2024+ CYBERDAYS | 21 - 22 MARZO

Centro di Competenze 5G

PRISMA

Cybersecurity Landscape: how to avoid Costly Errors (at low cost)

Giuseppe Bianchi

University of Roma Tor Vergata

Director, National CNIT Network Assurance & Monitoring LAB

IN COLLABORAZIONE CON fondazione sistema toscana | INTERNET FESTIVAL FORME DI FUTURO

POR CreO 2014 2020 REGIONE TOSCANA FONDO EUROPEO DI SVILUPPO REGIONALE | FSC Fondo per lo Sviluppo e la Coesione | FUB Fondazione Ugo Bordoni Ricerca e Innovazione | SviluppoToscana S.p.A. | comune di PRATO | UNIONE EUROPEA | REPUBBLICA ITALIANA | Regione Toscana

Let’s start with some conclusions…

The best is the enemy of the good:

Let’s <u>first</u> focus on the low-hanging fruit

*(i.e., the **<u>many</u> trivially identifiable and easily fixable issues**)*

But don’t stop here:
a mandatory base for… further improvement!

Outline

1. How things can go (badly!) wrong…
   - *learning from examples*

2. What to do?
   - *at the very minimum*
   - *Institutions might help? Yes! (some proposals)*

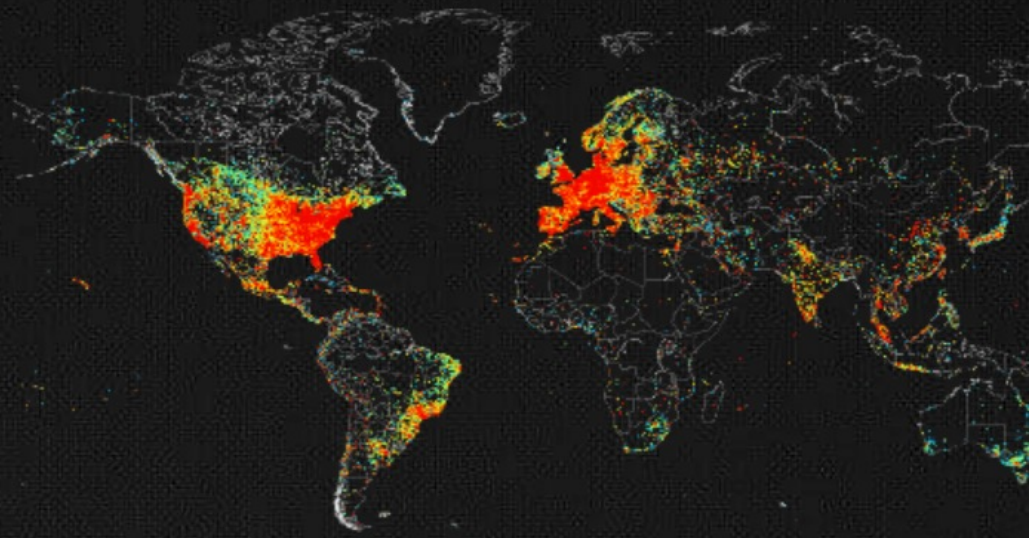
A first example - healthcare domain

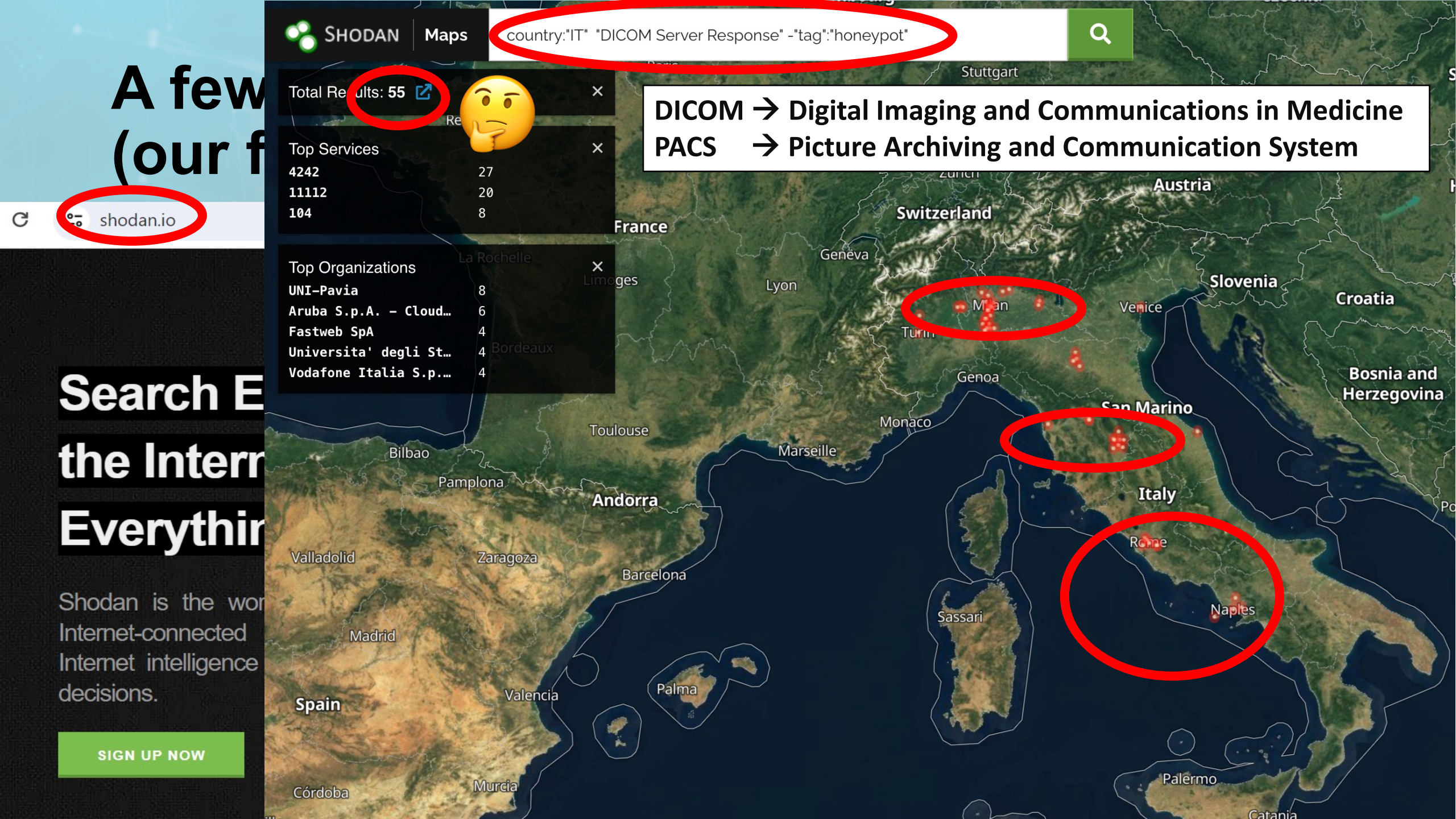
shodan.io

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW




A few
(our f
shodan.io
Search E
the Interr
Everythir
Shodan is the wor
Internet-connected
Internet intelligence
decisions.
SIGN UP NOW
SHODAN
Maps
country:"IT" "DICOM Server Response" -"tag":"honeypot"
Total Results: 55
Top Services
4242 27
11112 20
104 8
Top Organizations
UNI-Pavia 8
Aruba S.p.A. - Cloud… 6
Fastweb SpA 4
Universita' degli St… 4
Vodafone Italia S.p.… 4
DICOM → Digital Imaging and Communications in Medicine
PACS → Picture Archiving and Communication System
Stuttgart
Austria
Switzerland
France
Geneva
Lyon
Slovenia
Croatia
Venice
Genoa
Bosnia and Herzegovina
San Marino
Monaco
Marseille
Toulouse
Bilbao
Pamplona
Andorra
Italy
Valladolid
Zaragoza
Barcelona
Rome
Naples
Sassari
Madrid
Spain
Valencia
Palma
Córdoba
Murcia
Palermo
Bordeaux

A few (our f

shodan.io

Internet-connected Internet intelligence decisions.

