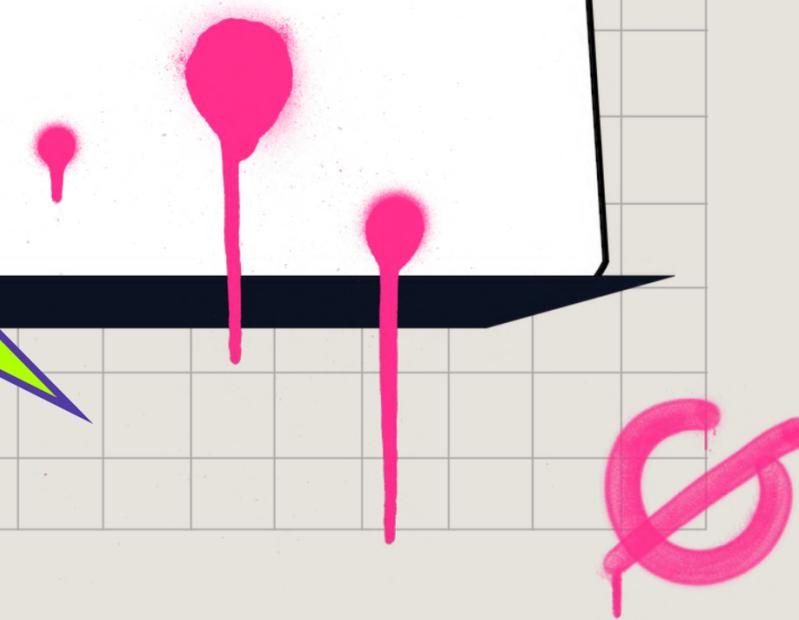




# Making it easy to get to SLSA level 2

Theofilos Petsios (@theofilospe)



(or)

**meet compliance requirements**

**hassle-free**

**while also getting value for your org**



# Software Supply Chain Attacks Gaining Popularity

Sonatype



Average Yearly Increase Since 2019 was 742%

Help Net Security



Supply Chain Attacks Surpass Malware-Based Attacks by 40% (2022)

Synopsys  
&  
Capterra

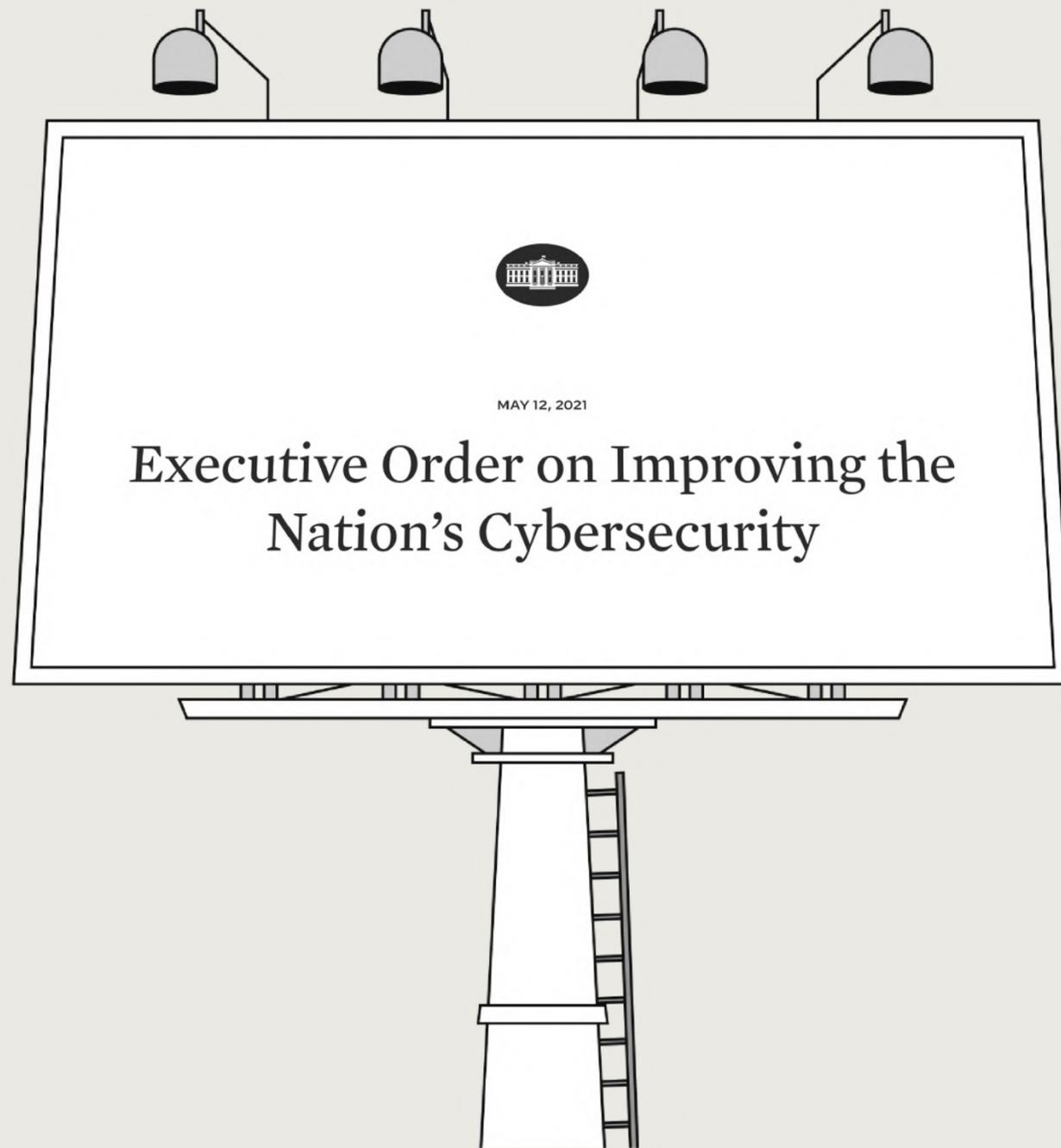


61% of US Businesses Impacted by a Supply Chain Attack  
(April 2022 - April 2023)



