APH10

NORDIC SOFTWARE SECURITY SUMMIT
NSSS.SE
THE SOFTWARE SECURITY REGULATION REVOLUTION

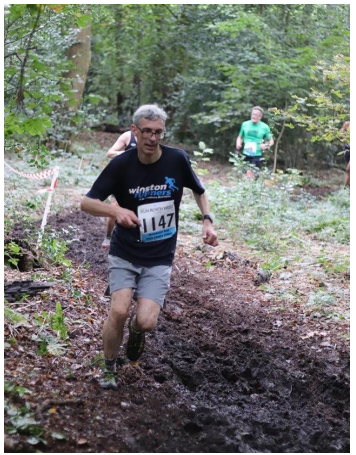
Empowering Organisations: Procuring a Secure Software Supply Chain

September 2024

Anthony Harrison (Founder)
anthony@aph10.com

APH10

- A career delivering mission critical solutions across multiple sectors
- Founder and Director APH10
- Open Source Software
- STEM Ambassador
- Mentor



CoderDojo

Agenda

- **Understanding the Supply Chain**
- **Empowered Development**
- **Conclusions**

Supply Chain Diagram

Raw Materials → Supplier → Manufacturer → Distributor → Retailer → Consumer

Software Supply Chain

THE APACHE SOFTWARE FOUNDATION

ECLIPSE FOUNDATION

Microsoft

THE LINUX FOUNDATION

aws

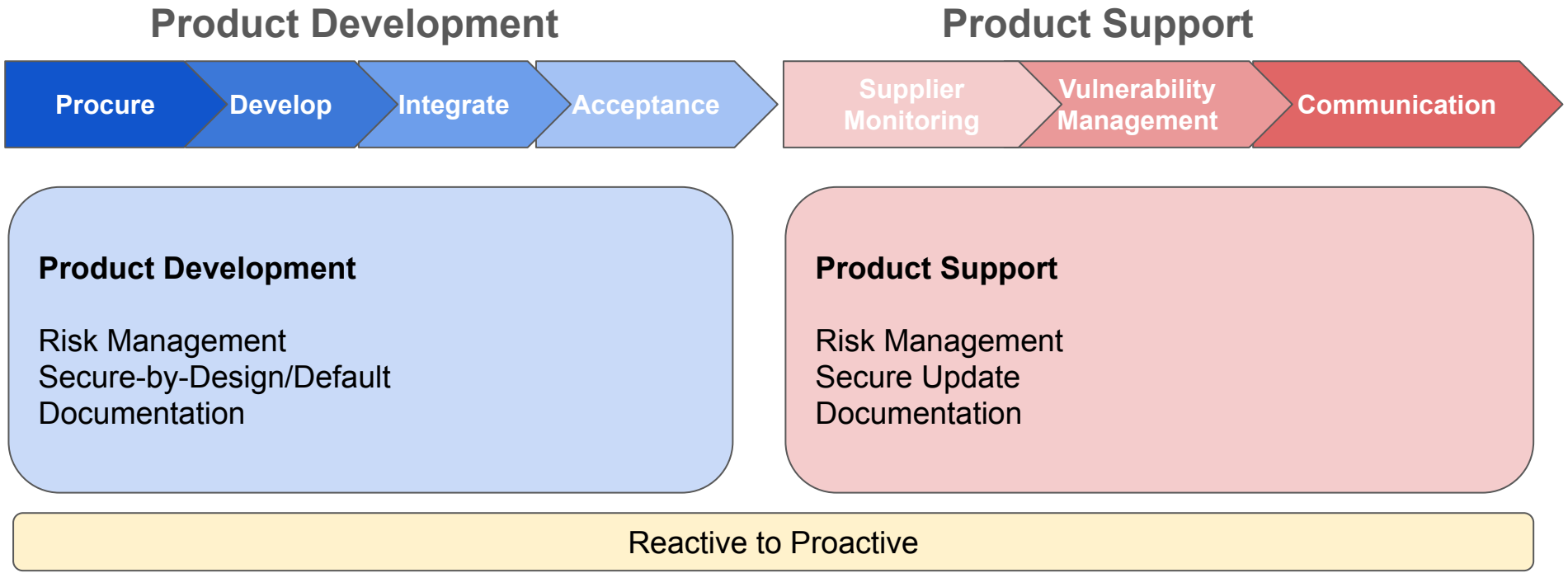
Developer / Foundation / Consolidator -> Integrator -> Customer

Understanding Software Supply Chain

- The traditional supply chain
  - Linear
  - Risks
    - Disruption
    - Quality
    - Failure
  - Alternative sources of supply
- Software Supply Chain
  - Non-linear
  - Risks
    - Disruption
    - Quality
    - Failure
  - Alternative sources of supply?

