİ

SIEM tarafından toplanan kayıtlar, SIEM izleme yeteneklerinin yanı sıra STM mühendisleri tarafından geliştirilen ilave uygulamalar, açık kaynak kodlu ve ticari araçlar yardımıyla siber güvenlik analistleri tarafından izlenir, araştırılır, değerlendirilir ve müdahale ihtiyacı raporlanır. İzleme Hizmeti kapsamında 5/8 ya da 7/24 hizmet verilebilmektedir.

DANIŞMANLIK VE YERİNDE DESTEK HİZMETİ

Hizmet verilen kuruma ait siber güvenlik bileşenleri analiz edilerek, kuruma ait sistemlerin güvenliğinin analiz edilmesi ve arttırılması konusunda kurum ile birlikte gerekli çalışmalar yapılır. Güvenliğin bütünleşik olarak sağlanması hedeflenir.



OLAY İNCELEME

Siber Ölüm Zinciri (Cyber Kill Chain) metodolojisi referans alınarak yapılan olay incelemelerinde; siber saldırının kaynağı, hedefi, kapsamı, atak vektörü ve etkilediği sistemler tespit edilir. Yapılan çalışmaların ardından elde edilen bulgular tüm detaylarıyla birlikte raporlanır ve müteakip dönemde gerçeklesmemesi için ihtiyaç olan tedbirler sunulur.

YERİNDE OLAY MÜDAHALE

Hizmet verilen kurumun kaynaklarına bir saldırı olduğunda olaya müdahale edilir ve saldırı esnasında oluşabilecek kaybın yok edilmesi veya en aza indirilmesi amacıyla gerekli çalışma, görevli personel ve kurum yetkilileriyle birlikte yapılır.

