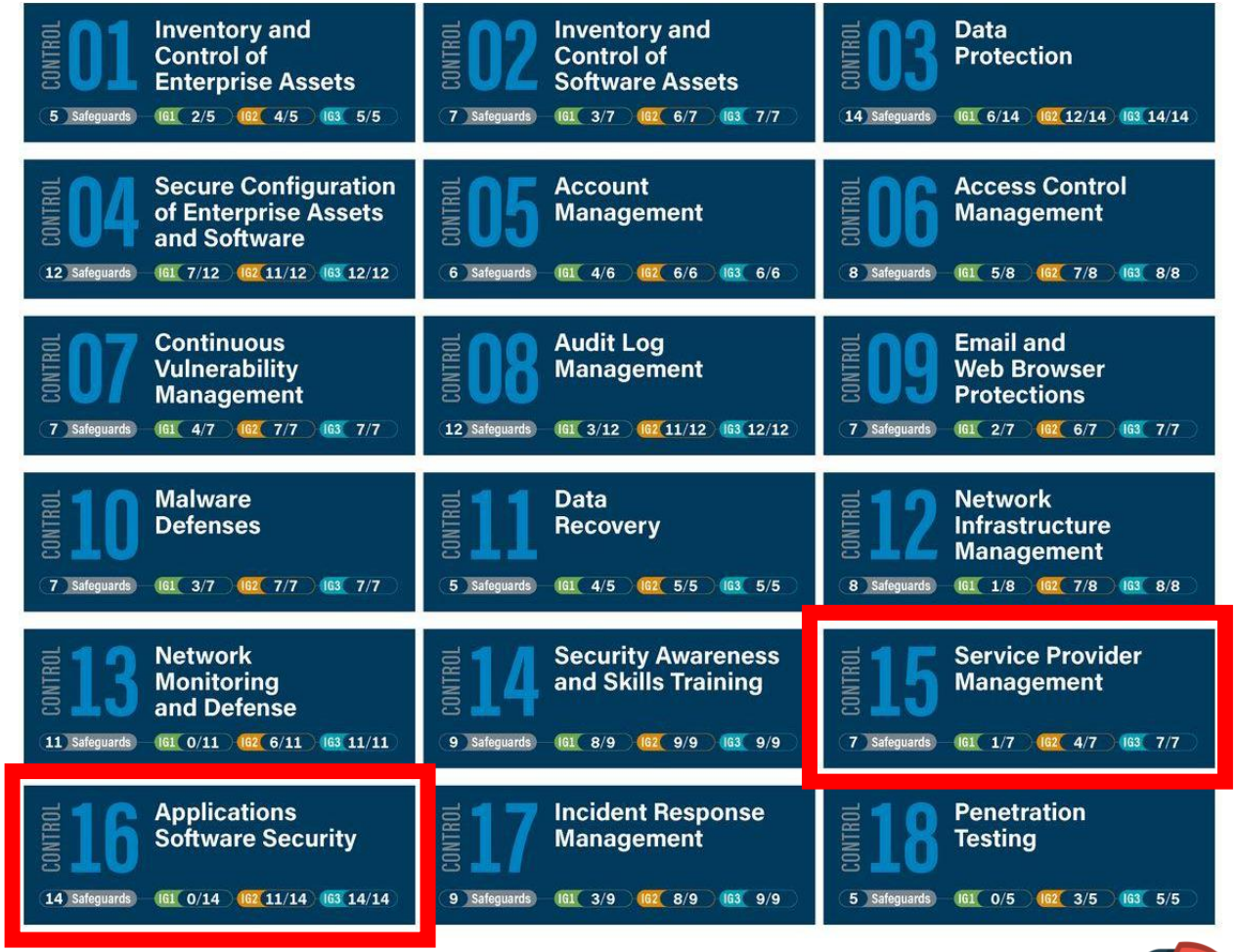
Supply chain in cyber security management

