Güvenliği Artırmak için Tehdit İstihbaratı ve Zafiyet Yönetiminin Birleşimi

Huzeyfe ÖNAL

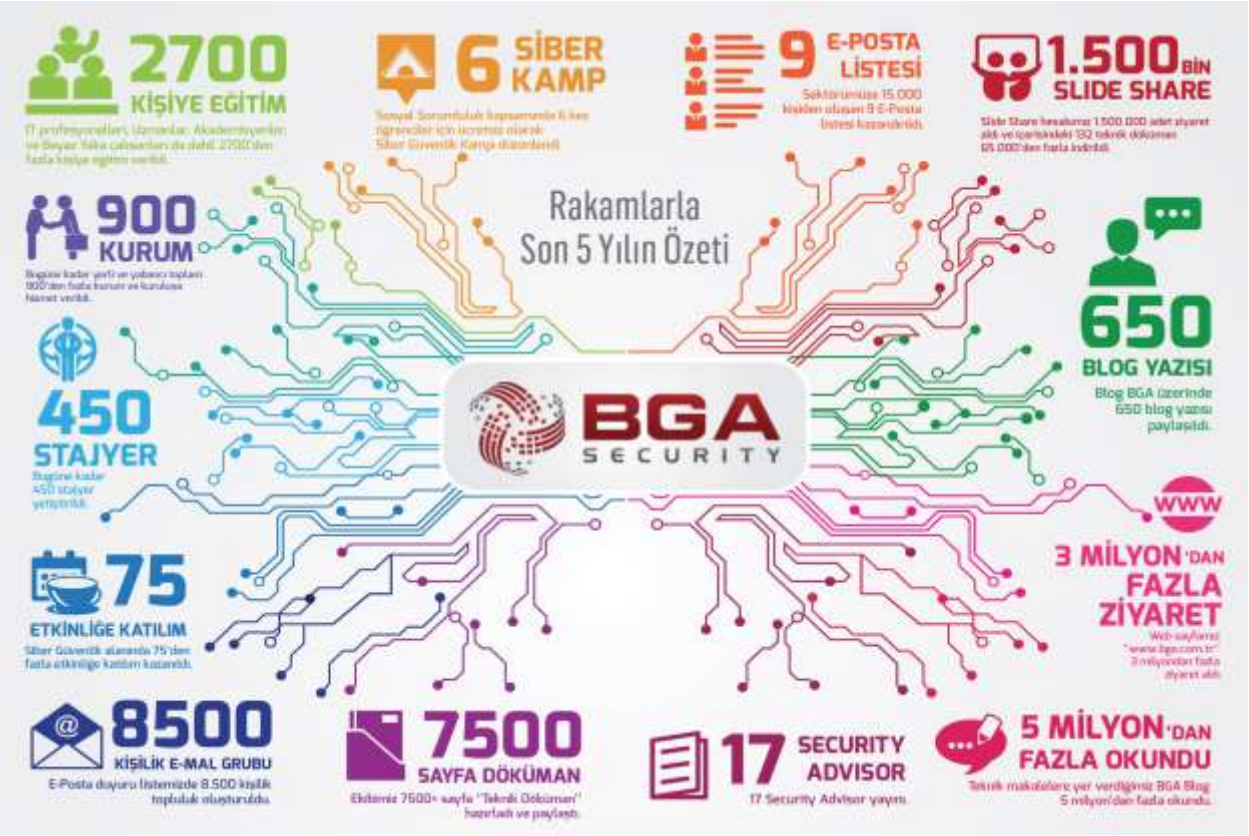
BGA Bilgi Güvenliği A.Ş.

Huzeyfe ÖNAL

- Yönetici Ortak – BGA Bilgi Güvenliği A.Ş.
- Sektör tecrübesi :2002-…
- Siber Güvenlik İnsiyatifi Kurul Üyesi (UDHB Bünyesinde)
- Öğretim Görevlisi (Siber Güvenlik Yüksek Lisans Programı)
  - Bilgi Üniversitesi (*Bilişim hukuku Yüksek Lisans Programı*)
  - Bahçeşehir Üniversitesi (*Siber Güvenlik Yüksek Lisans Programı*)
  - Şehir Üniversitesi (*Siber Güvenlik Yüksek Lisans Programı*)

Firma Hakkında: BGA Bilgi Güvenliği A.Ş.

- BGA markası ile 6 yıldır kurumlara stratejik siber güvenlik danışmanlığı sunmaktadır
- 45 teknik personel (Mühendis ağırlıklı)
- 2016 itibariyle Ankara, İstanbul, Bakü ve Virginia(USA) ofisleri
- Ağırlıklı çalışılan sektörler
  - Finans (32 Banka)
  - Enerji
  - Telekom
  - Savunma Sanayi
  - Kamu
- Bilgi Güvenliği AKADEMİSİ markası ile siber güvenlik konusunda üretim merkezi rolü



Sunum İçeriği:Ajanda

1. Güvenliğin Bağlı Olduğu Temel Esaslar
2. Efektif Zafiyet Yönetimi Esasları
3. Siber Tehdit İstihbaratı
4. Düzenli Güvenlik İzleme

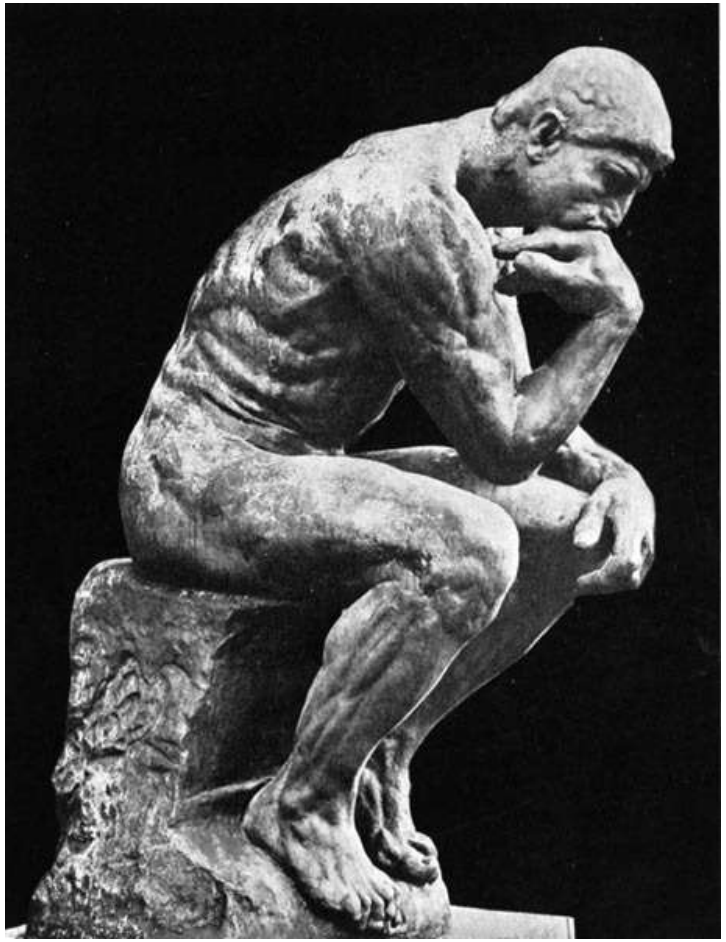
Başlangıç: Amaç

Nasıl “daha” güvende/güvenli oluruz sorusuna “samimi” ve “somut” birşeyler katma.

