“An attacker only needs to find one weakness while the defender needs to find every one,

Endüstriyel IT Sistemlerinde Siber Güvenlik

Huzeyfe ÖNAL

BGA Bilgi Güvenliği

A skilled and motivated attacker will always find a way.”

Ajanda

1. Kritik altyapı kavramları, protokoller ve detaylar

2. Türkiye ve Dünya’da ICS/SCADA Güvenliği Konusunda Gelişmeler & Son Durum

3. ICS/SCADA Sistemler Nasıl Hacklenir, Güvenlik Denetimi Nasıl Gerçekleştirilir?

4. Daimi/Düzenli ICS Güvenliği için Yol Haritası Ne Olmalı?

BGA Bilgi Güvenliği

- 2008 yılından beri kurumlara Siber Güvenlik konusunda danışmanlık sunuyoruz. (Ar-ge/Yazılım, Eğitim, Danışmanlık…)
- Ankara, İstanbul ve Bakü ofisleri
- Ağırlıklı olarak çalıştığımız sektörler: Sigortacılık, E-ticaret, Finans, Telekom, Kamu ve Enerji
- “BGA Group” olarak aktif 35 güvenlik danışmanı ile hizmet vermekteyiz.

BGA - ICS/SCADA Güvenliği İlişkisi

- SCADA Eğitimleri
  - Farkındalık Eğitimi
  - Güvenlik Eğitimi

- SCADA Penetration Test Hizmeti

- Security Assessment (NIST Uyumlu) & Score Card

- SCADA “Security Operation Center” Kurulumu
  - Türkiye’de tek
  - Açık kaynak kod ürünler kullanarak

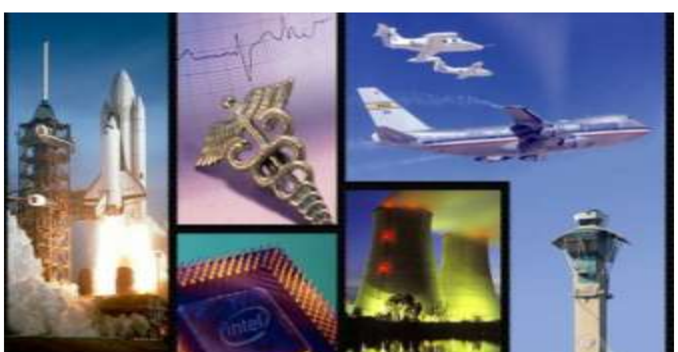
Katılımcılar

- Kaç kişi SCADA ile ilgili bir konuda çalışıyor
- Kaç kişi SCADA kelimesi/tanımını daha önce duymuş
- SCADA Denilince aklınıza ilk gelen nedir?
- Sizce elektrikleri kim kesti?

Kritik Altyapı Tanımı ve Önemi

- Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir.

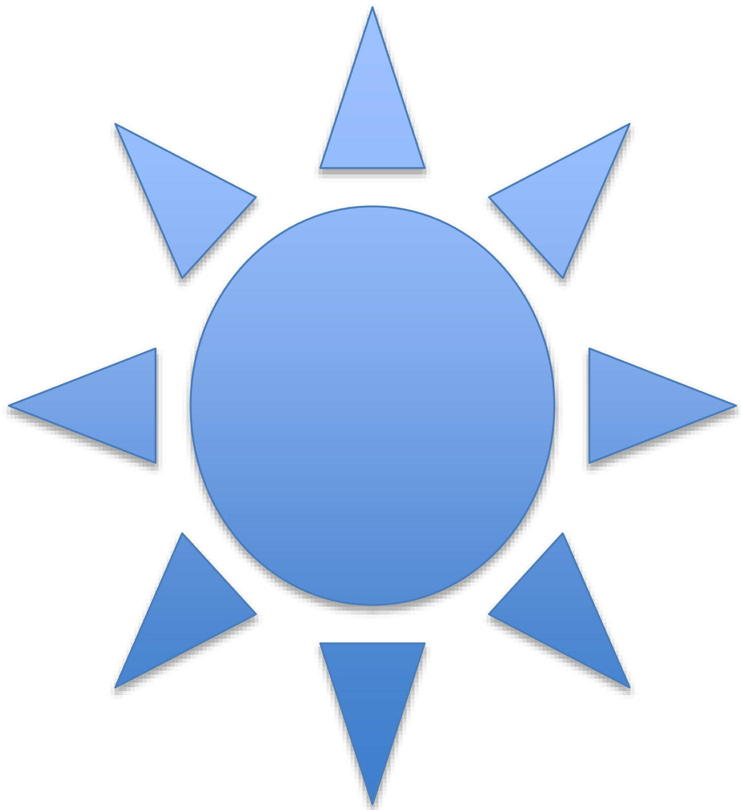
- Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir.



Internet of Things atası(!)

https://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html

Türkiye’nin En(?) Kritik Sistemi Nedir?



Kritik Altyapı Çeşitleri

- BT’yi kullanan kritik altyapılar:
  - Ulaşım
  - Bankacılık ve finans
  - Sağlık ve acil durum servisleri
  - Kritik kamu servisleri
- Tamamen BT’den oluşan kritik altyapılar:
  - Telekomünikasyon
- SCADA ile kontrol edilen ve izlenen kritik altyapılar:
  - Kritik üretim tesisleri
  - Enerji ve su
  - Elektrik…

SCADA Ne Amaçla Kullanılır... Örnekler

- Evimize gelen elektrik
- Evimize gelen su
- Trafik ışıkları
- Doğalgaz üretimi
- Ofisteki ısı derecelerinin ayarlanması
- Bindiğimiz trenin güvenliği, yönetimi
- Nükleer enerji santrallerinin yönetimi

Kritik Altyapılar ve IT Ortamlarından Farkları

Corporate IT	Automation Systems IT
Not life threatening	Safety first
Availability important	Non-interruption is critical
Transactional orientation	Real-time focus
IBM, SAP, Oracle, ...	ABB, Emerson, GE, Honeywell, Siemens...
People ~= Devices	Few people; Many, many devices
PCs and Servers	Sensors, Controllers, Servers
Web services model is dominant	Polled automation control model
MS Windows is dominant OS	Vendor-embedded operating systems
Many commercial software products installed on each PC	Purpose-specific devices and application
Protocol is primarily HTTP/HTTPS over TCP/IP -- widely known	Many industrial protocols, some over TCP/IP – vendor and sector-specific
Office environment, plus mobile	Harsh operating plant environments
Cross-industry IT jargon	Industry sector-specific jargon
Cross-industry regulations (mostly)	Industry-specific regulations

Kaynak: Gartner ICS Reports, 2014

ICS/SCADA Bileşenleri ve Temel Kavramlar

- Endüstriyel IT Sistemleri donanıma bağlı standart yazılım ve protokoller bütününden oluşmaktadır.
- SCADA
- ICS
- OPC
- DCS
- PLC
- RTU
- Modbus
- …

ICS

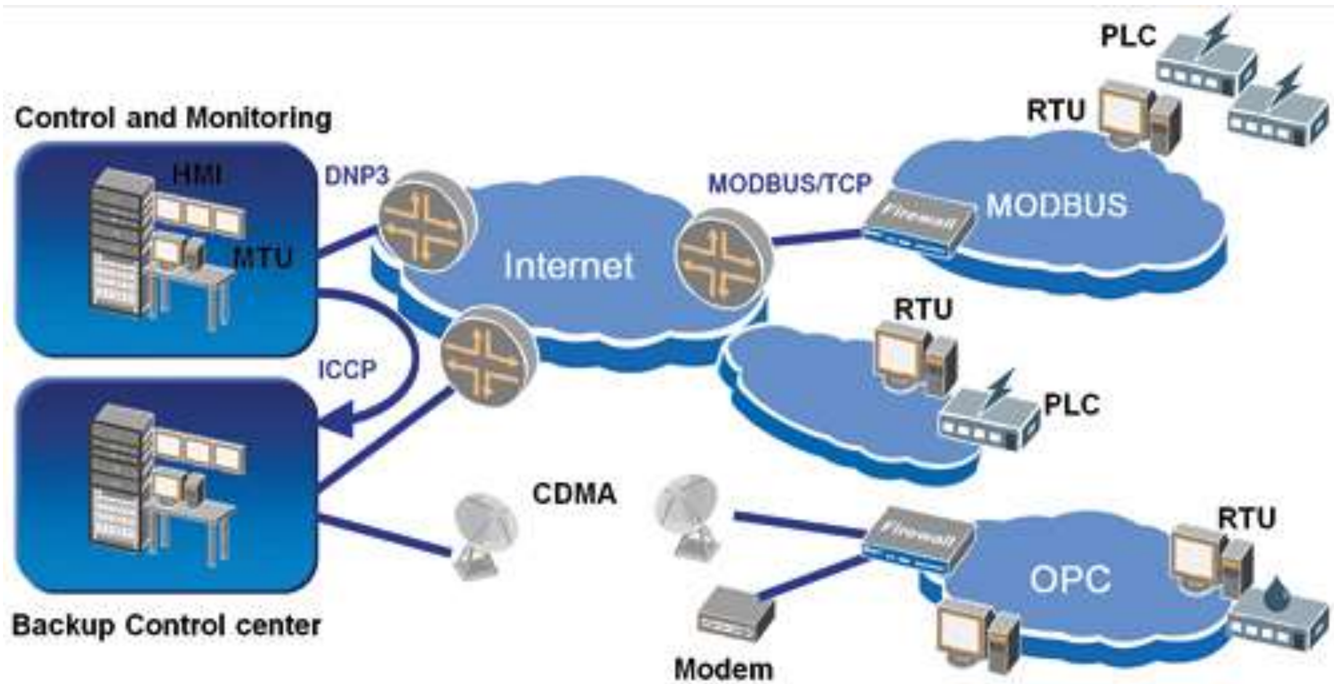
- ICS - Industrial Control Systems
- Genellikle SCADA ile karıştırılır

SCADA Nedir?

