asimily

NIST IoT

October 25, 2023

IoT Vulnerability Management Challenges faced by Asimily customers

Learn

Decide

Act

The challenge has moved from front-end Discovery

Learn

Act

Decide

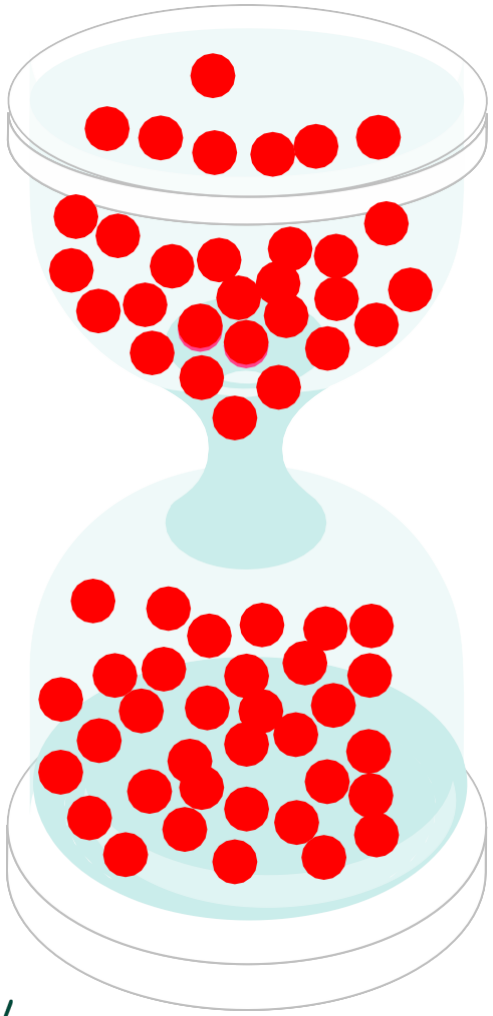
…to Final Mitigation

Learn

Decide

Act

Old: Vulnerability Counts and Severity



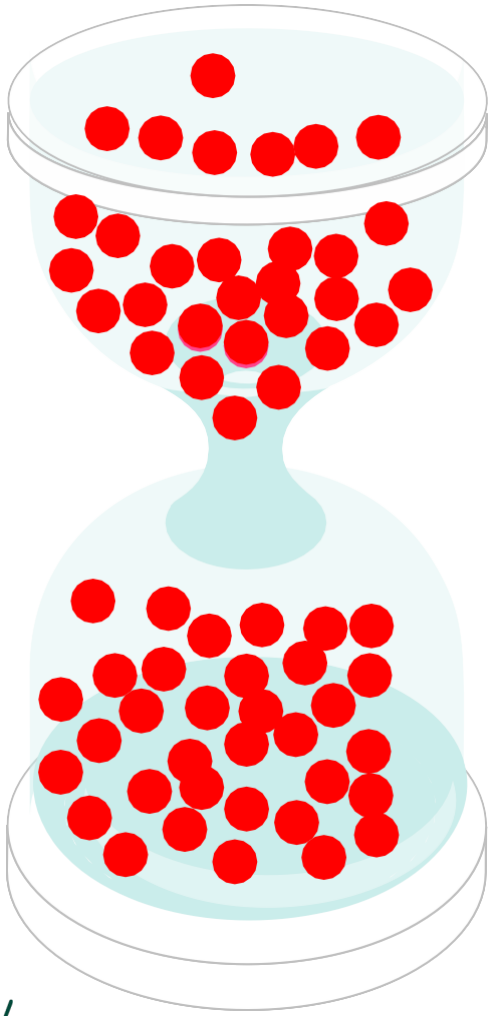
Without risk prioritization and without targeted fixes

91 problems
x 14 hours

1,274 hours total

asimily

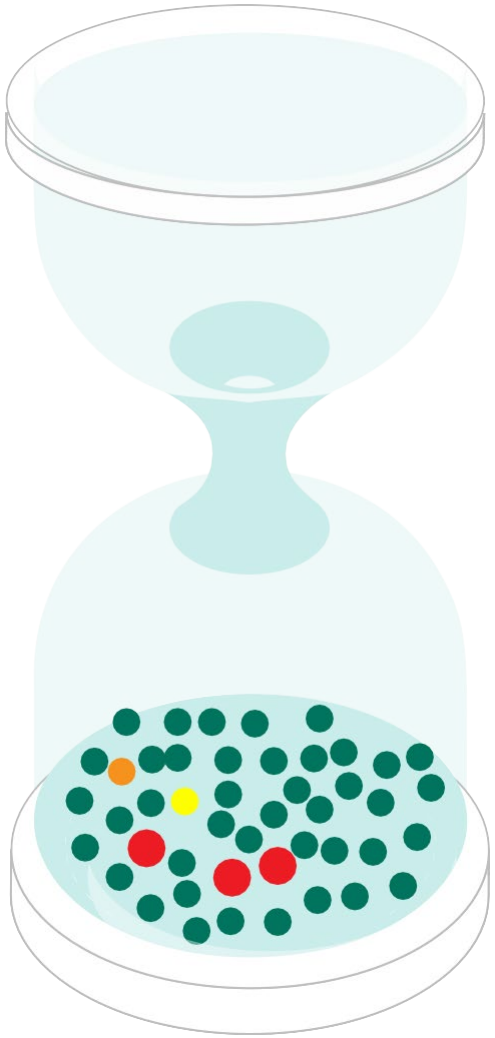
Old: Vulnerability Counts and Severity
New: Risk Reduction per Hour



Without risk prioritization and without targeted fixes

91 problems
x 14 hours

1,274 hours total



With risk prioritization and targeted fixes

3 problems
x 14 hours

2 problems
x 4 hours

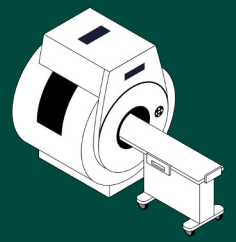
1 problem
x 3 hours

37 problems
x 2 hours

127 hours total

asimily

Example of Targeted Fixes for IoT



Siemens MAGNETOM Family Device - Serial X123YZ – Hospital 4, Floor 5

	Is it Clinically Valid?	Does it Reduce Risk Score?	Estimated Hours to Remediate
Block RDP port (3389)	Yes	-2 to Risk	2-3 Hours
Turn off IPv6 for the device	Yes	+0	1-2 Hours
Block external DNS access	Yes	+0	1-2 Hours
Patch OS	No – should be mfg approved	+0	2-3 Hours
Macrosegment	Yes	-1 to Risk	10-12 Hours
Microsegment	Yes	-2 to Risk	12-14 Hours

asimily

Potential Framework - “Common Mitigation Workflow”

Standardized Mitigation Prerequisites (Skills, Time)

Benefits:

- Common language for practitioners that can be used from firm to firm
- Fits well into formal training, which can target specific, known, common mitigation tasks
- Expandable

Each mitigation is unique for each environment, but a baseline can help for work planning, training, and quality control.

Questions?