Trials and Tribulations of Cybersecurity Information Sharing

Christian Popov

ASOC, Senior Analyst

kristiyan.popov@telelink.com

@ChrisPSecc

telelink

Agenda

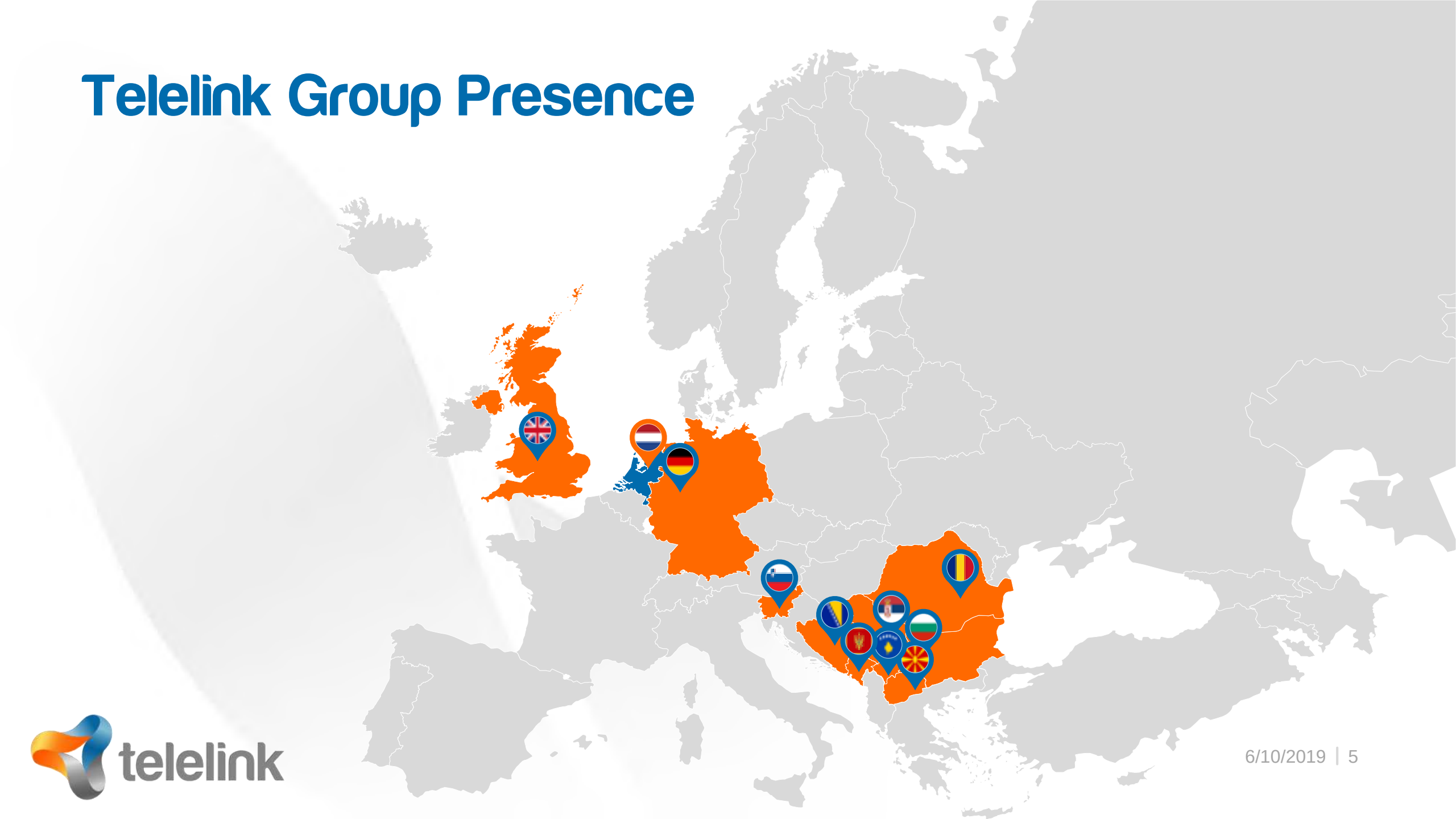
- The Information Age
- Cybersecurity Information Sharing
- Responsible Disclosure
- ASOC – Real Life Case Studies
- Telelink’s ASOC and Information Sharing
- Conclusions

Telelink Group at a Glance

- **18 years** of excellence
- **Global** network - presence in **10 countries**
- **Dedicated team of experts**
- **Partnerships with the leading global vendors**
- **€100M revenue** in 2018, targeting over €100M in 2018

telelink

Telelink Group Presence



telelink

Telelink Group Business Lines

Business Services

Engaging in business processes and customer needs in the field of IT infrastructure, information security, digital transformation, big data, and managed services

Infra Services

Engaging in delivering services for the construction and operation of communication infrastructure, delivery and integration of physical security systems, and building management systems

City Services

Engaging in developing and selling through partners Microsoft Azure based Smart City solutions

Labs

Engaging in research, development and training activities focusing on 5G networks and their application

telelink

TBS - Expertise and Services

Managed Services

- Managed Enterprise Networks
- Managed Security Services
- Equipment as a Service
- Data Protection Officer as a Service

Consulting Services

- Digital Transformation
- Cloud Enablement
- Governance, Risk, and Compliance
- Advisory Services

Digital Transformation

- Data Management
- Workplace Productivity
- Transformation Strategies
- Cloud Enablement
- Business Intelligence and Analytics

Cloud Services

- Microsoft Cloud Solutions
- Advanced Security Operations Center

Technical Services

- Design Services
- Deployment Services
- App Development

Enterprise Networks

- Wired and Wireless
- Communication and Collaboration
- Data Center Networking

Data Center

- Automation and Orchestration
- Computing and Storage
- Business Continuity
- Hybrid Data Center

Information Security

- Infrastructure and Endpoint Security
- Securing Hybrid IT
- Governance, Risk, and Compliance
- Assessment and Response
- Converged Security and Information Management

Support Services

- Extended Warranty
- Extended Support

telelink

Industry Partners

telelink

Main Clients

The Human Nature

"**Man is by nature a social animal**; an individual who is unsocial naturally and not accidentally is either beneath our notice or more than human.

Society is something that precedes the individual.

Anyone who either cannot lead the common life or is so self-sufficient as not to need to, and therefore does not partake of society, is either a beast or a god. "