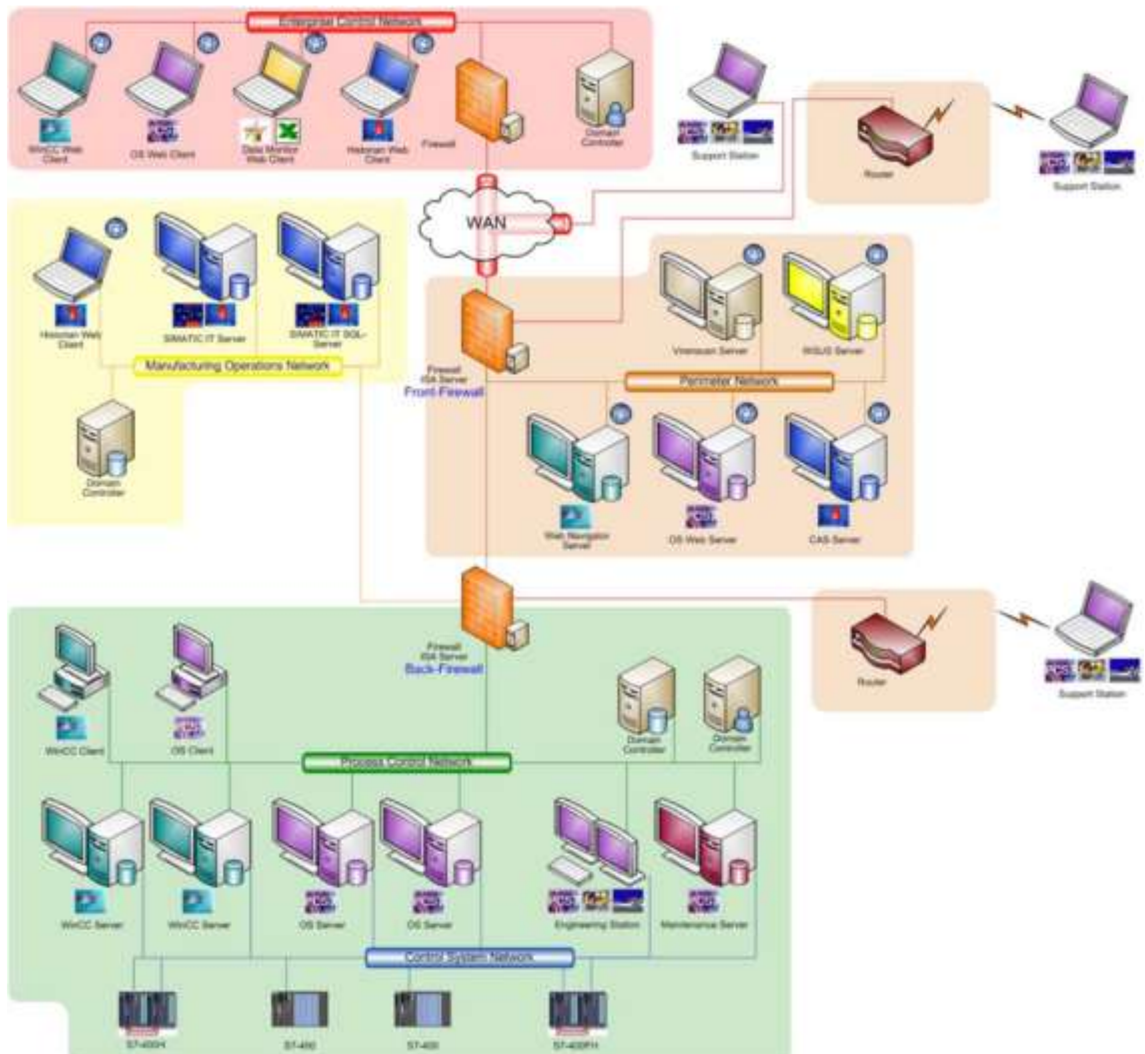
- Supervisory Control and Data Acquisition (SCADA)
- Enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini de sağlayan yapıdır.
- Prosesler için gözetleyici denetim ve veri toplama anlamına gelen SCADA uygulaması ilk olarak 1960'lı yıllarda Kuzey Amerika'da hayata geçirilmiştir.
- ICS Bileşenidir

SCADA Altyapı Bileşenleri?

- Yazılım, donanım, iletişim protokolleri, “İNSAN”

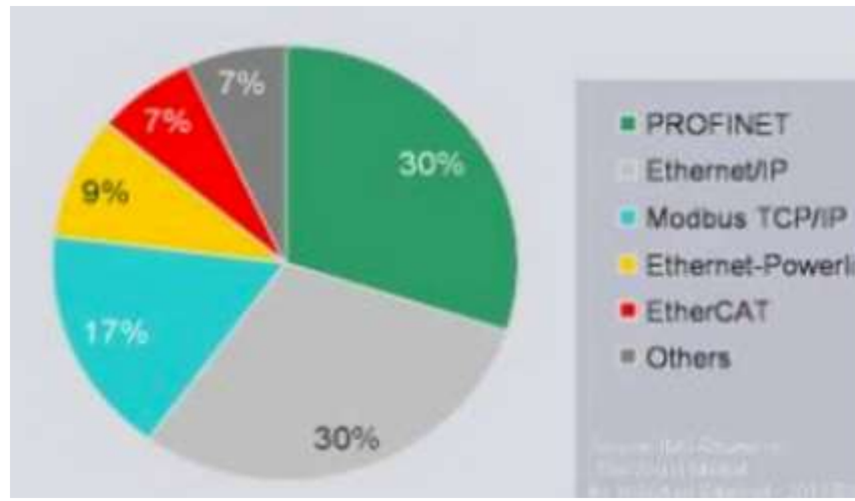


Örnek Bir SCADA Ağı



Sık Kullanılan Scada Protokolleri

- CIP, BACnet, CC-link, Ethernet/IP, Modbus, Profinet, S3, S5, S7, DNP3



Örnek SCADA Protokolü:>Modbus

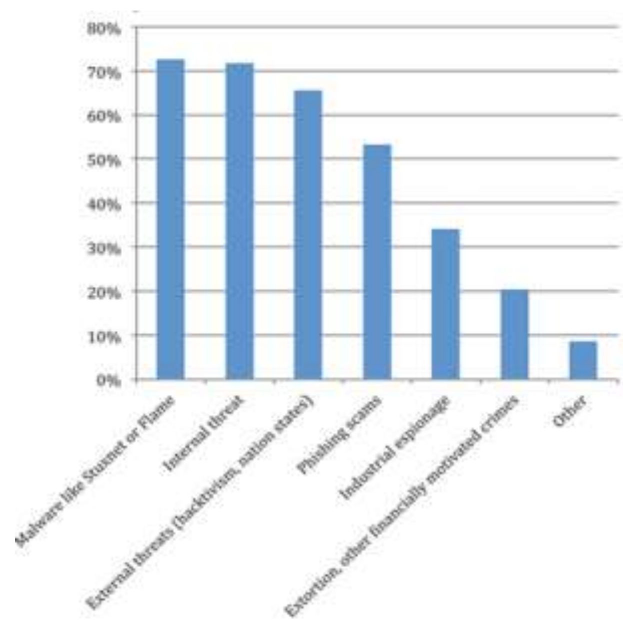
- 1979 yılında Schneider Elektrik tarafından Seri bağlantılar üzerinden kullanım için geliştirilmiş fakat günümüzde TCP üzerinden kullanılmaktadır.
  - TCP port 502
- Master/slave mantığı ile çalışır
- Genel modbus zafiyetleri
  - Clear-text bir protokoldür, MITM saldırılarından etkilenir
  - Kimlik doğrulama yoktur

