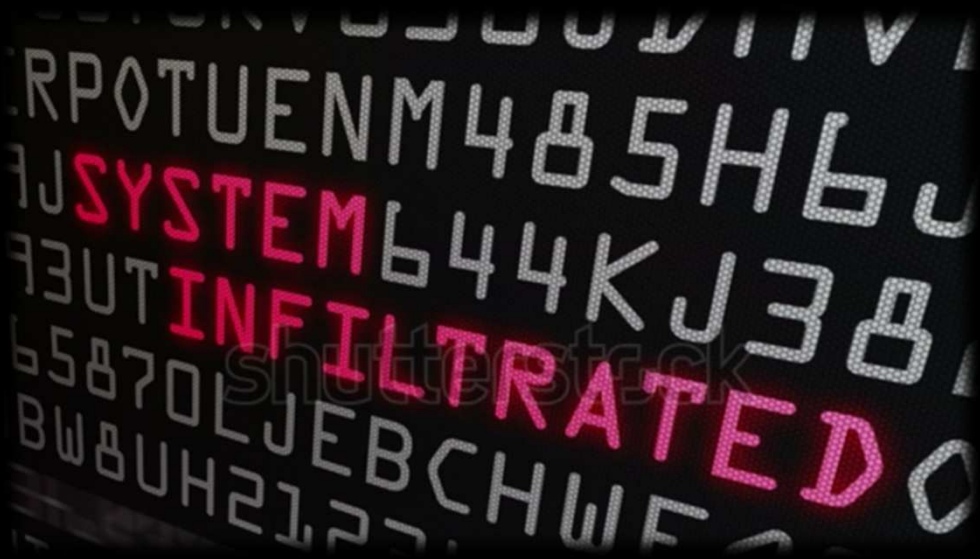
Daha Güçlü Türkiye için Etkin SOME'ler Nasıl Olmalı?



Mustafa AFYONLUOĞLU

Siber Güvenlik, e-Yönetişim ve e-Devlet Kıdemli Uzmanı

2017'DE SİBER DÜNYA

Saldırı Grubu	Kısa Adı	Ülke	Kuruluş Yılı	Motivasyonu	Hedef Kategoriler
Sandworm	Quedagh, BE2 APT	Rusya	2014	Casusluk, Sabotaj	**Hükümetler, Uluslararası Organizasyonlar, Avrupa, Amerika, Enerji Sektörü**
Fritillary	Cozy Bear, APT29, Office Monkeys	Rusya	2010	Casusluk Hükümet Devirme, Yıkma	**Hükümetler**, Düşünce Örgütleri, Medya, **Avrupa, Amerika**
Swallowtail	Fancy Bear, APT28, Sednit	Rusya	2007	Casusluk Hükümet Devirme, Yıkma	**Hükümetler, Avrupa, Amerika**
Cadelle	-	İran	2012	Casusluk	**Havayolları, İletişim, İran Vatandaşları, Hükümetler,** STK'lar
Appleworm	Lazarus	Kuzey Kore	2012	Casusluk, Sabotaj Hükümet Devirme, Yıkma	**Finans Sektörü, Askeriye, Hükümetler,** Eğlence sektörü, Elektronik Cihazlar
Housefly	Equation	ABD	2001	Casusluk	Ülke saldırganlarına yönelik hedefler
Strider	Remsec	Batı	2011	Casusluk	**Büyükelçilikler, Havayolları, Rusya, Çin, İsveç, Belçika**
Suckfly	-	Çin	2014	Casusluk	**e-Ticaret, Hükümetler,** Teknoloji, **Sağlık Sektörü, Finans Sektörü, Gemicilik Sektörü**
Buckeye	APT3, UPS, Gothic Panda	Çin	2009	Casusluk	**Askeri Alanlar, Savunma Endüstrisi,** Medya, Eğitim Sektörü, **ABD, İngiltere, Hong Kong**
Tick	-	Çin	2006	Casusluk	**Teknoloji,** Yayıncılık, **Japonya,** Su Mühendisliği

Dikkat Çekici Etkileri Olan ve Ülkeler Tarafından Desteklendiği Açıkça Bilinen Hedef Odaklı Saldırı Grupları

