CHECK POINT™

Guardians of Digital Trust

Project Sela TLV Conference – September 12

Dan Karpati | Chief Technologist

YOU DESERVE THE BEST SECURITY

BIS Innovation Hub

CHECK POINT™

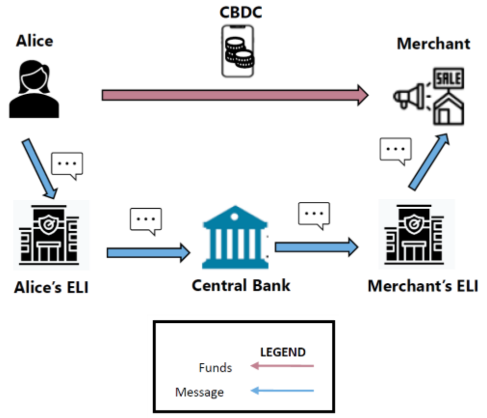
BANK OF ISRAEL בנק ישראל

HONG KONG MONETARY AUTHORITY
香港金融管理局

Project Sela

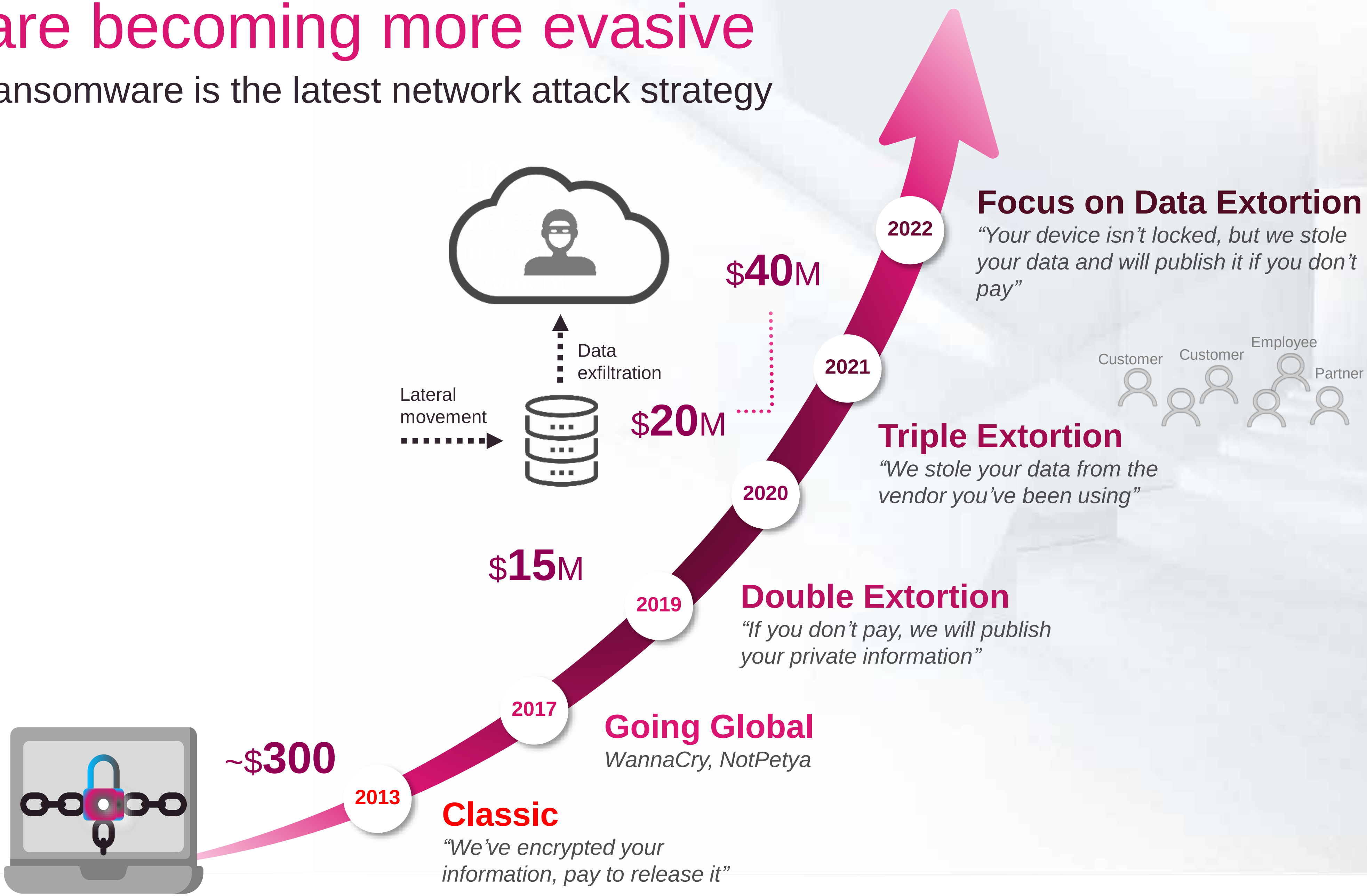
Two-Tier Retail CBDC with Exposure-less Cyber Secure Intermediaries

- **Cybersecurity Workstream Objectives:**
  - Provide practical and analytical cybersecurity insights into the architecture choices of a domestic exposure-less CBDC system
  - Minimize cybersecurity threats by preventative software design
  - Recommend cybersecurity echo systems & best practices
- **Members:**
  - Check Point's Security Committee, Distinguished Architects, Security Researchers, Penetration Testers



Ransomware becoming more evasive

Supply Chain + Ransomware is the latest network attack strategy



Classic

"We've encrypted your information, pay to release it"

Going Global

WannaCry, NotPetya

Double Extortion

"If you don't pay, we will publish your private information"

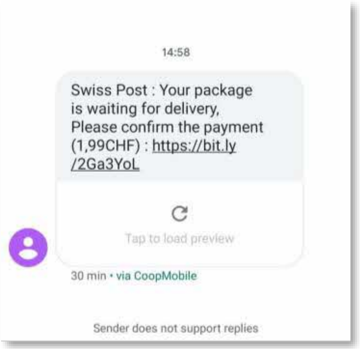
Triple Extortion

"We stole your data from the vendor you've been using"

Focus on Data Extortion

"Your device isn't locked, but we stole your data and will publish it if you don't pay"

Phishing mobile users.. – “Your Package Has Arrived!”