ModBus IDS Kuralları

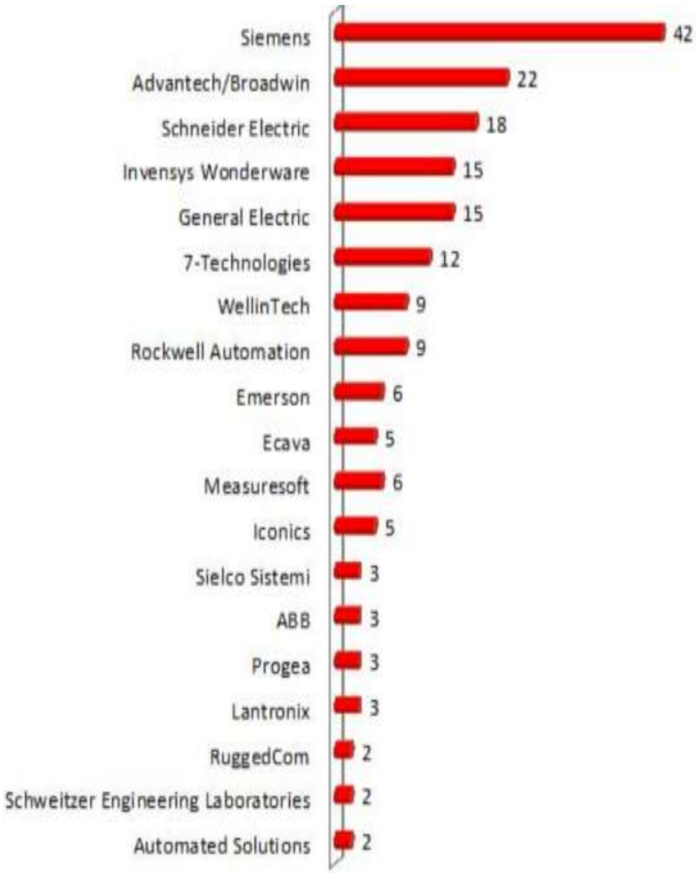
SID	Message
1111001	Modbus TCP – Force Listen Only Mode
1111002	Modbus TCP – Restart Communications Option
1111003	Modbus TCP – Clear Counters and Diagnostic Registers
1111004	Modbus TCP – Read Device Identification
1111005	Modbus TCP – Report Slave ID
1111006	Modbus TCP – Unauthorized Read Request to a PLC
1111007	Modbus TCP – Unauthorized Write Request to a PLC
1111008	Modbus TCP – Illegal Packet Size, Possible DOS Attack
1111009	Modbus TCP – Non-Modbus Communication on TCP Port 502
1111010	Modbus TCP – Slave Device Busy Exception Code Delay
1111011	Modbus TCP – Acknowledge Exception Code Delay
1111012	Modbus TCP – Incorrect Packet Length, Possible DOS Attack
1111013	Modbus TCP – Points List Scan
1111014	Modbus TCP – Function Code Scan

Genel SCADA Güvenliği

- Genel olarak bilişim sistemleri arasında en "güvensiz" olanları endüstriyel IT sistemleridir.
  - Temel sebepler
- Ülkelerin siber güvenlik stratejilerinde SCADA Güvenliğinin yeri
- SCADA sistemlerinde çıkan güvenlik zafiyetleri ve kullanım alanları



SCADA Sistemleri Neden Hedefte?



Silah Sistemi	Maliyet (USD)	Kimler Geliştirebilir?
Görünmez Savaş Uçağı	397 Milyar (F-35)	ABD, Çin, Rusya
Nükleer Denizaltı	11 Milyar	ABD, Rusya, İngiltere, Fransa, Çin, Hindistan
Askeri Hedefler için Siber Silah Programı	1 Milyar	Gelişmiş Ülkeler
Sivil Hedefler için Siber Silah Programı	100 Milyon	Gelişmiş ve gelişmekte olan tüm ülkeler
Kritik Bir Altyapıya Yönelik Siber Saldırı	5 Milyon	Herkes (devlet, teröristler, organize suç örgütleri vb.)
Ulusal Siber Güvenlik Programı (sivil)	> 1 Milyar	Politika, Strateji, İcra (5-10 sene)

Yaşanmış Güvenlik İhlal Olayları #video1

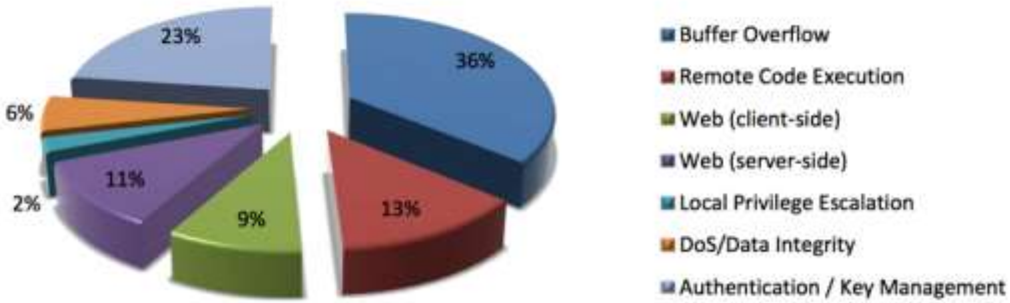
www.risidata.com/Database

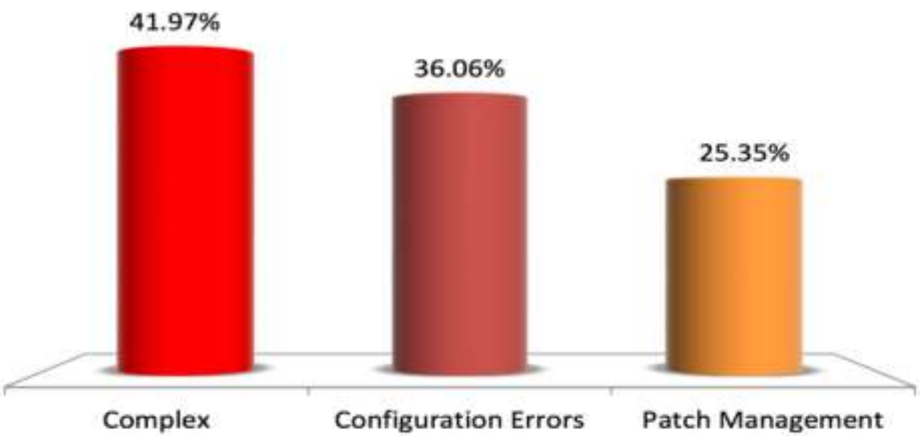
RISI — The Database | About | Contact

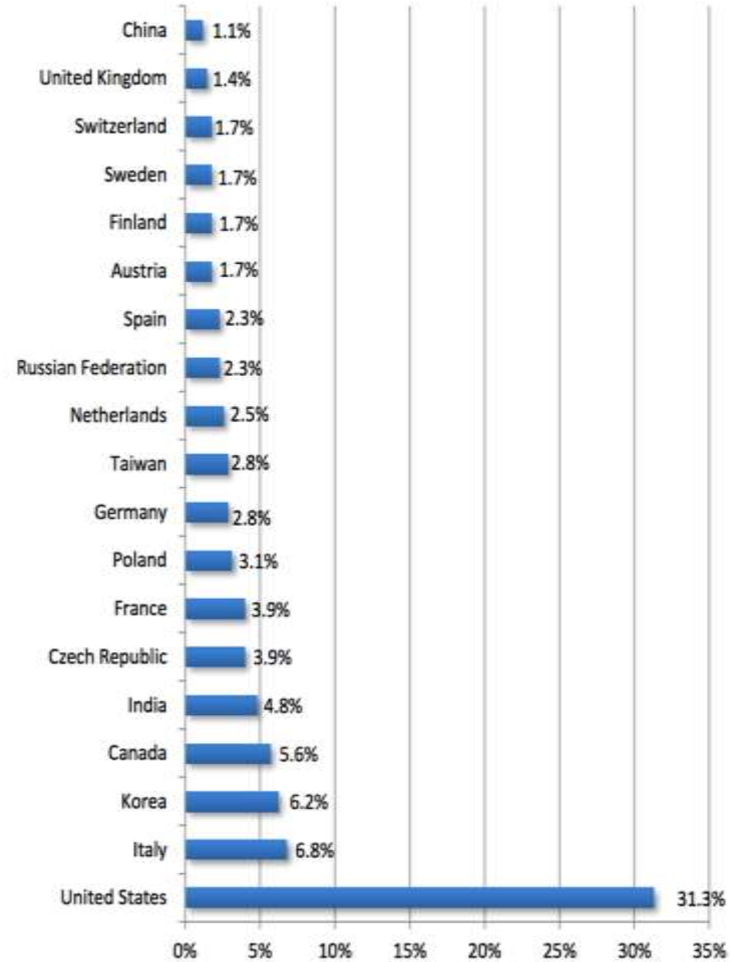
Last Updated: Wed, January 28, 2015

Title	Year	Industry Type	Country	Brief
Page 1 of 9 pages 1 2 3 > Last ›				
Baku-Tbilisi-Ceyhan Pipeline explosion	2008	Petroleum	Turkey	
Iranian Oil Terminal offline after malware attack	2012	Petroleum	Iran	
German Steel Mill Cyber Attack	2014	Metals	Germany	
Russian-Based Dragonfly Group Attacks Energy Industry	2014	Power and Utilities	United States	
U-2 spy plane caused widespread shutdown of U.S. flights: report	2014	Transportation	United States	
After 'Godzilla Attack!' U.S. warns about traffic-sign hackers	2014	Transportation	United States	
Public utility compromised after brute-force hack attack, says Homeland Security	2014	Power and Utilities	United States	
Broadcast Storm Shuts Down DCS Consoles	1997	Pulp and Paper	Canada	
PLC Password Change	1988	Pulp and Paper	Canada	
Duplicate IP Address Prevents Machine Startup	1996	Pulp and Paper	Canada	
Whitehat Takeover of DCS Consoles	2002	Petroleum	Canada	
Hackers Target Cal - ISO System	2001	Power and Utilities	United States	
Electronic Sabatoge of Venezuela Oil Operations	2002	Petroleum	Venezuela	
Nimda Impact on Manufacturing System	2001	Food & Beverage	United States	
CIA Trojan Causes Siberian Gas Pipeline Explosion	1982	Petroleum	Russian Federation	
Hacker Takes Over Russian Gas System	1999	Petroleum	Russian Federation	
Iranian Hackers Attempt to Disrupt Israel Power System	2003	Power and Utilities	Israel	