Understanding Software Supply Chain

Delivering an Empowered Life Cycle



What does good look like?

Product Development

- Secure by Design/Default
- Security Controls
- Control of supplier access

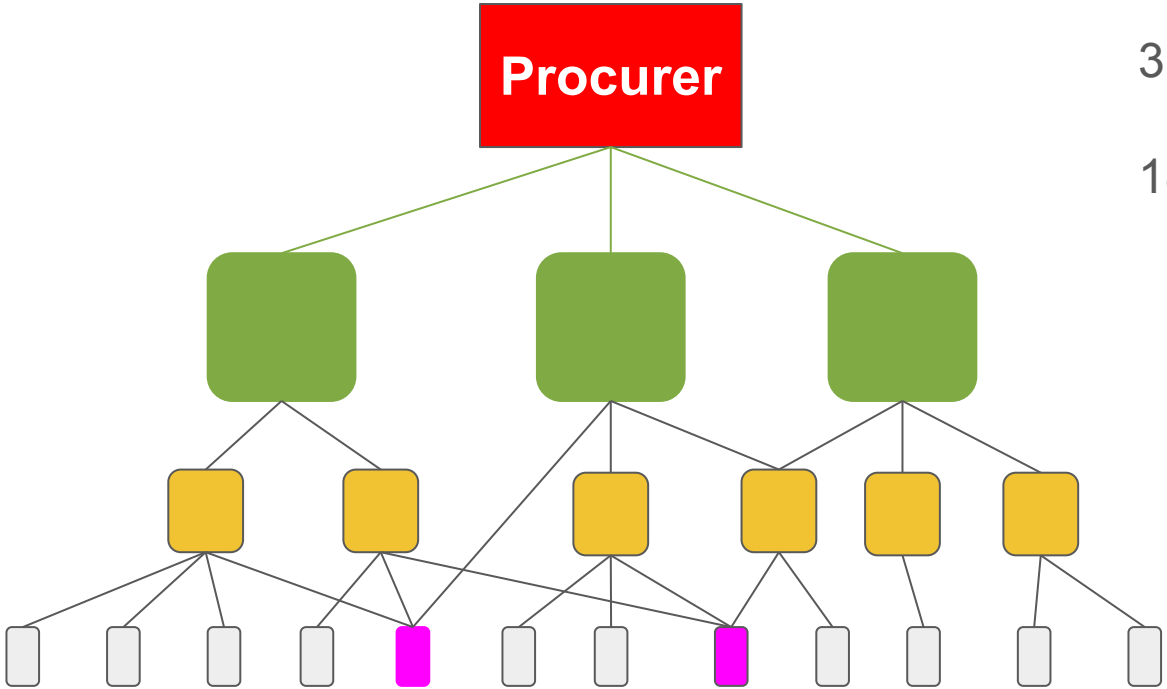
Product Support

- Vulnerability Management
- Incident Management
- Security Updates
- Customer Support

Organisation

- Secure Development Lifecycle
- Supplier Transparency
- Security Support
- Adopt Industry Standards
- Data Management

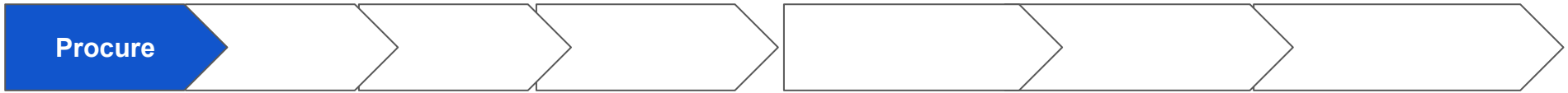
Supply Chain Relationships



3 Direct Dependencies

18 Indirect Dependencies

Procurement



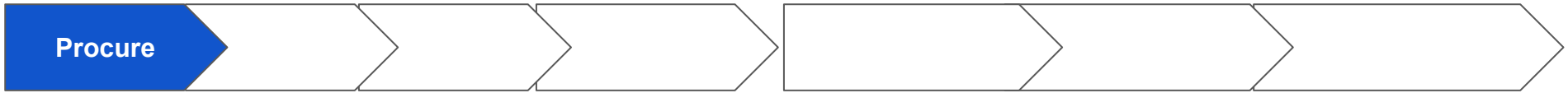
Multi-Disciplined Team

Evaluation

Selection

Negotiation

Procurement - Evaluation



Ask for an SBOM

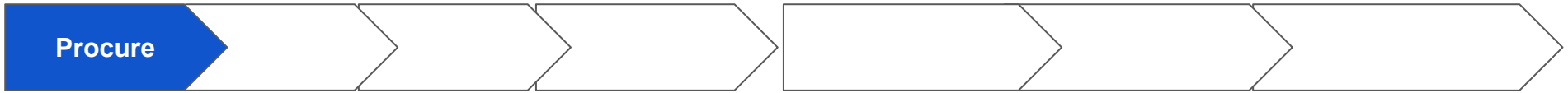
Key indicator of quality of software development

Recognise contractual constraints (NDA etc)

Which SBOM?