Maslow'un İhtiyaçlar Hiyerarşisi

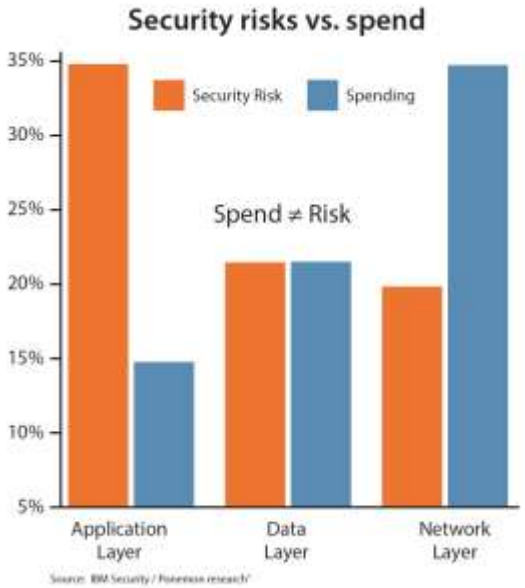
Maslow teorisi, insanların belirli kategorilerdeki ihtiyaçlarını karşılamalarıyla, kendi içlerinde bir hiyerarşi oluşturan daha 'üst ihtiyaçlar'ı tatmin etme arayışına girdiklerini ve bireyin kişilik gelişiminin, o an için baskın olan ihtiyaç kategorisinin niteliği tarafından belirlendiğini söz konusu etmektedir.

Siber Güvenliği Nasıl Sağlarız?



- Güvenliğin en temel bileşeni doğru sorularla işe başlamaktır.
  - Neyin güvenliğini sağlayacağız?
  - Güvenlikten anladığımız nedir?
  - Ne kadar güvenlik istiyoruz?

… düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz. ….. Ne kendinizi ne de düşmanı biliyorsanız, sizin için gireceğiniz her savaşta yenilgi kaçınılmazdır.
Sun Tzu, Art of War

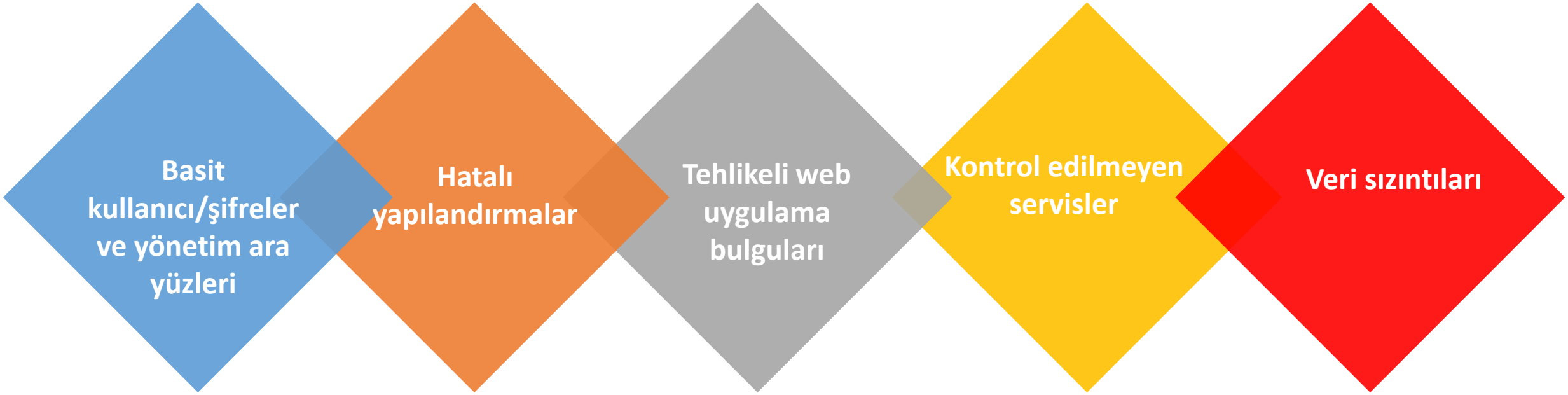


Değerli Olabilecek Varlık Listemiz #Asset

- IP Adresi, IP Blokları
- DNS sunucular
- Mail adresleri
- Alan Adı, web sitesi ve alt alan adları
- Blog & Portal
- Mobil Uygulamalar
- Kurum çalışanları(Yöneticiler)
- Belirlenecek marka anahtar kelimeler
- 3. parti çalışılan firmalar
- Kurum tarafından kullanılan yazılım/donanımlar
- Social Medya Hesapları(Twitter, FB, Instagram, LinkedIN..)

Neyi, neleri korumaya çalışıyoruz?

Basit Hatalar Can Yakmaya Devam Ediyor



Zafiyet Yönetimi İhtiyacı

/2012/01/17/devops-needs-to-become-devopssec/

development, operations and security are the root cause of the vast majority of critical system downtime, including downtime caused by breaches in security. For example, Gartner research shows that 75% of successful attacks occur against previously known vulnerabilities for which a patch or secure configuration standard was already available (actually, this used to be about 90%, but advanced and targeted attacks have changed the equation).

Orta ve büyük firmaların sistemlerinde her hafta ~250 güvenlik zafiyeti yayınlanmaktadır.

Ortalama her yıl 15.000 tekil güvenlik zafiyeti yayınlanmaktadır.

Yıl	Açıklık Sayısı	Ortalama		
		Aylık	Günlük	Saatlik
2015	15.000	1.250	41	2
2014	12.000	1.000	32	1

Büyük çoğunluğu kritik öneme sahip sistemlerdir.

Devlet kurumları ve finans sektörü başı çekmektedir.

Başarılı sonuçlanan atakların %75'i daha önce tespit edilmiş ve yaması bulunan zafiyetleri kullanmaktadır.

15,435 vulnerabilities across 3,870 applications were recorded in 2014

Posted on 25 March 2015.

In 2014, 15,435 vulnerabilities were discovered according to data from Secunia Research. The vulnerabilities are spread across 3,870 applications published by 500 different vendors, and these numbers alone demonstrate the challenge faced by IT teams trying to protect their environment against security breaches.

Türkiye'de OpenSSL ve IIS açıklığı barındıran sunucu sayısı 150.000

Zafiyet Yönetimi Nedir? Ne Değildir?