27 Nisan 2017 Symantec Corp. Internet Security Thread Report, Vol: 22

NATO OTAN

NORTH ATLANTIC TREATY ORGANIZATION

- **Şubat 2016**: Avrupa Birliği ile siber savunma işbirliği konusunda Teknik Düzenleme imzalandı.
- **Temmuz 2016**: Kara, Hava, Deniz ve Uzay'dan sonra **Siber Alan 5. operasyonel alanıdır.**
- **Aralık 2016**: Siber savunma, NATO'nun toplu savunma alanındaki temel görevlerinden biridir.
  - Uluslararası hukuk siber alanda da uygulanmalıdır.
  - NATO, siber eğitim ve tatbikat yeteneklerini geliştirecektir.

http://www.nato.int/cps/en/natohq/topics_78170.htm

SİBER GÜVENLİK ve MİLLİ GÜVENLİK

Milli Güvenlik: Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için **bölgesel** ve **küresel** ortamın izlenerek tehdit ve fırsatların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak **süreç ve unsurlar** (MGK)*

MİLLİ GÜVENLİK

- ASKERİ
- SİYASİ
- DİPLOMATİK
- EKONOMİK
- SİBER

NATO OTAN

2016 NATO VARŞOVA ZİRVESİ

2016: NATO Sistemlerine Saldırılar
Ayda **500** (2015'e göre %60 artış)

Ulusal Siber Güvenlik Bütçeleri
Fransa (2014): 1 Milyar € UK: **2.5 Milyar €** (2016)

2030 Siber Güvensizlik Hacmi: **90 Trilyon $**
(Denver Üniversitesi)

* http://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi
** http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm

Siber Güvenlik Üstyapısı Yakın Gelecek Planları

- ✓ Siber güvenlikte en üst seviye **Koordinasyon**
- ✓ **Milli Çözümler** ‘e en yüksek destek (Donanım/Yazılım)
- ✓ Nitelikli insan kaynağı **Kapasite Geliştirme**

Strateji ve Eylem Planı

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Sektörel Teşv

T.C BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI

Bilim, Sanayi ve Teknoloji Bakanlığı

Dü… Denetleyici Kurum

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

Bilgi Teknolojileri ve İletişim Kurumu

Operasyon ve AR-GE

Kapasite Geliştirme ve Teknik Destek

BÜSİBER BOĞAZİÇİ ÜNİVERSİTESİ SİBER GÜVENLİK MERKEZİ

Bogazici Universitesi Siber Güvenlik Merkezi

TÜBİ…

Türki… …imsel ve Tek… …ojik Araştırma Kurumu

Özel Sektör

aselsan

Electronic Industry

HAVELSAN

Air Electronic Industry

Siber İ… …hbarat

Emniyet Genel Müdürlüğü

Milli İstihbarat Teşkilatı

…ek çatı emri

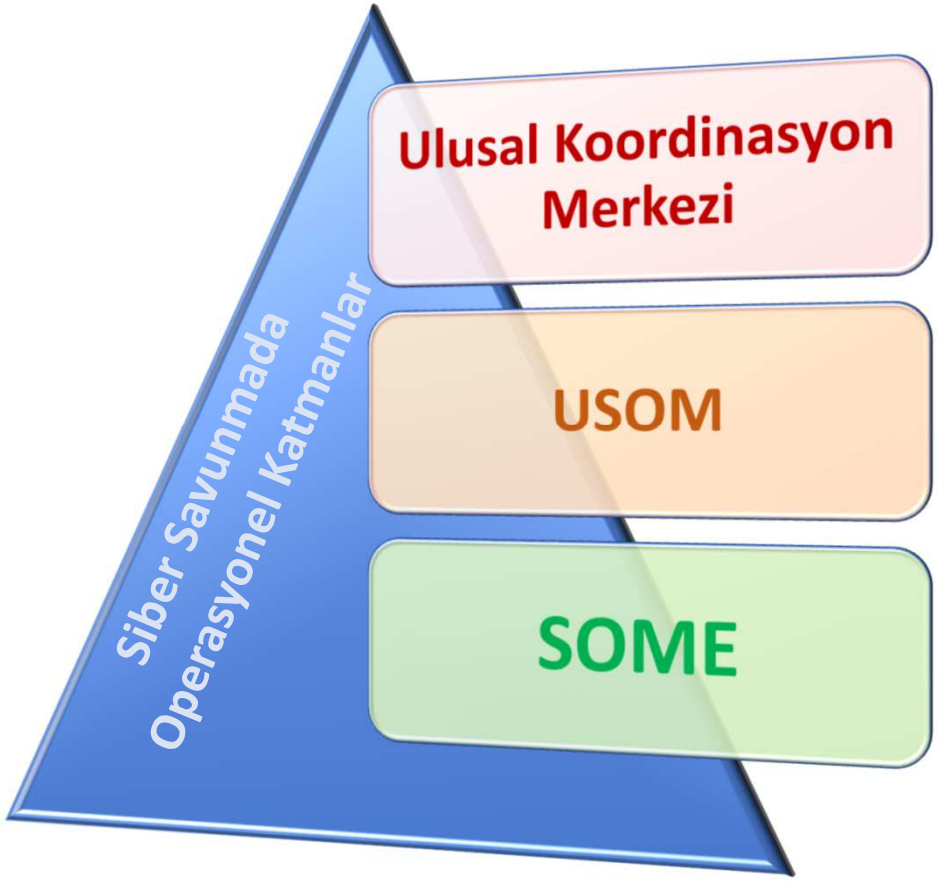
16 Şubat 2017 - 22:49| Son Güncelleme : 17 Şubat 2017 - 10:3

