ALL DAY DEVOPS

NOVEMBER 6, 2019

Kumar Mathialagan & Shiva Nouzari

Supply Chain Security – Where, What and How?

ADDO
ALL DAY DEVOPS

Hello!

“Cyber Security aficionados focusing to embed security into every aspect of the supply chain. Experience implementing security with Agile and DevOps frameworks.”

SHIVA NOUZARI

Supply Chain Security: Where, What, How

TRACK: DEVSECOPS

KUMAR MATHIALAGAN

Supply Chain Security: Where, What, How

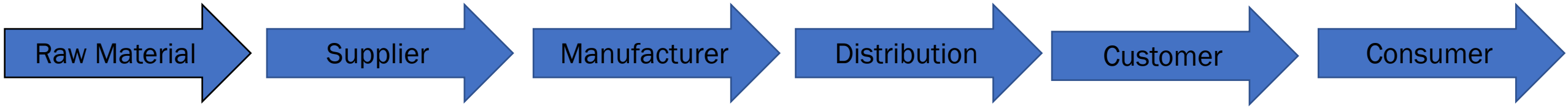
TRACK: DEVSECOPS

ADDO
ALL DAY DEVOPS

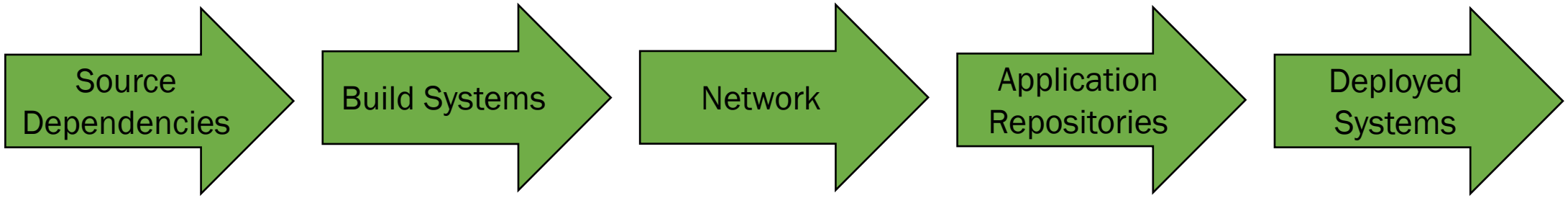
Objectives

- ❑ Overview of a Software Supply Chain
- ❑ Impact of Supply Chain Attack
- ❑ Supply Chain Attack Threat Modelling
- ❑ Controls to protect from Supply Chain Attack

Traditional vs Software Supply Chain



"A supply chain is the link between entities such as producers, vendors, transportation, companies, distribution and consumer to produce and distribute a product or service."



"Software source, components and packages that enter delivery pipeline at different stages and impacts the delivered output"

Image Courtesy - https://www.docker.com/blog/secure-supply-chain-kubernetes-2/

Software Supply Chain Security

Cyber security should be considered a subset of software supply chain and is focused on the management of cyber security requirements for information technology systems and software products. The two major security risks that affect the software supply chain include:

- ❑Disruptions that delay software delivery
- ❑Infusion of malicious or inferior software components

Attack targets:

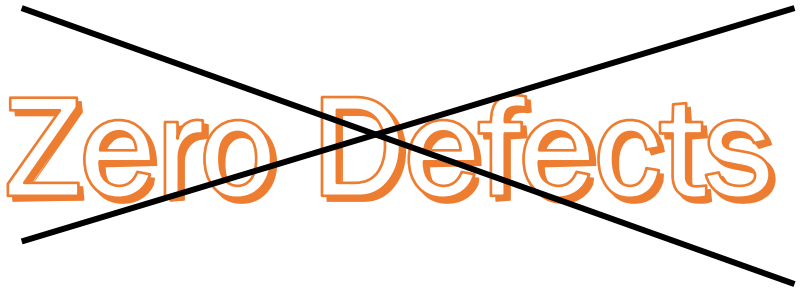
PII –SPII | Credit card information | Competency |Credentials |Business data

Why supply chain attack?