Grega Prešeren, CTO

CARBONSEC
CYBERSECURE YOUR BUSINESS

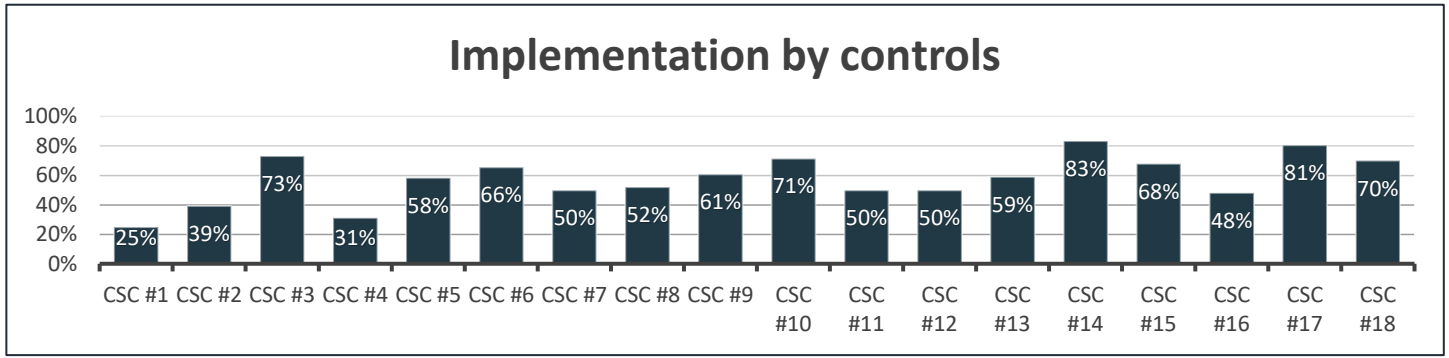
Cyber security management frameworks

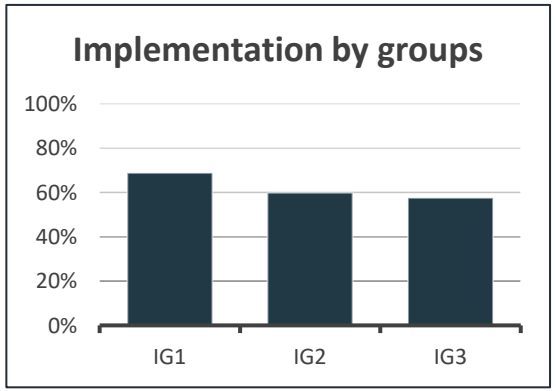
Source: NIST

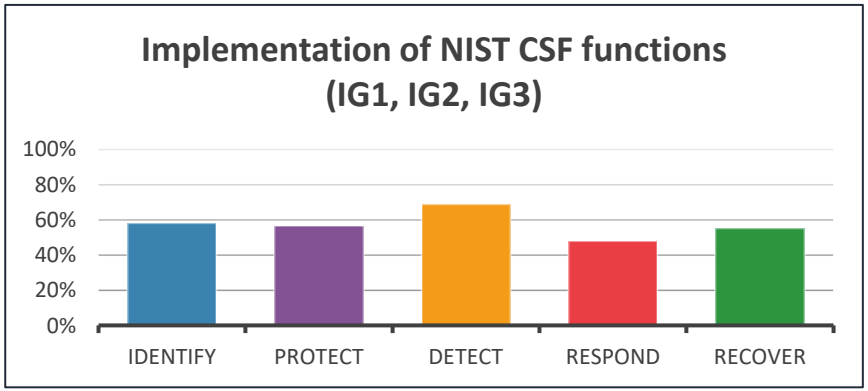

CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5
CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7
CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12
CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6
CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7
CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12
CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7
CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5
CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14
CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9
CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

Source: CIS

Cybersecurity Strategy







CARBONSEC


Supply chain
Technology
Employees

Regulations

NIS 2

- Article 7
  - National cybersecurity strategy
    - 2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:
      - (a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

NIS 2

- Article 21
  - Cybersecurity risk-management measures
    - 2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:
      - (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
    - 3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