What's an SBOM?

Procurement - Evaluation



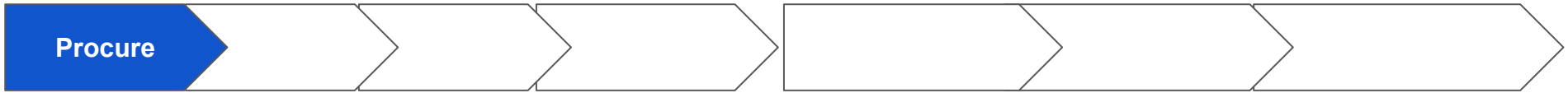
Need a Risk Management Process to assess SBOMs

Licenses, Component vulnerabilities, Component debt, Suppliers, Unmaintainable software, Unsupportable software

Share results with provider

- **Build a relationship**
- **Understand the viewpoint of product management and security**
- **Regular security update?**
- **How out of band/critical updates handled**

Procurement - Evaluation

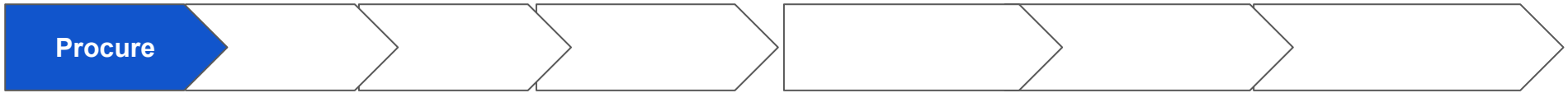


Understand why? Indicator of development practice

Explain the benefits of greater transparency

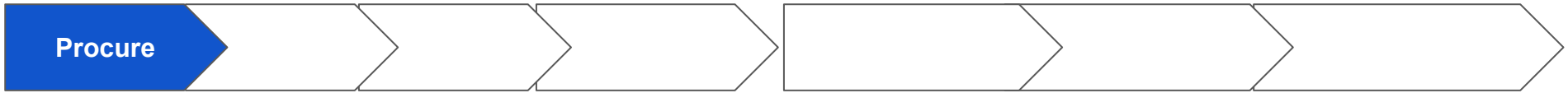
- **Build a relationship**
- **Understand the viewpoint of product management and security**

Procurement - Selection



- **SBOM won’t be only criteria**
- **Be transparent with how SBOMs used in evaluation**
- **Understand the key components of the whole supply chain not just the immediate/direct business relationships**
- **Understand business impact of failure of critical software suppliers**

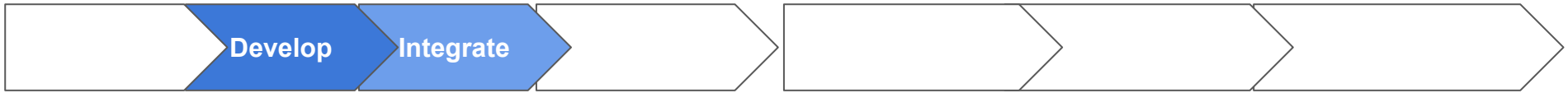
Procurement - Negotiation



Model Contract

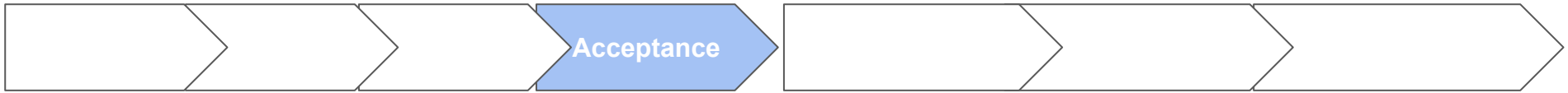
- **Expectations about timeliness and consistency of security support**
- **Secure by Design/Default and product capabilities**
- **Security Controls**
- **Supplier Access Management**
- **Expectations about behaviours and development practices**

Development and Integration



- **Continuous SBOM generation and monitoring**
- **Proactively share with upstream and downstream**
- **Understand and monitor changing risk profile**
- **Always know where you are so you can respond to stakeholders on demand**

Acceptance



DO

- Define criteria to identify which vulnerabilities need to be fixed
- Expect all KNOWN vulnerabilities to be assessed
- Work with all upstream and downstream partners to coordinate fixes

