AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

enisa

7 TH eHEALTH SECURITY CONFERENCE

10 OCTOBER, 2022
RIGSHOSPITALET, COPENHAGEN, DENMARK

# Cybersecurity strategy and approach to face supply chain risks in public Healthcare

Albert Haro

## Agenda

01 **Public Health Care in Catalonia**

02 **Health cybersecurity strategy**

03 **Main risks and challenges**

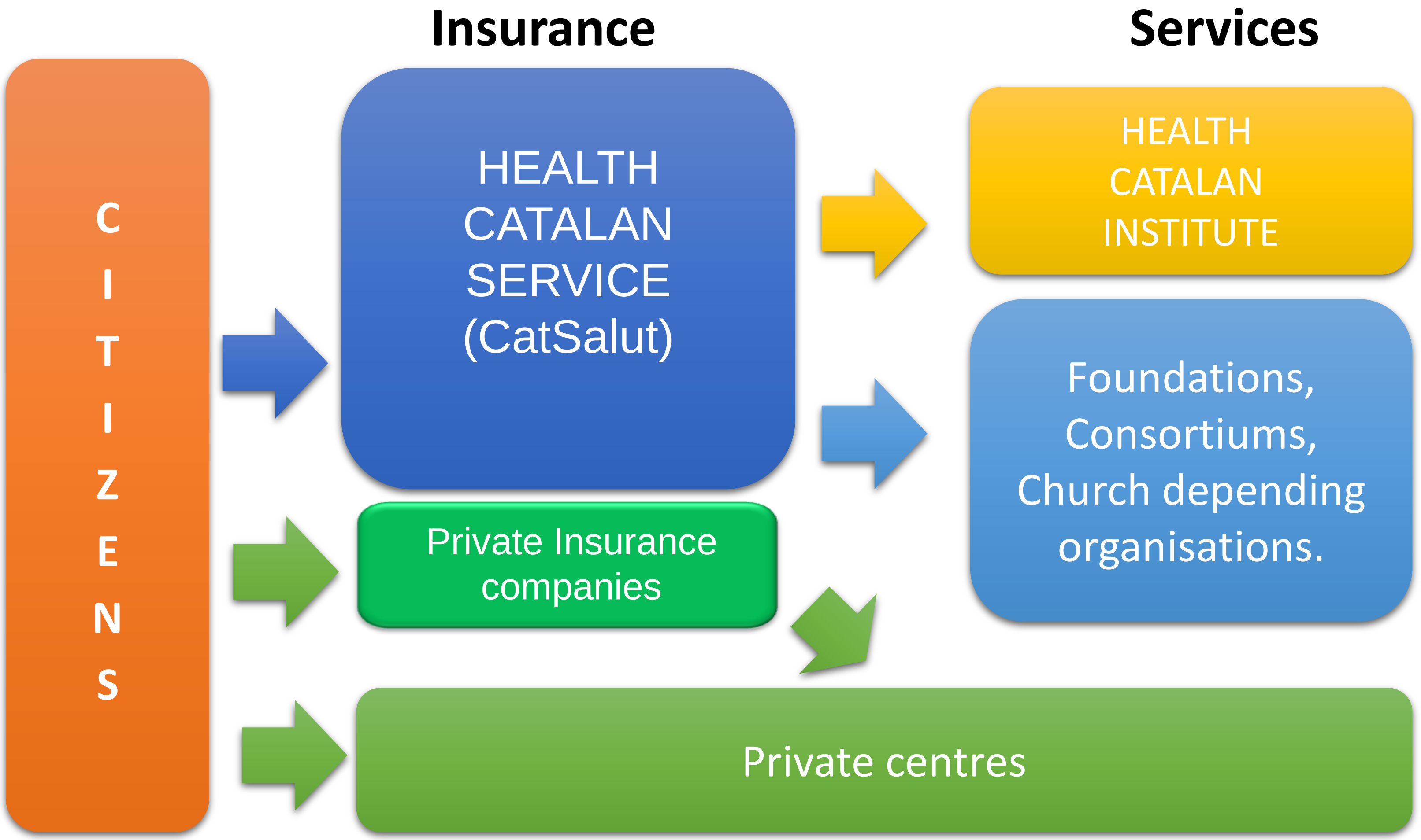
04 **Supply chain cyber incidents**

05 **Strategy and best practices**

06 **Main security controls**

07 **Incident Response**

# Health System in Catalonia



Insurance

Services

CITIZENS

HEALTH CATALAN SERVICE (CatSalut)

Private Insurance companies

HEALTH CATALAN INSTITUTE

Foundations, Consortiums, Church depending organisations.