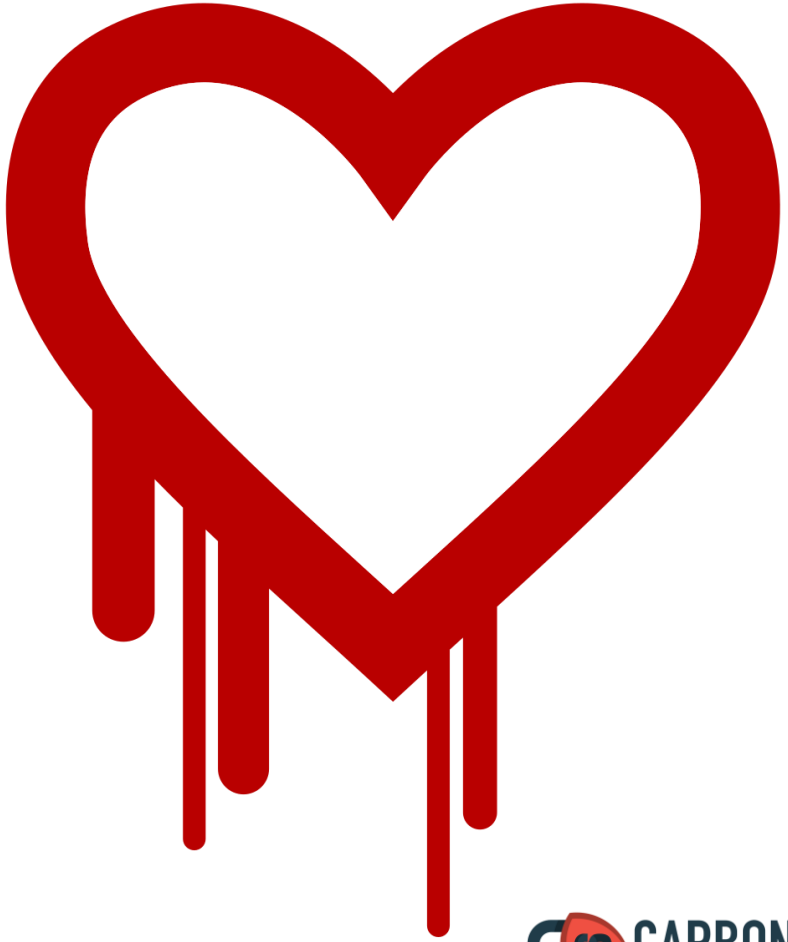
CRA

- The Regulation is expected to enter into force in early 2024. Manufacturers will have to apply the rules 36 months after their entry into force. The Commission will then periodically review the Act and report on its functioning.

Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

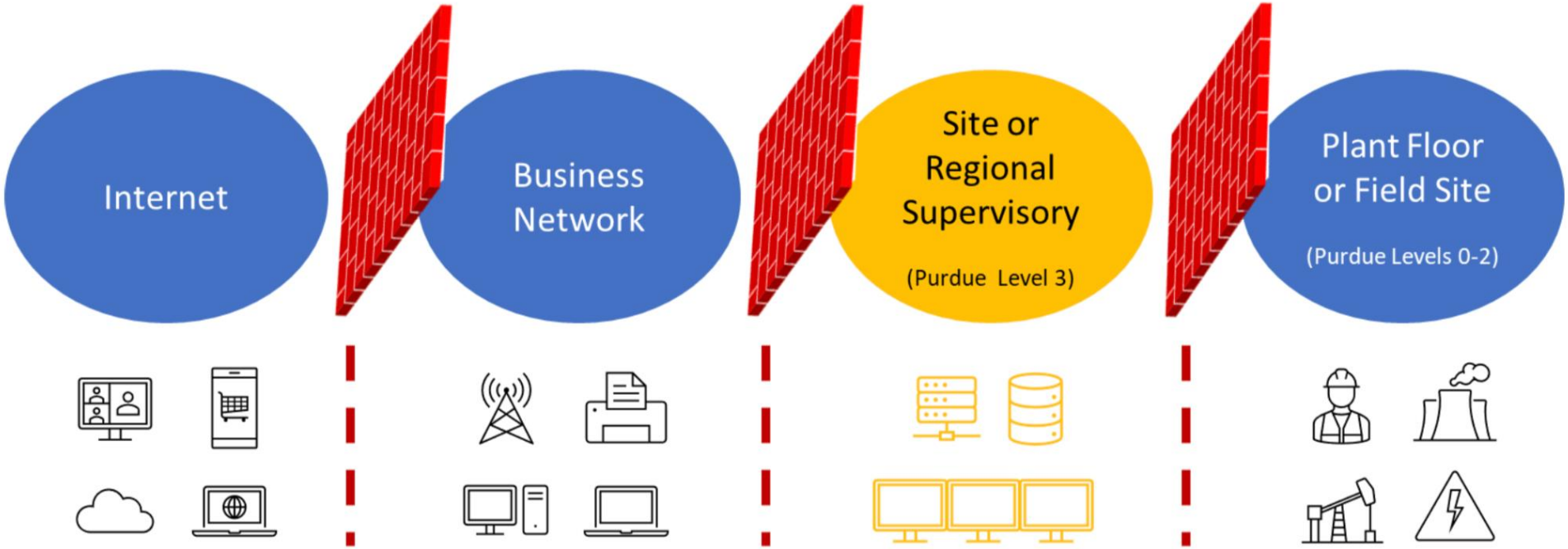
CARBONSEC

1 April 2014



solarwinds

KALI


Internet
Business Network
Site or Regional Supervisory
(Purdue Level 3)
Plant Floor or Field Site
(Purdue Levels 0-2)

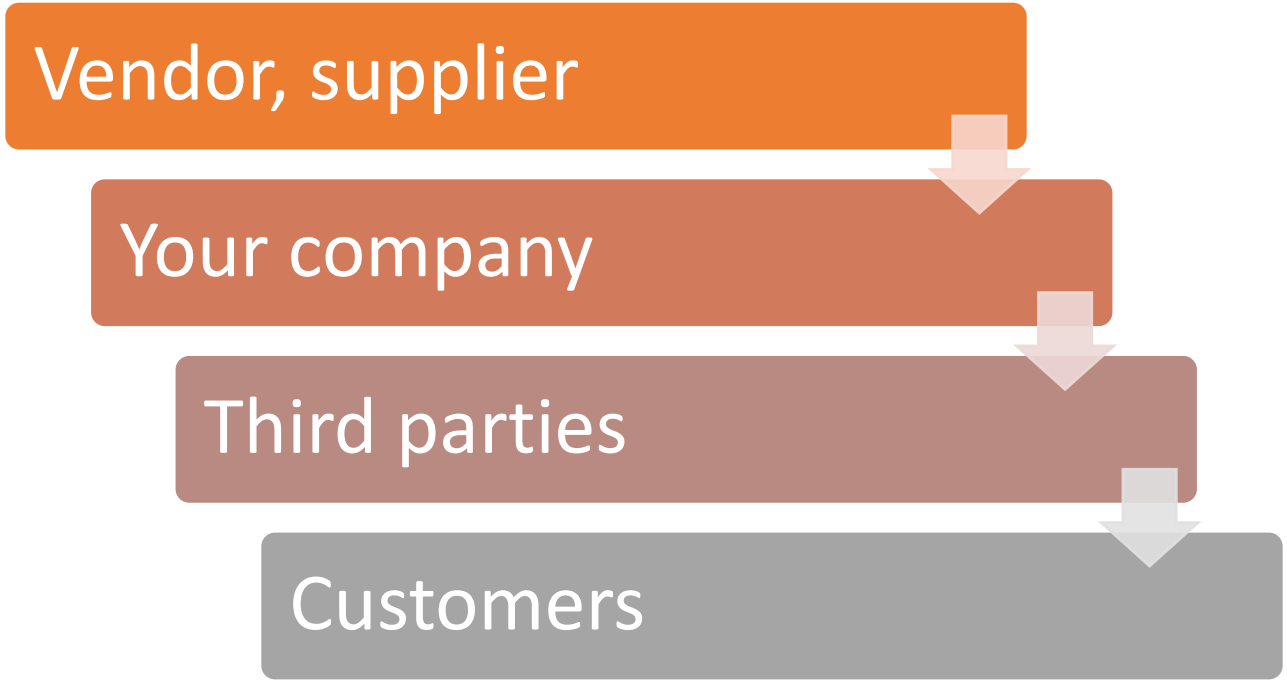
Source: SANS


PUMA

New acronyms

- TPRM - Third-Party Risk Management
- VRA – Vendor Risk Assessment
- VRM – Vendor Risk Management
- SCRM - Supply Chain Risk Management
- Etc.