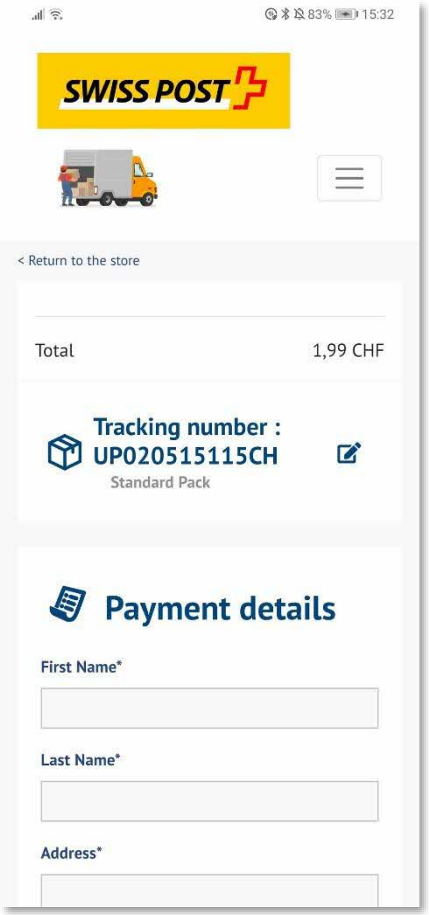
14:58

Swiss Post : Your package is waiting for delivery, Please confirm the payment (1,99CHF) : https://bit.ly/2Ga3YoL

Tap to load preview

30 min • via CoopMobile

Sender does not support replies



83% 15:32

< Return to the store

Total 1,99 CHF

Tracking number : UP020515115CH

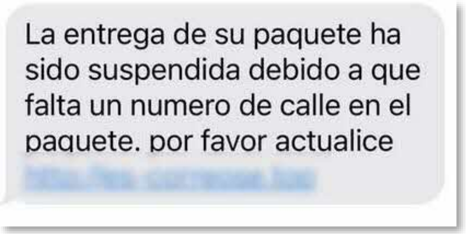
Standard Pack

Payment details

First Name*

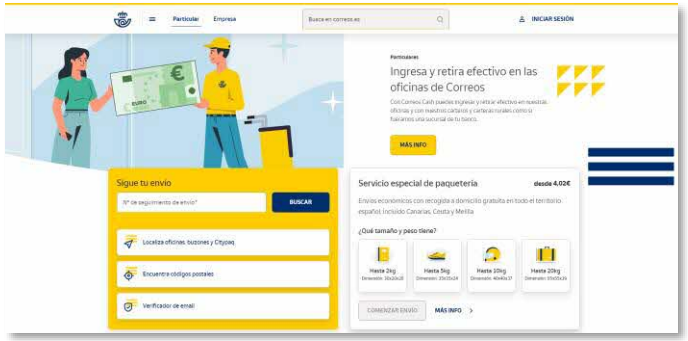
Last Name*

Address*



La entrega de su paquete ha sido suspendida debido a que falta un numero de calle en el paquete. por favor actualice

[redacted]



Particulares

Ingresa y retira efectivo en las oficinas de Correos

Con Correos Cash puedes ingresar y retirar efectivo en nuestras oficinas y con nuestros carteros y carteras rurales como si fuéramos una sucursal de tu banco.

Sigue tu envío

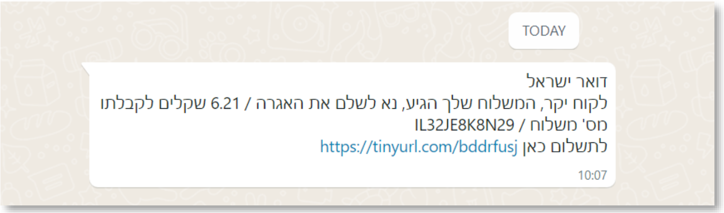
N° de seguimiento de envío*

BUSCAR
Localiza oficinas, buzones y Citypaq
Encuentra códigos postales
Verificador de email

Servicio especial de paquetería desde 4,02€

Envíos económicos con recogida a domicilio gratuita en todo el territorio español, incluido Canarias, Ceuta y Melilla

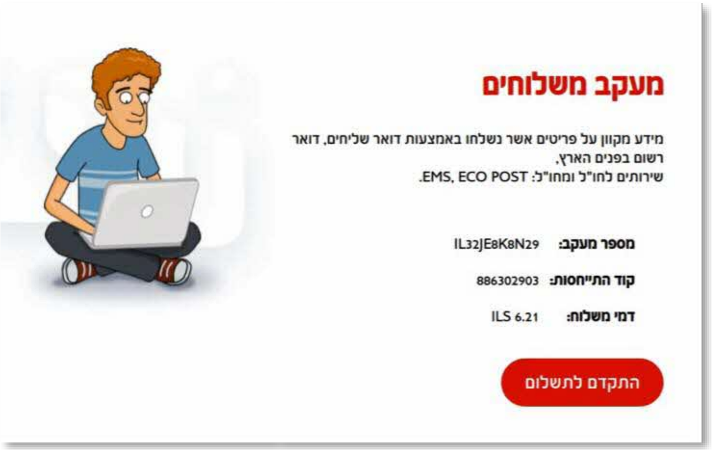
¿Qué tamaño y peso tiene?