Aristotle

telelink

Image source: Internet

The Internet Nature

Big Data

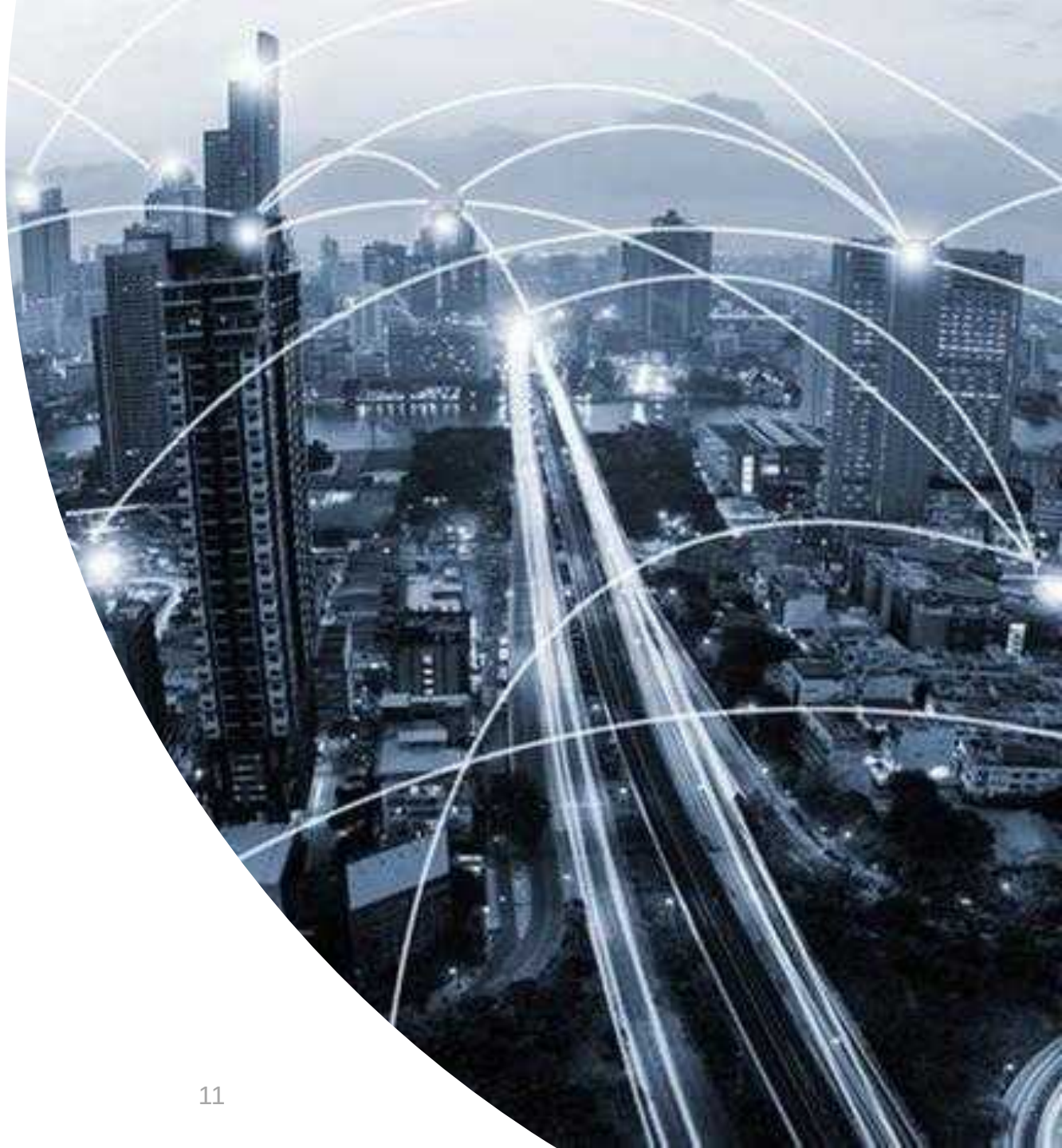
Machine Learning

AI

Dark Blockchain

Information Sharing

Social Media



telelink

Image source: Internet

Cybersecurity Information Sharing

Cybersecurity Information Sharing

Analyst to Analyst

Public Disclosure

Analyst to Enterprise

Enterprise to Enterprise

Responsible Disclosure

telelink

Analyst to Analyst

- Every day security researchers and analysts share information on trending topics in information security in order to help people better protect themselves from threats.
- Topics:
  - Indicators of compromise (IoCs)
  - New attack tactics (Tactics, Techniques, Procedures)
  - Defense tactics and detection (YARA rules, sigma rules, SIEM use cases)
  - Emerging threats
  - Security News
  - Experience and advice

Do not share private/company information!
If you're not sure if you can share it publicly - don't!

telelink

Analyst to Analyst

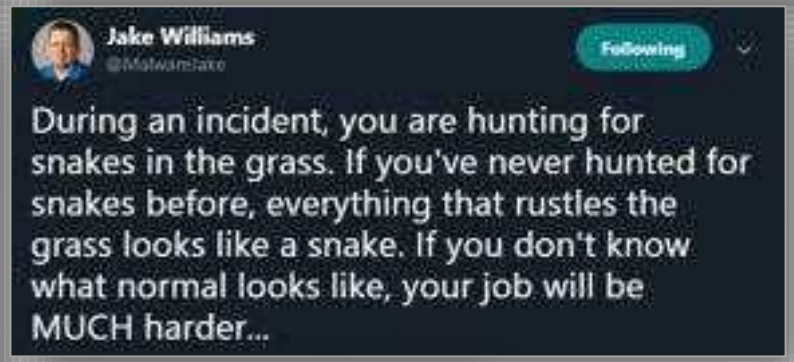


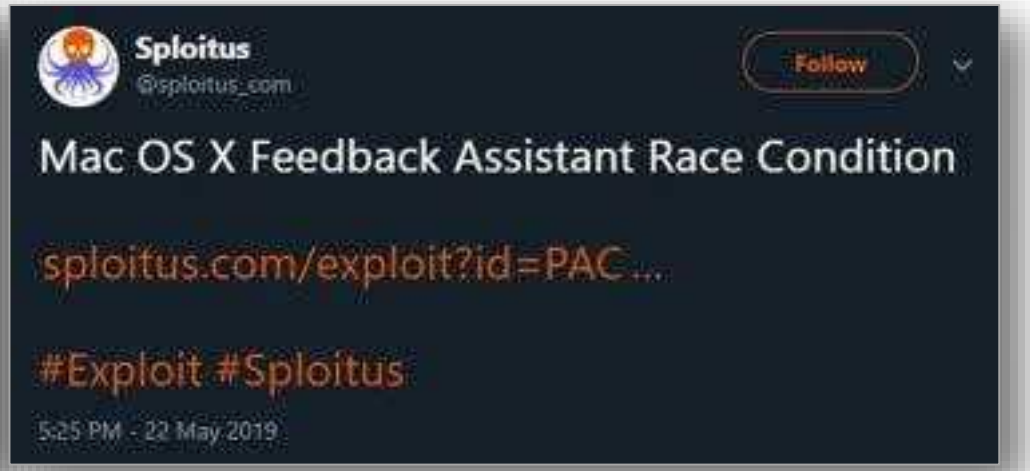
Image sources: Twitter

Public Disclosure

- Communicating the vulnerability to the public should have a broad impact to reach the awareness of the users, and it usually takes one of two possible paths.
  1. **Easy way** – publish blog post, share on cybersecurity forums and control the information
  2. **Hard way** – connect directly with a journalist from a responsible media, work together, but loose control over the information

- Handling the public disclosure comes with quite a bit of stress for the inexperienced as once the story starts rolling publicly you are not in control anymore.

Public Disclosure



telelink

Image sources: Twitter

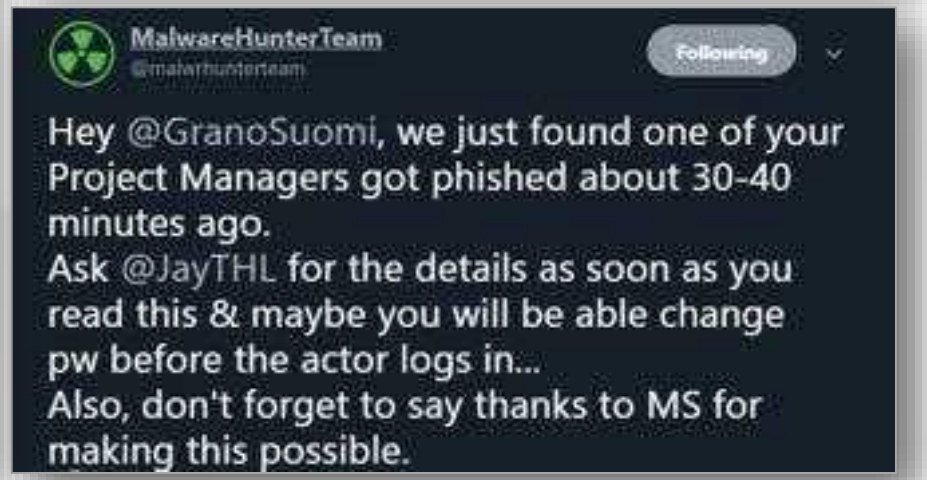
Analyst to Enterprise (disclose at your own risk…)