Supply chain definition(s)

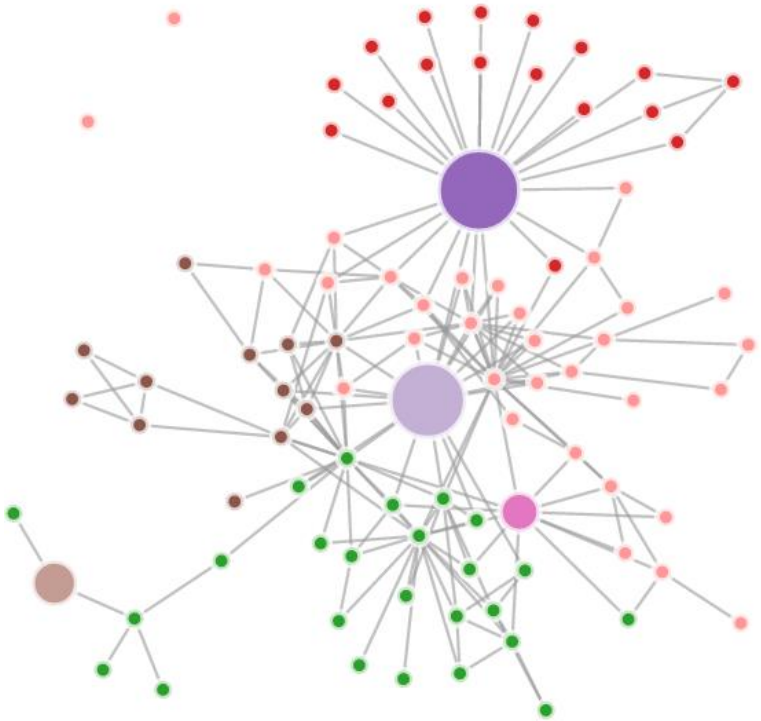


Supply chain dissected

- Code suppliers
- Software suppliers
- Cloud services
- Contractors (and subcontractors)
- ...

- Our definition
  - Everyone who is not your employee and works for you
  - Everything produced by others and used by you
  - Everything outside of your inventory and connected to your network