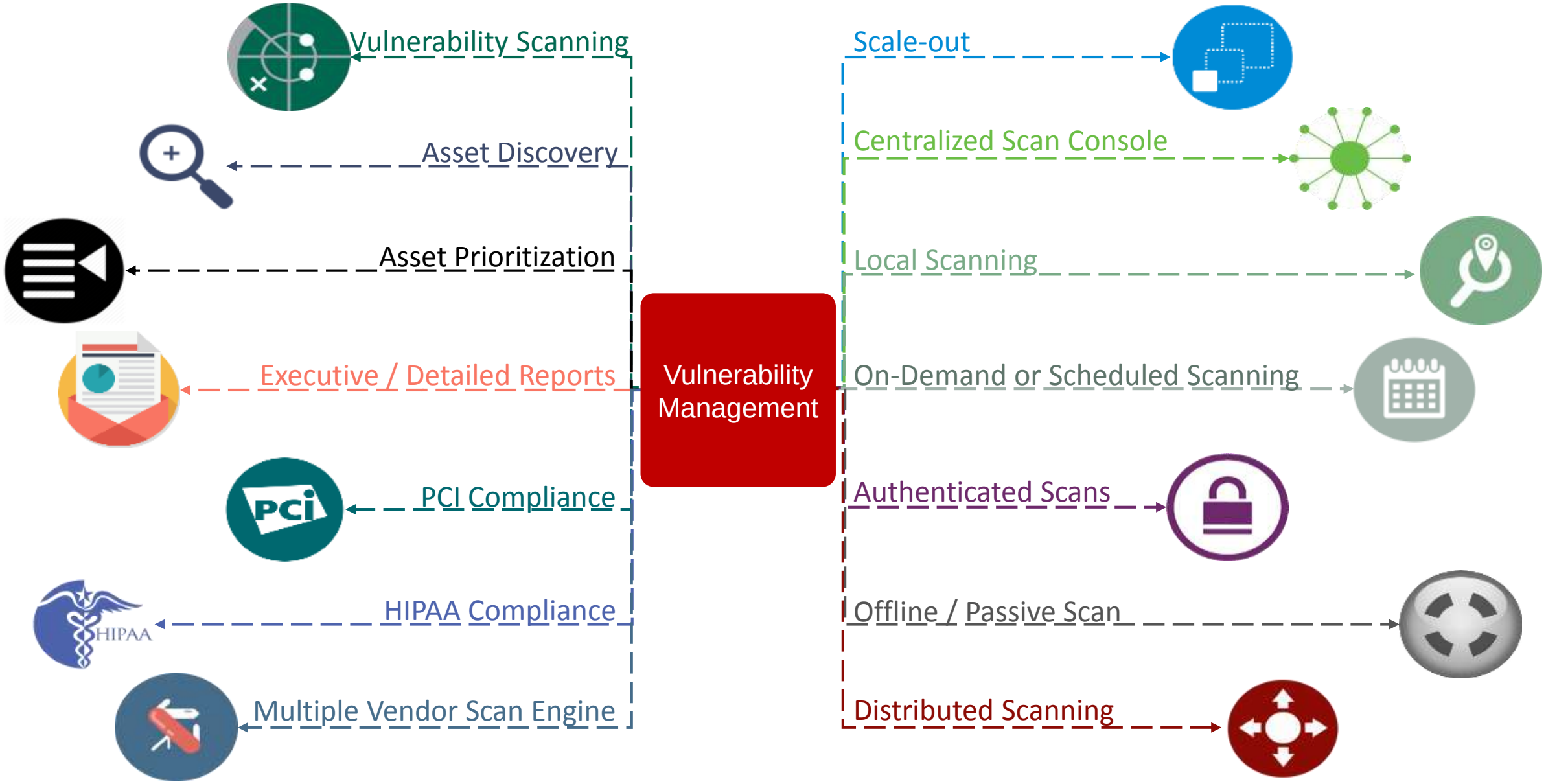
- Sahip olduğumuz varlıkları etkileyecek açıklıkların düzenli olarak takibi, uygulanması ve kontrolü işlemi.
- Zafiyet tarama, önceliklendirme, atama, takip aşamalarından oluşur
- Zafiyet tarama sıklığı önemlidir
  - Haftalık, Aylık? Yıllık?

- Zafiyet yönetimi tek bir araç, yazılım kullanarak sistemleri taramak değildir.
- Açıkları belirlemek ve atayıp beklemek değildir.
- Her bir açıklık tarama yazılımını kendi başına kullanmak değildir
- Sızma testi değildir

Veri sızıntısı ya da güvenlik problemi yaşayan firmaların %100'ü düzenli sızma testi hizmeti almaktadır.

Forrester Research

Merkezi Zafiyet Yönetimi #UVM Kavramı



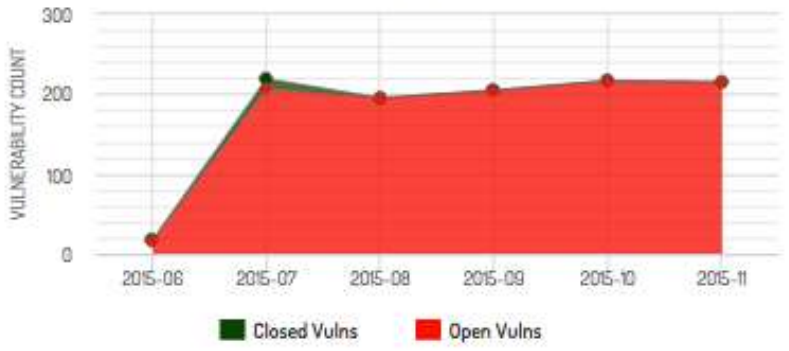
https://cloud.normshield.com

NormShield | Asset | Scan | Vulnerability 2740 | Intelligence 7 | Report | Admin | CANDAN

Dashboard - BGA BANK

20 Urgent Vulnerabilities	13 Running Active Scans	974 Active Alarms	36/37 Up/All Web Assets	0/1051 Up/All Network Assets	-26 days Closest Expiration
View Details	View Details	View Details	View Details	View Details	View Details

VULNERABILITY TREND

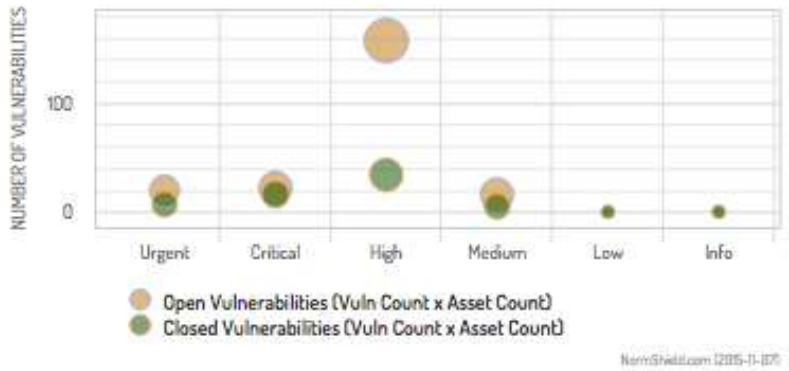


ASSET GROUPS RISK MAP

	bgabank_web	normshield	bgabank	bgabank_isube	bga_deneme	bgabank_internal	bgatest	anasayfa_web	omer_network_ip
Urgent	0	1	0	12	12	7	1	0	0
Critical	0	1	0	0	0	20	1	1	0
High	6	2	4	104	104	36	2	0	8
Medium	2	0	2	0	0	10	0	0	4
Low	0	0	0	0	0	0	0	0	0
Info	0	0	0	0	0	0	0	0	0

NormShield.com (2015-11-07)

WEIGHTED PERFORMANCE LEVELS



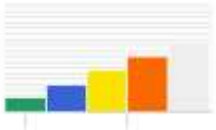
NormShield.com (2015-11-07)