SIGN UP NOW

SHODAN | Maps

country:"IT" "DICOM Server Response" -"tag":"honeypot"

Total Results: 55

Top Services

4242	27
11112	20
104	8

Top Organizations

UNI-Pavia
Aruba S.p.A. –
Fastweb SpA
Universita' deg
Vodafone Italia

What if some of such **exposed servers were not protected?**

DICOM Query/Retrieve

Patient Name	Patient ID	Date of Birth	Descripti...	Modality	# im	Date	Time	Source
				MR	783	08/01/24	13:27:02	
				MR	936	08/01/24	11:53:17	
			Cervical	MR	28	10/01/24	12:53:09	
			Cervical	MR	30	10/01/24	13:13:01	
			Cervical	MR	376	10/01/24	13:29:07	
			Mk Kopf	MR	583	08/01/24	11:33:38	
			Cervical	MR	628	09/01/24	15:56:26	
			Cervical	MR	431	09/01/24	17:16:20	
1			Scout	MR	3	09/01/24	17:20:09	
2			Se T1 Scou	MR	5	09/01/24	17:21:20	
3			Se T1 Scou	MR	5	09/01/24	17:22:15	
4			Fse T2 Sag	MR	9	09/01/24	17:29:00	
5			Fse T2 Tra	MR	26	09/01/24	17:36:12	
6			3D Hyce T	MR	366	09/01/24	17:43:50	
7			Fast Stirne	MR	17	09/01/24	17:49:35	
			Mk Kopf	MR	579	09/01/24	14:46:16	

Keep this window on top of all other windows — 22 studies found

Attacker could access, modify, and upload malware (realistic example)

Geneva · France · Slovenia · Croatia · Venice · Bosnia and Herzegovina · San Marino · Italy · Rome · Naples · Palermo · Catania · Valladolid · Madrid · Spain · Córdoba


SHODAN
Explore
Provincia di Prato - Regist
193.43.107.198
comune.prato.it
vas-exprv.comune.prato.it
Comune di Prato
Italy, Prato
SSL Certifi
Issued By:
|- Common Nam
RapidSSL TLS
CA G1
|- Organization:
DigiCert Inc
Issued To:
|- Common Nam
*.comune.prato
Supported SSL
TLSv1, TLSv1.1
TLSv1.2, TLSv1
Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2023-45802 When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their ow "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
CVE-2023-31122 Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
CVE-2023-25690 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-37436 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2022-36760 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
CVE-2022-31813 7.5Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2022-30556 5.0Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2022-29404 5.0In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-28615 6.4Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-28614 5.0The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2022-28330 5.0Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2022-26377 5.0Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2022-23943 7.5Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
CVE-2022-22721 5.8If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-22720 7.5Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2022-22719 5.0A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2021-44790 7.5A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
200+ other ~~vuln..~~ lines deleted
SHODAN
Explore
Down
193.43.107.198
Qualys. SSL Labs

SSL Report: vas-exprv.comune.prato.it (193.43.107.198)

Assessed on: Wed, 20 Mar 2024 14:04:07 UTC | Hide | Clear cache

Scan Another

Summary

Overall Rating

F

Visit our documentation page

This serve

This se

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK		
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK		
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK		
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK		
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	EC	) FS	WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK		
TLS_RSA_WITH_DES_CBC_SHA (0x9)	INSECURE		

Registro Provinciale del Terzo Settore

Associazioni di Promozione Sociale, Organizzazioni di Volontariato, Cooperative Sociali Onlus

Cooperative Sociali Onlus | Organizzazioni di Volontariato | Associazioni di Promozione Sociale

Ricerca nel Registro

Nome

Nome associazione...

Acronimo

Acronimo associazione...

Settore

Seleziona settore...

Località

Seleziona località...

Includi cancellazioni

Cerca

Selezionare una sezione del registro per accedere alle funzioni di consultazione e ricerca.

Upload forms: possible channels for SQL injection, or for XSS storing?

We CANNOT check without permission forbidden by law!

Hard-coded credentials hidden in plain sight

A perpetual issue: how to securely handle secrets in programs & apps

The (modern) survival guide to cybersecurity

Assume that your opponents know everything

If the **source code** or design blueprint were **leaked** today it should not change the security exposure of your product

(Quoting Thai Duong)