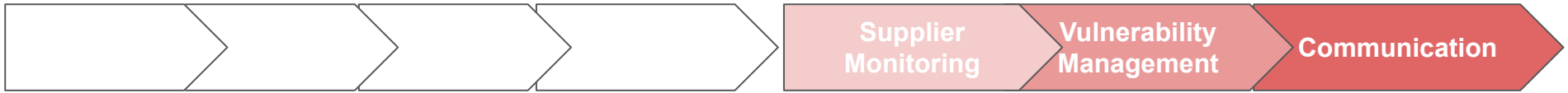
DON'T

- Expect NO KNOWN VULNERABILITIES
- Demand fix all HIGH or CRITICAL vulnerabilities
- Demand fix immediately

Define criteria in Contract

Understand that vulnerabilities are dynamic and are constantly appearing/changing

Operational



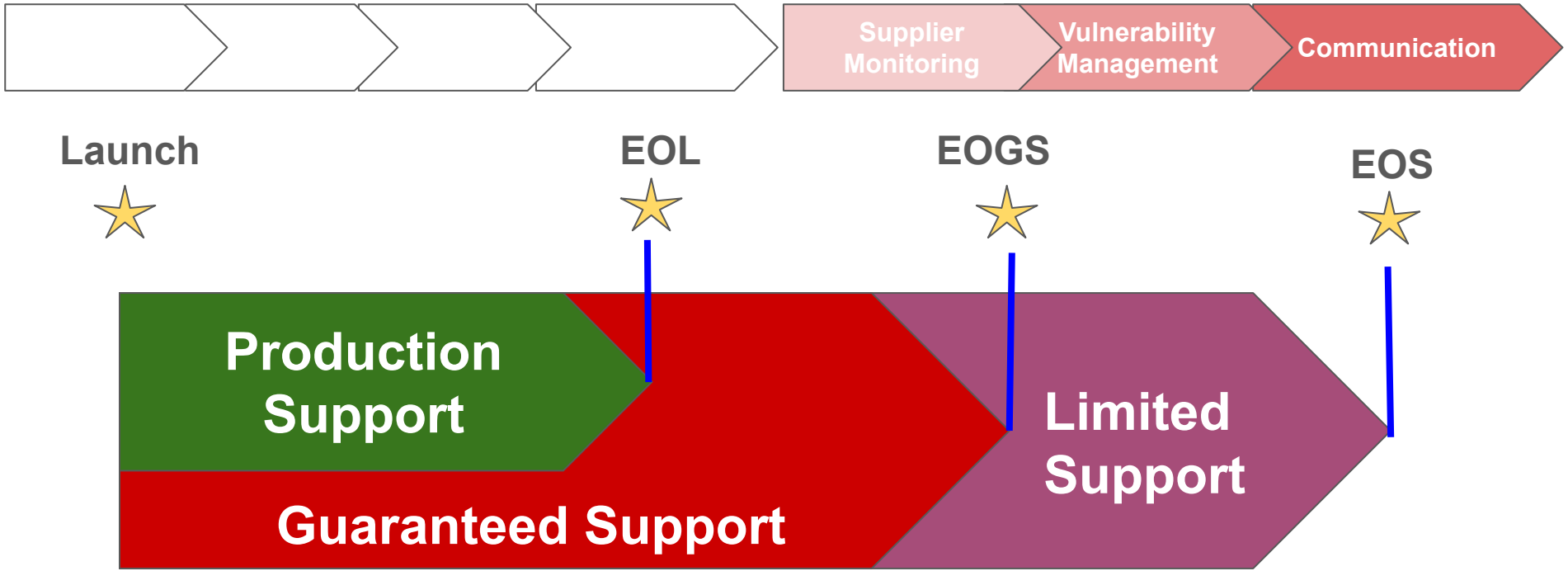
Same approach to risk management as during development

Ensure contract has identified actions related to vulnerabilities
- **If new vuln identified (proactively report)**
- **If new vuln and not exploitable (share assessment)**
- **If new vuln and expolit (proactively share and agree remediation approach)**

Supplier monitoring and incident reporting

Monitor EOX
- **Start looking at approach probably 2 years before EOL/EOS**
- **Risk and Service life will dictate approach**

Operational - EOX



EOL - Product no longer sold

EOS - Product no longer supported

EOGS - Product no longer guaranteed support

Conclusions

- The need for greater transparency to provide a clear picture of what is being acquired
- How to perform an effective due diligence on suppliers to ensure that expectations are understood by all parties
- The importance of relationships and partnerships within the supply chain
- The approach to be followed to ensure effective oversight of the supply chain is performed to manage the evolving risk landscape

GitHub

LinkedIn

APH10

Anthony Harrison
anthony@aph10.com