TODAY

דואר ישראל
לקוח יקר, המשלוח שלך הגיע, נא לשלם את האגרה / 6.21 שקלים לקבלתו
מס' משלוח / IL32JE8K8N29
לתשלום כאן https://tinyurl.com/bddrfusj

10:07



מעקב משלוחים

מידע מקוון על פריטים אשר נשלחו באמצעות דואר שליחים, דואר
רשום בפנים הארץ,
שירותים לחו"ל ומחו"ל: EMS, ECO POST.

מספר מעקב:	IL32JE8K8N29
קוד התייחסות:	886302903
דמי משלוח:	ILS 6.21

CHECK POINT™

Software Supply Chain Attacks

New Security Measures

SLSA Standard

SLSA

YOU DESERVE THE BEST SECURITY

Supply chain is the modern entry point for attacks

Supply Chain attacks keep coming: the latest is 3CX in Mar’23

3CX®

Mar’23

- **240,000** exposed phone management systems

LOG4J

Dec’21 – Jan’22

- **Over 46%** of attempts by known malicious groups.
- Attempted exploit on **over 36.8% of corporate networks globally**

solarwinds

Mar’20 – Dec’20

- Affected **18,000 customers** (out of 300K)

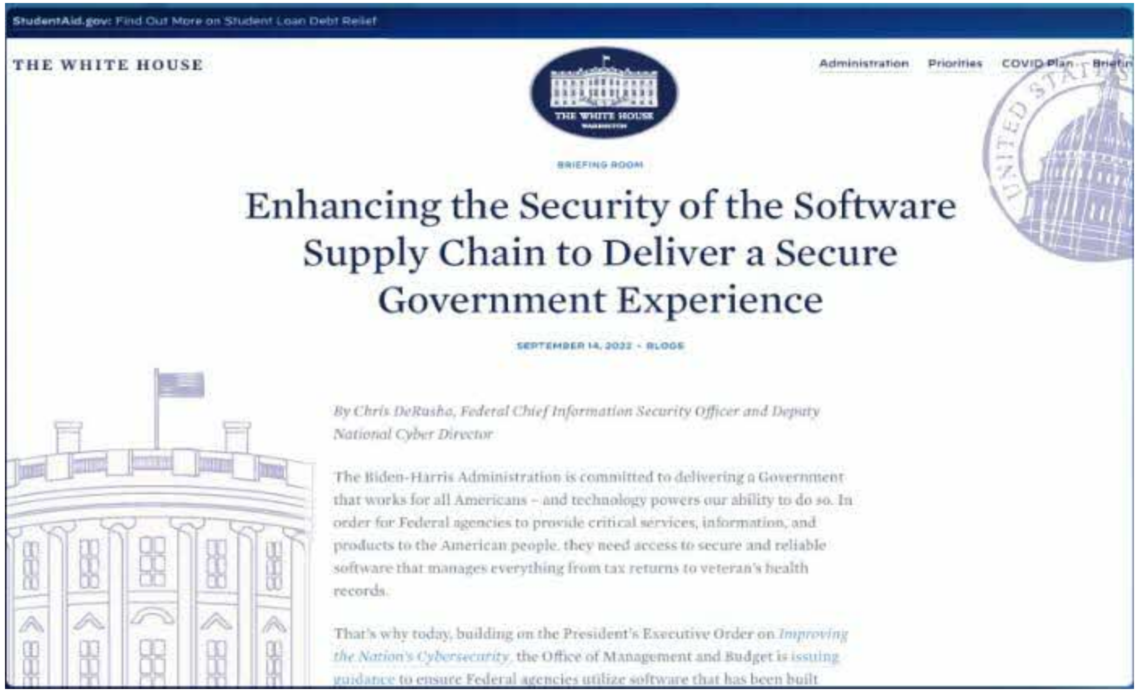
Prevented over 820,000 attempts
to allocate the Log4J vulnerability

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

NIST
National Institute of Standards and Technology



StudentAid.gov: Find Out More on Student Loan Debt Relief

THE WHITE HOUSE

Administration Priorities COVID Plan Briefin

BRIEFING ROOM

Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience

SEPTEMBER 14, 2022 · BLOGS

By Chris DeRusha, Federal Chief Information Security Officer and Deputy National Cyber Director

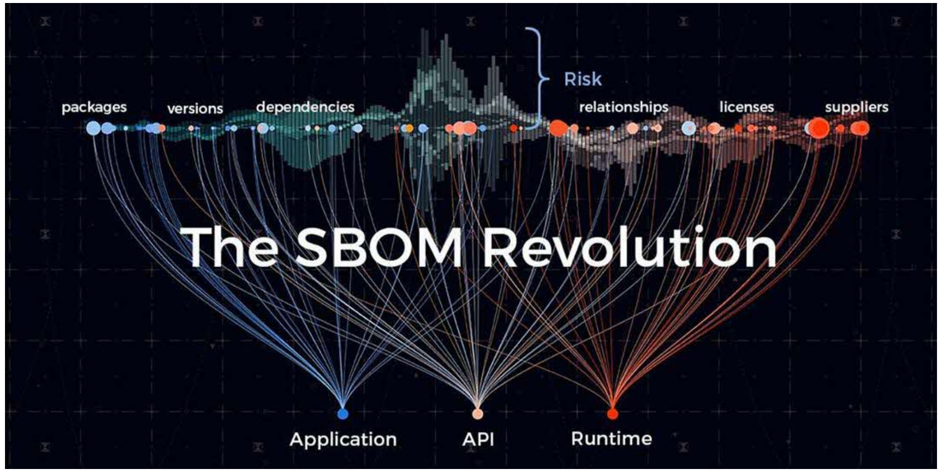
The Biden-Harris Administration is committed to delivering a Government that works for all Americans – and technology powers our ability to do so. In order for Federal agencies to provide critical services, information, and products to the American people, they need access to secure and reliable software that manages everything from tax returns to veteran's health records.