# Popularity Drives Policy Changes

*... guidance shall include standards, procedures, or criteria regarding:*



“ providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website ”

“ maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components ”



# Overview

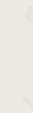
---

Concepts 101

Challenges

Chalk

Discussion



# Software Bills of Materials (SBOMs)

"List of ingredients" for software



```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.2",
  "serialNumber": "urn:uuid:371ffb8c-c11e-42b5-b5b9-9280fc62783e",
  "version": 1,
  "metadata": {
    "timestamp": "2020-08-03T08:53:09.834Z",
    "tools": [
      {
        "vendor": "CycloneDX",
        "name": "Node.js module",
        "version": "2.0.0"
      }
    ]
  },
  "component": {
    "type": "library",
    "bom-ref": "pkg:npm/protonmail-web@4.0.0-beta.20",
    "name": "protonmail-web",
    "version": "4.0.0-beta.20",
    "description": "Angular frontend for protonmail.com",
    "licenses": [
      {
        "license": {
          "id": "MIT"
        }
      }
    ],
    "purl": "pkg:npm/protonmail-web@4.0.0-beta.20",
    "externalReferences": [
      {
        "type": "website",
        "url": "https://github.com/ProtonMail/WebClient#readme"
      },
      {
        "type": "issue-tracker",
        "url": "https://github.com/ProtonMail/WebClient/issues"
      },
      {
        "type": "vcs",
        "url": "git+https://github.com/ProtonMail/WebClient.git"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "bom-ref": "pkg:npm/%40babel/polyfill@7.10.4",
      "group": "@babel",
      "name": "polyfill",
      "version": "7.10.4",
      "description": "Provides polyfills necessary for a full ES2015+ environment",
      "hashes": [
        {
          "alg": "SHA-512",
          "content": "f0161c9d5a90e64303d875e81c89c11fb1f56ffb8fdca767c026173aa1675ea82e3b2baee38dd65eeb1b2146d611f6376744f19343"
        }
      ],
      "licenses": [
        {
          "license": {
            "id": "MIT"
          }
        }
      ],
      "purl": "pkg:npm/%40babel/polyfill@7.10.4",
      "externalReferences": [
        {

```

# Provenance

How did the artifact get here?

- Who created it?
- Who packaged it?
- Who transported it?



# Reflections on Trusting Trust

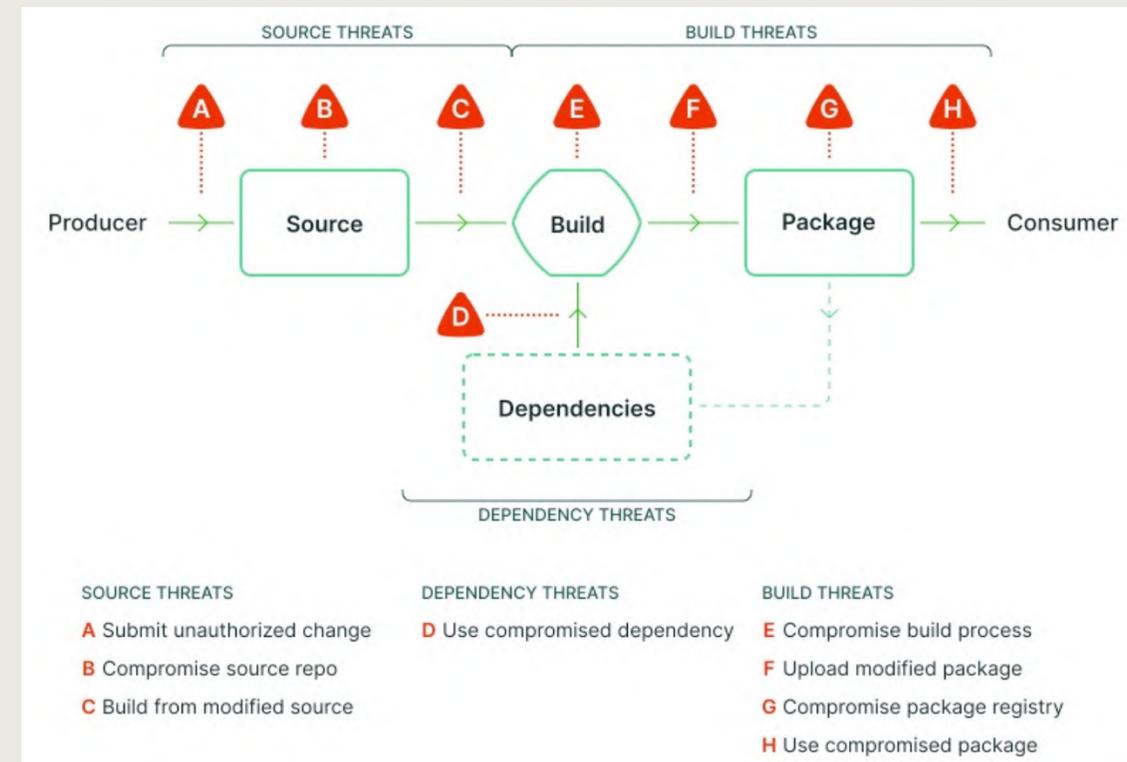
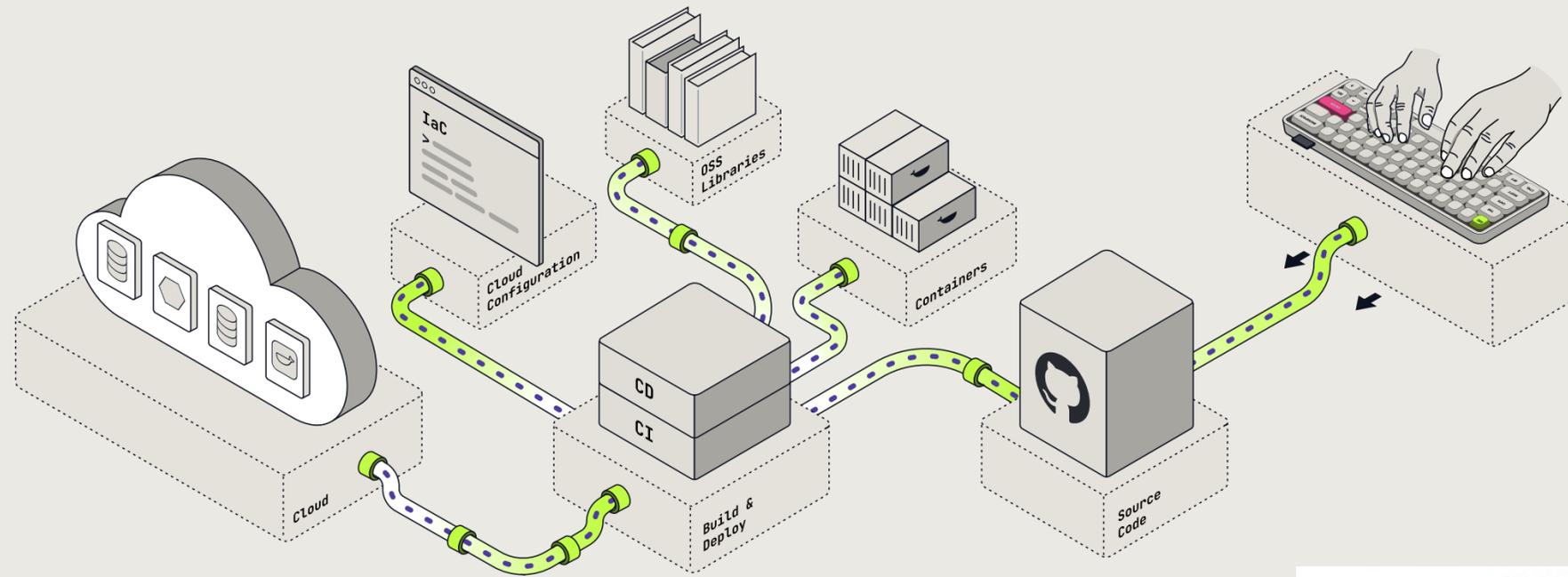