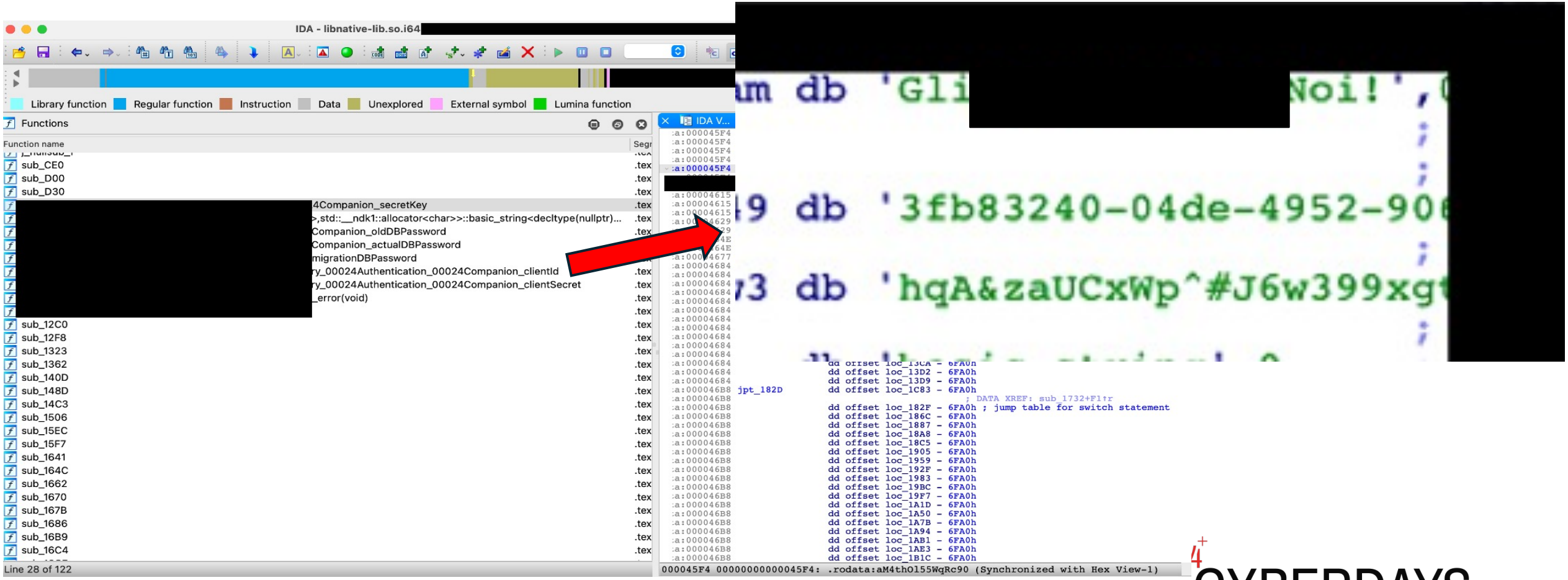
Plainly speaking:

Any practicioner can today reverse

so please DO NOT place secrets in plain sight within the code…

Hard-coded credentials hidden in plain sight

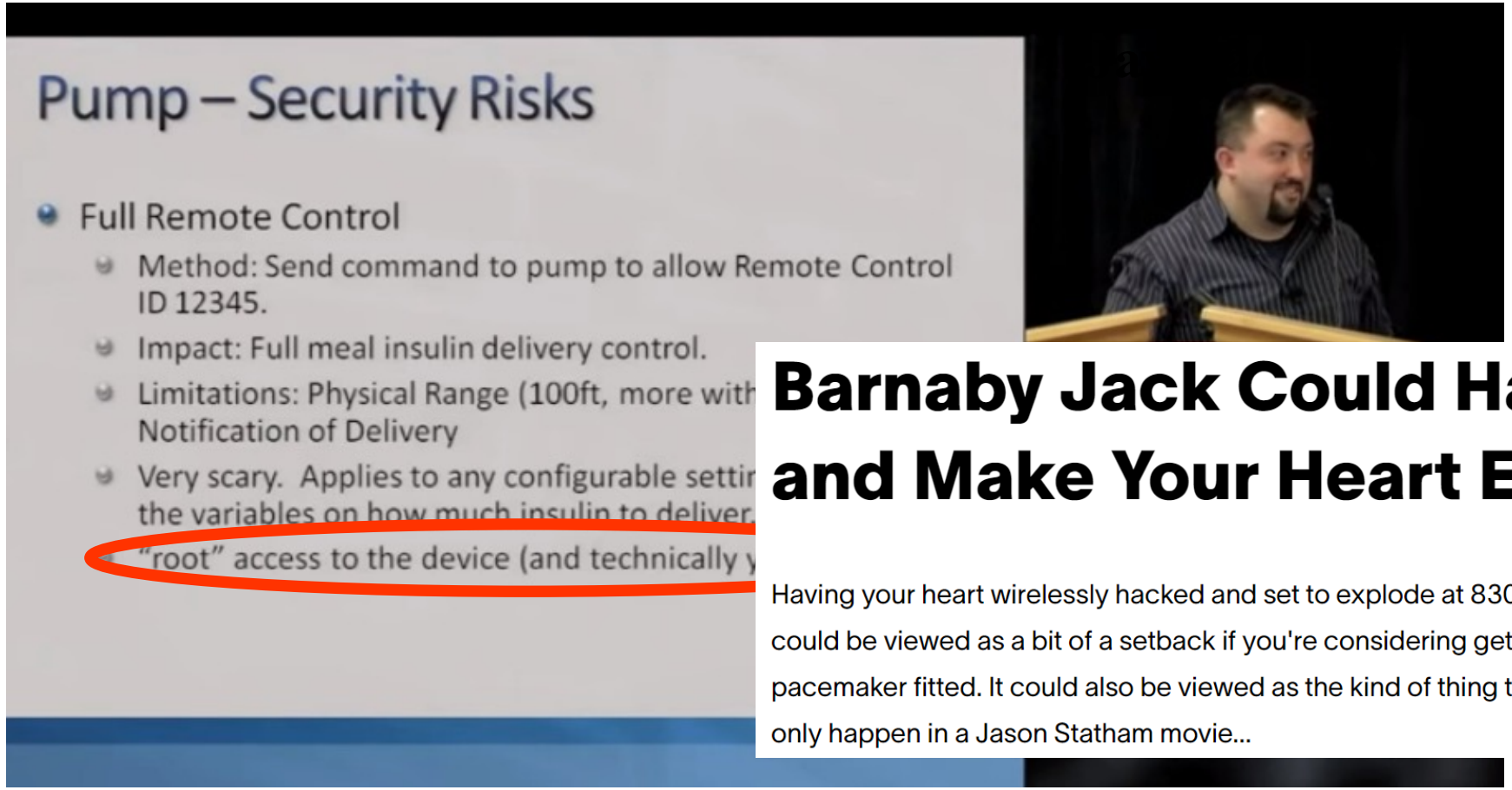
DITTO! Example from a (somewhat randomly chosen) medical device



