Siber Olaylara Müdahale Ekibi (Kurumsal SOME)

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

Sunum İçeriği

GİRİŞ

SOME Temel Konular

SOME Kurulum Aşamaları

Kurumsal SOME'lerin Görev ve Sorumlulukları

BY NC ND

1. GİRİŞ

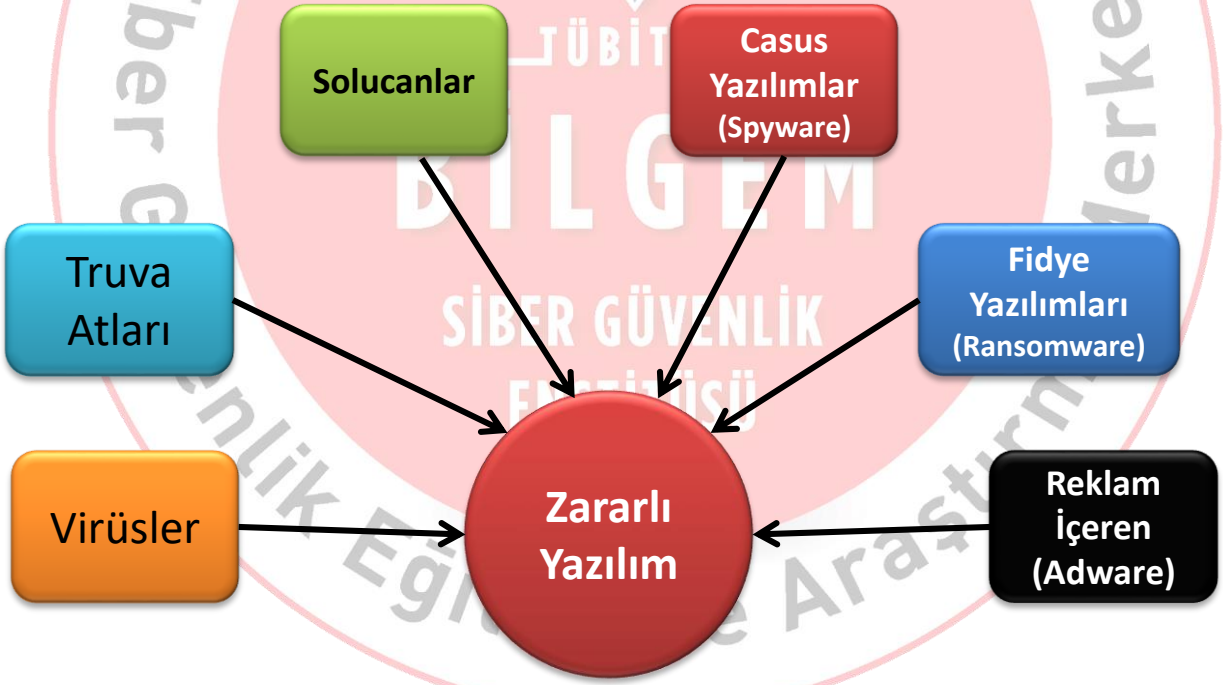
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

Zararlı Yazılımlar

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

Zararlı Yazılım Nedir?

Bir bilgisayarı veya içindeki bilgiyi sömürmek veya bilgisayarı saldırganın erişimine açmak için tasarlanmış özel yazılımdır.



cc BY NC ND

Zararlı Yazılımlar - Virüsler

- Virüsler, bulaştıkları sistemlere zarar vermek için oluşturulurlar.
- Virüslerin aktif olabilmesi için bir şekilde kullanıcı tarafından çalıştırılmaları gerekir.
- Bulaştıkları sistemlerde çalışan diğer programlara kendilerini enjekte ederler.

egitim.sge.gov.tr
TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü
Kamu Eğitim ve Araştırma Merkezi

CC BY NC ND

Zararlı Yazılımlar - Truva Atları (Trojan Horse)

- Truva atı, bilgisayar için yararlı gibi gözüken ve oltalama saldırıları kullanılarak aktif olan zararlı yazılımlardır.
- Bulaştığı sistemlere saldırganın erişimine açar.
- Amaç kullanıcı parolaları, banka hesapları, bilgi vb. verileri çalmaktır.
- Kendilerini virüsler gibi kopyalamazlar.

TÜBİTAK İLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

Zararlı Yazılımlar – Solucanlar (Worm)

- Solucanlar, dışarıdan bağımsız olarak yayılma ve kendini kopyalama kabiliyetine sahiptir.
- Bulaştıkları sistemlerde aşırı yavaşlamaya sebep olurlar.
- İşletim sistemi ve bazı programların zafiyetlerini kullanırlar.

egitim.sge.gov.tr • TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Zararlı Yazılımlar - Casus Yazılımlar (Spyware)

- Kullanıcıya ait ***bilgileri ele geçirmek*** amacı ile yazılan programlardır.
- Truva atından farkı, bulaştığı sistemi doğrudan saldırganın kullanımına açmaz. Topladığı bilgileri saldırgana gönderir.
- Bitmek bilmeyen **açılır pencerelere** neden olabilirler.
- Tarayıcımızda istem dışında araç çubukları kurabilirler.
- Web tarayıcımızda açılış sayfasının değişmesine neden olabilirler.

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü
Siber Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

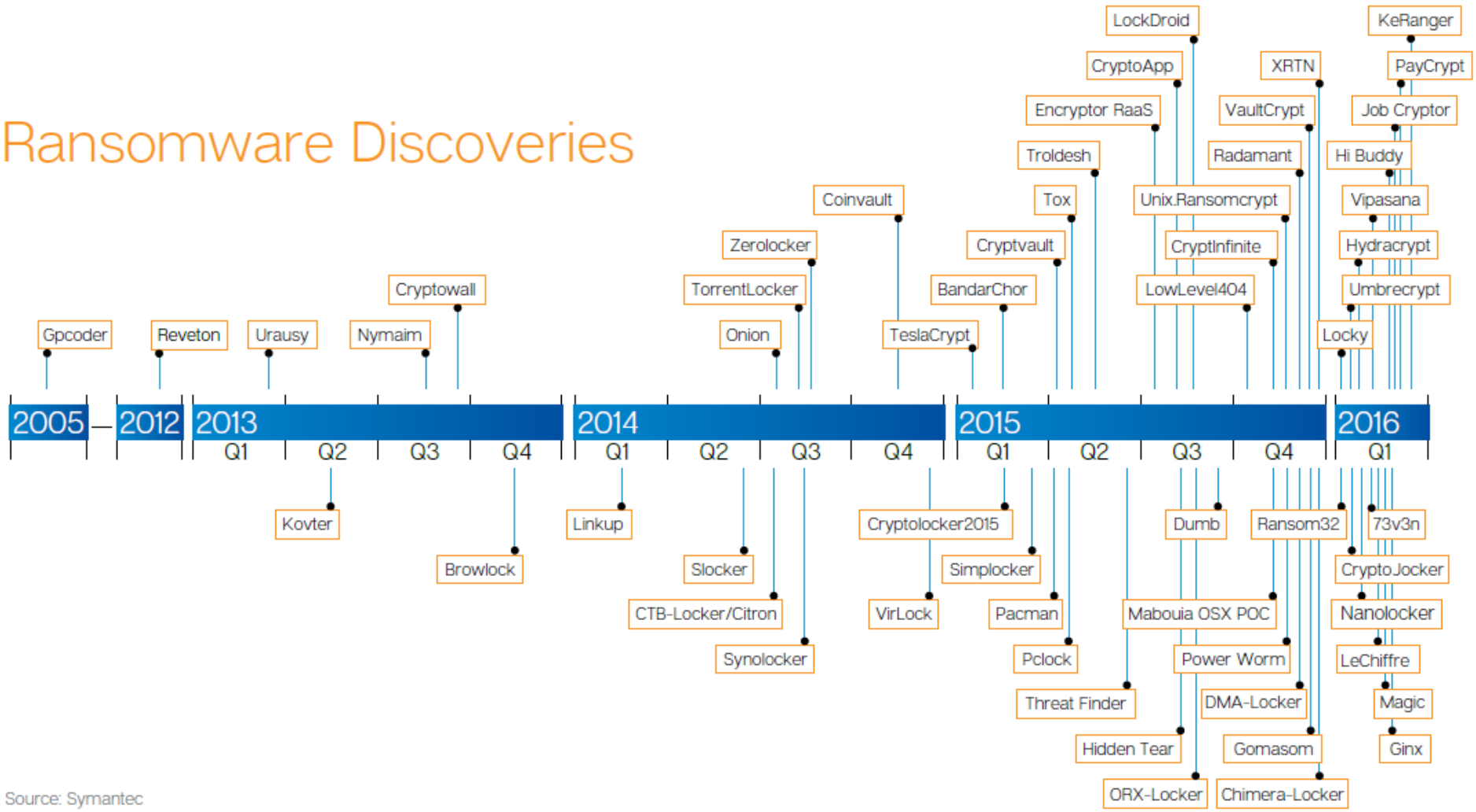
Zararlı Yazılımlar- Fidye Yazılımları (Ransomware)

- Bilgisayarınızı kullanmanıza engel olabilen,
- Dosyalarınızın ***ismini değiştirerek*** ya da dosyalarınızı ***şifreleyerek*** kullanmanıza engel olan,
- Şifreyi çözmek için karşılığında para istenen zararlı yazılım türüdür.

mrt@tubitak.gov.tr

BY NC ND

Zararlı Yazılımlar - Fidye Yazılımları



Source: Symantec

Symantec 2016 Internet Security Threat Report

BY NC ND

Zararlı Programlar – Fidye Yazılımları (Ransomware)

BY NC ND

Zararlı Yazılıma Karşı Savunma

- **Lisanslı** AV sistemleri kullanın.
- İmza dosyaları güncel olmalıdır.
- Yapılandırma yönetimi (**gereksiz portları** kapatın.)
- Uygulamaları güncel tutun (Yama yönetimi)
    - İşletim sistemleri
    - Web tarayıcılar
    - Acrobat reader, Flash player, MS Ofis vb. doküman programı ve oynatıcılar.
- E-posta eklentilerini tarayın
- USB ve hafıza kartlarını dikkatli kullanın.

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Bilgi Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

Web'de Bulunan Analiz Araçları

- Zararlı yazılım, şüpheli URL veya dosyayı online olarak inceleyebilirsiniz!
  - http://www.virustotal.com
    - Çoklu anti-virus taraması (62 tane AV)
    - URL incelemesi
  - http://whitelist.kaspersky.com/advisor#search/
    - Beyaz liste
  - https://fileadvisor.bit9.com/Services/search.aspx/
    - Beyaz liste
  - https://sitecheck.sucuri.net/
    - URL incelemesi

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
eğitim.bilgem.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

Siber Saldırgan Profilleri

- Genç Kuşak Saldırganlar
- Profesyonel Suçlular
- Endüstri ve Teknoloji Casusları
- Yabancı ülke yönetimleri ve istihbarat teşkilatları

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Bilgisayar Korsanları (Hacker)

- Hacktivistler
  - Anonymous, RedHack vs.
- Beyaz Şapkalılar
- Siyah Şapkalılar
- Gri Şapkalılar
- Script Kiddie

cc BY NC ND

Zararlı yazılım tarihçesi

1972 The Creeper virüsü (Worm)

Elk Cloner virüsü (rahatsızlık amaçlı)

Morris solucanı ve CERT CC

tim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Eğitim ve Araştırma Merkezi

Giriş - Önemli Organizasyonlar

1988 de Morris Solucanına müdahale için kuruldu

CERT/CC çalışma alanları:

Proaktif Çalışmalar

- Sistem Güvenliği
- Yazılım Güvenliği
- Kurumsal Güvenlik
- Müdahale Koordinasyonu
- Eğitim

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Giriş - Önemli Organizasyonlar

Terena Task Force Trusted Introducer

FIRST

US CERT

C SIRT

Önemli Siber Olaylar

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

2007 Estonya Krizi

- 26 Nisan 2007 tarihinde Estonya, "**Bronz Asker Heykeli**"ni yerinden kaldırmıştır.

ÖNCE

SONRA

CC BY NC ND

2007 Estonya Krizi

- **27 Nisan 2007**

  Rusya'dan kınama ve Tallinn'de gösteriler

- **27-29 Nisan 2007**

  Başlangıç seviyesi saldırılar

- **30 Nisan-18 Mayıs 2007**

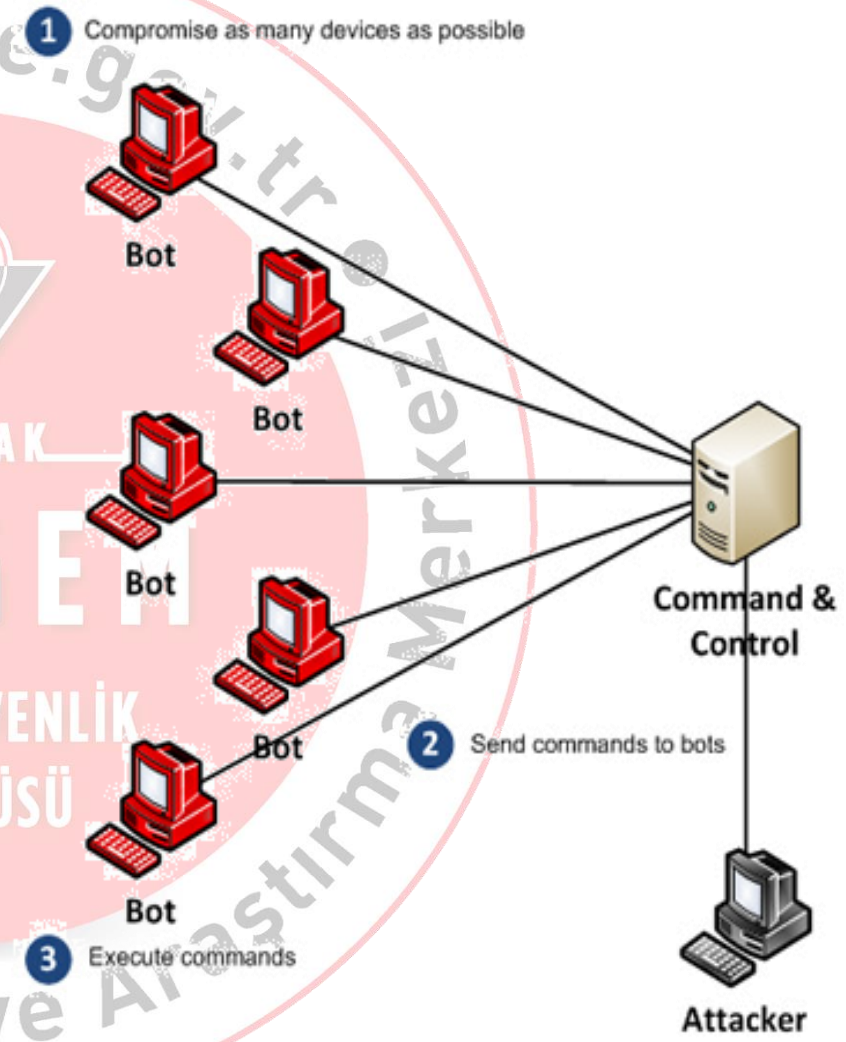
  Ulusal bilgi sistemleri, İnternet hizmet sağlayıcıları ve bankalara yönelik daha geniş katılımlı ve koordineli DDoS saldırıları

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

2007 Estonya Krizi

- İnternet bant genişliği büyük oranda saldırılar tarafından doldurulmuş ve ülkedeki İnternet sistemi çökme noktasına getirilmiştir.

- Saldırıların yönlendirildiği ülkeler arasında ABD ve AB üyesi ülkelerin de bulunduğu tespit edilmiştir. (Botnet)



eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

2007 Estonya Krizi

Radikal

< İNTERNET BASKISI >

Sanal Alem

İlk siber savaşın galibi 'Kızıl Ordu'

Geçtiğimiz ay sessiz sedasız ve yöntem olarak benzersiz bir savaş yaşandı. Rusya, Estonya'ya organize bir saldırı düzenledi ve ülkenin ticaret ve kamu düzenini dize getirmeyi başardı

04/06/2007 (6756 defa okundu)

Tanklar eşliğinde yeri göğü inleterek bir ülkeyi dize getirmek hâlâ mümkün. Ama artık başka yollar da var.

1918 yılında Alman ordularına yenilen Rusya'dan bağımsızlığını ilan eden Estonya, aynı Almanya'nın Rusya ile yaptığı gizli bir anlaşmanın ardından 1940 yılında Rus askerlerinin işgaliyle başlayan süreçte Sovyet Sosyalist Cumhuriyetler Birliği'nin bir üyesi olmak zorunda kalmıştı. 1989'da şarkılarla başlayan kıpırdanmanın ardından 1991 yılında sonunda Estonya yeniden bağımsızlığını kazandı. Ancak bu yeni süreçte Rusya'nın Estonya üstündeki hâkimiyet arzusunun söndüğü de söylenemez. Bunun son örneklerinden biri de geçtiğimiz günlerde internette yaşandı.

BY NC ND

2007 Estonya Krizi – Neden bu kadar önemli?

- Nüfusu **1.3 Milyon**
- **1 milyondan fazla** dijital kimlik kartı mevcut
- Mayıs 2007'den itibaren cep telefonlarında dijital kimlik tutulmaktadır.

- İnternet kullanımı çok yoğun

  Vergi beyanları **%80**

  Bankacılık işlemleri **%97**

  oranında İnternet üzerinden yapılmaktadır.

- Sağlık kayıtları **%100** oranında dijital ortamdadır.
- Ülke neredeyse her yerinde şifresiz kablosuz İnternet hizmeti
- Kurulan her 4 yeni şirketten 1 tanesi İnternet üzerinde kurulmaktadır.

Bu saldırılarla İnternet sistemi değil Estonya zarar görmüştür!

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
eğitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma Merkezi

Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes
Technology reporter, BBC News

23 September 2010 Last updated at 10:46 GMT

One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.

Stuxnet's complexity suggests it could only have been written by a "nation state", some researchers have claimed.

It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

It was first detected in June and has been intensely studied ever since.

Some have speculated the intended target was Iran's nuclear power plant

egitim.sge.gov.tr
TÜBİTAK BİLGİ SİBER GÜVENLİK ENSTİTÜSÜ
Eğitim ve Araştırma

CC BY NC ND

Şimdiye Kadar Geliştirilmiş En Karmaşık Siber Silah !

Stuxnet Worm Still Out of Control at Iran's Nuclear Sites, Experts Say

By Ed Barnes
Published December 09, 2010 | FoxNews.com

Iran International Photo Agency, via AFP

Aug 21: The first fuel is loaded into the reactor building at the Russian-built Bushehr nuclear power plant in Iran.

EXCLUSIVE: Iran's nuclear program is still in chaos despite its leaders' adamant claim that they have contained the computer worm that attacked their facilities, cybersecurity experts in the United States and Europe say.

The American and European experts say their security websites, which deal with the computer worm known as Stuxnet, continue to be swamped with traffic from Tehran and other places in the Islamic Republic, an indication that the worm continues to infect the computers at Iran's two nuclear sites.

The Stuxnet worm, named after initials found in its code, is the most sophisticated cyberweapon ever created. Examination of the worm shows it was a cybermissile designed to penetrate advanced security systems. It was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran's uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bashehr.

Stuxnet was designed to take over the control systems and evade detection, and it apparently was very successful. Last week President Mahmoud Ahmadinejad, after months of denials, admitted that the worm had penetrated Iran's nuclear sites, but he said it was detected and controlled.

egitim.sge.gov.tr
BILGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Bilgi Teknolojileri Eğitim ve Araştırma Merkezi

Ukrayna'da ne oldu? Elektrik santrali

- 23 Aralık 2015; 15:30
- Ivano Frankivsk
- Kırım'a karşı saldırı mı?
- 130 elektrik trafosunun 30'u devre dışı kaldı.
- 80 bin abone elektriksiz kaldı.
- i-Sight Partners, Sandworm

Siber Güvenlik Eğitim ve Araştırma
BİLGİ GÜVENLİK ENSTİTÜSÜ

Mirai Botnet Saldırısı

20 Ekim 2016

- KrebsOnSecurity'ye (Dyn DNS) DDoS Saldırısı
- Akamai tarafından host edilen KrebsOnSecurity sitesine yapılan saldırı
- Bugüne kadarki en büyük DDoS Saldırısı – 1 TBPS büyüklüğünde ve 150.000 webcam üzerinden yapılan

BY NC ND

Mirai Botnet Saldırı Analizi

Açıklık bulunan cihazlar üzerinden saldırı

- CCTV, NVR, DVR cihazları (video gözetim)
- Uydu Alıcıları
- Ağ Cihazları (Router, Hotspot ve ADSL modemler, vb.)
- Internet bağlantılı NAS cihazları (Network Attached Storage)

  - *CVE-2004-1653 - OpenSSH - TCP forwarding by default*
  - *Default Passwords*

http://blog.blackducksoftware.com/preventing-connected-devices-iot-bot

BY NC ND

Mirai Botnet Saldırısında kullanılan Parolalar

```
// root     xc3511    // root     vizxv          // root     admin
// admin    admin     // root     888888         // root     xmhdipc
// root     default   // root     juantech       // root     123456
// root     54321     // support  support        // root     (none)
// admin    password  // root     root           // root     12345
// user     user      // admin    (none)         // root     pass
// admin    admin1234 // root     1111           // admin    smcadmin
// admin    1111      // root     666666         // root     password
// root     1234      // root     klv123         // Administrator admin
// service  service   // supervisor supervisor   // guest    guest
// guest    12345     // guest    12345          // admin1   password
// administrator 1234 // 666666   666666         // 888888   888888
// ubnt     ubnt      // root     klv1234        // root     Zte521
// root     hi3518    // root     jvbzd          // root     anko
// root     zlxx.     // root     7ujMko0vizxv   // root     7ujMko0admin
// root     system    // root     ikwb           // root     dreambox
// root     user      // root     realtek        // root     00000000
// admin    1111111   // admin    1234           // admin    12345
// admin    54321     // admin    123456         // admin    7ujMko0admin
// admin    1234      // admin    pass           // admin    meinsm
// tech     tech
```

BY NC ND

ABD Seçimlerinde Rusya

"Two US State Election Systems Hacked to Steal Voter Databases — FBI Warns."

29 Ağustos 2016

"The NSA Chief Says Russia Hacked the 2016 Election."

16 Kasım 2016

http://www.motherjones.com/politics/2016/11/will-congress-investigate-russian-interference-2016-campaign

BY NC ND

ABD'den 35 Rus diplomat için sınır dışı kararı

*"ABD Başkanı Barack Obama, "**başkanlık seçimlerine siber saldırı iddiaları**" kapsamında Rusya'ya karşı aldığı yaptırım kararlarını açıkladı.*

Bu kapsamda başkent Washington ve San Francisco'da görevli 35 Rus diplomatın 72 saat içinde ülkeyi terk etmesi istendi.

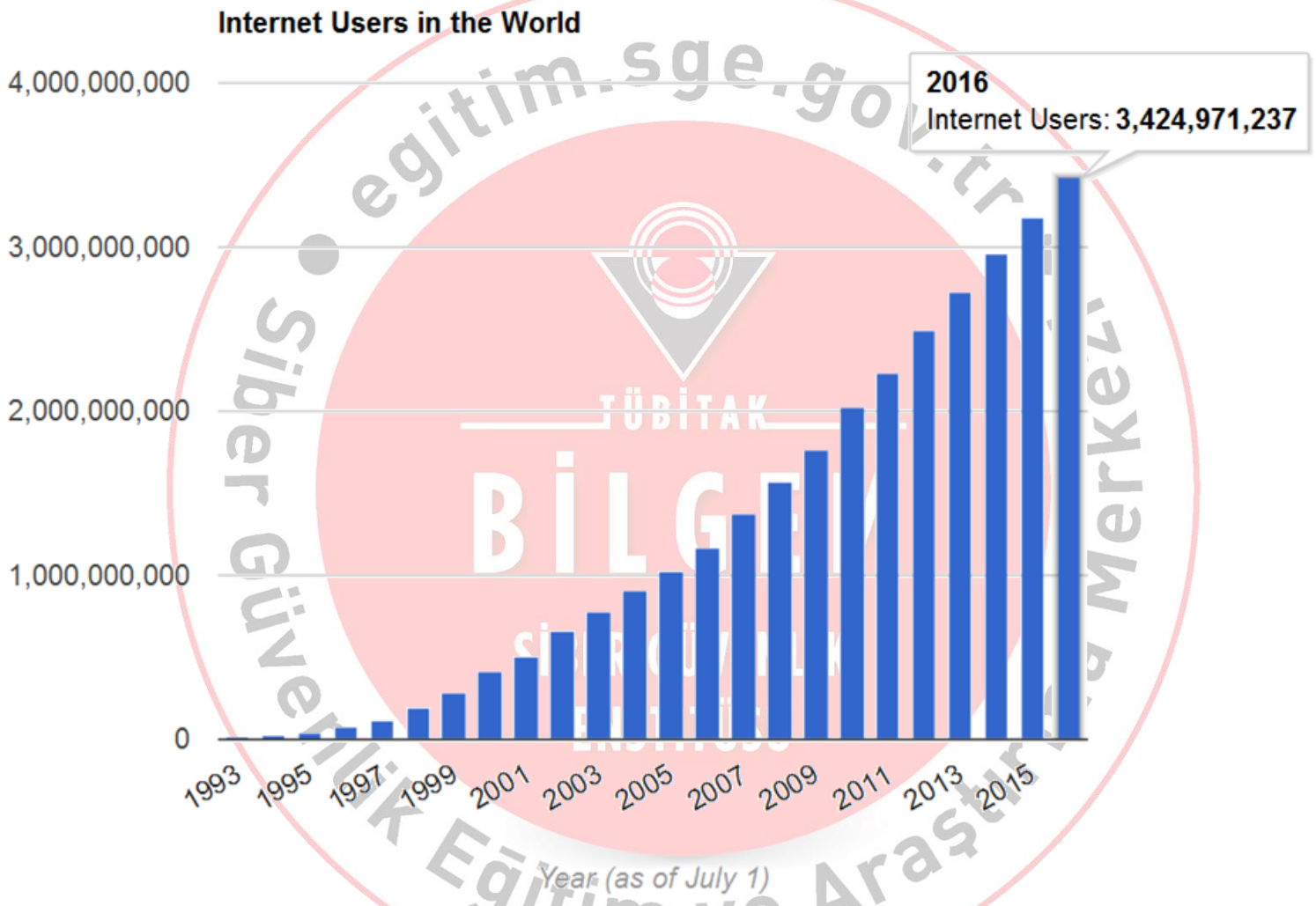
BY NC ND

http://www.hurriyet.com.tr/son-dakika-abdden-35-rus-diplomat-icin-sinir-disi-karari-40321533

Neden Siber Güvenlik?