Outsourcing

Open Source

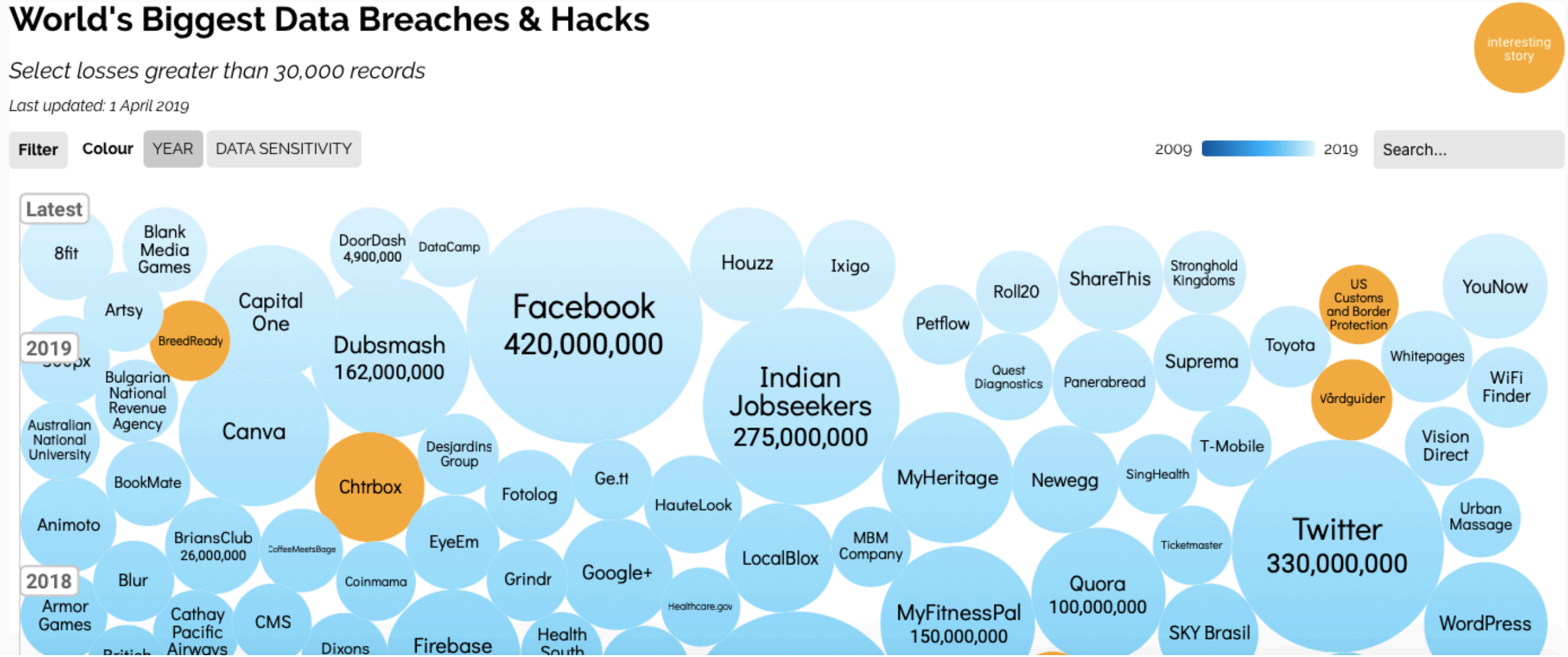
Commercial off-the-shelf



- ❑ Manipulation of design specifications
- ❑ Alterations and manipulation during distribution
- ❑ Modification during development
- ❑ Security Domain Specific Attack

ADDO
ALL DAY DEVOPS

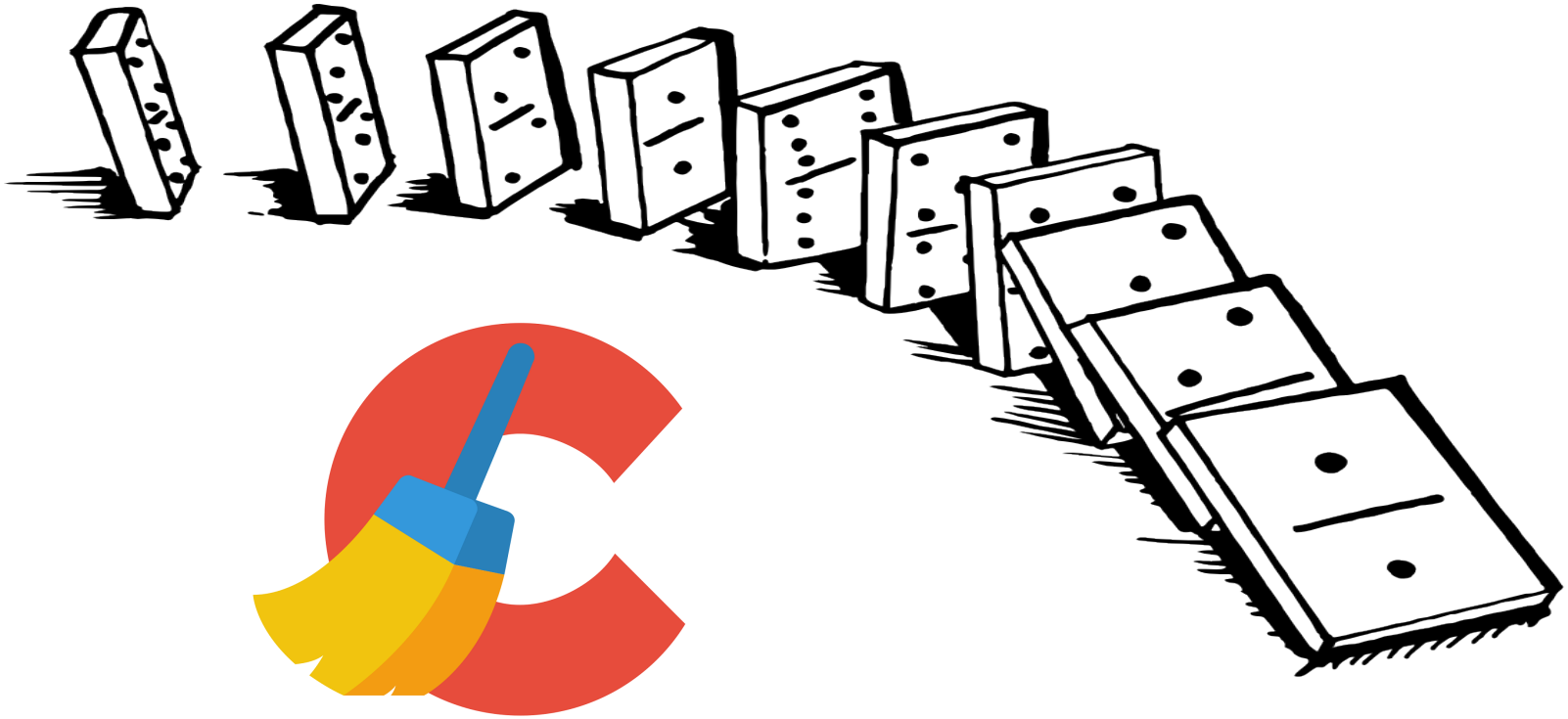
The threat is real...