…venlik alanında farklı kurumlarda yürütülen çalışmaları …alışma başlattı.

…Cumhurbaşkanı Tayy… Erdoğan’ın talimatıyla başlatılan çalışmalar kapsamında, siber güv…lik altyapısının yer… …tirilmesi, durum analizi yapılması ve alınması gereken tedbirl… …rtaya konulacak. Cu… …rbaşkanı Erdoğan, FETÖ’nün 15 Temmuz darbe girişimini… …dından kurmaylarına siber güvenlik altyapısının incelenmesi için talimat verdi. Devlet Denetleme Kurulu ve Erdoğan’ın teknoloji kurmaylarının yer aldığı çalışma kapsamında Bilim, Sanayi ve Teknoloji Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ile TÜBİTAK gibi kurumlarda ayrı ayrı yapılan siber güvenlik çalışmalarının tek çatı altında birleştirilmesi planlanıyor.

http://www.hurriyet.com.tr/siber-guvenlige-tek-cati-emri-40368316

USOM, SOME ve KURUMLARIMIZ



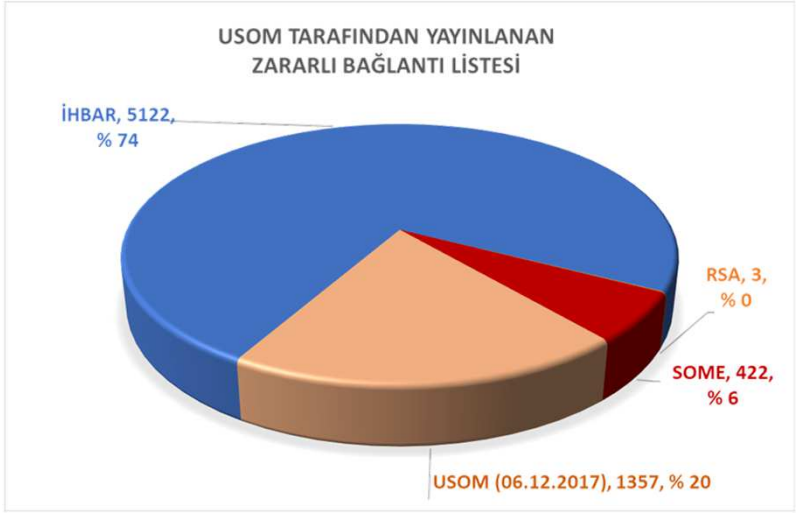
Stratejik Üst Seviye Koordinasyon

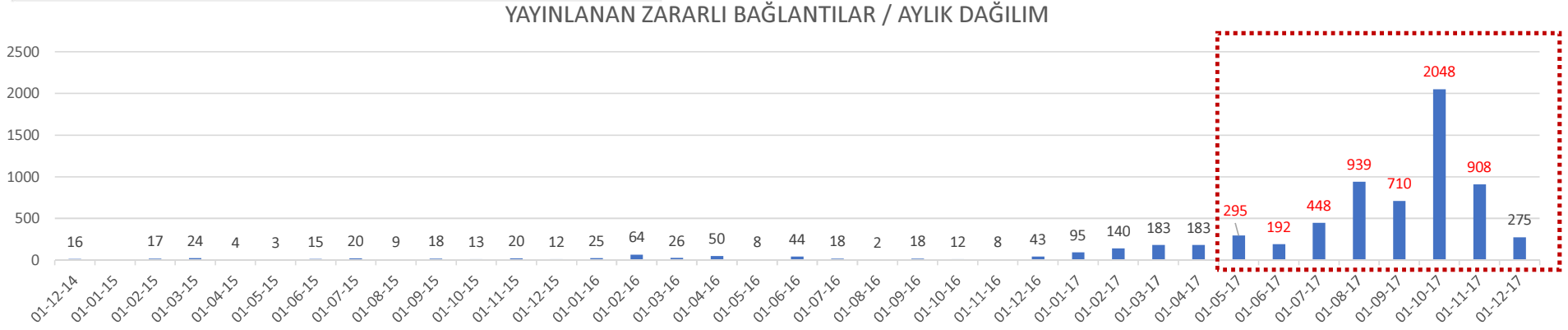
Bütüncül teknik yönetim için:
Taktik seviyede **«Komuta Merkezi»**
Teknik seviyede **«Koordinasyon Merkezi»** dir.

Kamu Kurumları ve Kritik Altyapılar için