Total Risk Score

2374

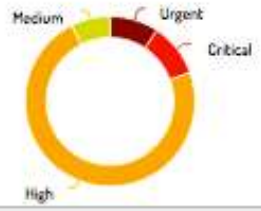
was 2374

Current Threat Level



Severe

Open Vulns



Closed Vulns

CVE Attack Exposure

%1

11 / 661
Last 30 days

Riskiest Ticket

1575

9 x 175 days
See Vulnerability

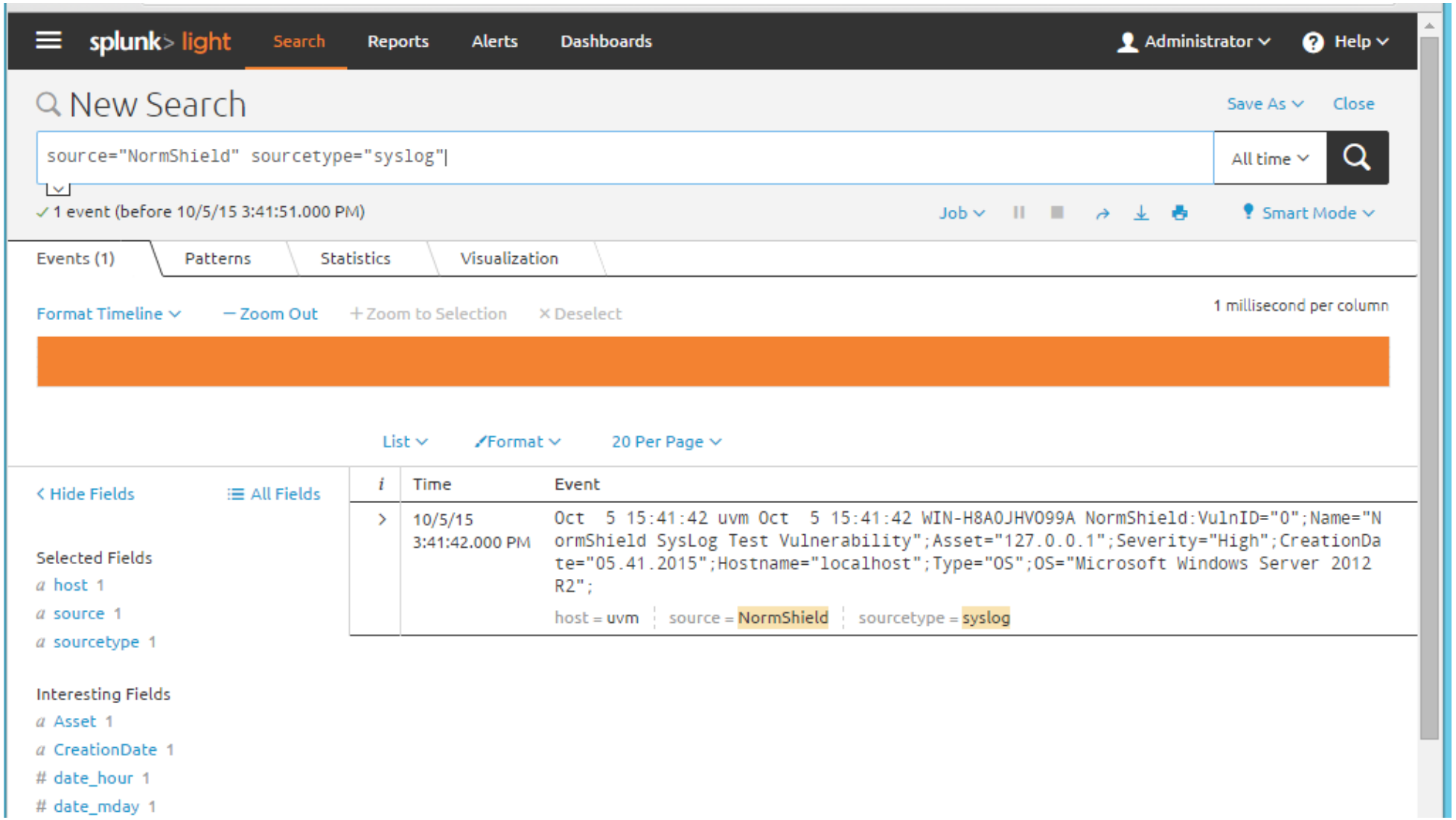
Most Recent Scans

ID	Name	Vuln	Status
5941	Nessus Test https://qube.bankbank.com	0	Completed

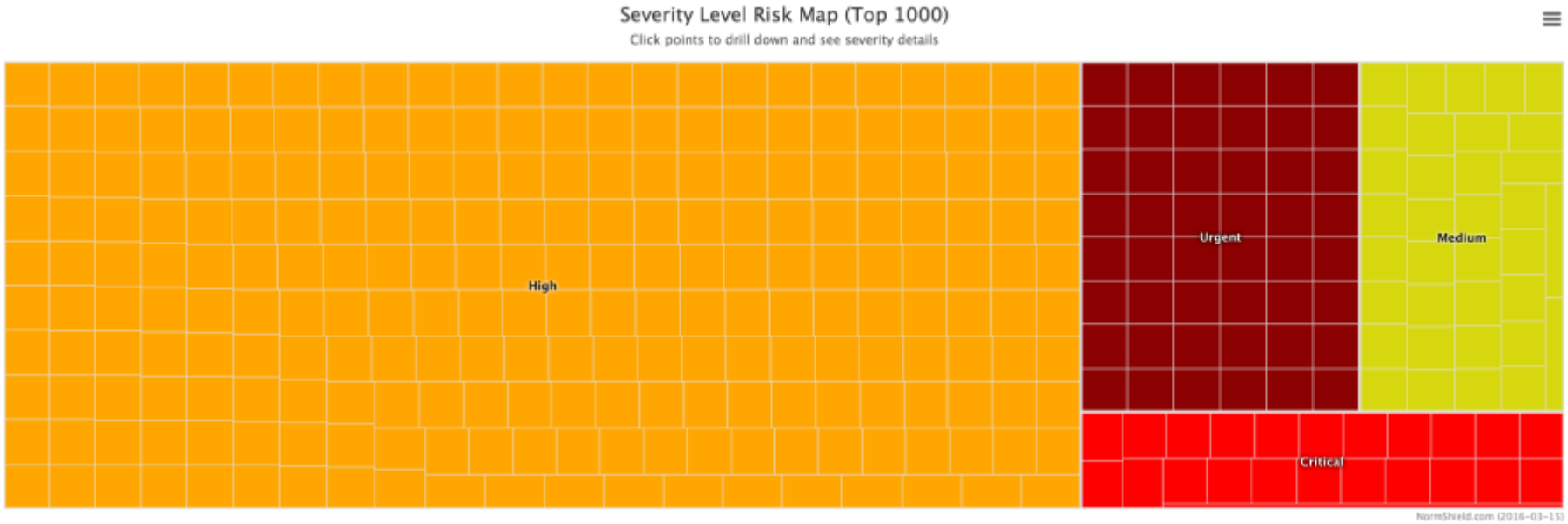
Inbox (CANDAN)

Date	Title
07.11.2015 22:16:33	Alert: Potential Data Leakage (BGA BANK)