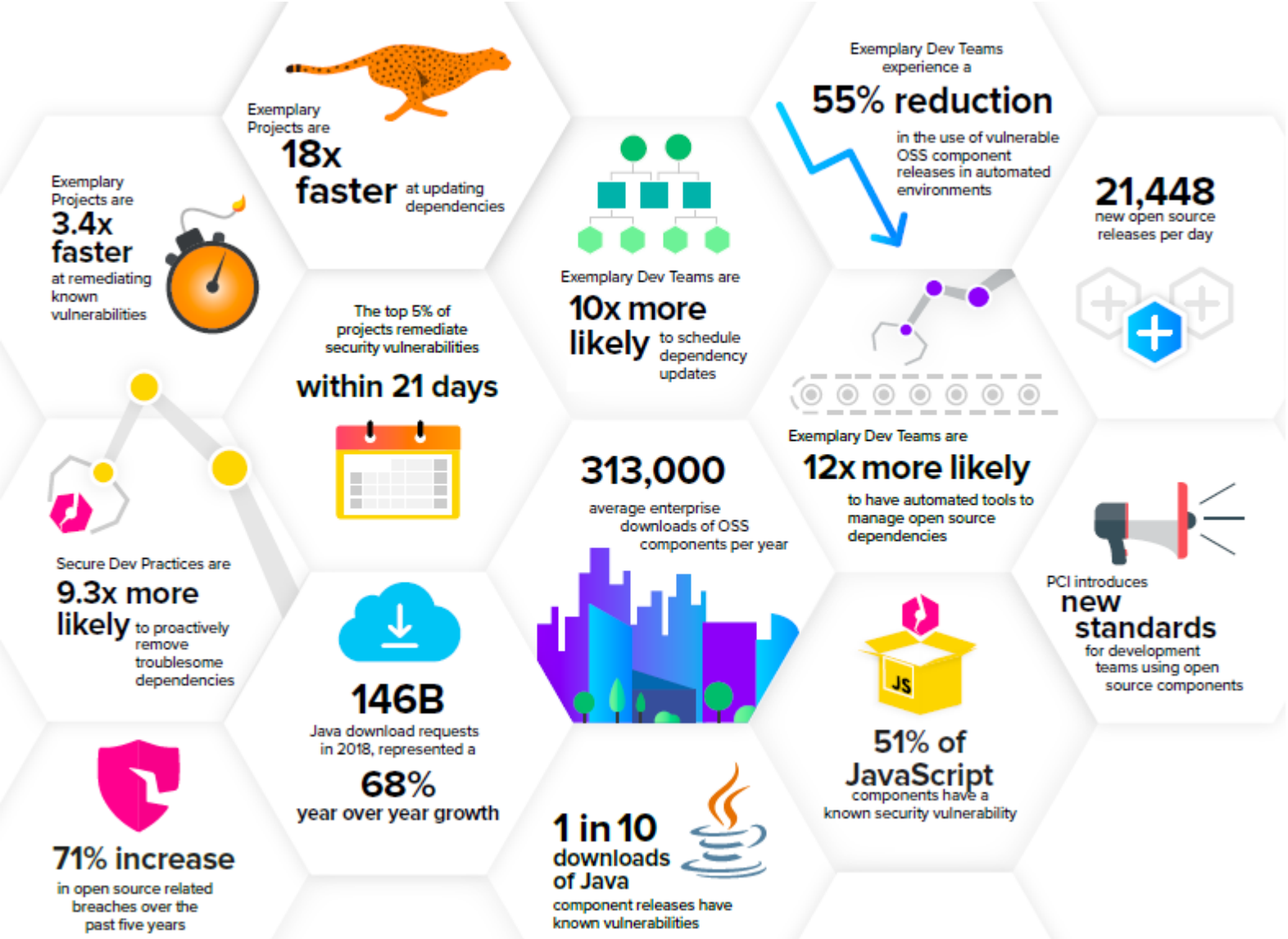
Infographic Courtesy:
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Recent Supply Chain Attacks