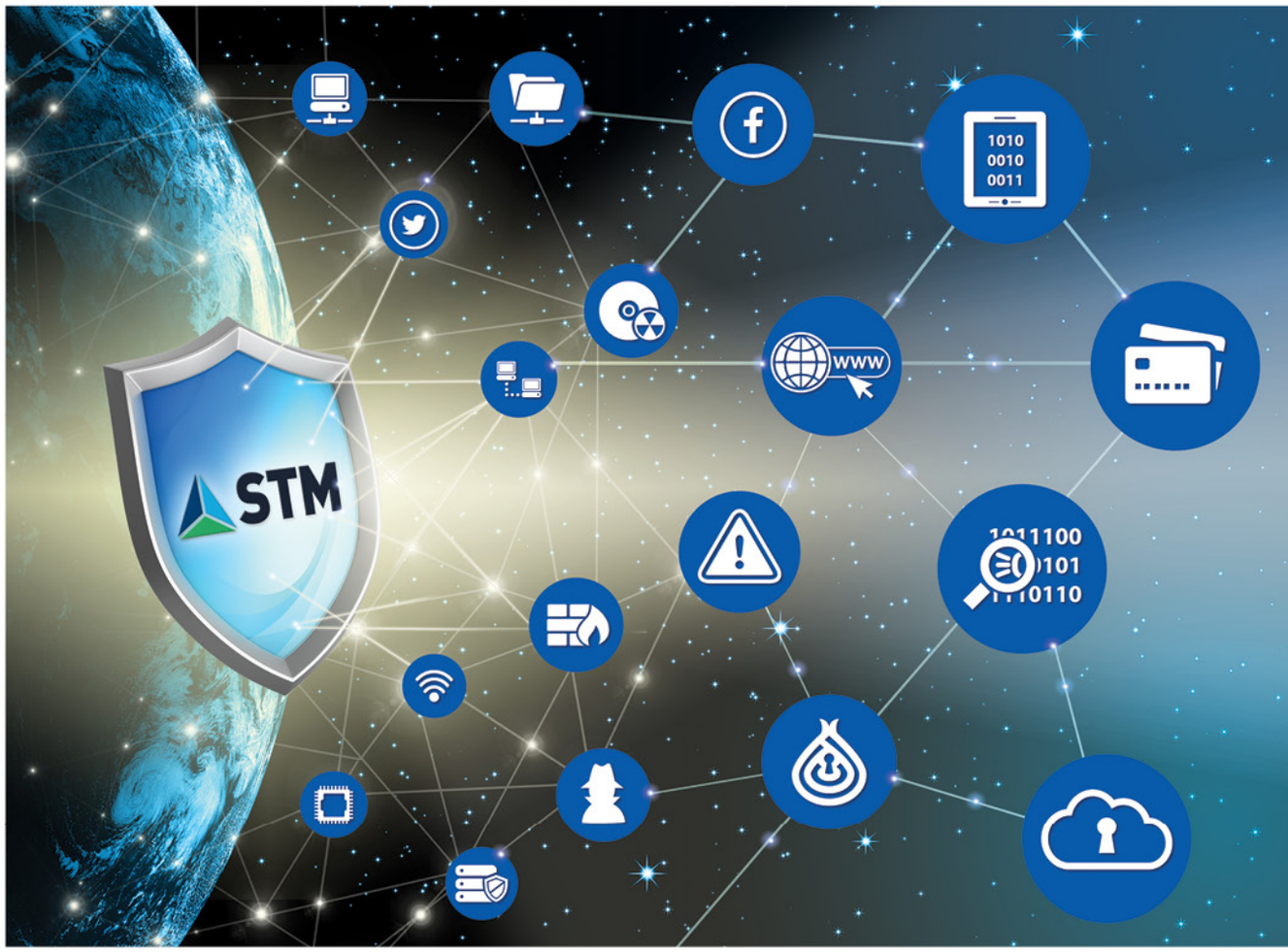
TEHDİT AVCILIĞI

Kuruma ait olan ağ ve sistemlerde proaktif bir şekilde gelişmiş düzeydeki siber tehdit varlığı farklı senaryolar göz önünde bulundurularak araştırılır. Potansiyel saldırganlar, bu saldırganların kullandıkları teknikler, kullanılan araçlar ve saldırı süreçleri aktif olarak takip edilir ve tanımlanır. Bu sayede Hedef Odaklı Saldırılara (Advanced Persistent Threat – APT) karşı alınması gereken önlemler tespit edilir ve kurumun bilişim teknolojileri altyapısındaki boşluklar belirlenir. Açık kaynak kodlu ve ticari araçlardan faydalanılarak potansiyel tehditler, şüpheli ve anormal aktiviteler, kötü amaçlı yazılımlar gibi tehlikeleri tanımlamak için gösterge tabloları ve raporlar oluşturulur. PCAP dosyaları, ağ akış verileri, uygulamalar ve diğer güvenlik araçları üzerinden gelen bilgiler düzenli bir şekilde ve derinlemesine analiz edilir.

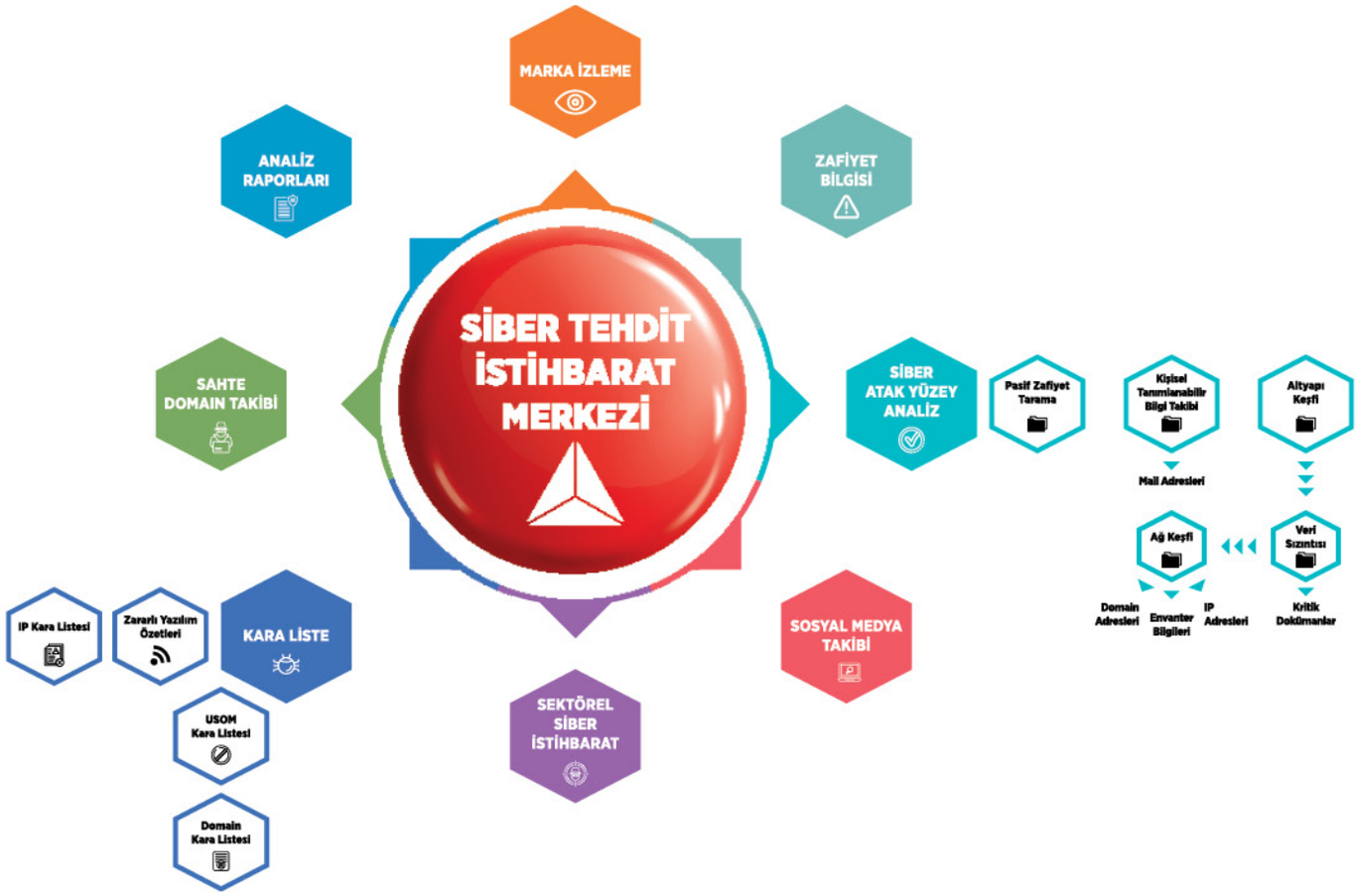
STM SİBER TEHDİT İSTİHBARAT MERKEZİ (STIM)