SCADA Güvenlik Araştırması Sonuçları







Dünya’da Gelişmeler ve Son Durum

s://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-c

The White House

Office of the Press Secretary

E-Mail Tweet Share +

For Immediate Release February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

For Immediate Release November 30, 2011

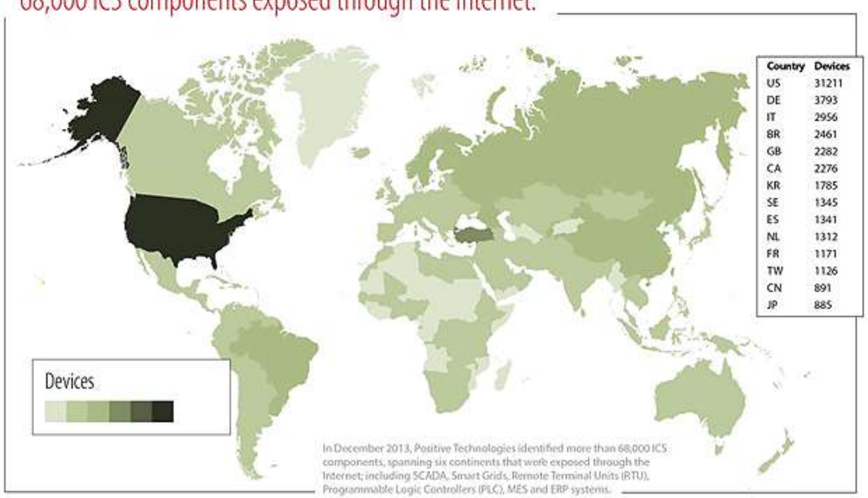
Presidential Proclamation -- Critical Infrastructure Protection Month, 2011

BY THE PRESIDENT OF THE UNITED STATES OF AMERICA

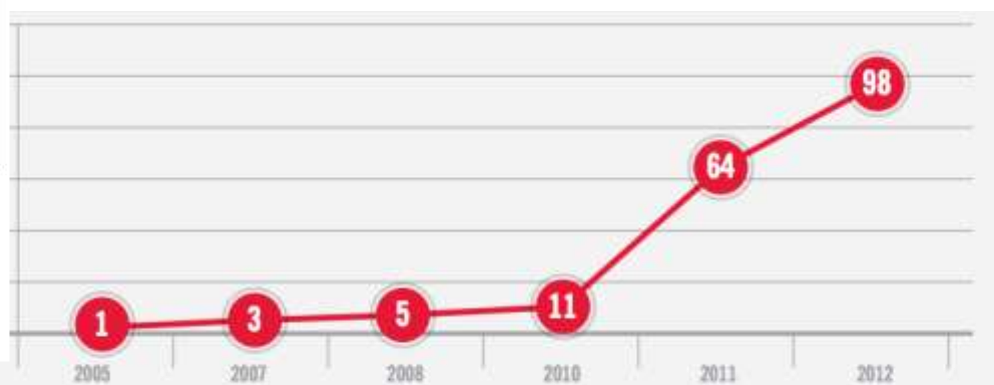
A PROCLAMATION

NSA direktörü: Çin, ABD’nin enerji altyapısına hasar verecek güçte

68,000 ICS components exposed through the Internet.



In December 2013, Positive Technologies identified more than 68,000 ICS components, spanning six continents that were exposed through the Internet, including SCADA, Smart Grids, Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), MES and ERP systems.



Türkiye’de Gelişmeler ve Son Durum

- Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında Kritik Altyapılar
- Kurumsal Seviyede Farkındalık Aşamasında…

“… insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve *aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları”*

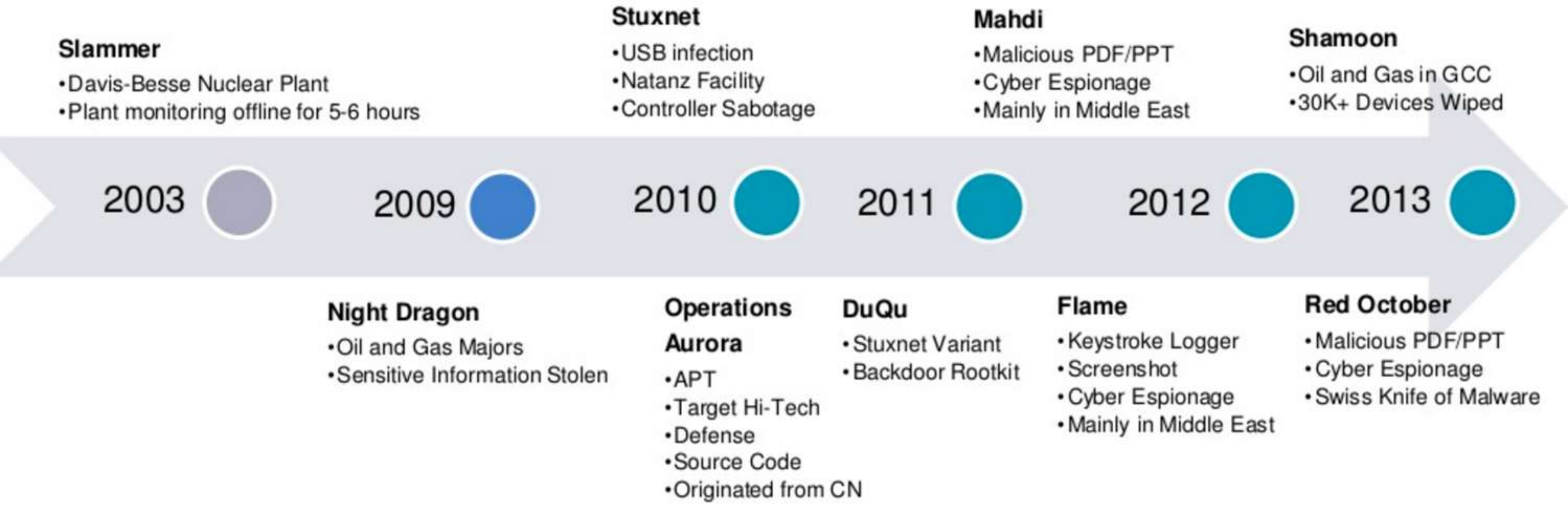
Enerji Bakanı Yıldız'dan elektrik kesintisi yorumu: Siber saldırı mıdır, söyleyemem

Paylaş Paylaş

Enerji Bakanı Taner Yıldız, Türkiye genelinde yaşanan elektrik kesintisiyle ilgili kriz merkezi kurulduğunu söyledi

SCADA Sistemler Nasıl Hacklenir?