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

Siber Uzay (Internet)



http://www.internetlivestats.com/internet-users/

CC BY NC ND

Siber Uzay (Internet)

#	Country	Internet Users (2016)	Penetration (% of Pop)	Population (2016)	Non-Users (internetless)	Users 1 Year Change (%)
1	China	721,434,547	52.2 %	1,382,323,332	660,888,785	2.2 %
2	India	462,124,989	34.8 %	1,326,801,576	864,676,587	30.5 %
3	U.S.	286,942,362	88.5 %	324,118,787	37,176,425	1.1 %
4	Brazil	139,111,185	66.4 %	209,567,920	70,456,735	5.1 %
5	Japan	115,111,595	91.1 %	126,323,715	11,212,120	0.1 %
6	Russia	102,258,256	71.3 %	143,439,832	41,181,576	0.3 %
7	Nigeria	86,219,965	46.1 %	186,987,563	100,767,598	5 %
8	Germany	71,016,605	88 %	80,682,351	9,665,746	0.6 %
9	U.K.	60,273,385	92.6 %	65,111,143	4,837,758	0.9 %
10	Mexico	58,016,997	45.1 %	128,632,004	70,615,007	2.1 %
11	France	55,860,330	86.4 %	64,668,129	8,807,799	1.4 %
12	Indonesia	53,236,719	20.4 %	260,581,100	207,344,381	6.5 %
13	Viet Nam	49,063,762	52 %	94,444,200	45,380,438	3.3 %
14	Turkey	46,196,720	58 %	79,622,062	33,425,342	5.1 %
15	Philippines	44,478,808	43.5 %	102,250,133	57,771,325	4.4 %

http://www.internetlivestats.com/internet-users-by-country/

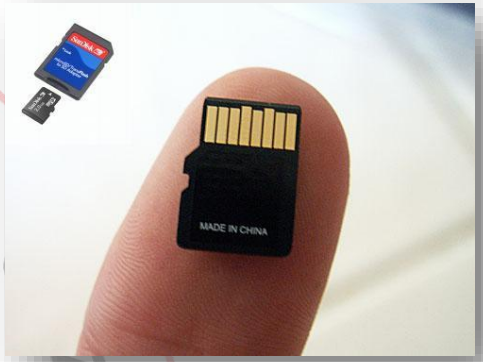
cc BY NC ND

GİRİŞ - Bilgi Güvenliği Gereksinimi

- **Bilgi Teknolojileri bağımlılık**
- **Değerli Bilgi Kaynakları**
  - Ticari / Askeri açıdan gizli bilgi
  - Müşteri, tedarikçi ve personele ait bilgiler
  - Fikri mülkiyet
  - Kurumsal birikim
- **Kanun ve sözleşmelerden kaynaklanan yükümlülükler**

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

GİRİŞ - Bilgi Güvenliğinin Artan Önemi



- ***Bilgisayar ve bilgisayar ağı sistemleri***
  Bilgi, merkezi olarak toplanıyor ve işleniyor
  Bilgiye erişim olanaklarının artması

- ***Kayıt ve depolama teknolojilerindeki gelişmeler***
  Hafıza kartları, yazılabilir diskler, sayısal fotoğraf makineleri vb…

- ***Bilgi teknolojilerinin günlük hayata girmesi***

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ

BY NC ND

GİRİŞ - Bilgi Teknolojilerinin Günlük Hayata Girmesi

2- SOME Temel Konular

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

2. SOME Temel Konular:

Mevzuat Altyapısı

egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ

DAYANAK

- “5809 sayılı Elektronik Haberleşme Kanununun 5 inci Maddesi 1 inci fıkrasının (h) bendi”,
- “11.06.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı”
- “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”
- “Tebliğ”e dayanılarak hazırlanmıştır.
- Siber Güvenlik Kurulu Kararları
- K-SOME ve S-SOME rehberleri

BY NC ND

5809 Elektronik Haberleşme kanunu

h) (Ek: 6/2/2014-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, Siber Güvenlik Kurulunun sekretaryasını yapmak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.

cc BY NC ND

Bakanlar Kurulu Kararı

20 Ekim 2012 CUMARTESİ Resmî Gazete Sayı : 28447

BAKANLAR KURULU KARARI

Karar Sayısı : 2012/3842

Ekli "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ın yürürlüğe konulması; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 11/6/2012 tarihli ve 1159 sayılı yazısı üzerine, Bakanlar Kurulu'nca 11/6/2012 tarihinde kararlaştırılmıştır.

Abdullah GÜL
CUMHURBAŞKANI

Recep Tayyip ERDOĞAN
Başbakan

B. ARINÇ
Başbakan Yardımcısı

A. BABACAN
Başbakan Yardımcısı

B. ATALAY
Başbakan Yardımcısı

B. BOZDAĞ
Başbakan Yardımcısı

S. ERGİN
Adalet Bakanı

F. ŞAHİN
Aile ve Sosyal Politikalar Bakanı

E. BAĞIŞ
Avrupa Birliği Bakanı

N. ERGÜN
Bilim, Sanayi ve Teknoloji Bakanı

H. YAZICI
Çalışma ve Sosyal Güvenlik Bakanı V.

E. BAYRAKTAR
Çevre ve Şehircilik Bakanı

A. DAVUTOĞLU
Dışişleri Bakanı

M. Z. ÇAĞLAYAN
Ekonomi Bakanı

T. YILDIZ
Enerji ve Tabii Kaynaklar Bakanı

S. KILIÇ
Gençlik ve Spor Bakanı

M. M. EKER
Gıda, Tarım ve Hayvancılık Bakanı

H. YAZICI
Gümrük ve Ticaret Bakanı

İ. N. ŞAHİN
İçişleri Bakanı

C. YILMAZ
Kalkınma Bakanı

E. GÜNAY
Kültür ve Turizm Bakanı

M. ŞİMŞEK
Maliye Bakanı

Ö. DİNÇER
Milli Eğitim Bakanı

İ. N. ŞAHİN
Milli Savunma Bakanı V.

V. EROĞLU
Orman ve Su İşleri Bakanı

R. AKDAĞ
Sağlık Bakanı

B. YILDIRIM
Ulaştırma, Denizcilik ve Haberleşme Bakanı

Bakanlar Kurulu Kararı

TÜBİTAK

ULUSAL SİBER GÜVENLİK ÇALIŞMALARININ YÜRÜTÜLMESİ, YÖNETİLMESİ VE KOORDİNASYONUNA İLİŞKİN KARAR

Amaç ve kapsam

MADDE 1- (1) Bu Kararın amaç ve kapsamı, kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemektir.

Siber Güvenlik Kurulu

MADDE 4- (1) Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur.

CC BY NC ND

USGEB 2013-2014

Madde 4	SOME ile İlgili alt eylem maddeleri
Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması	- Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması ve işletilmesi için çalışma esaslarının belirlenmesi, rehber dokümanların ve eğitim planının hazırlanması
	- Kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması, ekiplerin oluşturması, eğitimlerin alınması
	- Sektörel SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi - Sektörel SOME'lerin USOM'un sağladığı destekten yararlanması
	- Kamu kurumlarında SOME'lerinin kurulması
	- Kamu kurumları SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi - Kurumsal SOME'lerin varsa bağlı oldukları sektörel SOME ve USOM'un sağladığı destekten yararlanması

BY NC ND

11.11.2013 tarihli Tebliği

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar

1.Bölüm

- Amaç ve Kapsam
- Dayanak
- Tanımlar

2.Bölüm

- Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME)
- Kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması
- USOM'un sektörel SOME'lerin doğrudan koordinasyonunda faaliyet yürütmesi
- Kamu kurumlarında SOME'lerinin kurulması
- Kamu kurumları SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi

CC BY NC ND

Siber Güvenlik Kurulu Kararları

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar

2.Siber Güvenlik Kurulu Toplantısı

20/06/2013

- Kurumsal SOME'lerin bakanlıklarda ve ilgili kurum kuruluşlarda UDHB eşgüdümünde
- Sektörel SOME'lerin ise Denetleyici Düzenleyici Kurumlarda BTK eşgüdümünde oluşturulması ve gelişmelerin bir sonraki SGK toplantısına sunulması

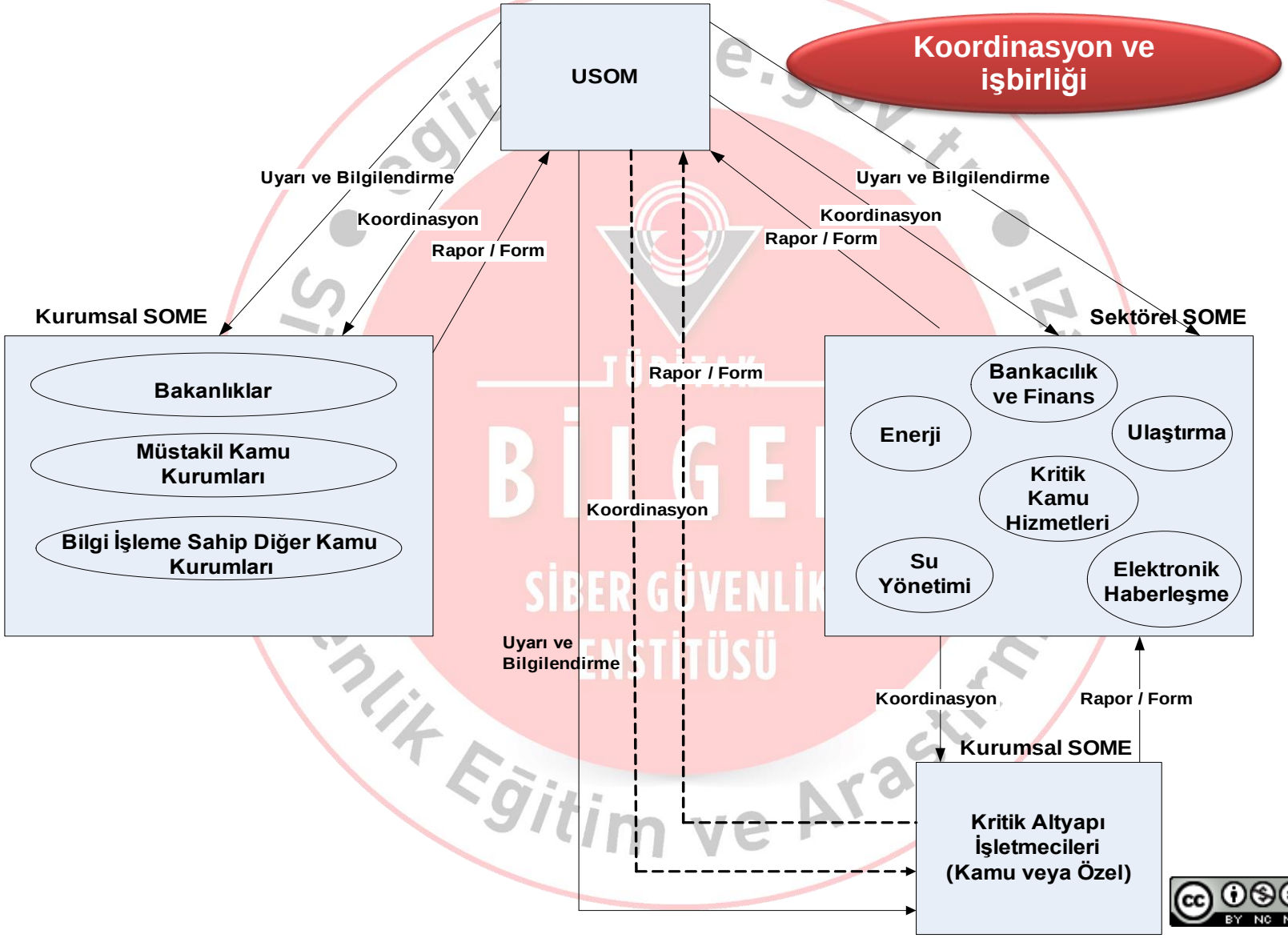
egitim.sge.gov.tr
Eğitim ve Araştırma Merkezi

Ulusal Siber Güvenlik

Organizasyon	Kurulduğu Kurum / Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	Kritik sektörü düzenleyici ve denetleyici kurumlar Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

cc BY NC ND

Ülkemizdeki Ulusal Koordinasyon



cc BY NC ND

Sektörel SOME

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum
Enerji	İlgili düzenleyici ve denetleyici kurum
Elektronik Haberleşme	
Finans	
Su yönetimi	Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık
Kritik Kamu Hizmetleri	
Ulaştırma	

Her bir kritik altyapı sektörü için Sektörel SOME kurulacaktır

Eğitim ve Ara

BY NC ND

SOME Rehber Dokümanları

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Haberleşme Genel Müdürlüğü

Sektörel SOME Kurulum ve Yönetim Rehberi

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Haberleşme Genel Müdürlüğü

Kurumsal SOME Kurulum ve Yönetim Rehberi

CC BY NC ND

3 - SOME Kurulum Aşamaları

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Enstitüsü

SOME Kurulum

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

SOME Nedir?

- Siber olayları bertaraf etmek/azaltmak oluşması muhtemel zararları önlemek veya azaltmak
- Siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliğinin sağlanması
- Ulusal işbirliği ve koordinasyon için kurum ya da kuruluşların bünyesinde etkin ve verimli bir Kurumsal SOME'nin kurulması,
- Kurumsal SOME'nin USOM ve varsa bağlı olduğu Sektörel SOME ile diğer Kurumsal SOME'lerle koordineli çalışması ve işbirliği halinde olması

USGEP 2013-2014 Eylem Planı'na göre K-SOME'ler Eylül 2014'e kadar kurulması öngörülmüştür(!).

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma
CC BY NC ND

Olay Yönetimi İhtiyacı

Kurumsal Bilgi

Kişisel Bilgi

Metodoloji/Plan/Sistem

Değerlendirme/uygun metod

Çalınmaya veya yok olma zararını azaltır

Daha kısa sürede sistem çalışır hale gelir

Tecrübe/Öğrenme

Sistem sıkılaştırma/İyileştirme

TÜBİTAK
SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve

cc BY NC ND

Yönetim desteği

- SOME kurulması için olmazsa olmazlardan biri yönetim desteğidir.
- Yönetim Desteğinin Somut Göstergeleri
  - Önemli SOME toplantılarının bazılarına katılım veya temsilci gönderilmesi,
  - Bilgi güvenliği bilinçlendirme faaliyetlerine katılım,
  - Üst yönetim için hazırlanan raporların incelenmesi ve geri besleme verilmesi,
  - Kurum güvenlik politikalarının uygulatılması,
  - Önemli güvenlik uyarılarının yönetim aracılığıyla duyurulması

eğitim.sge.gov.tr
TÜBİTAK BİLGEM
Güvenlik Farkındalık Eğitim Merkezi

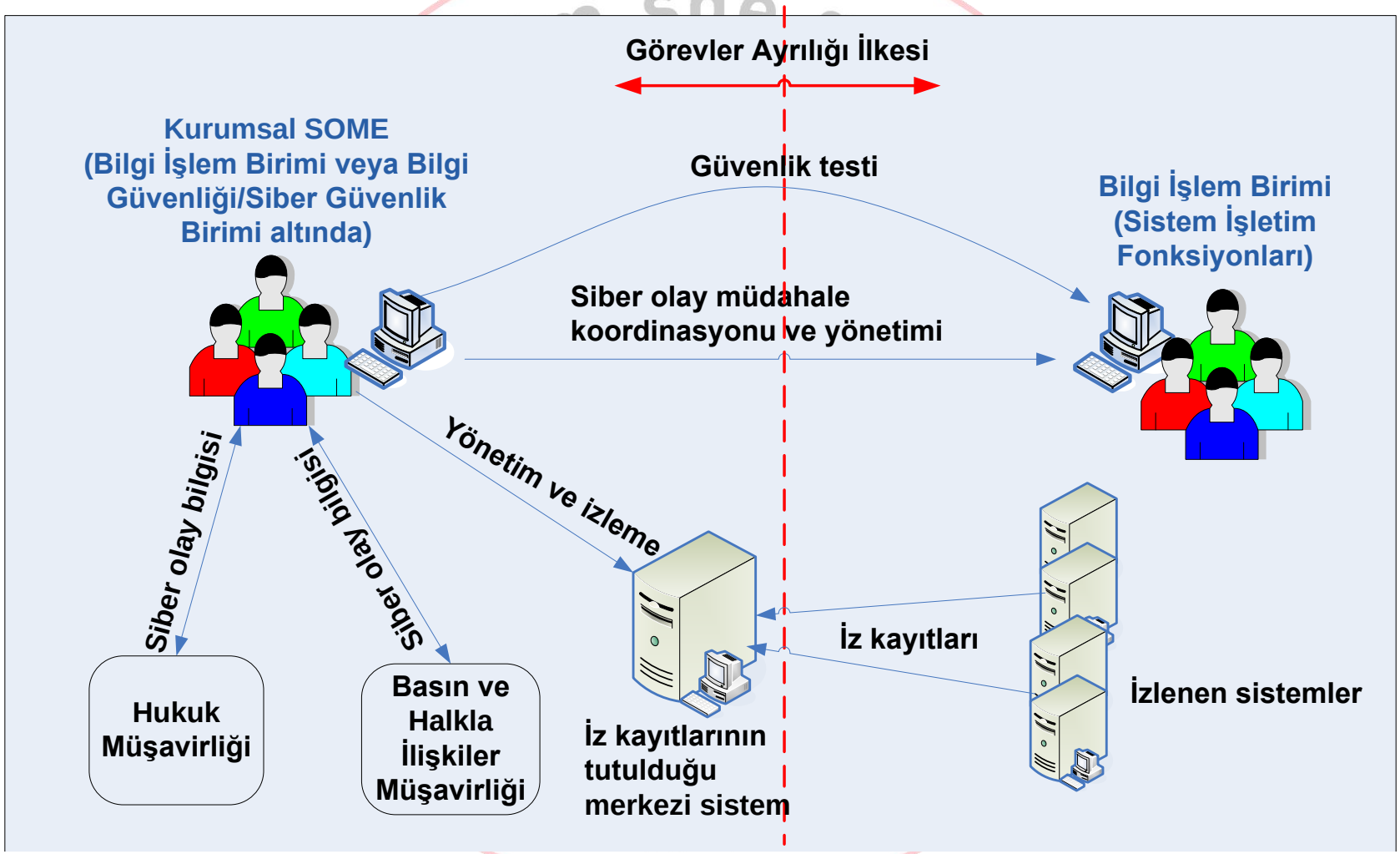
2- SOME Görev ve Sorumluluk Alanı

ÖRNEK: USOM Sorumluluk alanı

SOME Çeşidi	Görevi	Sorumluluk Alanı
Uluslararası Koordinasyon Merkezi	Diğer SOME'lerle koordinasyon içerisinde olarak dünyada geçerli olan güvenlik tehditleri ile ilgili bilgi sahibi olmak. SOME'ler arasında güven ilişkisini sağlamak.	Dünyadaki diğer SOME'ler
Kuruluş	Kuruluşta meydana gelen güvenlik olaylarına müdahale edilmesi ve olay sonrası elde edilen bilgilerin kuruluş güvenliğinin arttırılması amacıyla kullanılması	Kuruluştaki sistem yöneticileri ve kullanıcıları
Teknik	Belirli bir BT ürününün güvenlik seviyesinin arttırılması	Ürünün kullanıcıları

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

3 Kurum içi Paydaşlar; Bilgi Işlem ve K-SOME



BY NC ND

SOME görevleri

İdari

- Politikalara uygun faaliyet göstermek
- Yetkili makamlarla iletişime geçmek, kayıt vb veriyi yetkili makamlara aktarmak
- Olaya müdahale etmek, müdahale edilmesine yardımcı olmak

Teknik

- Rutin Güvenlik testleri yapar, yaptırır
- Rutin iz kayıtlarını takip eder
- Siber olay esnasında bilgi işlem biriminin yapacağı müdahaleyi yönetir

TÜBİTAK BİLGİ SİBER GÜVENLİK

SOME'nin kurum içerisindeki yeri

1. Kurum İçerisindeki Yeri ve Kapasite Planlaması

Kurumsal SOME,

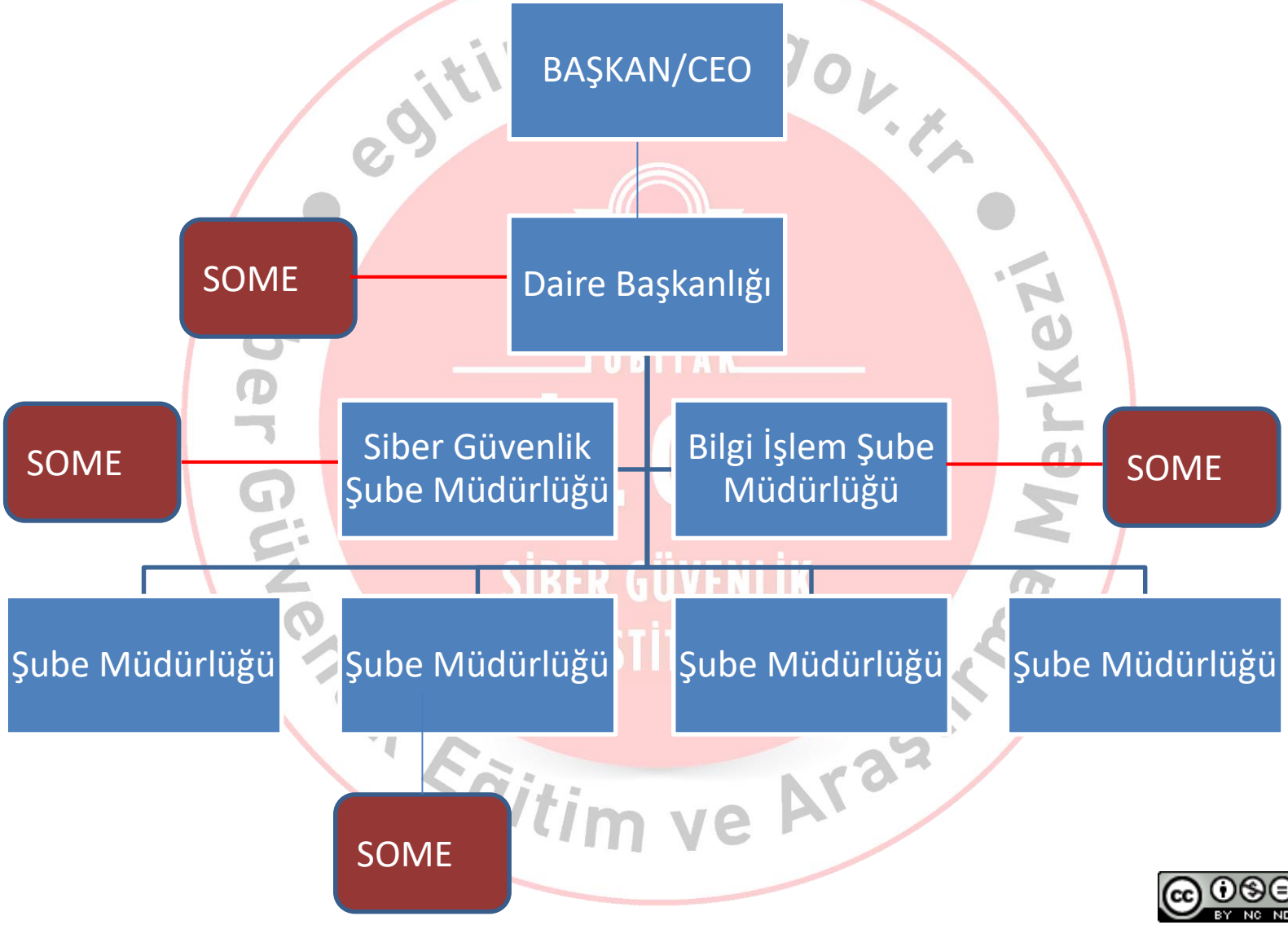
- Şube müdürlükleri
- Daire başkanlığında,
- Bilgi işlem birimi
- Bilgi işlem birimi dışında (Hukuk, İdari İşler, Strateji)
- Daha önce kurulmuş olan siber güvenlik biriminde kurulabilir.

2. SOME sorumlusu/amiri kim olmalı?

- Temel sorumluluğu siber güvenlik olan bir amir yönetiminde, bir birim olarak kurulması tavsiye edilir.
- Kurumsal SOME amirinin en az lisans derecesine sahip olan ve bilgi güvenliği/siber güvenlik konusunda uzmanlaşmış personel

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

2- Kurum İçerisindeki Yeri (Tartışma)



CC BY NC ND

Tartışma 1:

Kurumsal SOME'nin kurumsal organizasyondaki yeri neresi olmalı? Artıları ve Eksileri nelerdir?

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
TÜBİTAK
CC BY NC ND

SOME Birimleri/Faaliyet Alanları

Kurumsal SOME

- SOME birimi yönetimi fonksiyonu
- Olay müdahale yönetim ve koordinasyon fonksiyonu
- Sistem test ve denetimi fonksiyonu
- Kurumsal siber güvenlik bilinçlendirme fonksiyonu
- İz kayıt analiz fonksiyonu

Kurumsal SOME Fonksiyonları

TÜBİTAK
Siber Güvenlik Eğitim ve Araştırma Merkezi
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

İletişim & Koordinasyon

Paydaşlarla koordinasyon ve işbirliği

a. «Teknolojik çözüm ortakları»
   a. Bilgi işlem birimi,
   b. İnternet servis sağlayıcı, vb.
b. «İdari çözüm ortakları»
   a. USOM (Teknolojik + İdari),
   b. Sektörel SOME,
c. «Hukuki çözüm ortakları»
   a. Hukuk müşavirliği,
   b. Savcılık,
   c. Kolluk kuvveti ve
d. Basın müşavirliği

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
egitim.sge.gov.tr

Kurum Dışı Paydaşlarla İletişim Esasları

TÜBİTAK

EK-1 SOME iletişim Formu

EK-2 Siber olay Bildirim Formu

EK-3 Siber olay Değerlendirme Formu

7/24 Ulaşılabilir

Faaliyet Raporu

Sektörel SOME'ye verilir, yıllık verilir

SOME

Siber Olay Müdahale Raporu

Kurumsal Siber Güve
Risk değerlendirme
Risk Analizi raporu

Yıllık oluşturulur

Siber olay müdahale sonrası oluşturulur, USOM ve Sektörel SOME'ye verilir.