«Siber Birlikler»

MEVCUT DURUM: USOM

SAYILARLA USOM (Aralık 2017)





https://www.usom.gov.tr/url-list.xml

SAYILARLA USOM (Aralık 2017)

2017 YILI	OCAK	ŞUBAT	MART	NİSAN	MAYIS	HAZİRAN	TEMMUZ	AĞUSTOS	EYLÜL	EKİM	KASIM	ARALIK	TOPLAM
Bankacılık-Oltalama	68	109	64	49	52	67	370	857	474	486	696	186	3478
Oltalama	22	30	18	10	80	16	6	19	121	33	8	6	369
Siber Saldırı (Port Tarama, Kaba Kuvvet vb.)		1	14	9	1	1	1				1		28
Zararlı Yazılım Barındıran/Yayan Alan Adı	2		87	115	162	108	49	63	105	1147	178	82	2098
Zararlı Yazılım Barındıran/Yayan IP	3						22		10	382	25	1	443
TOPLAM	**95**	**140**	**183**	**183**	**295**	**192**	**448**	**939**	**710**	**2048**	**908**	**275**	**6416**
Aralık ayı sadece ilk hafta verilerini içerir													

World

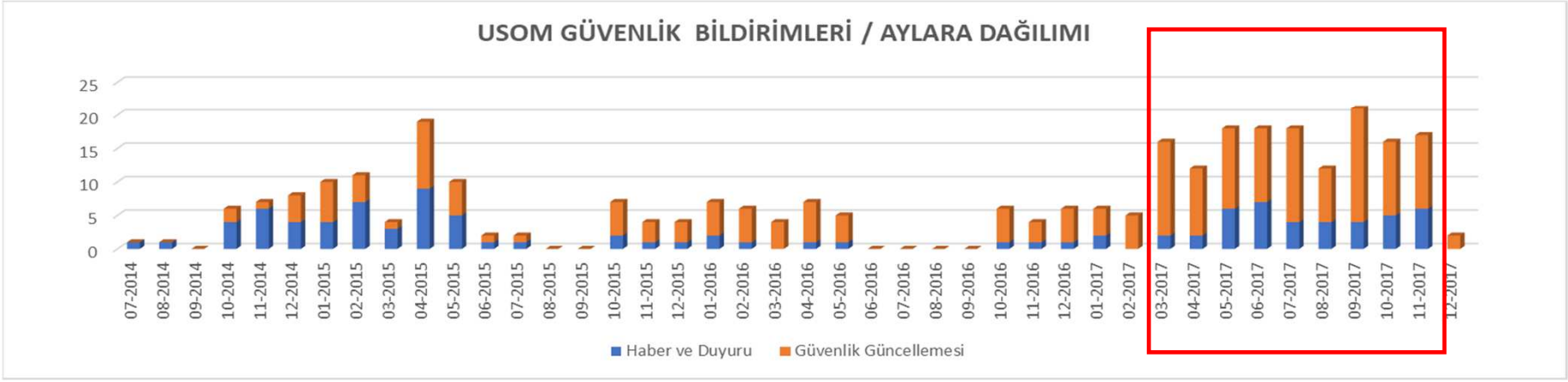
1	China	17.9 %
2	United States	10 %
3	Viet Nam	9.8 %
4	India	7.9 %
5	Brazil	3.5 %
6	Germany	2.5 %
7	France	2.4 %
8	Italy	2.3 %
9	Russian Federation	2.2 %
10	Iran, Islamic Republic Of	2.1 %
11	Mexico	2 %
12	Turkey	1.9 %
13	Indonesia	1.7 %
14	Netherlands	1.4 %
15	Pakistan	1.3 %

