Know thyself
then patch thyself

OpenStack Forum
2019-03-13

Nicolae Paladi

- Researcher at RI.SE Security
- Post-Doc at Lund University

LUNDS UNIVERSITET

#OpenStack
#Docker Swarm
#Kubernetes
#Micado-Scale (H2020 COLA)
SE-OvS (H2020 ASCLEPIOS)
#SMARTY (SSF, Firmware updates)
#IETF TEEP, SUIT

RI.SE

RISE North Research Datacenter (Luleå)

Topics and Non-Topics

✔ Vulnerability Ecosystem
✔ Example Vulnerability Management Process: OpenStack
✔ Do's and do not's
✔ "The Future"

✘ How do I secure my [insert technology stack] deployment?
✘ Choosing a vulnerability management system

Why “Know thyself”?

The unexamined life is not worth living.
(Socrates)

The unexamined deployment is not worth patching.
(made up for this presentation)

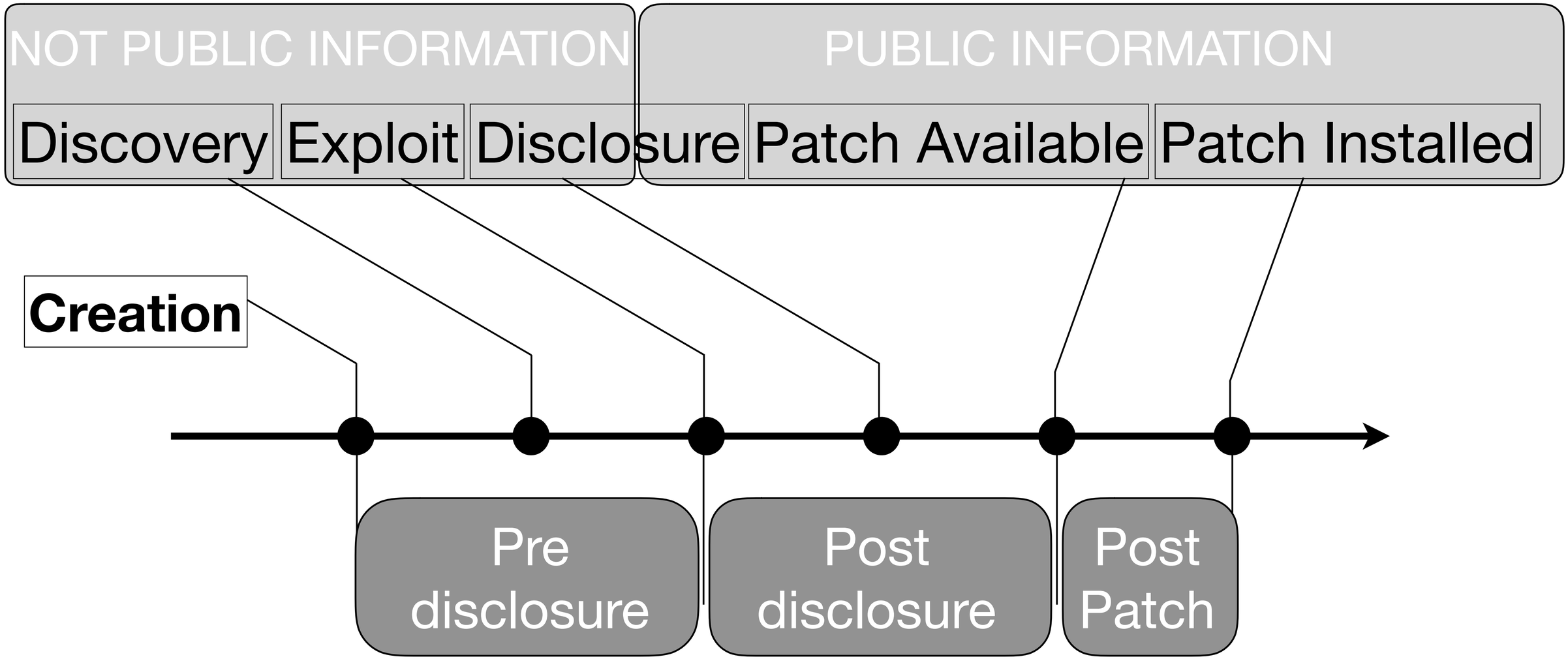
Why “patch thyself”?

- New vulnerabilities are disclosed daily
- Unpatched vulnerabilities are a threat to tenant and operator alike
- Regular release cycles are too long
- Cloud deployments include many, many third-party libraries not maintained by the cloud platform itself
- Vulnerabilities in hypervisors or container management systems can compromise the entire deployment.