Access control bypass in medical devices: which potential impact?

Insulin pumps, Defibrillators, Pacemakers …. Inside our bodies and wireless connected!

Attacks demonstrated since 2011!!



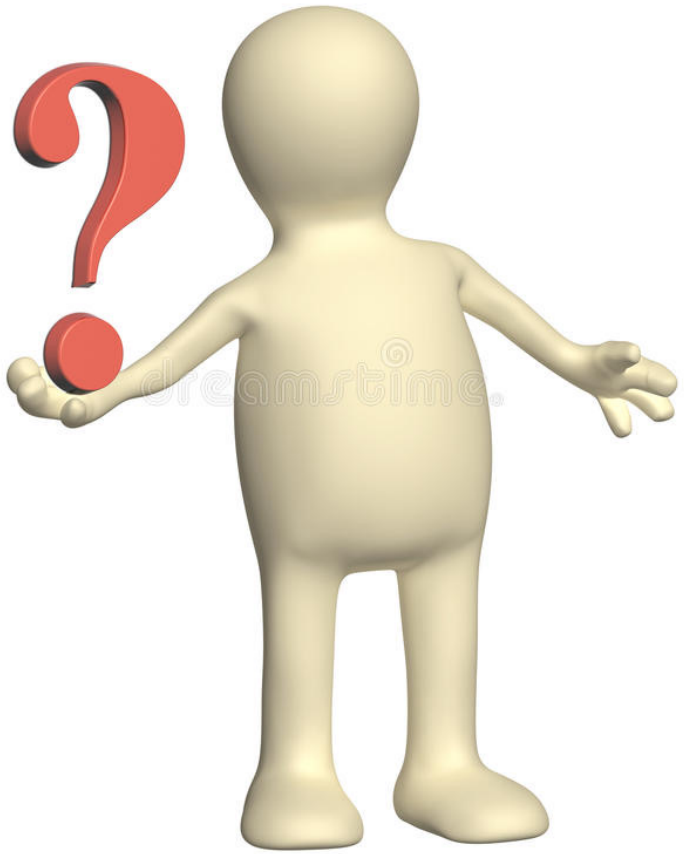
Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode

Having your heart wirelessly hacked and set to explode at 830 volts could be viewed as a bit of a setback if you're considering getting a pacemaker fitted. It could also be viewed as the kind of thing that would only happen in a Jason Statham movie...

Scheduled at Blackhat 2013

He died a week before…

Vice President Cheeney disabled pacemaker



So, what can we do?