Siber uzayda gerçekleşen saldırıların önceden tespit edilebilmesi ve önlem alınabilmesi amacıyla STM SiberTehdit İstihbarat Merkezi'nde açık kaynaklar üzerinden veri toplama, veriyi zenginleştirme ve veriye bilgi statüsü kazandırma ile bilginin analiz edilerek istihbarata dönüştürülmesi işlemleri gerçekleştirilmektedir.

Siber tehdit istihbaratı için gerekli veriler, tehdit unsurlarının ve küresel tehdit ekosisteminin teşhisi ve sürekli izlenmesini içeren bir süreçle toplanmaktadır. Bu süreçte tehdit verileri açık kaynaklardan, ticari kaynaklardan ve MISP benzeri platformlardan toplanarak aksiyon alınabilir istihbarat haline getirilmekte ve kendi yazılımlarımız üzerinden sunulmaktadır. Aynı zamanda elde edilen bu istihbarat verisi, siber tehdit analistlerince sektöre veya kuruma özel siber tehdit istihbaratına dönüştürülmektedir.



STIM tarafından toplanan verilerin, zenginleştirilmesi, depolanması ve doğrulanmasını müteakip elde edilen nihai siber tehdit istihbarat bilgileri, STM Siber Tehdit İstihbarat Platformu (CyThreat) üzerinden kurumlara servis olarak sunulmaktadır.



PENTEST VE KIRMIZI TAKIM HİZMETLERİ

- Kırmızı Takım Faaliyetleri
- Web Uygulama Testi
- IT ve OT Ağ altyapısı testi
- Sosyal Mühendislik
- DOS/DDOS Testi
- Kablosuz Ağ Testi
- Mobil Uygulama Testi
- Doğrulama Testi

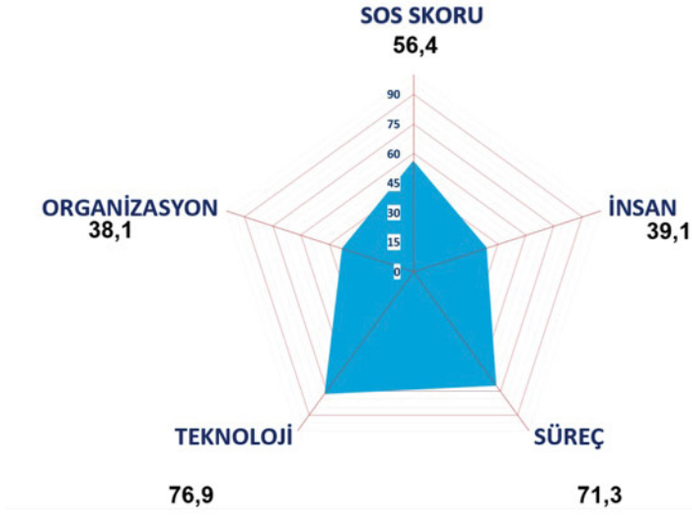
STM TSE Onaylı A Sınıfı Sızma Testi Firmasıdır.