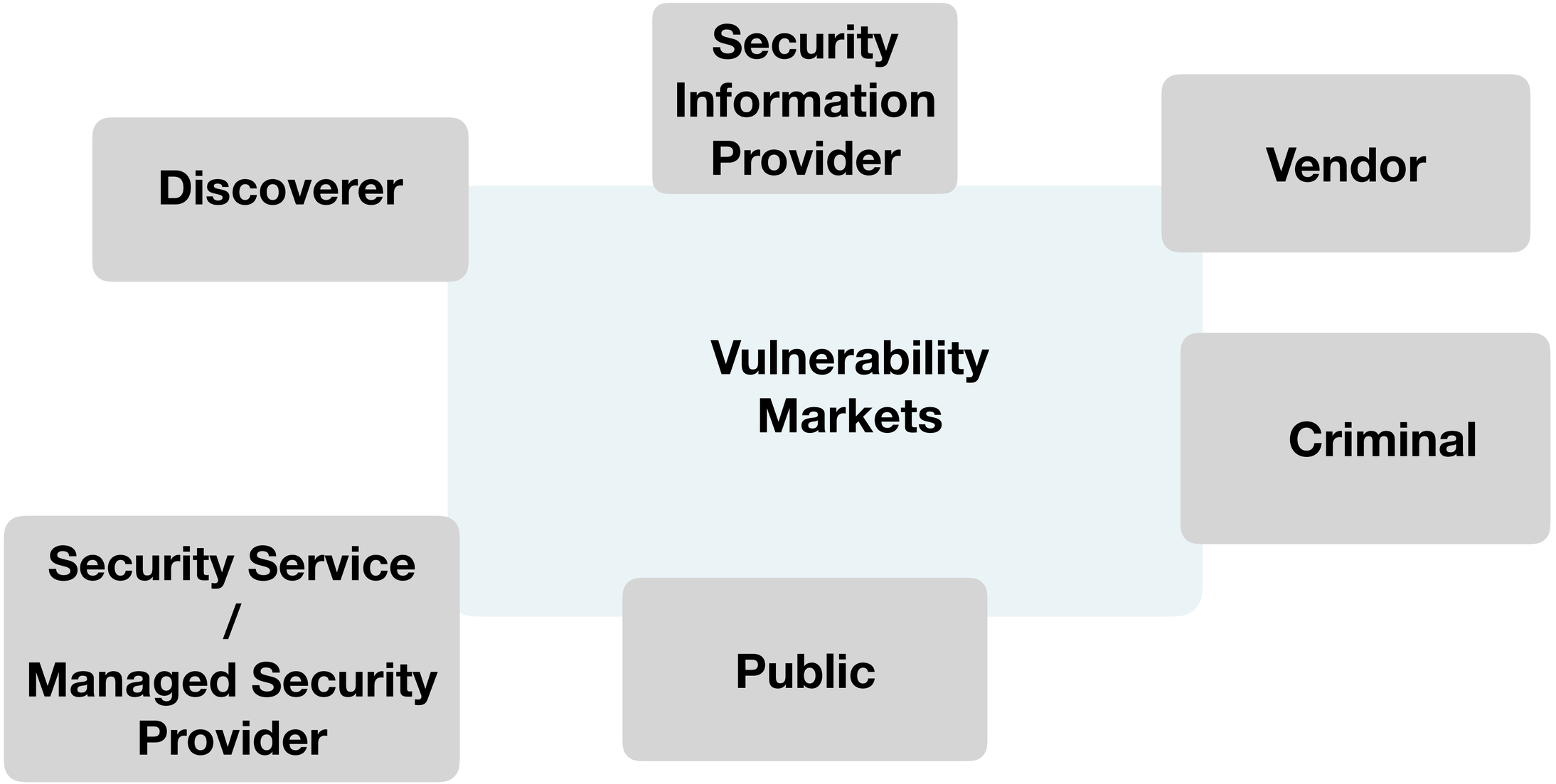
What is a vulnerability?