Private centres

**Public Health System**

68 Hospitals
434 Primary Healthcare centres
102 Social-healthcare Centres
40 Mental Health centres
428 ambulances
+ 900 non urgent transport
900 small facilities
100.000 Professionals

**Private Health System**

136 Clinics and Hospitals

## Highlights of the cybersecurity strategy

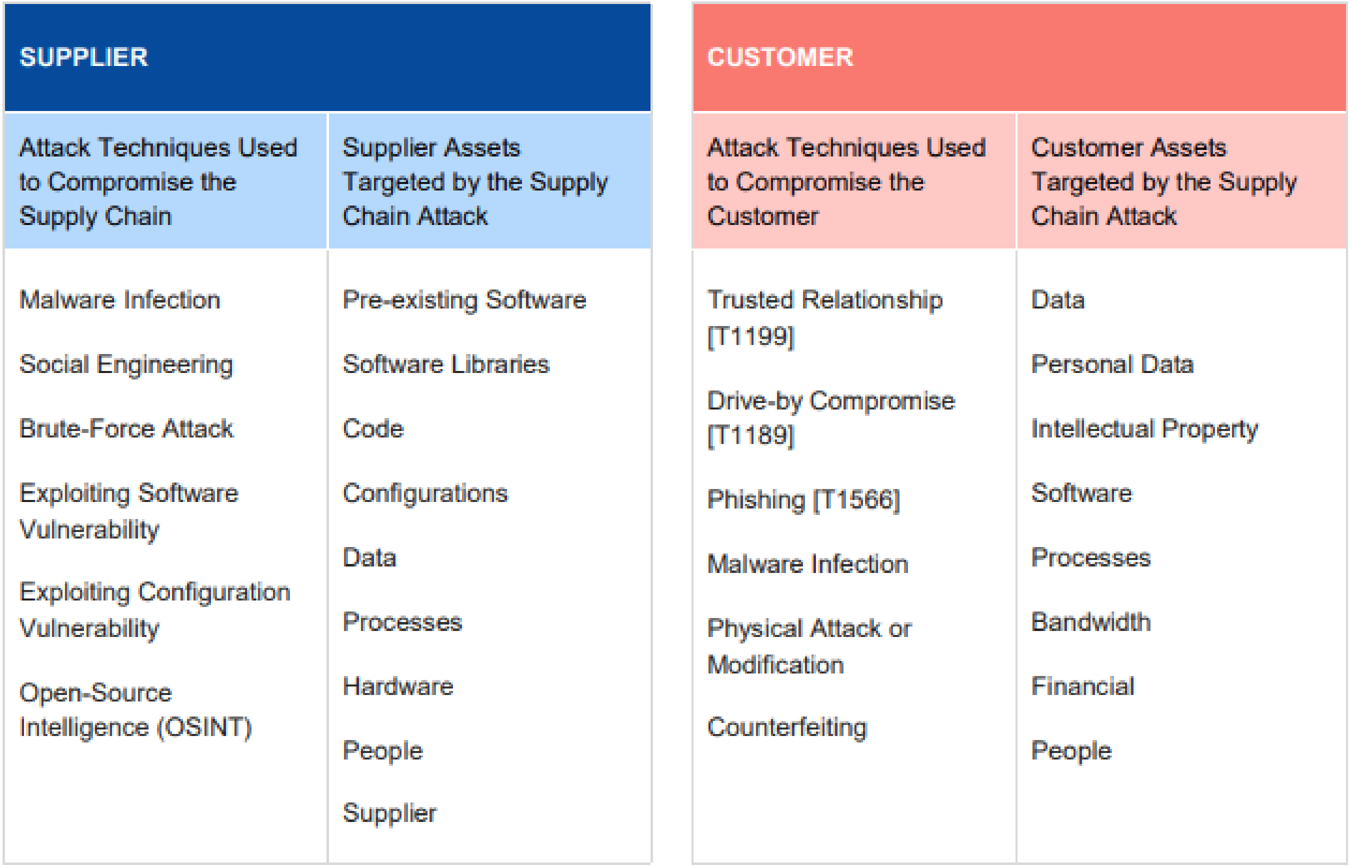
- ❑ Establishment of a Health Cybersecurity common model
- ❑ Make of the Health key Information systems a reference model (Primary Care Clinic, Shared Clinical History in Catalonia, Health Services Integrator IS3, Integrated Electronic Prescription System)
- ❑ Deployment of a cybersecurity governance model
- ❑ Health SOC and Health CERT supported by the CATALONIA-SOC and the CATALONIA-CERT®
  - ❑ Warning and alerts
  - ❑ Handling vulnerabilities
  - ❑ Incident response
- ❑ Progressive deployment of a cybersecurity perimeter
- ❑ Adapting the cybersecurity regulatory framework to the reality of the Public Health System
- ❑ Awareness-raising and capacity building program
- ❑ Training and IR exercises