Eğitim ve Araş

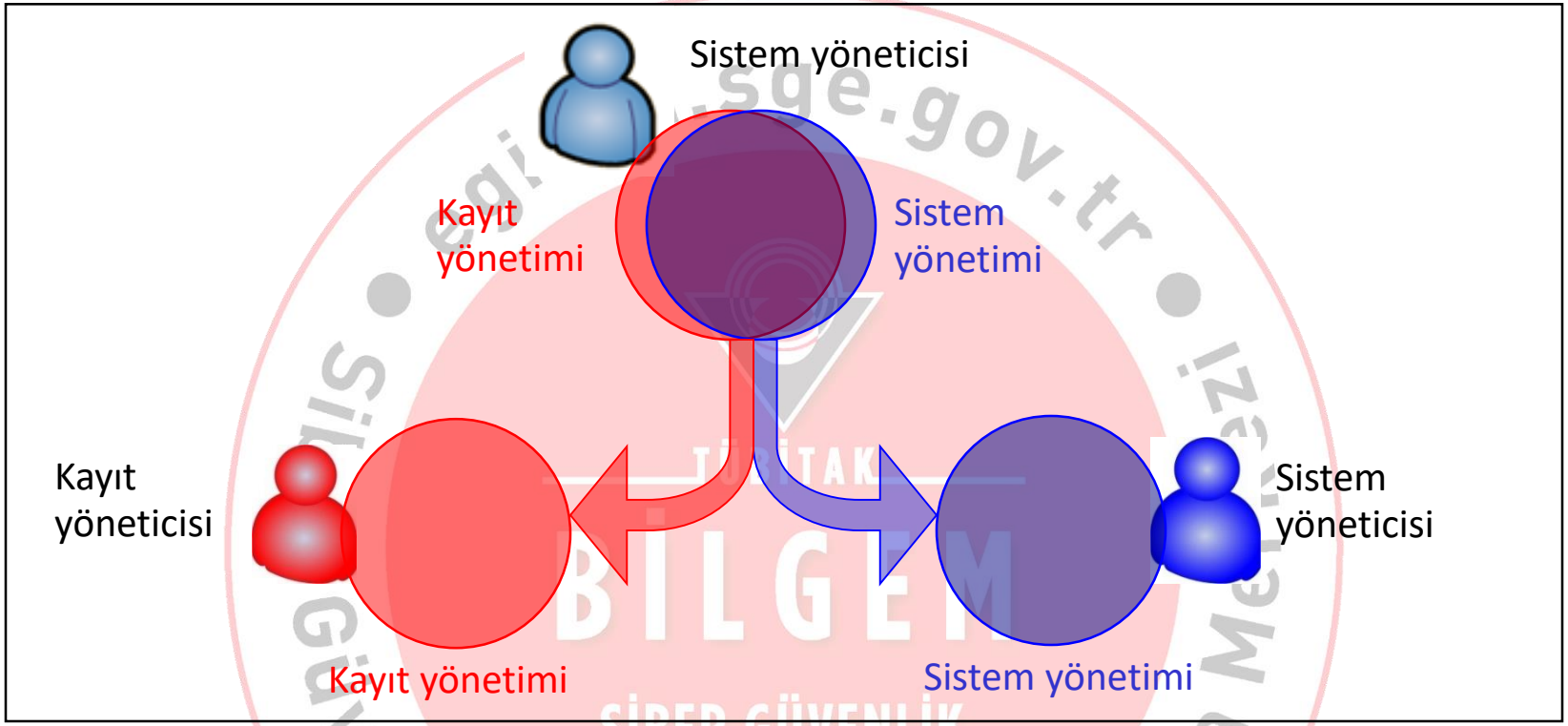
cc BY NC ND

Görevler Ayrılığı'nın tesis edilmesi

- İşin yapılması ile yetkilendirilmesi birbirinden ayrılmalıdır. *(ISO 27002:2005, 10.1.3 Görevler Ayrılığı)*
- Tetkikçiler kendi yaptıkları işi tetkik edemezler. *(ISO 27001:2005, 6. İç Tetkik)*
- Yasama/Yürütme/Yargı → Yetkilendirme/Yürütme/Tetkik

BY NC ND

Sistem Yöneticilerinin Durumu



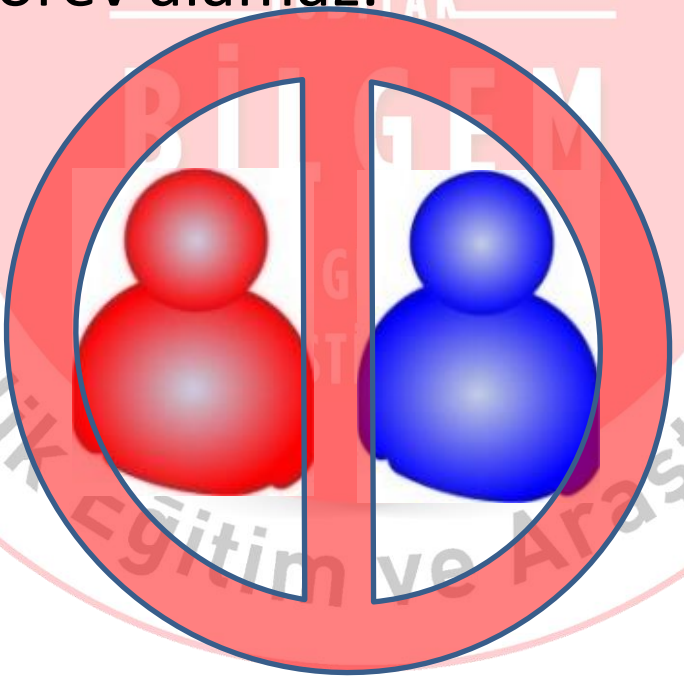
10.1.3 Görevler ayrılığı uyarınca sistem yönetimi ile kayıt yönetiminin ayrılması

- **Sistem yöneticilerinin** yaptıkları işlemlere ilişkin **kayıtlara erişememeleri**,
- **Kayıt yöneticilerinin** sistem üstünde **işlem yapamaması gerekir.**

CC BY NC ND

Kayıt Yönetimi ve Görevler Ayrılığı

- Sistem yöneticileri, yönettiği sistemle ilişkisi kesilmeden K-SOME'de kayıt yöneticisi olarak görev alamaz.
- K-SOME kayıt yöneticisi hiçbir sistemde yönetici olarak görev alamaz.



Kayıt yöneticisi

(SOME)

Sistem yöneticisi

(BİLGİ İŞLEM)

CC BY NC ND

Kurumsal SOME'lerin Görev ve Sorumlulukları

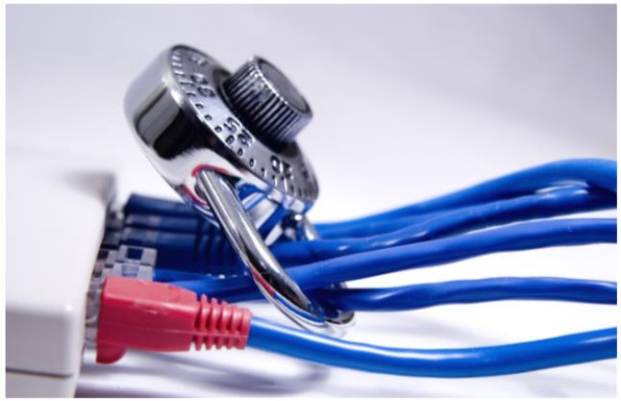
SİBER GÜVENLİK ENSTİTÜSÜ

egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma

K-SOME Rol ve Sorumluluklar

- ✓ İhlal Olayı Öncesi
- ✓ İhlal Olayı Esnası
- ✓ İhlal Olayı Sonrası

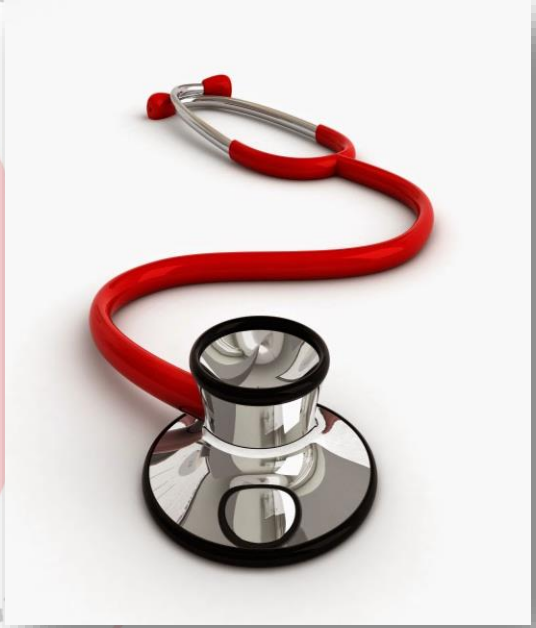
İhlal Olayı : ***Beklenen ve beklenmeyen, ya da sıradan ve sıra dışı güvenlik olaylarıdır***. (Erişim İhlalleri, Veri Bütünlük İhlalleri, Hizmet kesintisine ilişkin olaylar, İnsan katmanına yönelik olaylar (Sosyal Mühendislik vb.), Kötücül yazılım ve DDOS saldırıları



CC BY NC ND

4. Kurumsal SOME'lerin Görev ve Sorumlulukları

- 4.1 Siber Olay Öncesi
  - Kurum içi farkındalık arttırma çalışmaları
  - Kurumsal bilişim sistemleri güvenlik testlerinin yapılması / yaptırılması
  - İz kayıtlarının merkezi olarak yönetilmesi
- 4.2 Siber Olay Esnası
  - Olaya müdahale ve koordinasyon
- 4.3 Siber Olay Sonrası
  - Düzeltici önleyici faaliyetlerin belirlenmesi
  - Kurum yönetimine ve kurum dışındaki yetkililere raporlama vb. bildirimlerin yapılması



egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştır
CC BY NC ND

Siber Olay Öncesi: SOME Kurulum Hazırlık aşaması

egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ

Hazırlık aşaması

- Politika ve Prosedürler
- Temel Bilişim Varlıklarının belirlenmesi
- Risklerin tanımlanması ve önceliklendirilmesi
- Kapasite belirlenmesi ve açıklıklıkların tespiti

CC BY NC ND

Hazırlık aşaması

- Olay Müdahale Planı ve Prosedürlerinin hazırlanması
- Politika plan ve Prosedürlerin onaylanması
- Olay raporlama sürecinin belirlenmesi
- Tatbikatların düzenlenmesi

BY NC ND

Hazırlık aşaması

- Olay senaryolarının çıkarılması ve çözümlerin tartışılması
- Otomatik ve Manuel tespit sistemlerinin kurulması
- Kurumsal Farkındalık çalışmalarının yapılması
- Politika plan ve prosedürlerin gözden geçirilmesi

cc BY NC ND

Dokümantasyon

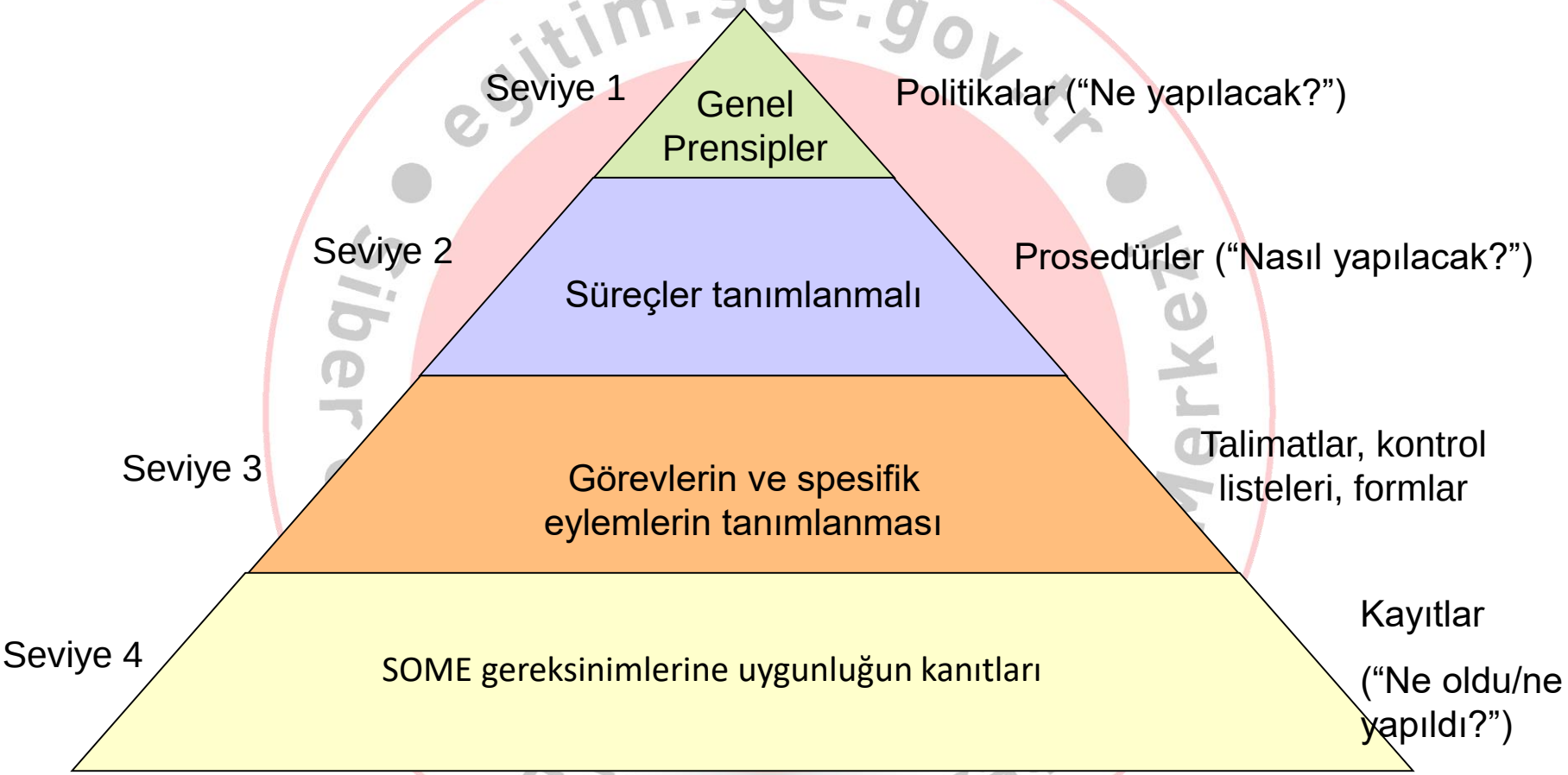
Politika	Ne yapacağım?
Prosedür	Nasıl yapacağım?
Kayıt **(= Delil)**	Ne yapıldı / Ne oldu?

- Belirlenen güvenlik önlemleri **politika ve prosedürlere** dönüştürülür. (Gözden geçirme ve geliştirmeye açıktır)

- **Kayıtlar** aracılığı ile önlemlerin çalışması izlenir. (Kayıtlar <u>değiştirilemez</u>).

BY NC ND

SOME Dokümantasyonu



eğitim.sge.gov.tr • Siber Güvenlik Merkezi • Eğitim ve Araştırma

İyi Politika / Prosedür

- *Çok uzun olmamalı ("İnsan okuyacak ☺")*
- *Talep ettikleri makul olmalı*
- *Tutarlı olmalı (bir işi bir yerde tanımla!)*
- *Orta derecede detaya girmeli*
  - *Çok detaylı olduğu zaman boşluklar oluşur.*
  - *Az detaylı olduğu zaman işe yaramaz.*
- *Okunaklı / biçim olarak çekici olmalı*

egitim.sge.gov.tr
Bilgi Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ

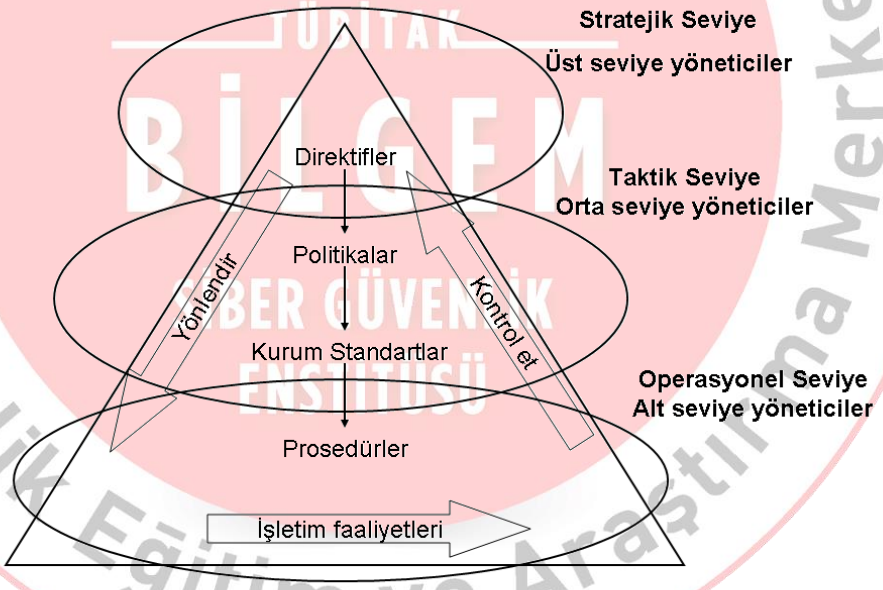
Politikalar ve Prosedürler

- Politikalar
  - Erişim Kontrol Politikası
  - Kabul Edilebilir Kullanım Politikası
  - Siber Olay Müdahale Politikası
  - Fiziksel ve Çevresel Güvenlik Politikası
  - Elektronik Posta Güvenlik Politikası
  - SOME Rol ve Sorumluluklar
- Prosedürler
  - Bilgi Varlıkları Sınıflandırma Prosedürü
  - Kayıt Yönetim Prosedürü
  - Güvenli İmha Prosedürü

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Seviye 1 - Politikalar

- Bilgi güvenliği için yönetim mekanizmalarının harekete geçirilmesi ve gerekli desteğin sağlanması.
- Yönetim politikayı belirler ve politikaya destek sağlar



eğitim sağlar
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Seviye 2 - Prosedürler

- Prosedürler
  - Uygulanan kontrollerin gerektirdiği prosedürler
    - Güvenlik süreçleri ile ilgili kim, ne, ne zaman ve nerede sorularının cevapları tanımlanmalı
- Örnek prosedürler;
  - Düzeltici/önleyici faaliyet prosedürü
  - Sınıflandırma Prosedürü
  - Kayıt Yönetim Prosedürü

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

Seviye 3 İş talimatları, Formlar

- İş talimatları, kontrol listeleri ve formlar
  - Spesifik talimatların veya eylemlerin detaylarının açıklamaları ve nasıl uygulanacakları listelenmeli
  - Ayrıntılı iş talimatları, formlar, akış diyagramları, servis standartları ve sistem kullanım kılavuzları bu seviyede bulunur

eğitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Üretilen Kayıtların Kontrolü

- Kayıt alma mekanizmaları kurulmalı ve sürdürülmeli:
- Kayıtlar korunmalı ve yönetilmeli
- Yasal ve düzenleyici hükümler dikkate almalı
- Kayıtların:
  - Tanınması (identification)
  - Depolanması (storage)
  - Korunması (protection)
  - Bulup getirilmesi (retrieval)
  - Muhafaza zamanı (retention time)
  - Düzenleme zamanları (disposition of records)

  için yöntem belirlenmeli ve dokümante edilmelidir.

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
eğitim.sge.gov.tr
CC BY NC ND

SOME Politikası

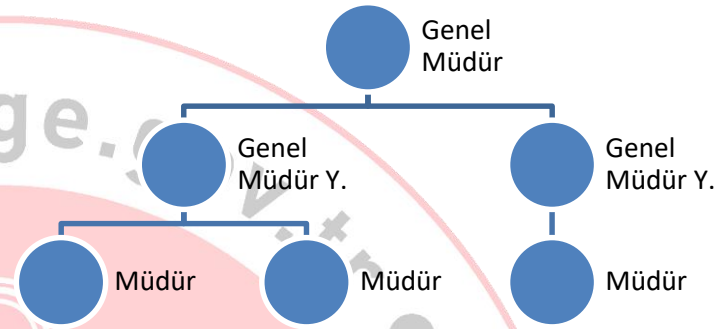
- SOME için yönetim mekanizmalarının harekete geçirilmesi ve gerekli desteğin sağlanması.
- Yönetim politikayı belirler ve politikaya destek sağlar
- SOME Servislerinin tanımlanması (SOME süreçleri)
- SOME Rol ve sorumluluklarının belirlenmesi ve atanması
- İletişim esallarının belirlenmesi

cc BY NC ND

SOME Politikası

Genel Gereksinimler:

- Görev Alanının tanımlanması
- Görev ve Yetkilerin Belirlenmesi
- Organizasyon Şeması
- Kurumsal SOME organizasyonu
- İhlal olayı tanım



cc BY NC ND

SOME Politikaları

Dğer Politikalar:

- Fiziksel Güvenlik
- Depolama (Fiziksel)
- Bilginin sınıflandırılması ve korunması
- Kayıt tutma
- E-Posta ile güvenli iletişim (PGP kullanımı
- Kayıt yok etme
- Bilgi Değişimi/Paylaşımı
- Erişim Politikası
- Kurumsal SOME sistemlerinin kullanımı
- Olay Müdahale Politikası
- Yama Yönetimi/ Antivirüs Politikası

Quelle: www.bsi.bund.de

BY NC ND

SOME Prosedürleri

Prosedürler yaşanabilecek ihlal olaylarına karşı hazırlanmalıdır

- Zaralı yazılım tanıma karantina ve temizleme
- Şüpheli saldırgan profilleri
- DDOS
- Sistemin izole edilmesi
- Gözden geçirme ve yama yönetimi
- Antivirüs
- Ölçüm
- Yedekleme ve yedekten geri dönme
- İz kayıtlarının yönetimi

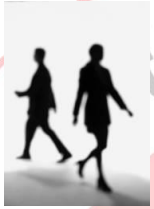
CC BY NC ND

Varlıklar

- İnsanlar *(personel, müşteriler, tedarikçiler..)*
- Bilgi *(kağıt ve elektronik ortamdaki)*
- Yazılım varlıkları
- Fiziksel varlıklar *(bilgisayar ve iletişim donanımı, altyapı varlıkları)*
- Hizmetler *(bilişim, ısıtma, havalandırma..)*
- Kurum imajı ve itibarı

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Varlık Envanteri

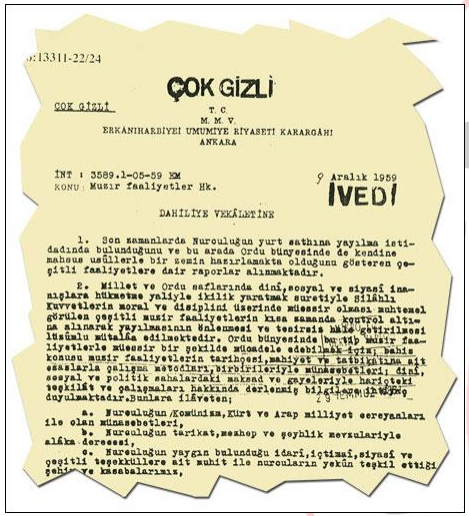


Personel	Sahibi	Değeri	Konum
Bilgi (Elektronik/Basılı)	Sahibi	Değeri	Konum
Yazılım varlıkları	Sahibi	Değeri	Konum
Donanım Bilgisayar, Modem, vb.	Sahibi	Değeri	Konum
Hizmetler	Sahibi	Değeri	Konum

TÜRKSAT

cc BY NC ND

Varlıkların sınıflandırılması



ÇOK GİZLİ

ÇOK GİZLİ

T.C.
M.M.V.
ERKANIHARBİYEİ UMUMİYE RİYASETİ KARARGÂHI
ANKARA

İNT : 3589.1-05-59 KM
KONU : Muzır faaliyetler Hk.

9 Aralık 1959
İVEDİ

DAHİLİYE VEKÂLETİNE

1. Son zamanlarda Nurculuğun yurt sathına yayılma istidadında bulunduğunu ve bu arada Ordu bünyesinde de kendine mahsus usûllerle bir zemin hazırlamakta olduğunu gösteren çeşitli faaliyetlere dair raporlar alınmaktadır.

