SİBER GÜVENLİK VE BÜYÜK VERİNİN ENDÜSTRİ 4.0'DAKİ YERİ

Ömer Korkut
Teknolojiden Sorumlu GMY

14 EKİM 2016

ENDÜSTRİLEŞMEDE SAFHALAR

1.0
- Üretimi makineleştirmek için su ve buhar gücü kullanımı

2.0
- Elektrik enerjisi ile seri üretimin önünün açılması

3.0
- Bilgi teknolojilerinden istifadeyle üretimin otomatik hale getirilmesi

4.0
- Üretimin tamamen bilgisayar kontrollü hale gelmesi ve sayısal dönüşüm

STM

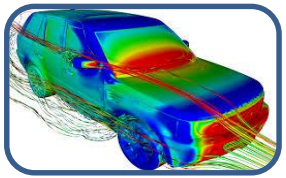
RAKAMLARLA ENDÜSTRİ 4.0

- Şirketlerin **%85**'inin, önümüzdeki **5** yıl içinde kendileri için önemli iş kollarında Endüstri 4.0 çözümlerini uygulayacakları tahmin ediliyor.
  - **2020** yılına kadar her yıl **Avrupa'da 140 Milyar Avro, küresel ölçekte 907 Milyar ABD Doları** yatırım.
- Endüstri 4.0'ın sağlayacağı esnek ve yalın üretimle, önümüzdeki **5** yılda verimliliğin ve kaynak etkinliğinin **%18** artacağı, stokların ve maliyetlerin yıllık **%2,6** azalacağı öngörülüyor.
- Almanya'da Endüstri 4.0'ın önümüzdeki **10** yıl boyunca gayrisafi yurtiçi hasılaya düzenli olarak **%1** katkı sağlaması, **390.000** yeni iş yaratması ve üretim yatırımlarını **250 Milyar Avro** arttırması bekleniyor.

STM

ENDÜSTRİ 4.0'IN YAPI TAŞI 9 TEKNOLOJİ

Otonom Robotlar



Simülasyon

Bulut Bilişim

Büyük Veri ve Analitik

Artırılmış Gerçeklik

Siber Güvenlik

Üç Boyutlu Üretim

Yatay ve Dikey Entegrasyon

Endüstriyel Nesnelerin İnterneti

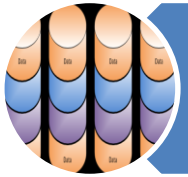
STM

BÜYÜK VERİ VE ANALİTİK

- Endüstri 4.0'ın yakıtı, **veri**.
- Hangi verinin mevcut olduğunu ve ne değer taşıdığını keşfetme devrinden, veriyi anlamlandırma ve **veriden karar üretme** devrine geçiş.

- Kurumlarda başarılı sayısal uygulamaların olmazsa olmazı, başarılı **veri analitiği**.

BÜYÜK VERİNİN V'LERİ



Büyük Hacimli Duran Veri (Volume)

(Yoğun Kurumsal Sayısallaştırma)

Çok Hızla Akan Veri (Velocity)

(Artan Sensörler ve Bağlantı İhtiyacı)

Çok Farklı Formatta Veri (Variety)