UYUM VE DENETİM HİZMETLERİ

BİGR Danışmanlık ve Denetim Hizmeti

Siber Güvenlik Olgunluk Seviyesi Analizi

Alan uzmanları ile kurumunuzun organizasyonel, teknolojik, süreçsel, insan bazlı siber güvenlik yaklaşımını ulusal/uluslararası standartlara göre özelleştirdiğimiz soru listelerimiz ışığında değerlendiriyor ve siber güvenlik olgunluğunun artırılmasına yönelik önerilerimizi sunuyoruz.



STM ZARARLI YAZILIM ANALİZ LABORATUVARI (Z-LAB)

Zararlı Yazılım Analiz Laboratuvarı'nda, zararlı olduğu değerlendirilen veya şüphelenilen dosyaların analizleri profesyonel analistler tarafından gerçekleştirilmektedir. Söz konusu analizler ile yazılımın zararlı olup olmadığı, şüpheli dosyanın arka planda neler yaptığı, asıl amacının ne olduğu ve kendisini nasıl gizlediği gibi özel davranışlar ortaya çıkarılmaya çalışılmaktadır.

Zararlı Yazılım Analiz Laboratuvarı'nda Windows, Linux ve MacOSX işletim sistemlerine ek olarak akıllı telefonlar ve tablet bilgisayarlarda kullanılan Android ve iOS işletim sistemleri üzerinde çalışan zararlı yazılımların analizi yapılabilmektedir.

Analistlerin analiz yapabilecekleri birbirinden bağımsız ağlar ve simülasyon ortamları sayesinde, zararlı yazılımın ihtiyaç duyduğu internet ortamı simüle edilebileceği gibi hiçbir internet bağlantısı olmadan da analiz yapılabilmesi sağlanabilmektedir.

ZARARLI YAZILIM ANALİZİ YAPILAN PLATFORMLAR

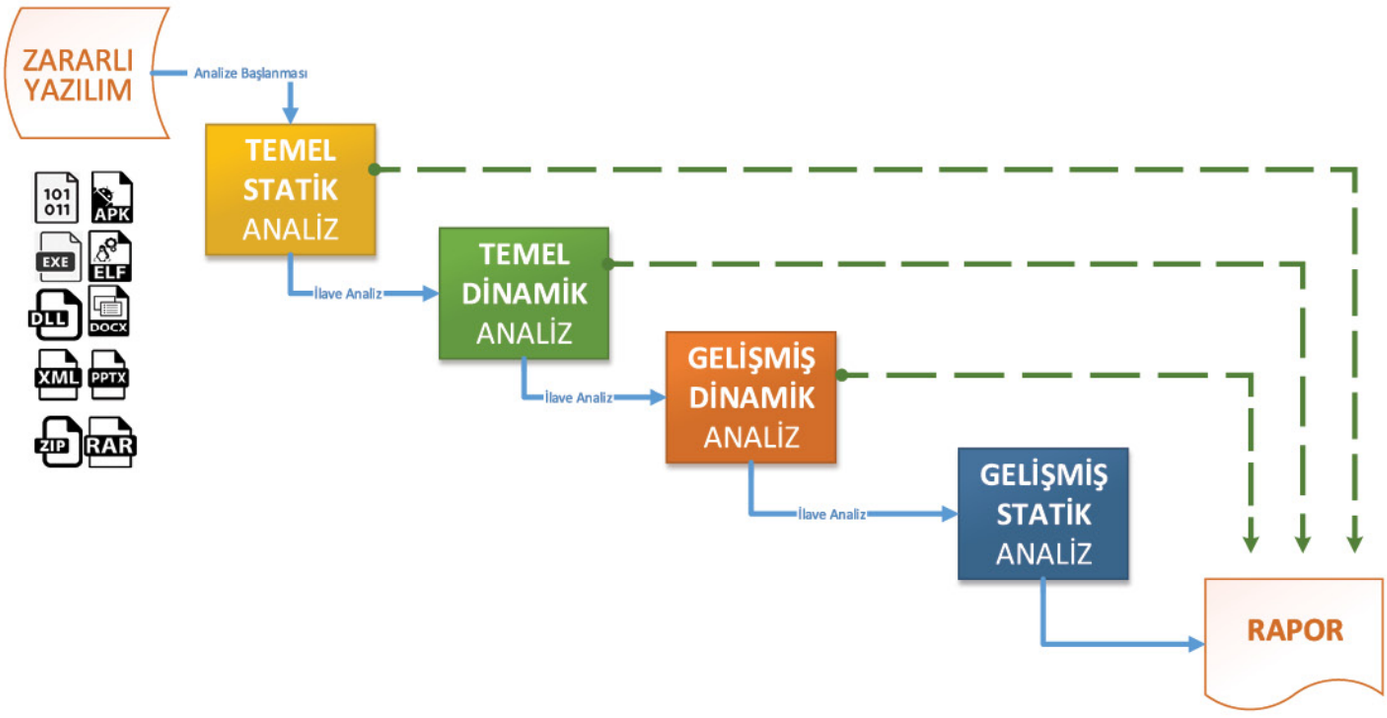
- Windows
- Linux
- OSX
- iOS
- Android

ANALİZ YÖNTEMLERİ

- Temel Statik Analiz
- Temel Dinamik Analiz
- Gelişmiş Statik Analiz
- Gelişmiş Dinamik Analiz