# Attestation



- Need to ensure data is not tampered with and comes from a trusted source
- Anyone should be able to verify the integrity
- Clear assumptions around the threat model

# DevOps Pipelines In Practice



Source: [slsa.dev](https://slsa.dev)



# Supply chain Levels for Software Artifacts (SLSA)

L1: Provenance shows how the package was built (documentation)

L2: Signed provenance, generated by hosted build platform (tampering post build)

L3: Hardened build platform (tampering during the build)

Implementer	Requirement	Degree	L1	L2	L3
Producer	Choose an appropriate build platform		✓	✓	✓
	Follow a consistent build process		✓	✓	✓
	Distribute provenance		✓	✓	✓
Build platform	Provenance generation	Exists	✓	✓	✓
		Authentic		✓	✓
		Unforgeable			✓
	Isolation strength	Hosted		✓	✓
		Isolated			✓



Source: [slsa.dev](https://slsa.dev)



**ok, how do I do this?**



# Surely there must be tools for this already

## LUNGI DELL'OLIO

Secondo un sondaggio la maggioranza dei malati ha smesso di andare a svolgere le necessarie terapie in ospedale sia per paura di contagio e sia perché le strutture sono oberate. Intanto però la ricerca sta facendo passi in avanti

L'emergenza dovuta alla pandemia di Coronavirus complica ulteriormente la diagnosi delle persone affette da malattie rare, come si definiscono le patologie a numero ridotto di casi diagnosticati e sotto una certa soglia, che nell'Unione europea è di uno ogni 2 mila abitanti.

Tra la concentrazione dell'attenzione sanitaria verso i malati di Covid 19 e il timore degli stessi malati di restare in ospedale, c'è un crescente bisogno di assistenza che non viene soddisfatto in queste settimane. Anche se, guardando al di là dell'emergenza del momento, va detto che sia a livello istituzionale, che di case farmaceutiche va crescendo l'atteggiamento verso i farmaci orfani, per quanto spesso la loro nascita e commercializzazione non siano remunerative.

## L'INDAGINE

Secondo un sondaggio condotto dal Centro nazionale malattie rare (Cnmr) dell'istituto superiore di sanità e dalla Federazione delle associazioni di malati rare Unimus, dal lo scoppio della pandemia più della metà dei malati (il 57 per cento) ha rimosso o interrotto i percorsi terapeutici. Il 46 per cento su consiglio del medico di famiglia o del pediatra di libera scelta o dello specialista del centro di riferimento per la propria patologia, gli altri si hanno mosso di propria iniziativa, soprattutto per paura del contagio in ospedale. Inoltre, circa un paziente su tre ha segnalato la mancanza di assistenza sanitaria e sociale, con come pesante difficoltà di accesso a informazioni pratiche rispetto ai percorsi e certifica il lavoro. I rischi preoccupanti se si considera che i pazienti affetti da malattie rare hanno bisogno di cure continue, dai controlli alla riabilitazione, dai dispositivi medici alle terapie che spesso possono essere somministrate solo in ospedale. Coloro che difficoltà rilevate possono produrre alcuni preventivi.

## NUMERI

Il numero di malattie rare diagnosticate oscilla tra le 7 mila e le 8 mila, con numeri che crescono di pari passo con l'avanzare della scienza, e in particolare con i progressi



La ricerca genetica. Considerate nel loro insieme, le persone affette da questo tipo di patologie sono diverse milioni in tutta Europa. In base ai dati riportati dal Registro Nazionale Malattie Rare dell'Istituto Superiore di Sanità, in Italia si stimano 20 casi ogni 10 mila abitanti e ogni anno sono circa 19 mila i nuovi casi segnalati dalle oltre 300 strutture sanitarie diffuse in tutta la Penisola.