SIEM Korelasyonunda Zafiyet Yönetimi Etkisi



Önceliklendirme #RootCause



Yönetilmesi Gereken En Önemli Zafiyet Bileşeni…

Teen Hackers: A '5-Year-Old' Could Have Hacked into CIA Director's Emails

October 19, 2015 // 05:54 PM EST

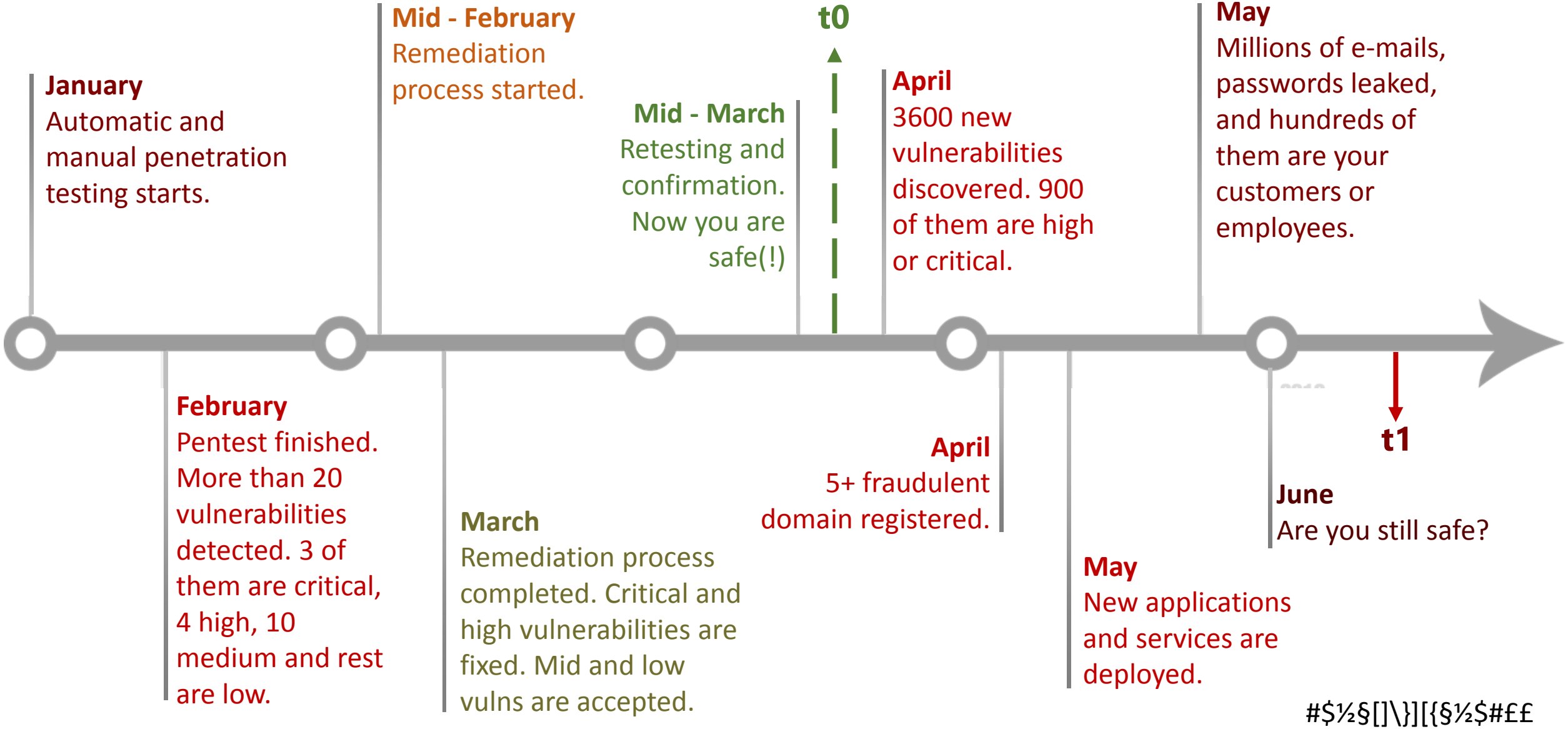
Hacking into the CIA Director's personal email was apparently child's play, according to the group who claimed the feat on Monday.

The hacker group, which calls itself "Crackas With Attitude" or CWA, said that hacking into John Brennan's email was "not hard at all."

"Like a 5 year old could do it," one of the group's hackers, who called himself "cubed," told Motherboard.

Türkiye Cryptolocker ortalaması %85

Zafiyet Yönetiminde Tehdit İstihbaratının Önemi



#$½§[]\}][{§½$#££

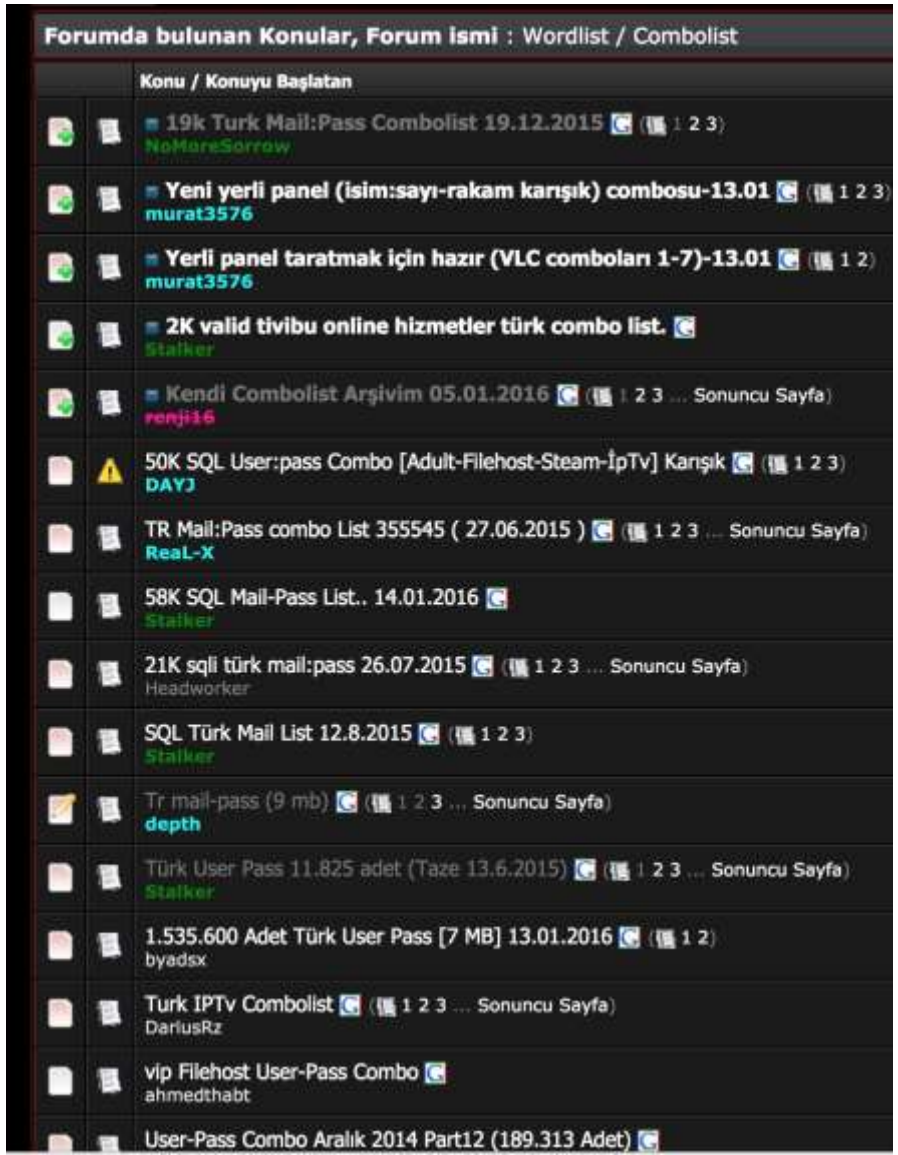
Siber (“Tehdit”) İstihbaratı #ThreatIntel #CyberInt

