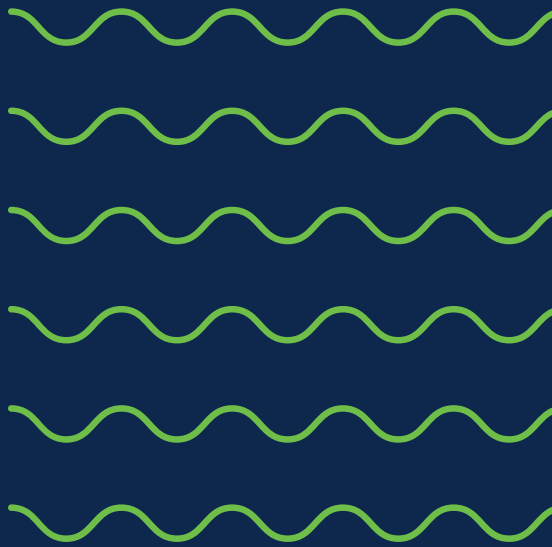
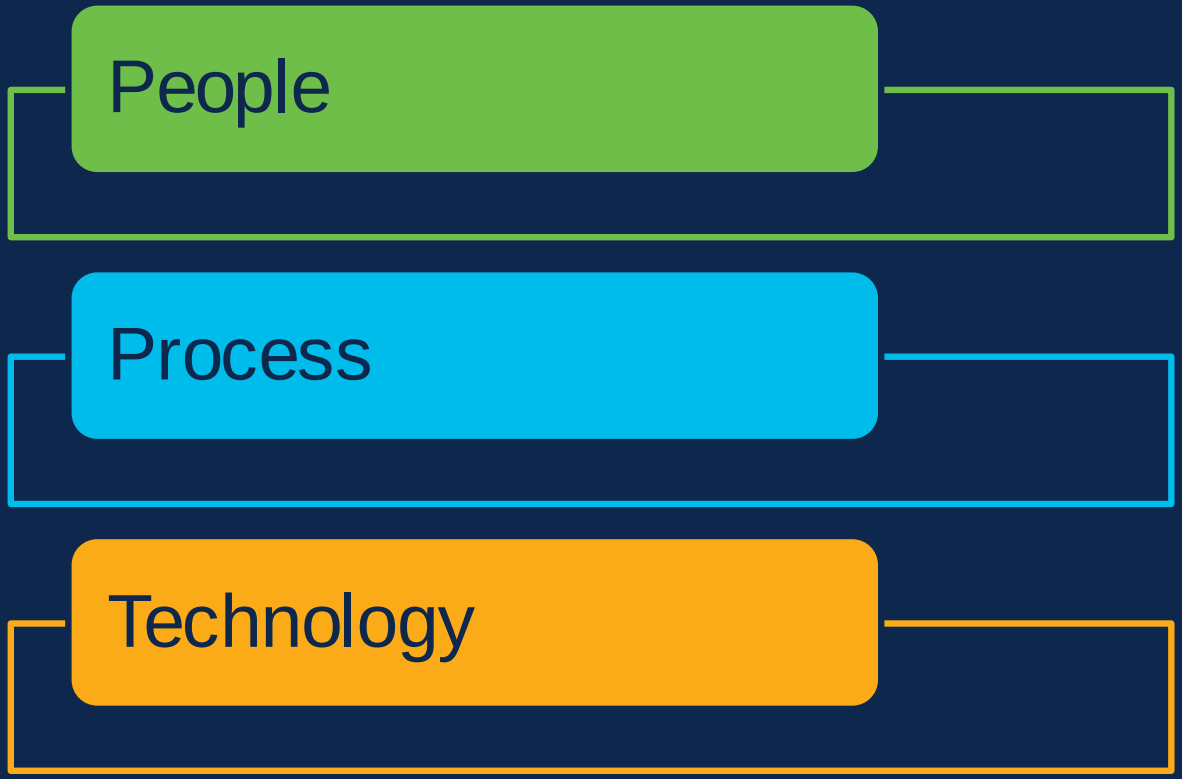
CISCO
SECURE