SCADA Sistemlerinin Etkileyen Malware'ler

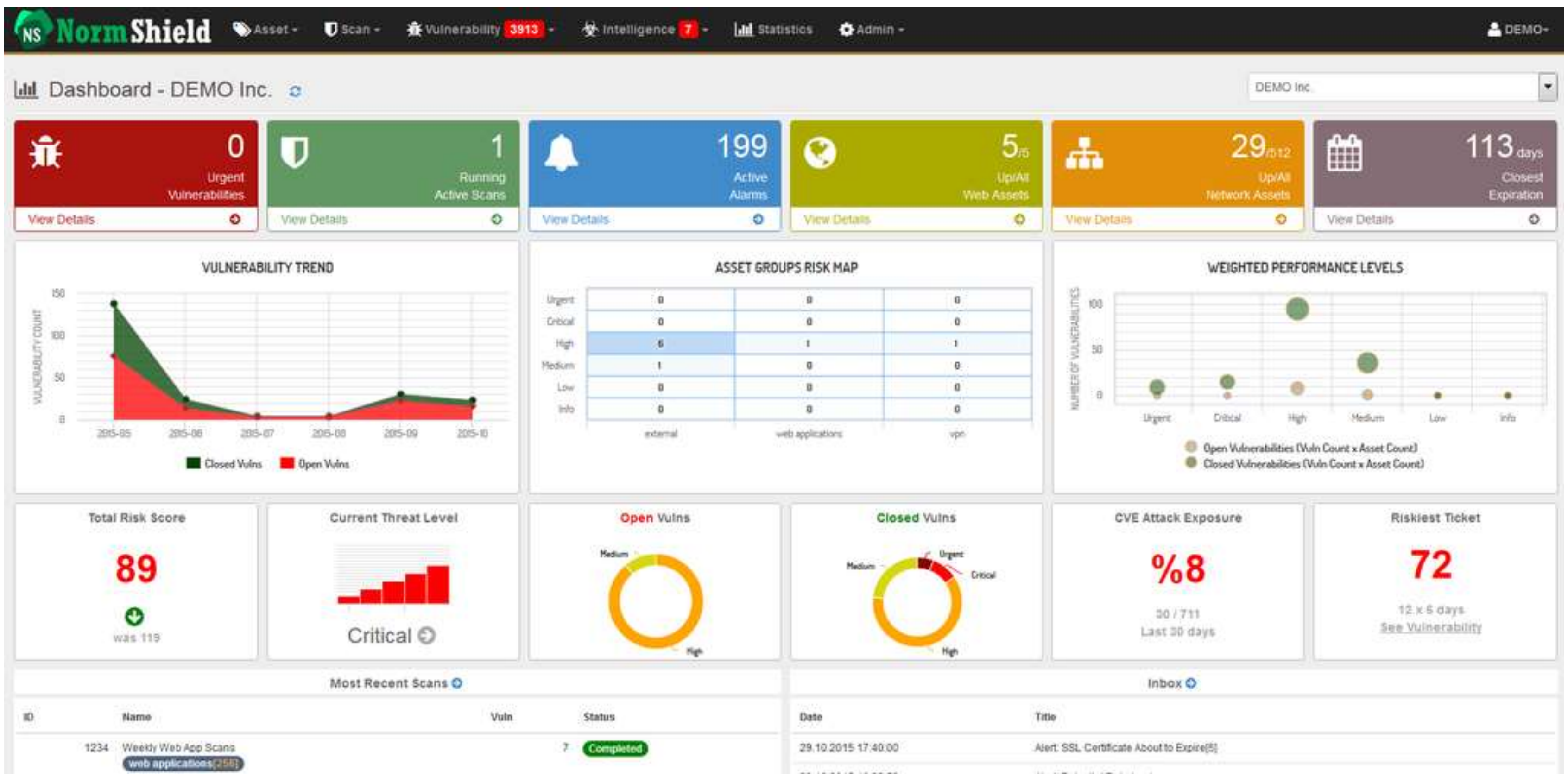


Örnek “SCADA Güvenlik Denetimi” Sonuçları

- SCADA sistemlerine internet üzerinden korumasız VPN erişimleri
- Ağlar arası yetkisiz erişim problemi
- Güncel olmayan yazılım kullanımı
  - Yama yönetimi
- Kimlik Doğrulama
- Yetkilendirme
- Parola güvenliği
- Fiziksel Güvenlik
- İnsan…

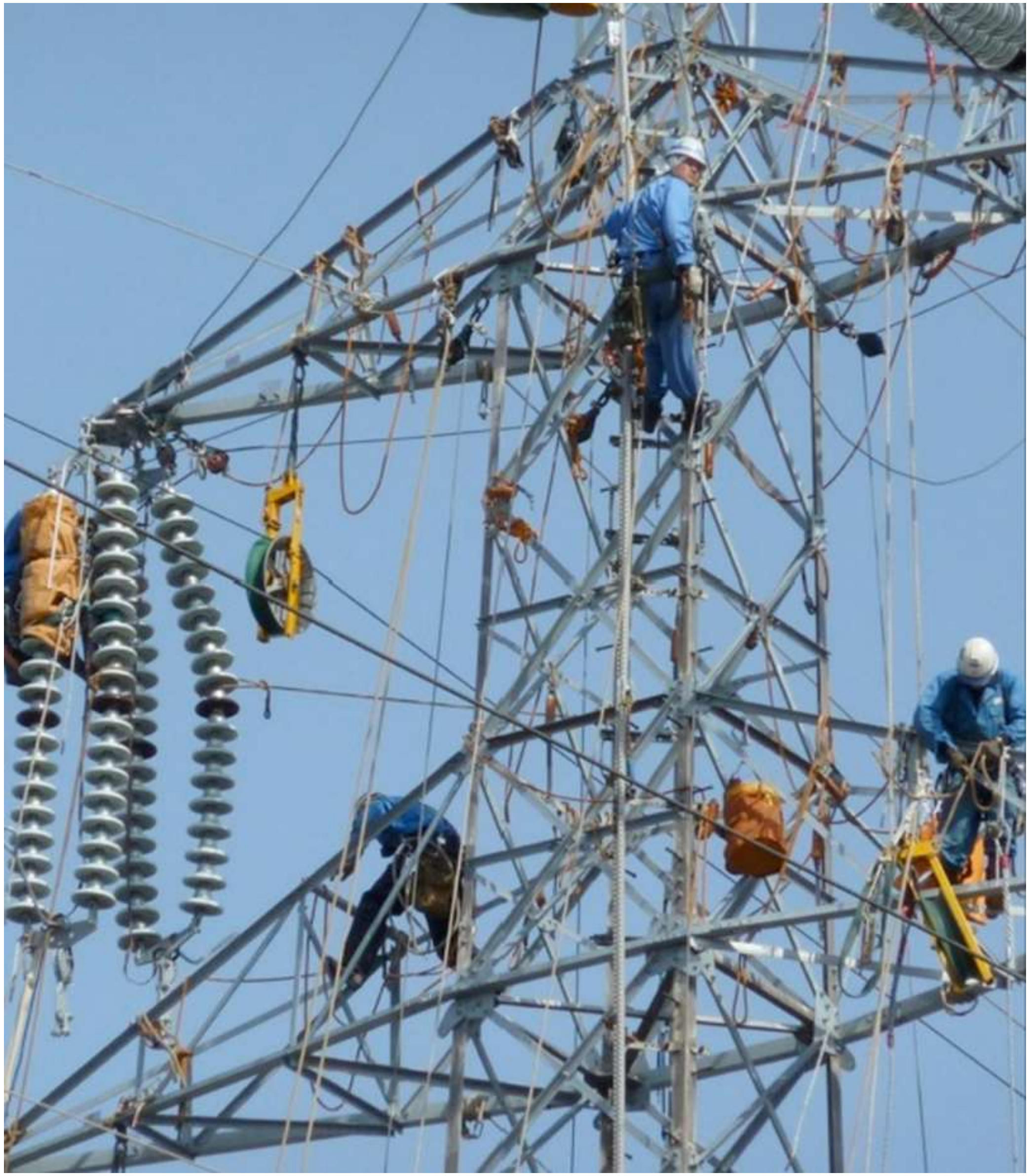
SCADA Ortamlarında Zafiyet Yönetimi

- Güvenlik bir sonuç değil süreçtir.
  - Günlük yayınlanan güvenlik zafiyeti sayısı 50 Adet
- Aktif Denetim yerine pasif denetim



SCADA Penetration Test

"İlk Kural"