Europe

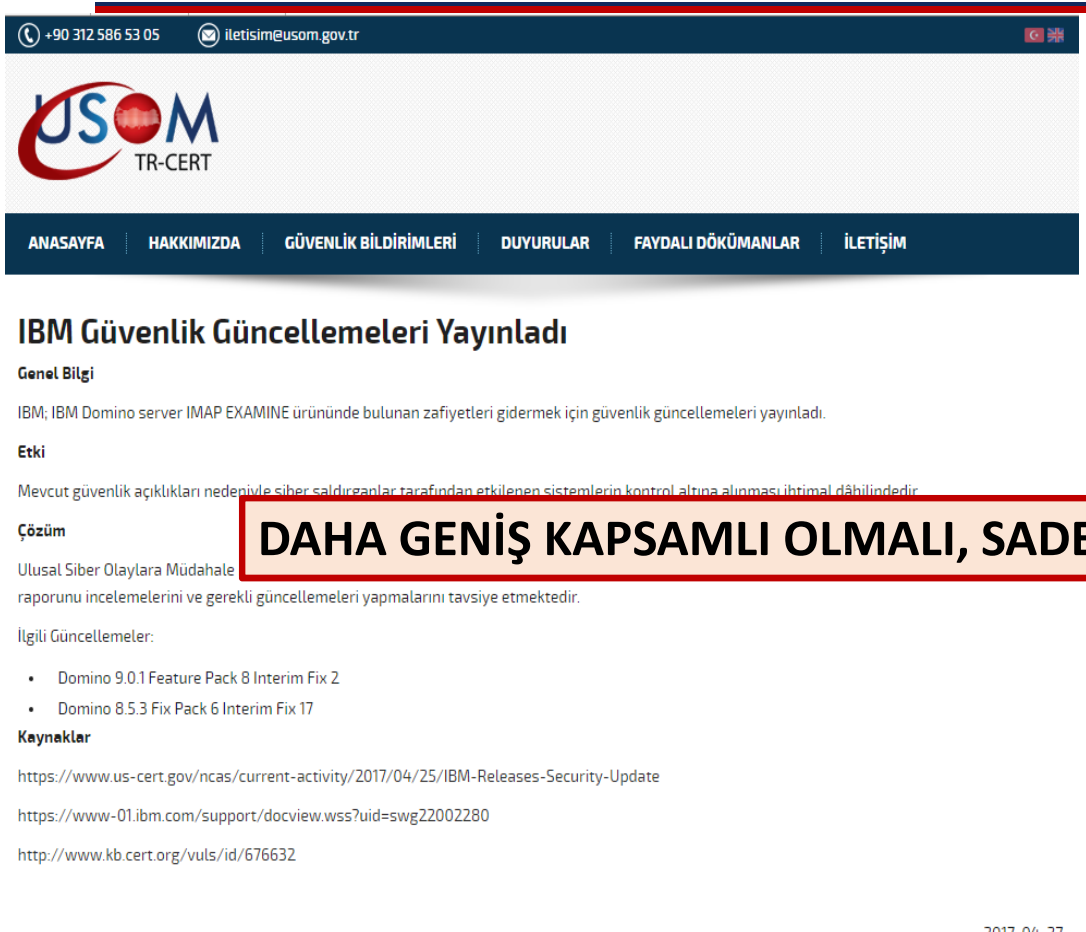
1	Germany	2.5 %
2	France	2.4 %
3	Italy	2.3 %
4	Turkey	1.9 %
5	Netherlands	1.4 %
6	United Kingdom	1 %

5 Kasım- 5 Aralık 2017 Kaspersky Spam Raporu - https://securelist.com/statistics/

SAYILARLA USOM (Aralık 2017)