CISCO The bridge to possible

Securing the Supply Chain Without Drowning In the Data



Wendy Nather
Head of Advisory CISOs, Cisco
@wendynather



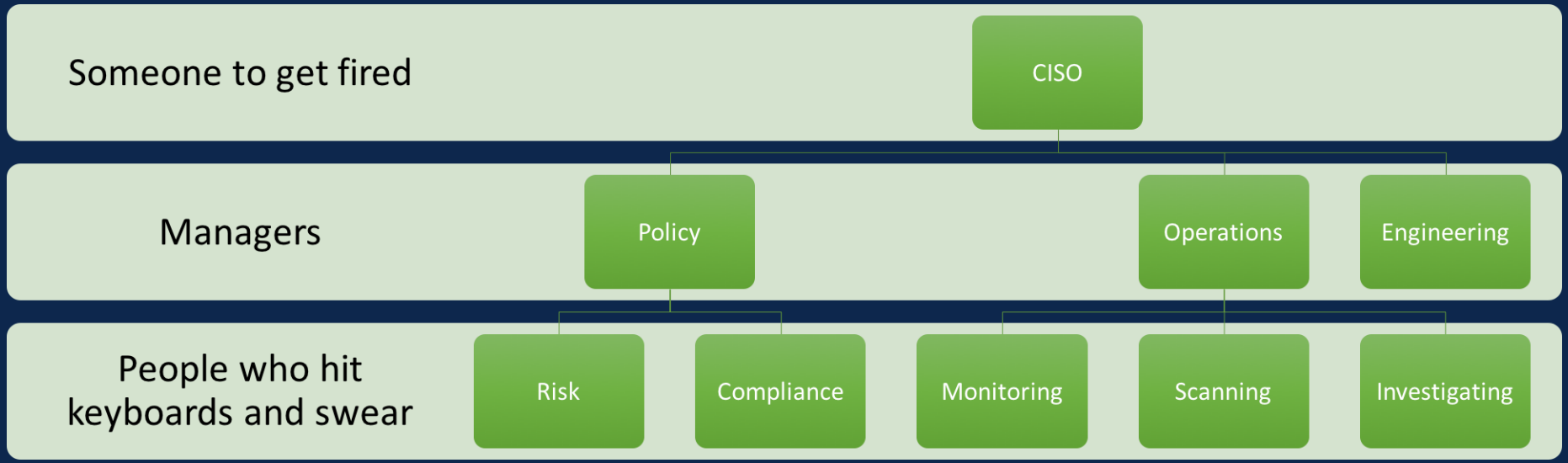
People

- Relationship
- Incentives
- Expertise
- Influence

People

- Relationship
- Incentives
- Expertise CERTS
- Influence

Process



Process

- Knowledge
- Controls
- Practices

Process

- Knowledge CERTS
- Controls CERTS
- Practices CERTS

cisco SECURE

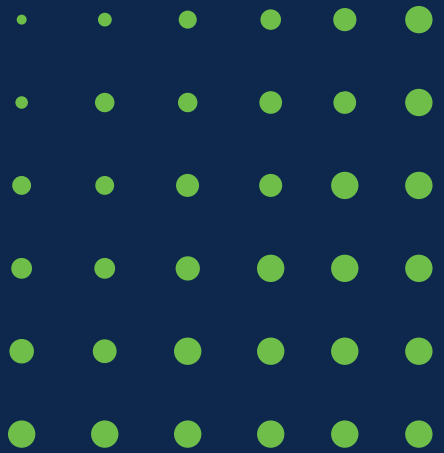
Technology

- Infrastructure
- Tools
- Configurations
- Components

Technology

- Infrastructure
- Tools
- Configurations CERTS
- Components SBOM

What do you do with the data?



Sources of supply chain security data

- Assertions (answers to questionnaires, docs, etc.)
- Audits / certifications
- Testing (scanning, pentests, etc.)
- Monitoring / sampling

Sources of supply chain security data

- Assertions (answers to questionnaires, docs, etc.)
- Audits / certifications
- Testing (scanning, pentests, etc.)
- Monitoring / sampling

RISK MANAGEMENT

"What do we need to change, mitigate or stop using?"

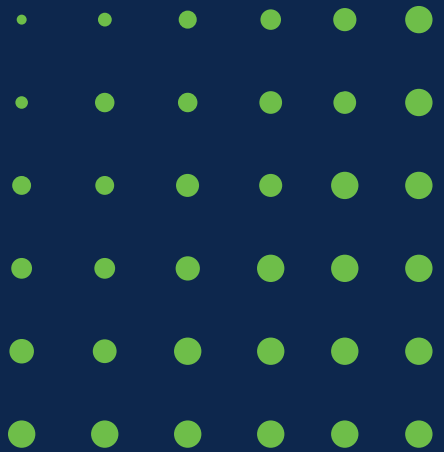
ACCOUNTABILITY

"You said you were doing this and now we see you're not."