Il 20 per cento delle patologie coinvolge persone in età pediatrica (sino a 14 anni). Le più diffuse sono le malformazioni congenite, le malattie delle ghiandole endocrine, della nutrizione e del metabolismo e i disturbi immunitari. Tra gli adulti, invece, le più frequenti appartengono al gruppo delle patologie del sistema nervoso e degli organi di senso.

**FARMACI** La ricerca in questo campo è sulla frontiera più avanzata della scienza e della tecnologia. Su 39 farmaci considerati come i più innovativi nell'ultimo quarto di secolo, 30 sono stati inizialmente sviluppati per malattie rare. Uno studio di recente ha sottolineato la rilevanza degli investimenti da parte dell'industria farmaceutica in questi anni: tra il 2000 e il 2018, si sono state 2.121 designazioni di "farmaco orfano", che hanno portato a oltre 190

nuovi trattamenti autorizzati per circa 90 patologie. Il termine "orfano" è stato scelto per indicare ai medicinali destinati alla cura delle malattie talmente rare da non consentire la realizzazione, da parte delle aziende farmaceutiche, di ricavi che permettano di recuperare le spese sostenute per il loro sviluppo. Questo perché il processo che va dalla scoperta di una nuova molecola alla sua commercializzazione dura in media dieci anni, costa diverse decine di milioni di euro ed è molto aleatorio: tra dieci molecole testate, una sola può avere effetto terapeutico. Siamo ancora molto lontani dal soddisfare il bisogno medico di tutte le persone con malattie rare - parliamo di oltre 20 milioni di persone - ma le diverse fra loro - ma le coperture fatte fino ad ora sono state pensate anche grazie al fatto che una popolazione prima trascurata è riuscita a far sentire la propria voce. Così, secondo l'ultimo rapporto Monitorare, l'ecosistema di farmaci orfani tra il 2003 e il 2017 sono aumentati del 60,25 in termini assoluti e del 66,09 in termini relativi sul totale. Mentre la spesa per medicinali di nuova molecola è cresciuta del 74,7 per cento in termini assoluti. Il risultato da tenere a mente, segnalato che nell'ultimo quinquennio vi è stata una crescita costante del nu-

## L'analisi

CARLO BASTIANI

### segue dalla prima

In questione ci sono ovviamente il futuro di lavoratori e imprese, ma anche la tenuta di un'area economica che la crisi renderà più disomogenea. L'arricchimento della cooperazione dell'orizzonte e, infine, in un Paese del Sud, le sorti di un governo che, non volendo adattare le risorse del Fondo salva stati. Ma, spera che gli studi vengano ripresi proprio dal Fondo per la ripresa. L'attenzione italiana - analisti al fondo come scritto del Moe - dovrebbe essere rivolta a un aspetto più sostanziale, che sarà definito dalle scelte della Commissione europea. Dopo esser stata presentata, la proposta della Commissione sarà oggetto di un completo negoziato con le altre istituzioni europee e soprattutto con governi e Parlamenti nazionali. Essendo agganciata all'approvazione del prossimo bilancio settoriale dell'Ue, la proposta ha bisogno di essere approvata all'unanimità. Questi due fattori - rapidità e unanimità - stanno determinando il carattere della più importante iniziativa finanziaria della storia europea e purtroppo rischia di limitarne sia il potenziale finanziario, sia quello politico, cioè di sostegno alla convergenza tra i Paesi e al risanamento dei legami. La presidente Ursula von der Leyen ha di fronte a sé un'alternativa: procedere rapidamente verso un progetto che si limiti al minimo comune denominatore tra gli Stati, oppure rischiare un periodo di contrasti, ma sfruttare il Fondo per la ripresa per dare all'Ue grandi obiettivi e grandi risorse comuni. Una soluzione intergovernativa in prima, contro una soluzione comunitaria. Ma non si tratta affatto solo di soldi ma di istituzioni. La soluzione rapida e minimale è la più probabile. Von der Leyen dovrà corteggiare il consenso unanime di tutti i Paesi, da quelli che meno hanno bisogno a quelli più deboli, non

solo secondo una direttrice convenzionale - Nord e Sud - ma anche avendo riguardo alle pretese dei Paesi dell'Est. Europa, per ottenerne privilegiati dai fondi del bilancio europeo e oggi poco inclini a investire Italia e Spagna. A favore della stessa moneta gioca anche l'argomentazione delle risorse. Il nuovo bilancio Ue comincerà il 1° gennaio, ma il suo iter prevede una soluzione ponte che consenta di mobilitare parte delle risorse già in essere. Il 1° giugno, il Consiglio Ue dovrà aver adottato il pacchetto di misure approvate il mese scorso, ma subito dopo dovrà arrivare all'approvazione del Fondo per la ripresa. Tenere molto stretti per convogliare le capitali ad altri di coraggio e solidarietà. La dimensione del Fondo dipenderà dalla scelta tra la soluzione intergovernativa e quella comunitaria. Stando parlando infatti di un ammontare imprecisato tra 300 e 1.500 miliardi di euro, il valore finale dipenderà da un effetto leva che rischia il mancato del passo Juncker del 2014. Allora le risorse Ue mobilitano investimenti privati abbastanza copiosi. Ma in quella fase l'economia si stava riprendendo dopo la crisi del debito sovrano. Nel 2021 le condizioni potrebbero invece essere ancora deboli ed è difficile immaginare che gli investitori privati contribuiscano a moltiplicare i fondi governativi dell'Ue. Dietro una retorica di cifre mirabolanti potrebbe nascondersi un ammontare del tutto insufficiente a contrastare la più profonda crisi economica a memoria d'uomo. Per l'Italia si