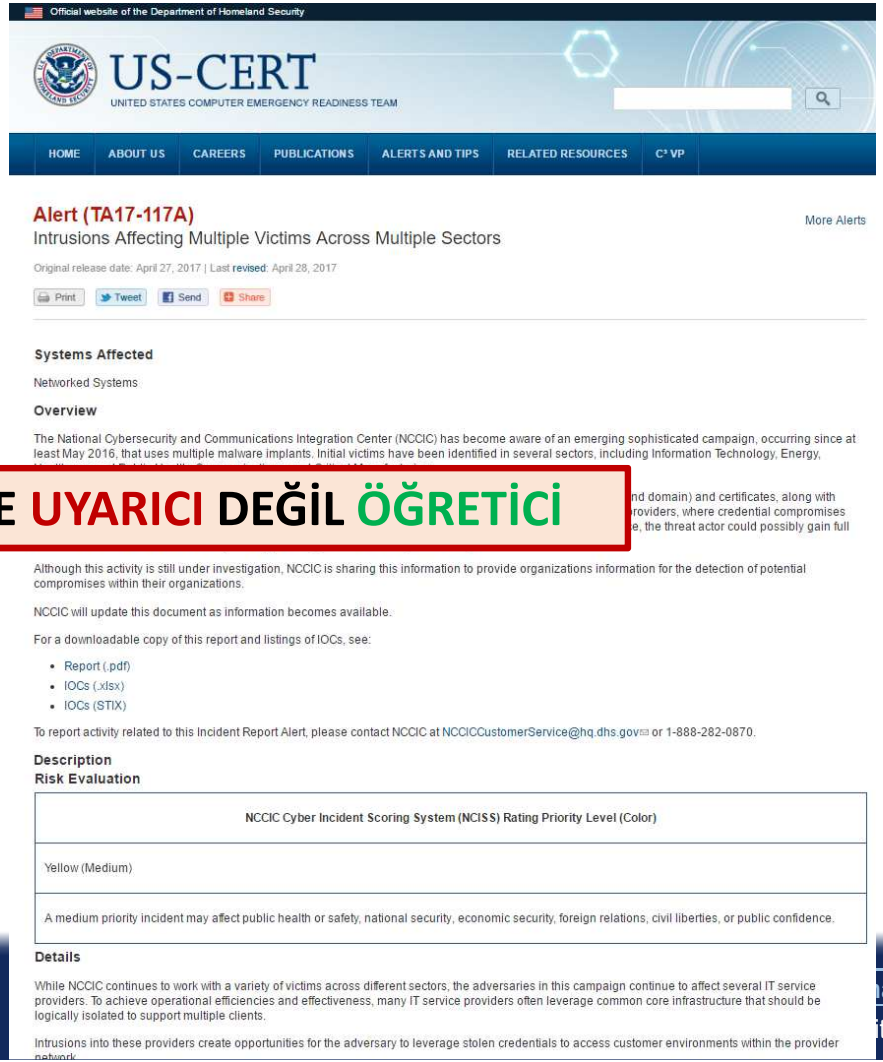


SAYILARLA USOM

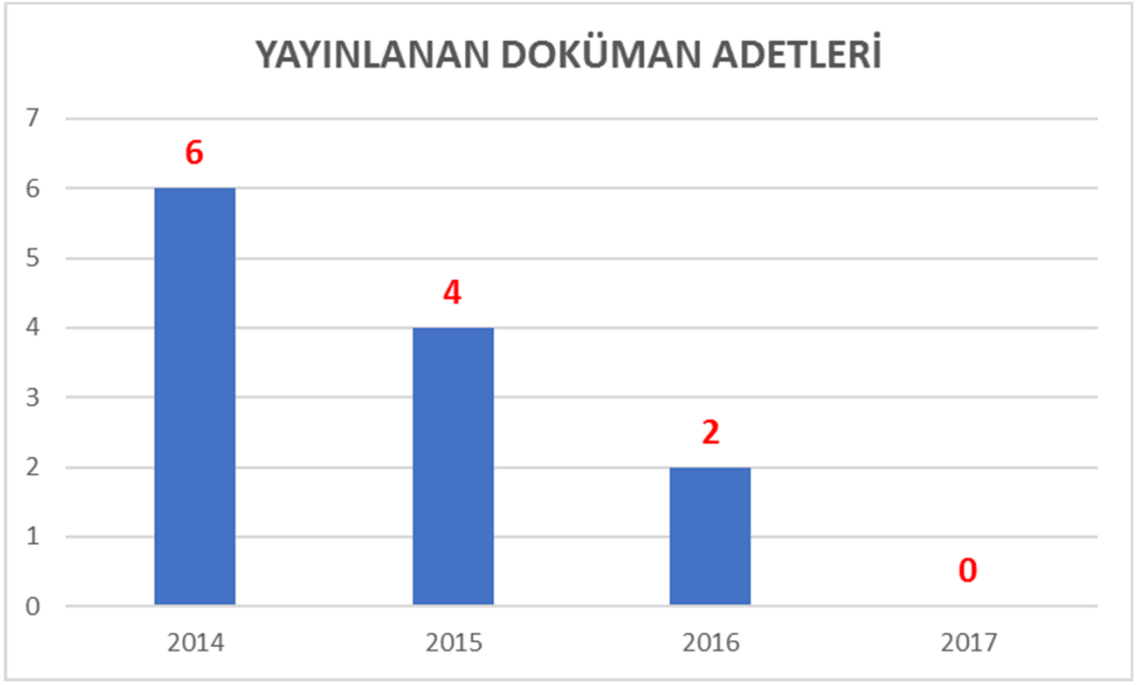


https://www.usom.gov.tr/tehdit.html

DAHA GENİŞ KAPSAMLI OLMALI, SADECE UYARICI DEĞİL ÖĞRETİCİ



SAYILARLA USOM



https://www.usom.gov.tr/tehdit.html