NOTIFICATION

"We need to notify our partners/customers because it affects them."

Looking at SBOMs as an example



What is a Software Bill of Materials?

Artifact ID

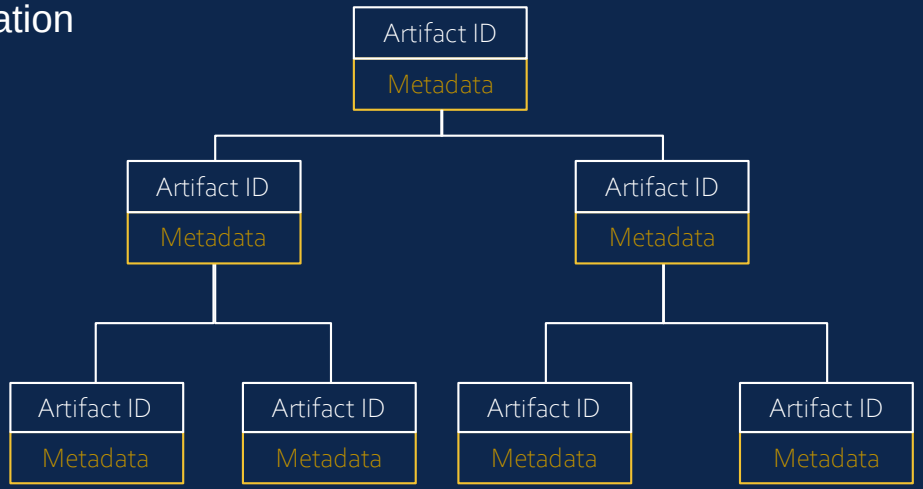
Identifies an

- executable
- .o
- .c
- .h
- .java
- .class
- .py
- .go
- .a
- .so
- container

Metadata

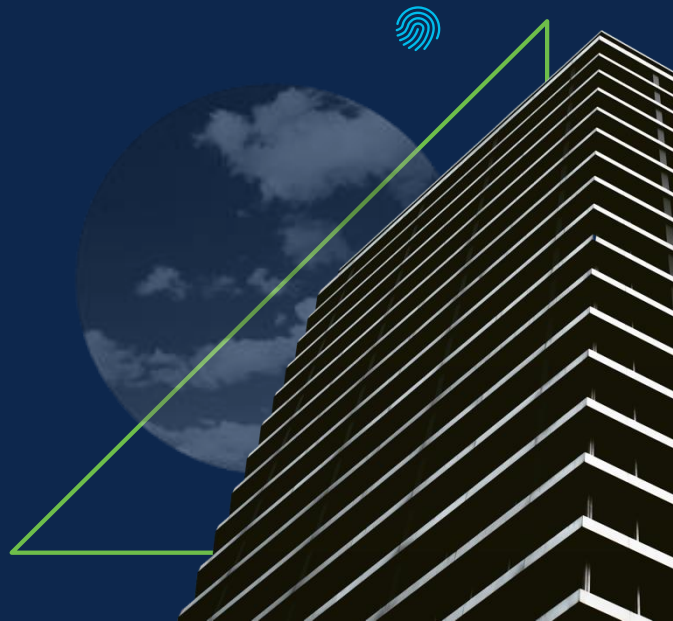
Information about the artifact like:

- vendor
- release version
- contact information
- license
- copyright



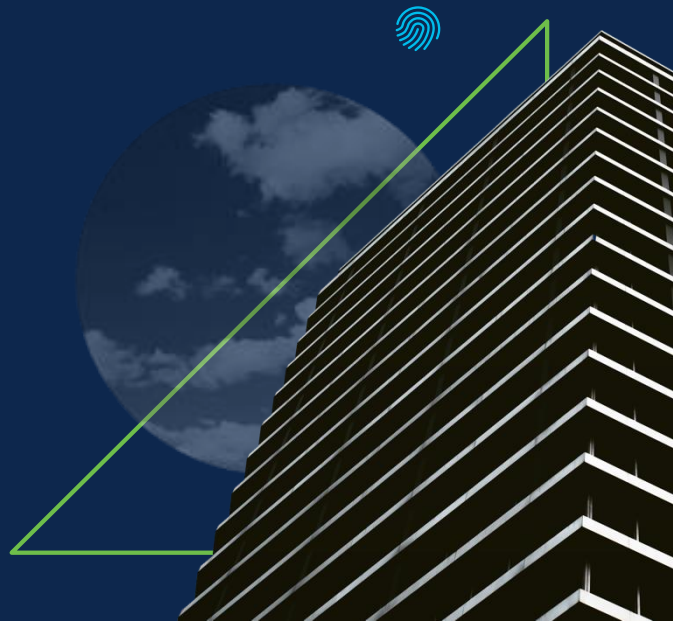
Pre-procurement

- Avoiding licensing conflicts or duplications



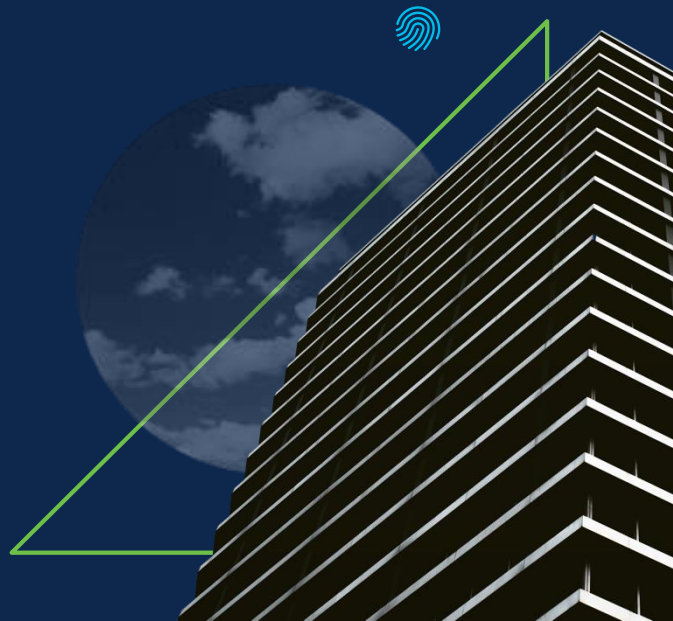
Pre-procurement

- Checking provenance (sanctioned countries etc.)



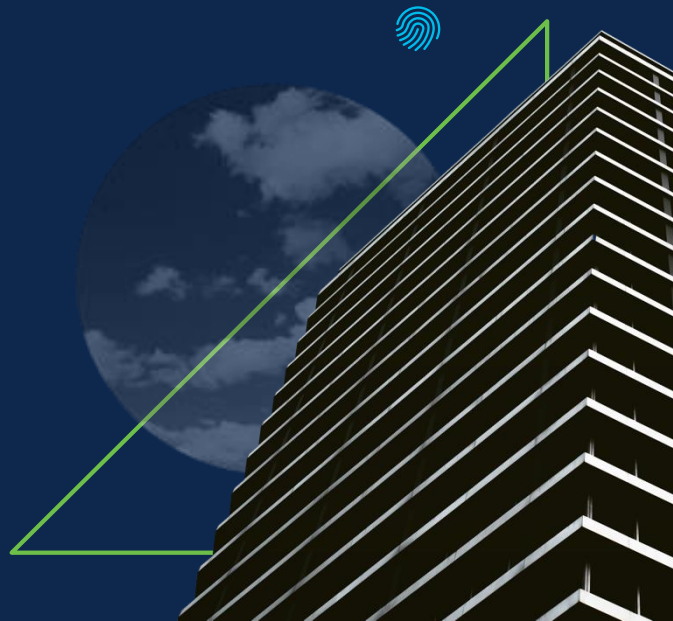
Pre-procurement

- Big-ticket vulnerabilities (but this will hold up the procurement and take negotiation)