## L'opinione

Una proposta minimale otterrà più facilmente il consenso di tutti, ma non aiuterà a colmare le differenze strutturali tra i Paesi

## L'intervento

CRISTINA BETTINELLI \* e SALVATORE SCIASCIA \*\*

Il passaggio generazionale nelle imprese familiari è un fenomeno di grande interesse perché riguarda una parte importante di cui la produttività e il benessere sono costituiti da due o più membri della stessa famiglia, così che in Italia riguardano dal 70 al 90 per cento delle imprese. I dati del nostro sistema di lavoro, sanità e welfare ci dicono che in Italia nei prossimi anni di lavoro molti casi di questo tipo, perché il 33 per cento ha più di 50 anni. Sul passaggio generazionale esistono diverse condizioni che meritano di essere affrontate. La prima è che se i tratti del passaggio di un business, in realtà i testimoni sono due, non necessariamente cognati leadership generazionale e proprietà. Possono essere fratelli o cugini, o anche un terzo si può vedere solo l'uno o l'altro. Il secondo mito è che, per poter parlare di passaggio generazionale di successo, tutto debba avvenire all'interno della cerchia familiare. In realtà leadership e proprietà possono anche passare nelle mani di soggetti non familiari per garantire la prosperità dell'impresa. Le opzioni a disposizione sono diverse e ampie, ognuna con i suoi vantaggi e i suoi svantaggi: la cosa importante è dotare l'impresa di capitale umano e finanziario e di un piano di successione adeguato. Il terzo mito è che il passaggio sia una grande minaccia per la sopravvivenza dell'impresa, tant'è che in ogni Paese esiste almeno un provvedimento per ricordare che la sopravvivenza della prima alla seconda generazione è buona e distribuita. Il quarto mito è che il passaggio sia un fatto che si può gestire in un'ora. In realtà, se ben gestito, il passaggio generazionale può rappresentare un'occasione preziosa per riflettere sul business e ridare energia all'impresa attraverso nuovi capitali, conoscenze e competenze. Sono innumerevoli i casi di imprese familiari che, grazie all'ingresso della nuova generazione, hanno saputo cogliere le sfide della globalizzazione.

Non a caso le imprese più longeve sono proprio quelle familiari, di quarto, e sono protagoniste, non a caso, di un passaggio generazionale che un momento, che avviene all'interno di un'azienda, ma che, per funzionare, deve durare mediamente 7 anni. Ci sono degli step da seguire secondo Zenger (2017) il successo prima di tutto dipende da obiettivi e priorità del predecessore e del successore. Riguardo al passo al punto di intraprendere un passaggio generazionale: se la risposta è no, oppure è incerta, è inutile proseguire, investendo denaro e tempo

## Il libro

MARCO PANARA

## È

forte l'impressione che così com'è oggi il capitalismo non sia in grado di risolvere i problemi che crea. È il sistema al quale dobbiamo il più alto livello di prosperità che il genere umano abbia mai conosciuto, per un certo periodo storico, più o meno tra il 1945 e il 1980 e il resto è dovuto anche a distribuzioni accidentali. Non è cattivo in sé, come gli ideologi hanno sostenuto, ma forse in sé come altre ideologie continuava a sostenere. La sua qualità dipende dalle istituzioni che regolano i diritti, i doveri, il mercato. Il deterioramento del capitalismo si può allora limitare da questi mezzi secondo il pacifismo di quello delle istituzioni, che a sua volta dipende dalla dinamica economica sociale, dalla dispersione dell'identità e dell'appartenenza, dalla razionalizzazione degli obblighi reciproci. C'è molto da ricostruire, e una sfida di cui è protagonista da mettere in campo. Per avere un capitalismo etico è utile uno Stato etico, che non può essere senza una rete di obblighi reciproci che legano al fine comune di una società migliore cittadini, famiglie, imprese e istituzioni.