2. Millet ve Ordu saflarında dinî,sosyal ve siyasî inanışlara hükmetme yoliyle ikilik yaratmak suretiyle dilâhlı Kuvvetlerin moral ve disiplini üzerinde müessir olması muhtemel görülen çeşitli muzır faaliyetlerin kısa zamanda kontrol altına alınarak yayılmasının önlenmesi ve tesirsiz hâle getirilmesi lüzumlu mütalâa edilmektedir. Ordu bünyesinde bu tip muzır faaliyetlerle müessir bir şekilde mücadele edebilmek için, bahis konusu muzır faaliyetlerin tarihçesi,mahiyet ve tatbikatına ait esaslarla çalışma metodları,tiplerileriyle münasebetleri: dinî, sosyal ve politik sahalardaki maksad ve gayeleriyle hariçteki teşkilât ve çalışmaları hakkında derlenmiş bilgi [illegible] duyulmaktadır.Bunlara ilâveten;

a. Nurculuğun komünizm,Kürt ve Arap milliyet cereyanları ile olan münasebetleri,

b. Nurculuğun tarikat,mezhep ve şeyhlik mevzularıyle alâka derecesi,

c. Nurculuğun yaygın bulunduğu idarî,içtimaî,siyasî ve çeşitli teşekküllere ait muhit ile nurcuların yekûn teşkil ettiği şehir ve kasabalarımız,

Gizli

Hizmete Özel

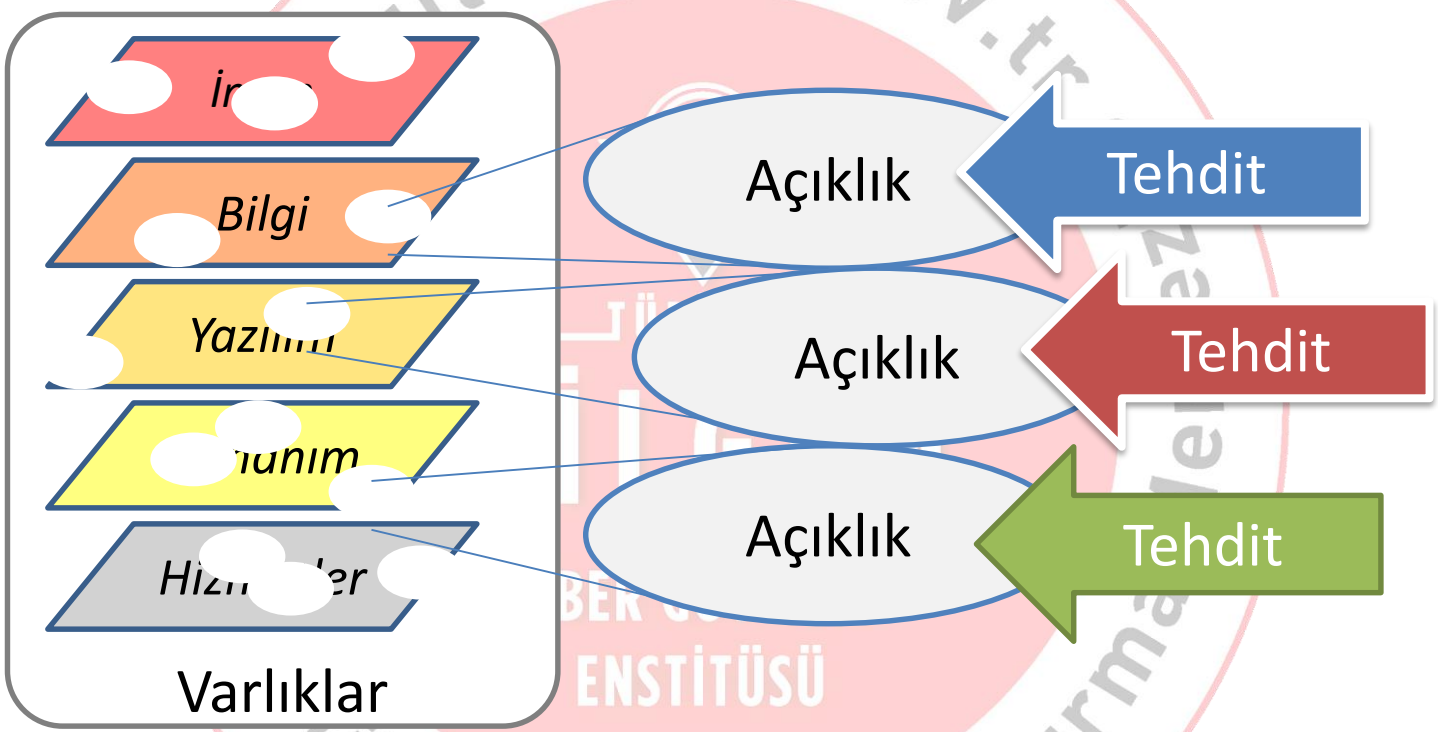
Gizli

7.2.2 Bilginin sınıflandırılması ve etiketlenmesi

eğitim.sge.gov
TÜBİTAK BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

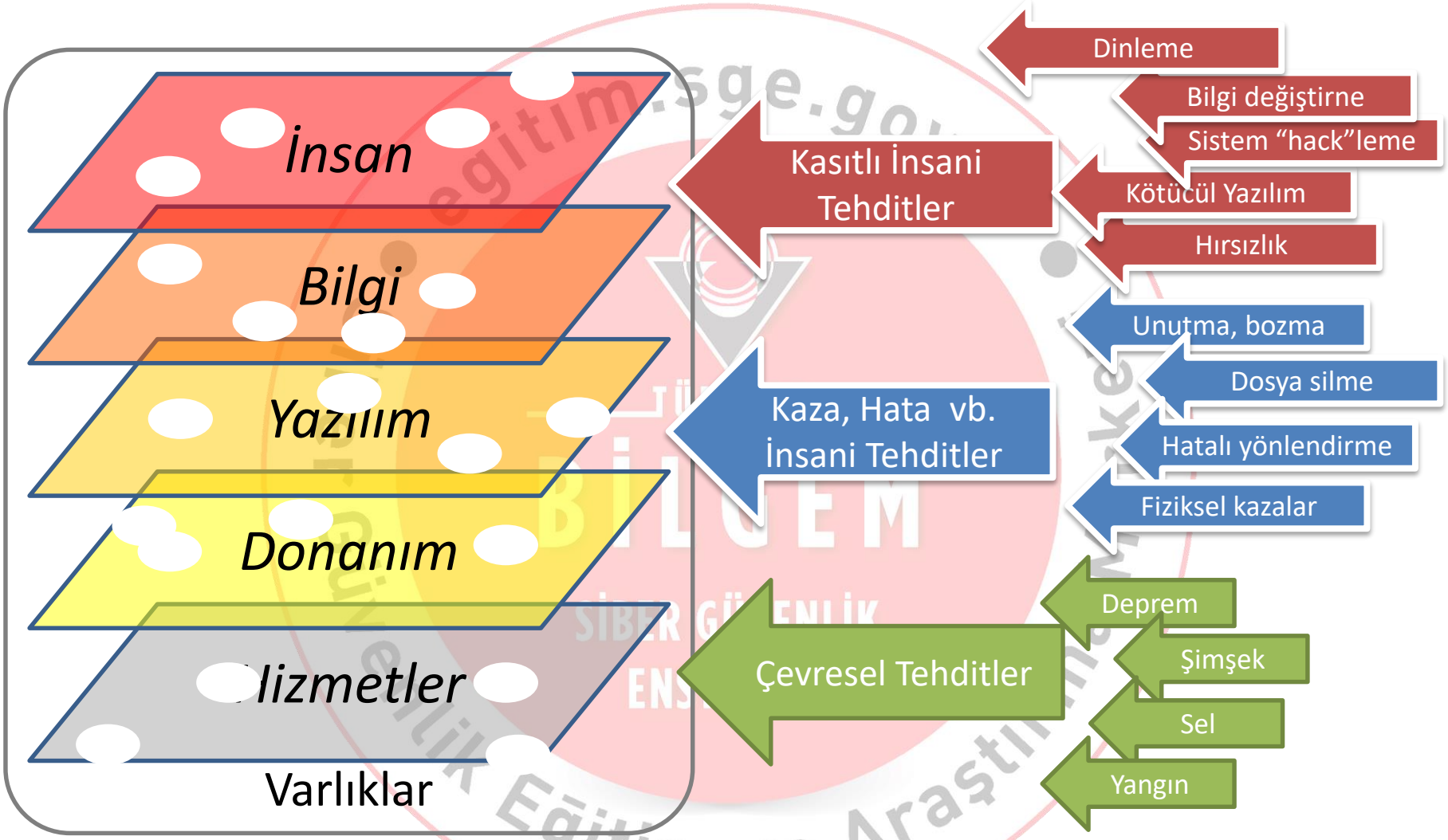
CC BY NC ND

Açıklıklar ve Tehditler



BY NC ND

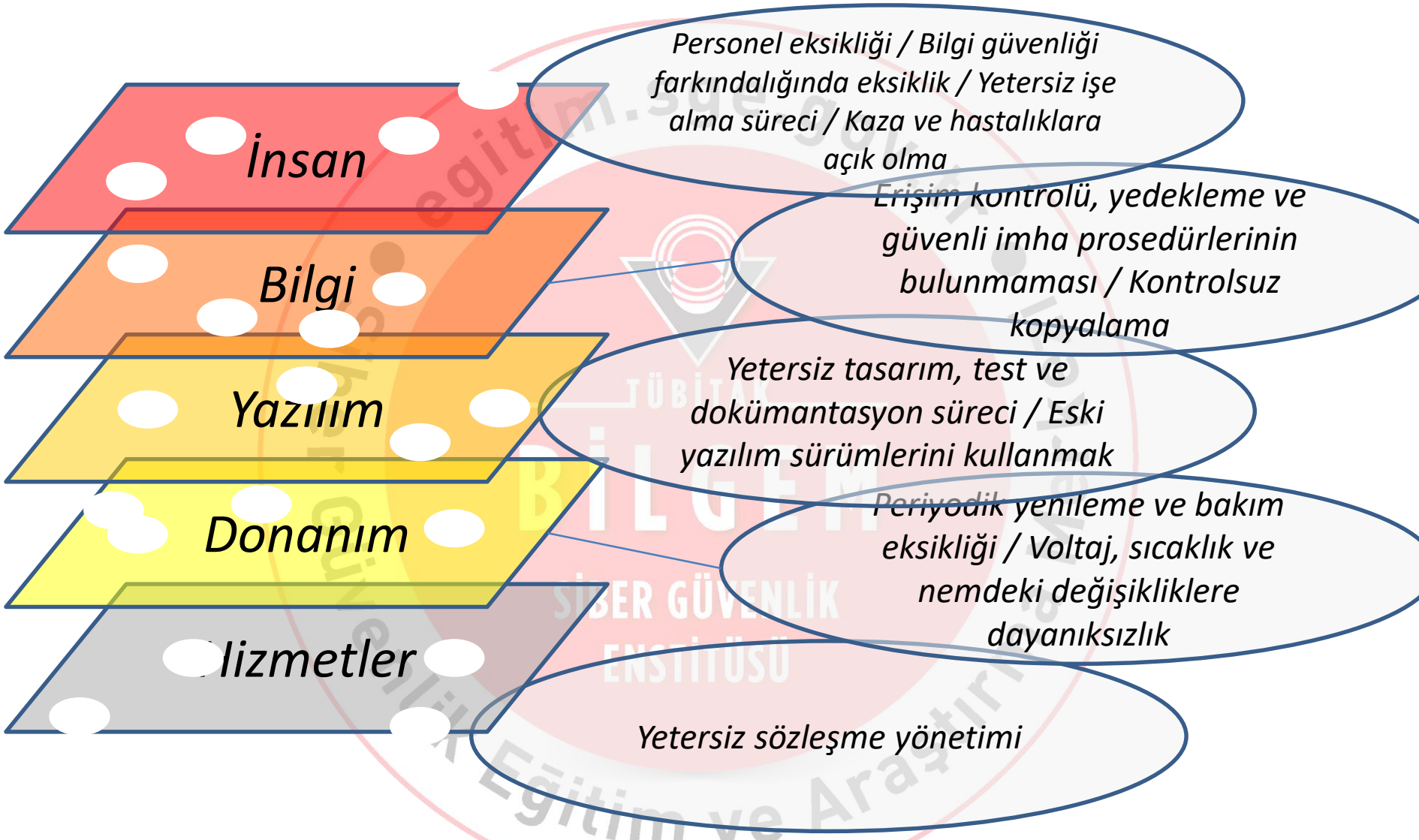
Tehditler*



(*) ISO/IEC 13335-1:2004 - Concepts and models for information and communications technology security management – Threats.

cc BY NC ND

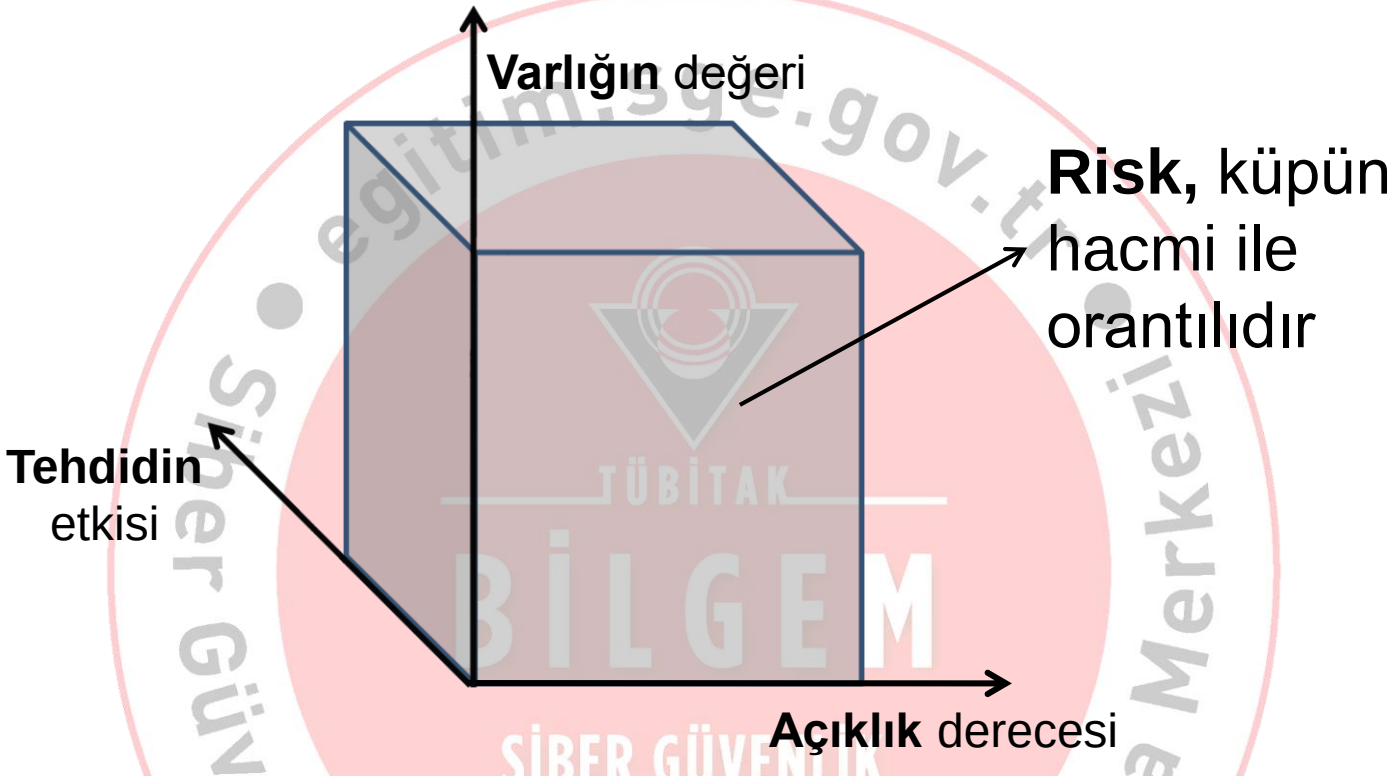
Açıklıklar*



(*) ISO/IEC TR 13335-3 - Techniques for the Management of IT Security – Annex D - Common Vulnerabilities

CC BY NC ND

Risk Derecelendirme



Risk = F(Varlık, Açıklık, Tehdit)

Zarar x Olasılık

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi

Risk Yönetimi & Analizi

Varlık üzerindeki bir **açıklığın** bir **tehdit** tarafından kullanılmasına bağlı **zarar beklentisidir.**

Zarar beklentisi = f(Varlık, Açıklık, Tehdit)

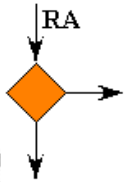
- Risk = Zarar x Olasılık

SİBER GÜVENLİK ENSTİTÜSÜ
Yetişkin Eğitim ve Araştırma

Risklerin belirlenmesi

- Risk Yönetimi

  - Risklerin Belirlenmesi (Identification)
  - Risk Değerlendirme (Assessment)
    - Risk Analizi (Analysis)
    - Risk Derecelendirme (Evaluation)
  - Risk İşleme (Treatment)



eğitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Risklerin değerlendirilmesi

- **Varlıkların ve** varlık **sahiplerinin** belirlenmesi
- Varlığa yönelik **tehditlerin** belirlenmesi
- Bu tehditlerin kullanabileceği **açıklıkların** belirlenmesi
- Tehdit ve açıklıkların varlığın gizlilik, bütünlük veya erişilebilirliğine **etkisinin belirlenmesi**

Varlık sahibi = Birey veya birim

Varlığın üretilmesinden, geliştirilmesinden, bakımından kullanımından ve güvenliğinden sorumludur.

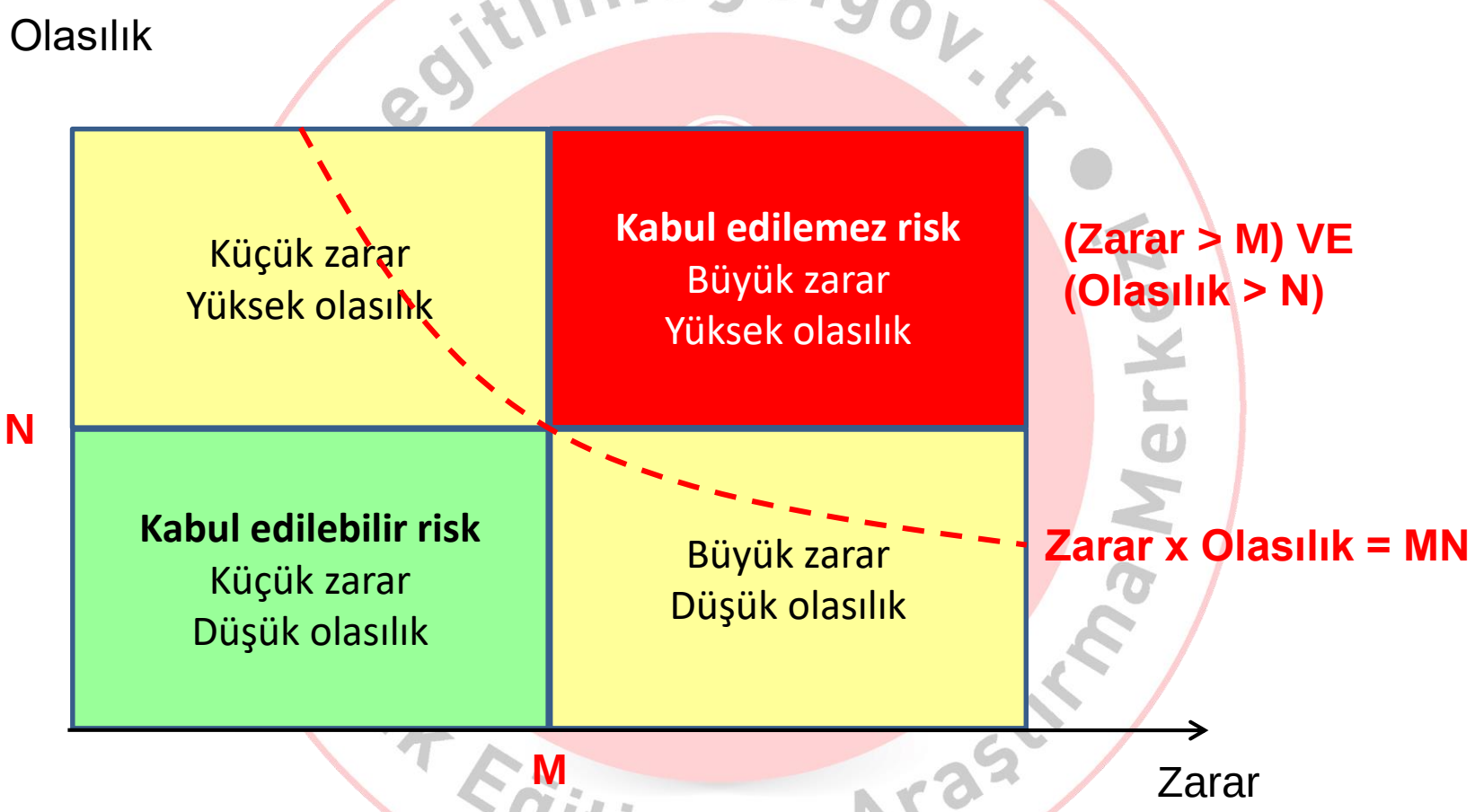
- Varlığın ***sınıflandırılması***
- Erişim haklarının belirlenmesi ve ***gözden geçirilmesi***

TÜBİTAK BİLGEM Siber Güvenlik Eğitim ve Araştırma Merkezi
SİBER GÜVENLİK ENSTİTÜSÜ
eğitim sağlayıcı
CC BY NC ND

Riskler

BY NC ND

Risk Derecelendirme



egitim.sge.gov.tr
Eğitim ve Araştırma Merkezi

Olay Müdahale Planı

Olay müdahalede kullanılacak olan teknik plan prosedür, kontrol listeleri, formlar ve iş akışlarından oluşan dokümante edilmiş bir plandır.

- Detaylı
- Teknik
- İletişim
- Zaman
- Gözden geçirme
- Ders çıkarma
- Ölçüm
- Dış kaynaklar
- Tatbikat planı

CC BY NC ND

Kurum İçi Farkındalık

- Kullanıcılar
  - Parola güvenliği
  - «Spam» ve «Phishing»'e karşı farkındalık
  - Hafıza kartı vb. bileşenlerin doğru kullanımı
  - Sunumlar, posterler, e-posta ve bültenler

- Bilgi İşlem ve Kurumsal SOME çalışanları
  - Yazılım güvenliği,
  - İşletim sistemi güvenliği,
  - Ağ güvenliği,
  - Kayıt yönetimi vb. konusunda eğitim, eğitim, eğitim.

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Parola Güvenliği

TÜBİTAK

Sızdırılan 15 milyon parola arasında en çok kullanılanlar!

No	Sayısı (gmail?)	Parola	No	Sayısı (yandex,mail.ru?)	Parola
1	112951	qwerty	1	47779	123456
2	47986	123456	2	11524	password
3	37672	qwertyuiop	3	11145	123456789
4	29197	qwe123	4	8083	12345
5	9132	klaster	5	5908	qwerty
6	7893	qweqwe	6	5241	12345678
7	7393	1qaz2wsx	7	3515	111111
8	6940	1q2w3e4r	8	3008	abc123
9	6893	qazwsx	9	2968	123123
10	4223	123qwe	10	2904	1234567
11	4166	1q2w3e	11	2706	1234567890
12	4029	123456789	12	2411	
13	3991	1q2w3e4r5t	13	1983	1234
14	3489	zxcvbnm	14	1973	iloveyou
15	3098	qwer1234	15	1852	password1
16	3000	111111	16	1742	000000
17	2741	1234qwer	17	1722	27653
18	2120	asdfgh	18	1538	zaq12wsx
19	1739	marina	19	1534	tinkle
20	1731	q1w2e3r4t5	20	1514	qwerty123

cc BY NC ND

www.bilgimikoruyorum.org.tr

TÜBİTAK

Ana Sayfa | Hakkımızda | TÜBİTAK | BİLGEM

TÜBİTAK BİLGEM

Bilgimi Koruyorum

Google™ Özel Arama | Ara

Bilgimi Koruyorum ▸ Ana Sayfa

B!resi biTgileranizi demiftirse

Öeler olapilix?
Ne hi$$ebersiniz?
Nz yaşarsıMız?

Bilgi güvenliği; kendimizi geliştirmekle, öğrendiklerimizi uygulamakla ve öğrendiklerimizi yakınlarımızla paylaşmakla sorumlu olduğumuz bir konu. **Güvenlik tedbirleri almadan bilişim teknolojilerini kullanmak** günümüzde "*inanılmaz bir risk alıyorsunuz*" anlamına geldi. Kısacası bu konudan uzak durmak istesek bile o bizim yakamızı bırakacak gibi görünmüyor.

Öyleyse **en iyisi öğrenmek**. Aslında günlük yaşamımızdan hiç yabancısı olmadığımız bir çok kavram ve yaklaşım içeren bu konuyu, Çağlar Bey ve arkadaşlarının dünyasında geçen olaylarla irdelemeye, bilişim dünyasında bilinçli hareket etmeye hoş geldiniz.