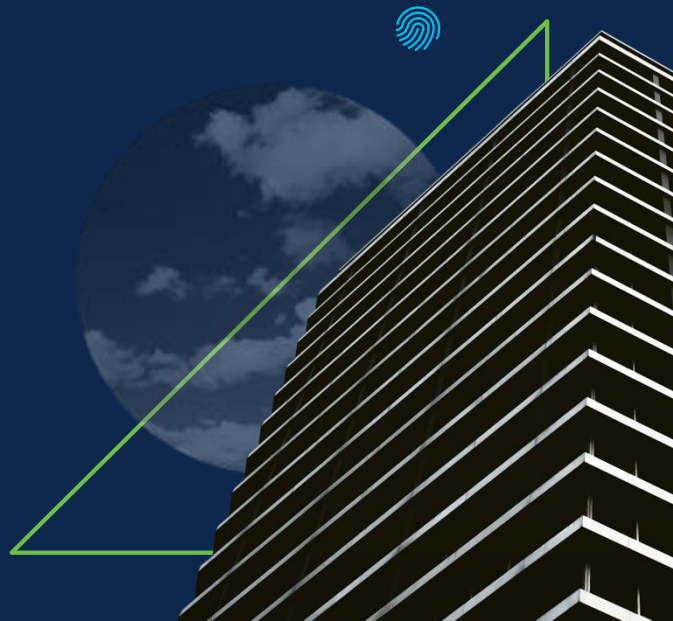
Pre-procurement

- Focus on what can be automatically stopped or flagged; the rest can be logged for notifications later

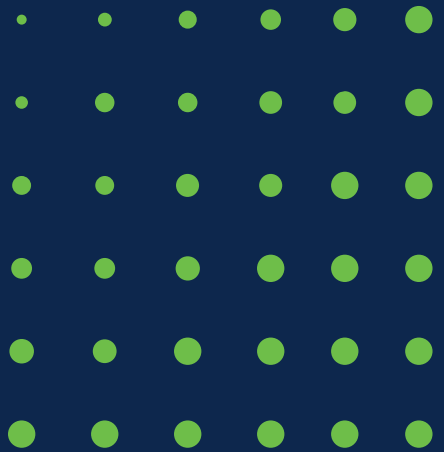


Pre-procurement

- Can you use SBOMs in lieu of SDLC questionnaires or pentests? NO.

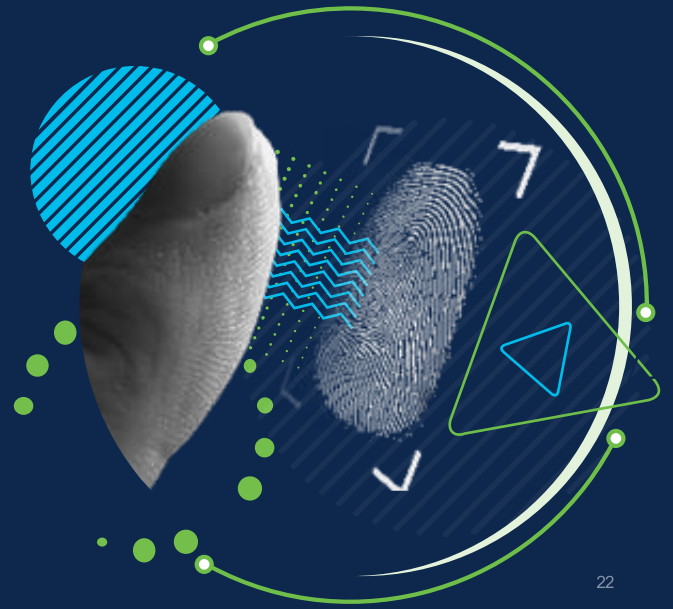


Risk and vulnerability management



What can we learn from vulnerability management?

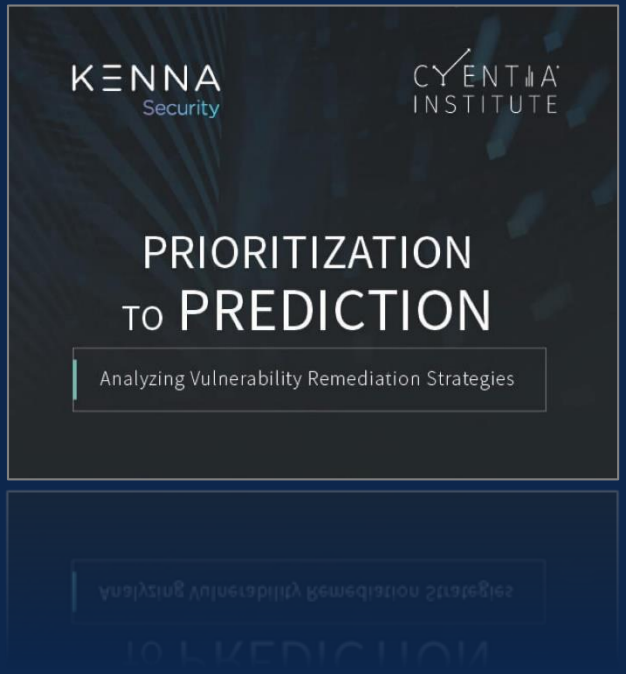
- Someone else's criticality rating isn't always going to be yours



What can we learn from vulnerability management?