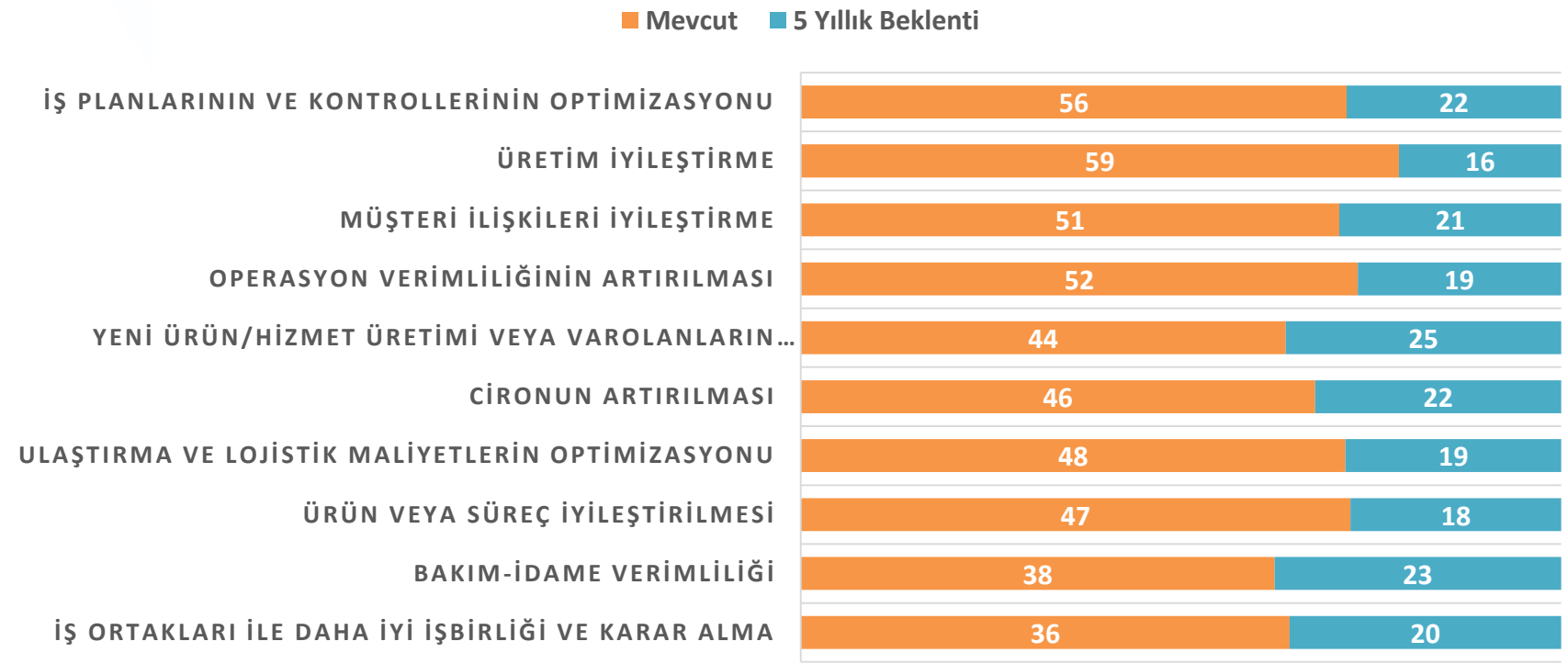
(Farklı Kaynaklarda, Farklı Maksatlarla Üretilen Veri)

Kararsız, Şüpheli, Belirsiz Veri (Veracity)

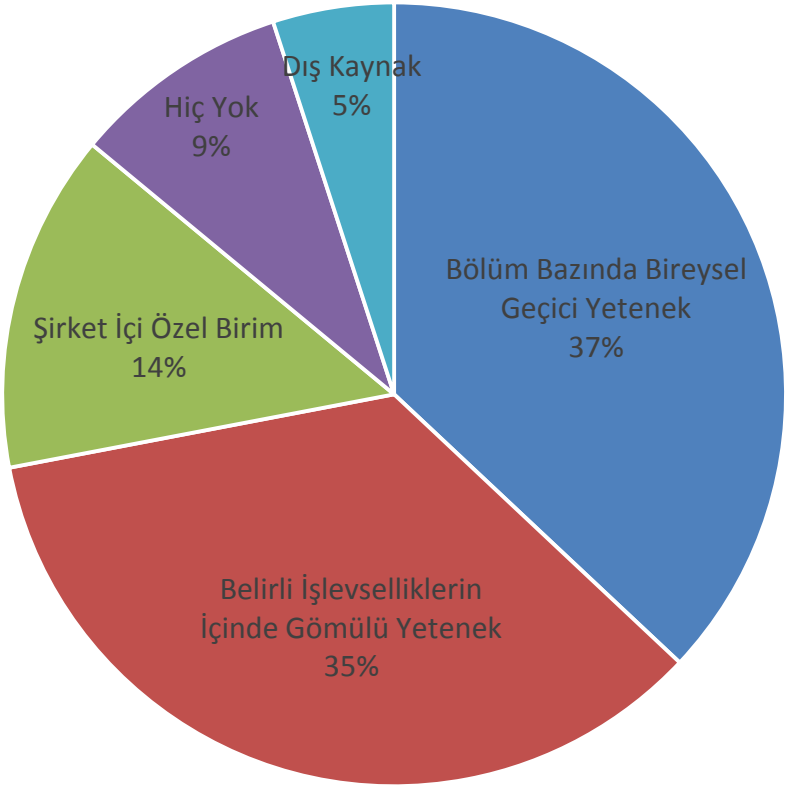
(Bütünlüğü Sağlanamamış, Eksik Kalmış Veri)

STM

BÜYÜK VERİ VE ANALİTİĞİN KULLANILDIĞI ALANLAR



VERİ ANALİTİĞİ YETENEĞİNDE MEVCUT DURUM



STM

OPTİMİZASYON İÇİN VERİ ANALİTİĞİ (OVERA)

- Büyük veri işleme ve füzyon.
- Her türlü veriyi (metin, ses, görüntü vb.) işleme kabiliyeti.
- Tüm dikey sektörler için veri analitiği ve optimizasyon yeteneği.
- Milli algoritmalar.
- STM Siber Füzyon Merkezinin büyük veri ve veri analitiği altyapısı.