- Whenever an security researcher finds a security flaw he/she has a choice to make:
  1. Disclose/Notify the affected party
  2. Keep it a secret and potentially use the vulnerability
  3. Do nothing

- Most security researchers will opt to contact the company or vendor and notify them.
- However that is not always the case…

telelink

Analyst to Enterprise (Disclose at your own risk …)



telelink

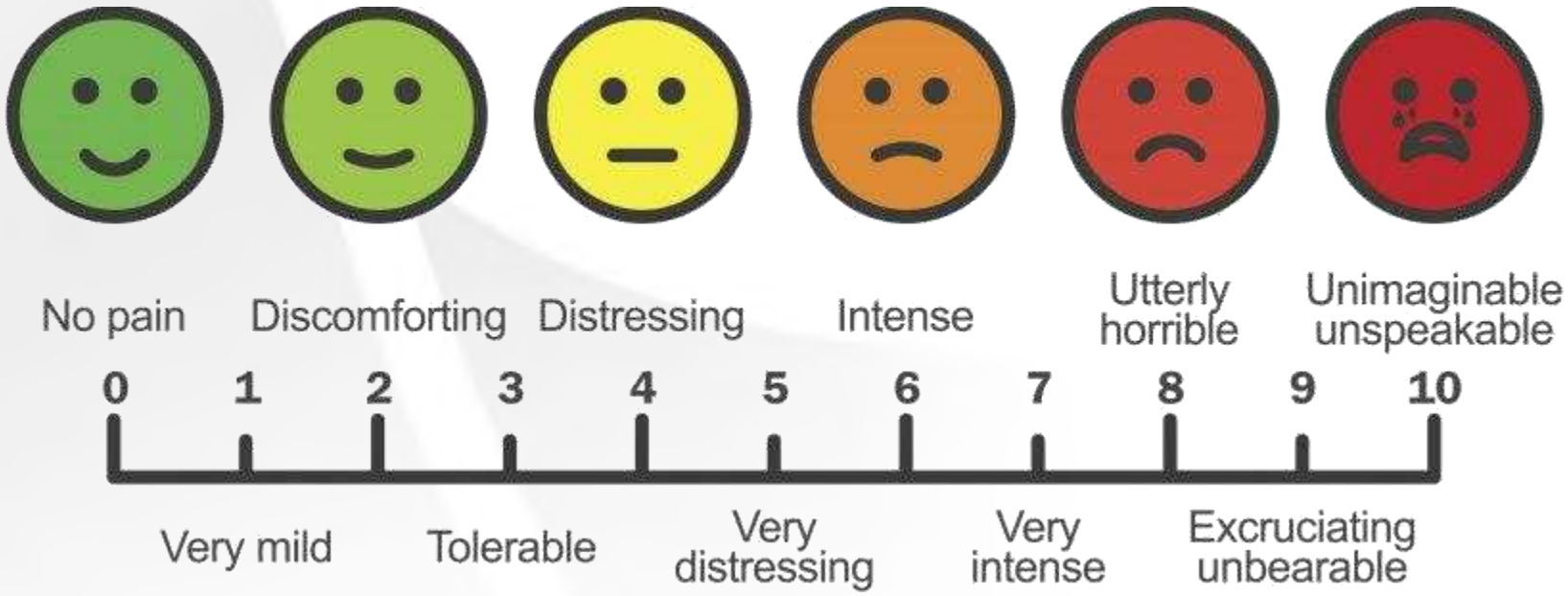
Image sources: Twitter

The Reactions

Thank you!!
You are the best!
We're sending
you all the $$$!!

Whatever

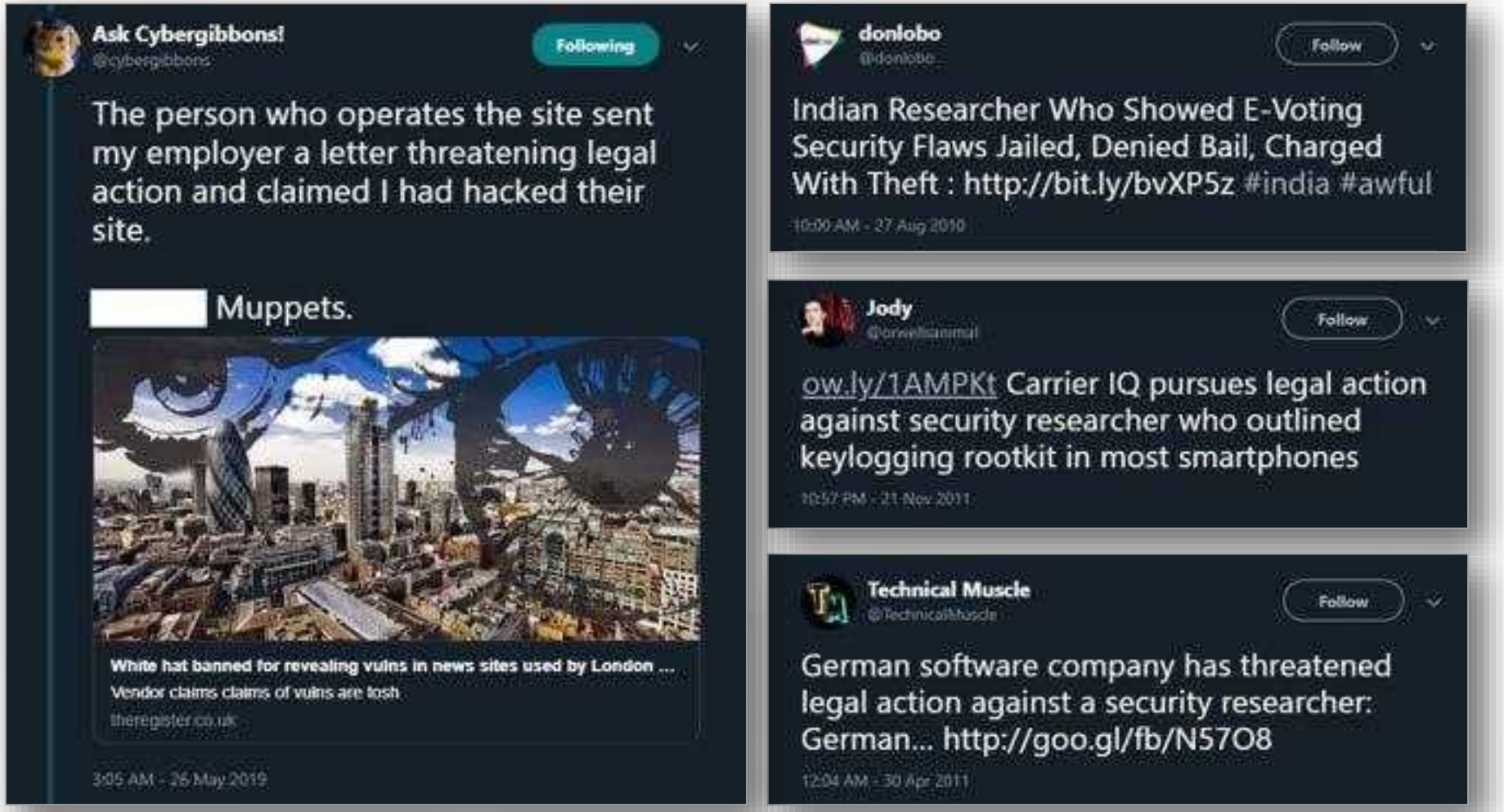
Who are you??
How did you get this
information??
We are getting our
lawyers!



telelink

Image source: Internet

The Legal Action(s)