ANALİZ MECRALARI

- Sanal bilgisayarlar üzerinde analiz
- Kum havuzları üzerinde analiz
  - Ticari kum havuzları kullanılarak
  - Açık kaynak kum havuzları kullanılarak
- Fiziki cihazlar
  - Cep telefonu
  - Tablet
  - Bilgisayar

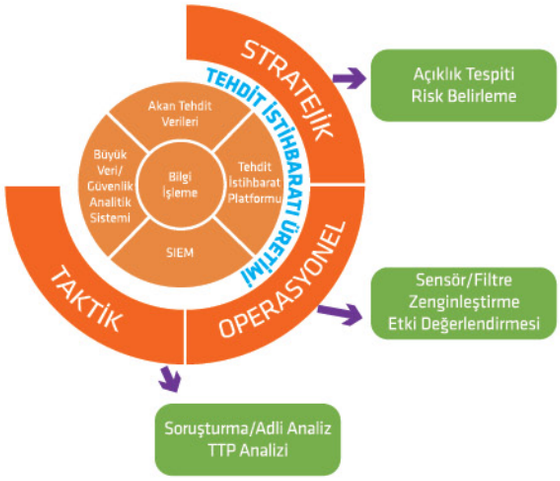


DevSecOps Danışmanlık Hizmeti:

- DevOps süreçlerine siber güvenlik bakış açısının eklenmesi için danışmanlık hizmeti verilmektedir.
- SAST (Static Application Security Testing) ve DAST (Dynamic Application Security Testing) çözümlerinin var olan iş akışlarına eklenmesi için gerekli danışmanlık hizmeti verilmektedir.

Zararlı Yazılım Analiz Laboratuvarı Kurulum Hizmeti:

- Büyük ölçekli kurumlarda zararlı yazılım analizinin yerinde yapılabilmesi için Zararlı Yazılım Analiz Laboratuvarı kurulumu ve danışmanlık hizmeti verilmektedir.



Capture The Flag (CTF):

- Capture The Flag yarışması için gerekli olan altyapı hizmeti sağlanmaktadır.
- CTF platformunun kurulum hizmeti verilmektedir.
- Her yıl siber güvenlik farkındalık kapsamında STM CTF yarışması düzenlenmektedir.

Zararlı Yazılım Analizi Hizmetleri:

- Bir siber güvenlik olayından sonra elde edilen şüpheli dosyaların zararlı yazılım kapsamında analiz edilip detaylı raporlanması hizmeti verilmektedir.

DDOS:

- Ağ güvenlik ürünlerinin yapılandırmalarının kontrollerini sağlamak amacıyla farklı coğrafi bölgelerden dağıtık servis dışı bırakma saldırı simülasyonu hizmeti verilmektedir.

Ürün Geliştirme:

- Siber güvenlik projeleri kapsamında müşteri ihtiyaçlarını karşılamaya yönelik ürün geliştirme hizmeti verilmektedir.
- Siber güvenlik ürünlerinin yapılandırmalarını ve tespit kabiliyetlerini test etmek amacıyla özelleştirilmiş zararlı yazılım simülasyon hizmeti verilmektedir.