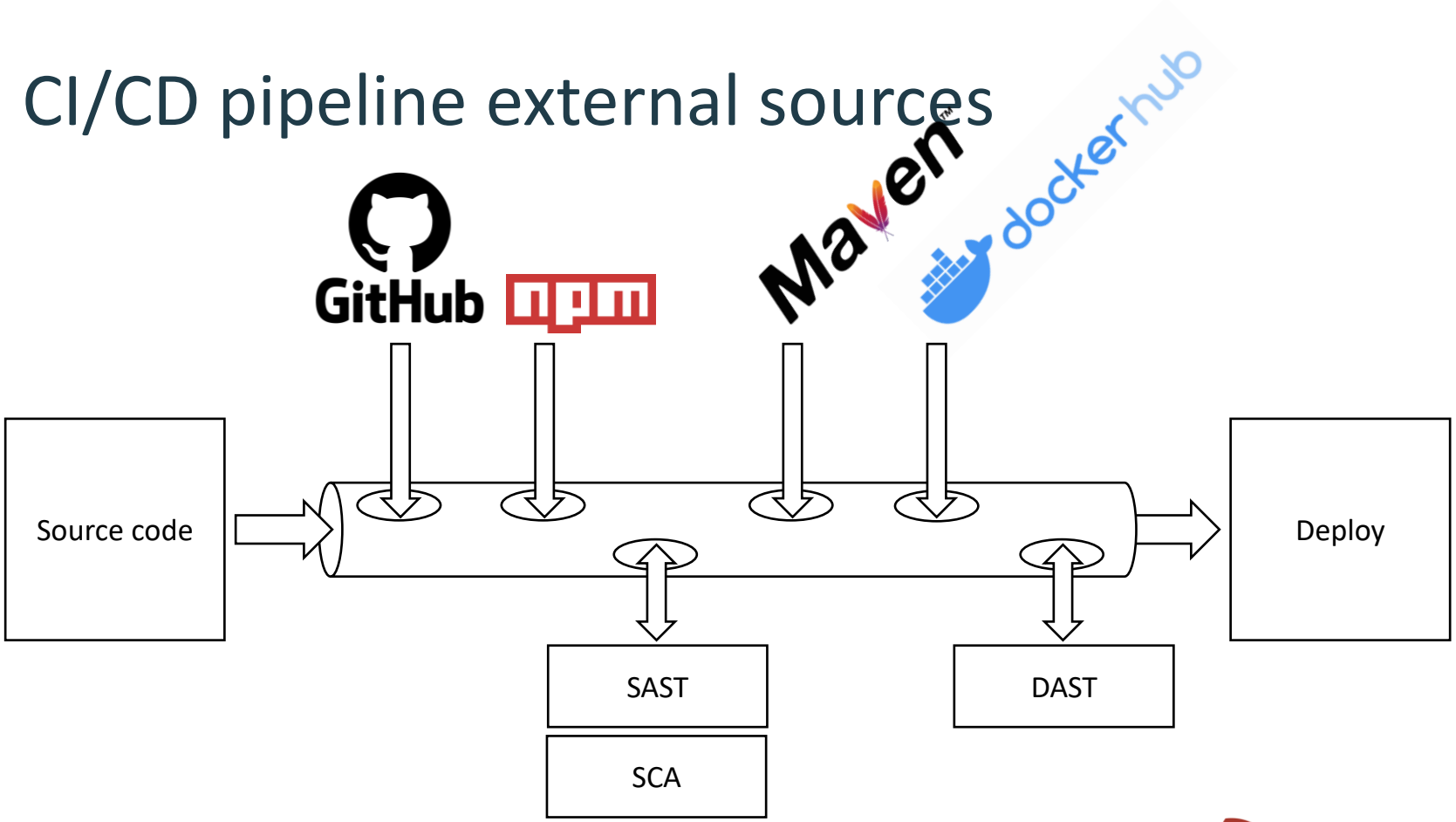
Nth parties



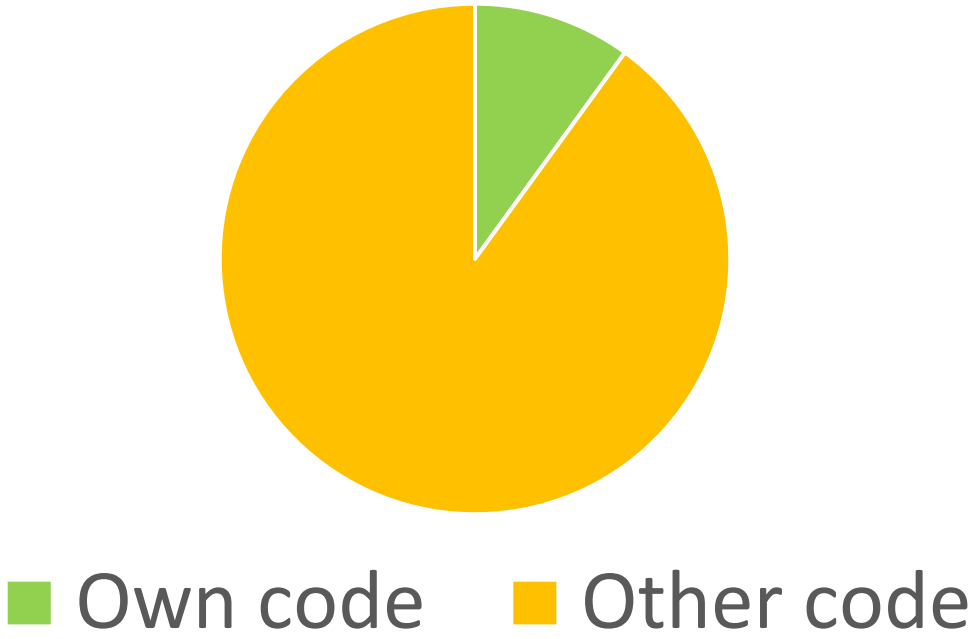
Cyber security management of supply chain