## Il futuro del capitalismo

Paul Collier  
Laura  
Pagine 320  
Euro 20

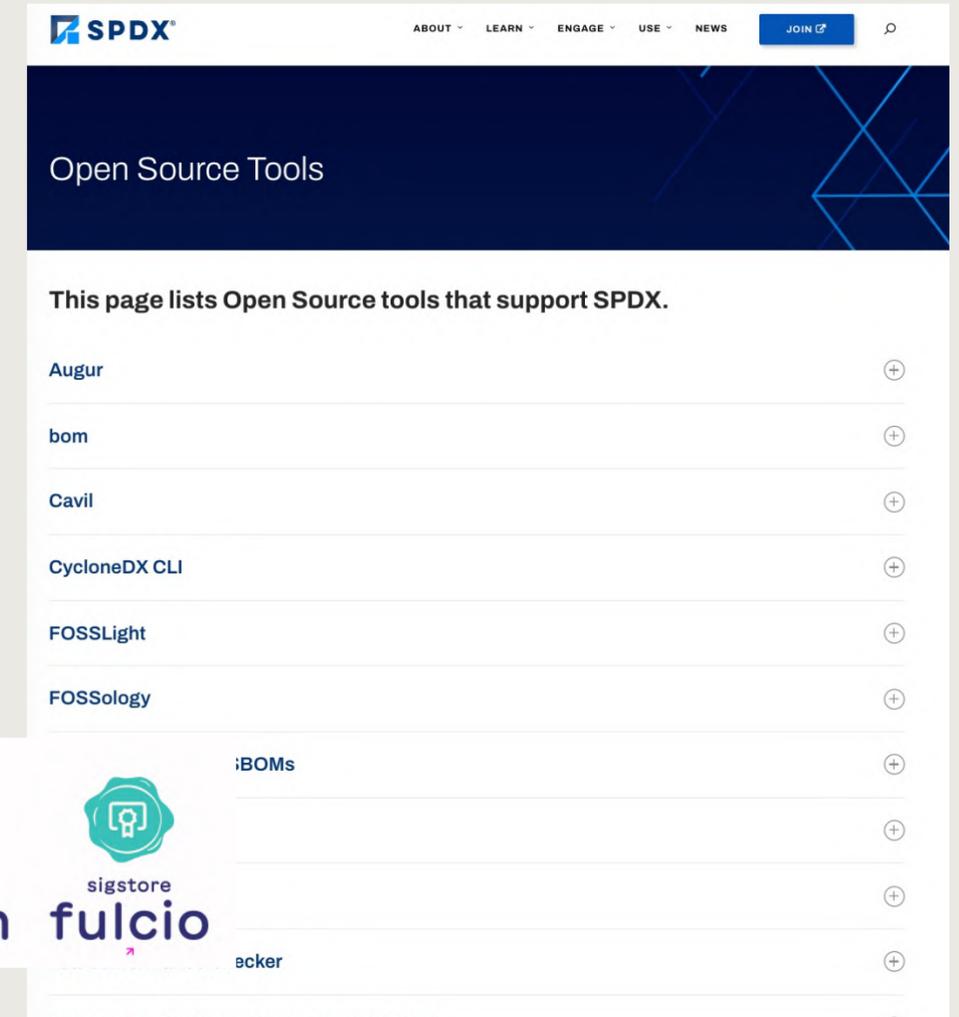
tratta di un aspetto vitale: una finalità non dichiarata del Fondo di ripresa è infatti di conciliare risorse sufficienti al bilancio italiano, senza ricorrere a trasferimenti diretti, in modo da ridurre le esportazioni di capitali italiani nei prossimi mesi ed evitare che alla crisi economica segua una crisi del debito sovrano come nel 2010. Tuttavia, un negoziato tra il confronto tra gli interessi degli Stati rischia di essere determinato dalle esigenze immediate del governo nazionale meno volte possibili da parte degli Stati più ricchi, magari dovendo essere assorbiti dal per un migliore richiamo di leveva risorse del governo peruviano. In sostanza, il Fondo si tradurrebbe in un trasferimento di risorse, pur consistente, dal quale l'economia europea emergente e non diversa da oggi, ma anzi con un approfondimento delle divergenze strutturali tra i Paesi. E quindi con l'Italia in condizione di persistente debole.

Una soluzione intergovernativa in prima, contro una soluzione comunitaria. Ma non si tratta affatto solo di soldi ma di istituzioni. La soluzione rapida e minimale è la più probabile. Von der Leyen dovrà corteggiare il consenso unanime di tutti i Paesi, da quelli che meno hanno bisogno a quelli più deboli, non solo secondo una direttrice convenzionale - Nord e Sud - ma anche avendo riguardo alle pretese dei Paesi dell'Est. Europa, per ottenerne privilegiati dai fondi del bilancio europeo e oggi poco inclini a investire Italia e Spagna. A favore della stessa moneta gioca anche l'argomentazione delle risorse. Il nuovo bilancio Ue comincerà il 1° gennaio, ma il suo iter prevede una soluzione ponte che consenta di mobilitare parte delle risorse già in essere. Il 1° giugno, il Consiglio Ue dovrà aver adottato il pacchetto di misure approvate il mese scorso, ma subito dopo dovrà arrivare all'approvazione del Fondo per la ripresa. Tenere molto stretti per convogliare le capitali ad altri di coraggio e solidarietà. La dimensione del Fondo dipenderà dalla scelta tra la soluzione intergovernativa e quella comunitaria. Stando parlando infatti di un ammontare imprecisato tra 300 e 1.500 miliardi di euro, il valore finale dipenderà da un effetto leva che rischia il mancato del passo Juncker del 2014. Allora le risorse Ue mobilitano investimenti privati abbastanza copiosi. Ma in quella fase l'economia si stava riprendendo dopo la crisi del debito sovrano. Nel 2021 le condizioni potrebbero invece essere ancora deboli ed è difficile immaginare che gli investitori privati contribuiscano a moltiplicare i fondi governativi dell'Ue. Dietro una retorica di cifre mirabolanti potrebbe nascondersi un ammontare del tutto insufficiente a contrastare la più profonda crisi economica a memoria d'uomo. Per l'Italia si