That's why today, building on the President's Executive Order on *Improving the Nation's Cybersecurity*, the Office of Management and Budget is issuing guidance to ensure Federal agencies utilize software that has been built

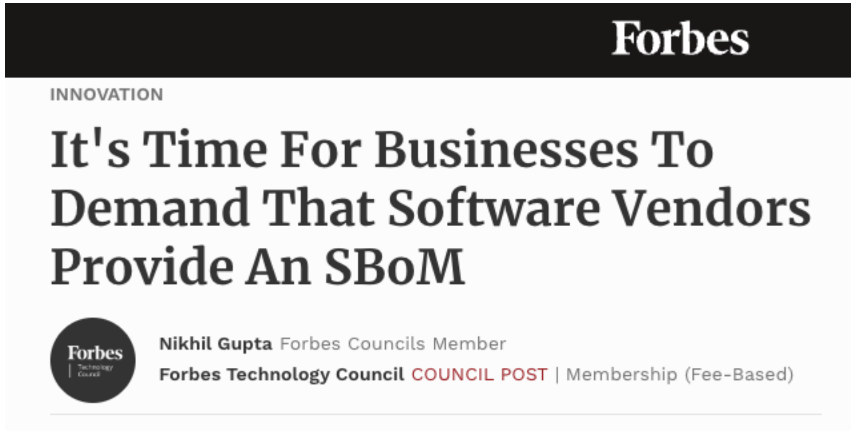
- **The White House** Executive Order (EO) 14028 from May 2021
- Tasked **NIST** (SSDF and SSCSG)
- **U.S. agencies** will be required to **obtain** from their **software producers SBOMs** and documented processes to validate **code integrity**
- **11 Billion market / year**

Gartner

More than 60% of organizations will have adopted SBOMs by 2025



Companies Joining The Effort

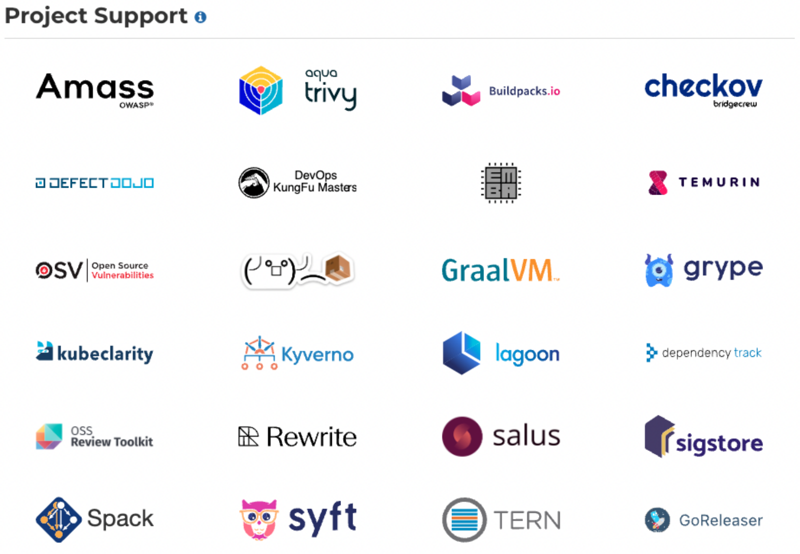


Forbes

INNOVATION

It's Time For Businesses To Demand That Software Vendors Provide An SBoM

Nikhil Gupta Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

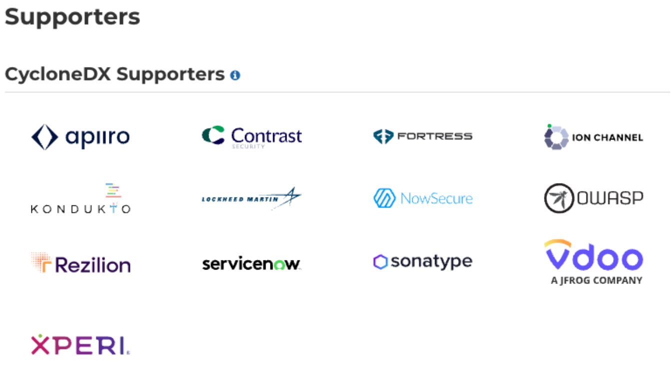


Project Support

Amass OWASP, aqua trivy, Buildpacks.io, checkov bridgecrew
DEFECTDOJO, DevOps KungFu Masters, TEMURIN
OSV Open Source Vulnerabilities, GraalVM, grype
kubeclarity, Kyverno, lagoon, dependency track
OSS Review Toolkit, Rewrite, salus, sigstore
Spack, syft, TERN, GoReleaser

Vendor Support

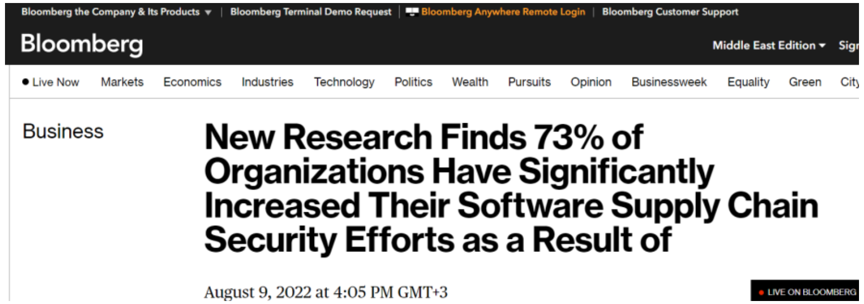
18F, anchore, apiiro, aqua
ArmorCode, BlackBerry, BYTESAFE, [illegible]
Chainguard, Checkmarx, cisco, CLOUD NATIVE
cloudsmith, CodeNotary, Contrast, CYBEATS
C/D CYBELLUM, CyberTest, deepfence, enso
FOSSA, FINITE STATE, Flexera, FORTRESS
GitLab, Google, GRAMMATECH, IBM
intel, ION CHANNEL, JDisc, JFrog
JupiterOne, KONDUKTO, medcrypt, MedSec
MEND, MergeBase, MICRO FOCUS, NETRISE
NowSecure, ORACLE, paloalto, RKVST
Red Hat, [illegible], RELIZA, revenera
REVERSINGLABS, Rezilion, SAP, SCANOSS
SECURESTACK, ShiftLeft, snyk, sonar
sonatype, SYNOPSYS, TIDELIFT, Trust Source
vmware, vdoo A JFROG COMPANY, VERACODE, nexB



