Vulnerability Coordination Maturity Model

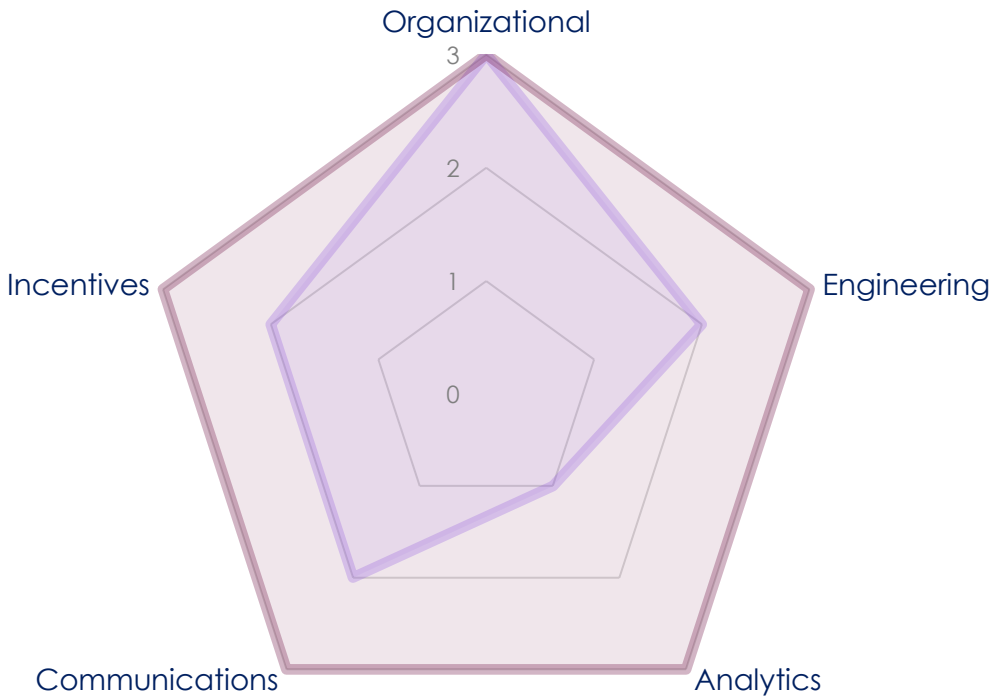
LUTA SECURITY

So You Think You're Ready for a Vulnerability Disclosure Program or Bug Bounty?

- Managing vulnerabilities and improving security goes well beyond receiving bug reports.
- Organizations must first assess several important factors and processes to understand their operational capacity and maturity before implementing a vulnerability disclosure program (VDP) or bug bounty.
- By using the Vulnerability Coordination Maturity Model (VCMM), organizations can benchmark their capabilities and identify and prioritize the areas that need improvement as well as evolve their vulnerability management and overall security.

Vulnerability Coordination Maturity Model

- The model provides guidance on how to organize and improve vulnerability coordination processes
- 5 Capability Areas: Organizational, Engineering, Communications, Analytics and Incentives
- 3 Maturity Levels for each Capability: Basic, Advanced or Expert
- Organizations can benchmark their current capabilities
- Creates a roadmap for success



Organizational:

People, process and resources to handle bugs

Level -- Capability

- Basic: Executive support to respond to vulnerability reports and a commitment to security and quality as core organizational values.
- Advanced: Policy and process for addressing vulnerabilities according to ISO 29147 and ISO 30111, or a comparable framework.
- Expert: You have executive support, processes, budget, and dedicated personnel for handling vulnerability reports.

Engineering:

Capabilities to evaluate & remediate security holes and improve secure development lifecycle

Level -- Capability

- Basic: Clear way to receive vulnerability reports, and an internal bug database to track them to resolution. See ISO 29147
- Advanced: Dedicated security bug tracking and documentation of security decisions, deferrals, and trade-offs.
- Expert: Use vulnerability trends and root cause analysis to eliminate entire classes of vulnerabilities. See ISOs 29147, 30111, 27034.

Communications:

Ability to communicate with internal & external audiences about bugs

Level -- Capability

- Basic: Ability to receive vulnerability reports and a verifiable channel to distribute advisories to affected parties. See ISO 29147.
- Advanced: Tailored, repeatable communications for each audience, including security researchers, partners, customers, and media.
- Expert: Structured information sharing programs with coordinated distribution of remediation, e.g., giving point of contact to partners ahead of the day formerly known as patch Tuesday.

Analytics:

Data analysis of vulnerabilities to identify trends and improve processes

Level -- Capability

- Basic: Track the number and severity of vulnerabilities over time to measure improvements in code quality.
- Advanced: Use root cause analysis to feed back into your software development lifecycle. See ISOs 29147, 30111, 27034.
- Expert: Track real-time telemetry of active exploitation to drive dynamic pivots of remediation strategy, e.g., if there is an uptick of exploitation in the wild, you may decide to release a mitigation in an advisory, even though the patch is not yet ready.

Incentives:

Ability to encourage security researchers to report vulnerabilities directly

Level -- Capability

- Basic: Show thanks or give swag. Clearly state that no legal action will be taken against researchers who report bugs.
- Advanced: Develop unique incentives that only your organization can give, like special tours or meetings with distinguished individuals at your organization. Or give financial rewards or bug bounties. Either of these can be used as incentives to encourage reporting the most serious vulnerabilities.
- Expert: Understand adversary behavior and vulnerability markets, and structure advanced incentives to disrupt them.

5 Proactive Steps for Organizations

1. **Use the Vulnerability Coordination Maturity Model** to assess your capabilities
2. **Ask for help** from those who have come before to develop your strategic and tactical plan for the inevitable vulnerability report
3. **Consider your goals** if seeking a bug bounty or any other security service provider
4. **Vulnerability disclosure is among your first steps**, master it, and practice the process maturity that security requires.
5. **Build security in** whenever you can, but know that you will not be able to catch everything

Bug Bounties won't replace other security testing.

Hackers can help you – if you let them!

Contact Luta Security

All code has vulnerabilities. We can help.

Contact: VCMM@LutaSecurity.com

www.LutaSecurity.com