ENDÜSTRİ 4.0 DEVRİNDE SİBER GÜVENLİK

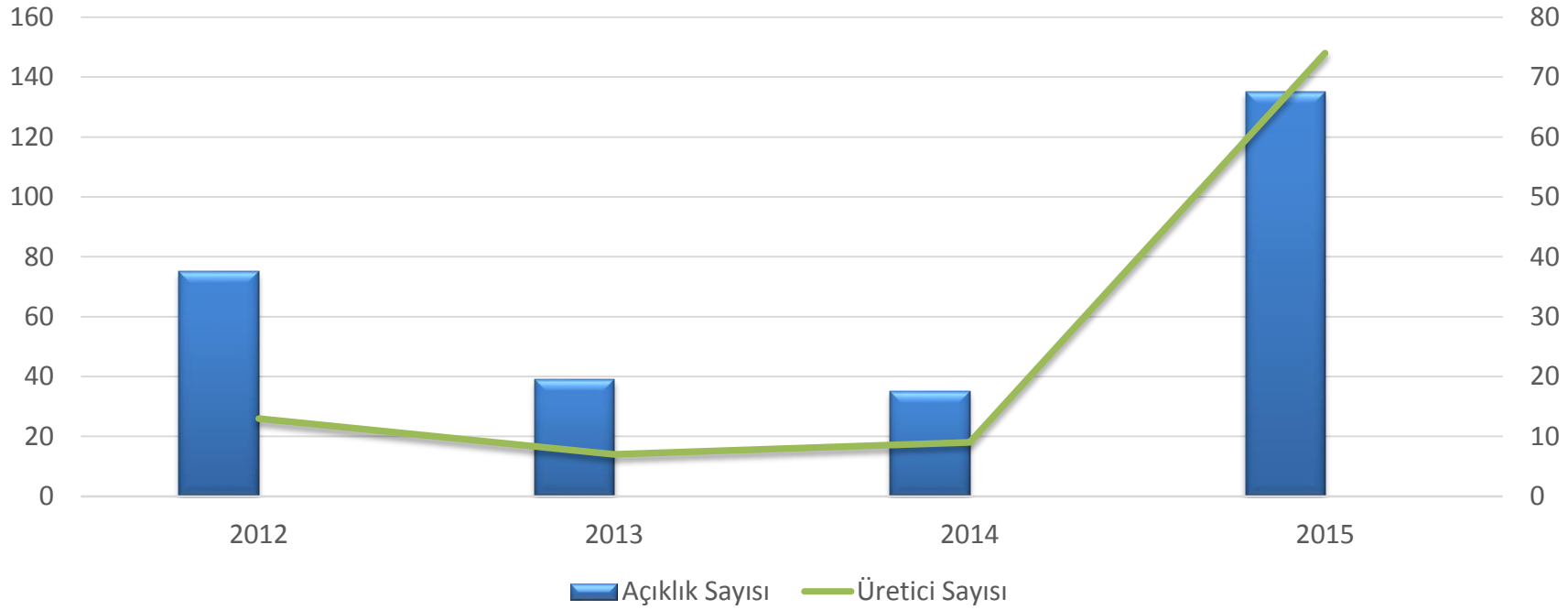
- Her gün **5,5 milyon** yeni nesne bağlantısı.
- Yıl sonunda bağlantılı nesne sayısı **6.4 milyar**.
- Sıkı bağlı sayısal ekosistemin ve yoğun veri kullanımının getirdiği siber güvenlik riskleri.
- **2015** yılında endüstride siber güvenlik sorunlarının yol açtığı kayıplarda **%38**'lik ciddi artış.

- **2015** yılında küresel ölçekte siber saldırıların yol açtığı zarar **3 Trilyon ABD Doları**. **2021**'de beklenen zarar **6 Trilyon ABD Doları**.