Supporters

CycloneDX Supporters

apiiro, Contrast, FORTRESS, ION CHANNEL
KONDUKTO, LOCKHEED MARTIN, NowSecure, OWASP
Rezilion, servicenow, sonatype, vdoo A JFROG COMPANY
XPERI



Bloomberg the Company & Its Products ▾ | Bloomberg Terminal Demo Request | Bloomberg Anywhere Remote Login | Bloomberg Customer Support
Bloomberg
Middle East Edition ▾ Sign
● Live Now Markets Economics Industries Technology Politics Wealth Pursuits Opinion Businessweek Equality Green City
LIVE ON BLOOMBERG

Business

New Research Finds 73% of Organizations Have Significantly Increased Their Software Supply Chain Security Efforts as a Result of

August 9, 2022 at 4:05 PM GMT+3

New Policies & Standards

SLSA (Supply Chain Levels for Software Artifacts)

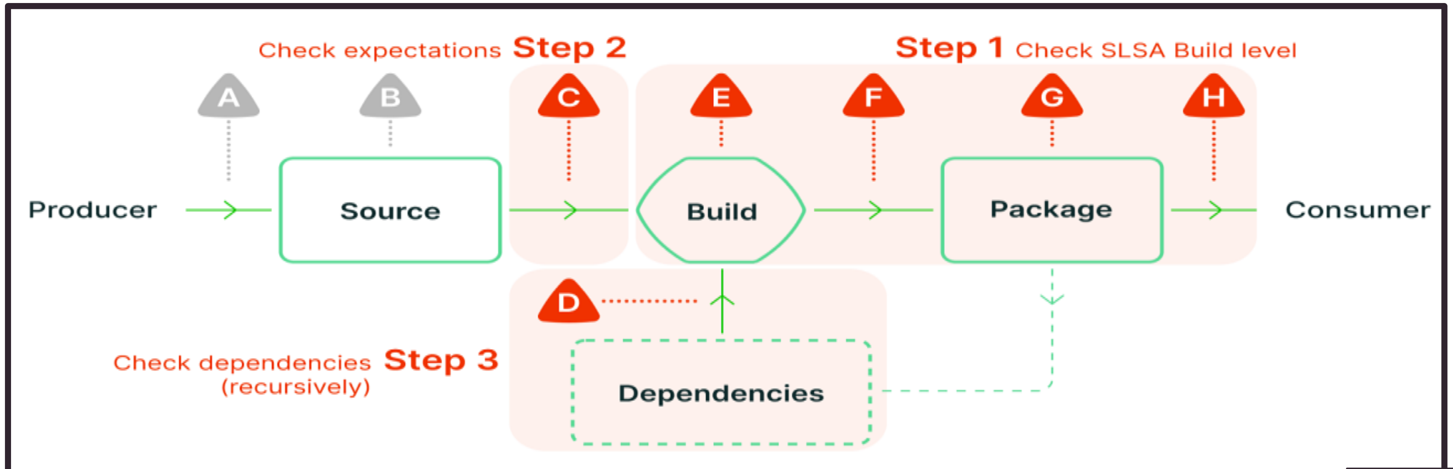
https://slsa.dev

An industry collaboration

SLSA is led by an initial cross-organization, vendor-neutral steering group committed to improving the security ecosystem for everyone.

Part of the Open Source Security Foundation

Source & artifacts integrity



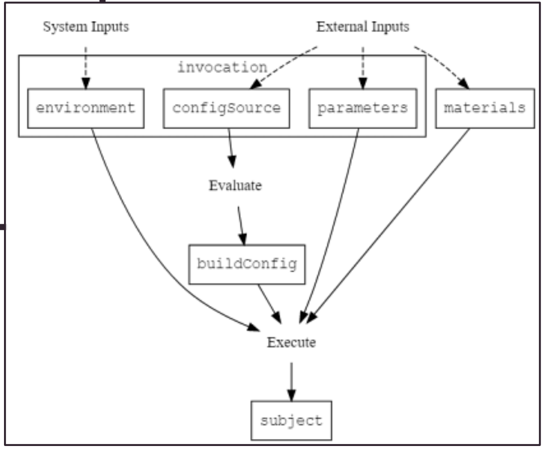
Check expectations Step 2
Step 1 Check SLSA Build level
A
B
C
E
F
G
H
Producer
Source
Build
Package
Consumer
D
Check dependencies Step 3
(recursively)
Dependencies

SOURCE THREATS
- A Submit unauthorized change
- B Compromise source repo
- C Build from modified source

DEPENDENCY THREATS
- D Use compromised dependency

BUILD THREATS
- E Compromise build process
- F Upload modified package
- G Compromise package repo
- H Use compromised package