- A set of questionnairs for all third-parties
  - Often biasedly filled
- Rating based on public services
  - Could mostly point to e.g. CDN or cloud infrastructure
    - Not directly related to any internal security practice
- Monitoring/auditing
  - Already in use in other areas
    - Financial audit of a supplier
    - Quality audit of a supplier (pharmaceuticals, automotive, and aerospace)
- Analyzing shared cyber security information
  - Pentest reports excerpt
  - Certificates
- Pentesting (red teaming)
  - Supplier's network and systems
  - Interconnection points (VPNs)

CI/CD pipeline external sources



Product (source) code



Source: Webinar ‘Understanding Supply Chain Risk - Using SCA to protect your application’

Readme | Code Beta | 0 Dependencies | 2.163 Dependents | 71 Versions

build unknown | npm v1.0.37 | downloads 13M/week | jsDelivr 173M hits/month | cdnjs v1.0.37

UAParser.js

JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-side).

- Author : Faisal Salman <f@faisalman.com>
- Demo : https://faisalman.github.io/ua-parser-js

Install

```
> npm i ua-parser-js
```

Repository
github.com/faisalman/ua-parser-js

Homepage
github.com/faisalman/ua-parser-js

❤Fund this package

Weekly Downloads
12.510.003

Version
1.0.37

License
MIT

Unpacked Size
112 kB

Total Files
7

Acc development, 7k installations per week

Posted: October 5, 2021

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this.

There is no 2FA on the account. Login and password access. The password is enough to change your email.

Suitable for distributing installations, miners, creating a botnet

Start $10k
Step $1k
Blitz $20k

Source: Webinar ‘Understanding Supply Chain Risk - Using SCA to protect your application’

CVEdetails.com
powered by SecurityScorecard

Vulnerabilities
- By Date
- By Type
- Known Exploited
- Assigners
- CVSS Scores
- EPSS Scores
- Search

Vulnerable Software
- Vendors
- Products
- Version Search

Vulnerability Intel.
- Newsfeed
- Open Source Vulns
- Emerging CVEs
- Feeds
- Exploits
- Advisories

Ua-parser-js Project : Security Vulnerabilities, CVEs,

Published in: 2024 January February March April

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2021-4229

A vulnerability was found in ua-parser-js 0.7.29/0.8.0/1.0.0. It has been rated as critical. This issue affects the crypto mining component which introduces a backdoor. Upgrading to version 0.7.30, 0.8.1 and 1.0.1 is able to address this issue. It is recommended to upgrade the affected component.

Max CVSS	8.8
EPSS Score	0.48%
Published	2022-05-24
Updated	2022-06-06

CVE-2020-7733

The package ua-parser-js before 0.7.22 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex for Redmi Phones and Mi Pad Tablets UA.

Max CVSS	7.5
EPSS Score	0.39%
Published	2020-09-16
Updated	2022-10-07

CVE-2020-7793

The package ua-parser-js before 0.7.23 are vulnerable to Regular Expression Denial of Service (ReDoS) in multiple regexes (see linked commit for more info).

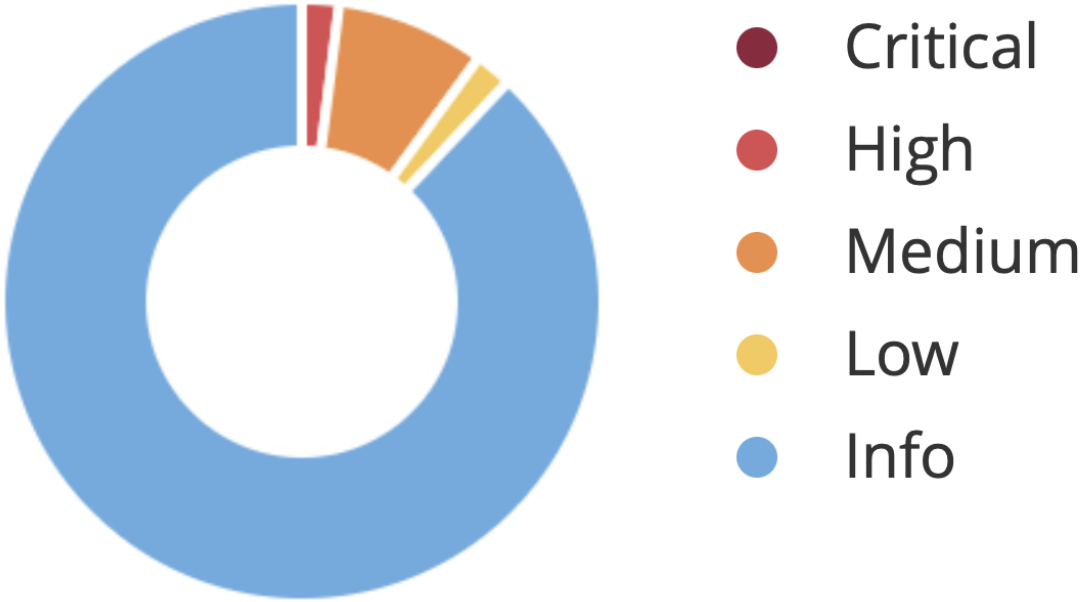
Max CVSS	7.5
EPSS Score	0.27%
Published	2020-12-11
Updated	2022-09-13