# Supply chain management risks and challenges

## Cyber Supply Chain Security Principles (from NIST Best practices):

1. Develop your defenses based on the principle that your systems will be breached.
2. Cybersecurity is never just a technology problem, it’s a people, processes and knowledge problem.
3. Security is Security. There should be no gap between physical and cybersecurity.

## Proposed taxonomy for supply chain attacks
(ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS July 2021)



| SUPPLIER | | CUSTOMER | |
|---|---|---|---|
| Attack Techniques Used to Compromise the Supply Chain | Supplier Assets Targeted by the Supply Chain Attack | Attack Techniques Used to Compromise the Customer | Customer Assets Targeted by the Supply Chain Attack |
| Malware Infection<br>Social Engineering<br>Brute-Force Attack<br>Exploiting Software Vulnerability<br>Exploiting Configuration Vulnerability<br>Open-Source Intelligence (OSINT) | Pre-existing Software<br>Software Libraries<br>Code<br>Configurations<br>Data<br>Processes<br>Hardware<br>People<br>Supplier | Trusted Relationship [T1199]<br>Drive-by Compromise [T1189]<br>Phishing [T1566]<br>Malware Infection<br>Physical Attack or Modification<br>Counterfeiting | Data<br>Personal Data<br>Intellectual Property<br>Software<br>Processes<br>Bandwidth<br>Financial<br>People |