A security issue with an assigned CVE identifier

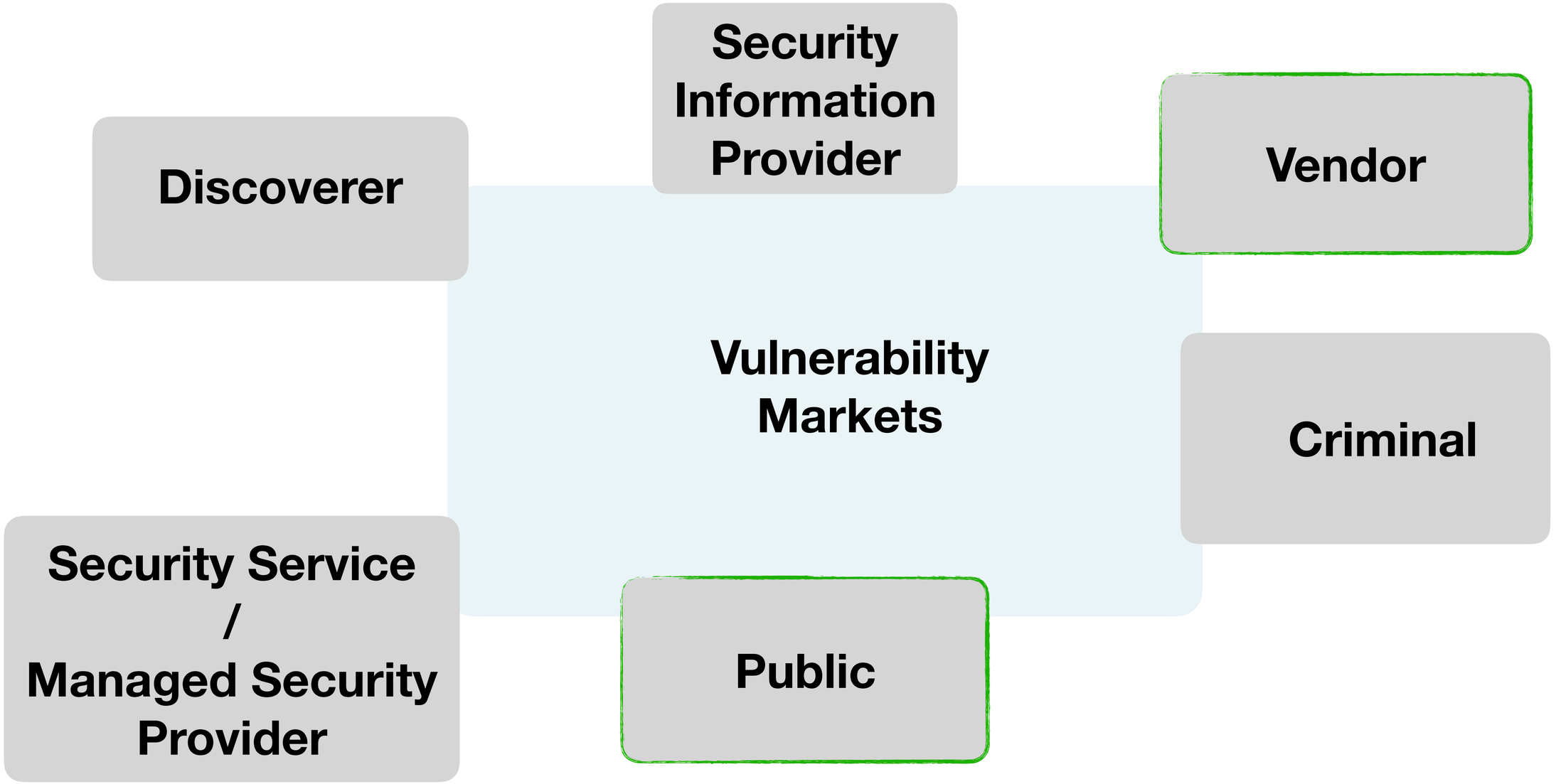
Vulnerability lifecycle



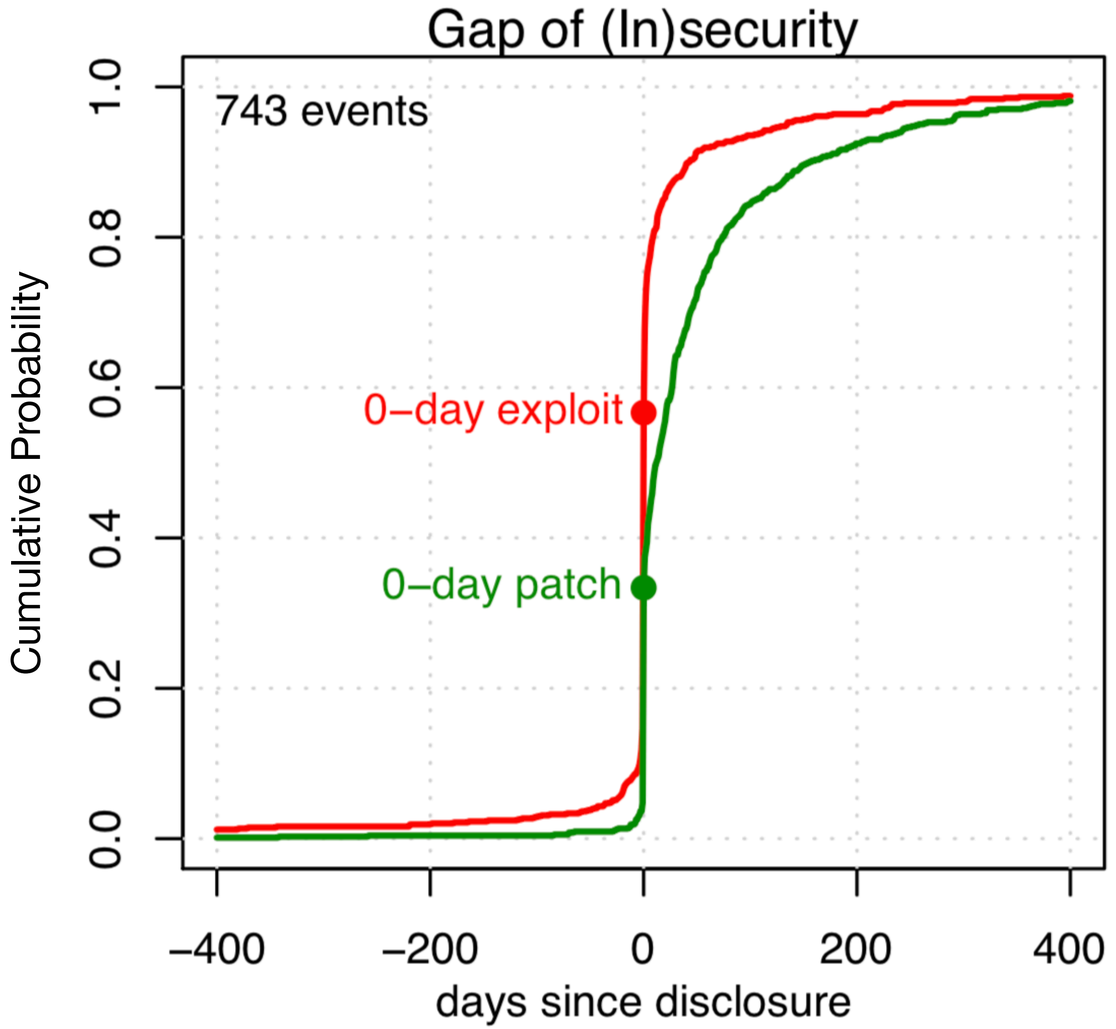
The (in) security ecosystem