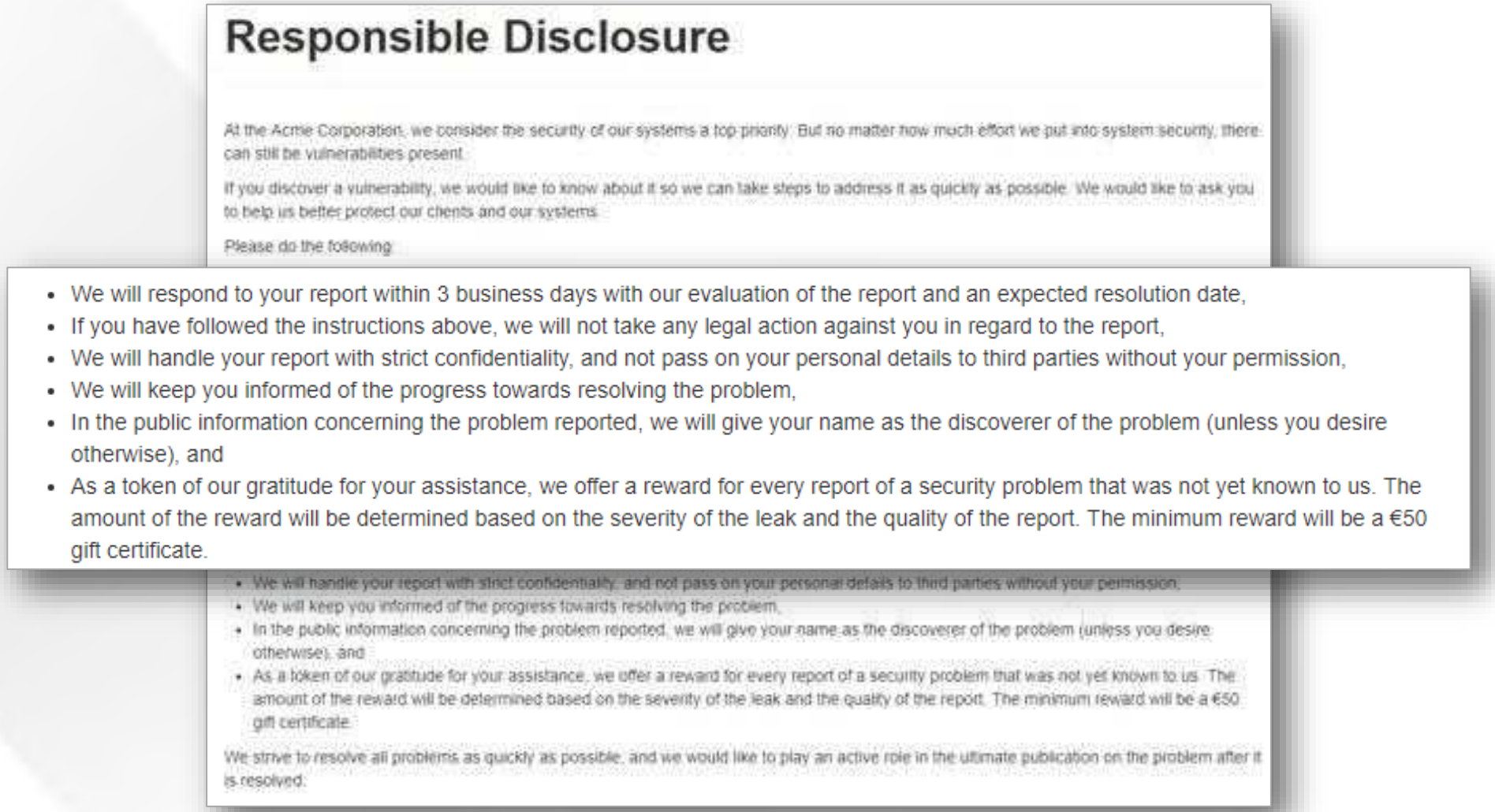
telelink

Image source: Twitter

Cybersecurity Information Disclosure

https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/
https://threatpost.com/the-vulnerability-disclosure-process-still-broken/137180/

Responsible Disclosure Policy



Responsible Disclosure

At the Acme Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

https://responsibledisclosure.nl/en/

Enterprise to Enterprise

Following the various Responsible disclosure policies companies can still share the vulnerabilities found in their own or another company's product

telelink

Google policy - https://www.google.com/about/appsecurity/
Palo Alto policy - https://www.paloaltonetworks.com/security-disclosure

Responsible Disclosure

What Happens when a Vulnerability is Found?

- A security researcher will **privately** report the breach to the company and will allow the team a reasonable timeframe to fix the issue, but in the case they do not, they may publicize the exploit to alert the public.
- Disclosing a vulnerability to the **public** is known as full disclosure, and there are different reasons why a security researcher may go about this path.

telelink

Vulnerability Disclosure

A security researcher may disclose a vulnerability if:

- They are unable to get in contact with the company.
- Their vulnerability report was ignored (no reply or unhelpful response).
- Their vulnerability report was not fixed.
- They felt notifying the public would prompt a fix.
- They are afraid of legal prosecution.