# Supply chain cyberincidents

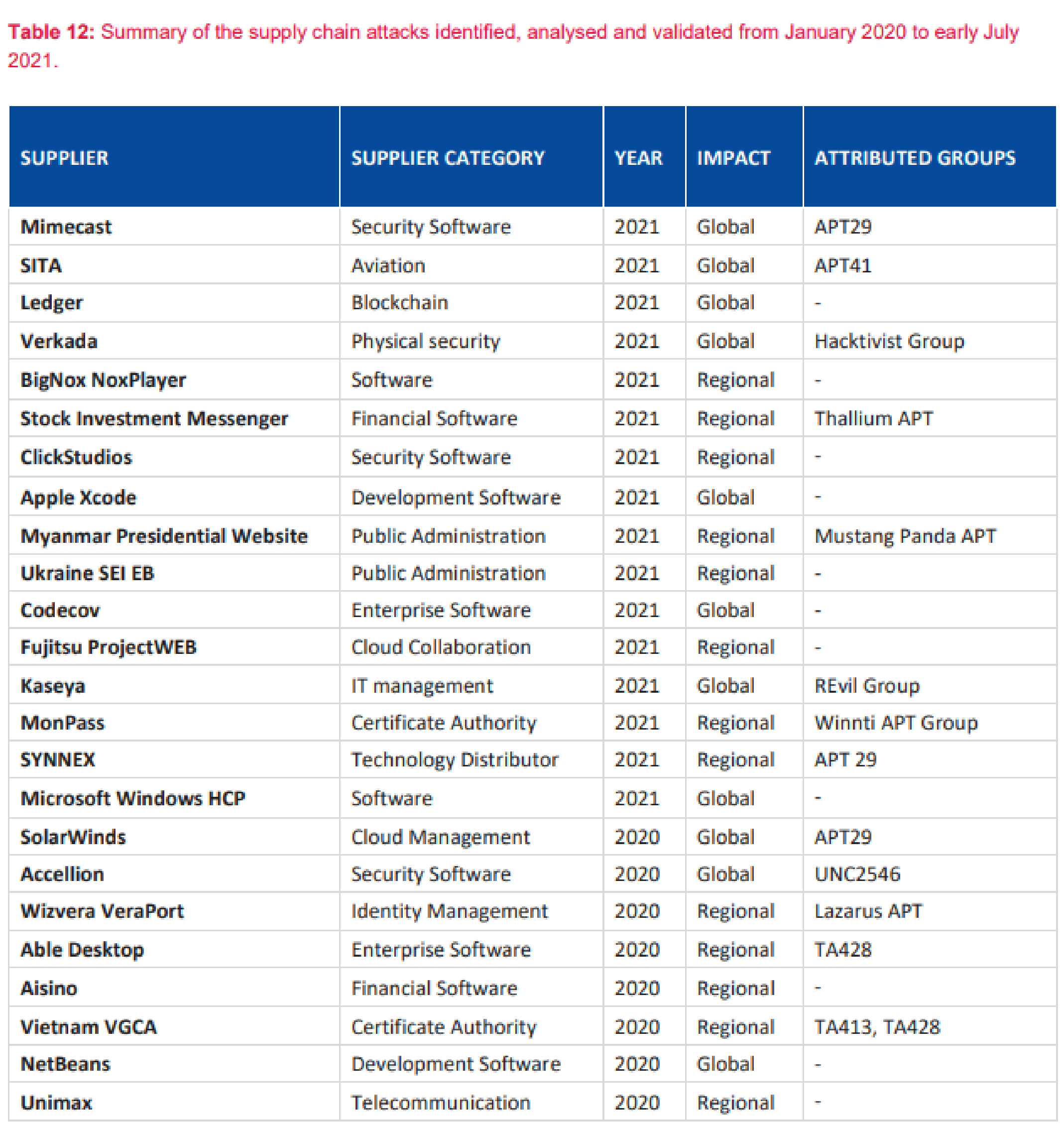
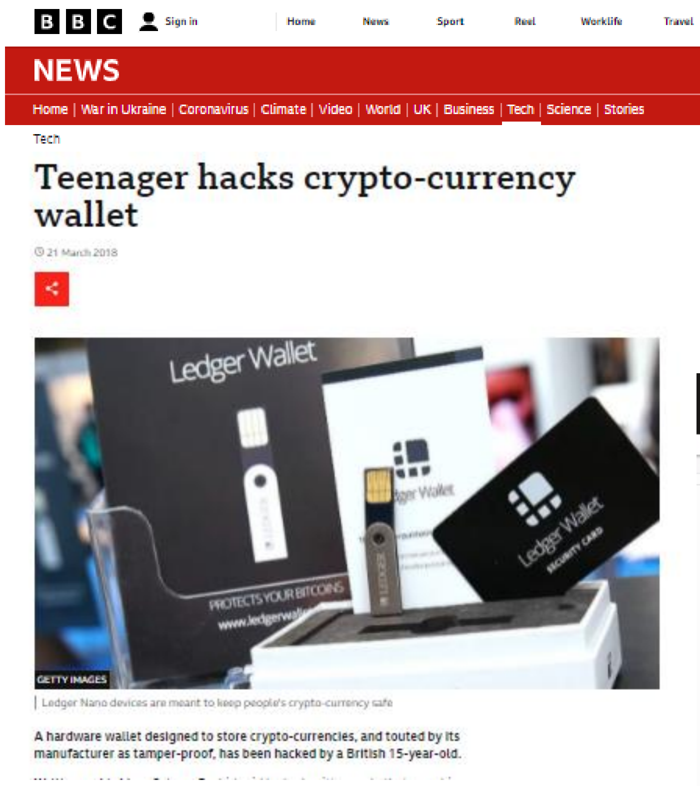


**Table 12:** Summary of the supply chain attacks identified, analysed and validated from January 2020 to early July 2021.

