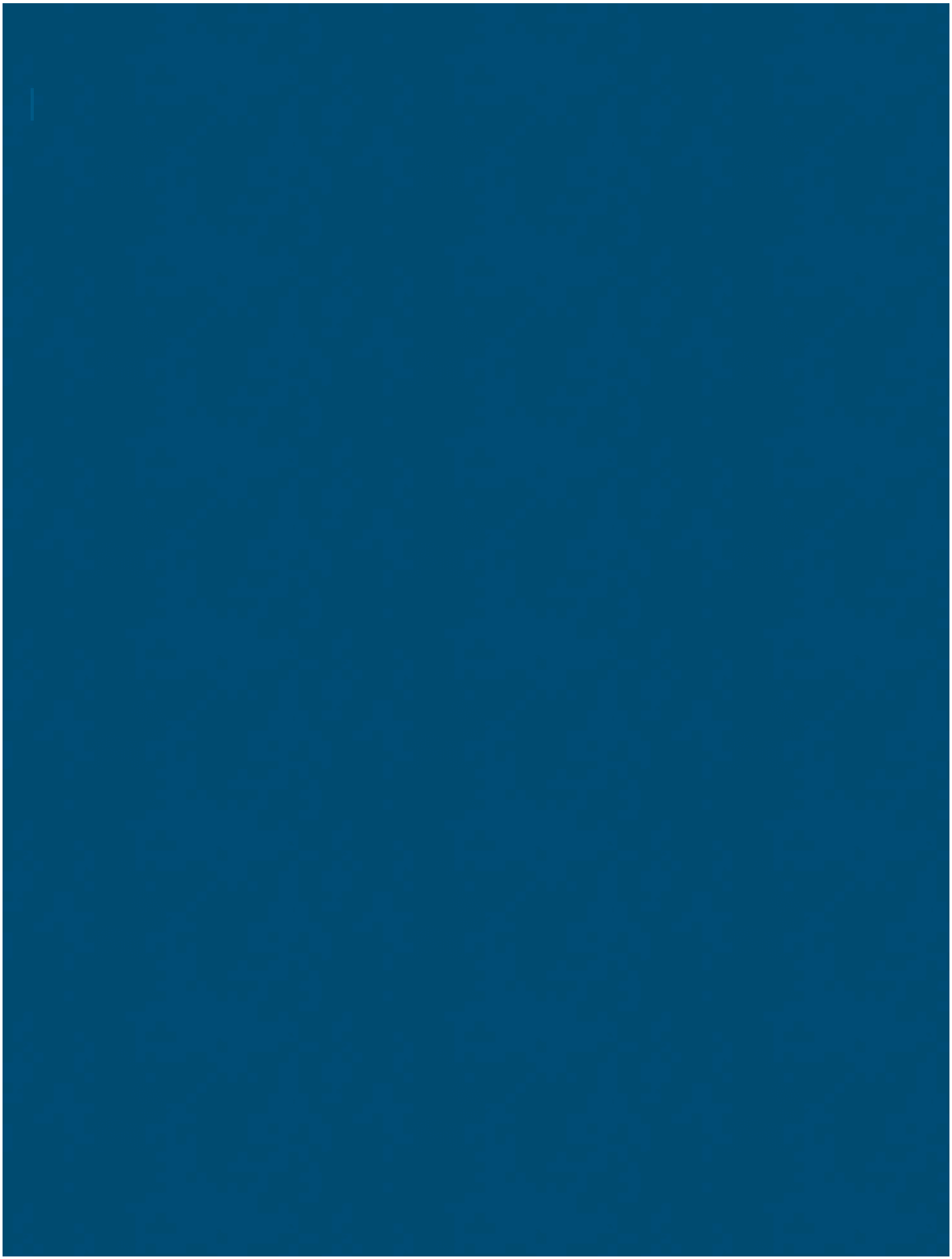


Your Governance is Broken

and what to do about it

I live here

work here

teach Cloud and DevSecOps classes

do open source things

do cloud things

organize a security conference

a security meetup

a local security community