Bilgi güvenliği: Nedenleri / Sorumluluklar

Bilgisayara giriş güvenliği

Parola güvenliği

Konu Listesi / Menü

- Bilgimi Koruyorum
- Bilgi Güvenliği
- Bilgisayar ve Erişim Güvenliği
- Tehditler ve Korunma Yöntemleri
- Internet ve Ağ Güvenliği

Sözlük

TÜBİTAK | TÜBİTAK BİLGEM

◂ Bilgimi Koruyorum

Eğitime Başlarken (Öneriler) ▸

© 2011 Tüm hakları TUBİTAK-BİLGEM'e aittir. Kullanım Şartları yerine getirilmeden ve referans gösterilmeden alıntı yapılamaz.
Bu sayfa DPT tarafından desteklenen Ulusal Bilgi Sistemleri Güvenlik Programı kapsamında yapılmıştır.
Bilgi için bilgi@bilgimikoruyorum.org.tr

cc BY NC ND

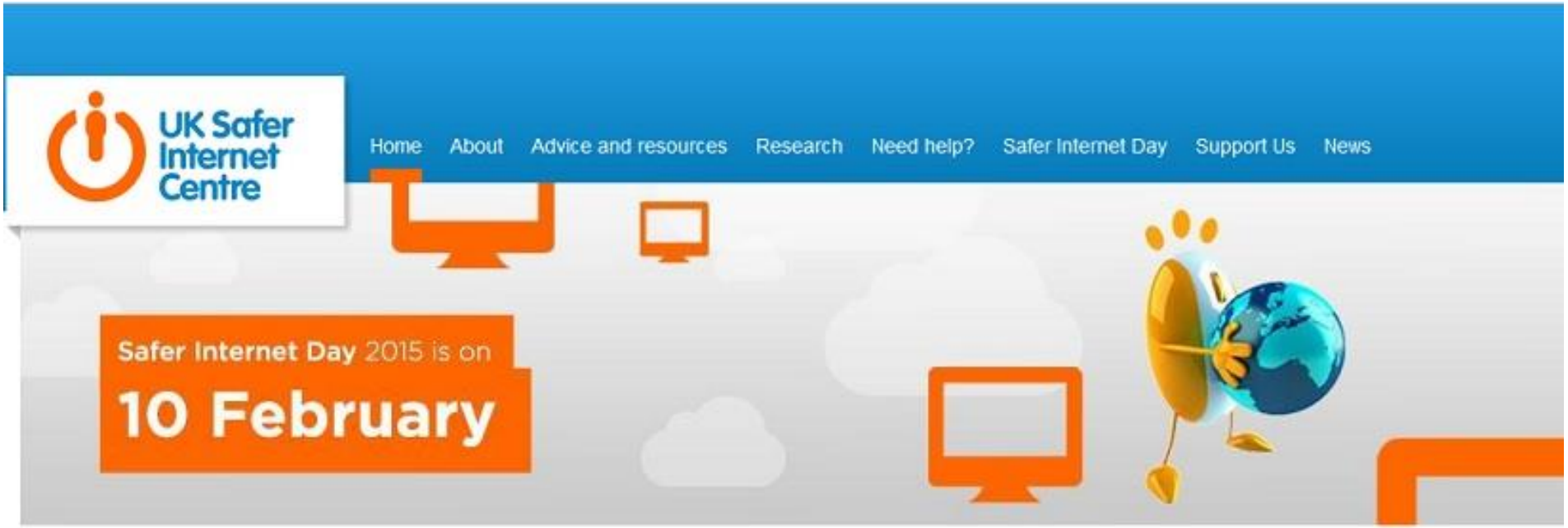
www.guvenliweb.org.tr

BY NC ND

www.stopthinkconnect.org

BY NC ND

www.saferinternet.org.uk



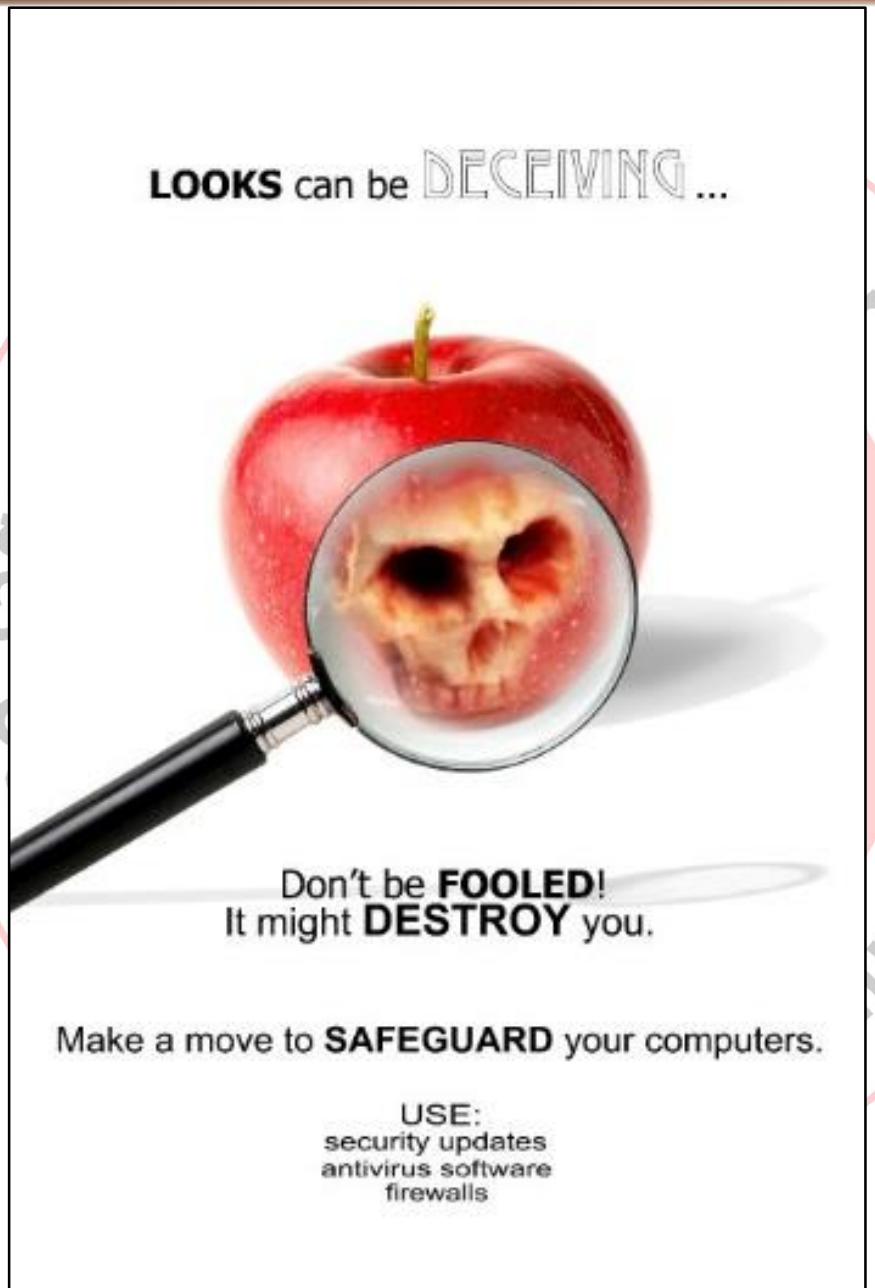
Welcome to the UK Safer Internet Centre, where you can find e-safety tips, advice and resources to help children and young people stay safe on the internet.

BY NC ND

Posterler

KURUM_AL
GÜV_ _LİK
SEN'siz Olmaz!
BİLGEM
SGE
Siber Güvenlik Enstitüsü
www.bilgiguvenligi.gov.tr
www.bilgimikoruyorum.org.tr
www.bilgem.tubitak.gov.tr

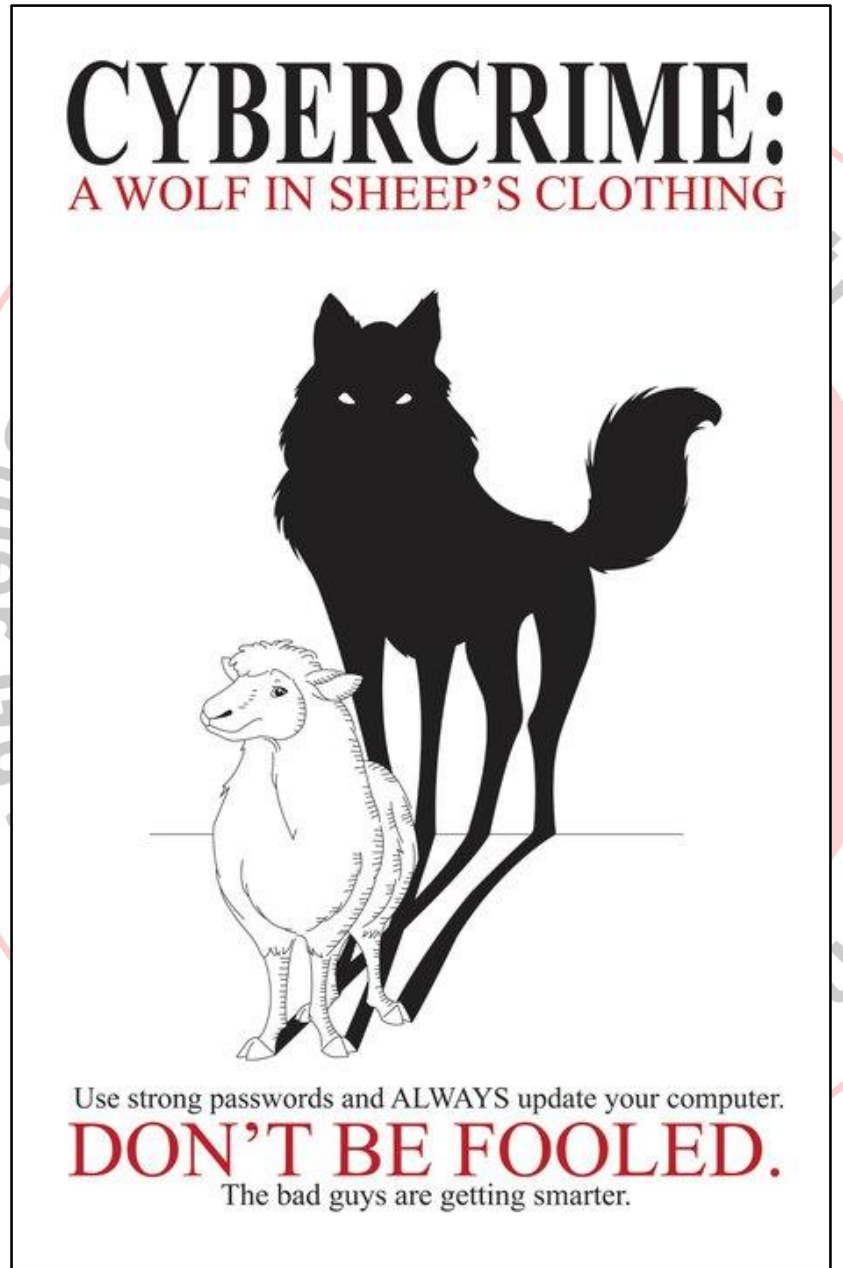
Posterler



www.educause.edu

TÜBİTAK

Posterler



STOPTHINKCONNECT.ORG

BY NC ND

Siber Olay Öncesi: Kurumsal Bilişim Sistemleri Güvenlik Testleri

egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ

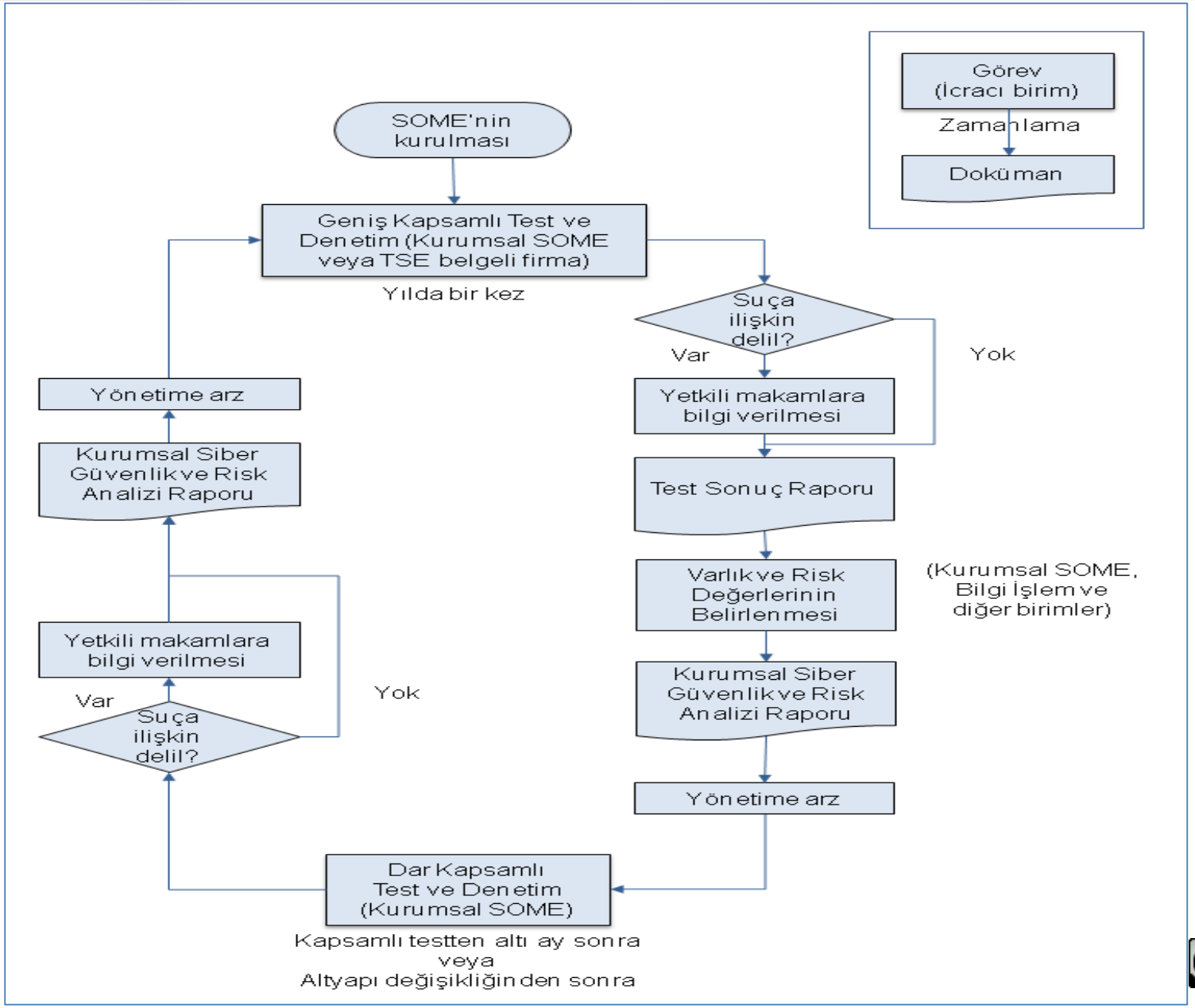
TÜBİTAK
CC BY NC ND

Kurumsal Bilişim Sistemleri Güvenlik Testleri

- Temel Kavramlar
- Neden Pentest?
- Pentest Yaklaşımları
- Planlama
- Amaç
- Süreçler
- Riskler
- Yasal Durumlar
- Standartlar
- Raporlama

TÜBİTAK
BY NC ND

Güvenlik Testleri Süreci



BY NC ND

Temel Kavramlar

Siber Güvenlik Testleri ve Denetimleri

Güvenlik Denetimleri
(Security Audits)

Zafiyet Değerlendirme
(Vulnerability Assesment)

Sızma Testleri
(Penetration Tests)

CC BY NC ND

Siber Güvenlik Test Türleri

- Güvenlik Denetimleri (Security Audits)

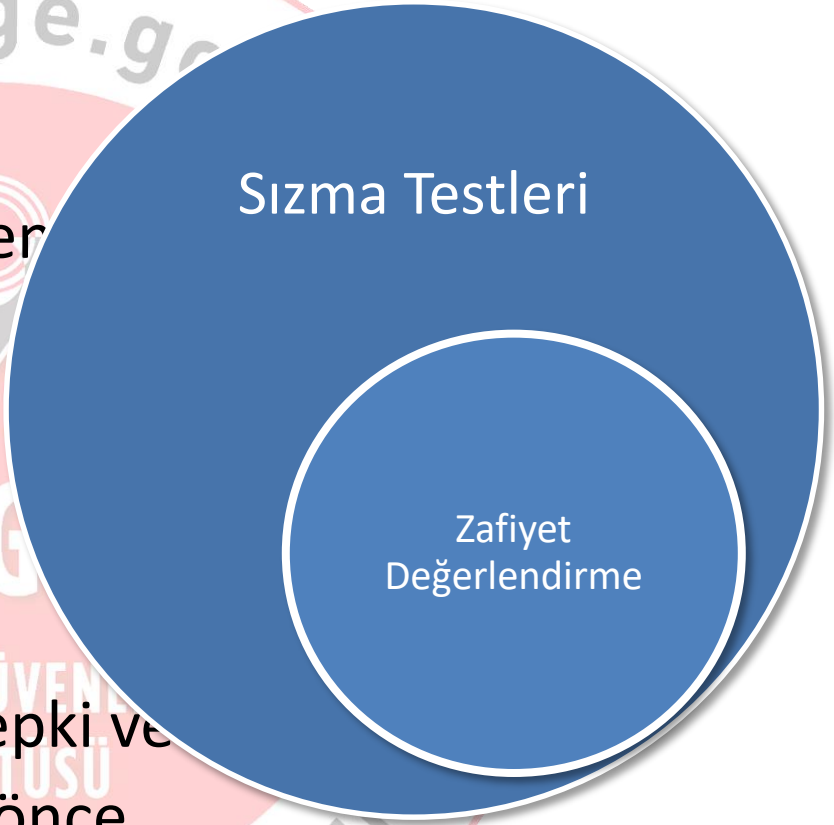
- Konfigürasyon (Yapılandırma) Testleri
- Bileşen bazlı
- Savunma bakış açısı

eğitim.sge.gov.tr • Siber Güvenlik Eğitim Merkezi

CC BY NC ND

Siber Güvenlik Test Türleri

- Sızma Testleri (Penetration Tests)
- Penetrasyon Testleri; Pentest
- Saldırgan bakış açısı
- Sistemi bir bütün olarak değerler
  - İnsan, sistemin bir parçasıdır!
- Hem dışardan, hem içerden…
- Nedir?
- Saldırı simülasyonu
- Sistem bir saldırıya karşı nasıl tepki ve
- Amaç: Kötü niyetli insanlardan önce
  - Zafiyetlerin ve
  - Bu zafiyetlerle neler yapılabileceğinin tespit edilmesi



CC BY NC ND

Neden Pentest yaptırmalıyım?

Zayıf Yönlerim

Güçlü Yönlerim

Tehditler

dreamstime.com
BY NC ND

1. Pentest Yaklaşımları

- **Zero-knowledge** (Black-Box)
- **Partial-knowledge** (Gray box)
- **Full-knowledge** (White Box)

TÜBİTAK BİLGEM SİBER GÜVENLİK Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

2. Kapsam

- Dış Ağ
- İç Ağ
- Web Uygulamaları
- Kablosuz Ağ
- Sunucular
- Aktif cihazlar
- Veritabanı
- Uygulamalar
- Sosyal mühendislik
- DDoS
- Fiziksel güvenlik ….

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma
BİLGİ SİBER ENSTİTÜSÜ

3. Gereksinimler

- Gerekli araçlar
- Alt yapı kurulumu
  (yazılım, donanımsal ağ mimarisi)
- Acil önlem planı
- Yedekleme yapılması gerekenler
- İzleme Sistemleri

eğitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma

4. Sınırlamalar

- Kapsam (Scope)
- Zaman
- Erişim (sunucu ağı,intranet)
- Method
  (Atak teknikleri)
  Örnek: Brute force yapılmasın!

eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

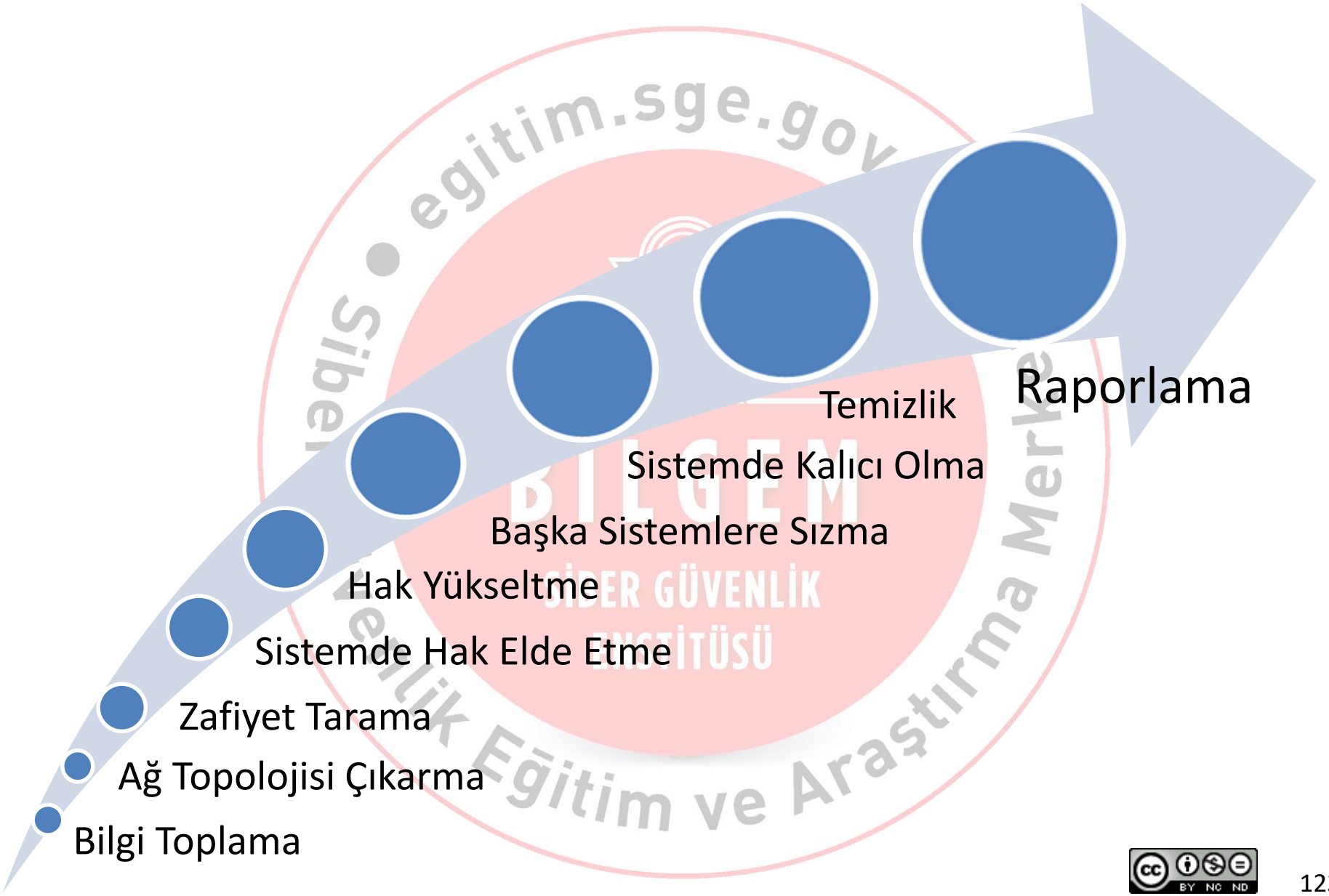
CC BY NC ND

5. Uzman/Firma Seçimi

- Kabiliyetler
- Sertifikasyonlar
  C|EH, L|PT, GSEC, GPEN, OSCP
- Referanslar
- Klerans

egitim.sge.gov.tr
Eğitim ve Araştırma Merkezi

Sızma Testi Süreci



egitim.sge.gov
Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

Sızma Testi Standartları

- PCI DSS
- OWASP
- PTES
- OSSTMM
- NIST SP 800-115

BY NC ND

Pentest sırasında kullanılan bazı araçlar

Keşif	• Nmap • Hping • Scapy...
Sniffer	• Cain & Abel • Tcpdump • Wireshark...
Zafiyet Tarama	• Nessus • Metasploit • Immunity Canvas
Brute Force	• Hydra • John the Ripper • Cain, Ophcrack...
Web	• Burp • Acunetix • Net Sparker...

TÜBİTAK

Raporlama

- Giriş - Özet
  -Amaç, hedef, kapsam, genel bilgiler
- Yönetici Özeti
- Bulgular
- Tavsiyeler
- Referanslar
- Raporlamada dikkat edilecek hususlar

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araş
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

Raporlama

CC BY NC ND

Raporlama

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

Raporlama

Tam Kapsam

- İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması
- Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
- Dışa açık web uygulamalarının sızma testleri
- Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri
- Veri tabanı yapılandırma testleri
- Kuruma özel geliştirilmiş yazılımlar
- DNS servisi testleri
- E-posta servisi testleri
- Sosyal mühendislik testleri
- Sadece kurum içinden erişilen web uygulamaları sızma testleri
- Dağıtık servis dışı bırakma (DDoS) testleri
- Sanallaştırma sistemleri testleri
- Kablosuz ağ testleri
- Güvenlik duvarı testleri
- URL ve içerik filtreleme testleri

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

Dar Kapsam

- İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması
- Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
- Dışa açık web uygulamalarının sızma testleri
- Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri
- Veri tabanı yapılandırma testleri

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

Sızma Testi Sonuçlandırma

- Rapor gizlidir, iyi korunmalıdır.
- Test sonrası doğrulama testi istenebilir.
- Sızma testi tüm zafiyetleri tespit edemez.
- Gerekli sıkılaştırmalar yapılmazsa pentest para kaybıdır.

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Gizlilik Beyannamesi

Kurum/Kuruluş tarafından sızma testi ve güvenlik analizi yapmak üzere yetkilendirildiğim **başlangıç tarihi** ve **bitiş tarihi** arasında elde ettiğim sonuçların gizliliğini korumak için, başta çevrimdışı ortamlarda saklamak üzere elimden gelen her türlü önlemi alacağımı, sonuçları yazılı ve görsel basına hiçbir şekilde aktarmayacağımı, blog, uzmanlık gruplarına ait siteler, tartışma grupları ve benzeri çevrimiçi ortamlarda hiçbir şekilde paylaşmayacağımı, konferans, seminer ve benzeri etkinliklerde poster veya makale şeklinde yayınlamayacağımı ve yapacağım sunumlarda kullanmayacağımı kabul ve beyan ederim.

- T.C. Kimlik No :
- Adı Soyadı :
- İmza :

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
egitim.sge.gov.tr

Siber Olay Öncesi: İz Kayıtlarının Merkezi Olarak Yönetilmesi

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

İz Kayıtlarının Merkezi Olarak Yönetilmesi

- Kayıt (Log) Nedir?
- Kayıt (Log) Neye Yarar?
- Yaygın Kayıt Türleri
- Kayıt Toplamada Karşılaşılan Problemler
- Merkezi Kayıt Yönetimi
- Kurulum Aşamaları
- Örnek Saldırı Senaryosunun İncelenmesi

BY NC ND

Kayıt (Log) Nedir?

- **Kayıt = Delil**
- Her tür (iç/dış/uluslar arası) saldırıda
  - Hukuktan faydalanmak için,
  - Faillerin yakalanması ve caydırıcılık için gerekli.
- İç tetkik birimleri, ulusal veya uluslar arası mahkemeler tarafından değerlendirilir.

BY NC ND

Kayıt (Log) Nedir?