| SUPPLIER | SUPPLIER CATEGORY | YEAR | IMPACT | ATTRIBUTED GROUPS |
|---|---|---|---|---|
| **Mimecast** | Security Software | 2021 | Global | APT29 |
| **SITA** | Aviation | 2021 | Global | APT41 |
| **Ledger** | Blockchain | 2021 | Global | - |
| **Verkada** | Physical security | 2021 | Global | Hacktivist Group |
| **BigNox NoxPlayer** | Software | 2021 | Regional | - |
| **Stock Investment Messenger** | Financial Software | 2021 | Regional | Thallium APT |
| **ClickStudios** | Security Software | 2021 | Regional | - |
| **Apple Xcode** | Development Software | 2021 | Global | - |
| **Myanmar Presidential Website** | Public Administration | 2021 | Regional | Mustang Panda APT |
| **Ukraine SEI EB** | Public Administration | 2021 | Regional | - |
| **Codecov** | Enterprise Software | 2021 | Global | - |
| **Fujitsu ProjectWEB** | Cloud Collaboration | 2021 | Regional | - |
| **Kaseya** | IT management | 2021 | Global | REvil Group |
| **MonPass** | Certificate Authority | 2021 | Regional | Winnti APT Group |
| **SYNNEX** | Technology Distributor | 2021 | Regional | APT 29 |
| **Microsoft Windows HCP** | Software | 2021 | Global | - |
| **SolarWinds** | Cloud Management | 2020 | Global | APT29 |
| **Accellion** | Security Software | 2020 | Global | UNC2546 |
| **Wizvera VeraPort** | Identity Management | 2020 | Regional | Lazarus APT |
| **Able Desktop** | Enterprise Software | 2020 | Regional | TA428 |
| **Aisino** | Financial Software | 2020 | Regional | - |
| **Vietnam VGCA** | Certificate Authority | 2020 | Regional | TA413, TA428 |
| **NetBeans** | Development Software | 2020 | Global | - |
| **Unimax** | Telecommunication | 2020 | Regional | - |

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

July 2021


BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
NEWS
Home | War in Ukraine | Coronavirus | Climate | Video | World | UK | Business | Tech | Science | Stories
Tech
Ledger Wallet
PROTECTS YOUR BITCOINS
GETTY IMAGES

## Teenager hacks crypto-currency wallet

21 March 2018

Ledger Nano devices are meant to keep people's crypto-currency safe

A hardware wallet designed to store crypto-currencies, and touted by its manufacturer as tamper-proof, has been hacked by a British 15-year-old.

OPINION

## Why Was SolarWinds So Vulnerable to a Hack?

It's the economy, stupid.