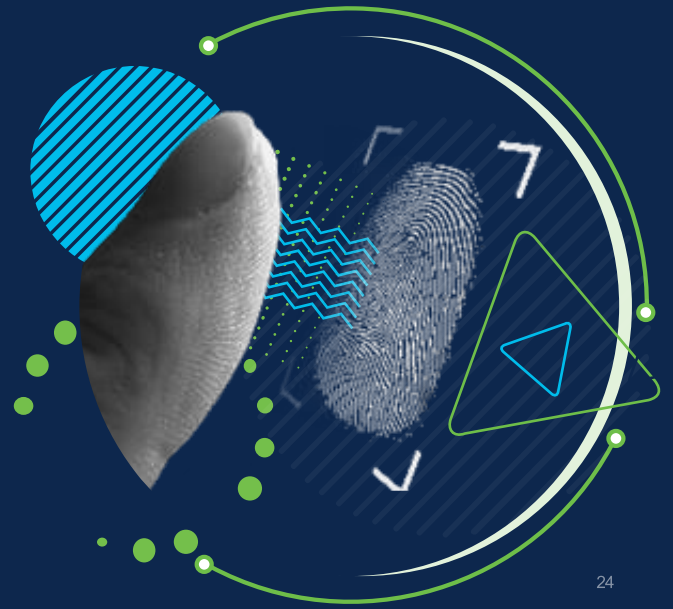
- Cyentia/Kenna: any given prioritization method likely no better than random patching

  https://www.kennasecurity.com/resources/prioritization-to-prediction-report/



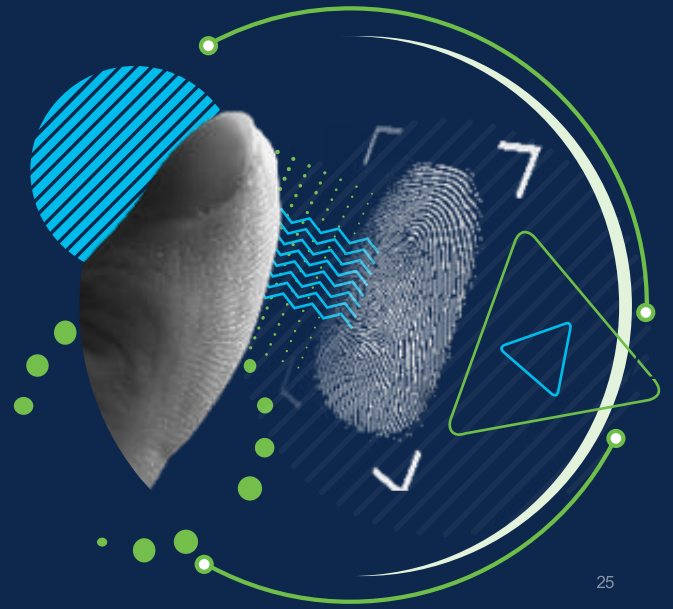
What can we learn from vulnerability management?

- Annotating what's really definitely affected and what isn't



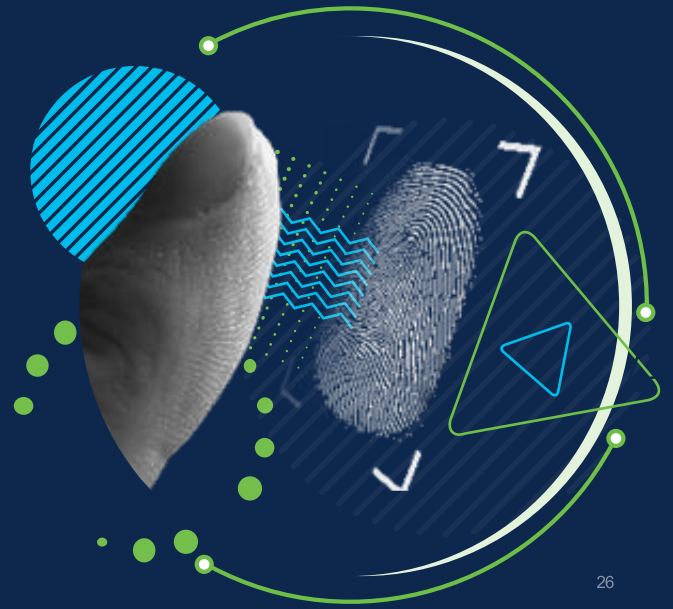
What can we learn from vulnerability management?