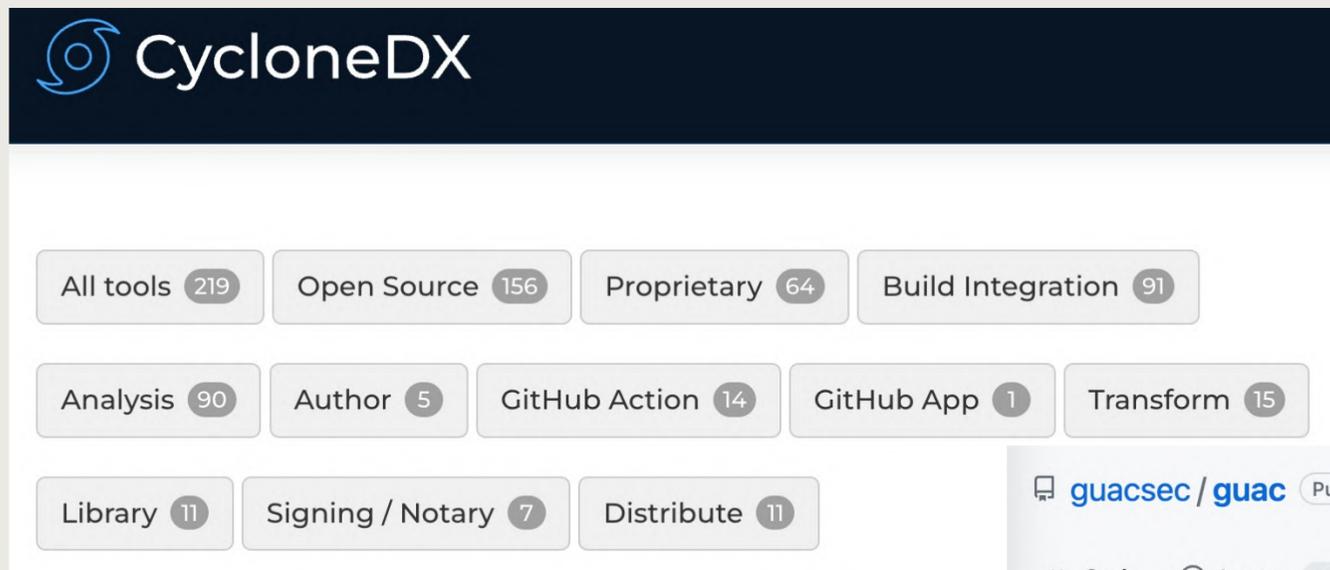
per consumare e piani che con ogni probabilità non si realizzeranno. Allora, come si può vedere, i costi sono alti e il tempo è lungo. La risposta deve essere minima, razionalizzando le risorse e riducendo il capitale di rischio. Una volta chiariti obiettivi e priorità, sarà necessario realizzare le vie attraverso le imprese in azienda in passato per comprendere come possono essere migliorate, anche in modo lento, nelle opportunità che il passaggio generazionale, a quel punto occorre definire un piano di successione mettendo "meno su bilancia". Come risulta facile definire un piano d'azione per il lancio di un nuovo prodotto, allo stesso modo sarà necessario studiare un piano, con scadenze precise, che definisca a chi ed entro quando diversi diritti e responsabilità verranno trasferiti. In questo punto gli studiosi sono concordi: il passaggio generazionale deve essere graduale e successore per almeno un paio di mesi possibile condividere le responsabilità così da far leva sull'esperienza e l'esperienza di entrambi e ridare un'impulso nel tempo dal predecessore e allo stesso tempo integrare gli assetti nuove energie e idee del successore, le più il passaggio del testimone si intende alla proprietà allora sarà necessario realizzare le istituzioni che, che sono la realizzazione dell'azienda, il funzionamento del passaggio di proprietà e la definizione degli aspetti legali e fiscali. Il rispetto dell'ordine con il quale questi step vengono implementati determinerà il successo dell'operazione. L'ultimo mito? Che sia un fenomeno che riguarda solo le imprese familiari. Tutte le imprese, per non dire tutte le istituzioni, si trovano prima o poi ad affrontare cambiamenti nella leadership e nella proprietà e il fenomeno riguarda davvero tutti. \*Università di Bergamo \*\*Università Cattolica - L'Espresso

# Where do I start?

- Which standard / tool do I use?
- Outputs are largely inconsistent
- How do I deploy these / consume the data?



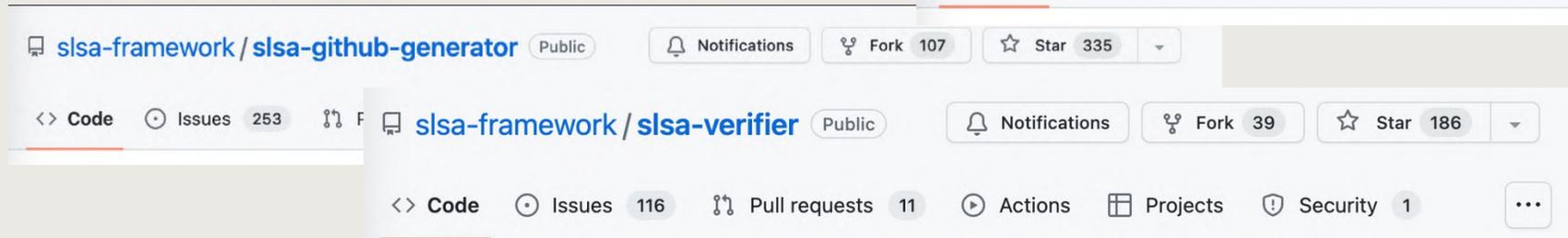
The screenshot shows the 'Open Source Tools' page on the SPDX website. The page lists various tools that support SPDX, including Augur, bom, Cavil, CycloneDX CLI, FOSSLight, FOSSology, iBOMs, and acker. Each tool name is followed by a plus sign icon, indicating that more information can be expanded for each tool.



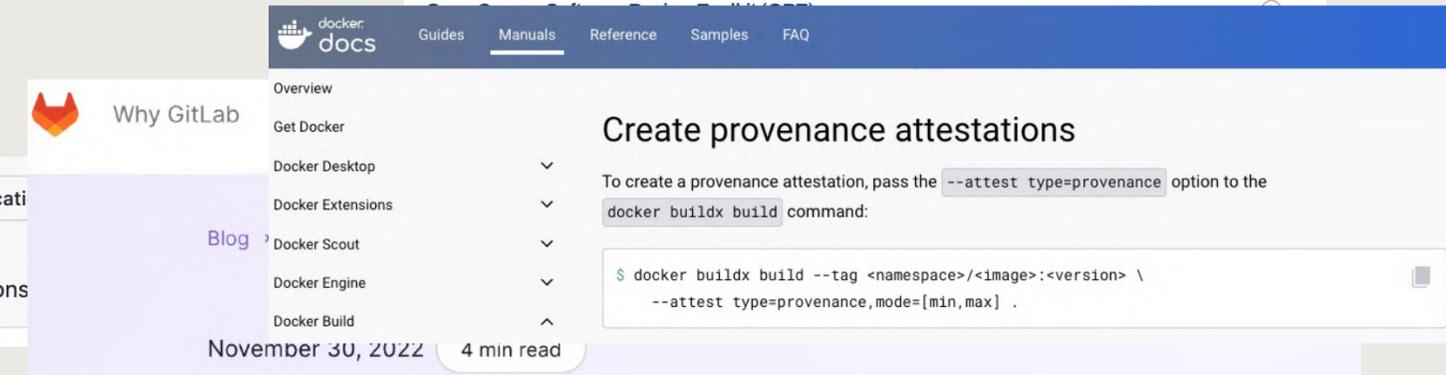
The screenshot shows the CycloneDX website. The header features the CycloneDX logo. Below the header, there are several filter buttons for tool categories: All tools (219), Open Source (156), Proprietary (64), Build Integration (91), Analysis (90), Author (5), GitHub Action (14), GitHub App (1), Transform (15), Library (11), Signing / Notary (7), and Distribute (11).