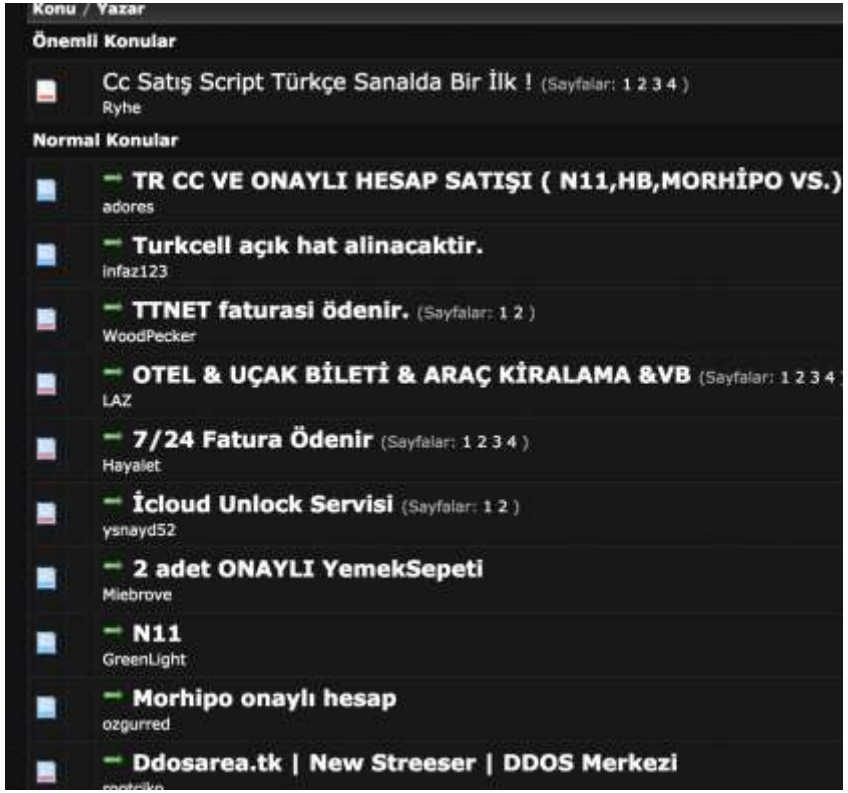
- **İstihbarat**, siyasi makamlara sunulmak üzere toplanmış ve çözümlenmiş izlemsel veya taktik içerikli işlenmiş bilgilere denir.
- Her türlü kaynaktan elde edilen ham bilgi ilişkisiz gibi görünen parçalardan oluşan, çelişkili, güvenilmez, yanıltıcı veya yanlış olabilir(*WikiPedia*)
- İngilizcede “intelligence” ve akıl, zeka, haber bilgi ve istihbarat anlamına gelir.
- Bu vurgu, haberin toplanmasında değil, toplananların birleştirilmesinde, işlenmesinde, değerlendirilmesindedir.
- Siber Tehdit istihbaratı…

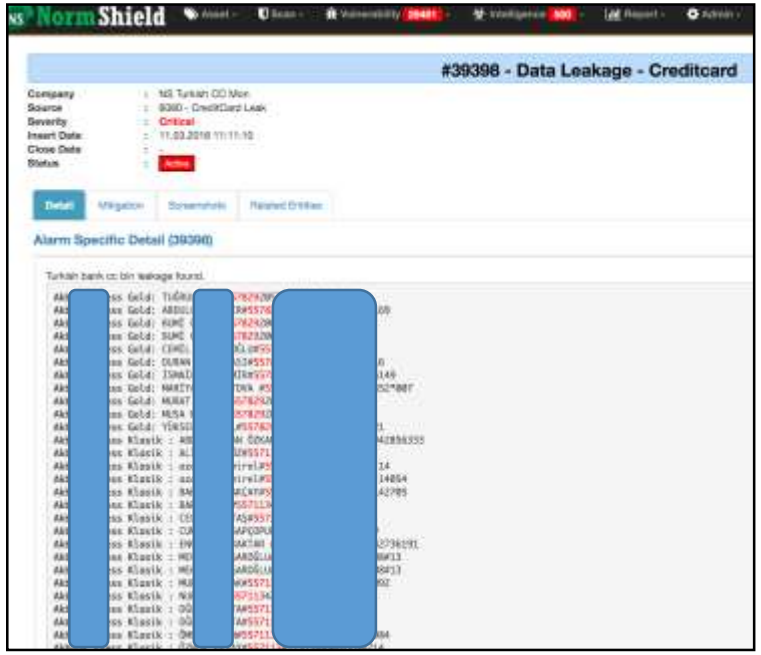
•1HUMINT (Human Intelligence)
•2GEOINT (Geospatial Intelligence)
•3MASINT (Measurement and Signature Intelligence)
•4OSINT (Open source intelligence)5
•SIGINT (Signals intelligence)
•6TECHINT (Technical intelligence)
•7CYBINT/DNINT (Cyber Intelligence/Digital Network Intelligence)
•FININT (Financial intelligence)

Neden Siber İstihbarata İhtiyaç Duyarız?

Normal Bir Günde Underground DünyadaDurum

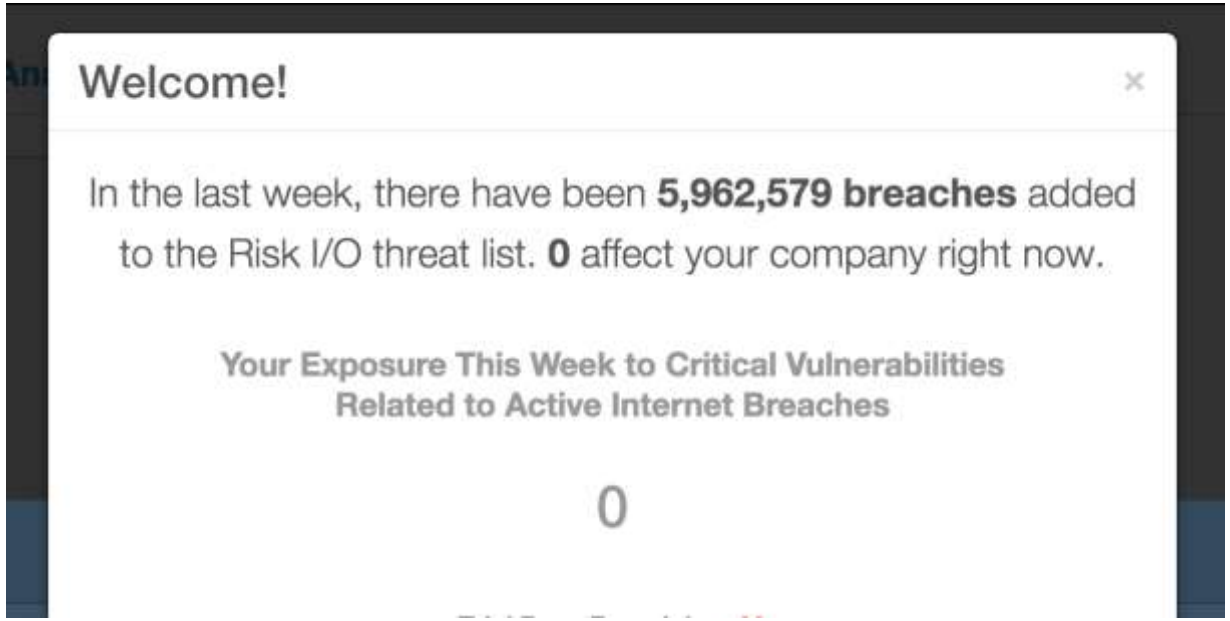






Gerçek Hayatta Nasıl Faydalanılır?