"Exploit vulnerabilities in the most basic trust model governing the the code user run on machines"



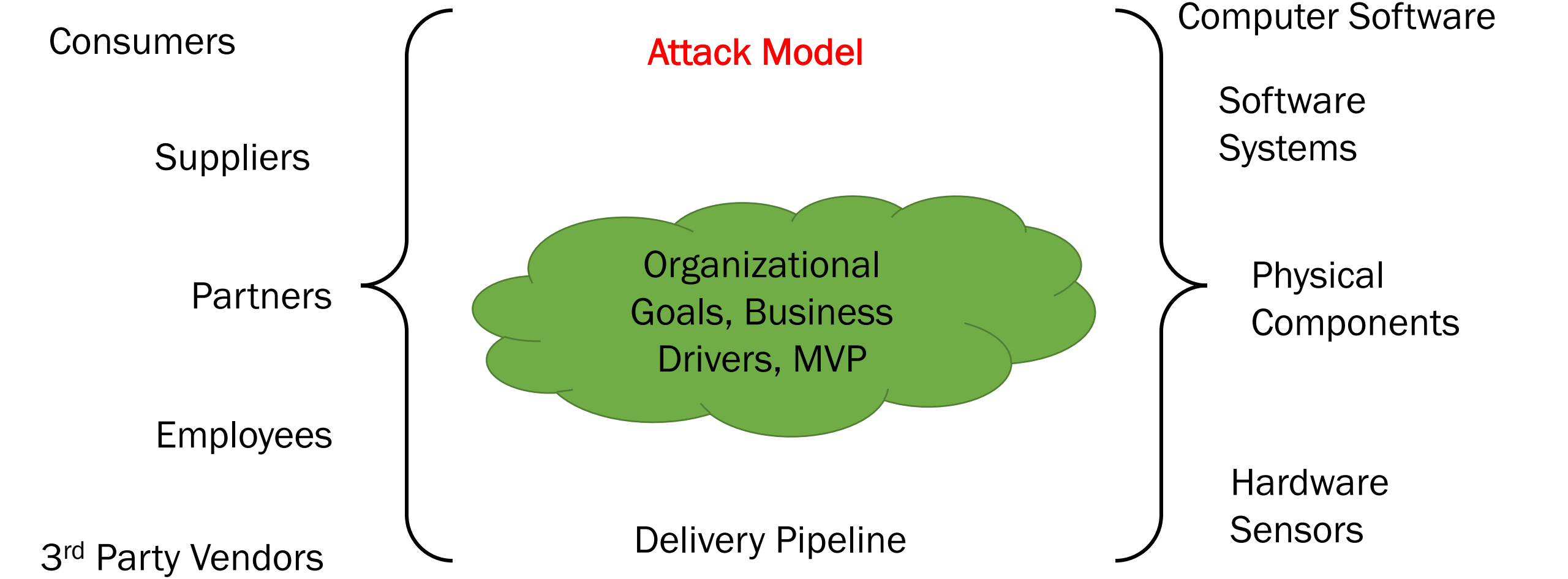
Some Facts & Figures



- 75% growth in supply of open source component releases over the past two years
- 68% year over year growth in download requests from the Central Repository to 146 billion
- 18x faster median time to update dependencies for exemplary open source components
- 71% increase in confirmed or suspected open source related breaches since 2014