- Do we patch or do they patch?
- What are the risk/impact of partial remediation?



What can we learn from vulnerability management?

- Going to need more remediation/update processes to assess dependencies, cost



What can we learn from threat intelligence?

- Do you trust the SBOM?
  - Where can you get technical details when you have questions?
  - If you do your own scanning, be careful

What can we learn from threat intelligence?

- Who is going to need this info, and who simply needs an FYI?

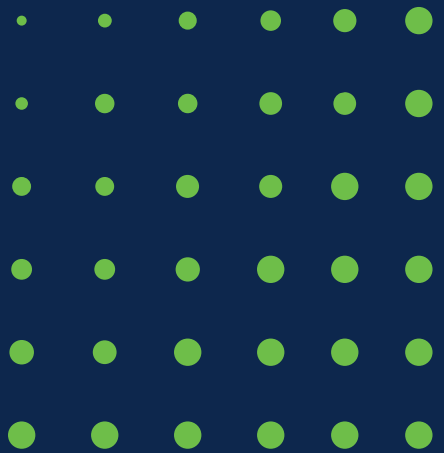
What can we learn from threat intelligence?

- Social graphs are fun, but what are you really going to do with them?

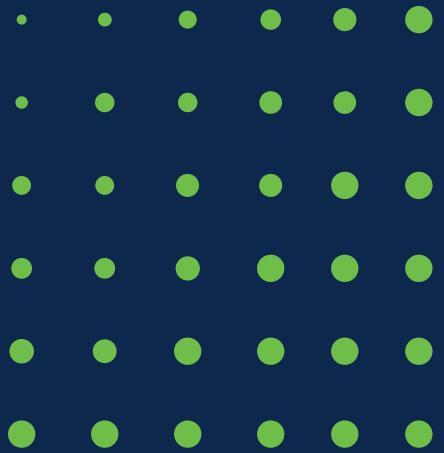
What can we learn from threat intelligence?

- Remember: “blocking is breaking” in AppSec
- Use automation with caution

Automation goes best with certainty, precision, transparency, and commitment



Notifications



Know the limits of your supply chain data

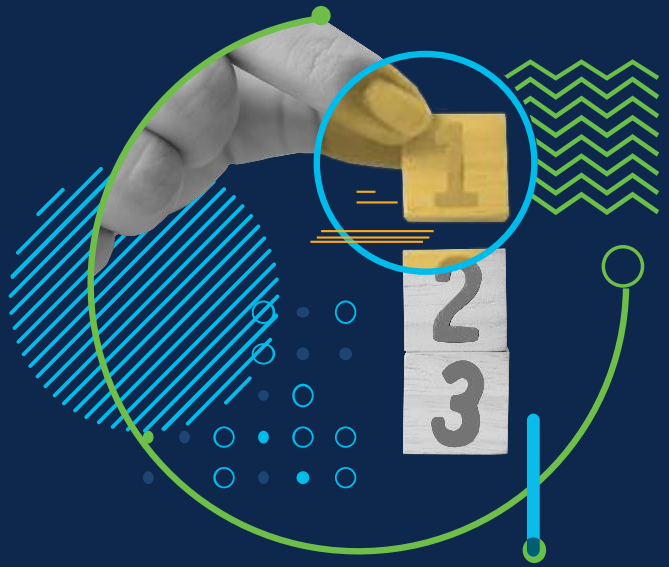
- Do you really have logs on when each version of a component was in use in each location? Like, from which date to which date?

Know the limits of your supply chain data

- Do you really have logs on when each version of a component was in use in each location? Like, from which date to which date?
- Do you know enough about how each component is used to know whether it was really exploited?