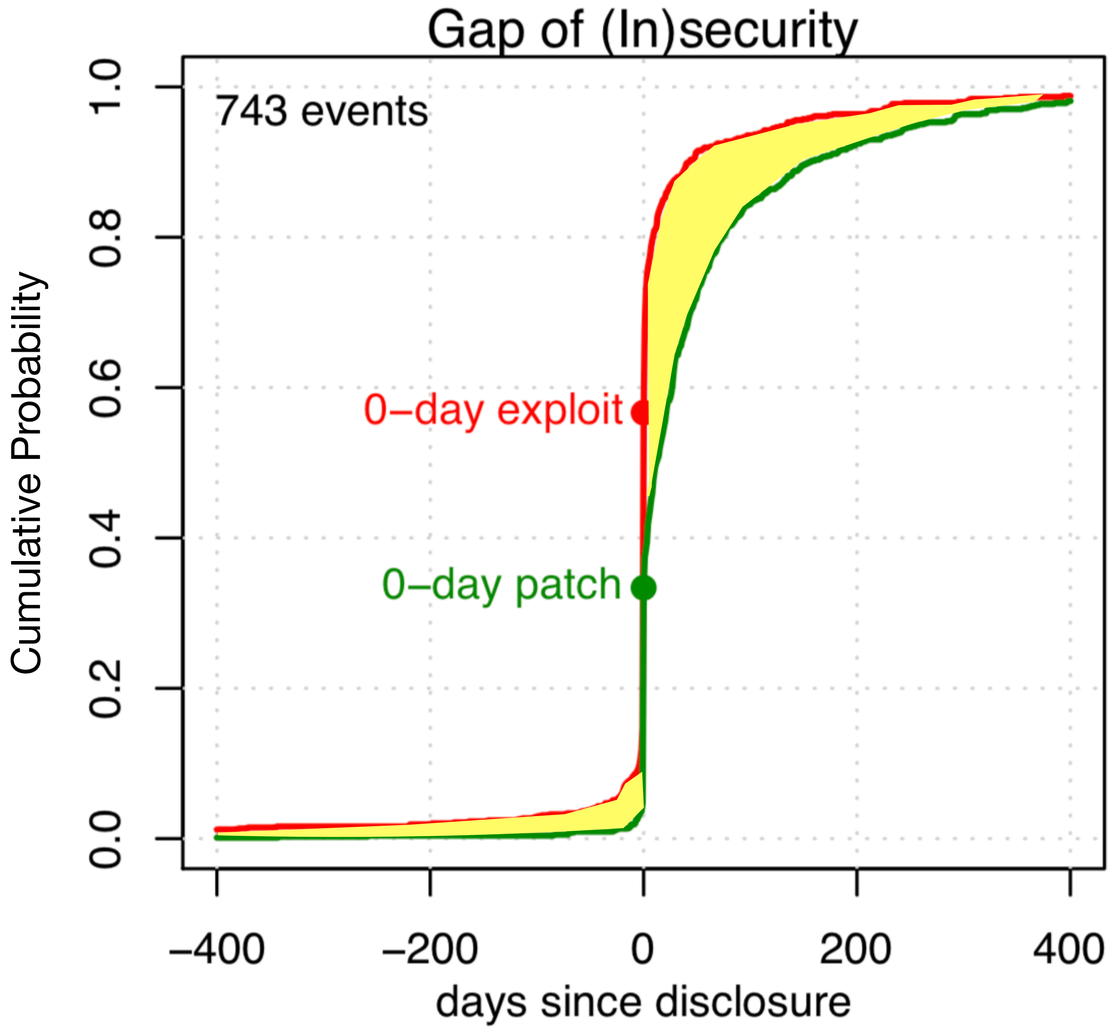
The (in) security ecosystem



Patch Availability vs Exploit Availability



Patch Availability vs Exploit Availability



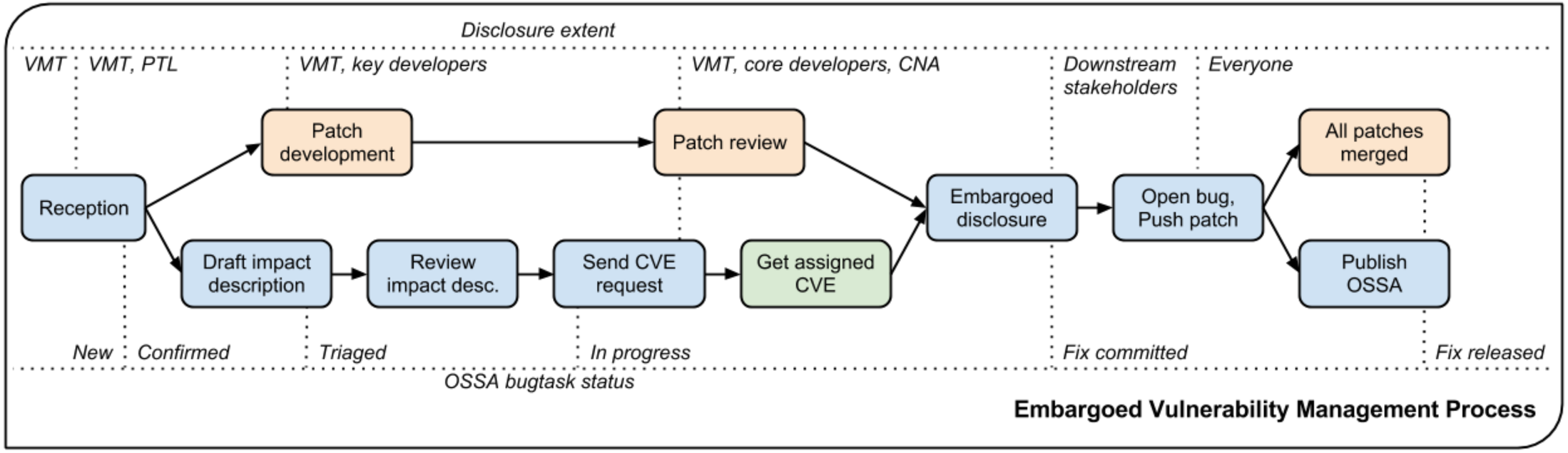
Why not (yet) patched?