MEVCUT DURUM: BİLGİ İŞLEM DAİRE BAŞKANLIKLARI ve SOME'ler

BÜTÜNCÜL, ETKİN ve YETKİN İDARİ YAPI

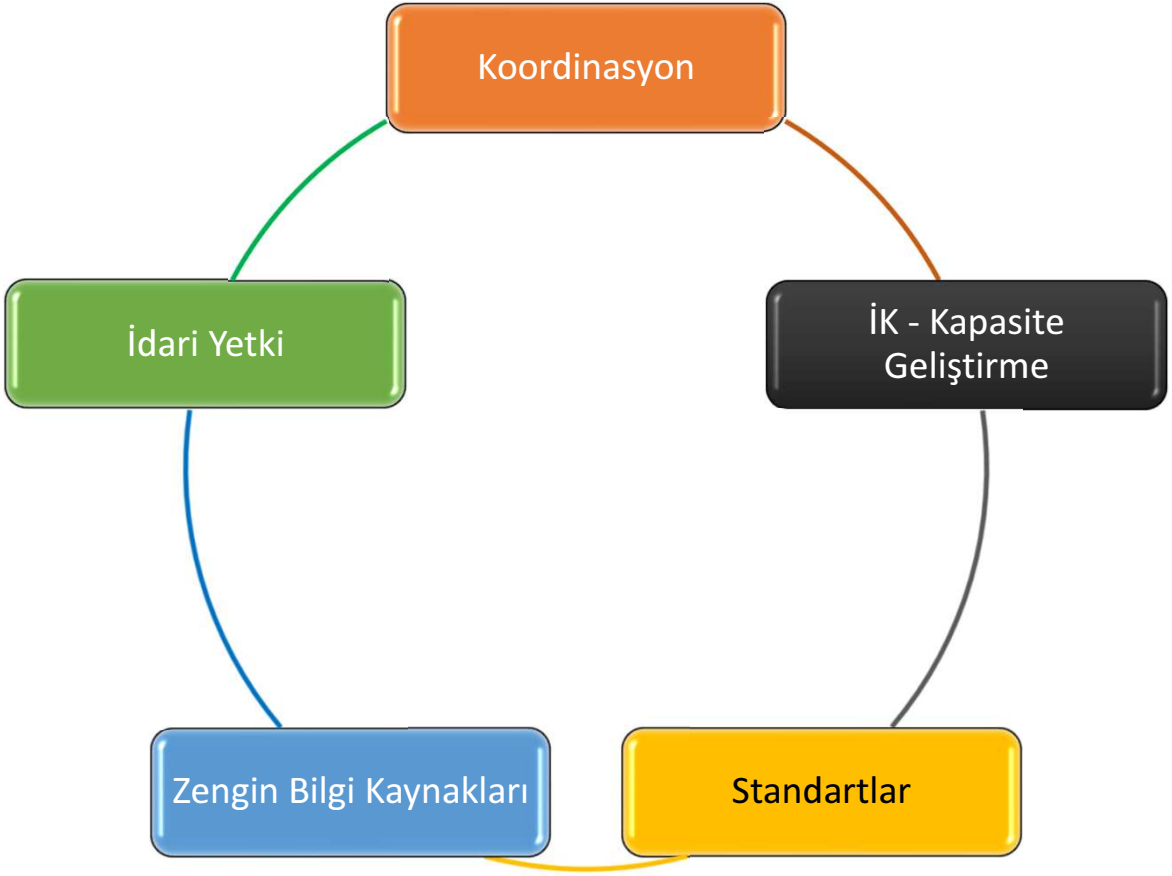
MEVCUT DURUM

BÜTÜNCÜL, ETKİN ve YETKİN İDARİ YAPI

ÖNERİLEN İDARİ MODEL

MEVCUT DURUM: SOME'LER

SOME'ler ve Kritik Bileşenler: «Ne» Gerekiyor ?