İkinci Kural

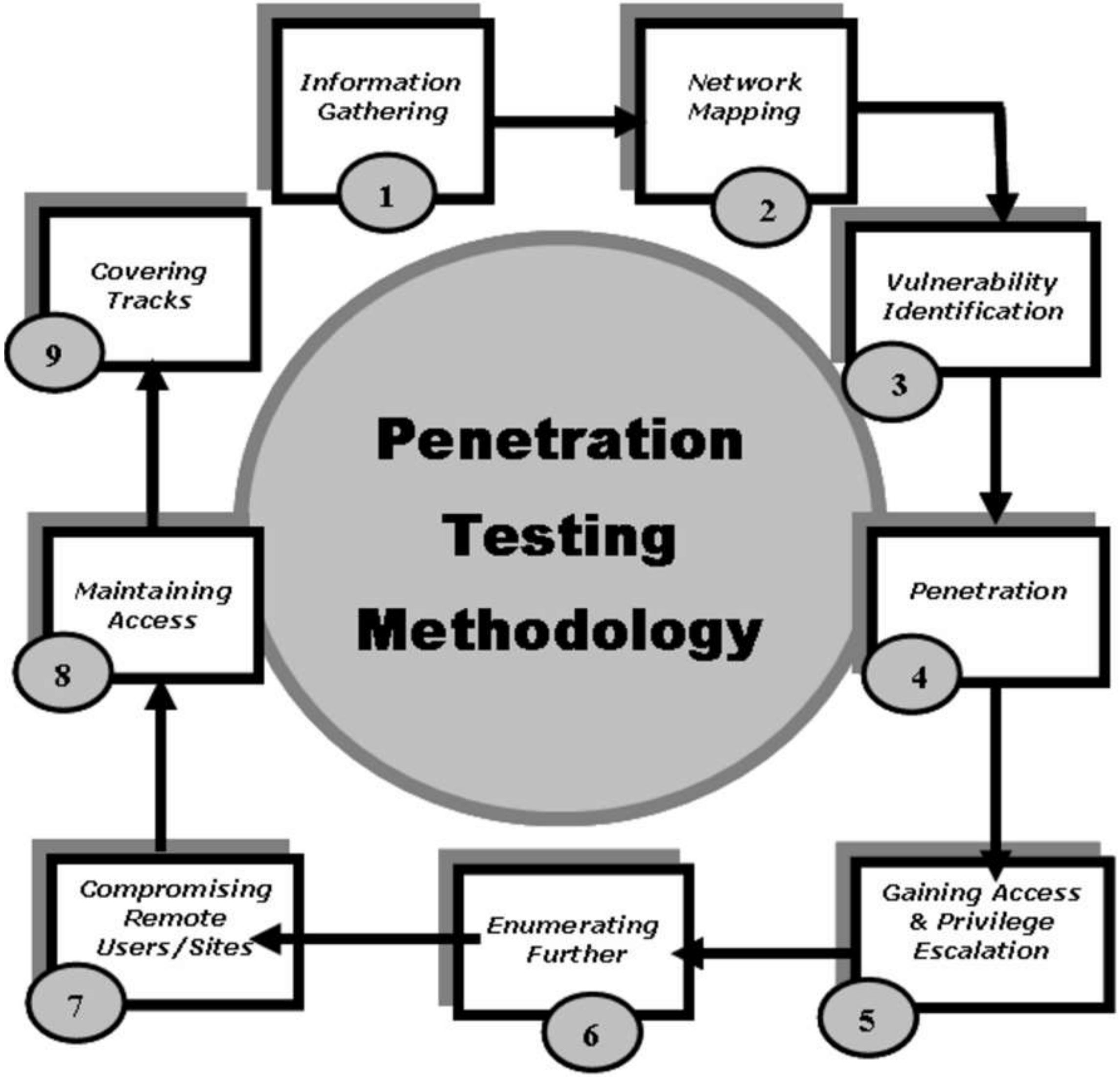
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

Unintentional Internal Security Consequences

- **Vulnerability Scanner Incidents[13].** While a ping sweep was being performed on an active SCADA network that controlled 3 meter (9 foot) robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers. See Section 4.2.6 for additional guidance on ICS vulnerability assessments.

- **Penetration Testing Incident[14].** A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

SCADA Pentest Metodolojisi



Ağ Keşif Ve Envanter Tespiti

- Dikkat edilmesi gereken en önemli konu taramalar yapılırken çok hassas olunmalı
  - Nmap ile tarama yaparken –scan-delay=1
  - SYN tarama seçenği yerine TCP Scan kullanılmalı
  - UDP tarama denenmemeli

```
nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host>
```

Script Output

```
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   Positive response for sid = 0x64
|     SLAVE ID DATA: \xFA\xFFPM710PowerMeter
|     DEVICE IDENTIFICATION: Schneider Electric PM710 v03.110
|_  Positive error response for sid = 0x96 (GATEWAY TARGET DEVICE FAILED TO RESPONSE)
```

Internet Üzerinden Bilgi Toplama

- Shodan Araştırma Sonuçları
- Belirli SCADA Protokolleri ve yazılımlarının Shodan benzeri arama motorları kullanarak araştırılması

Project SHINE / SCADA Araştırma Sonuçları

- SHODAN (Sentient Hyper-Optimized Data Access Network)
  - Arama motoru
- Shine - “Shodan INtelligence Extraction”
- Çalışma kapsamında incelenen portlar

- File Transfer Protocol (FTP) – port 21
- Telnet (TELNET) – port 23
- Unsecured Web (HTTP) – port 80
- Secured Shell (SSH) – port 22
- Simple Network Mgmt Protocol – port 161
- Secured Web (HTTPS) – port 443

- Siemens SIMATIC / ICCP – port 102
- DNP3 – port 20000
- BACNet – port 47808
- MODBUS/TCP – port 502
- Ethernet/IP – port 44818

Siemens SIMATIC / ICCP (Port 102) – Top 5 Countries

[Sampling data collected as of 31-Jan-2014]

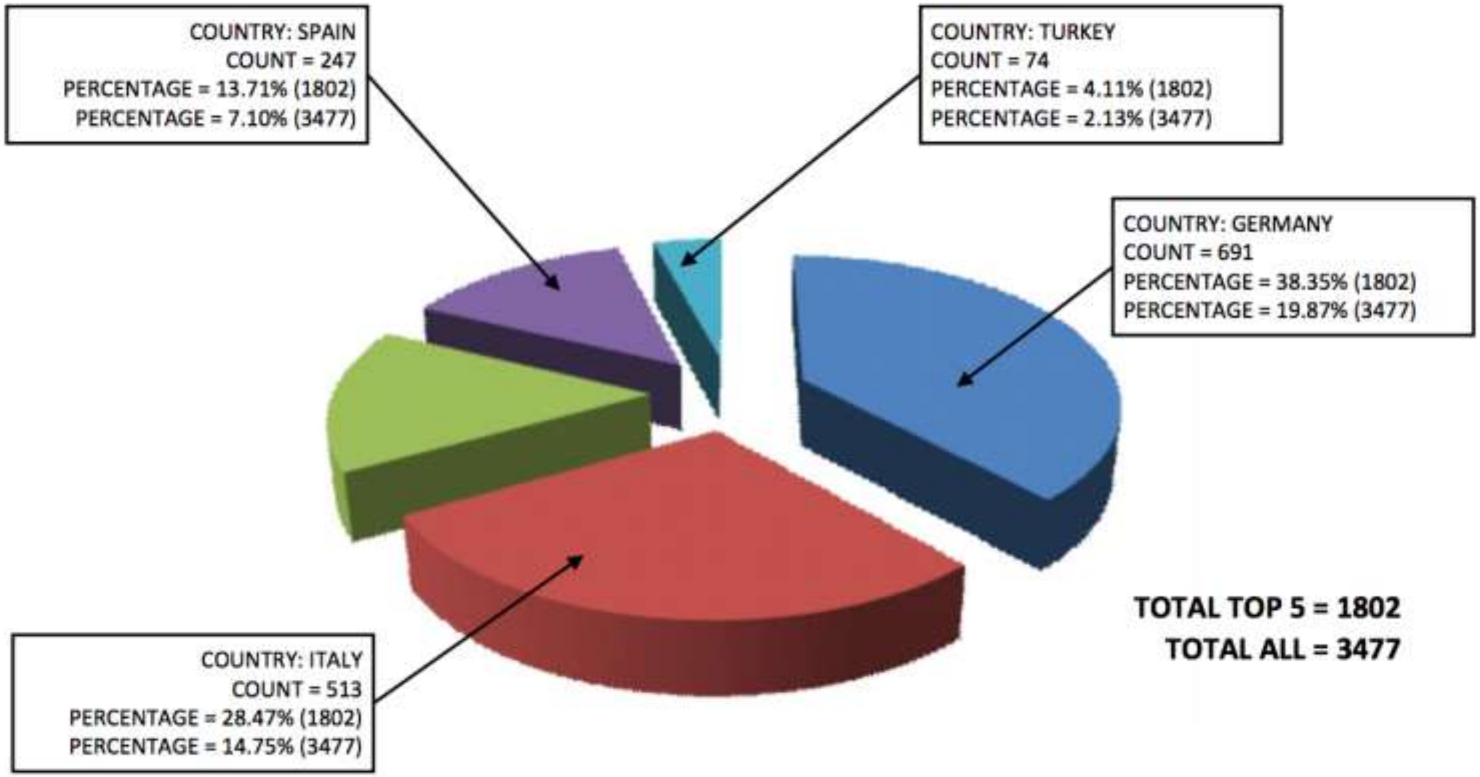


Figure 7.

Position	Country	Count	% Out of 1802	% Out of 3477
1	Germany	691	38.35%	19.87%
2	Italy	513	28.47%	14.75%
3	United States	277	15.37%	7.97%
4	Spain	247	13.71%	7.10%
5	Turkey	74	4.11%	2.13%
		1802 (total)		

Figure 8.