The screenshot shows a row of Sigstore tools: cosign, rekor, gitsign, and fulcio. Each tool is represented by its logo and name, with a small red arrow pointing to the right below the name.



The screenshot shows two GitHub repository pages. The top one is for 'guacsec / guac' (Public), with 116 issues, 13 pull requests, and 107 forks. The bottom one is for 'slsa-framework / slsa-verifier' (Public), with 253 issues, 11 pull requests, and 39 forks. Both pages show the repository name, star count, and navigation options like Code, Issues, Pull requests, and Actions.



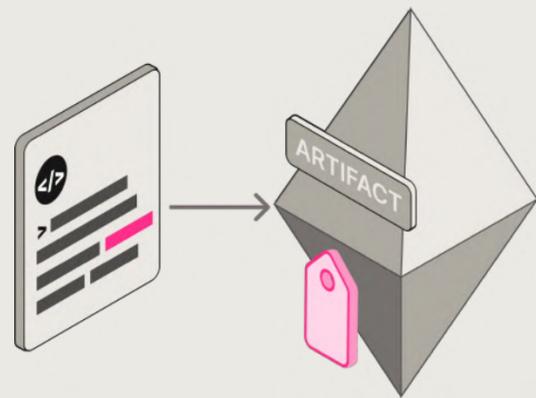
The screenshot shows two overlapping content pieces. On the left is the Docker documentation page for 'Create provenance attestations', which includes a code snippet: `docker buildx build --tag <namespace>/<image>:<version> \ --attest type=provenance,mode=[min,max] .`. On the right is a GitLab blog post titled 'Why GitLab' dated November 30, 2022, with a 4-minute read time.

**Achieve SLSA Level 2 compliance with GitLab**

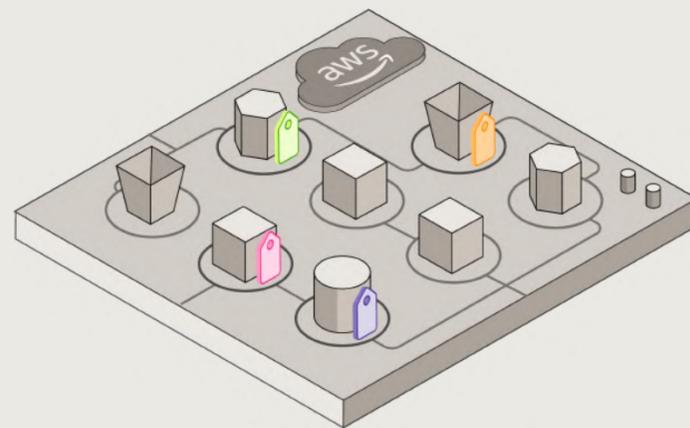




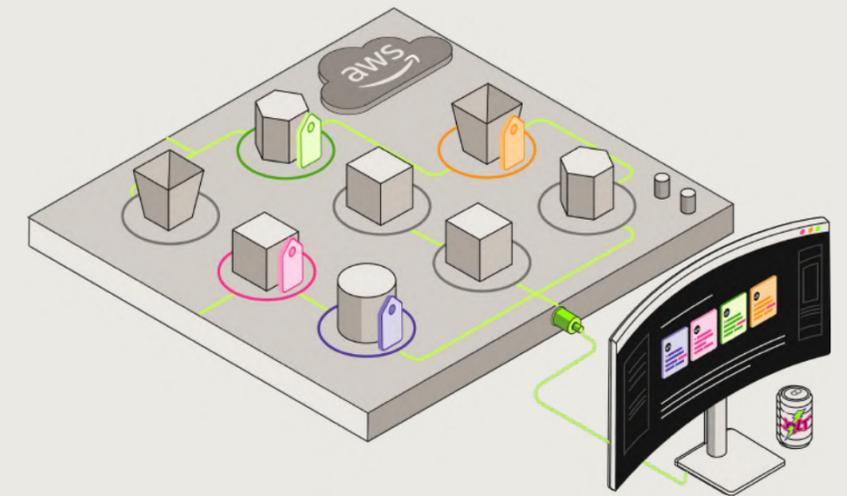
# Introducing Chalk



Embed metadata (chalk marks)  
into your artifacts  
(binaries/images etc.)  
during, or post build time



Deploy artifacts to production



Get metadata feeds  
(chalk reports) from  
artifacts running in  
production





demo

# Deploying With Chalk

## ✓ Generate and distribute SBOMs

```
SBOM {"syft": {"$schema": "http://cyclonedx.org/sc
```

## ✓ Provenance

exec	crashappsec/chalk-demo
build	crashappsec/chalk-demo

## ✓ Artifact integrity

**Details**

- Action ID: 36d5a4c99830d8bc
- Operation: build
- Datetime: **Signing data collected**
- Compliance:

✓ SLSA L2



**what more can you do?**



# Reduce Incident Response Times



# Application Inventory & Change Management



# Much, much more

---

- Not just containers!
- Deploy and run static and dynamic analysis tools
- Custom plugins for metadata surfacing!



# Try it out!

- Open-Source @ <https://github.com/crashappsec/chalk>
- Written in [Nim!](#)
- Welcoming feature requests!



# Backup Slides



# A deeper look into chalk

- Rich set of out-of-the box available [metadata options](#)
- Metadata can be grouped and published independently:
  - Reports aggregate metadata of interest
  - Publish them to different destinations (sinks)
- Plugin architecture
- Configuration language  
(e.g., set rule to only set a report if within a docker container)
- Effortless config loading



```
./chalk load https://chalkdust.io/basic\_compliance.c4m
```