- 5Ne 1Kim
  - Ne?
    - Yetkisiz erişim, kayıtlar silindi, yetkili kullanıcı oluşturuldu...
  - Ne zaman?
    - Cum 28 15:44:28 2015, 10/08/2015, 2015-01-30 15:45:44
    - 12350495043800345345, 12.01.2015 10:33:56
  - Nerede?
    - Dosya sunucu, e-posta, web servisiniz, aktif dizin?
  - Nereden?
    - Saldırı 99.214.77.13 adresinden Guanjou Internet Sağlayıcı, Beijing Çin
    - Ofisin 3.katından biri, rus hacker'lar
    - Çalınan veri 56.2.3.5 adresine Karachi, Pakistan'a gönderildi
  - Nasıl?
    - SQL enjeksiyonu, kaba kuvvet saldırısı, spam, sosyal mühendislik...
  - Kim?
    - 10.2.2.4, mehmet, FF01::101, 01:23:45:67:89:AB

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

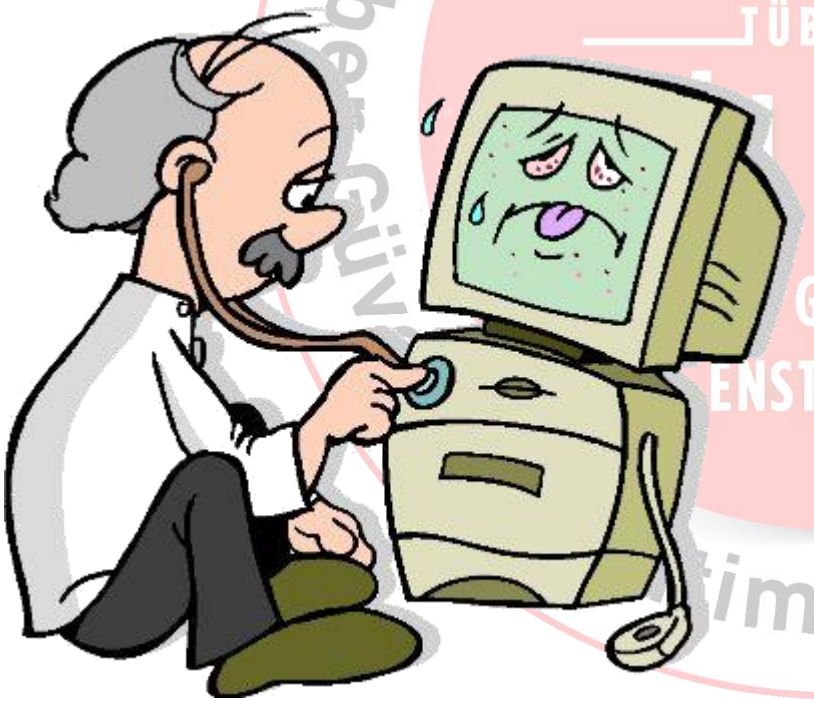
Kayıt (Log) Neye Yarar? Kayıt İzleme

BY NC ND

Kayıt (Log) Neye Yarar? Kayıt Analizi

BY NC ND

Kayıt (Log) Neye Yarar? Problem Giderme



egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

Kayıt (Log) Neye Yarar? Geçmişte Ne Oldu?

m.sge.gov.tr ● Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

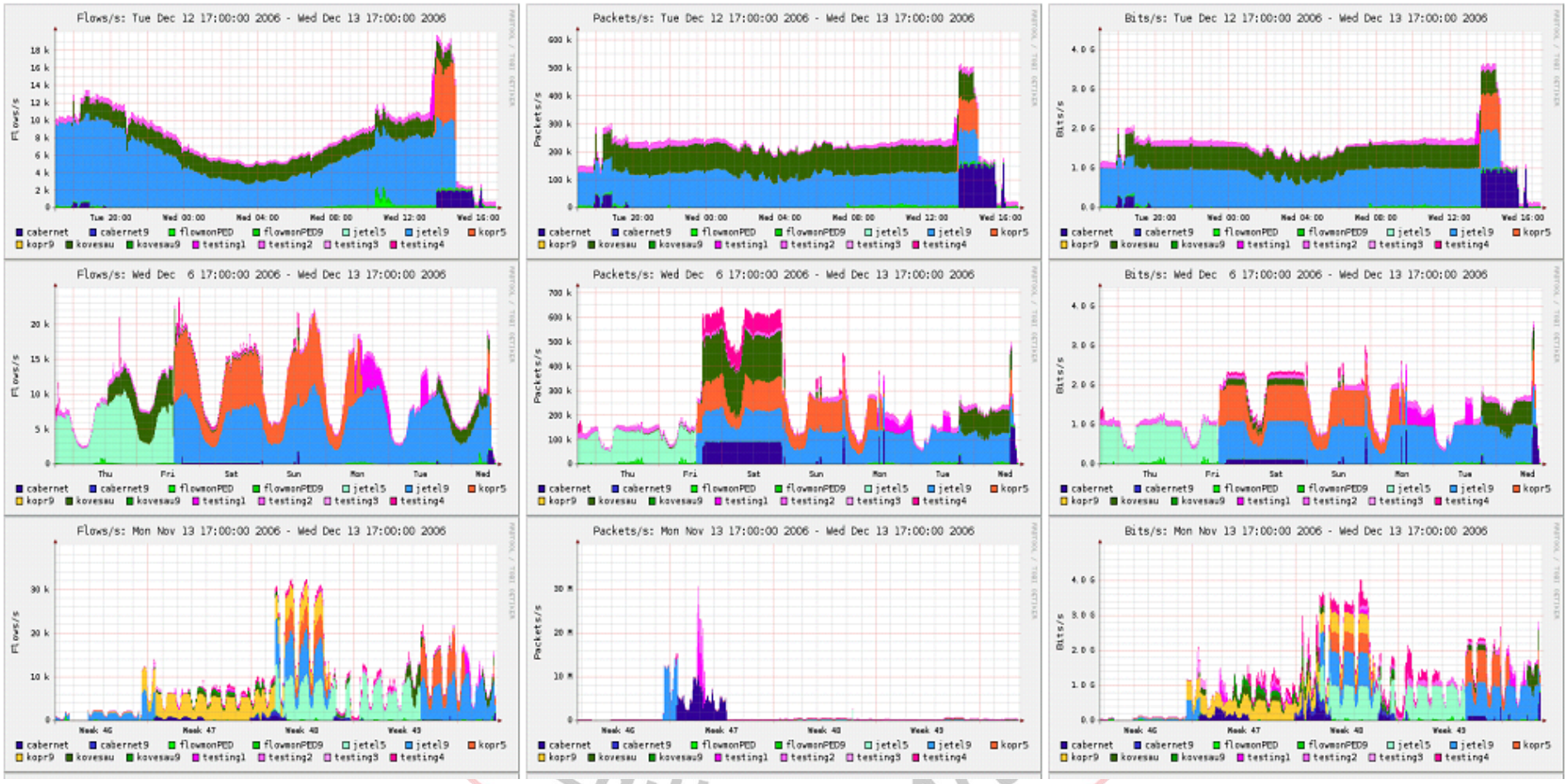
Kayıt (Log) Neye Yarar? Adli Delil

BY NC ND

Kayıt (Log) Neye Yarar? Olay Müdahale

BY NC ND

Kayıt (Log) Neye Yarar? Performans Ölçümü / Kapasite Planlama



BY NC ND

Kayıt (Log) Neye Yarar? Mevzuata Uygunluk

1. Firmalar yolsuzluk yaptı

2. Polisler yakaladı

Sarbanes Oxley
3. Politikacılar kanunu yazdı

4.Tasarı onaylandı

5. Bize de kurallara uymak kaldı

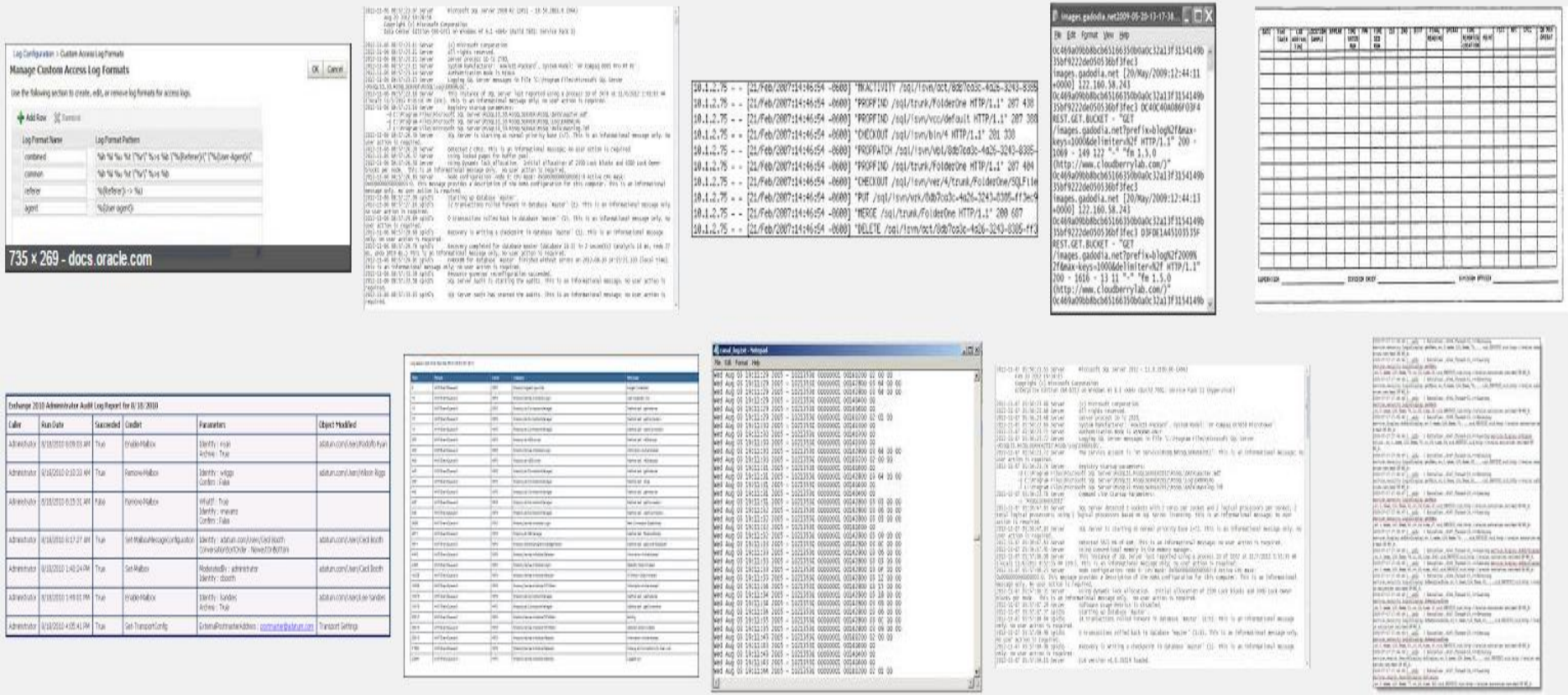
BY NC ND

Yaygın Kayıt Türleri

- Windows Eventlog
- UNIX Syslog
- Cisco Netflow
- Performans Kayıtları
- Uygulama Kayıtları
- Firewall
  - Checkpoint
  - Juniper Netscreen
  - Cisco PIX/ASA/FWSM
- IDS log formatları
  - Sourcefire Snort
  - McAfee Intrushield
  - Cisco IPS
  - Tippingpoint
- Web sunucuları
  - Apache
  - Tomcat
  - Internet Information Systems (IIS)

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Yaygın Kayıt Türleri - Örneğin;



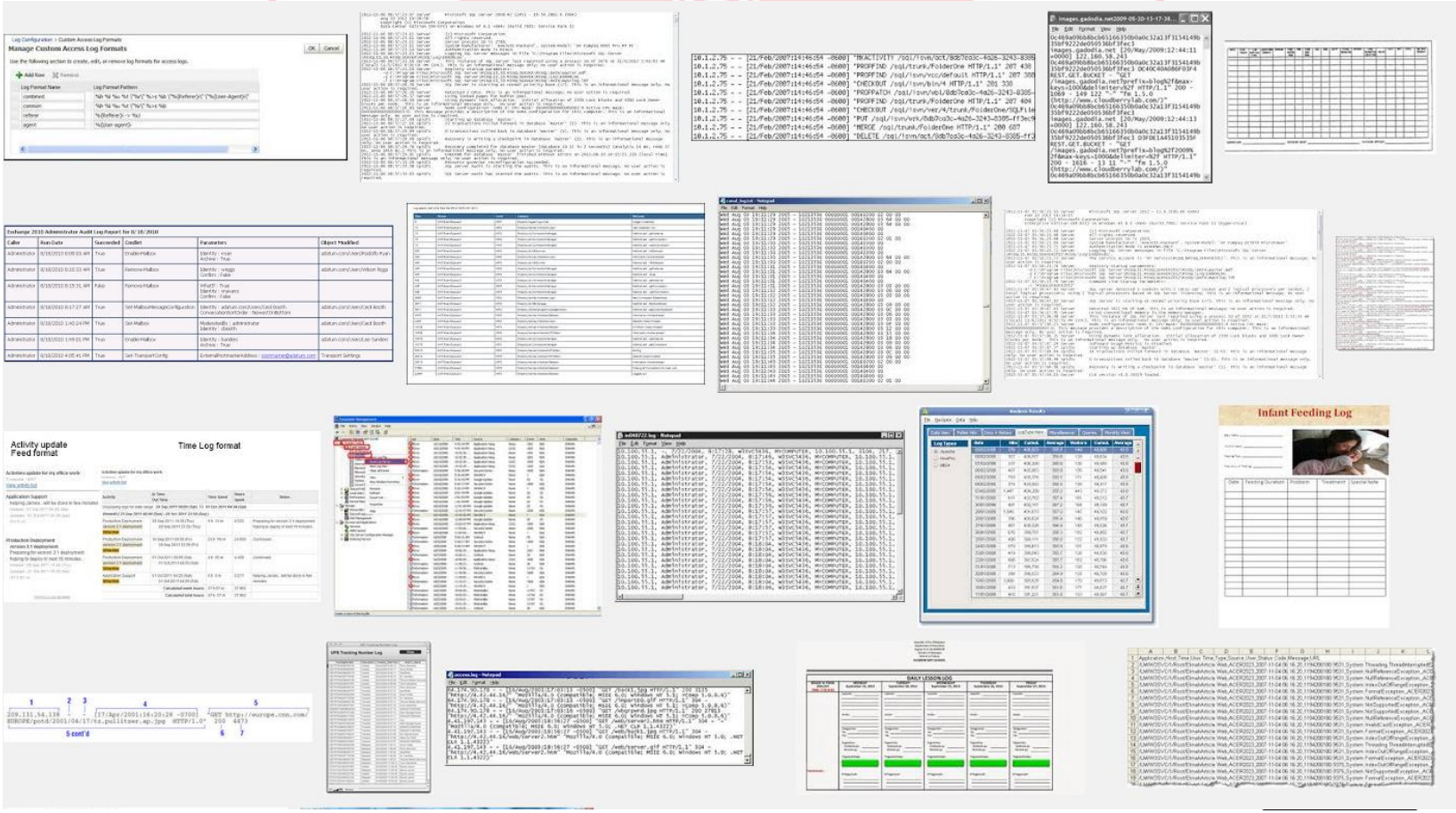
Kayıt Toplamada Karşılaşılan Problemler

- İzlenecek çok sayıda bileşen var
- Kayıtlar farklı yerlerde dağınık olarak duruyor

BY NC ND

Kayıt Toplamada Karşılaşılan Problemler

- Kayıt inceleme yazılımları tek başlarına yetersiz
- Farklı biçim ve türde çok fazla kayıt



eğitim.sge.gov.tr

Kayıt Toplamada Karşılaşılan Problemler

- Hata, ikaz, bilgi, uyarı?
- Protokol farklılıkları

IIS7 internet information services

Apache

UDP 514

sFlow

NetFlow

TCP/IP

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

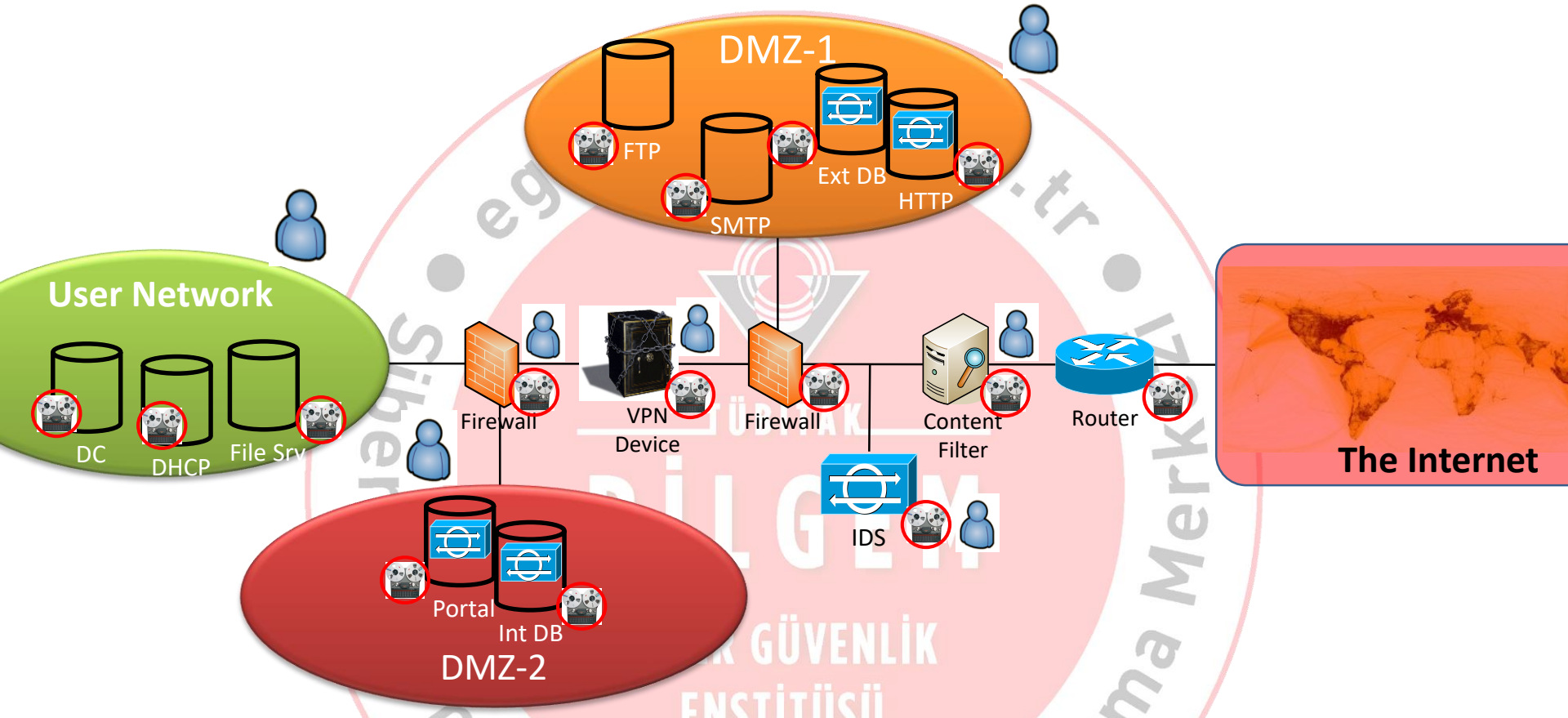
Kayıt Toplamada Karşılaşılan Problemler

- Farklı yapılandırma ayarları
- Standart bir formatın bulunmaması
- Uygulama bazlı kayıtlar

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

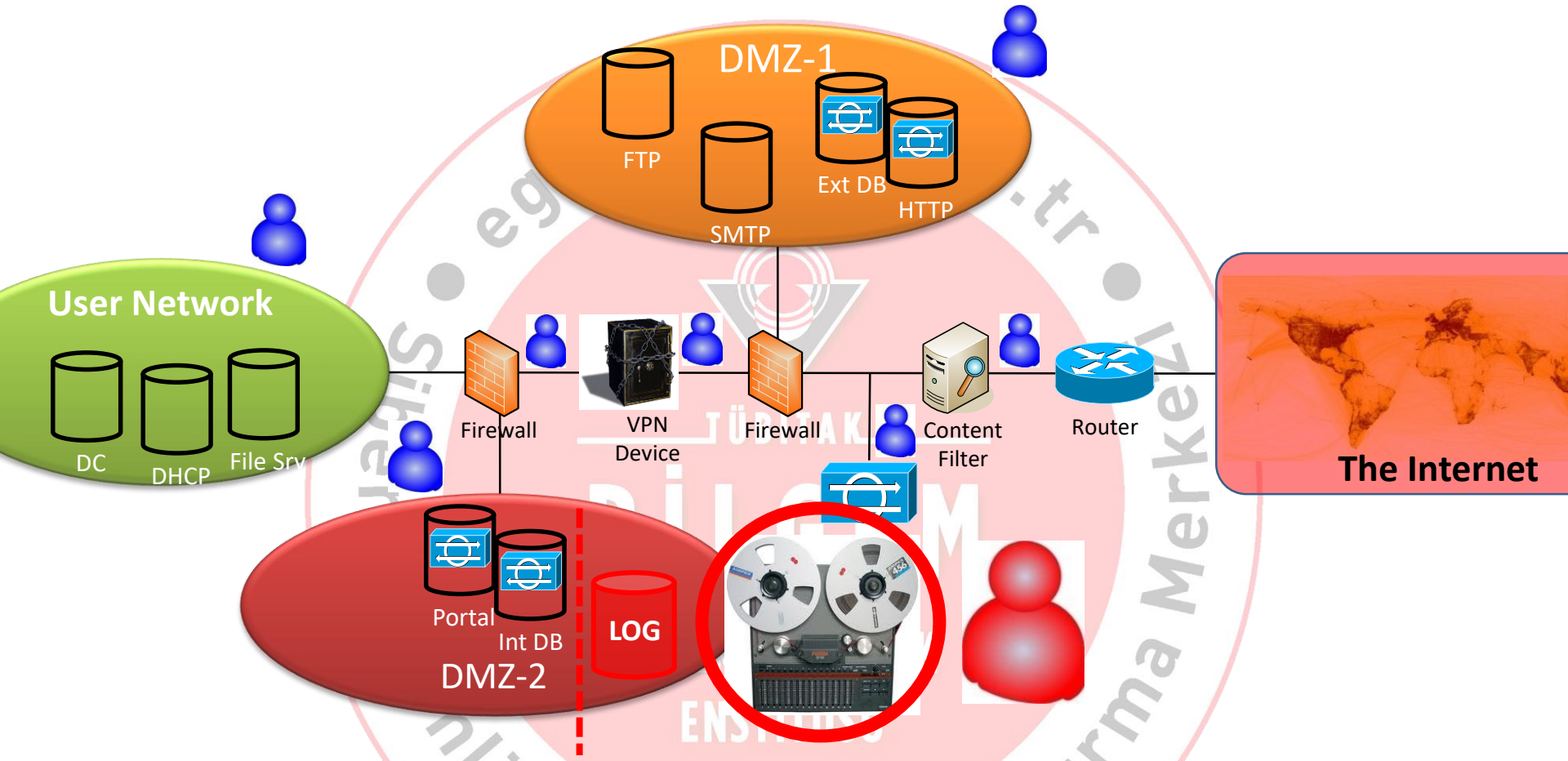
Kayıtların Toplanması (Mevcut Durum)



- Sunucu vb. bileşenlerin ürettiği **kayıtlar,** ürediği yerde saklanıyor.
  - Saklama alanı yeterli mi?
  - **Sistem yöneticileri** hatalarını örtebilir mi?
  - **Sistem yöneticilerinin** **kayıt yönetimi** konusunda eğitimli mi?

BY NC ND

Kayıtların Toplanması (İdeal Durum)

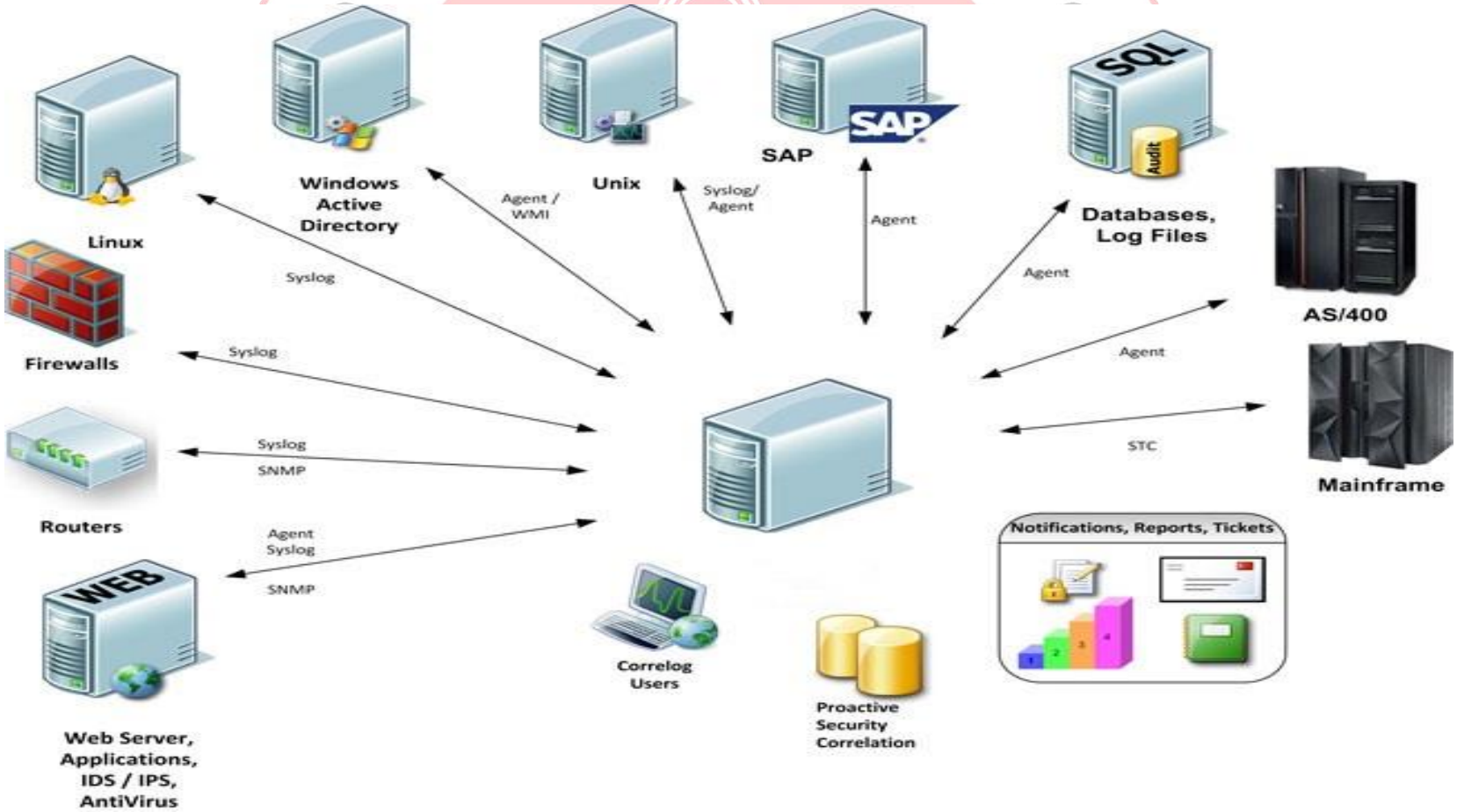


- Sunucu vb. bileşenlerin ürettiği kayıtlar, **kayıt sunucusunda** saklanır.
  - Saklama alanı tek noktada. Bakımı/izlenmesi kolay. («SIEM»)
  - **Sistem yöneticileri** hatalarını örtemez.
  - **Kayıt yöneticisinin** uzmanlaşması yeterli.

CC BY NC ND

Çözüm - Merkezi Kayıt Yönetimi

- BT altyapısı içerisinde gerçekleşen olaylara ait kayıtların belirlenmiş kriterlere göre merkezi olarak toplanması ve işlenmesidir.