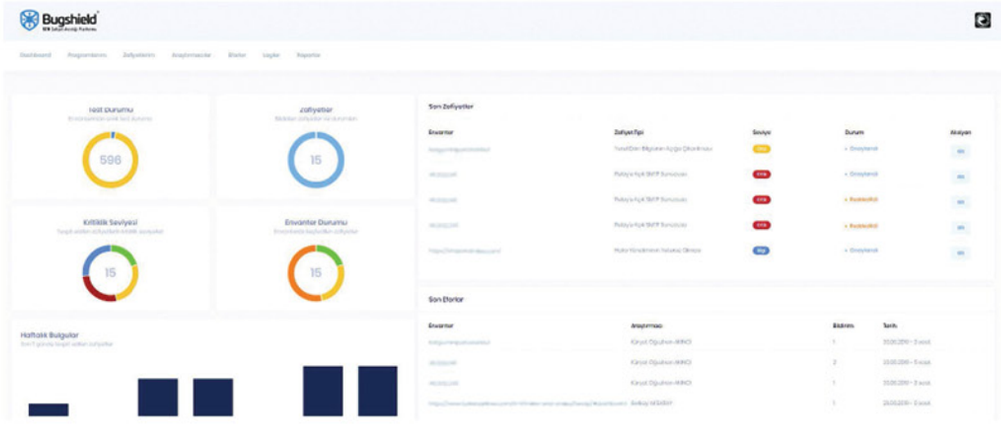
BUGSHIELD

Kesintisiz Siber Güvenlik

STM Bugshield; “hacker” bakış açısı ile müşteri kaynaklarındaki zafiyetlerin araştırıldığı, bulunan zafiyetlerin raporlandığı Sürekli Sızma Testi ve Ödül Avcılığı Platformudur.

STM Bugshield; müşteri, analist ve araştırmacı profilleri bulunan rol tabanlı yönetim yeteneğine sahiptir. Araştırmacı rolünde farklı alanlarda yetkin siber güvenlik uzmanları zafiyet araştırması yapar; analist ise tespit edilen zafiyetleri doğrular ve onay süreci sonrasında müşteriyi platform üzerinden bilgilendirir ve bu sayede müşteri, tespit edilen zafiyetlere hızlı yanıt verebilir. Platforma bütünleşik geliştirilen biletleme (ticketing) mekanizması ile bulgular ve durum değişiklikleri anlık olarak izlenebilir. Bugshield üzerinden gönderilen uyarılara ek olarak e-posta ve SMS ile de bildirimler iletilebilmektedir.

- Sistemlerin “Sürekli Sızma Testi Metodolojisi” ile müşteri tarafından belirlenen zaman aralıklarında farklı güvenlik araştırmacıları tarafından test edilmesiyle, yeni çıkan zafiyetlerin hızlı bir şekilde tespiti hedeflenmektedir. Tespit edilen zafiyetler iki aşamalı onay sürecine tabi tutularak, doğruluğu onaylanan bulgular müşteriye anlık bildirimlerle iletilmektedir. Bu sayede zafiyetin bulunması ile kapatılması arasındaki süre kısaltılmaktadır.
- Testlerin durumu, bulunan zafiyetler, zafiyetlerin kritiklik seviyeleri, zafiyetlere yönelik yapılan işlemler ve zafiyet envanteri portal üzerinden izlenebilmektedir.
- Kurumlar, envanter listelerini ve test politikalarını belirleyerek zafiyet araştırması talep edebilmektedir.
- Kurumlar, zafiyet araştırması sonuçlarını pdf, word (docx), csv ve json formatlarında ve istedikleri filtrelemeyi uygulayarak otomatik rapor oluşturabilmektedir.



Test Durumu
Test edilen veya edilmesi planlanan envanterin görüldüğü ekrandır.

Zafiyetler
Bildirilen zafiyetlerin onay durumlarının yer aldığı ekrandır.

Kritiklik Seviyesi
Kritik, yüksek, orta ve bilgi seviyesinde tespit edilen zafiyetlerin görüldüğü ekrandır.

Envanter Durumu
Zafiyetlerin kaç adet uygulama, IP adresi veya alan adında (domain) bulunduğunu gösteren ekrandır.

ÖNE ÇIKAN ÖZELLİKLER

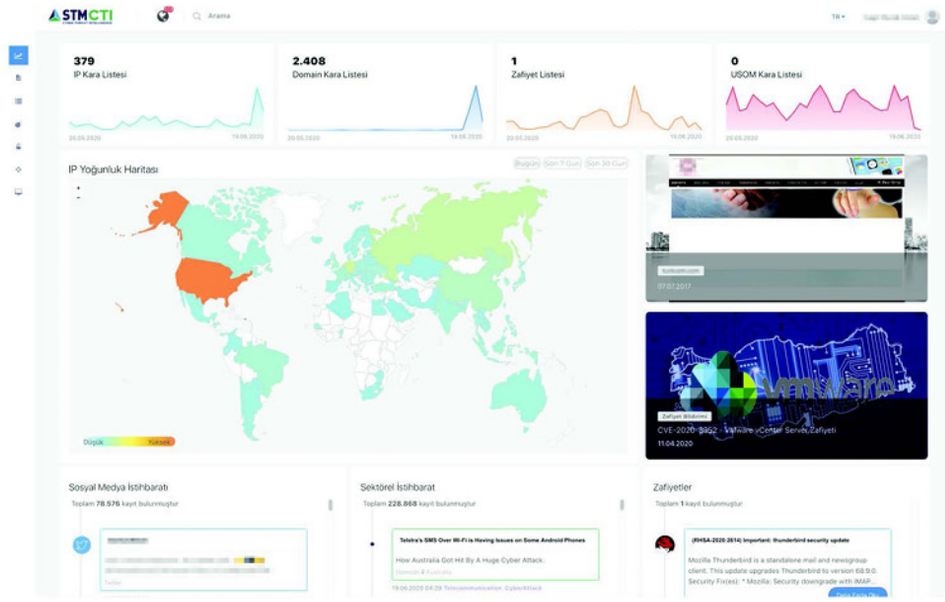
Güvenilirlik: Zafiyetlerin gizlilik sözleşmesi imzalamış güvenilir bir araştırmacı grubu tarafından tespit edilmesi
Kalite: Envantere birden fazla araştırmacının bakması ve tespit edilen zafiyetlerin STM analistleri tarafından kontrol edilip onaylanması
Çeviklik: Tespit edilen tüm zafiyetlere anlık bildirim gönderilmesi ve aksiyon alınabilmesi
Süreklilik: Dönemsel sızma testlerinin aksine daha sık aralıklarla testlerin gerçekleştirilmesi