2 HIGH RISKS

- CLEARTEXT SQLITE DATABASE [DAST] [M2] [CWE-312]

- USAGE OF UNENCRYPTED HTTP PROTOCOL [SAST] [M3] [CWE-319]
  - HttpsURLConnection conn = (HttpsURLConnection) url.openConnection();

Vulnerabilities




EU DIGITAL COVID CERTIFICATE
Nom(s) de famille et pré
Date de naissance
CERTIFICAT DE VACCINATION
COVID-19
SARS-CoV-2 mRNA
vaccine
COVID-19 Vaccine

Trust Center

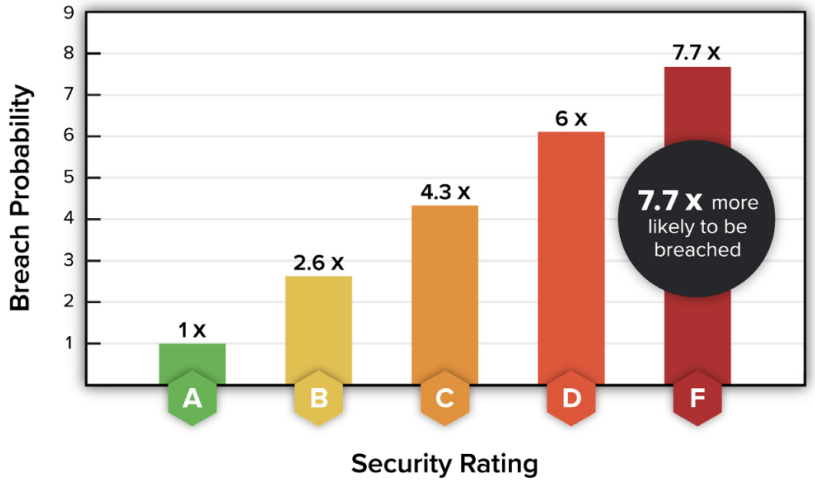
- Common elements of Trust Center
  - Overview
  - Compliance certifications
    - ISO, PCI, etc.
  - Security documentation
    - Penetration testing report excerpts, security/privacy whitepapers, etc.
  - Knowledge base of answers to common buyer questions
  - Public updates log
  - Security review checklist items
    - Details about product security features, etc.

TPRM program requirements

- Must ensure compliance
  - NIS2
  - DORA
- Must be objective
- Must be continuous
  - Offer also historical data
- Must be scalable
  - E.g. when we go from critical to all suppliers
    - Storing, processing, comparing questionnaires
    - Monitoring suppliers' ratings

Supply chain ratings

- Ratings based on
  - IP reputation
  - Network security
  - DNS health
  - Web application security
  - Patching cadence
  - Hacker chatter
  - Leaked credentials
- Notifications when rating changes
  - Leaked credentials notifications
  - Breach notifications



Pragmatic steps

- Manage who, when, for how long, and from/by which device can access your systems
- Include cyber security requirements in contracts (if not done already)
- Reserve the right to pentest a supplied product
- Reserve the right to audit/pentest a supplier
- Require a certificate for a product
- Validate product security when integrated into your environment
- Manage questionnaires
- Monitor ratings of suppliers that reflect their cyber hygiene

info@carbonsec.com