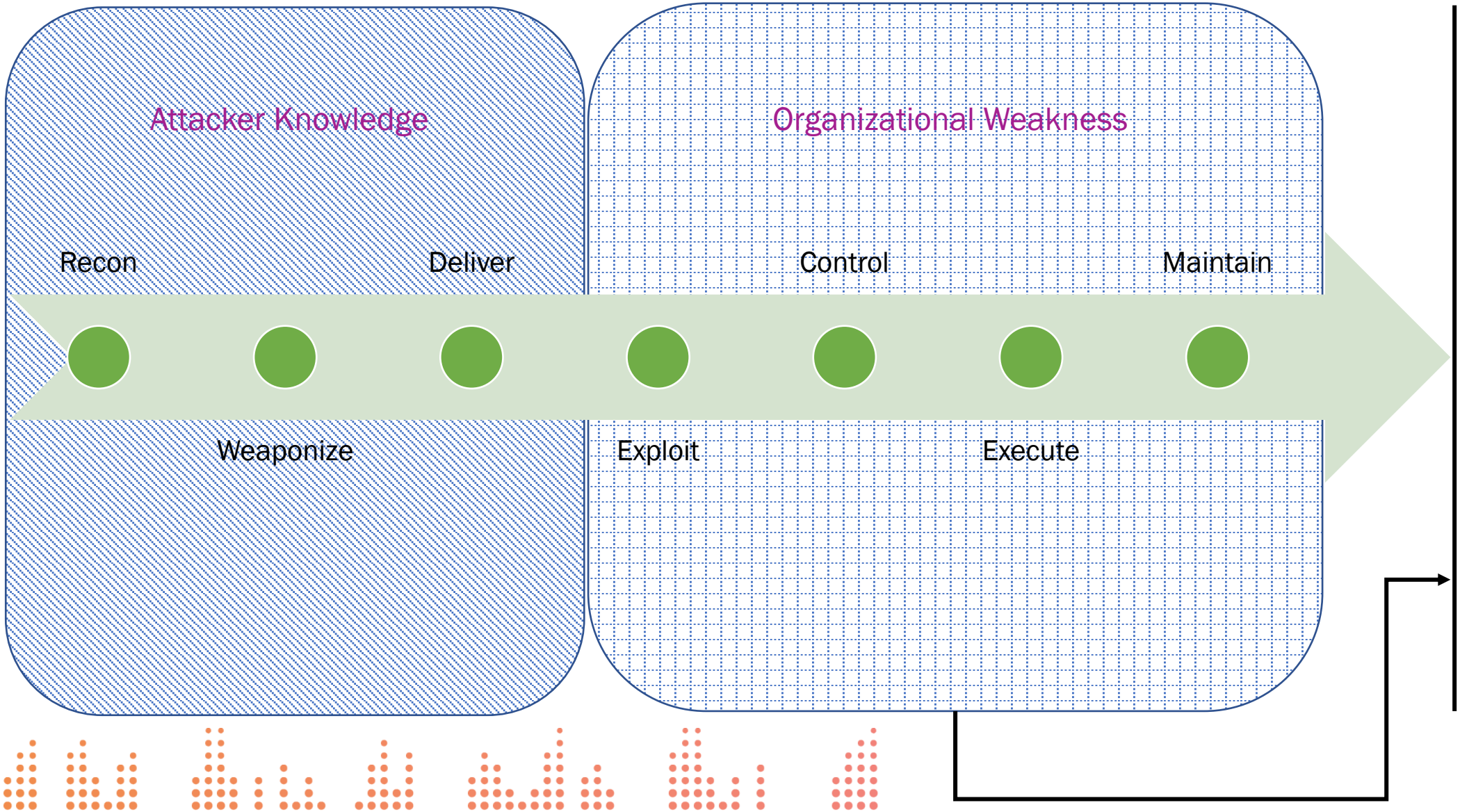
Source: 2019 State of the Software Supply Chain

Supply Chain Attack Process



ADDO
ALL DAY DEVOPS

MiTRE Attack Chain



Supply Chain Attack Model

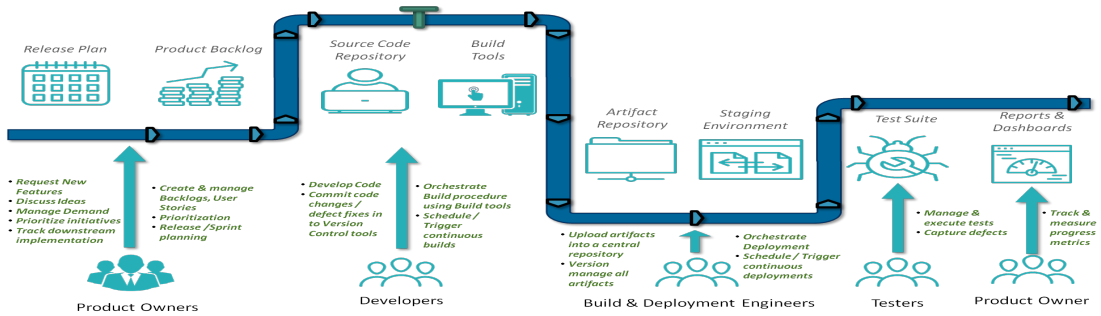
Software Suppliers

CSP's / Data Analytics

3rd Party Service Providers

Vendors

Source Control | Build Tools | Containerization | Configuration Management | Monitoring