Bugshield
STM Zafiyet Avcılığı Platformu

CyThreat

Siber Tehdit İstihbarat Platformu

CyThreat, çeşitli kaynaklardan (deep/dark webten, sosyal medyadan, bloglardan, forumlardan vb.) otomatize bir şekilde topladığı siber tehdit istihbarat verilerini STM analistlerinin konu ve olay bazındaki raporları ile zenginleştirerek müşterilerine sunar. Bu sayede, siber tehdit aktörlerinin aktivitelerinin tespit edilmesi, siber saldırıların gerçekleşmeden önüne geçilmesi ve koruyucu önlem alınması mümkün olmaktadır. Böylece, olası saldırılar sonucunda meydana gelebilecek finansal kayıplar ve itibar kaybı önlenebilmektedir. İstihbarat verileri (kara liste IP adresleri, alan adları, zararlı yazılım hash değerleri, zafiyet verileri), API ve STIX/TAXII aracılığıyla güvenlik cihazlarına entegre edilebilmektedir. Görev yönetimi özelliği ile tespit edilen bulgular için müşteriye manuel/otomatik olarak görev tanımlanabilmekte ve bu sayede olay takibi yapılabilmektedir.



KARA LİSTELER

- IP Adresleri
- URL & Alan Adları
- Zararlı Yazılım Hash Değerleri
- USOM Zararlı Bağlantılar

ZAFİYET LİSTESİ

- Zafiyet tanımı
- CVSS skoru
- Zafiyetin etkilediği ürünler

ANALİZ RAPORLARI

- Zararlı yazılım analiz raporları
- Siber tehdit durum raporları
- Atak yüzey analiz raporları

POTANSİYEL OLTALAMA SİTELERİ

- Kuruma yönelik oltalama saldırısı yapmak amacıyla kullanılabileceği değerlendirilen alan adlarının tespit edilmesi ve ilgili müşteriye sunulması

SOSYAL MEDYA İZLEME

- Sosyal medya platformlarından müşteriye yönelik elde edilen verilerin sunulması

GÖREV YÖNETİMİ

- Manuel ve otomatik görev tanımlamalarıyla olay takibinin yapılmasını sağlar.

SEKTÖREL SİBER İSTİHBARAT

- Müşterinin bulunduğu sektöre yönelik tehdit verileri açık kaynaklardan, çeşitli forumlardan, haber kaynaklarından ve deep/dark web üzerinden toplanarak kullanıcılara sunulmaktadır.

MARKA İZLEME

- Markaya yönelik veriler bloglardan, forumlardan, haber sitelerinden ve deep/dark web üzerinden toplanarak arayüzde kullanıcılara sunulmaktadır.

İHLAL VERİLERİ

- Tespit edilen kurumsal e-posta adreslerinin kullanıcılara sunulduğu arayüzdür. Her bir e-posta adresine ait sızıntı bilgisi, nereden sızdırıldığı ve tespit edildiği tarih bilgisi paylaşılmaktadır.

RAPORLAMA

- Raporlama özelliği ile kullanıcılar, arayüz üzerinden sunulan verileri filtreleyerek tek seferlik veya zamanlanmış rapor oluşturabilir.