Merkezi Kayıt Yönetiminin Yetenekleri

- BT altyapısından olan olaylar hakkında bilgi sahibi olma
- Sistemde olan kritik olaylar hakkında haber verme yetenekleri
- Gelişmiş saldırıların tespiti
- Olay ilişkilendirme
- Risk hesaplama
- Detaylı raporlama ve olay takibi
- Aynı kayıtların birleştirilebilmesi
- Uyarı, alarm mekanizmaları
- Dashboard'lar yardımı ile görsel analiz
- Mevzuata uyumluluk
- Kayıtların uzun süreli saklanabilmesi
- Adli analiz
- Gerçek zamanlı veri ve kullanıcı izleme
- Tehdit bilgisi
- Uygulamaların izlenmesi
- Tek merkezden yönetim

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Merkezi Kayıt Yönetiminin Faydaları - Detaylı Arama

- 18 Ocak 2014 tarihinde 20:00-24:00 saatleri arasında kimler çalışıyordu ?
- Bu zaman aralığında USB depolama aygıtlarını kullanan oldu mu ?
- Bu zaman aralığında dosya sunucusuna kimler erişti ?
- Muhasebe bilgisayarından ekran görüntüsü alan var mı ?
- Dosya sunucuda bulunan personel_bilgiler.xls ve maaşlar.xls dosyasına kimler erişti ?
- Yıllık finansal analiz raporunu kim, ne zaman , hangi yazıcıdan çıktı aldı ?
- E-Posta, Web ve yedekleme sunucularında ilgili servislerin durumu
- Etki alanı yöneticileri grubuna yeni bir kullanıcı eklendiğinde
- Etki alanına üye olmayan bir bilgisayar ağa bağlandığında
- Önemli sunuculara yazılım yüklendiğinde
- Önemli klasörlere yapılan erişimlerin günlük olarak sorumlusuna raporlanması
- Haftalık olarak yetkisiz erişim denemelerinin raporlanması
- Haftalık olarak hesabı kilitlenen kullanıcıların sayısı

cc BY NC ND

Merkezi Kayıt Yönetiminin Faydaları

- Teknolojik Faydalar
  - Gelişmiş saldırıların analizi kolaylaşmaktadır
  - Saldırıların ilerleme durumu ve zarar derecesi hakkında bilgi edinilebilmektedir.
  - Çok sayıda kayıt arasından gerçek önemli olaylar ayıklanabilmektedir.
  - Saldırılar önceliklendirilebilmektedir
  - Saldırılardan zamanında haberdar olunmaktadır
- Kurumsal Faydalar
  - Olay analizi kolaylaşmakta ve analizi yapması gereken personel azalmaktadır.
  - Personel sayısı zaten az ise daha etkin çalışması sağlanmaktadır
  - Hatalı pozitif olay kayıtları için iş gücü harcanmamaktadır.
  - Karşı önlemler yerinde ve zamanında alınabilmektedir.

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
eğitim.sge.gov.tr
CC BY NC ND

Kurulum Aşamaları - Planlama

- Kurum bilgi sistemlerinin varlık envanterinin çıkartılması
- Varlık envanterindeki varlıklara risk değeri ataması
- Kurum ağ topolojisinin çıkartılması
- Toplanacak kayıtların (logların) önceliklendirilmesi ve belirlenmesi
- Merkezi Kayıt Yönetimi ve Güvenlik İzleme Sistemi bileşenlerinin planlanması

eğitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Kurulum Aşamaları-Bileşenlerin Kurulumu

- Kayıt (Log) sunucularının kurulumu
- Merkezi Güvenlik İzleme sunucusunu kurulumu
- Sensorlerin kurulumu
- Raporlama araçlarının kurulumu
- Depolama alanlarının kurulumu

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Kayıtların Toplanması

- Uygulamalar
- Web / Uygulama sunucuları
- Veritabanları
- Yetkilendirme sunucuları
  - LDAP
  - AD
  - Aruba Radius
- İşletim sistemleri
- Windows
- Linux
- Sanallaştırma Sistemi
- Yedekleme sistemi
- Güvenlik cihazları
  - Güvenlik Duvarı
  - Saldırı Tespit ve Önleme sistemi (IDS/IPS)
  - Antivirus Sistemleri
  - İçerik Filtreleyiciler
  - Veri Kaçağı Önleme Sistemi
- Ağ ve aktif Cihazlar
  - Yönlendiriciler ve Anahtarlama Cihazları
  - Ağ Akış Kayıtları (Netflow)

siber.egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Saldırı Tespit Sistemi

- Dış ağa saldırı tespit ve önleme (IDS/IPS) kurulumu ve yapılandırılması
- DMZ saldırı tespit ve önleme (IDS/IPS) kurulumu ve yapılandırılması
- İç ağ saldırı tespit ve önleme (IDS/IPS) kurulumu ve yapılandırılması
- Kritik sunucularda denetim (loglarının açılması) kayıtlarının tutulması için yapılandırmaların yapılması

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Kayıtların Çözümlenmesi

- Tüm kayıtların çözümlemesinin yapılması
- Tüm kayıtlar için eklentilerin (plugin) yazılması
  - Regex
- Çoklu kayıtların indirgenmesi
- Normalization

e-eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

İlişkilendirme ve Saldırı Senaryoları

- Hazır ilişkilendirme kurallarının uyarlanması
- Muhtemel saldırı senaryolarının belirlenip kuralların oluşturulması
  - Brute force
  - Port scan
  - Pass the hash
  - Simetrik bağlantılar
  - Mesai dışı hareketler
  - Aşırı bandwith kullanımı
  - Aynı hesabın birden çok makinada login olması
  - Sistem yönetici makinalarına erişim denemeleri
  - Kritik kullanıcılara erişim denemeleri
  - Kritik sunuculara yetkisiz ağlardan erişim denemeleri
- Uyarı / önlem mekanizmalarının belirlenmesi
  - E-posta uyarı mekanizmalarının oluşturulması
  - Saldırı engelleme ya da saldırı tespit sistemi olarak çalışma modunun ayarlanması.

eğitim.sge.gov.tr • Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Dashboard Tasarımı

BY NC ND

Olay Müdahale ve Alarm Üretimi

- Üretilen alarmlar incelenir
- Gerekli durumlarda ilgili birimler harekete geçirilir
- Gerekli aksiyonlar alınarak sorun giderilir
- Sistem eski haline getirilir
- Sorunun kaynağı raporlanır
- Gerçekleştirilen tüm işlemler kayıt altına alınır
- Aynı sorunun tekrar yaşanmaması için ilgili önlemler alınır

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Raporlama

- Üretilecek raporların belirlenmesi
  - Yekilendirme ve kimlik doğrulama raporları
  - Ağ aktivite raporu
  - Zararlı yazılım aktivite raporu
  - Kritik hata ve göçme raporları
  - Sistem ve veri değişiklikleri raporu
  - Kaynaklara erişim raprorları
  - İhtiyacınız olan diğer raporlar
- Periyodik raporlar üretilerek incelenir

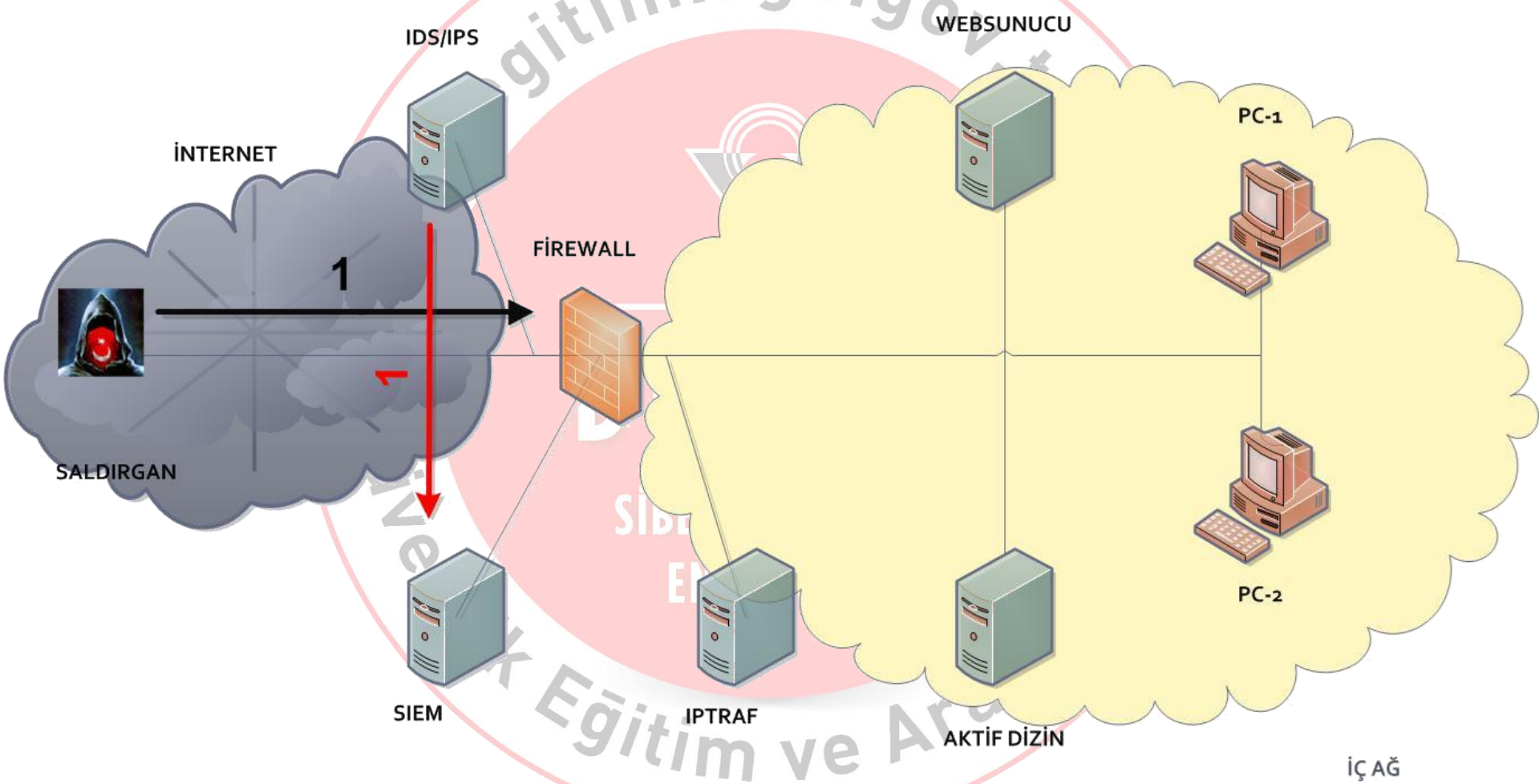
eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Örnek Saldırı Senaryosunun İncelenmesi

BY NC ND

Zafiyet Taramasının Tespit Edilmesi

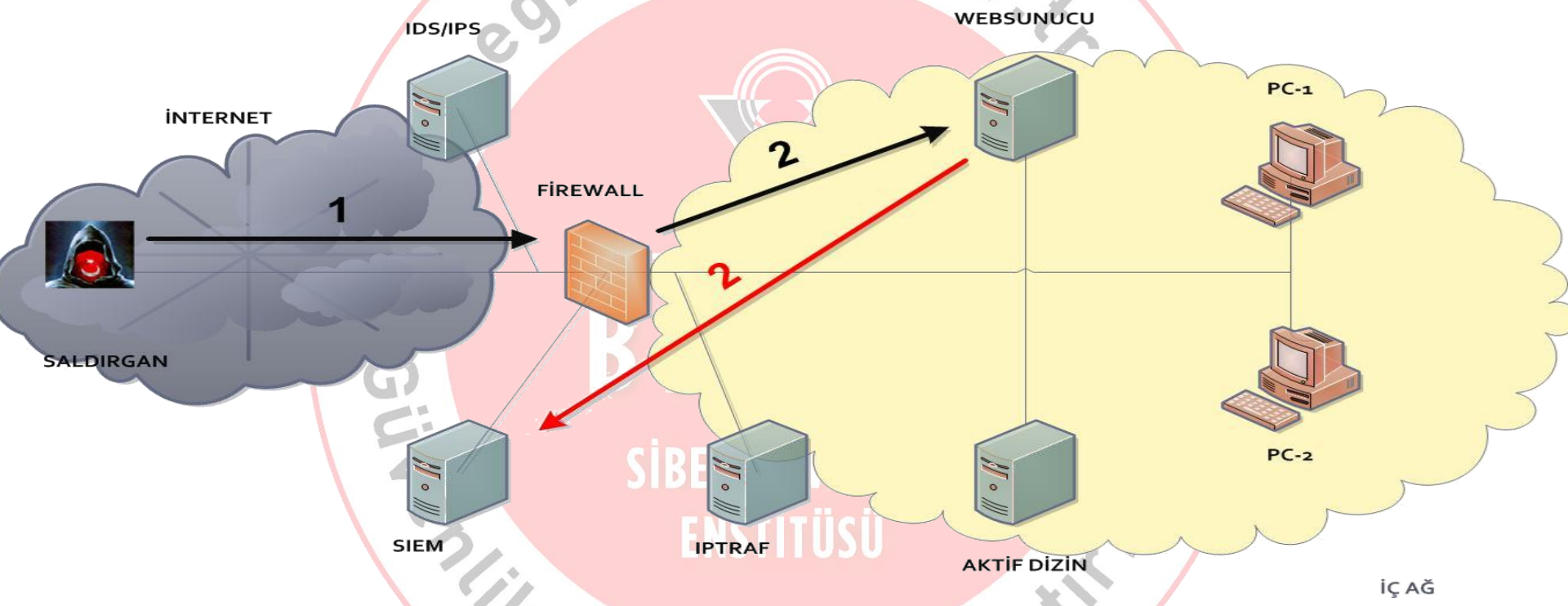
- Saldırı Tespit ve Önleme Sistemi (IDS/IPS) kayıtları



BY NC ND

SQL Enjeksiyonunun Tespit Edilmesi

- Web Sunucu Kayıtları

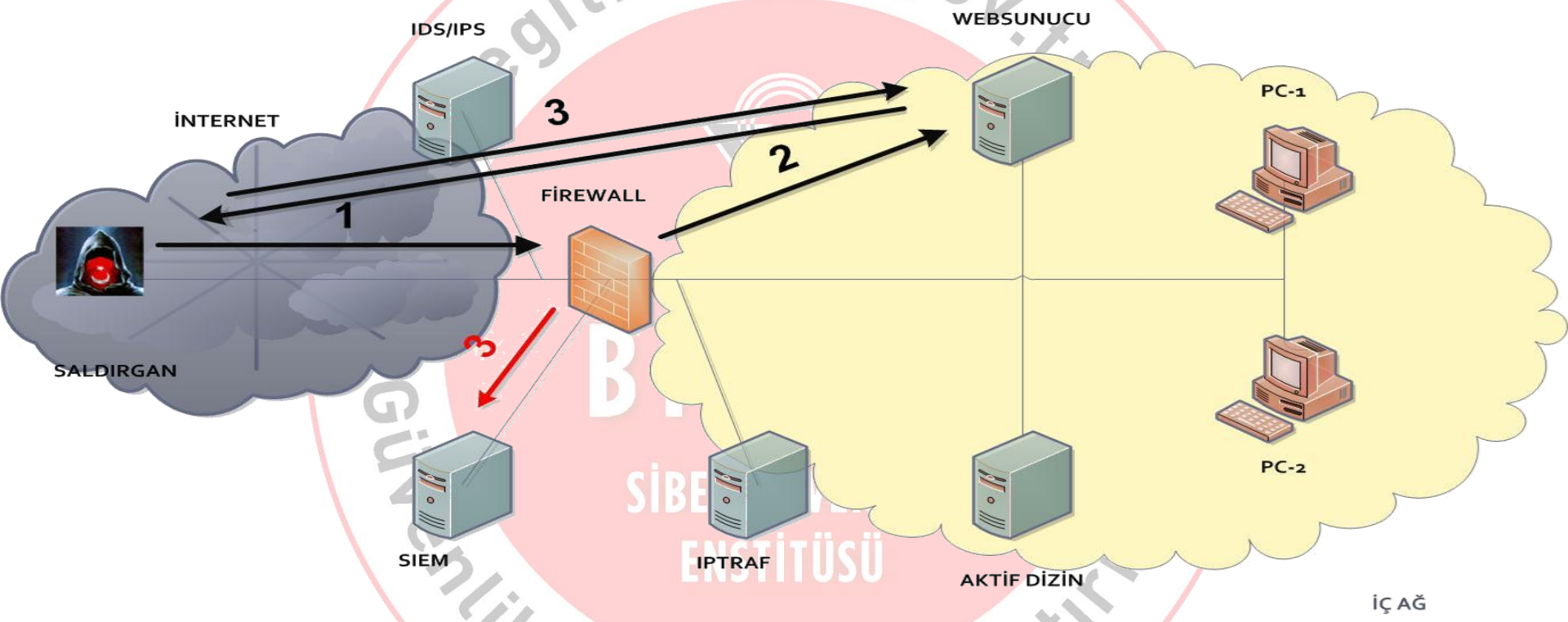


egitim.sge.gov.tr
Güvenlik Eğitim ve Araştır
SİBER ENSTİTÜSÜ

cc BY NC ND

TCP Bağlantısının Tespit Edilmesi

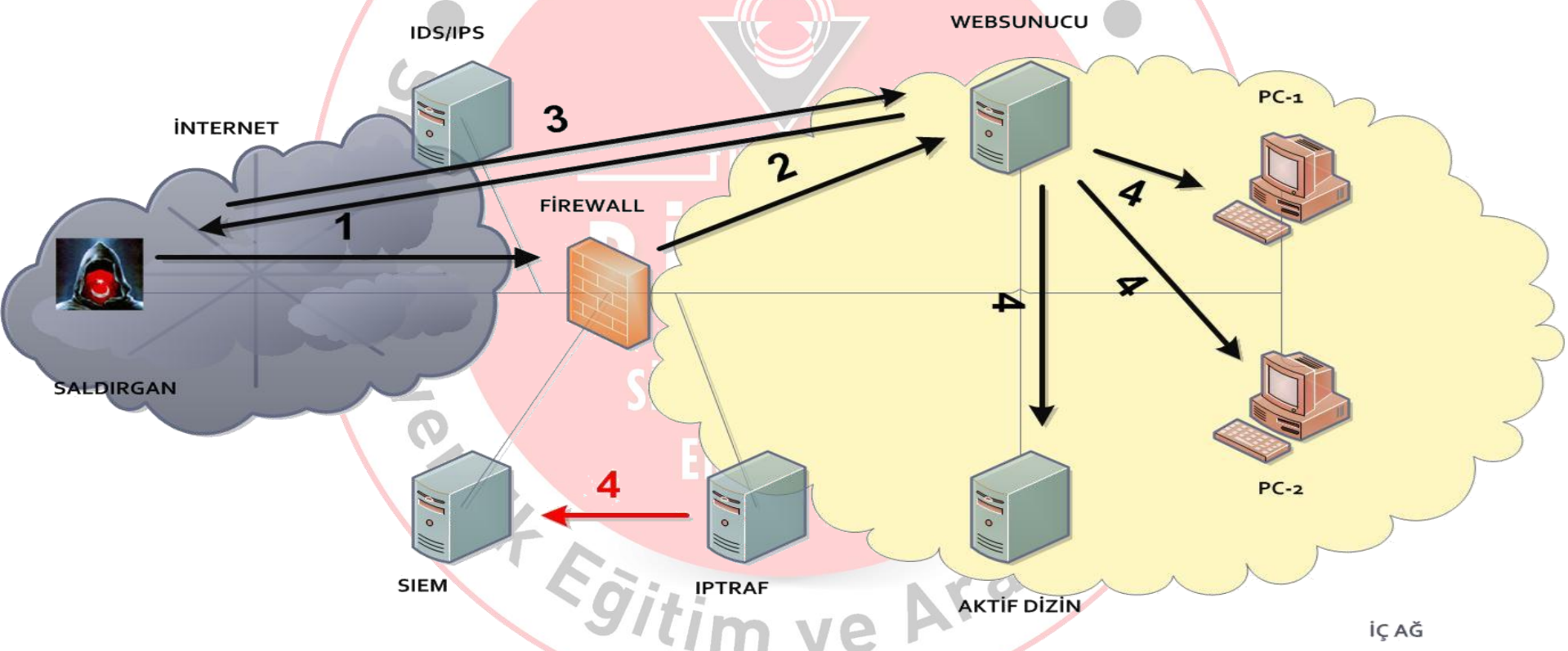
- Güvenlik Duvarı Kayıtları



egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ

Domain Admin Hesabının Eklendiğinin Tespiti

- Aktif Dizin Kayıtları



eğitim.sge.gov.tr

CC BY NC ND

Siber Olay Öncesi: Diğer Sorumluluklar

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Enstitüsü

TÜBİTAK
BY NC ND

Diğer Sorumluluklar

a. Görev ve sorumlulukların belirlenmesi,
b. Olay yönetimi (bildirim + müdahale) talimatlarının hazırlanması
c. Tatbikatlara katılımın sağlanması
d. USOM ve S-SOME etkinliklerine katılım
e. Güvenlik ürünlerinin seçimine destek
f. Güvenlik ürünlerinin kullanım politikaları

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
TÜBİTAK
CC BY NC ND

Siber Olay Esnasında

TÜBİTAK

BY NC ND

Olay Tipleri

1) Servis Dışı Bırakma Saldırısı («Denial of Service Attack»)
2) Sosyal mühendislik saldırıları («Spam», «Phishing» vb.)
3) WEB sayfalarının değiştirilmesi
4) Zararlı yazılım saldırısı
5) Yetkisiz erişim (Kurum içinden/dışından)
   - Cihaz çaldırma
6) Zafiyet tarama («Port scanning»)

Her olay tipi için

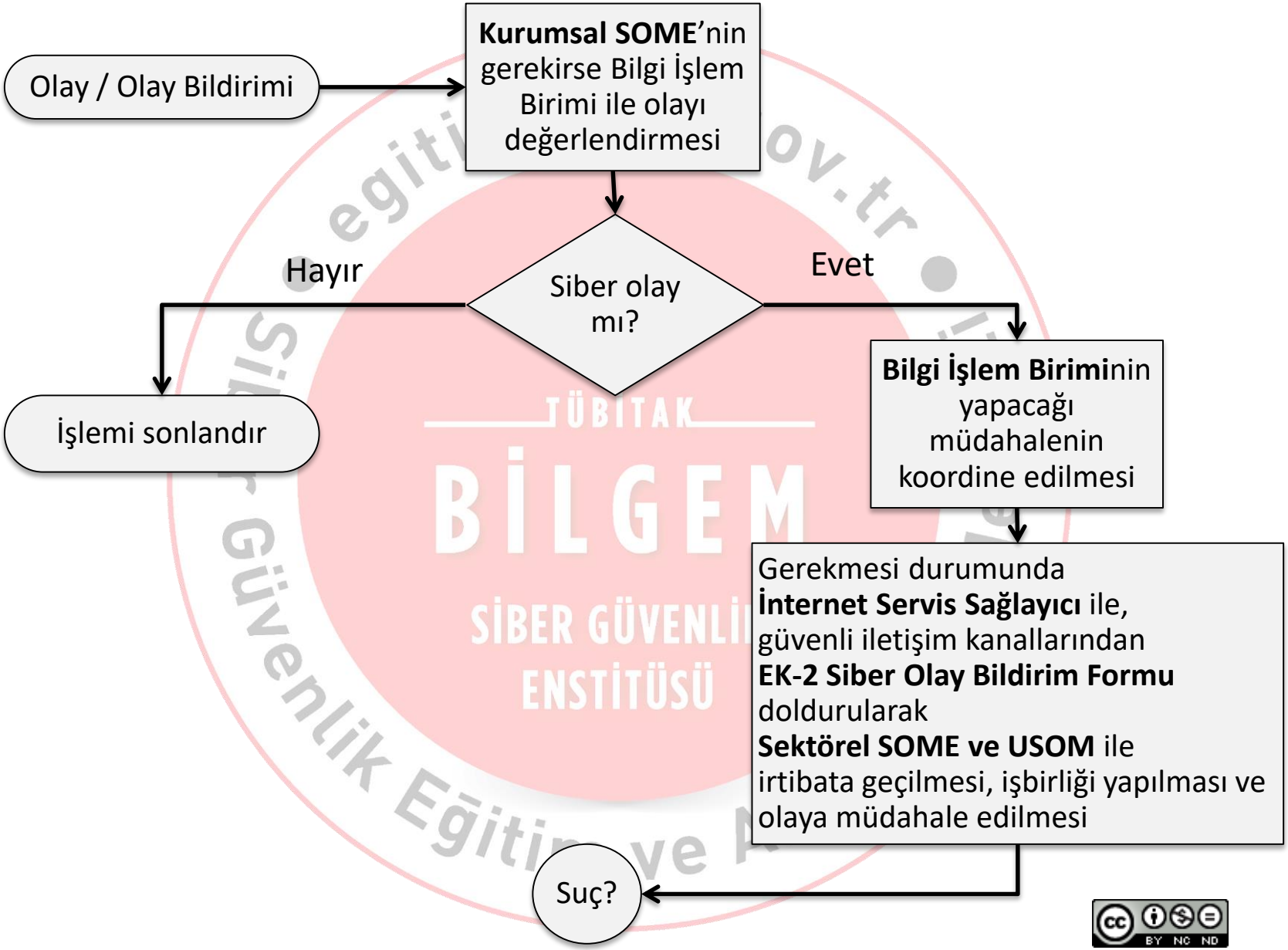
a. Kim/nasıl algılar?

b. Kim/nasıl düzeltir?