- **cost** – plain and simple
- **disruption** – upgrades disrupt business and “steal” resources
- **compatibility/dependencies** – specialist applications may not operate reliably on newer operating systems
- **operations** – major software upgrades are inherently risky, and user tools may work differently

Vulnerability assessment in OpenStack

- OpenStack vulnerability management team
- OpenStack Security Notes (OSSNs)
- OpenStack-discuss mailing list

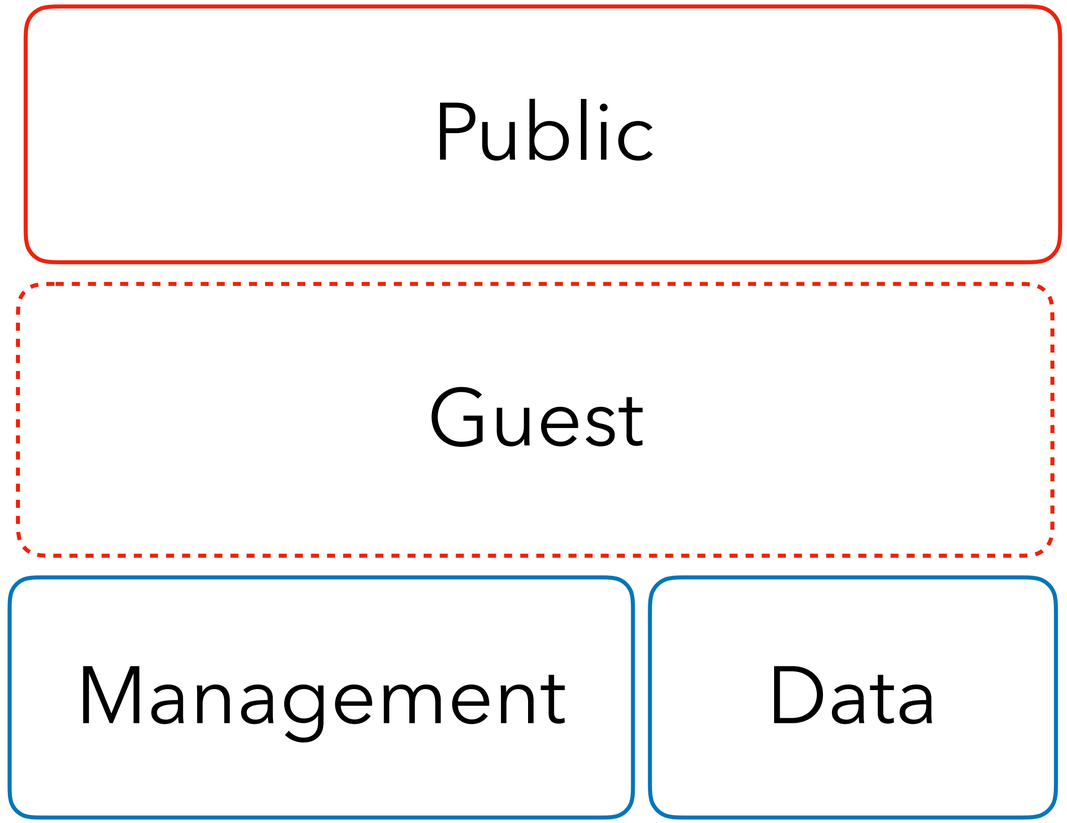
OpenStack Vulnerability Management Process



Security information for OpenStack deployers

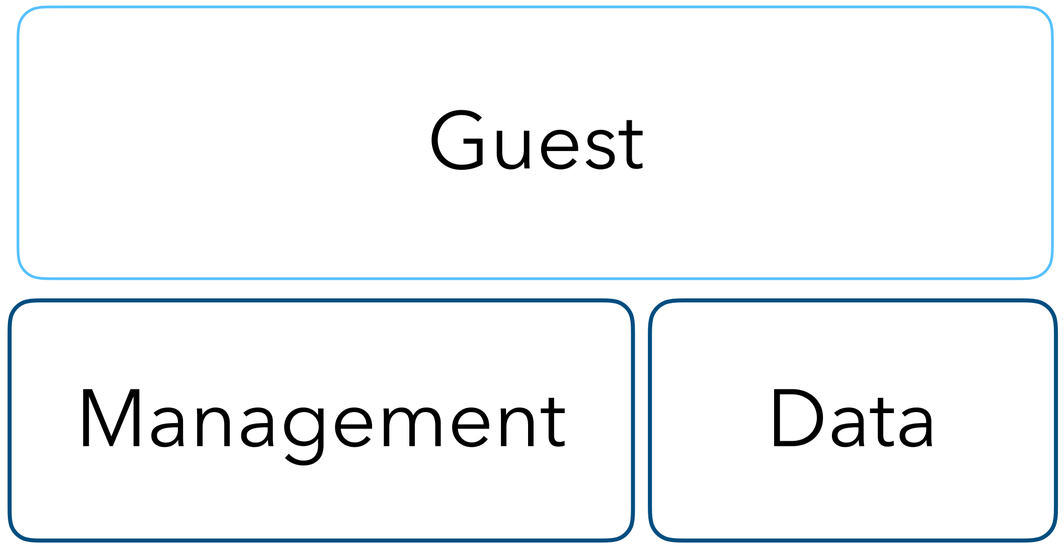
- OpenStack Security Advisories (OSSA)
- OpenStack Security Notes (OSSN)
- OpenStack Security Guide
- OpenStack Security Project blog

Security Domains in OpenStack



Source: https://docs.openstack.org/security-guide/introduction/security-boundaries-and-threats.html#

Security Domains in OpenStack



Source: https://docs.openstack.org/security-guide/introduction/security-boundaries-and-threats.html#

Vulnerability and patch selection

Assess

Triage

Prioritize

Vulnerability and patch selection

Assess

Automated vulnerability assessment tools?...