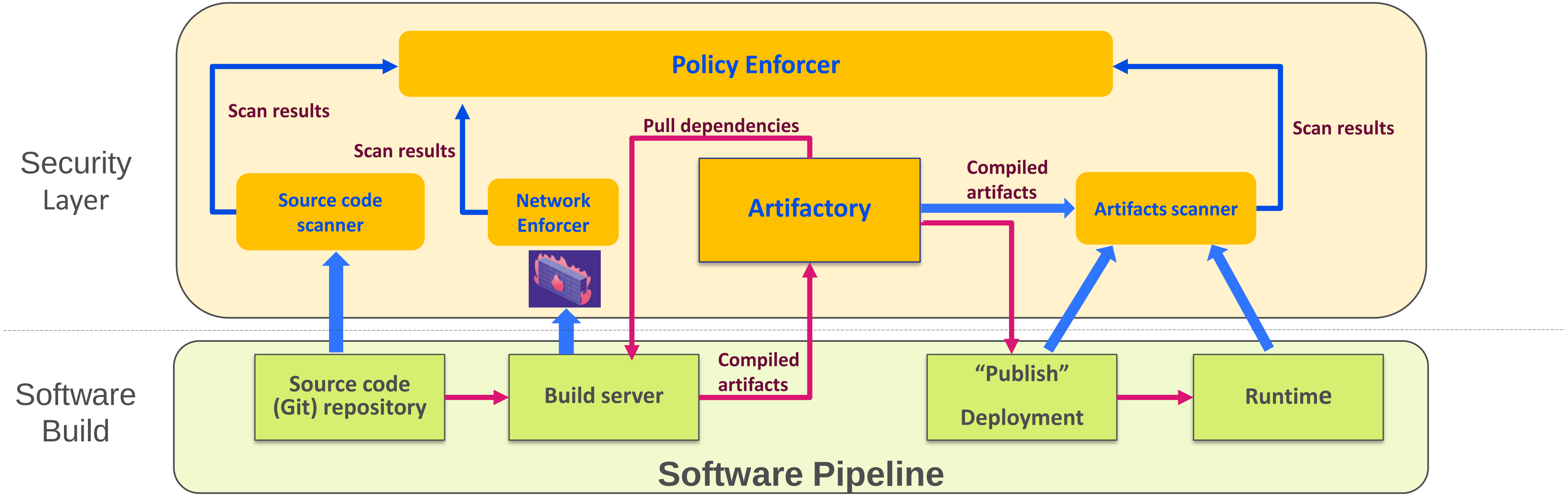
Provenance



SLSA: Enable **SLSA level 4** by producing SBOMs

Secure Software Development Life Cycle

== “Cleanroom”



CHECK POINT™

Few words about Generative AI

YOU DESERVE THE BEST SECURITY

2023
THE YEAR OF AI

MIDJOURNEY
All about imagination

OpenAI/Whisper

Google DeepMind

OpenAI

AI DUNGEON

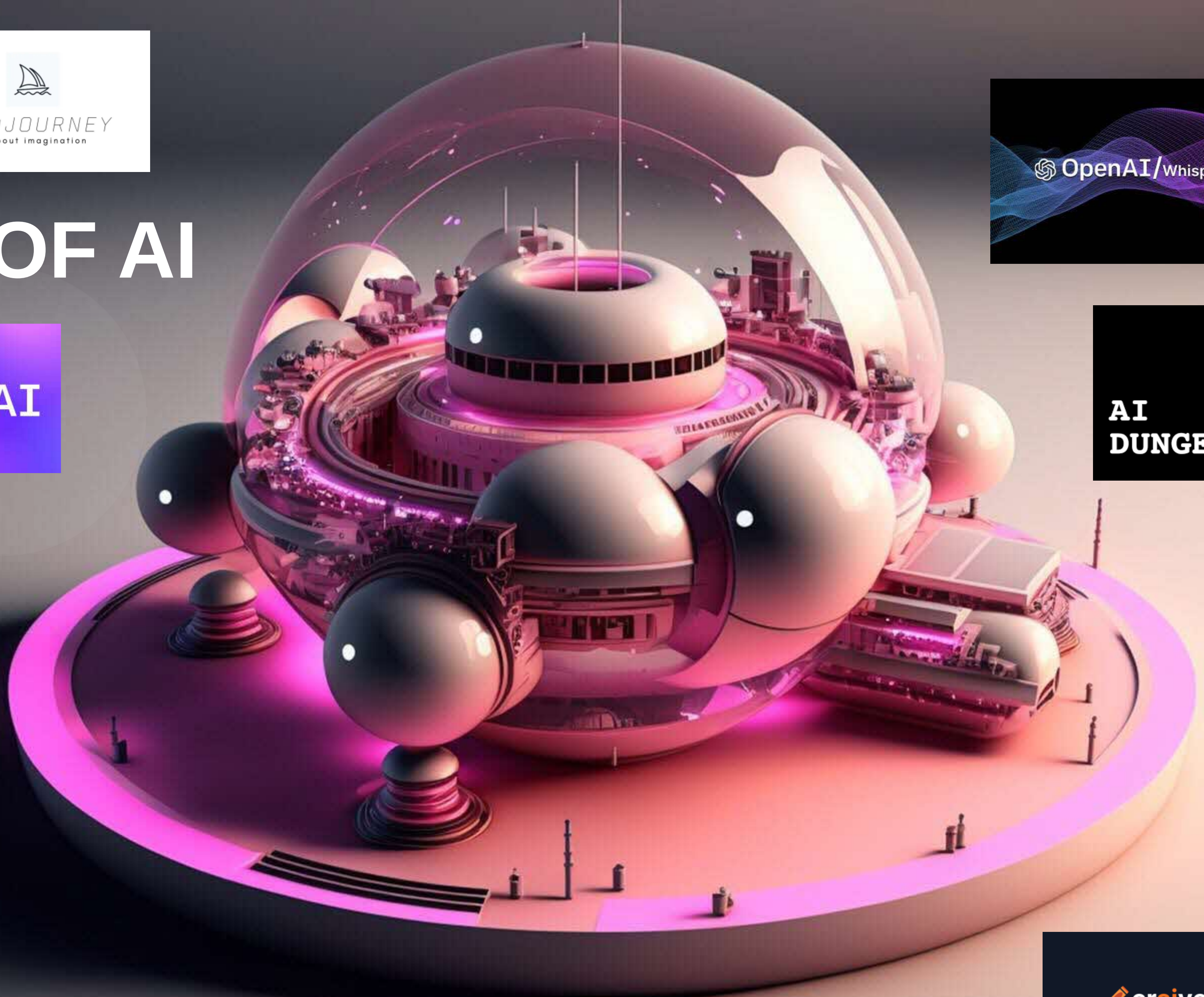
BARD AI

DALL·E 2

GitHub Copilot

DeepMind ALPHA CODE

craiyon



CHECK POINT™

AI Technology Trends

Current and Future effects on Cybersecurity

Shaping the “next normal” of human experience

- Human-machine Interfaces in Natural language
- Generative AI for extreme automation of usability and productivity