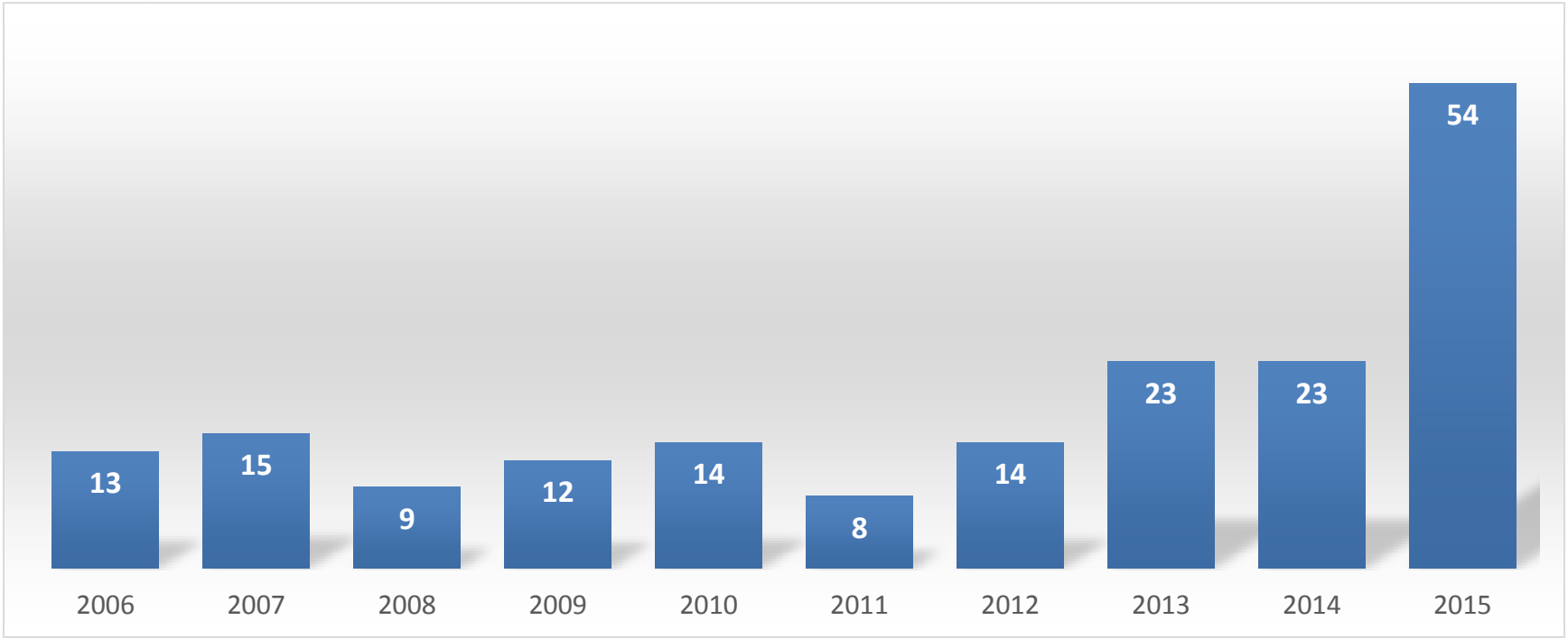
SİBER TEHDİTLER VE AKTÖRLER

Aktörler	Tehditler
Siber Korsanlar 	- DDoS atakları ile servis kesintisi, - Web sitesi tahrifi, - Zararlı yazılım yüklemesi.
Siber Suçlular 	- Fidye yazılımları, - Hassas verinin çalınması, - Endüstriyel süreçlerin sekteye uğratılması.
Casuslar 	- Entelektüel bilginin çalınması/sızdırılması, - Hedef odaklı saldırılar