Software Delivery Pipeline

Component Phase → Subsystem Phase → System → Production

E-commerce website

Attacker

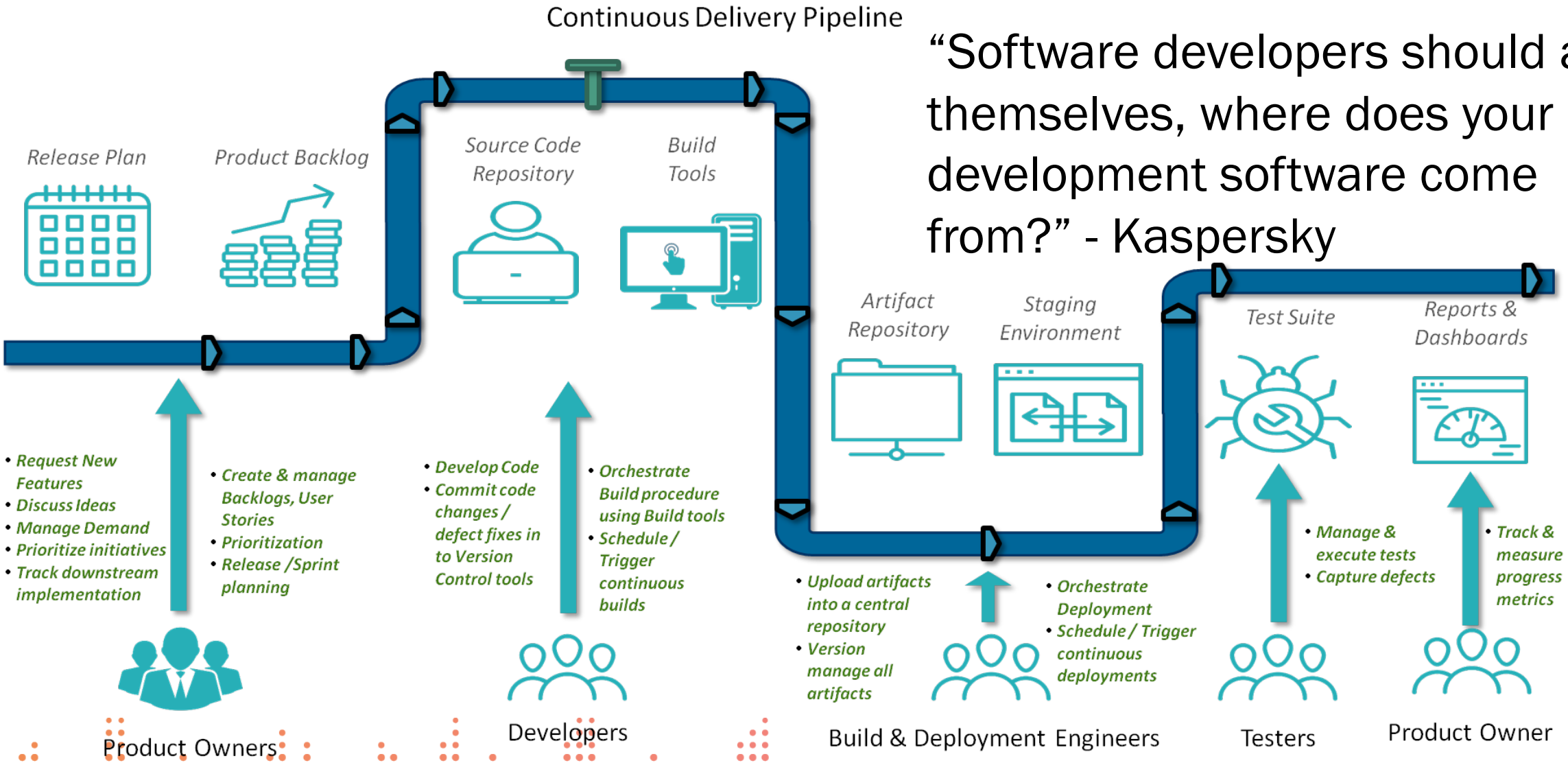
Reconnaissance → Experiment → Exploit → Command & Control

Customers

Customers

Customers

Software Delivery Pipeline - Sample



"Software developers should ask themselves, where does your development software come from?" - Kaspersky