API

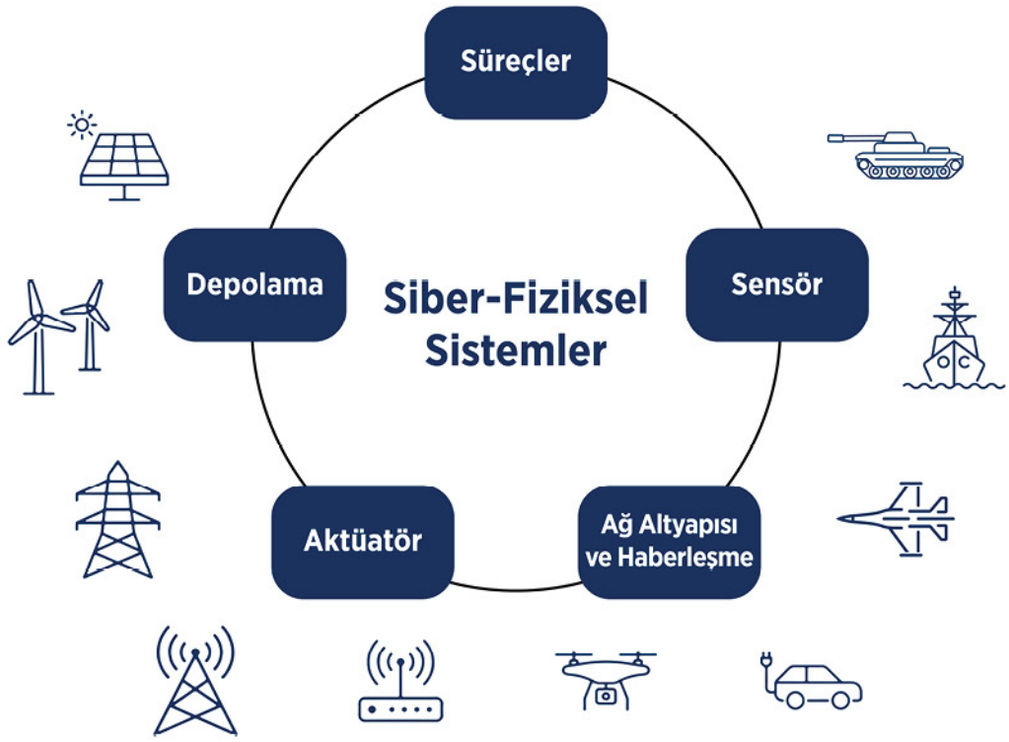
- Kara liste IP adresleri
- Kara liste alan adları
- USOM zararlı bağlantılar
- Zararlı yazılım hash değerleri
- Ürün bazlı zafiyet verisi

CYTHREAT
SİBER TEHDİT İSTİHBARATI

PLATFORM, DONANIM VE SİBER-FİZİKSEL SİSTEMLER İÇİN SİBER GÜVENLİK DANIŞMANLIK HİZMETLERİ

Kara, hava ve deniz platformları için;

- Siber Güvenlik Analizlerinin Yapılması, Mimari Oluşturma, Gereksinimlerin Belirlenmesi ve Denetlenmesi için Danışmanlık Hizmetleri
- Doğrulama, Test ve İyileştirme Hizmetleri Danışmanlığı
- Laboratuvar Kurulum/İşletim Danışmanlığı
- Platforma Özgü Ürün Projelendirme/Geliştirme Hizmetleri



ULUSAL/ULUSLARARASI İŞBİRLİKLERİ

CCDCOE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

Nato Müşterek Siber Güvenlik Mükemmeliyet Merkezi (CCD COE) tarafından düzenlenen tatbikat ve konferanslara görevli personel sağlayan kurumlar arasında yer almaktayız.

LOCKED SHIELDS

Locked shields CCDOE üyeleri arasında işbirliğini sağlamak için eşsiz bir fırsattır.

NCI AGENCY

NATO Communications and Information Agency

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

Türkiye Siber Güvenlik Kümelenmesi

ECS EUROPEAN ORGANISATION FOR SECURITY

European Organisation for Security

ECS EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Organisation

CYSPA EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

European Cyber Security Protection Alliance

TÜRKAK Personel TS EN ISO/IEC 17024 AB-0021-P

ISO 17025 - Laboratuvar ve Test

CERT AUTHORIZED TO USE CERT Carnegie Mellon University Software Engineering Institute — CARNEGIE MELLON UNIVERSITY CERT IS A REGISTERED TRADEMARK OF CARNEGIE

Computer Emergency Response Team (CERT)

TSE

TSE Sızma Testi Firma Belgesi

MISP Threat Sharing

MISP Threat Sharing

STM SAVUNMA TEKNOLOJİLERİ MÜHENDİSLİK VE TİCARET A.Ş.

Mustafa Kemal Mah. İsmail Karakaya Cad. No: 3A
İç Kapı No: 1 **Çankaya - ANKARA / TÜRKİYE**

+90 312 266 35 50
+90 312 266 35 51

www.stm.com.tr

/ @STMDefence

@stmdefenceinternational @StmDefenceInt @stm-defence-international