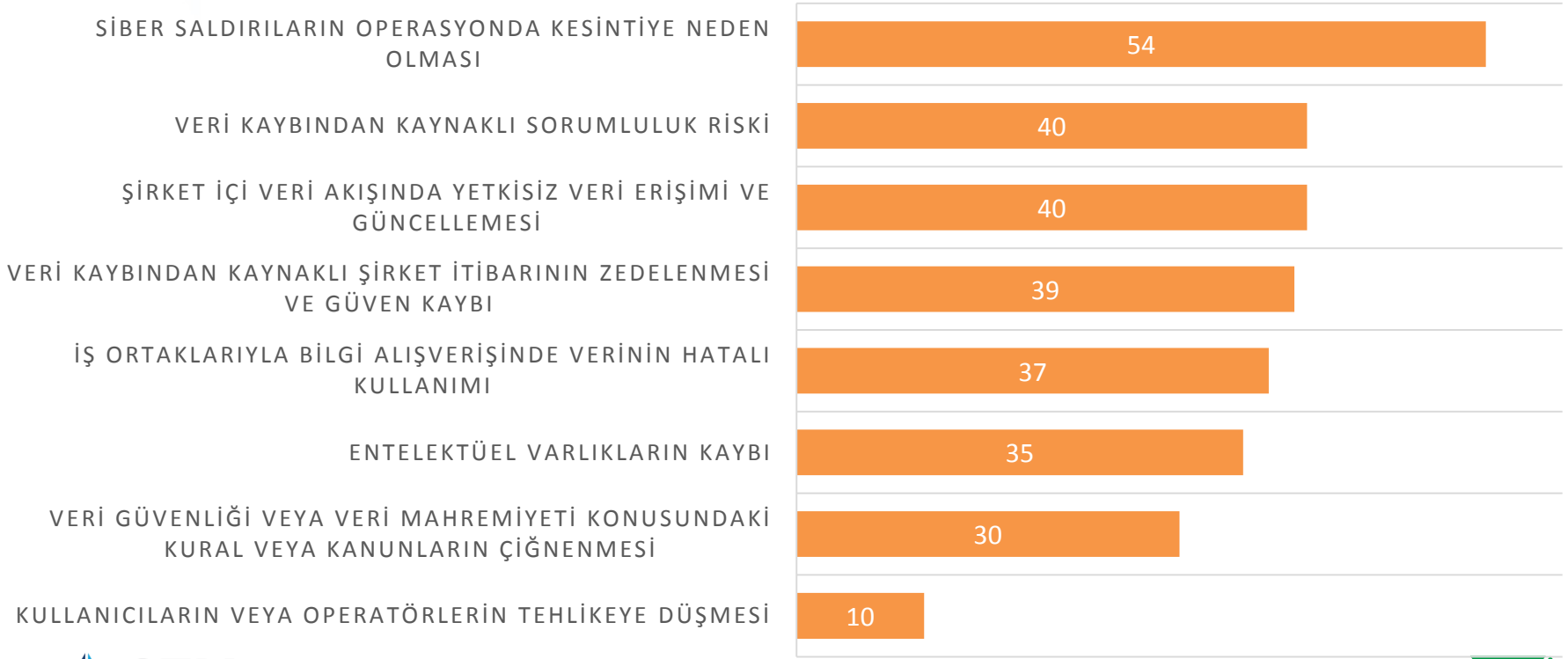
ENDÜSTRİYEL KONTROL SİSTEMLERİNİN AÇIKLIKLARI



SIFIRINCI GÜN AÇIKLIKLARI



SİBER GÜVENLİK RİSK ALGISI



STM

EN BELİRGİN ZAFİYETLER

- Bilgi güvenliği politikası eksikliği,
- Endüstriyel Kontrol Sistemleri protokollerindeki zayıflıklar,
- Korumasız ağ bağlantıları,
- Eğitimsiz personel,
- Ağ varlıklarının etkin yönetilmemesi,
- Erişim haklarının belirlenmemesi/kontrollerinin yapılmaması,
- Risk ve zafiyet analizi yapılmaması,

- Etkin uç nokta koruması eksikliği,
- Periyodik sızma testlerinin ihmali,
- Güvenli geliştirilmiş yazılım kullanılaması.

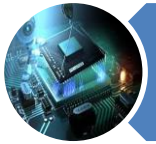
STM

STM SİBER GÜVENLİK YAKLAŞIMI

- **İnsan**, **süreç** ve **teknolojinin** bütünleştirilerek, siber güvenlik harekâtının, siber tehdit istihbaratının desteğiyle gerçekleştirilmesi.