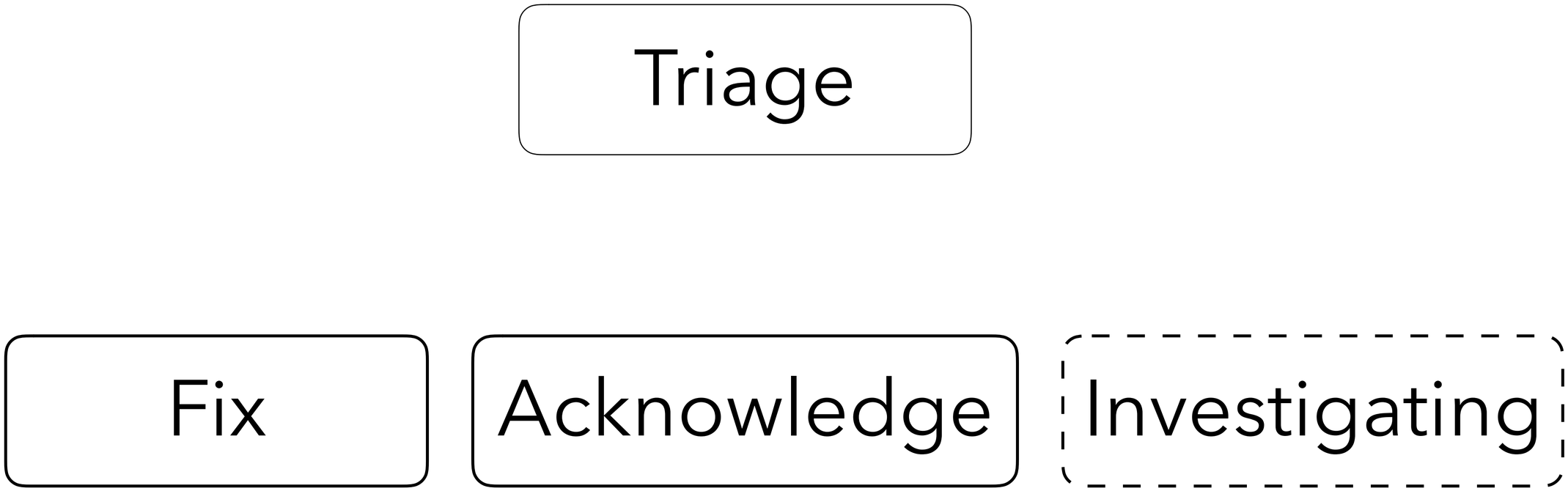
Vulnerability and patch selection

Triage

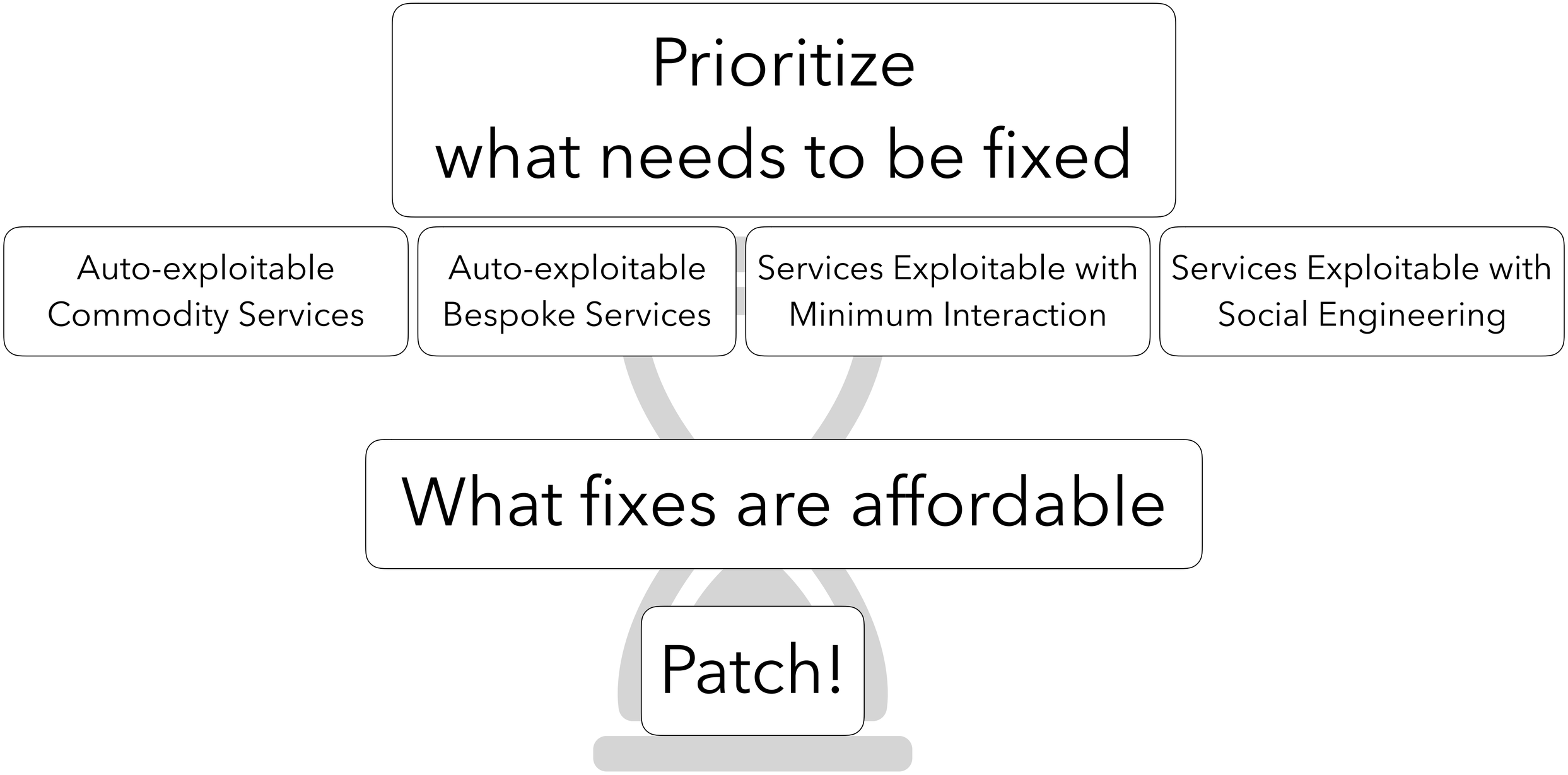
✗ select an arbitrary score above which vulnerabilities must be fixed, ignoring all issues below that level