- Zafiyet önceliklendirme
- Sahte alan adlarının tespiti
- Cryptolocker gibi zararlı yazılımların önceden tespiti
- Bağlı olunan 3. parti veya güvenlik sistemlerinin kontrolü
- Ağ trafiği üzerinde tespit



Cyber Intelligence Dünyasında Sıradan Bir Gün

NormShield Alarms @ns_alarms · Mar 13
New Possible Fraudulent Domains
finasnbank.com
finansbank-enpara.com
kredikartiborcunusorgulama.org

NormShield Alarms @ns_alarms · Mar 12
New Possible Fraudulent Domains
turkcell19.biz
efatura.top
kuveytturk-tr.com
onlinesorguislemleri.com
1 1

NormShield Alarms @ns_alarms · Mar 12
turkcell16(.)net
turkcell68(.)org
turkcell99(.)com
turkcell46(.)com
turkcell51(.)org
turkcell75(.)biz
3 2

NormShield Alarms @ns_alarms · Mar 10
New Possible Fraudulent Domains
isbnkasionlineisubesi.com
isbnkasisubesionline.com
e-devlett.com
ttnetbasvurumerkezi.com

NormShield Alarms @ns_alarms · Mar 10
New Possible Fraudulent Domains
atmkredikartiborcsorgulama.com
hsbc-internetbanking.com
borcsorgulamaakbank.com
borcsorgulamaisbank.com
1

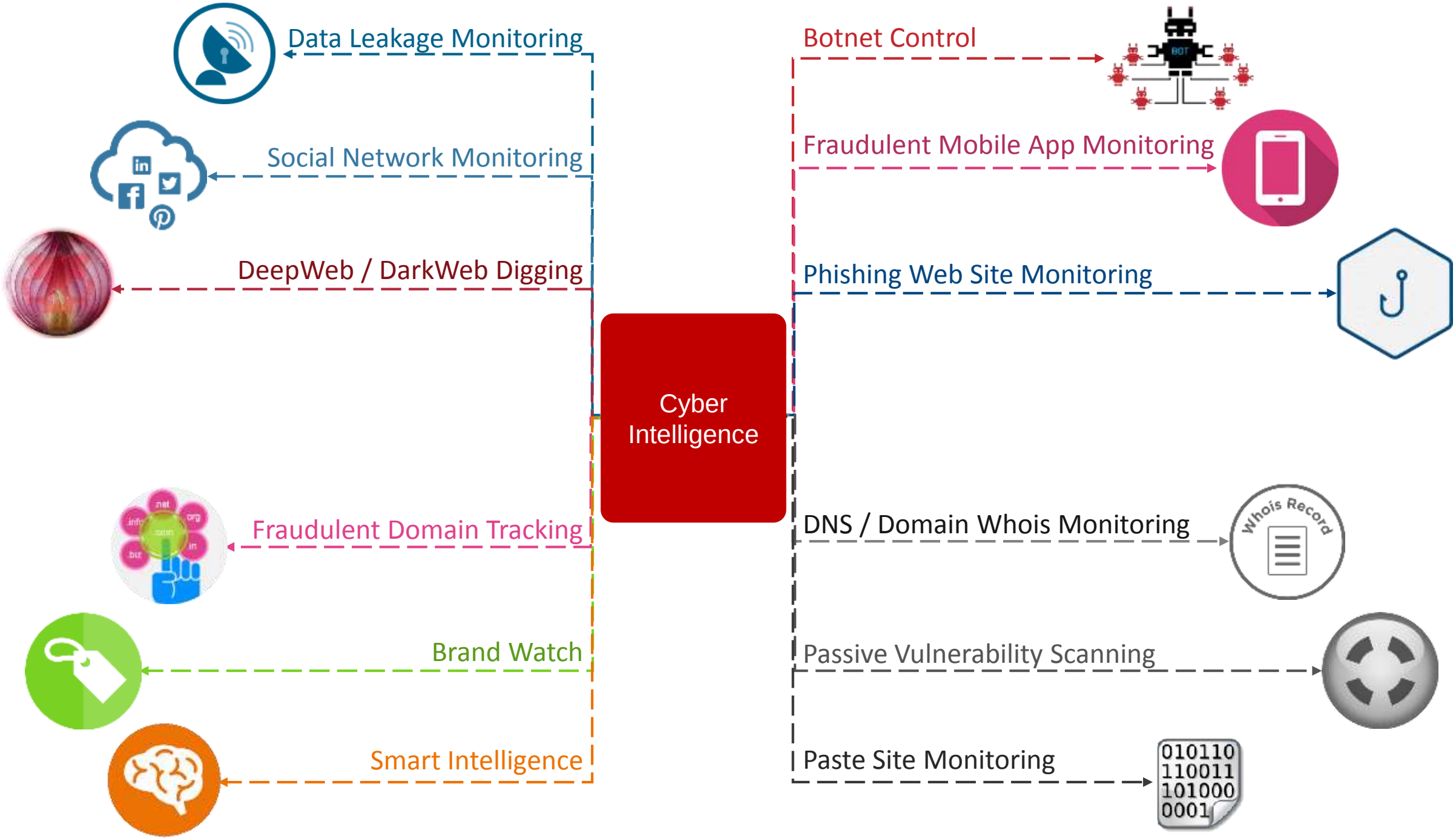
NormShield Alarms @ns_alarms · Mar 10
New Possible Fraudulent Domain
borcsorgulamavakifbank.com
borcsorgulamayapikredi.com
borcsorgulamafinansbank.com
borcsorgulamagarantibank.com
4 1

1000 USD / Day

NormShield Alarms @ns_alarms · Mar 7
New Possible Fraudulent Domains
app-faceboookredircet.online (Deceptive
faturaborcuodeme.com
elektrikfaturasiodeme.biz
tlyuklemee(.)com

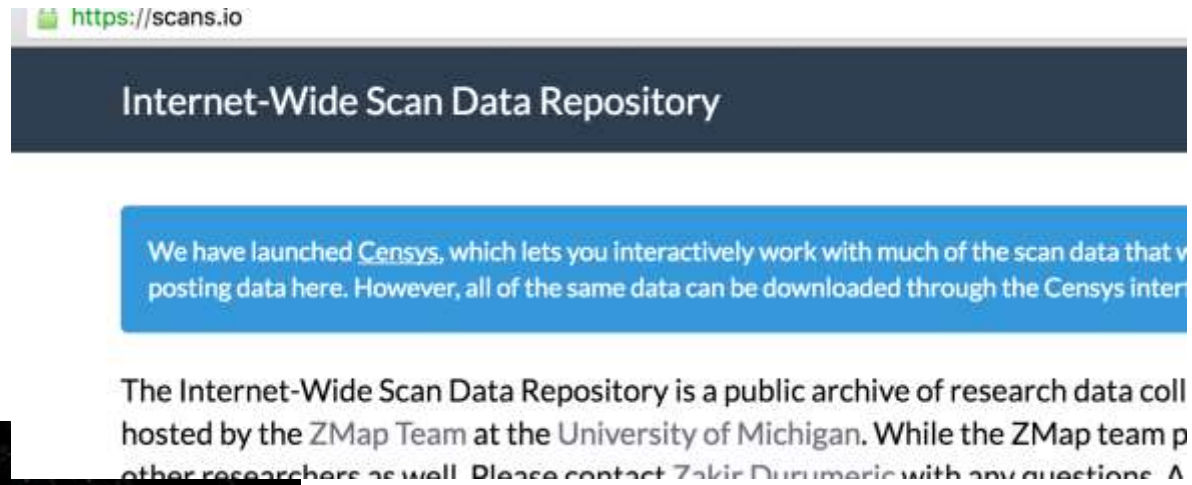
NormShield Alarms @ns_alarms · Mar 5
New Possible Fraudulent Domains
faturabayisi.net
mobilfaturaniz.com
akfaturaodeme.com
finansbankborcumusorgula.com