Unparalleled threat prevention

- AI-powered Security and Threat Prevention to find anomalies
- Unprecedented scale, speed and efficiency

AI and emerging cyber threat

- Attackers will use AI
- Secure vulnerabilities in the AI Technology

Data as a Strategy

- **Data first mind-set**
- Automate, scale and re-use

ChatGPT - Risks

- ChatGPT usage has cyber security Implications..
- Employees are eager to take advantage of Generative AI

- Risks:
  - Leakage of sensitive data
  - Leakage of code
  - Supply chain attack (code poisoning)
  - Leakage via 3rd party SaaS plugins (AI-based)
- Opportunities:
  - Data-Leakage solutions, Hashing PII data
  - Prompt inspection with AI
  - Local LLM – privacy, security, costs

Security Operations will be Augmented & Automated

Generative AI can assist in automating security operations daily tasks

- Threat Intelligence:
  - Analyze news - identify emerging threats and patterns
- Incident Response:
  - Categorize, prioritize, and analyze security incidents
  - Automated workflows & incident response
- Security Policy:
  - Ensuring policies enforced consistently across the organization
  - Alert policy violations
  - Recommend remediation & actions
  - Create zero-trust networks
  - Resolve tickets
  - Assist projects
  - Optimize resources - activate security blades on demand

- ➢ **“Why many users complain about Zoom connectivity?”**
- ➢ **“Am I impacted by CVE-2023-4852?”**
- ➢ **“Please solve ticket SR84215”**

Enterprises will isolate their Data in walled gardens

- Data will become an intellectual-property
- Enterprises will harness data-first strategy
- Companies will isolate their data
- Enterprises will accumulate huge amounts of raw data
- Un-reasonable to upload to cloud (amounts, privacy, regulations)
- More local processing AI power – at the Edge

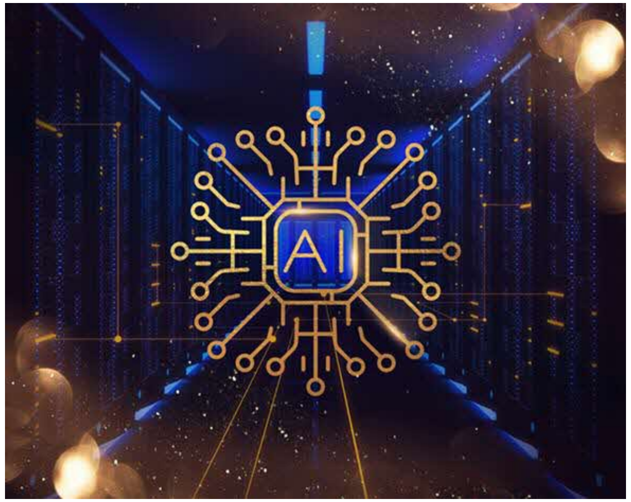
Opportunities:

- GPUs (LLMs) @ Edge
- Personalized adaptive security, Whitening traffic

New types of attacks will emerge

- AI models becoming a target
- Adversaries re-engineer how AI trained & operates
- Guess weaknesses by the input and results
- Poison the data trained, mis-information, unbalanced data
- Offensive Cyber, DeepFake (voice, video, chat, e-mail)

- Opportunities:
  - Polymorphic protections with GenAI – gain resiliency
  - AI ‘Shield’



Machine-to-machine interactions (Auto-GPT)

- Generative-AI will replace back-office tasks
- Human roles will be automated
- Future will be machine-to-machine (AI-to-AI) interactions
  - E.g. call center: customer support request will trigger actions in multiple systems
- AI will code, build and deploy fixes
- AI will instantiate infrastructure..
- Attackers can fool systems to orchestrate devastating attacks
- .. harmless workloads could freak out

Opportunities:

- Prompt security – input & output..
- Identify intent

Data Becomes a Strategy

- Data mindset
  - **Data-first** mind-set = competitive edge
  - Reinforcement Learning Human Feedback (RLHF)

- AI mindset in products operations
  - Code generation
  - Code testing
  - Protections generation
  - Performance optimization
  - AI @ edge (GPUs at firewalls, endpoints) - privacy, security, Costs

CHECK POINT™

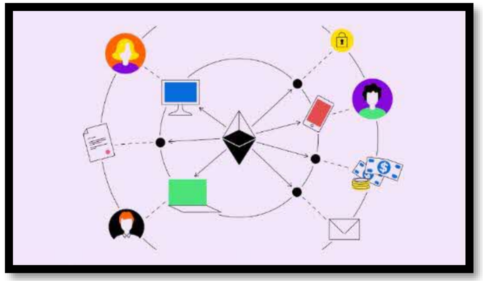
Web 3.0 & Blockchain

AI-Empowered Security

YOU DESERVE THE BEST SECURITY

Web 3.0 building blocks

Decentralized application

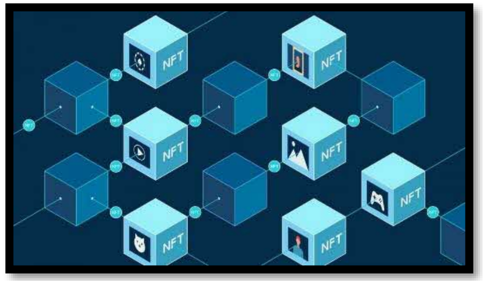


Mobile App

Smart Contract

Backend App

Blockchain System



Hosted Cloud

Blockchains Attacks Categories

Category A

Attacker produces malicious Smart Contract (e.g Currency)