✗ take raw CVSS scores without taking into account organisation specific mitigations or priorities

Vulnerability and patch selection



Vulnerability and patch selection



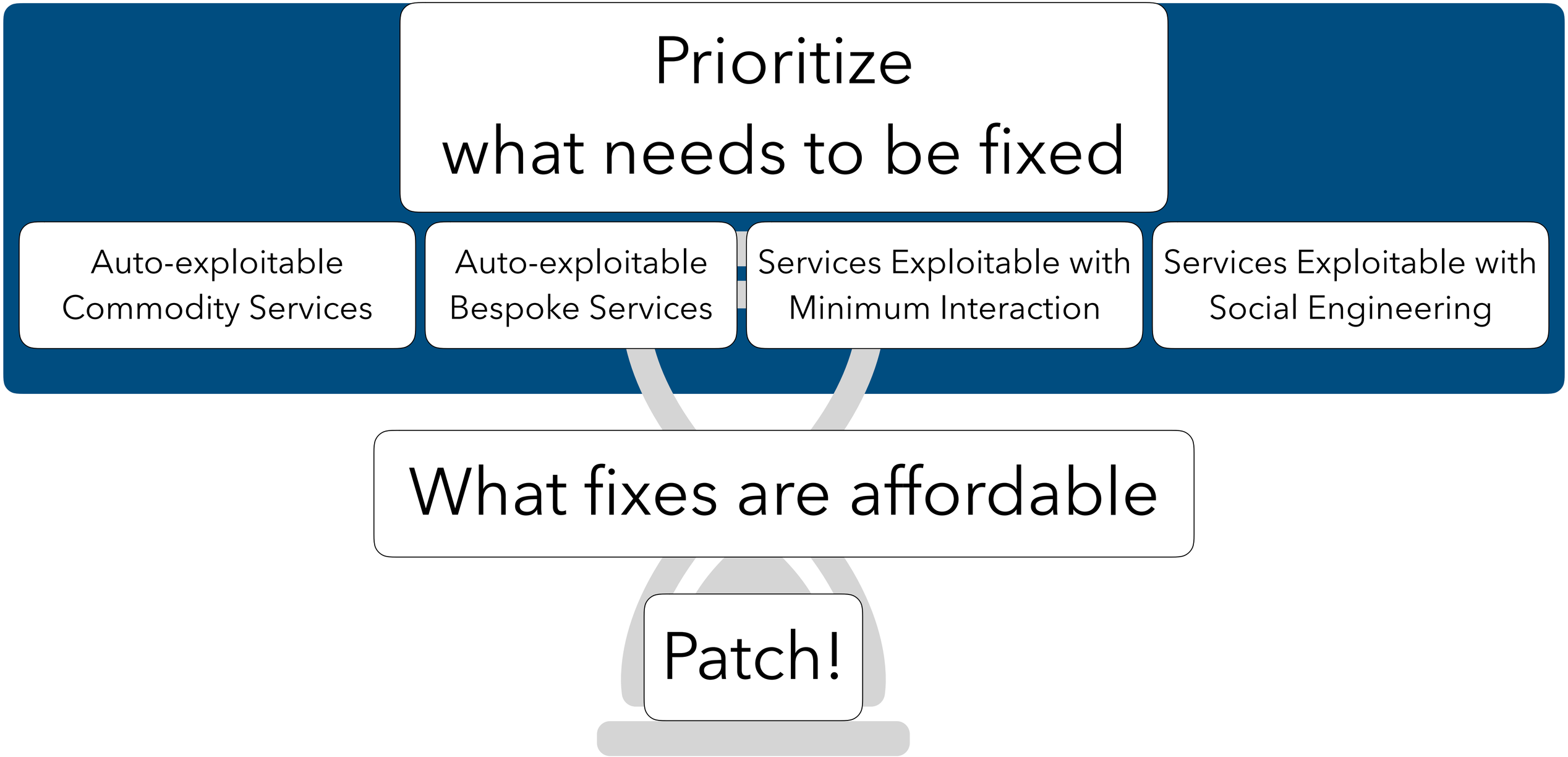
Automated patch selection

…is in its early infancy…

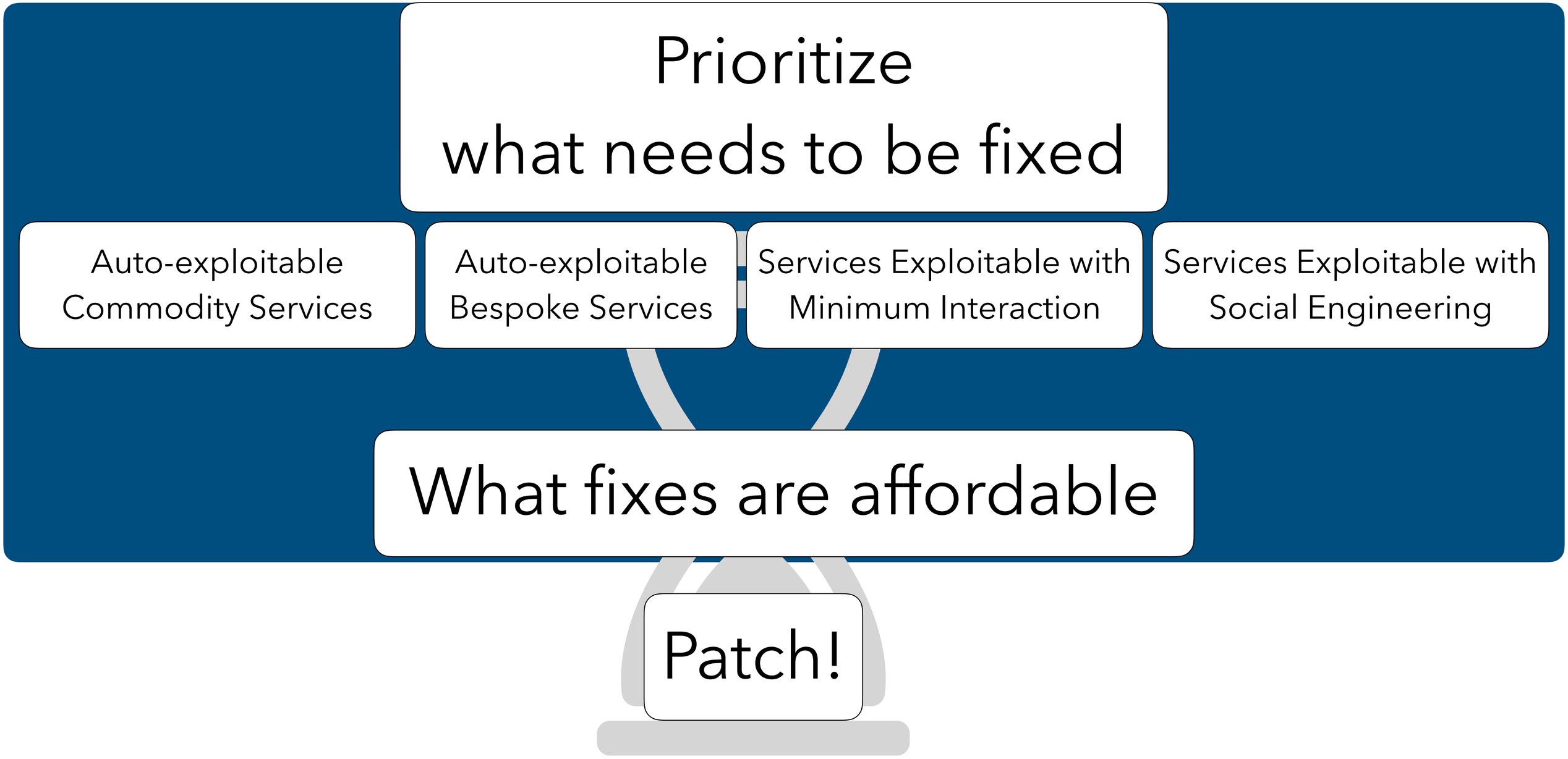
- Farris, Katheryn A., et al. "Vulcon: A system for vulnerability prioritization, mitigation, and management." *ACM Transactions on Privacy and Security (TOPS)* 21.4 (2018): 16.

- **SMARTY** (Säkra mjukvaruuppdateringar för den smarta staden)
  - Cobleigh, Alexander, et al. "Identifying, Prioritizing and Evaluating Vulnerabilities in Third Party Code." *2018 IEEE 22nd International Enterprise Distributed Object Computing Workshop (EDOCW)*. IEEE, 2018.

Vulnerability and patch selection



Vulnerability and patch selection



References

- Vulnerability management Guidance to help organisations assess and prioritise vulnerabilities. https://www.ncsc.gov.uk/guidance/vulnerability-management
- Application Container Security Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
- Markets for Cybercrime Tools and Stolen Data https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
- Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner. 2006. Large-scale vulnerability analysis. In Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defence (LSAD '06). ACM, New York, NY, USA, 131-138. DOI=http://dx.doi.org/10.1145/1162666.1162671
- OpenStack Vulnerability Management Process https://security.openstack.org/vmt-process.html#ossa-task-status
- Vulnerability awareness in OpenStack https://docs.openstack.org/security-guide/compute/vulnerability-awareness.html
- Identifying, Prioritizing and Evaluating Vulnerabilities in Third Party Code https://ieeexplore.ieee.org/abstract/document/8536124
- MiCADO - autoscaling framework for Docker services https://github.com/micado-scale/
- Säkra mjukvaruuppdateringar för den smarta staden **https://portal.research.lu.se/portal/en/projects/sakra-mjukvaruuppdateringar-foer-den-smarta-staden(d81348d8-c491-440c-af06-7bc563b3538a).html**

Questions