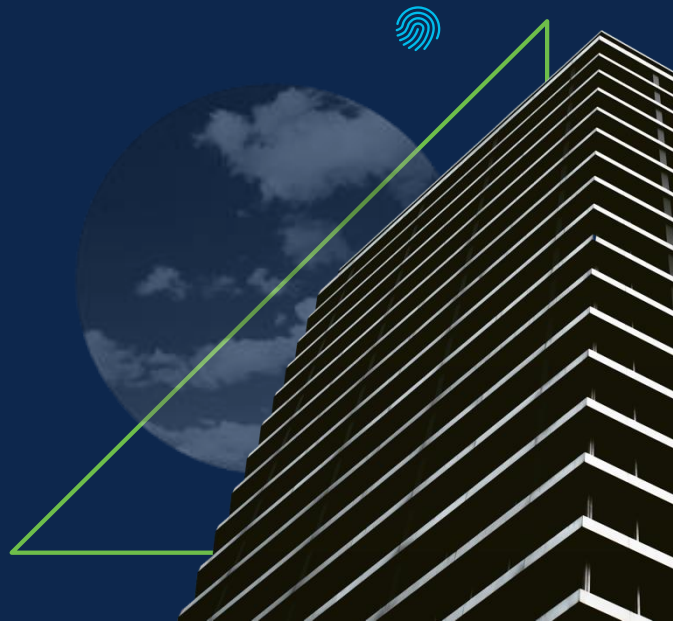
Why your Legal team will cry

- Incomplete data usually requires a breach notification



You'll have to draw a line somewhere

- What about SaaS? Is it SBOMs all the way down?
- You will not always get all the details that you want

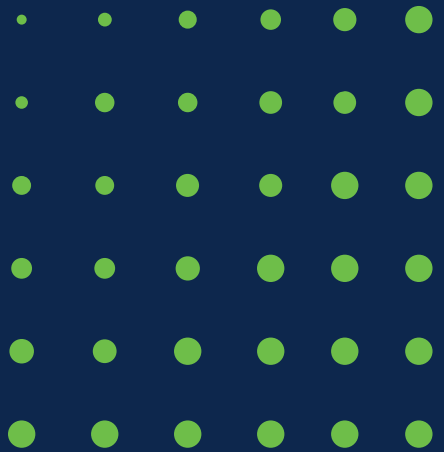


It’s not a supply chain; it’s a web

There is no terminal point at the end of a supply chain.

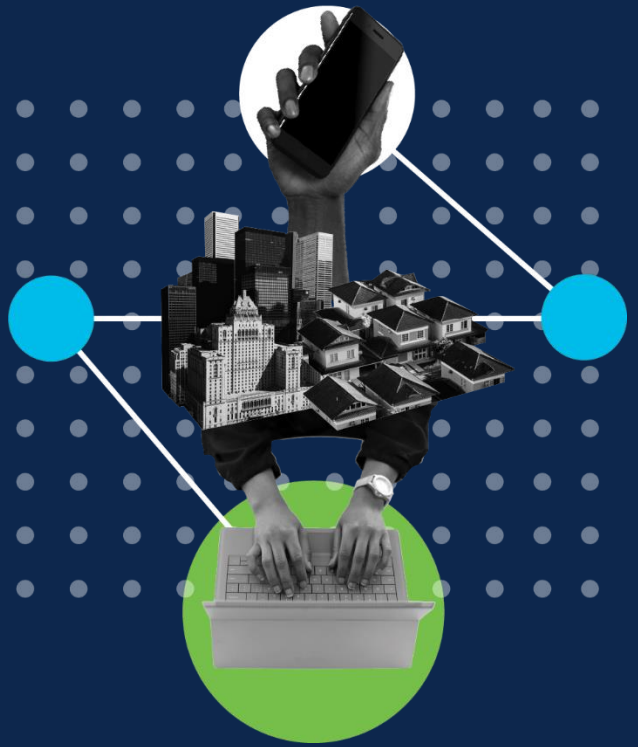
— Helen Patton, Advisory CISO, Cisco

Summary



How not to drown in the data

- Know whether you will use the data for risk and vulnerability management, accountability, or notifications.
- Risk/vuln management: keep close and reference often, as that will be the most dynamic data set
- Accountability can go offline since it's really just a backup
- Notifications will be needed most often if you are midstream in the supply chain



More Thoughts

- Prioritize go/no-go decisions that can be made with unambiguous data
- Document general policy and processes for using the other data
- SBOMs represent a whole new layer of deep detail that many organizations might not be ready to handle
- Negotiation cannot be automated

Resources

- Prioritization to Prediction (Kenna Security/Cyentia)
  https://www.kennasecurity.com/resources/prioritization-to-prediction-report/
- *If you're going to put SBOMs in a vendor contract:*
  NTIA's SBOM Options and Decision Points
  https://www.ntia.gov/files/ntia/publications/sbom_options_and_decision_points_20210427-1.pdf
- ENISA Guidelines For Securing the Internet of Things
  https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

SECURE