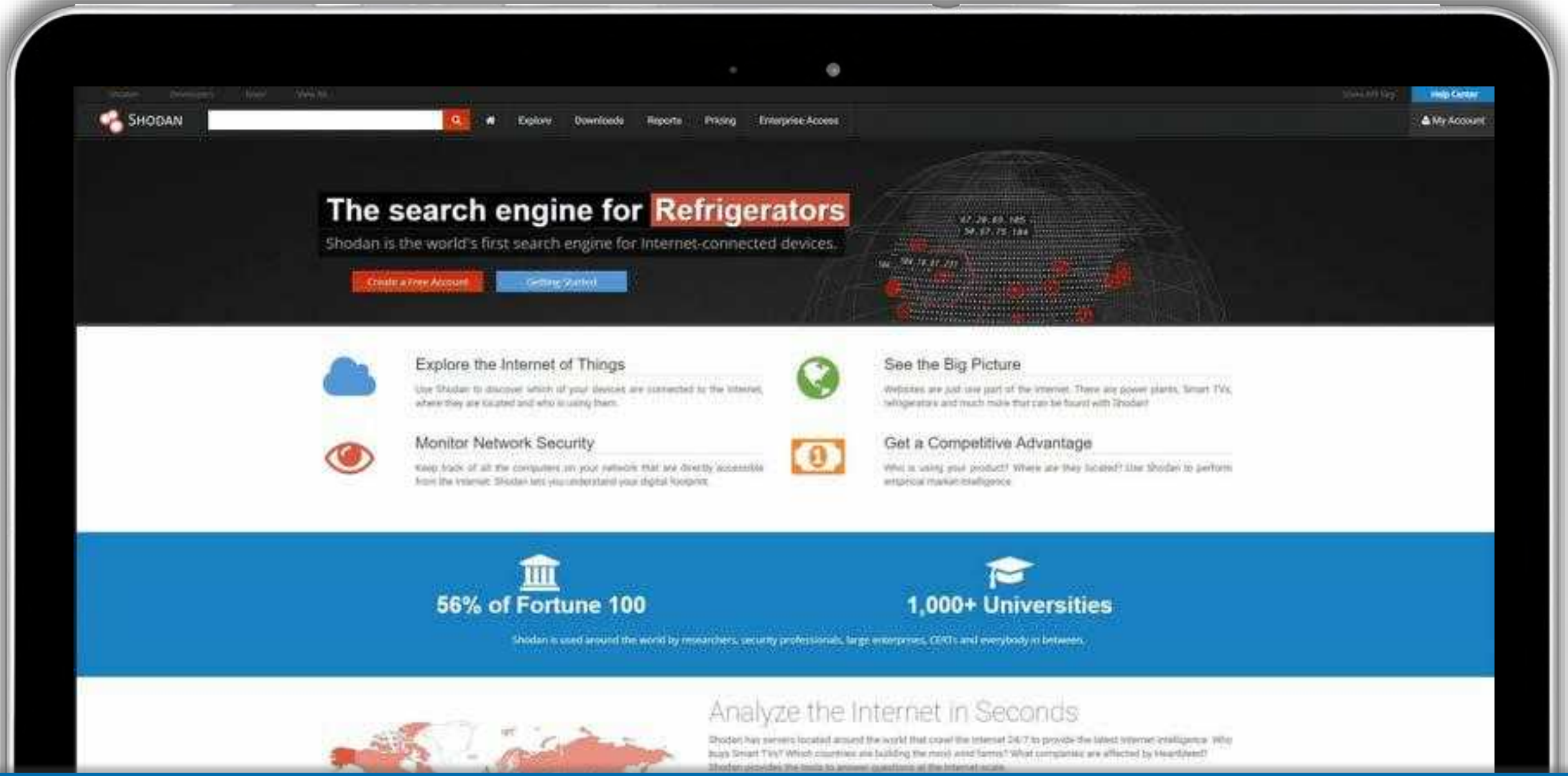
Responsible Disclosure Examples

telelink

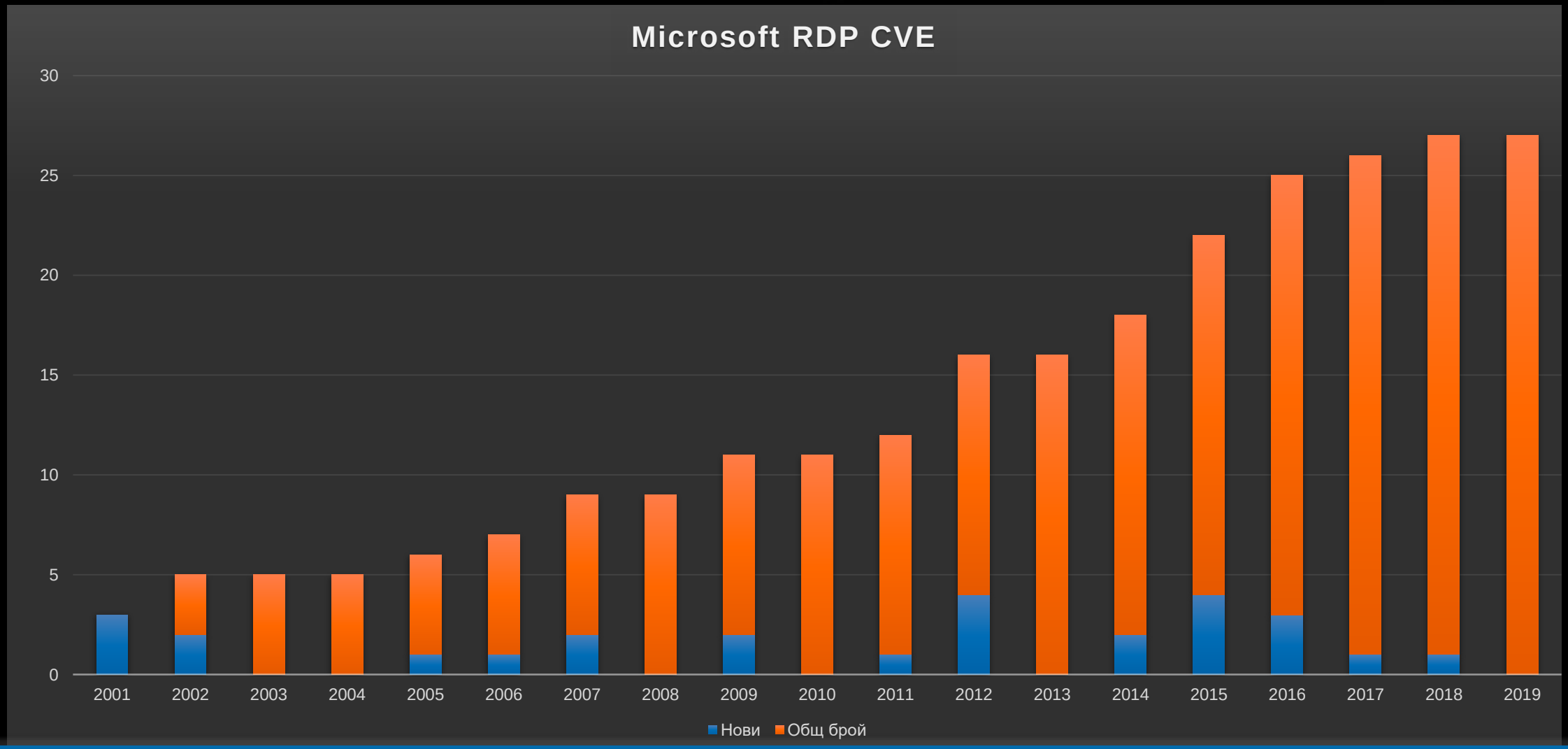
Image sources: Twitter

ASOC – Real Life Case Studies

telelink



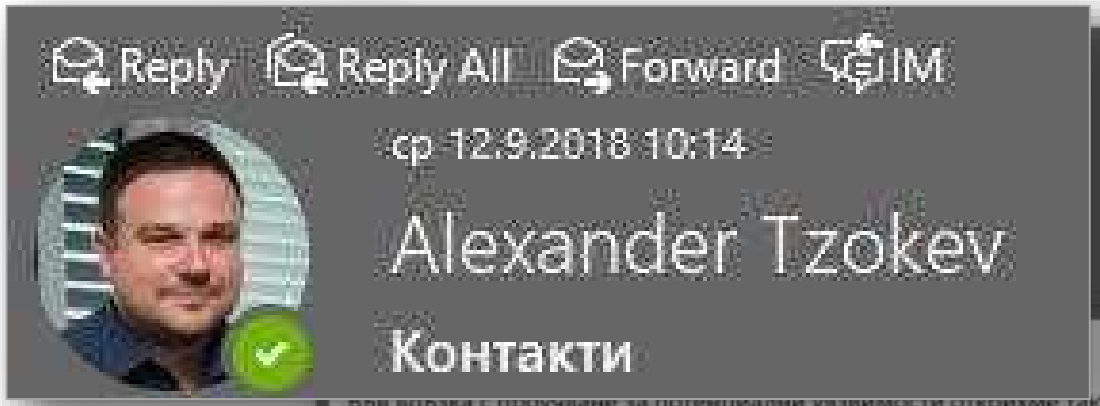
Shodan.io
Search for SCADA



Vulnerable SCADA

ASOC OSINT

The Vulnerable SCADA System



Искаме да се свържем с компанията, използваща посочения по-долу IP адрес и да ги информираме за проблемите, но нямаме контактна информация.

IP адресът е [redacted] и като доставчик е посочен "Vida optics TVV Ltd.".

Моля, да ни изпратите контакти или ако адресът не е към ваша AS да ни информирате.