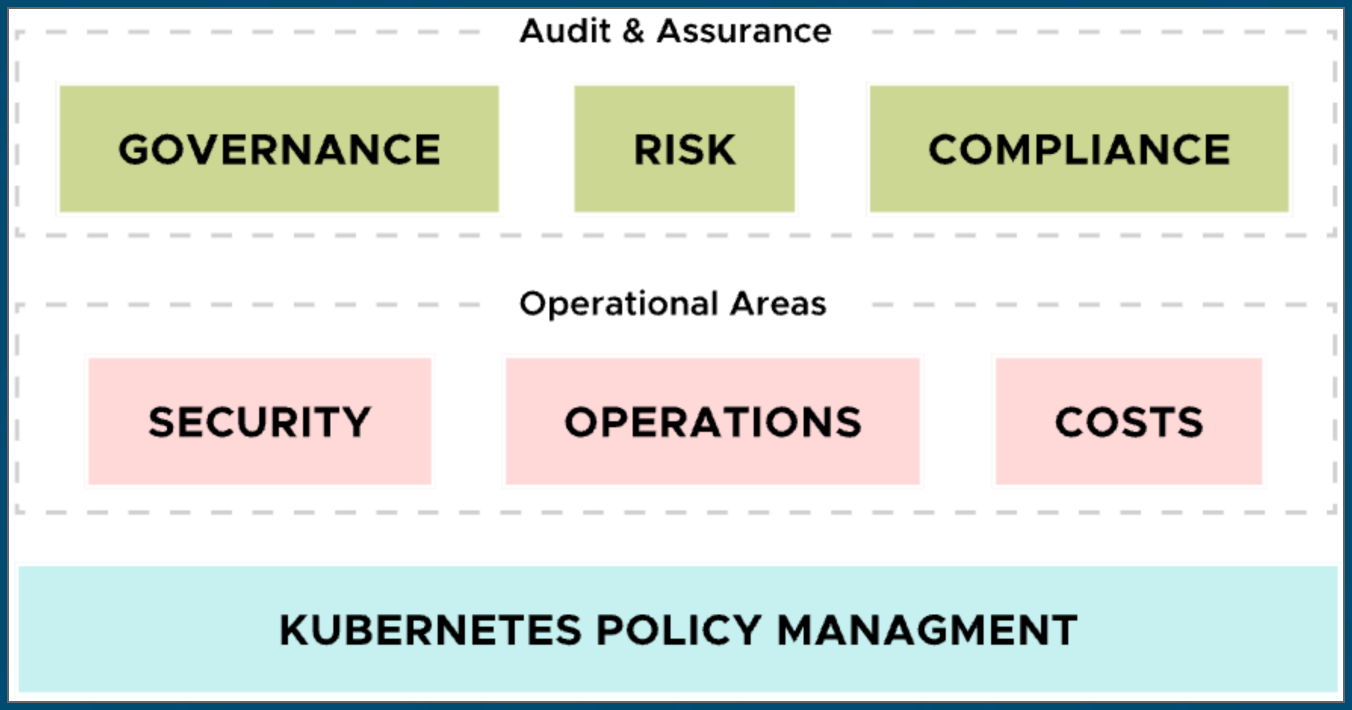
and I'm starting something new!

CNCF Cloud Native Security

https://sei.so/cloud-native-security

(Logo coming soon!)

Governance


Audit & Assurance
GOVERNANCE
RISK
COMPLIANCE
Operational Areas
SECURITY
OPERATIONS
COSTS
KUBERNETES POLICY MANAGMENT