Prevention is better than recovery!

Control, control, use very pragmatic controls! Don't leave cyber doors badly opened!

Example: CIS Controls – very practical and «actionable»

tailored to SMEs

IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Critical Security Controls v8

01 Inventory and Control of Enterprise Assets
02 Inventory and Control of Software Assets
03 Data Protection
04 Secure Configuration of Enterprise Assets and Software
05 Account Management
06 Access Control Management
07 Continuous Vulnerability Management
08 Audit Log Management
09 Email and Web Browser Protection
10 Malware Defenses
11 Data Recovery
12 Network Infrastructure Management
13 Network Monitoring and Defense
14 Security Awareness and Skills Training
15 Service Provider Management
16 Applications Software Security
17 Incident Response Management
18 Penetration Testing

01 Inventory and Control of Enterprise Assets

1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

02 Inventory and Control of Software Assets

2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●

04 Secure Configuration of Enterprise Assets and Software

4.1	Establish and Maintain a Secure Configuration Process	●	●	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●	●	●
4.4	Implement and Manage a Firewall on Servers	●	●	●
4.5	Implement and Manage a Firewall on End-User Devices	●	●	●
4.6	Securely Manage Enterprise Assets and Software	●	●	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●	●	●
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		●	●
4.9	Configure Trusted DNS Servers on Enterprise Assets		●	●
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		●	●
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		●	●
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			●

Cyber Threat Awareness → phishing resilience

One of the most important… «control»!

14	Security Awareness and Skills Training			
14.1	Establish and Maintain a Security Awareness Program	●	●	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●
14.3	Train Workforce Members on Authentication Best Practices	●	●	●
14.4	Train Workforce on Data Handling Best Practices	●	●	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●	●	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●
14.9	Conduct Role-Specific Security Awareness and Skills Training		●	●

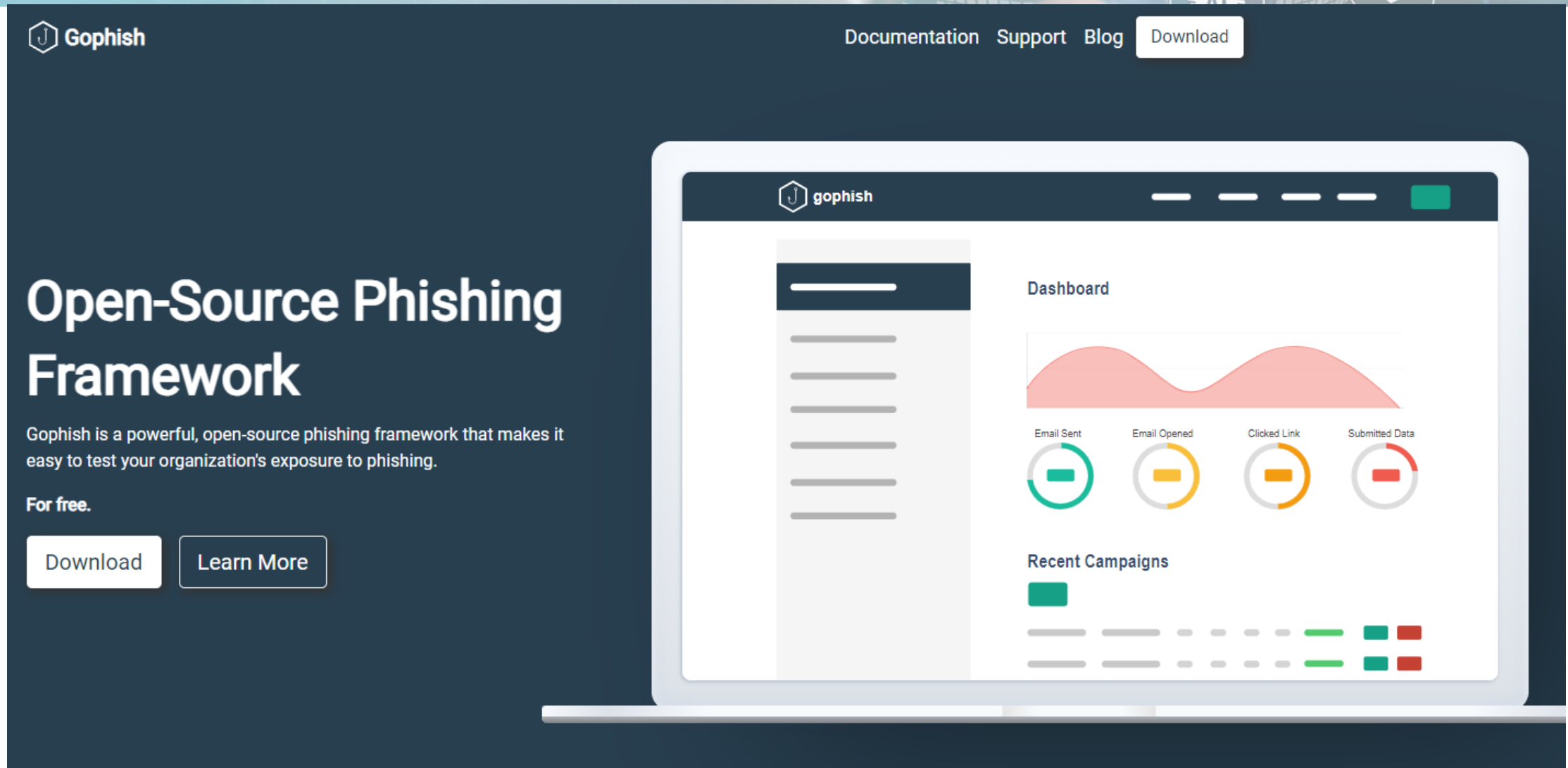
Compare with:

13	Network Monitoring and Defense		
13.1	Centralize Security Event Alerting	●	●
13.2	Deploy a Host-Based Intrusion Detection Solution	●	●
13.3	Deploy a Network Intrusion Detection Solution	●	●
13.4	Perform Traffic Filtering Between Network Segments	●	●
13.5	Manage Access Control for Remote Assets	●	●
13.6	Collect Network Traffic Flow Logs	●	●
13.7	Deploy a Host-Based Intrusion Prevention Solution		●
13.8	Deploy a Network Intrusion Prevention Solution		●
13.9	Deploy Port-Level Access Control		●
13.10	Perform Application Layer Filtering		●
13.11	Tune Security Event Alerting Thresholds		●

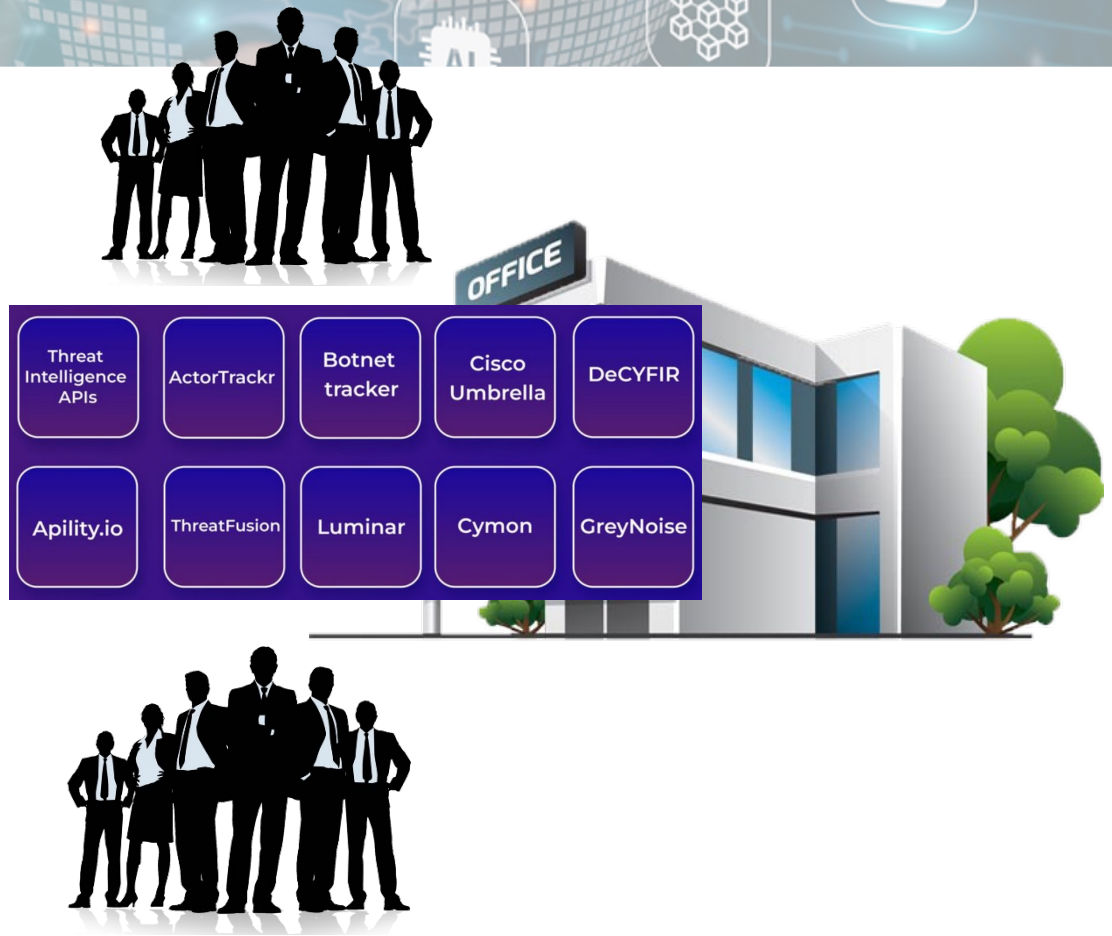
MARZO

Cyber Threat Awareness → phishing resilience

and low-cost services and (even zero-cost!) solutions available



Institutions can SIGNIFICANTLY help…
a) with centralized reconnaissance teams



Lower costs (better value for money)

Institutions can SIGNIFICANTLY help…
b) by strengthening proactive/preventive support

(57) As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.

We obviously cannot recommend specific products, but this is a list of tools that can help you implement these recommended controls…

Guiding principles:

1. ***Support for prevention: also advocated by NIS2***
2. ***Extensively assess patches (lack of skills → mistakes likely!)***

Institutions c) by en

Ac

- **Encourage ma**
  - *Rather than*

United Nations | Office of Information and Cor

Home | Analytics | Cybersecurity | E

Home » UN Information Security Hall of Fame

UN Information Security Hall of Fame

To improve the protection of its Information Communicati the United Nations encourages the public to assist with its vulnerabilities in the United Nations' publicly accessible ir

Following are individuals and organizations that helped th the security of the Organization's systems, data, and ICT security issues and vulnerabilities discovered.

- **Bug bounty programs**
  - *non necessarily money: social reward also VERY appealing!*

If even very «critical» bodies do this, see e.g. US DoD's Hack-The-Pentagon; Why shouldn't we do the same?