Feb. 23, 2021

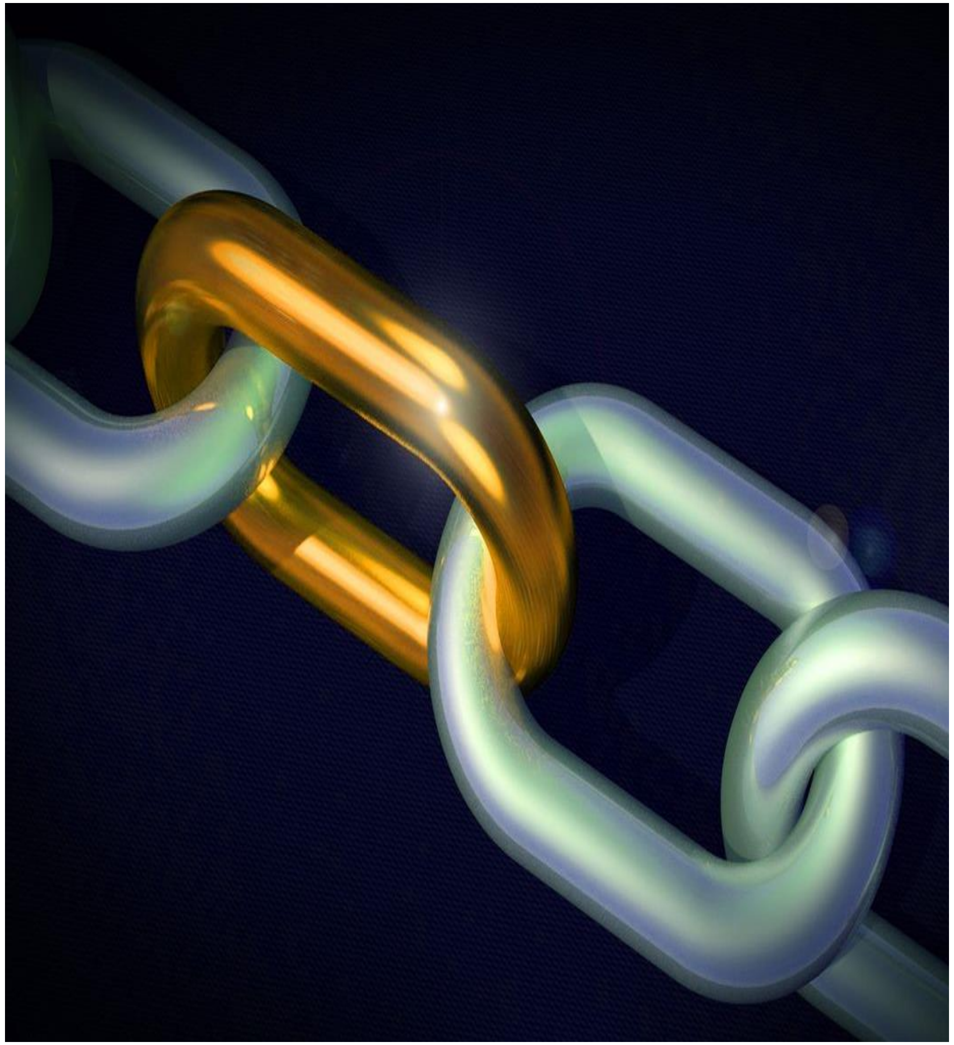
INNOVATION

## The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks

**Ondrej Krehel** Forbes Councils Member
**Forbes Technology Council** COUNCIL POST | Membership (Fee-Based)

Jan 25, 2022, 08:45am EST

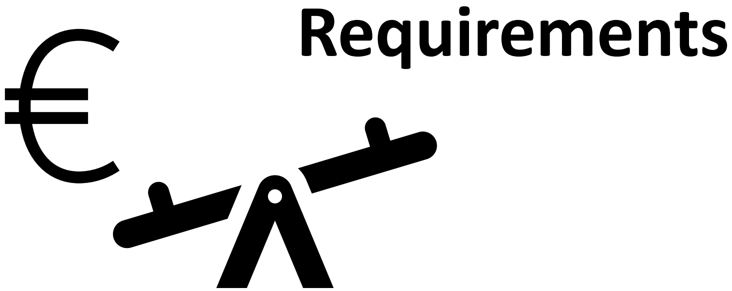
# Supply chain management strategy and best practices



❑ Supplier management based on risk analysis

**Low → High Risk**

❑ Requirements proportional risk assessment



❑ Establishment of monitoring activities during the contract

❑ Define beforehand the return process

# Main security controls

- ❑Backup, BCP/DRP (including off-line copy)
- ❑Patch and harden systems
  - ❑ Prioritize high impact, actively exploited vulnerabilities
- ❑Implement MFA (at least for privileged users and remote access solutions)
- ❑Penetration testing, vulnerability scanning
  - ❑ Establish SLAs for vulnerability management
- ❑Inventory of hardware and software, vulnerabilities, hardening measures. Including the assets that will be accessible by the supplier
- ❑Use of Privileged Access Management (PAM) solutions
- ❑Certify that cybersecurity audits include
  - ❑ Principle of least privilege
  - ❑ Controlled physical access
  - ❑ Remote access to corporate network
- ❑Establishment of mechanisms for notification and incident management

# Incident Response

- Preparation—Identification of suppliers and risk assessment. Identification of sensitive assets, define which are critical security incidents. Monitoring.
- Identification—monitor IT systems to detect deviations from normal operations. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
- Containment—perform short-term containment. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
- Eradication—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
- Recovery—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
- Lessons learned

**Thank you for your attention,**

***aharo@ciberseguretat.cat***