TODO: Ivan request

Governance Operations

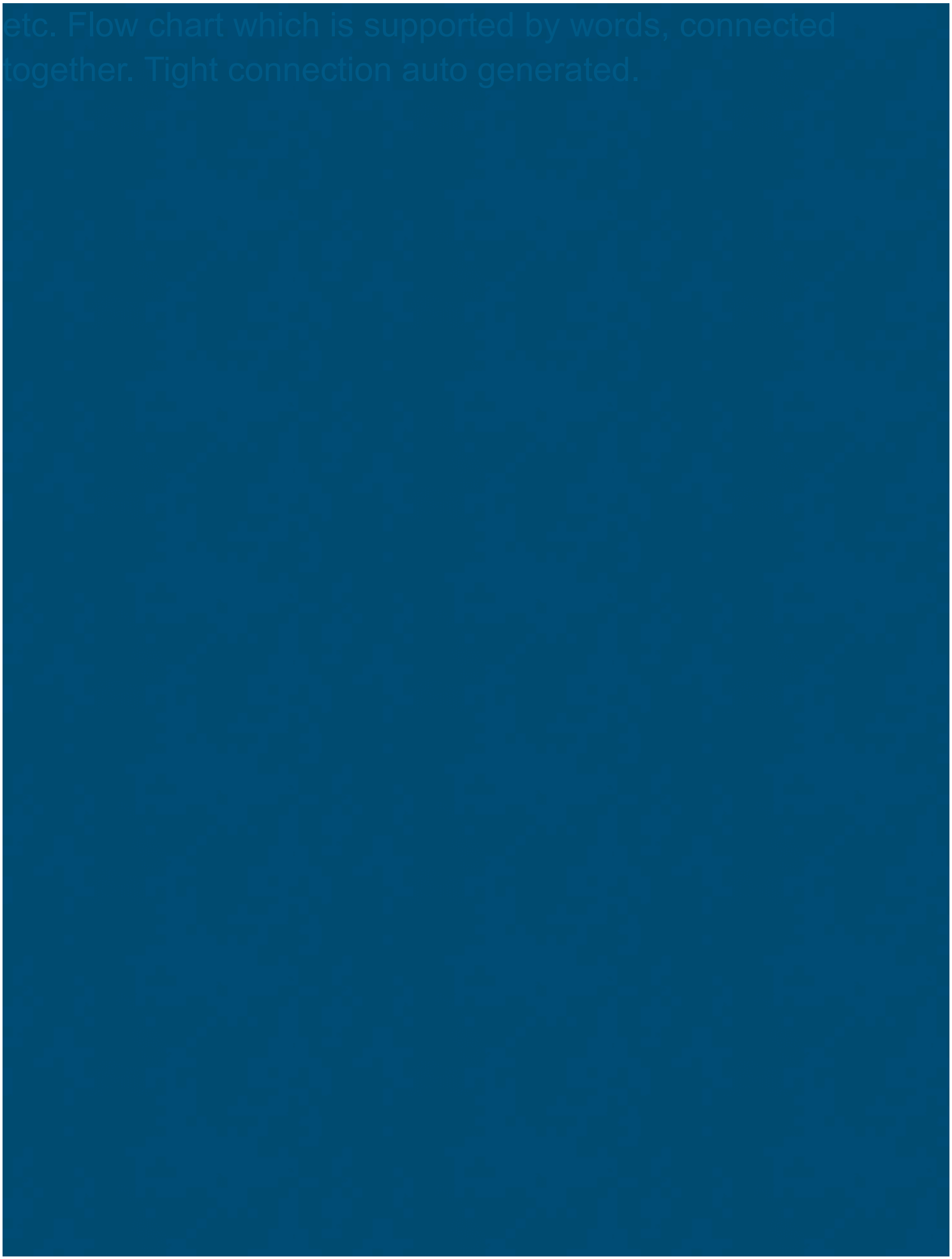
Too specific - Policies needing revision for algorithm updates or software versions Saying that employees must have at least WPA2 encryption on their home wifi Having specific departmental responsibilities. Instead, compose it together based on team names and a mapping outside of the policy Not specific enough - never referring to approved tools or where to find them Having specific events / times in a policy. LIke, we are gathering this and will have an update by DATE. Grey areas and uncertain terms due to not being measured. How approvals/exceptions are submit, tracked, managed. “Unless approved by senior management” - is claiming that it was verbally approved OK? Unsure where a statement came from, and why it’s there Length - way too long and extra information not needed. Should/May vs Must. SLO vs SLA. “All” statements vs compliance percentages. Arbitrary timeframes like 90 days, 30 days, continuously, etc. Having internal references to files that get renamed over time, causing auditability to be confusing. Renaming “rules” to “questionnaire” but not updating the reference to it in a Policy, etc. Flow chart which is supported by words, connected together. Tight connection auto generated.