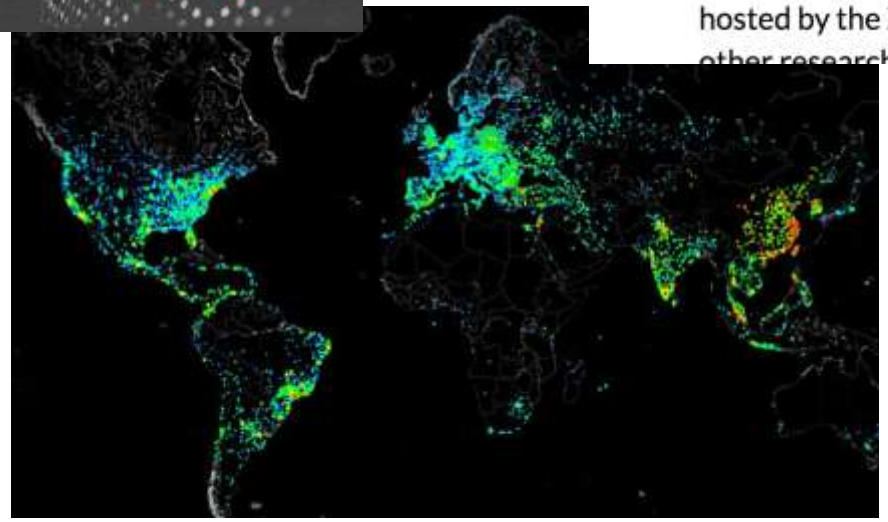
NormShield Alarms @ns_alarms · Mar 4
New Possible Fraudulent Domains
sorguhizmetleri.net
hsbcbankings(.)com
loginfacebooks(.)info
devletkredisi(.)com
trfaturabankmatik.com
1 1

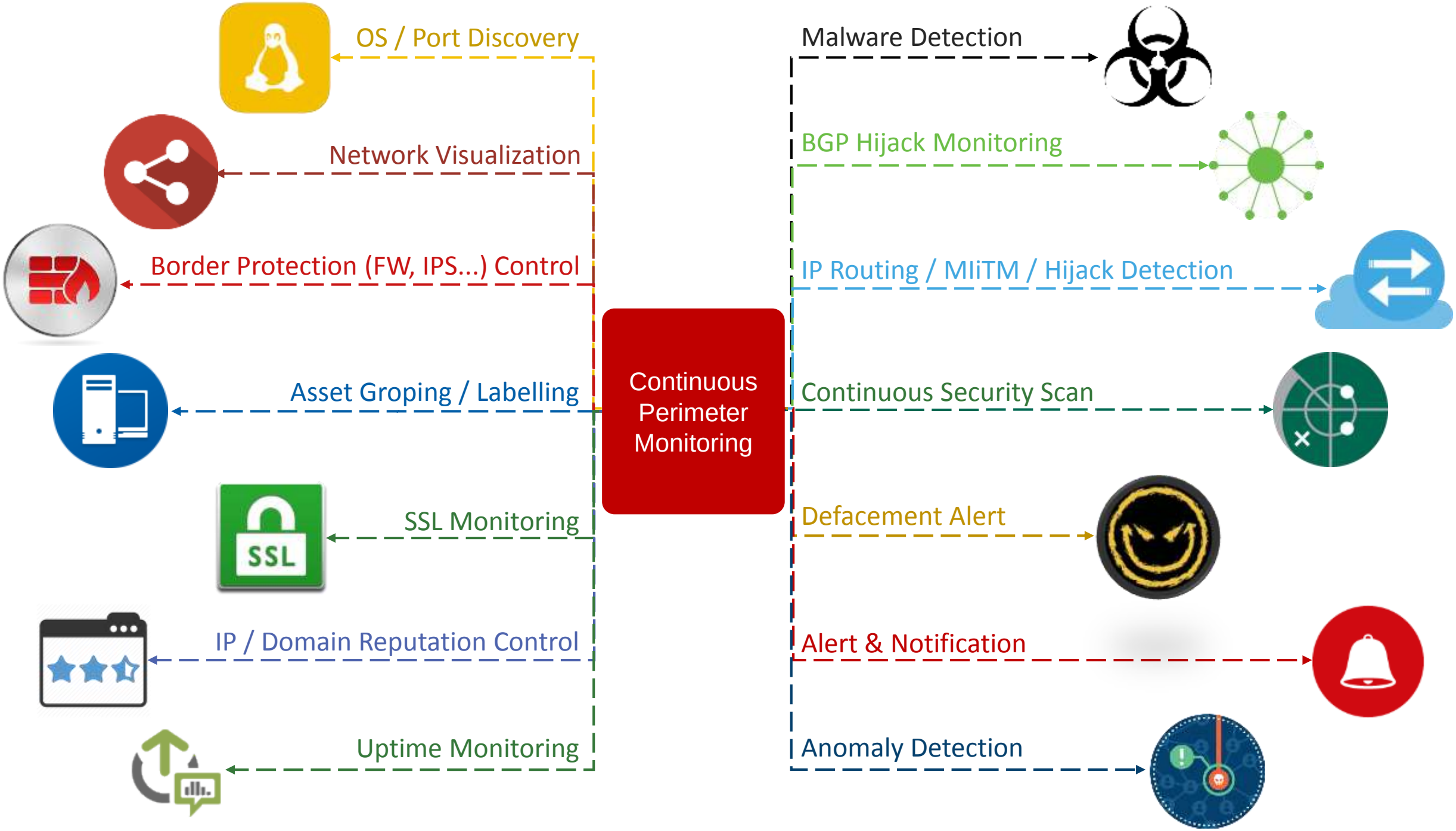

Cyber Intelligence
Data Leakage Monitoring
Social Network Monitoring
DeepWeb / DarkWeb Digging
Fraudulent Domain Tracking
Brand Watch
Smart Intelligence
Botnet Control
Fraudulent Mobile App Monitoring
Phishing Web Site Monitoring
DNS / Domain Whois Monitoring
Whois Record
Passive Vulnerability Scanning
Paste Site Monitoring
010110
110011
101000
0001

Düzenli Güvenlik İzleme #CPM #SOC Radar

- Birilerinin internete açık sistemlerimizi düzenli olarak tarıyor ve kontrol ediyor, ya siz?






Continuous Perimeter Monitoring
OS / Port Discovery
Network Visualization
Border Protection (FW, IPS...) Control
Asset Groping / Labelling
SSL Monitoring
SSL
IP / Domain Reputation Control
Uptime Monitoring
Malware Detection
BGP Hijack Monitoring
IP Routing / MIiTM / Hijack Detection
Continuous Security Scan
Defacement Alert
Alert & Notification
Anomaly Detection

Teşekkürler

İletişim Bilgileri

Blog

- www.lifeoverip.net
- Blog.bga.com.tr

Twitter

- @bgakademisi
- @huzeyfeonal

İletişim

- huzeyfe@lifeoverip.net
- Huzeyfe.onal@bga.com.tr