İnsan

Süreç



Teknoloji

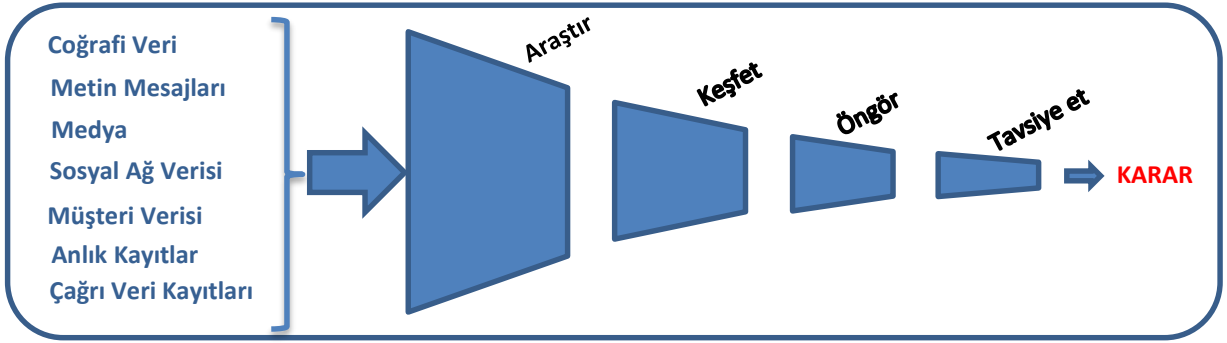
STM

STM SİBER GÜVENLİK YAKLAŞIMI

- Siber tehdit istihbaratı için gerekli veriler ancak tehdit unsurlarının ve küresel tehdit ekosisteminin **teşhisi** ve **sürekli izlenmesini** içeren bir süreçle toplanabilir.

- Bu süreçte toplanan birbirinden farklı araştırma verilerinin **tamamlanmış istihbarata** dönüştürülebilmesi, içerisinde kurallı süreçler ve gelişmiş araçlar kullanan tecrübeli **analizcilerin** görev yapacağı bir **füzyon merkezi** gerektirmektedir.

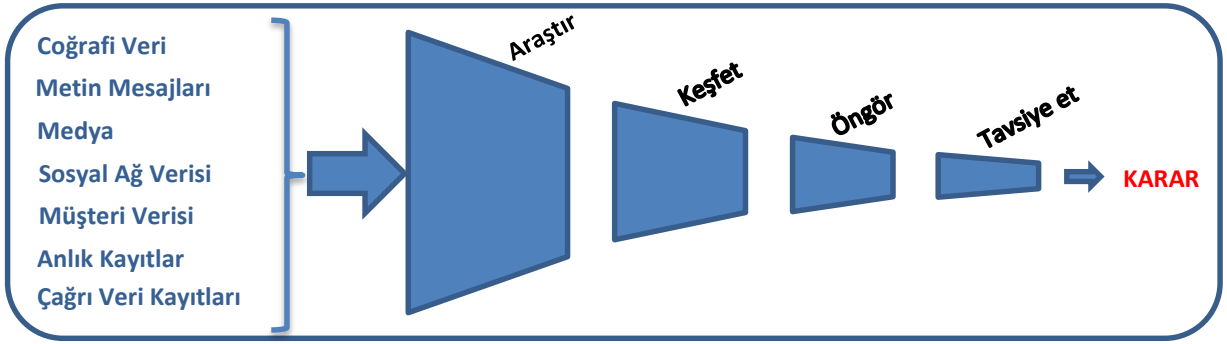
SİBER FÜZYON MERKEZİ KONSEPTİ (VERİDEN KARARA)



- **SFM'nin Araştırma ve Keşif Görevlerini Yerine Getirmek İçin İzlediği Süreç :**
  - **Veri Toplama** - Gerçek zamanlı ve durağan veri kaynakları kullanılması,
  - **Gerçek Zamanlı Veri İşleme** - Verinin alınması anında analiz edilerek gerçek zamanlı çıkarımlarda bulunulması,
  - **Verinin Saklanması** – Verinin uygun biçimde dönüştürülerek derin depolama alanlarında saklanması,
  - **Gerçek Zamanlı Uyarılar** - Tehditlerin tespit edilmesi durumunda uyarılan üretilmesi.

STM

SİBER FÜZYON MERKEZİ KONSEPTİ (VERİDEN KARARA)



- **SFM'nin Veriden Çıkarımda Bulunmak Üzere Kullandığı Bilimsel Yöntemler ve Teknikler:**
  - Makine öğrenme teknikleri,
  - İstatistik bilimi,
  - Doğal dil işleme teknikleri,
  - Kategorilendirme,
  - Ontoloji bilimi,
  - Yapay zeka teknikleri.

STM SİBER FÜZYON MERKEZİ

Siber İstihbarat Merkezi

Siber Harekât Merkezi

Zararlı Yazılım Analiz Laboratuvarı

SİBER FÜZYON MERKEZİ

MÜHENDİSLİK | TEKNOLOJİ | DANIŞMANLIK

MUSTAFA KEMAL MAHALLESİ 2151 CAD. NO 3
ÇANKAYA / TÜRKİYE

t : +90 312 266 35 50 **f** : +90 312 266 35 51

www.stm.com.tr