→ ***Cevaplar: Olay talimatları***

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
eğitim.sge.gov.tr
CC BY NC ND

Siber Olay Müdahale

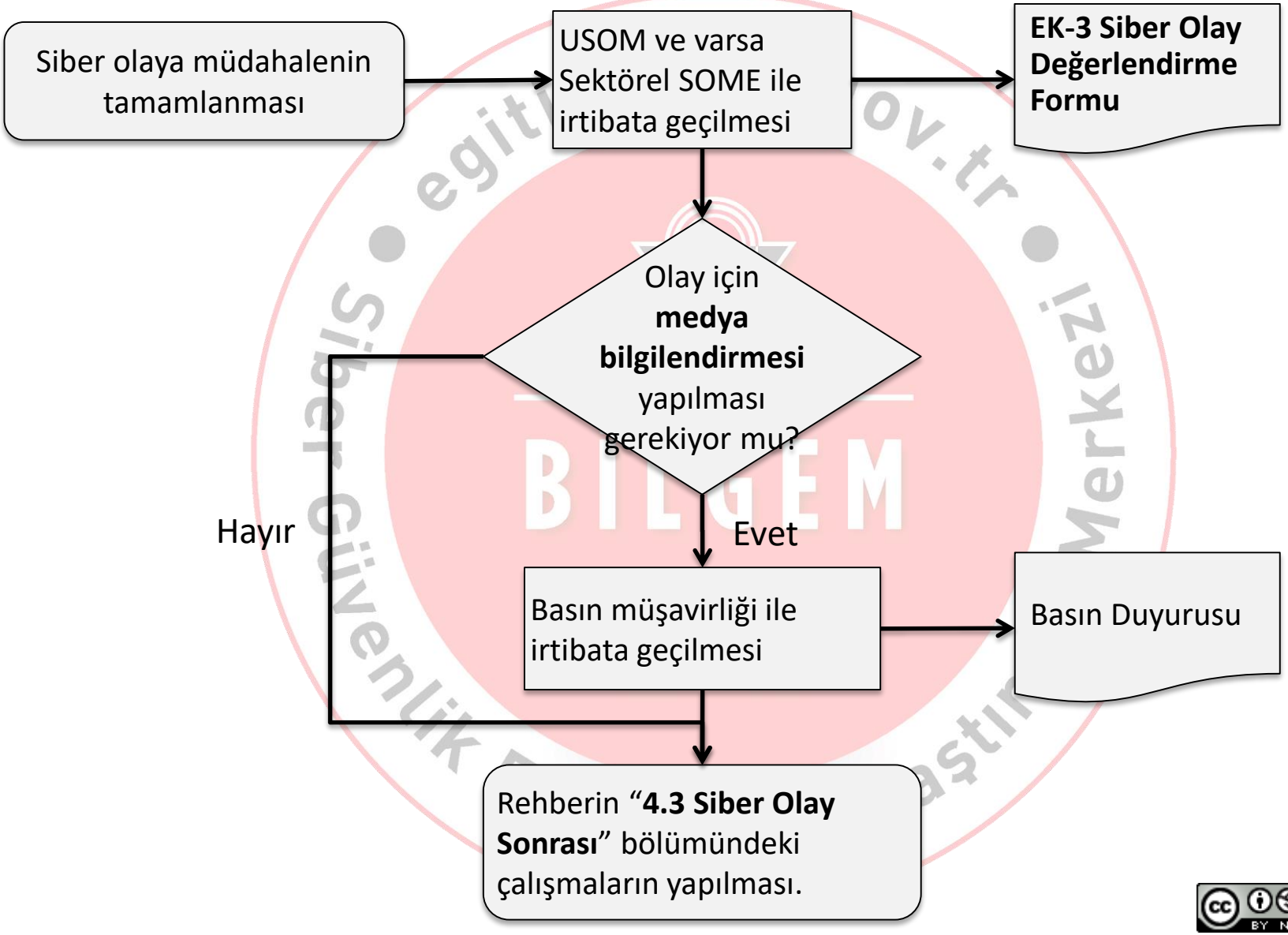


TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma
CC BY NC ND

Siber Olay Müdahale

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Siber Olay Müdahale



egitim.gov.tr • Siber Güvenlik Eğitim Merkezi • BILGEM

Tespit ve Analiz Aşaması

- Saldırı karakteristiğinin tespit edilmesi
- Tespit sistemlerinin izlenmesi kayıtlarının kontrol edilmesi
- Saldırı indikatörlerinin/vektörünün tespiti
- Olay raporlama

BY NC ND

Tespit ve Analiz Aşaması

- İz kayıtlarının toplanması ve korunması
- Acil durum, Felaket durumu
- SOME paydaşları ile durum değerlendirme
- Zararın/Kompromislerin tespiti. Zarar azaltma planının geliştirilmesi

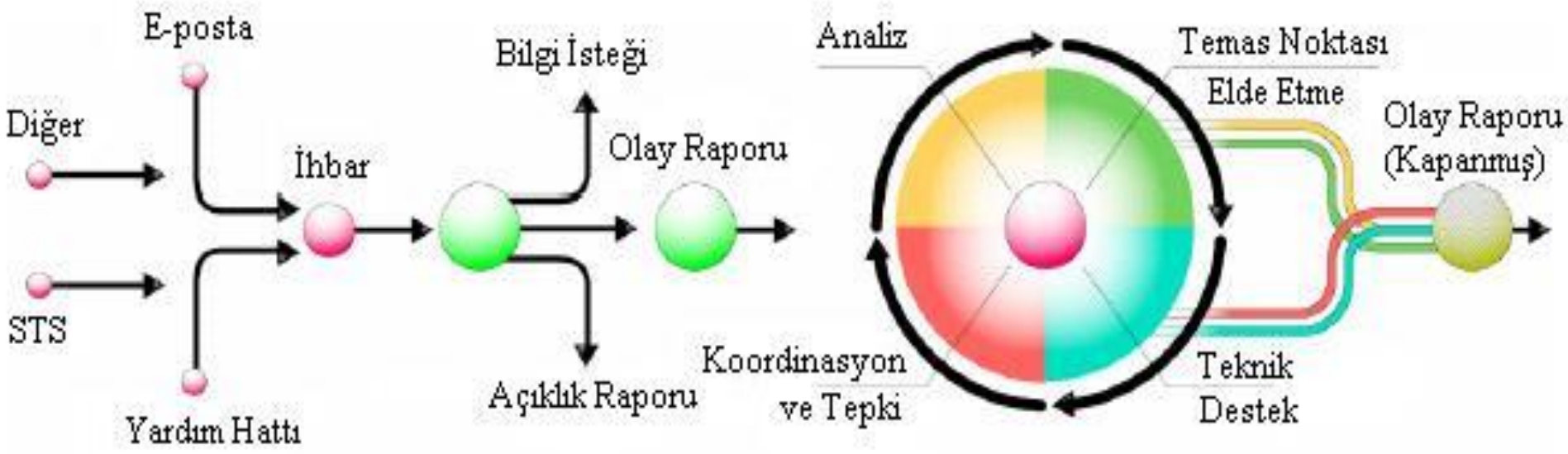
BY NC ND

Zarar azaltma ve sistem geri kurulumu

- Olayın durdurulması / izole edilmesi
- Sistemin zarardan temizlenmesi (Virüs, Truva vb..)
- Yeni kurulum / Sistemin tekrar çalışmaya başlatılması
- Sistemin geri kurulumun izlenmesi

BY NC ND

Olay Yaşam Döngüsü



ENSTİTÜSÜ
Eğitim ve Araştırma

UYGULAMA -1-

SENARYO

1.Kurumunuzun resmi web sayfasının içeriği yetkisiz kişilerce gerçekleştirilen saldırı sonrasında değiştirilmiştir.

2.Giriş sayfanıza saldırgan tarafından eklenen yazıda kurum çalışanlarınıza ve kurumunuzdan hizmet alan vatandaşlara ait bilgilerin ele geçirildiği ve yakında bu bilgilerin İnternet üzerinden yayımlanacağı görülmektedir.

3.25 Ocak 2016 tarihinde saat 13.35'te bilgi işlem biriminizi arayan kurum içi bir kullanıcının sayesinde durumdan haberdar olunmuştur.

4.Kurumunuzun uğradığı saldırıyla ilgili ulusal basın yayın organlarında 25 Ocak 2016 tarihinde saat 15.23'te haberler çıkmaya başlamıştır.

CC BY NC ND

UYGULAMA 1

AŞAĞIDAKİ SORULARIN CEVAPLARI BULUNMALIDIR.

1.Bilgi işlem birimine kurum içi kullanıcı tarafından ihbar geldikten sonra olay nasıl doğrulanmıştır?

2. Sayfanın ele geçirildiği belirlendikten sonra yapılan teknik faaliyetler nelerdir?

a. Sistemin ne zaman ele geçirildiği nasıl tespit edilmiştir?
b. Veri sızması olup olmadığı nasıl tespit edilmiştir?

3.Sayfanın tekrar uygun içerikle erişilebilir olması nasıl, ne kadar sürede sağlanmıştır?

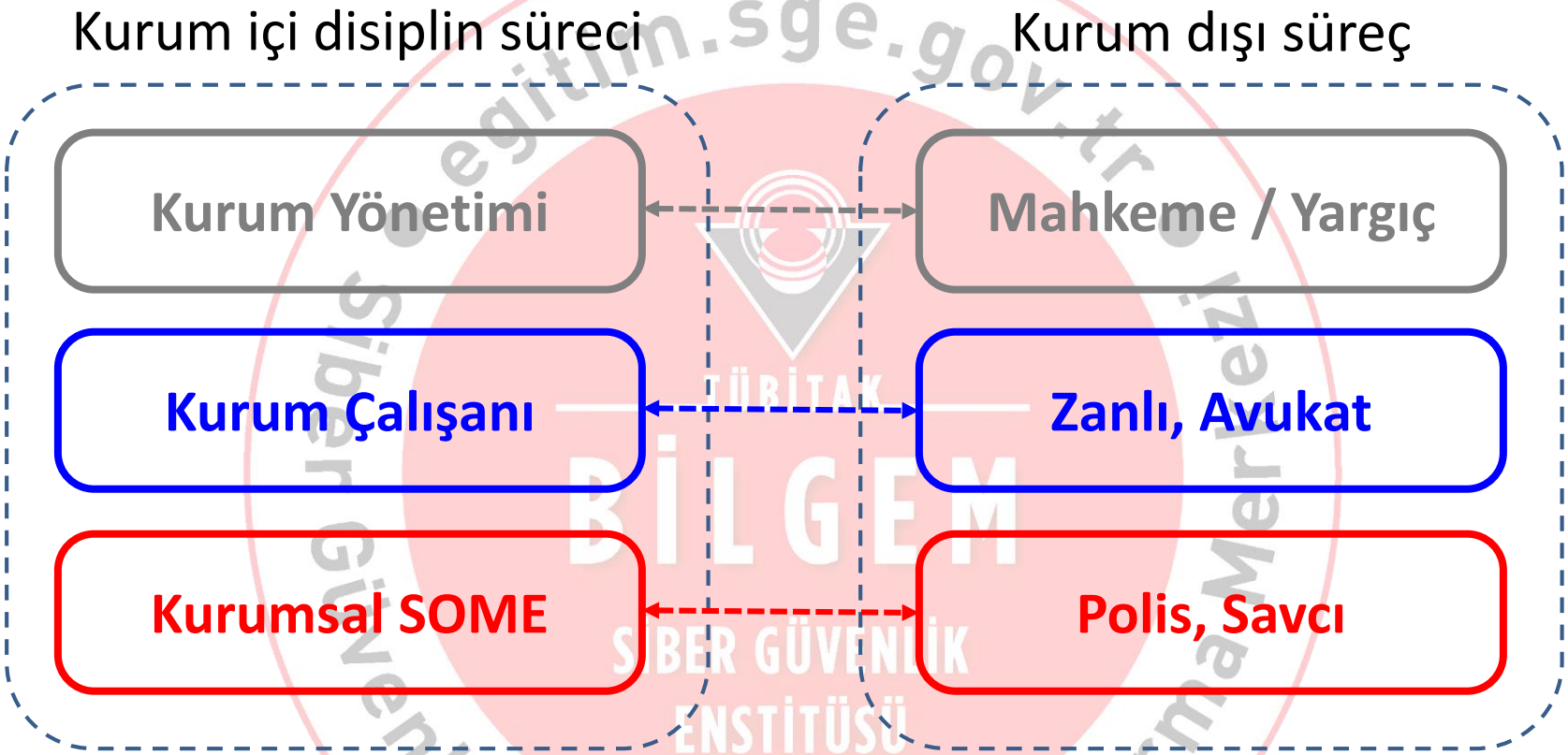
4.Diğer sistemlerin zarar görmesi nasıl önlenmiştir?

5.İlgili olayda hukuki olarak bir çalışma yapılmış mıdır?
a. Suç duyurusu ve ekleri nelerdir?

6.Basında çıkan haberlerden kurumun etkilenmemesi için ne yapılmıştır?

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Kurum içi/ Kurum Dışı Disiplin Süreçleri



Olay, yönetimin kararı ile kurum dışına taşınabilir. Gerekçeler:

1. Saldırgan kurum dışından
2. Saldırının etkisi çok büyük. Paydaşlar etkilenmiş, olay duyulmuş durumda

Olay Müdahale- Gizlilik

- Paydaşlarla bilgi paylaşım esasları:
  - Başka SOME'lerle bilgi paylaşma
  - Üreticilerle bilgi paylaşma
  - Uzmanlarla bilgi paylaşma
- Bilgi paylaşma metodu
- Paylaşılan bilginin temizlenmesi

eğitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Olay Müdahale – Önceliklendirme-Triage

- Olay Müdahale Servisi'ne ulaşan tüm bilgilerin hangi yoldan olursa olsun (Telefon, e-posta, faks vs.) tek bir noktadan ulaşmasını amaçlar.
- Ulaşan bilgilerin gerekli olan SOME iç birimlere iletilmesi bu işlevin görevidir.
- İşlevin tam yerine getirilebilmesi için servis çalışanlarının telefon ve e-posta gibi iletişim bilgileri gizli tutulmalıdır.
- Birçok servis için tek önceliklendirme işlevi kullanılabilir.

BY NC ND

Olay Müdahale Servisi - Önceliklendirme

- Önceliklendirme İşlevinin yerine getirilebilmesi için sorumluluk alanı aşağıdaki konularda önceden bilgilendirilmelidir:
  - Açıkça tanımlanmış bir temas noktası
  - Temas noktasının erişilebilirliği hakkında detaylı açıklamalar
  - İzlenecek prosedürler (basit, iyi tanımlı)
    - Ne zaman hangi yolla rapor iletilecek
    - Raporda hangi bilgiler bulundurulacak
- Hangi olaylara müdahale edileceğiyle ilgili açıklamalar
- Rapor eden kişinin kullanacağı destek dokümanları (Rapor formları vs.)

egitim.sge.gov.tr
TÜBİTAK BİLGE SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Olay Müdahale - Cevap

– Temas noktasına bilgi ulaşınca, alındı bilgisi gönderir.
– Temas kendisine gelen bilgileri, çağrıları

- **Eğer şifreliyse, dosyayı açar**
- **Önceliklendirir**
- **İzleme numarası verir**
- **Servis içerisindeki ilgili işleve iletir**

– Eğer gelen form basılı kopyaysa bunu dijital ortama aktarır ve basılı kopyayı saklar.

egitim.sge.gov.tr • İzleyici
TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü
Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Olay Müdahale-Yazılım

– Temas noktası kendisine ulaşan bilgileri otomatik olarak işleyebilmek için çeşitli yazılımlar kullanabilir.

– Kullanılacak yazılımlarla:
  - **Yeni olaylar**
  - **İzlenme durumunda olan olaylarla ilgili bilgiler**
  - **Kapatılmış olaylarla ilgili bilgiler**
  - **Ayrı olarak izlenen ama aralarında ilişki olabilecek olaylar**
  - **Olay müdahale servisinin kapsamı dışında kalan olaylar**

olarak belirlenebilir.

BY NC ND

Olay Müdahale Servisi – Olay Tespit

– Bu işlevin amacı sorumluluk alanı tarafından gelen çağrılara ve ulaşan raporlara cevap verebilmektir.

– Minimum olarak işlev aşağıdaki özellikleri bulundurmalıdır:
  - Raporlama Noktası
  - Analiz
  - Uyarı

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma
BİLGİ
SİBER GÜVENLİK ENSTİTÜSÜ

TÜBİTAK

Kayıt Dosyalarının İncelenmesi

- Güncel birçok sistem kayıt dosyası içerir.
- Kayıt dosyalarında,
  - Kim, ne zaman, nereden sisteme girdi
  - Ne çeşit bir yolla sisteme girildi (SSH, telnet, rlogin vs.)
  - Hangi adreslere e-posta yollandı
  - Sistemde hangi tarihte ne tür hatalar meydana geldi

  benzeri bilgiler bulunur.

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi • TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

TÜBİTAK

Deliller nerede incelenmeli?

- Genelde zararlı kodlar hedef sistem üzerinde incelenmez.
- Olayın gerçekleştiği sistemin mümkün olabildiğince benzeri izole bir test ortamı oluşturulmalı ve analizler burada yapılmalıdır.(Sanallaştırma)
- Test ortamının başka ağlara bağlantısı varsa mutlaka güvenlik duvarı kullanılmalı.
  - INND testinin canlı sistemde yapılması

egitim.sge.gov.tr
BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Bilgi Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Olay Müdahale Servisi – Olay Analizi

Yazılım ortamının analizinde aşağıdaki kurallara dikkat edilmelidir:

- Yazılım ortamının incelenmesi ve analizi delil analizi yapan kişi tarafından yapılmalıdır.
- Delilleri elde etmek ve analiz etmek için canlı sistemin birebir eşi (yazılım versiyonu, uygulanan yamalar, sürücüler vs.) olan bir sistem kurmak gereklidir.
- Canlı sistemin üzerinde delilleri test etmek büyük hasara sebep olabilir.

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Olay Bilgisinin Saklanması

- İzlenen olay bilgilerinin saklama süresi SOME politikalarına bağlı olarak belirlenir.
- Olayın tekrar açılma ihtimali olduğundan olay bilgileri en az birkaç ay saklanmalıdır.
- Olay bilgilerinin saklandığı ortamın güvenliğine dikkat edilmelidir. (Fiziksel güvenlik, kripto, erişim kontrolü vs.)

e-egitim.bilgem.tubitak.gov.tr
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Bilgi Güvenlik Eğitim ve Araştırma Merkezi

Olay Müdahale – Duyuru

- Duyuru işlevi sorumluluk alanı için uygun hale getirilmiş bilgi üretir ve bunun dağıtımını yapar
- Duyuruların amaçları:
  - Etkisi devam eden tehditler hakkında açılamalar yapmak
  - Sorumluluk alanının sistemlerini bu tehditlerden korumak, bu tehditleri tespit ve tedavi edecek yöntemleri sağlayarak saldırıya uğramış sistemleri kısa zamanda eski hallerine getirmek
  - SOME'ye yeni rapor edilmiş saldırıların kapsamı ve izleri hakkında bilgi vermek.
- Duyuru işlevi yerine getirilirken aşağıdaki hususlar dikkate alınmalıdır:
  - Bir SOME'de duyuru servisi olmak zorunda değildir, isteğe bağlı bir servistir.
  - SOME'nin günlük bir işi olarak yapılmalıdır.
  - Olay Müdahale servisinin bir parçası olmak zorunda değildir, kendi başına bir servis olarak da işleyebilir.
  - Bir saldırı hakkında bilgilendirme yapılırken saldırıdan korunmayı sağlayacak bilgi verilir, saldırıda hakkında gereğinden fazla bilgi vererek saldırının gerçekleştirilmesine imkan verilmez.

egitim.sge.gov.tr
TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü
Ulusal Eğitim ve Araştırma Merkezi
CC BY NC ND

Olay Müdahale Servisi – Olay KApatma

– Bir olay kapatılırken,

- Olayın kapatıldığı olayla ilgili tüm şahıslara bildirilmelidir.
- Olay yeni bilgi geldiğinde tekrar açılabilir.

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Siber Olay Sonrası

TÜBİTAK

BY NC ND

Siber Olay *Sonrasında* Görev ve Sorumluluklar

- Bilgi İşlem ve kurum içi paydaşlarla
  - Açıklığın belirlenmesi
  - Olay türü + Maliyetin ölçülmesi
  - Düzeltici/Önleyici faaliyetlerin önerilmesi

- Müdahale Raporu → Kurum üst yönetimi, USOM, S-SOME

- EK-3 Değerlendirme Formu → USOM, S-SOME

eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Düzeltici Önleyici Faaliyet

- Tek bir olayın zararını ortadan kaldırmak değildir.
- Kök Sebep analizinin yapılması
- Olaya neden olan açıklığı ortadan kaldırmaktır
  - Politika güncelleme
  - Süreçte düzeltme
  - Prosedür güncelleme
- Düzeltici / önleyici faaliyet maliyetinin olay maliyetinden düşük olması

eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
TÜBİTAK
CC BY NC ND

SOME Operasyonel Elemanları

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ
BY NC ND

SOME Operasyonel Elemanları: İnsan Kaynağı

egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ

TÜBİTAK

CC BY NC ND

Hatırlayalım !! SOME Birimleri/Faaliyet Alanları

Kurumsal SOME

- SOME birimi yönetimi fonksiyonu
- Olay müdahale yönetim ve koordinasyon fonksiyonu
- Sistem test ve denetimi fonksiyonu
- Kurumsal siber güvenlik bilinçlendirme fonksiyonu
- İz kayıt analiz fonksiyonu

Kurumsal SOME Fonksiyonları

TÜBİTAK
SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

İnsan Kaynağı

- SOME Yöneticisi
  - Kurumsal SOME'nin, temel sorumluluğu siber güvenlik olan bir amir yönetiminde,
  - en az lisans derecesine sahip
  - Bilgi güvenliği/Siber güvenlik konusunda uzmanlaşmış
- Kurumsal SOME Faaliyeletleri için birer personelin bulunması tavsiye edilmektedir
  - SOME birimi yönetimi fonksiyonu
  - Olay müdahale yönetim ve koordinasyon fonksiyonu
  - Sistem test ve denetimi fonksiyonu
  - Kurumsal siber güvenlik bilinçlendirme fonksiyonu
  - İz kayıt analiz fonksiyonu

En İdeal Durumda 6 Kişilik bir ekibin kurulması tavsiye edilmektedir

egitim.sge.gov.tr
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma
CC BY NC ND

İnsan Kaynağı

- Personel
  - ön lisans veya lisans programlarından mezun
  - 2 yıl bilgi işlem tecrübesine sahip
  - bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip
- Hizmet alımı
  - Birikim ve tecrübe kriterlerinin uygunluğu
  - güvenlik soruşturması (adli sicil kaydı, şahıs güvenlik belgesi vb.
  - Gizlilik sözleşmesi
  - Risklerin gözetilmesi

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

İnsan Kaynağı

- Personel
  - ön lisans veya lisans programlarından mezun
  - 2 yıl bilgi işlem tecrübesine sahip
  - bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip
- Hizmet alımı
  - Birikim ve tecrübe kriterlerinin uygunluğu
  - güvenlik soruşturması (adli sicil kaydı, şahıs güvenlik belgesi v.b.
  - Gizlilik sözleşmesi
  - Risklern gözetilmesi

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Eğitim

Temel Yetenek	Eğitimler
Açıklık Analizi	Temel Güvenlik Denetim Eğitimi Sistem Güvenlik Denetim Eğitimi Sızma Testleri Eğitimi Saldırı Teknikleri Eğitimi
Kayıt Yönetimi	Saldırı Tespit Sistemi Eğitimi Kayıt Yönetimi Eğitimi Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü Eğitim ve Araştırma Merkezi

CC BY NC ND

Eğitim

Temel Yetenek	Eğitimler
Siber Olay Müdahale	SOME Eğitimi Bilgi Sistemleri Adli Analizi Eğitimi Bilgisayar Adli Analizi – Derinlemesine Windows Eğitimi İleri Bilgisayar Adli Analizi ve Olay Müdahale Eğitimi Ağ Adli Analizi Eğitimi Zararlı Yazılım Analiz Yöntemleri Eğitimi DDoS Saldırıları ve Korunma Yolları Eğitimi Bilişim Hukuku
Bilgi Güvenliği Yönetimi	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi ISO 22301 İş Sürekliliği / Felaket Kurtarım Planlaması Eğitimi

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü Eğitim ve Araştırma Merkezi

SOME Operasyonel Elemanları: Yazılım Donanım

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Fiziksel Ortamlar

- Kritik Bilişim sistemleri odaları giriş-çıkış kayıtları,
- Kritik Bilişim sistemleri odaları giriş-çıkış kamera kayıtları,
- Çalışma ortamları giriş-çıkış kayıtları,
- Çalışma ortamları giriş-çıkış kamera kayıtları.
- Hizmet alımı
  - Birikim ve tecrübe kriterlerinin uygunluğu
  - güvenlik soruşturması (adli sicil kaydı, şahıs güvenlik belgesi vb.
  - Gizlilik sözleşmesi
  - Risklerin gözetilmesi

eğitim.sge.gov.tr
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Sanal Ortamlar

Sanal ortam kayıtları:

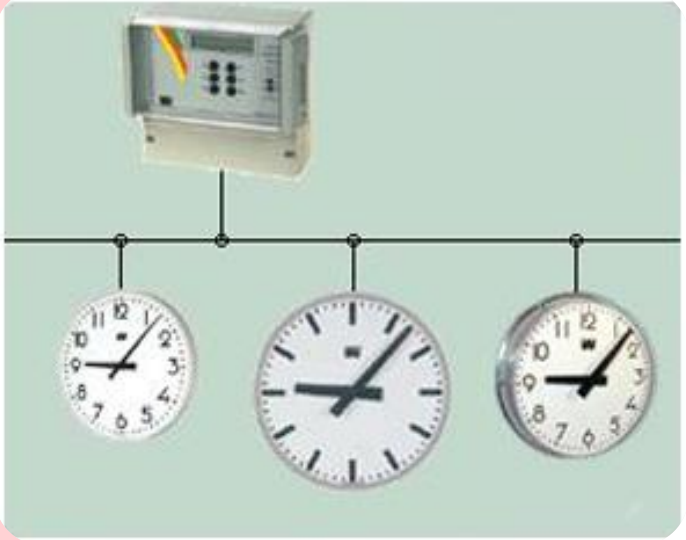
- Güvenlik duvarları,
- Antivirüs yazılımları,
- Saldırı tespit/önleme sistemleri,
- Yönlendiriciler ve anahtarlama cihazları,
- Sunucular,
- İş uygulamaları (Kritik Kurumsal projeler),
- Veri tabanları,
- Sanal özel ağ sistemleri

e-eğitim.sge.gov.tr
TÜBİTAK BİLGİ SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma

Merkezi İz Kayıt Yönetimi

- Merkezi kayıt yönetimi yazılımının
  - iz kayıtlarının daha etkin, verimli ve güvenli bir şekilde toplanması, ilişkilendirilmesi, arşivlenmesi, raporlanması nı sağlamalıdır

- Saat Senkronizasyonu
  - Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması
  - Ağ Zaman Protokolü (NTP-Network Time Protocol) sunucusu kurulması
  - Kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesi
  - Bunun yanında farklı ülkelerde birimleri olan kurumlar için saat dilimi (timezone) de dikkate alınmalıdır.



eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

TÜBİTAK

Teşekkürler