Governance Pain

"A foolish consistency is the hobgoblin of little minds"

- Ralph Waldo Emerson

Too specific - Policies needing revision for algorithm updates or software versions Saying that employees must have at least WPA2 encryption on their home wifi Having specific departmental responsibilities. Instead, compose it together based on team names and a mapping outside of the policy Not specific enough - never referring to approved tools or where to find them Having specific events / times in a policy. LIke, we are gathering this and will have an update by DATE. Grey areas and uncertain terms due to not being measured. How approvals/exceptions are submit, tracked, managed. “Unless approved by senior management” - is claiming that it was verbally approved OK? Unsure where a statement came from, and why it’s there Length - way too long and extra information not needed. Should/May vs Must. SLO vs SLA. “All” statements vs compliance percentages. Arbitrary timeframes like 90 days, 30 days, continuously, etc. Having internal references to files that get renamed over time, causing auditability to be confusing. Renaming “rules” to “questionnaire” but not updating the reference to it in a Policy,


etc. Flow chart which is supported by words, connected together. Tight connection auto generated.

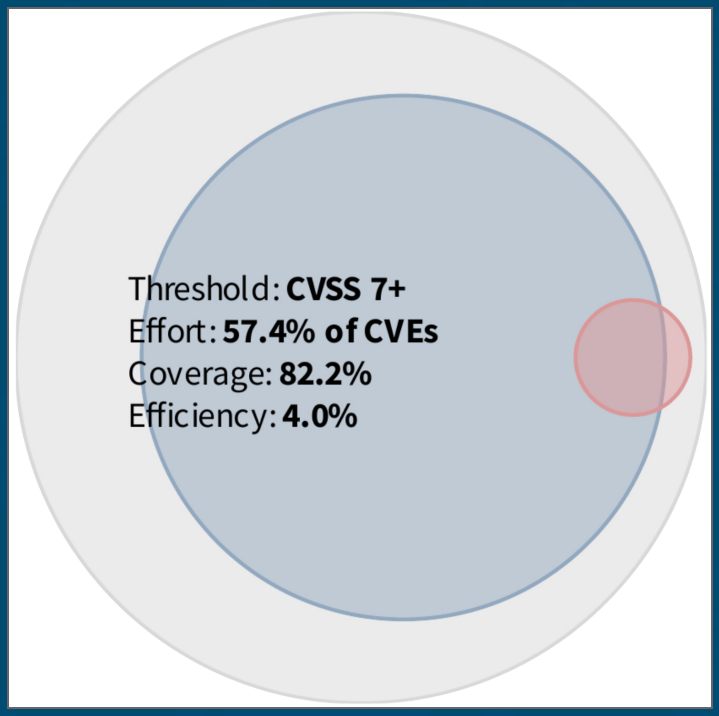
Case Study

Vulnerability Management (Roadmap)

Identified vulnerabilities should be fixed within a specific time, based on their severity as rated by the Common Vulnerability Scoring System (CVSS).