Software <<Pipeline>> AppSec ⟷ Tools

Source Control

Containerization

Monitoring

Build Tools

Config. Management

Pipeline Phases

Component Phase

Subsystem Phase

System Phase

Production Phase

- Intake Process
- Triage
- Test
- Deliver

AppSec Pipeline Stages

Code Scan

Network Scan

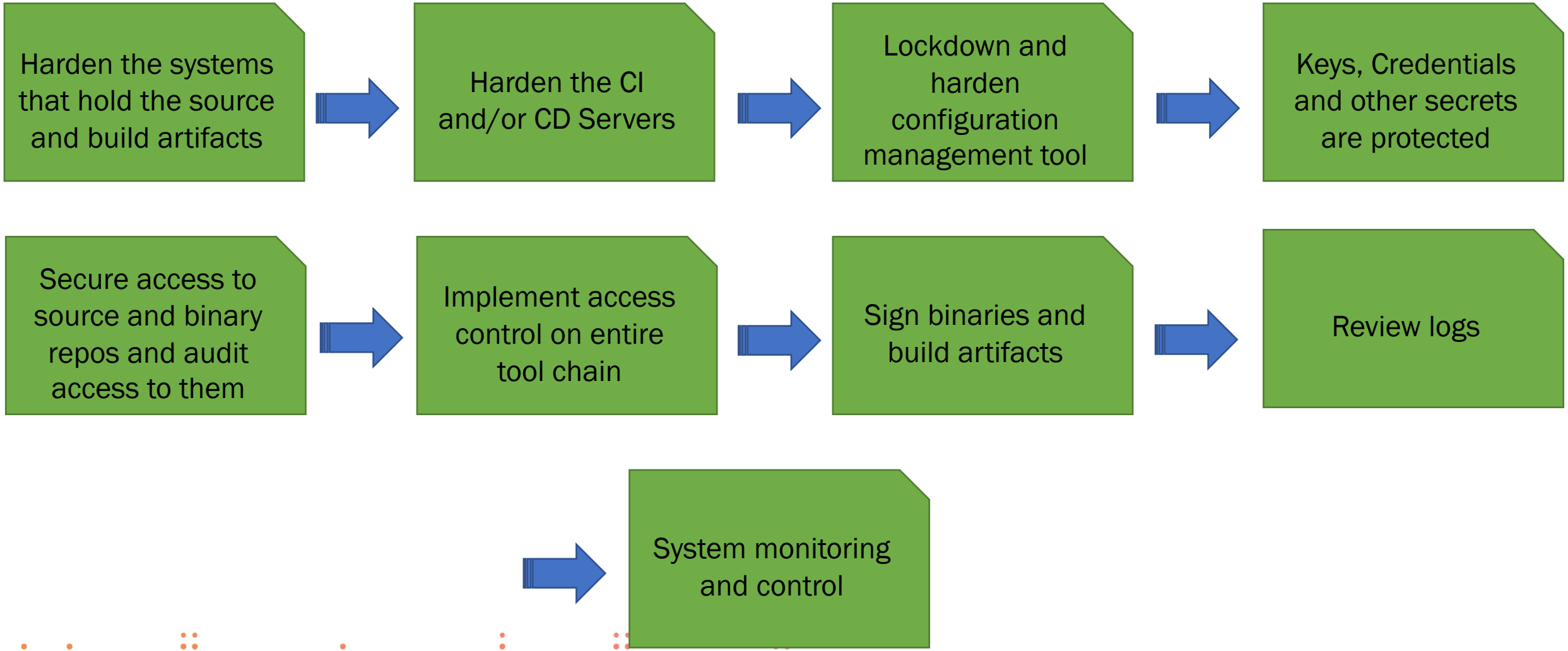
Penetration Test

Host Scan

API Testing

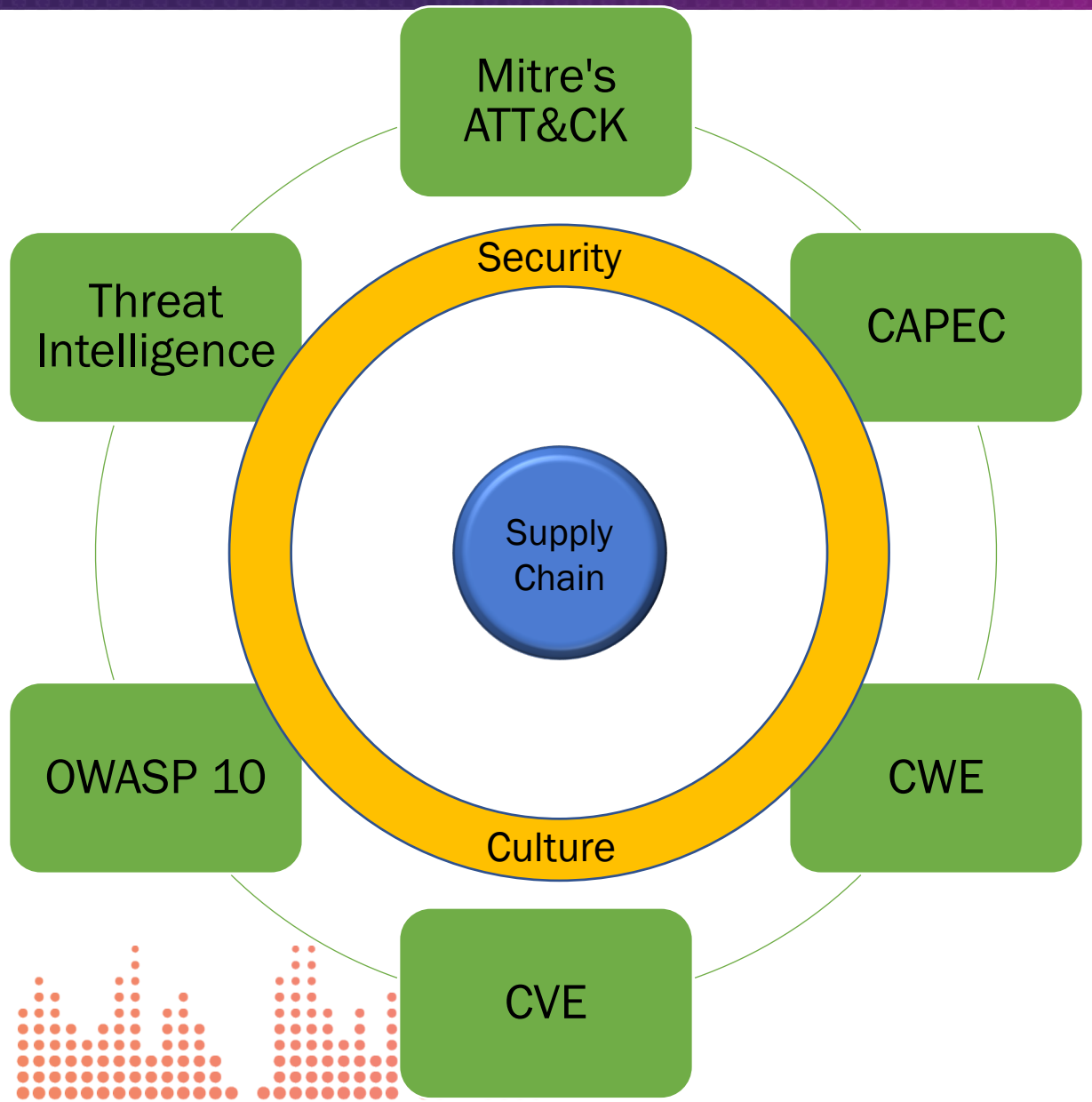
ADDO
ALL DAY DEVOPS

Continuous (*Secure*) Delivery



ADDO
ALL DAY DEVOPS

Supply Chain Protection Model



Security Culture and Controls

ADDO
ALL DAY DEVOPS

Basic and Default Security Framework

Software and Hardware Inventory

- Maintain CMDB
- Dev, UAT and Prod
- Infrastructure Details

Asset Classification

- Categorize assets
- Identify ownership
- Set custodianship responsibility