What? Having THEM (!) attacking me???

YES! With:

- *clear rules of engagement*
- *Structured processes for reporting vulnerabilities*

In scope

Doctolib public-facing websites:
www.doctolib.fr www.doctolib.de www.doctolib.it

Doctolib web application for professionals:
pro.doctolib.fr pro.doctolib.de pro.doctolib.it

Doctolib B2B website:
info.doctolib.fr info.doctolib.de info.doctolib.it

Doctolib API gateway:
api.doctolib.fr api.doctolib.de api.doctolib.it

Doctolib public infrastructure:
*.doctolib.(fr|de|it|com|net)

Doctolib iOS App:
https://apps.apple.com/fr/app/doctolib/id925339063

Doctolib Android App:
https://play.google.com/store/apps/details?id=fr.doctolib.www&hl=fr

Unauthenticated remote code execution against underlying Doctolib Cloud infrastructure.

Authentication bypass for Doctolib Pro software products (with bypass of multi-factor authentication).

Conclusions

Ask yourself / your CEO (also) cybersecurity-related questions…

(Question #7 from ENISA's Cybersecurity Maturity Assessment for SME)

What will be the level of impact on my business if:

- ***Our accounting / financial data are totally lost***
- ***All our data are made unavailable for 1 month***
- ***Data of our core business is stolen and made available online and/or to our competitors***
- ***Confidential data of our customers has been stolen, the offenders threaten to publish them online and advertise our customers unless we pay a ransom***
- ***Our customer database is stolen and sold to our competitors***

Conclusions

… And prioritize prevention / controls:
it's in YOUR interest! And do it before others ☺

Who would you attack?

Crime do care only about money…
Weaker victims are preferable!

Thank you!

Giuseppe Bianchi

Giuseppe.bianchi@uniroma2.it

University of Roma Tor Vergata

Director, National CNIT Network Assurance & Monitoring LAB

s ☺

Who would you attack?

Crime do care only about money…
Weaker victims are preferable!

2024+ CYBERDAYS | 21 - 22 MARZO