DNP3 (Port 20000) – Top 5 Countries

[Sampling data collected as of 31-Jan-2014]

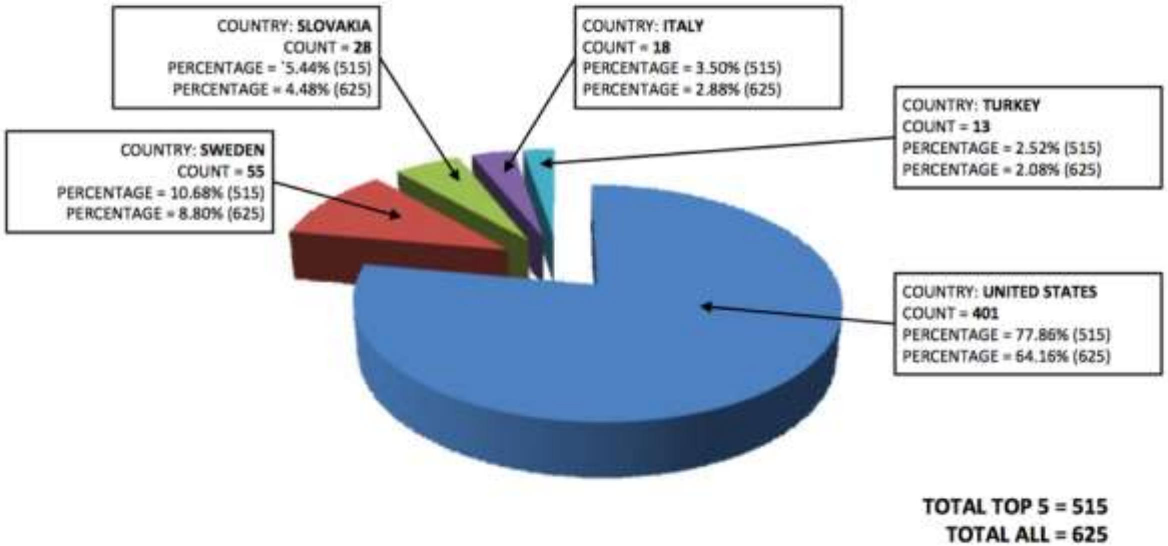
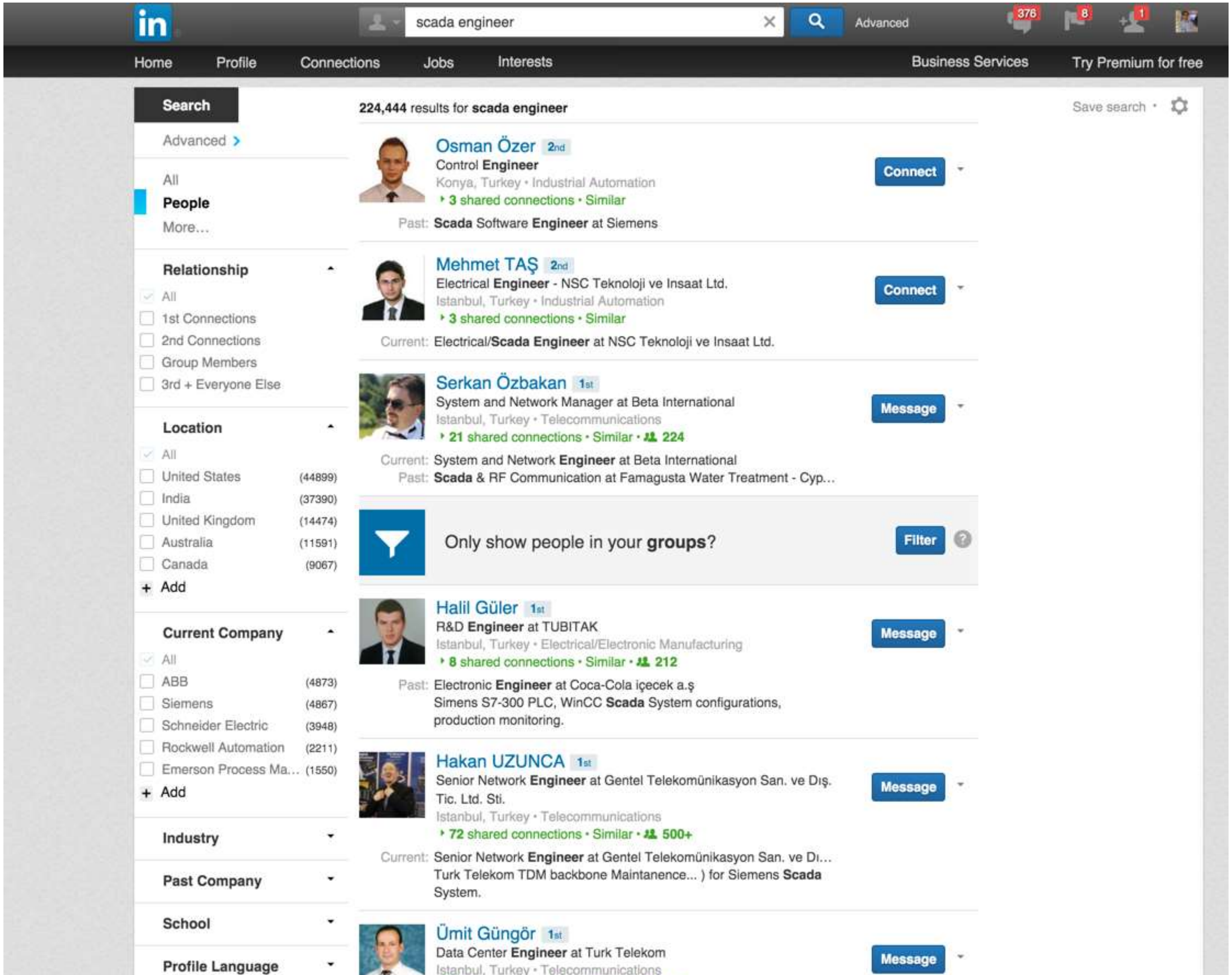


Figure 15.

Position	Country	Count	% Out of 515	% Out of 625
1	United States	401	77.86%	64.16%
2	Sweden	55	10.68%	8.80%
3	Slovakia	28	5.44%	4.48%
4	Italy	18	3.50%	2.88%
5	Turkey	13	2.52%	2.08%
		515 (total)		

Figure 16.

Sosyal Mühendislik / Oltalama / APT



Scada Güvenlik Denetimi

- Önerilen Standart Dökümanları

  - ISA-99 / IEC-62443
  - NERC-CIP
  - NIST 800-82
  - ISO27001:2013

Güvenlik Denetimi Kontrol Listesi

Matrix of International SCADA Security Controls-NERC-CFATS-ISAS99.xls

	A	B	C	D
1	**Standards, Policies, or Procedures that Map to the Controls >>**	**NERC CIP >> REQUIRED**	**CFATS (DHS) >> CHEMICALS STANDARD**	**ISA S99 >> INTERNATIONAL BEST PRACTICE**
2	**Six Layers of Controls**			
3	**1. PHYSICAL SECURITY**			
4	**Physically Secure Access to Control Devices** - Secure physical access to control system components that monitor or control chemical processing, chemical storage, or transportation.	CIP-006	RBPS 2 - Secure Site Access, RBPS 3 - Screen and Control Access, and RBPS 4 - Deter, Detect, and Delay	ISA-TR99.00.002, 6.7.1 Hardware Assets and Components (Physical)
5	**Physically Secure Access to Control Networks** - Control Networks and Field Networks should be physically secured. All critical cyber devices that are used for monitoring or control must be physically secured with 6-walls of protection (i.e. fencing, cages, walls, etc...)	CIP-006	RBPS 2 - Secure Site Access, RBPS 3 - Screen and Control Access, and RBPS 4 - Deter, Detect, and Delay	ISA-TR99.00.002, 6.6.8.3, "Physical and Environmental Security
6	**Role-based Physical Access Controls** - Prevent physical access to control system equipment - The facility should have role-based physical access controls to restrict access to critical cyber systems and information storage media.	CIP-006	Metric 8.3.5 – Physical Access to Cyber Systems and Information Storage Media	ISA-TR99.00.002, 6.6.8.3, "Physical and Environmental Security
7	**Visitor Controls** - The facility has documented and implemented visitor identification, escort, and access control procedures that include verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.	CIP-001	Metric 7.3 – Visitor Controls	ISA-TR99.00.002, 6.6.8.3, "Physical and Environmental Security
8	**Inspection and Testing of Physical Controls** - The facility has written procedures, including responsibilities, tasks, and frequencies, to regularly inspect, test, calibrate, repair and maintain security systems (e.g., gates, cameras, lights, alarms, keypad entry systems) and related equipment such as communications and emergency notification equipment.	CIP-006	Metric 10.1 – Inspection, Testing, and Preventative Maintenance (ITPM) Procedures	ISA-TR99.00.002, 6.6.8.3, "Physical and Environmental Security
9	**Temporary Physical Security During an Outage** - Appropriate temporary security measures are implemented in response to non-routine outages, equipment failures and malfunctions, and such incidents are documented and promptly reported to the Site Security Officer.	CIP-006	Metric 10.2 – Outages	
10	**Written Plan to Repair Physical Security Deficiences** - The facility has a written plan to record and repair deficiencies in security-related equipment.	CIP-006	Metric 10.3 – Repairs	
11	**Identification of Security Maintenance Personnel** - The facility has procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment	CIP-006	Metric 10.4 – Maintenance Personnel Surety	
12	**2. Networking Architecture (Firewalls, Routers, Switches, Hubs)**			
13	**Firewalls** - A manufacturing process control network must be segregated from the so-called DMZ by an inner firewall. The DMZ must also be segregated from the corporate IT network through an outer firewall.	CIP-005	Metric 8.3.3 – Access Control Lists	ISA-TR99.00.002, 6.6.8.2.3 Network Access Control
	Typical Network Traffic - All authorized non-local communications with the process control network shall be through one or both of the DMZ firewalls, depending on the impact of a breach from external access.	CIP-005	Metric 8.2.2 – External Connections	ISA-TR99.00.002, 6.6.8.2.3 Network Access Control,