Category B

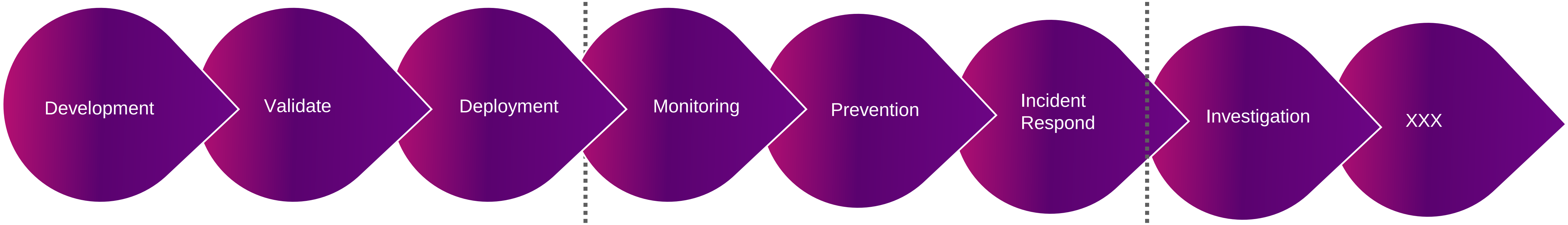
Attacker targets vulnerability in a legitimate Smart Contract

Web3 Security – 3 main categories

Before uploading the smart contracts

Smart contracts on chain / Run time

After the fact



Smart Contracts Audit

Monitoring & protection

Forensics & compliance

Top companies

$15M

CERTIK

PeckShield

SLOWMIST

CYVERS

ironblocks

HYPERNATIVE

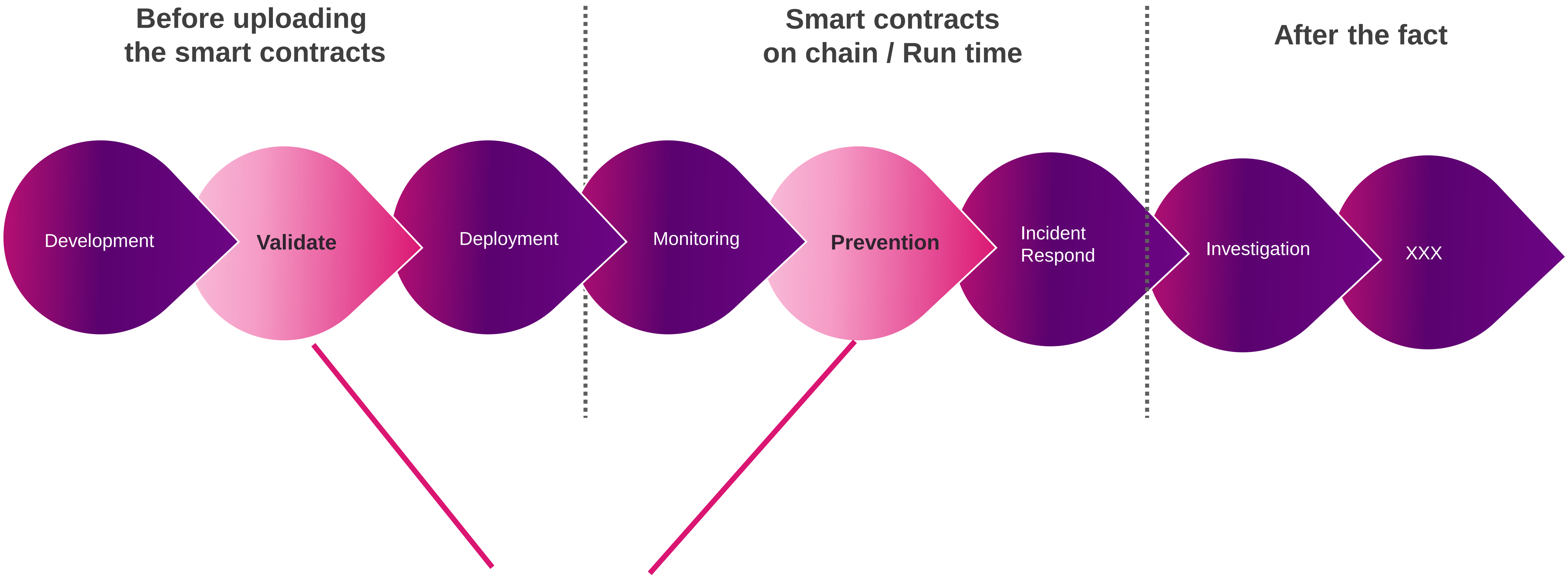
Forta

Chainalysis

CIPHERTRACE

ELLIPTIC

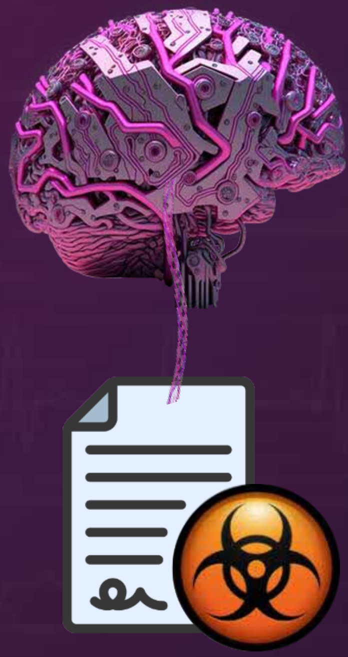
Web3 Security – 3 main categories



Goal is to **prevent** the Web3.0 attack before it happens

Securing the Smart Contract

Solution A



API to scan malicious Smart Contract

Solution B

AI 'Shield' to protect Vulnerable Contracts

CHECK POINT™

Summary

- **Software Life Cycle = “Cleanroom”**
- **Blockchain Smart Contract is the weakest link**
- **Generative AI is shaping the “next normal” of human experience**

YOU DESERVE THE BEST SECURITY

CHECK POINT™

THANK YOU

YOU DESERVE THE BEST SECURITY