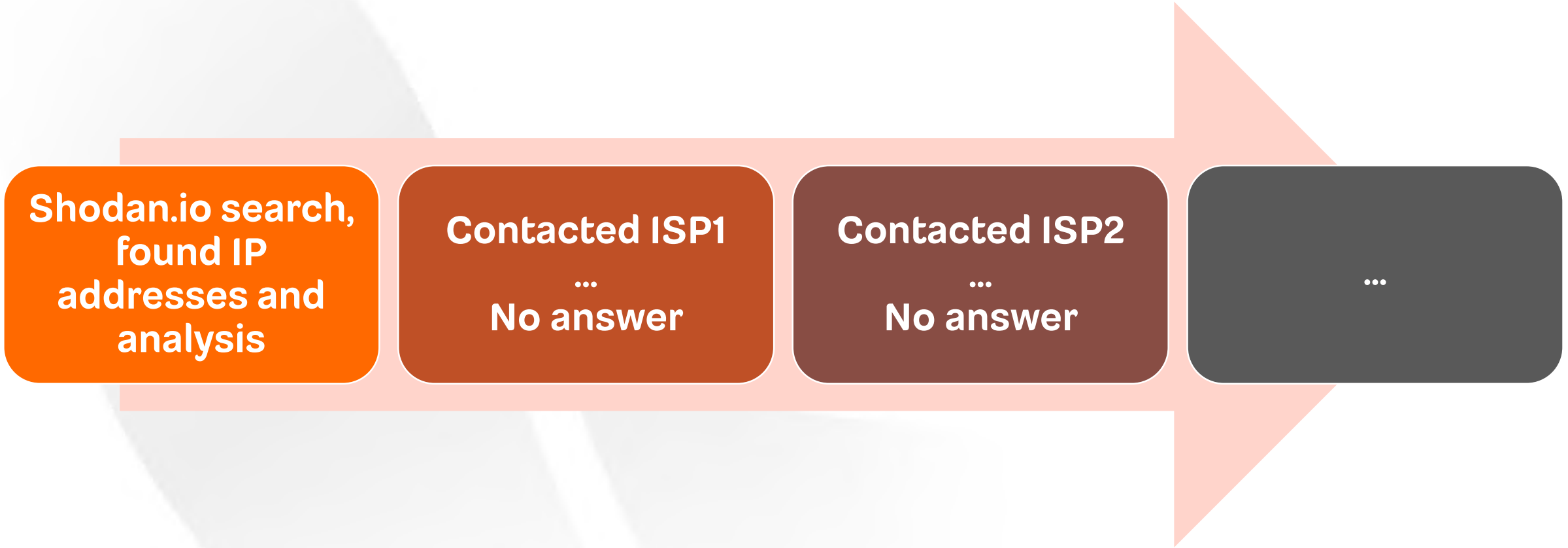
Предварително ви благодаря.

Alexander Tzokev | Department Manager - ASOC
Telelink Business Services | alexander.tzokev@telelink.com
M: +359 879 676 712 | www.telelink.com

telelink

telelink

The Vulnerable SCADA System



telelink

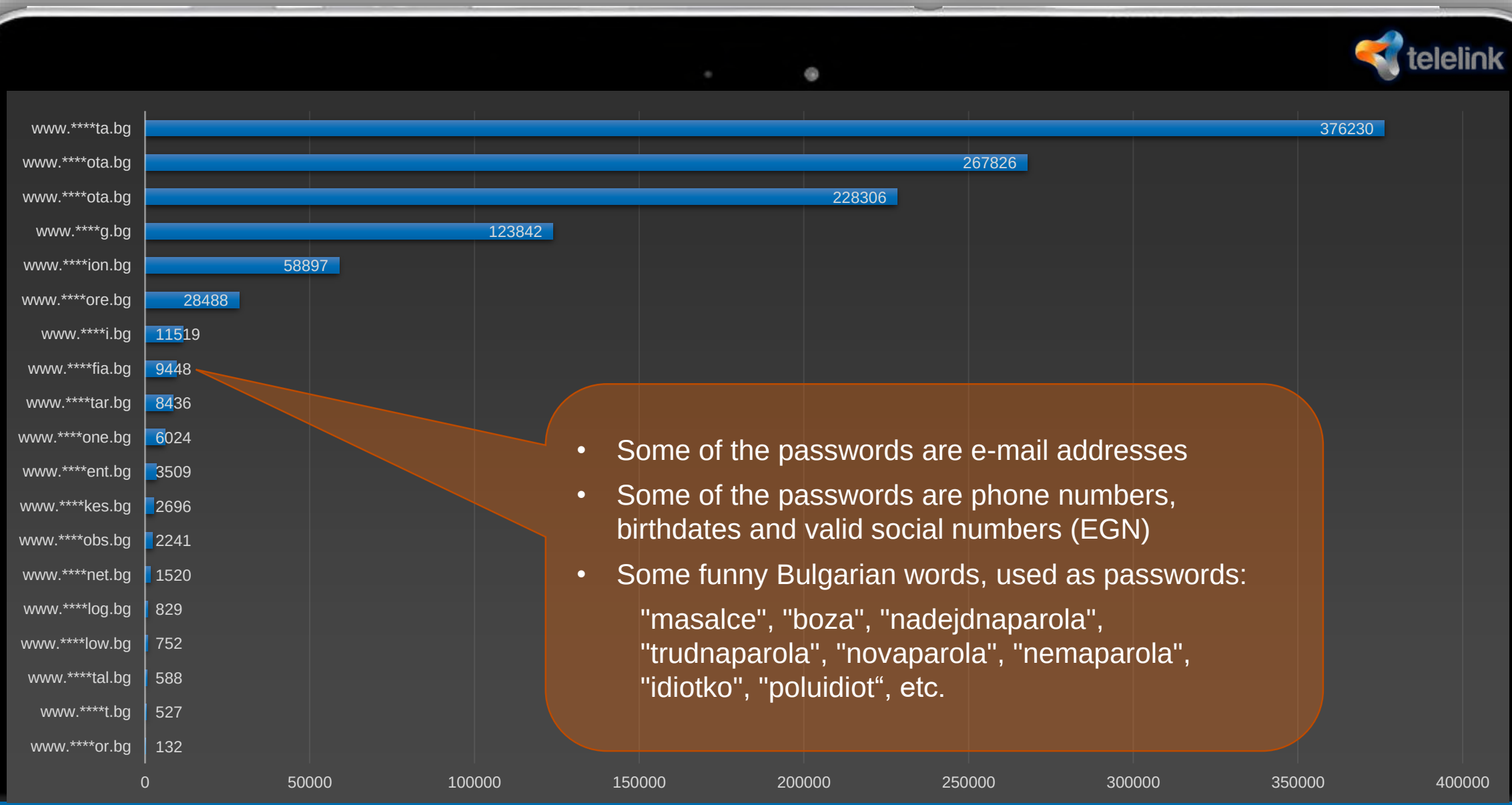
Encountered Problems

- Limited contact information
- No feedback

Collections #1-5

- 900+ GB archives, containing text files with leaked accounts (in most cases *email:password*)
- Passwords are in clear text and cryptographic hashes
- 6 000 000 000+ accounts
- 19 domains ending with ".bg" and congaing "-bg" in the name were found

Image source: Internet



Collections #2-5

Analysis of some of the Bulgarian sites

Collections #1-5

telelink

Encountered Problems

- Analyzing all the data
- Contacting Bulgarian companies and academical institution (owners of the leaked sites).
- Bipolar reactions were observed.

Lessons Learned

Contacting the cybersecurity targets (victims) is a complex task.