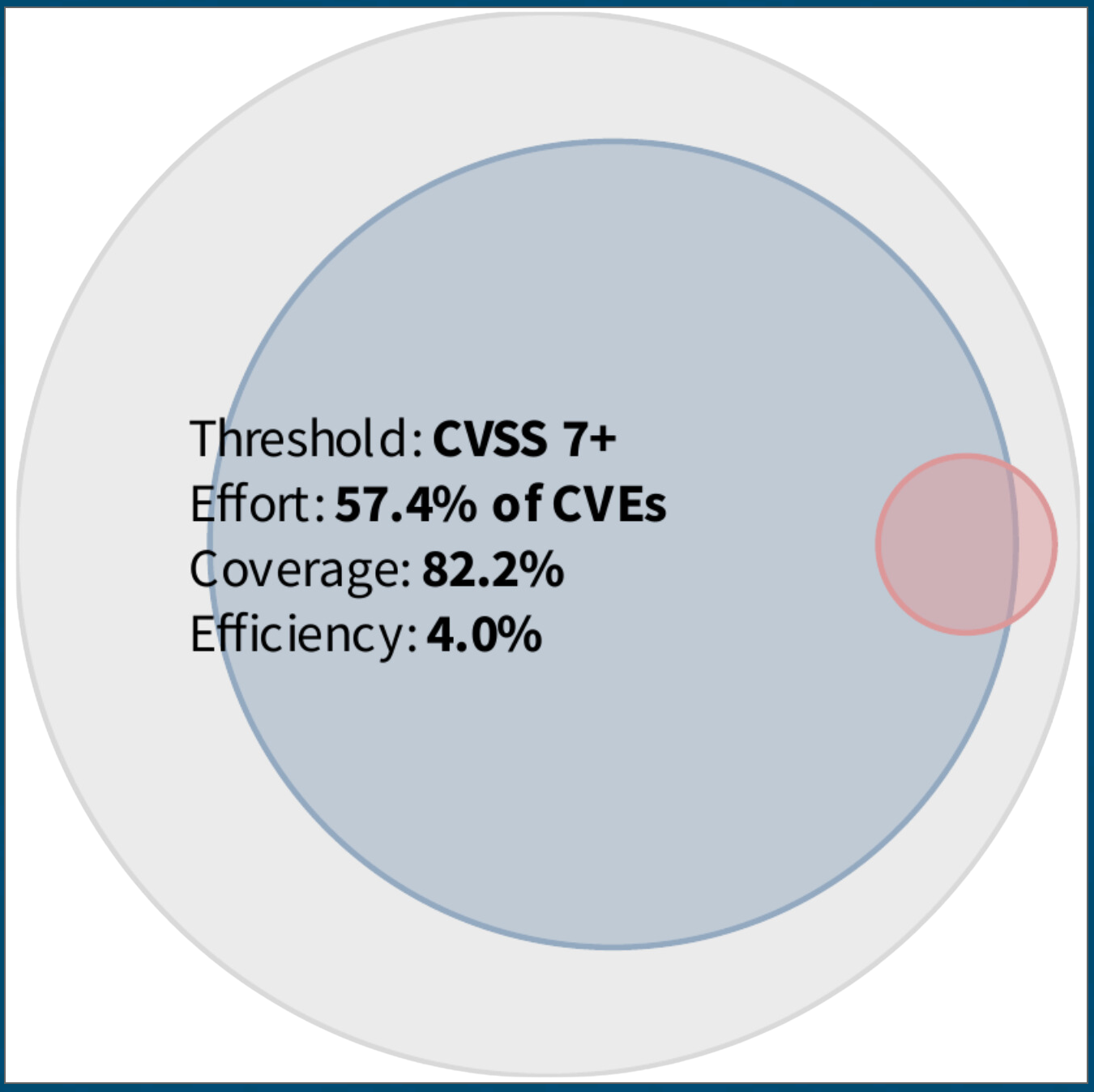
Critical vulnerabilities, with a CVSS rating between 9.0 and 10.0, are required to be remediated within 14 days of detection. Those classified as High, with CVSS scores ranging from 7.0 to 8.9, must be addressed within 30 days. Additionally, vulnerabilities assessed as Medium, having CVSS ratings between 4.0 and 6.9, are to be resolved within a 90-day period.

Fix the base problems - container 3 problems and then auto updates

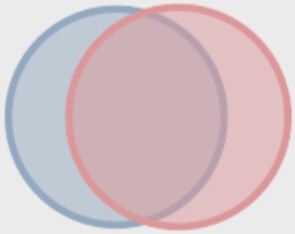


https://first.org/epss/model

Epss


Threshold: **CVSS 7+**
Effort: **57.4% of CVEs**
Coverage: **82.2%**
Efficiency: **4.0%**

Threshold: **EPSS 0.1+**
Effort: **2.7% of CVEs**
Coverage: **63.2%**
Efficiency: **65.2%**



https://first.org/epss/model

Pen test

Cvss

Questions?

Thank you!

https://www.linkedin.com/in/jonzeolla

Speaker notes