«NASIL» ?

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

11 KASIM 2013

Kurumsal SOME'lerin görev ve sorumlulukları

Madde 5: (2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar.

(8) [ve Made 7-(6)] Kurumsal (Sektörel) SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.

PROBLEMLER

- Bazı SOME ekip üyeleri, kendilerinin **SOME'de görevli** olduğunu bilmemekte
- SOME ekip üyeleri, genelde bunu **mevcut görevlerine ek olarak** yerine getirmekte
- SOME ekip üyeleri, genelde bu görevleri öncesinde, **SOME ile ilişkili bir uzmanlığa** sahip olmamakta
- SOME ekip üyelerine genelde bu alanda standartlara uygun ve **nitelikli eğitim** sağlanmamakta

USOM: Ulusal Siber Olaylara Müdahale Merkezi

KAPASİTE GELİŞTİRME ÖNERİLERİ

- USOM, SOME'ler için daha güçlü ve nitelikli bir bilgi kaynağı haline gelmeli, ilgili kurumları bu amaç çerçevesinde koordine etmelidir.
- Daha çok bilgilendirici rapor ve rehber hazırlamalıdır:
  İlgili ENISA Raporları, NIST dokümanları ve CERT Kılavuzları ('*First Responders Guide to Computer Forensics' gibi*) Türkçeleştirilebilir.
- USOM ve üniversiteler tarafından yapılan bu çalışmalar USOM sitesindeki DOKÜMANLAR kısmında kolay erişilebilir formatta yayınlanmalıdır.
- USOM sitesinde kamu, özel sektör, üniversiteler, STK, SOME ve USOM tarafından siber güvenlik alanında gerçekleştirilen/gerçekleştirilecek etkinlikler ve bunların sonucunda elde edilen sonuç bildirileri yayınlanabilir.
- Webinar'lar sağlanmalı ve sitede webinar kütüphanesi oluşturulmalıdır. Uzaktan ve 7/24 izlenebilen eğitim yaklaşımı hedeflenmelidir.
- Üniversiteler ile işbirliği içerisinde sistematik SOME eğitimleri sağlanmalı, bu eğitimlerde mutlaka pratik tecrübe oluşturacak lab'lar yer almalıdır. «Olay Müdahalesinde Yapılan Yanlışlar ve Dikkat Edilmesi Gereken Noktalar", olay müdahalelerinde etkin görev alan kurum uzmanlarından benzer tecrübe aktarım eğitimleri verilmelidir.

SOME'de NİTELİKLİ İNSAN KAYNAĞI

- **Siber Güvenlik**, **Veri Güvenliği**, **Kişisel Veri** Uzmanlıkları tanımlanmalı
- Üniversitelerdeki siber güvenlik alanındaki merkezler ve akredite edilmiş özel sektör eğitim merkezleri tarafından **uzmanlık sertifikaları** verilmeli
- Üniversitelerdeki siber güvenlik alanındaki merkezler, akreditasyon ile **uluslararası hedefler** belirlemeli: «Küresel Kapasite Geliştirme Gücü»
- Sertifika programları **pratik saha tecrübesi** de oluşturmalı, Tatbikatlara Mecburi Katılım
- USOM ve SOME'lerde **görev ön şartı** için uzmanlık sertifikası + sahada pratik tecrübe ön şart olmalı
- SOME Ekibi için **özel mali teşvik olmalı**: 7 x 24 Çalışma, Kritik Görev Alanı

Daha Güçlü Türkiye için Etkin SOME'ler Nasıl Olmalı?

Mustafa AFYONLUOĞLU
Siber Güvenlik, e-Yönetişim ve e-Devlet Kıdemli Uzmanı
afyonluoglu [at] gmail.com
Linkedin: http://linkedin.com/in/afyonluoglu
Twitter: http://twitter.com/#!/afyonluoglu
Web: afyonluoglu.org