Plan Security Initiatives

- Risk Management
- Access Control Matrix
- Log Review and Monitoring

Security Testing

- Vulnerability Management
- Patching
- DAST and SAST
- Penetration Testing

Definitive Security Support System

Security Awareness

- Employee Awareness
- Customer education
- Security first culture

Supplier Management

- Security profiling
- Access Restriction
- Periodic Certification

Compliance

- PCI DSS
- BSIMM
- SA –CMM
- ISO 27001

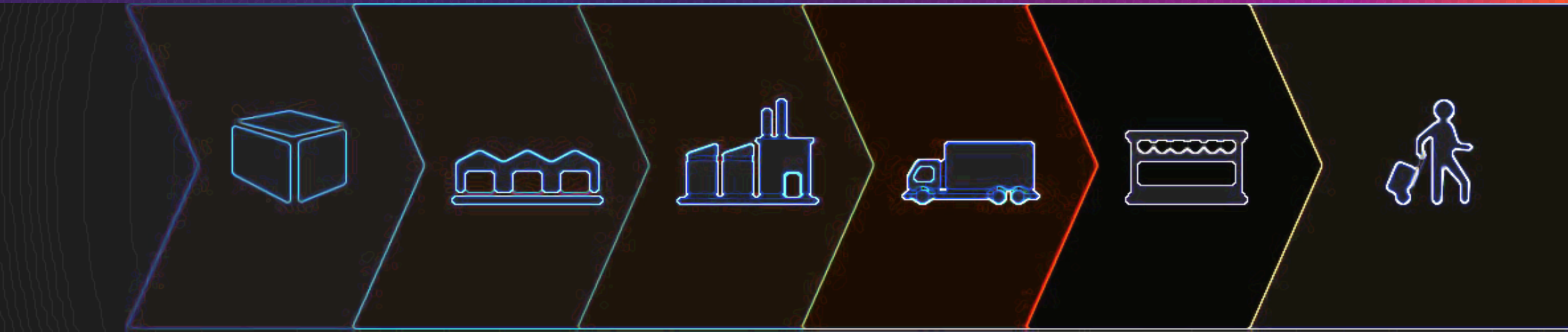
Operational Security

- BIA
- DR/BCP
- Set Operational Thresholds
- Risk Control Self Assessment

Conclusion

- Supply Chain Attack - Clear and Present Danger
- Multipronged Detection Mechanism
- Require Proactive Prevention Tactics
- Agile Security Monitoring
- Application Security Practices

ADDO
ALL DAY DEVOPS



Thank you!