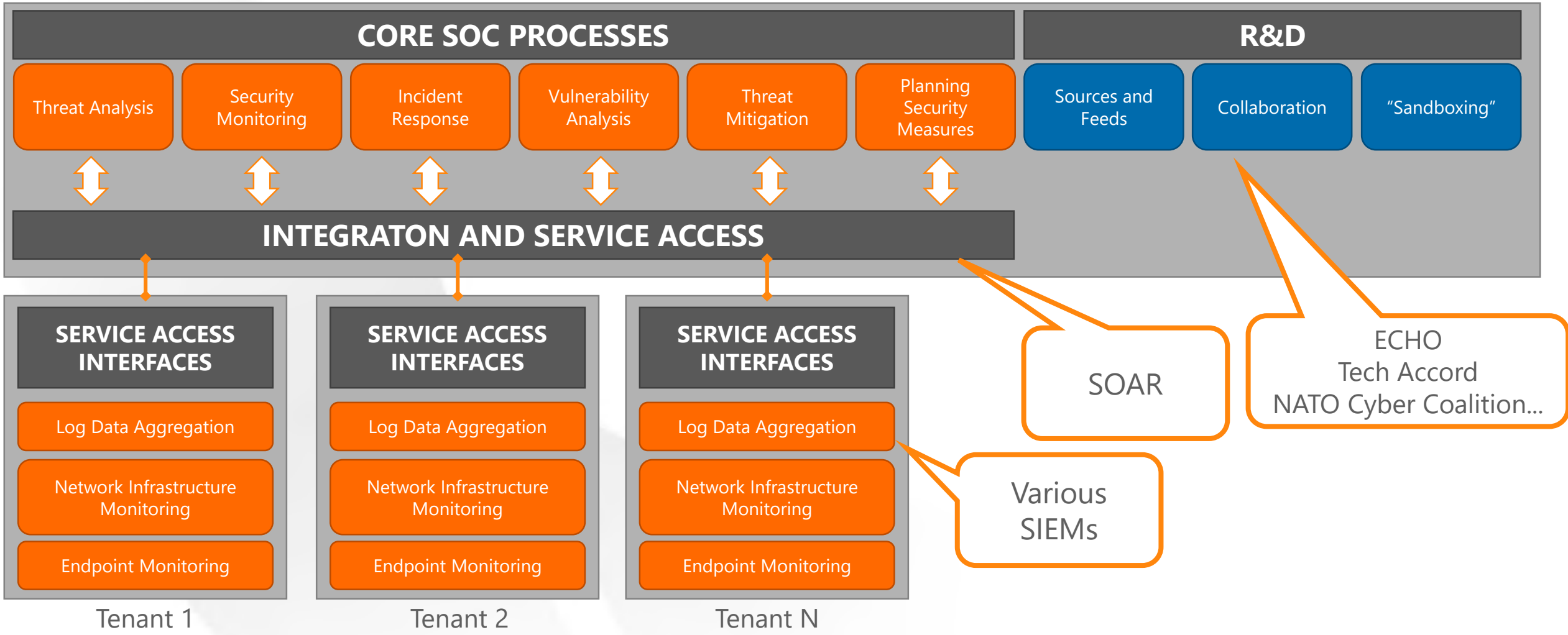
Image source: Internet

Telelink's ASOC and Information Sharing

Telelink Holistic Approach to Cybersecurity

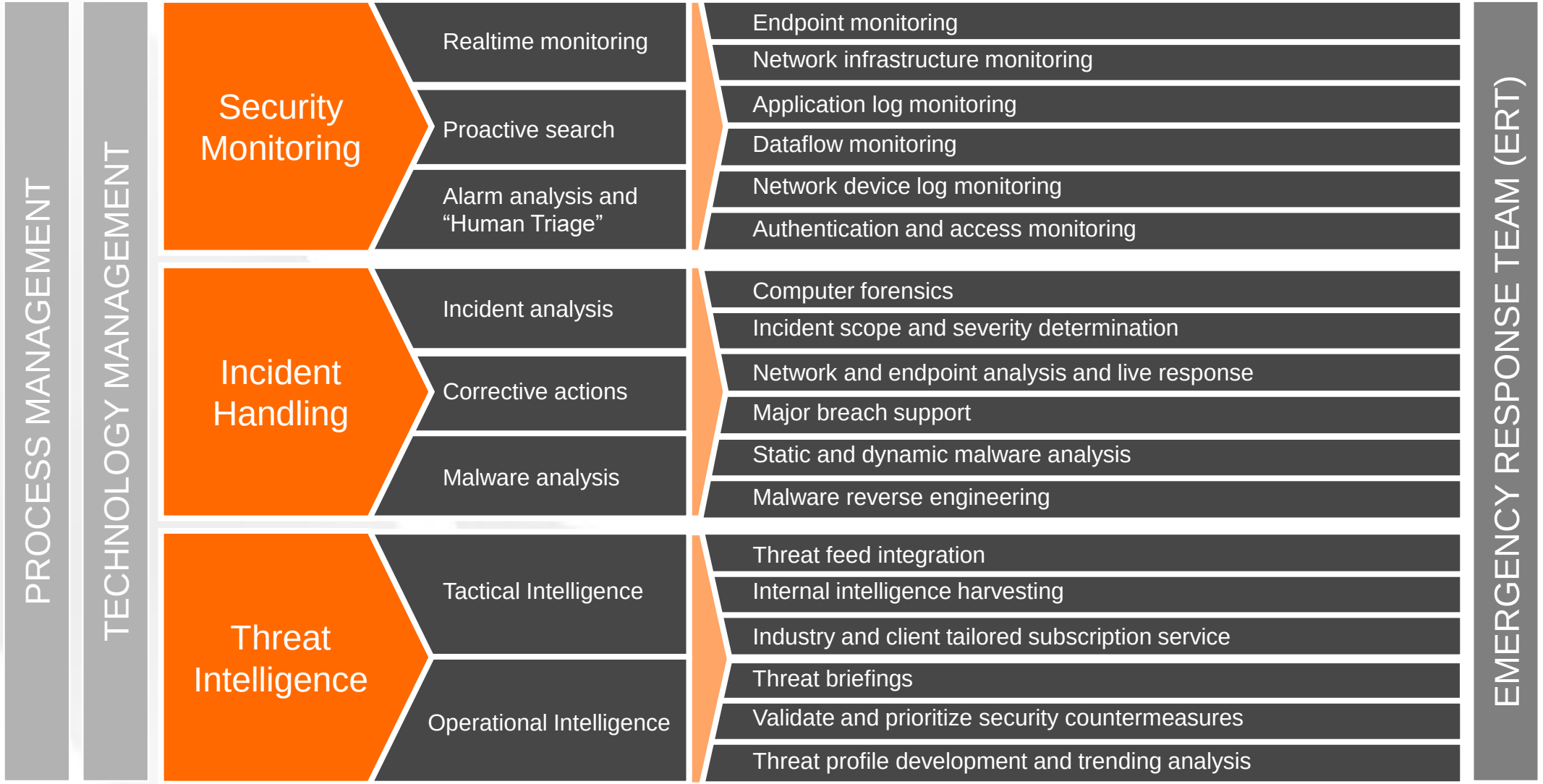
telelink

The ASOC Structure



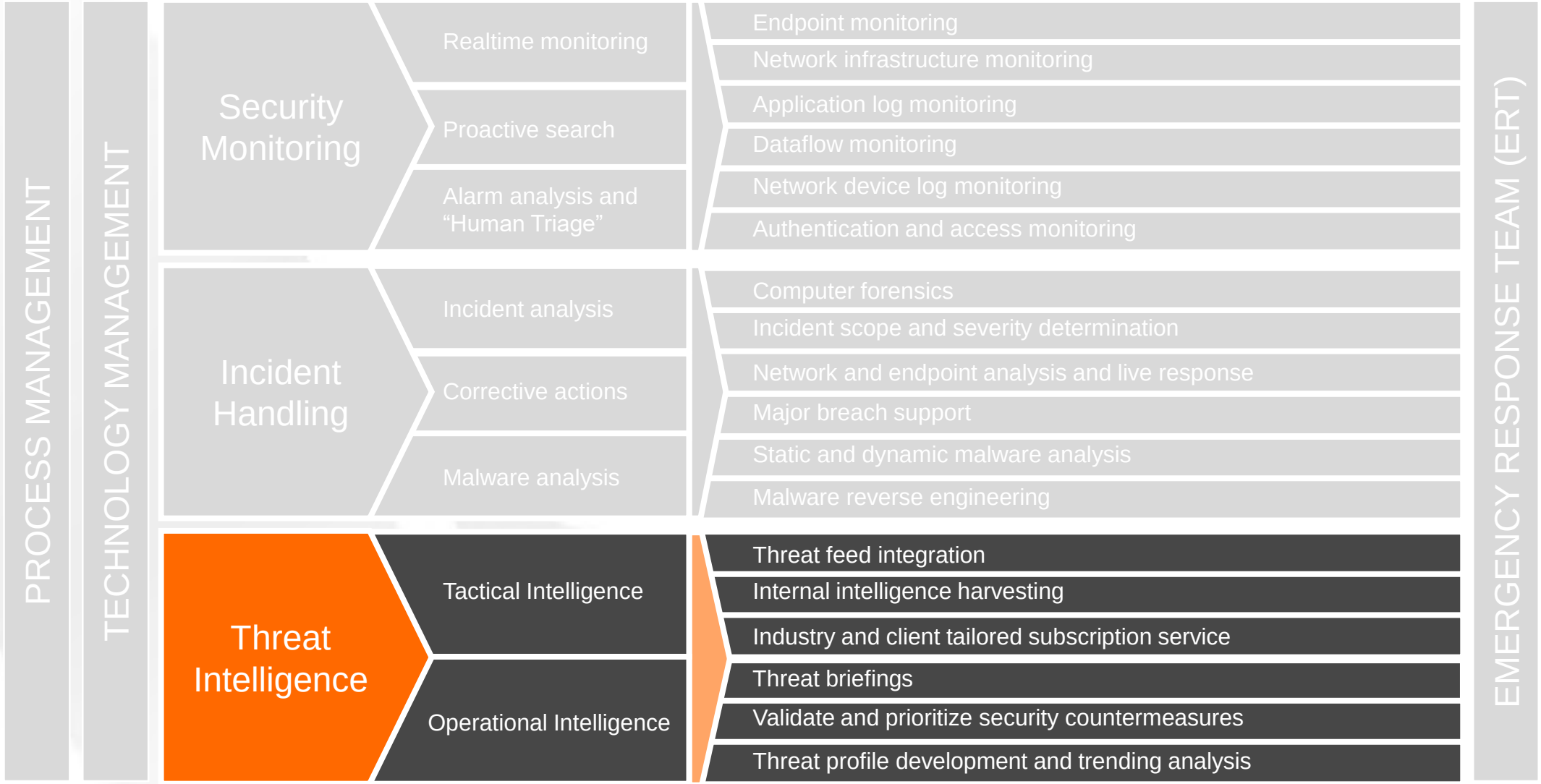
telelink

ASOC



telelink

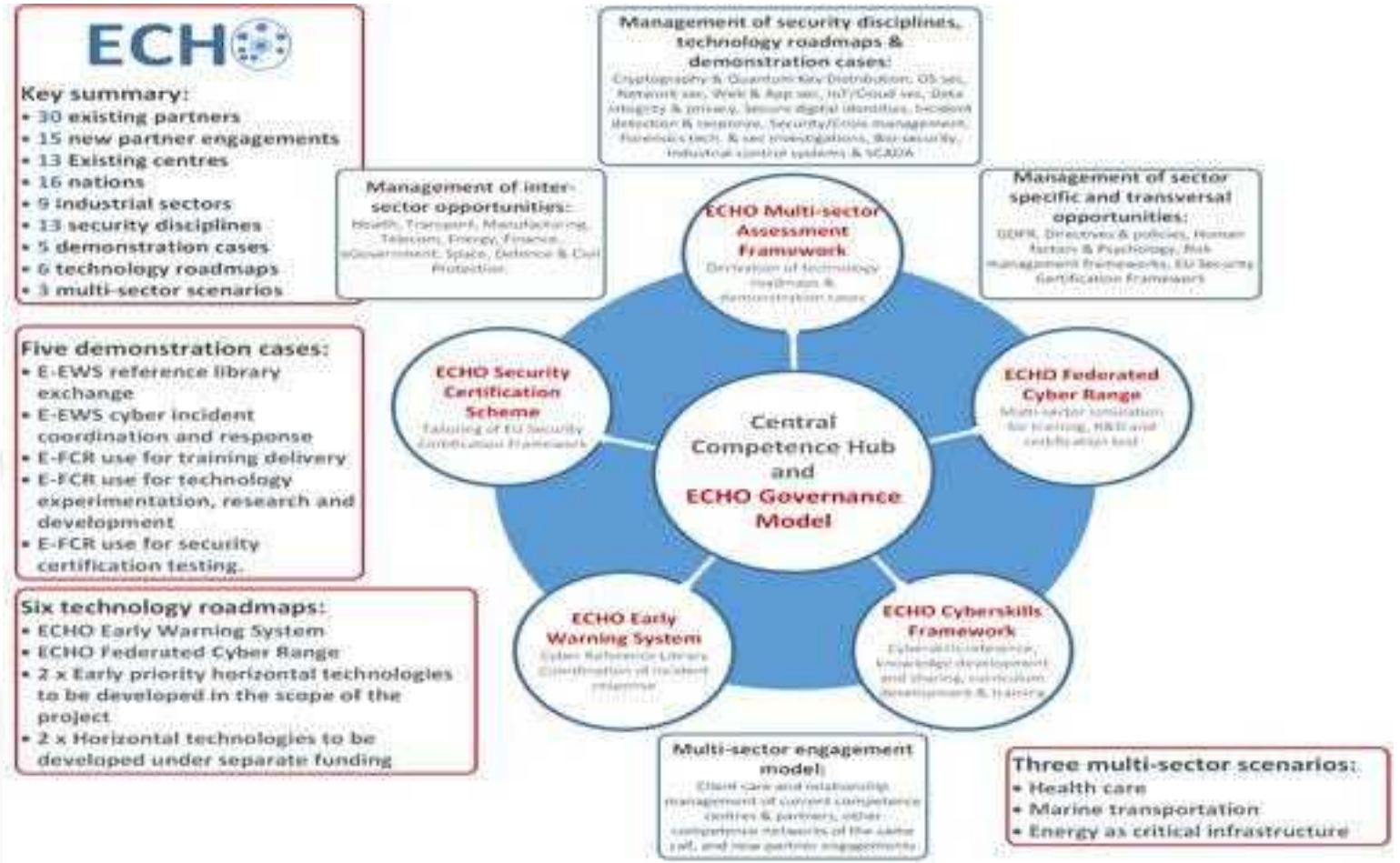
ASOC



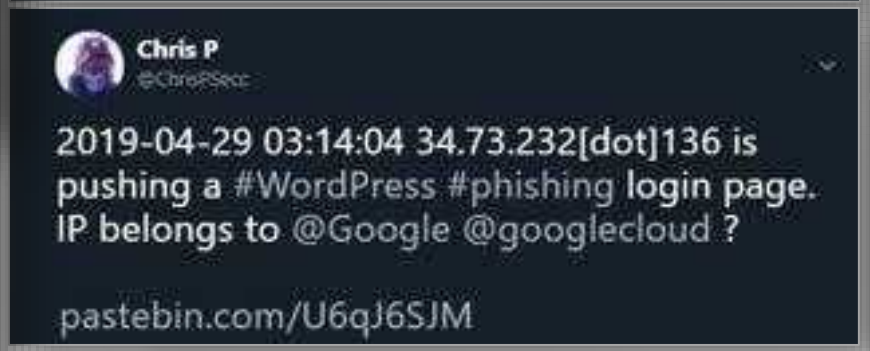
telelink

ECHO - EUROPEAN NETWORK OF CYBERSECURITY CENTERS AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

- Research and Development project, funded by EU, Part of Horizon2020
- Consortia consisting of 30 partners, including Royal Military Academy of Belgium, RHEA systems, Universities, Ship builders, etc…
- 48 months, started in February 2019



ASOC Information Sharing



telelink

Image sources: Twitter

Conclusions

Conclusions

- Security information sharing is still maturing.
- There are still some gray areas and risks around disclosing vulnerabilities.
- Security researches should seek out proper channels for disclosing vulnerabilities and share information.
- Companies need to develop their own disclosure policies.
- **There is much to be gained from sharing information.**
- **Sharing is caring.**

@TBS_Infosec

telelink

Thank you for your attention!

telelink