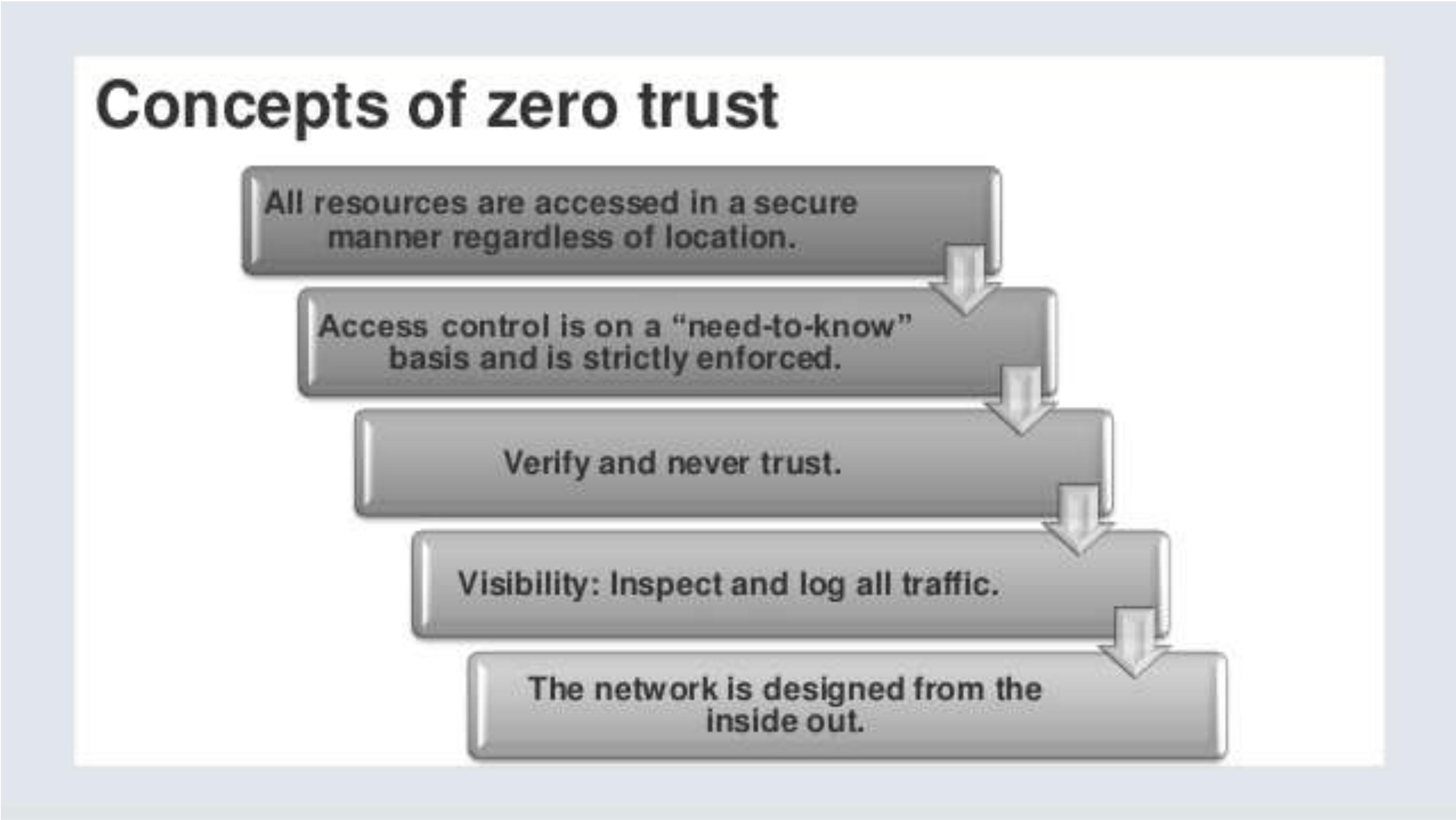
Güvenli SCADA Kurulum Adımları

- 1. Adım: Üst Yönetim Farkındalık ve Destek
  - Politika ve prosedürlerin tamamlanması (Hazırlık)
- 2. Adım:GAP Analizi ve Varolan Durum Tespiti
  - Güvenlik denetimi, risk assessment, önceliklendirme
- 3. Adım:Harekete Geçme, Uygulama
  - Önceliklendirme sırasına göre önlemleri alma, uygulama
- 4. Adım:Düzenli Güvenlik İzleme, Alarm Sistemi
  - Kurulan altyapıyı kullanarak oluşabilecek güvenlik ihlal ve anormalliklerinin tespiti

Önerilen Adımlar

- SCADA mühendisleri için farklındalık eğitimleri ve “testleri”
- Tüm SCADA sistemini düzenli olarak aylık güvenlik (pasif) taramadan geçirilmesi
- SCADA ağına yeni bir sistem takıldığında haberdar edecek sensörlerin kurulumu
- SCADA sistemlerine yönelik gerçekleştirilecek siber saldırıların simülasyonu
- 7/24 güvenlik izleme sisteminin kurulumu

Zero Trust Modeli



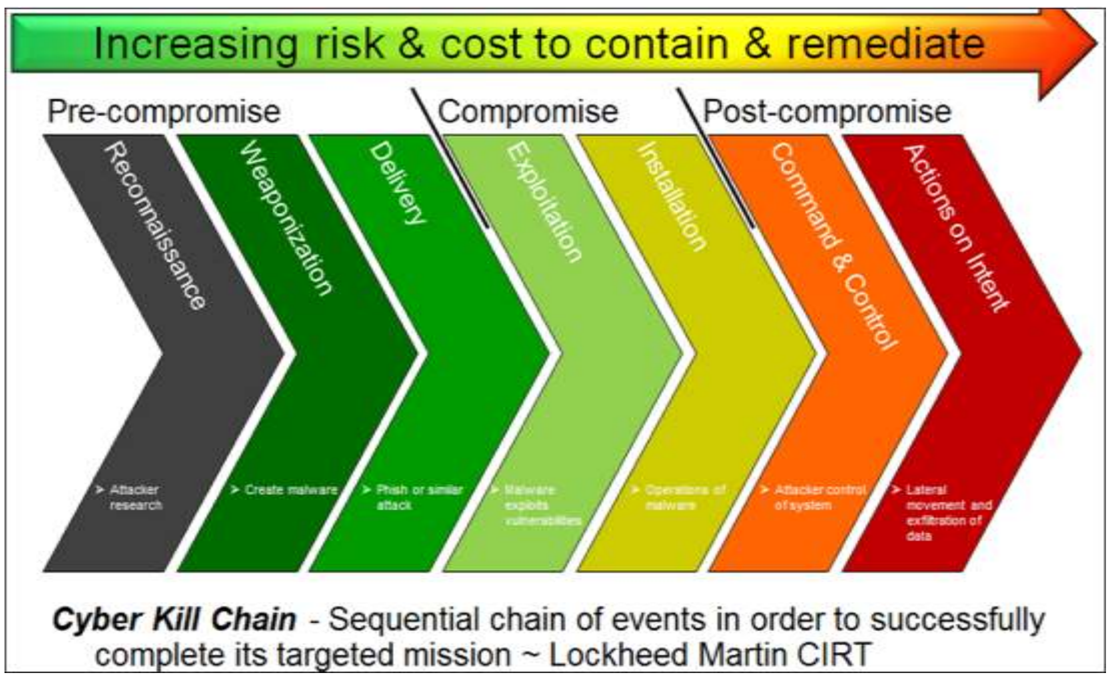
SCADA Güvenlik İzleme Projesi

- SCADA Güvenlik Olayları İzleme projesinde tüm dünyada en fazla kullanılan yazılım “Snort” tercih edilmiştir.

SCADA Siber Tehdit Simülasyonu

- Siber Güvenlik Tatbikat çalışması bir kurumun dış ve iç siber saldırgan gözüyle kurumdaki tüm güvenlik bileşenleri (çalışanlar dahil) gerçek hayattakine benzer bir saldırı simulasyonu ile ölçümüdür.

"Cyber Kill Chain"



Kaynak:theimf

7X24 Güvenlik İzleme - SOC

İletişim Bilgileri

Blog
- www.bga.com.tr
- Blog.bga.com.tr

Twitter
- @bgasecurity
- @huzeyfeonal

İletişim
- some@bga.com.tr