EO 14028 Guidelines for Enhancing Software Supply Chain Security

Vulnerability Disclosure Programs: Available Standards & Best Practices

KATIE MOUSSOURIS

FOUNDER & CEO, LUTA SECURITY

NOVEMBER 8, 2021

Katie Moussouris Luta Security

- **Katie Moussouris, Founder & CEO, Luta Security:** As a computer hacker with more than 20 years of professional cybersecurity experience, Katie has a unique and unparalleled perspective on security research, vulnerability disclosure, and bug bounties. She serves as an advisor to several governments and large organizations around the world. Working with the U.S. Department of Defense, Katie led the launch of the U.S. government's first bug bounty program, "Hack the Pentagon." During her tenure with Microsoft, her work included industry-leading initiatives such as Microsoft Vulnerability Research and the company's first bug bounty program. Katie is also the co-author and co-editor of ISO 29147 vulnerability disclosure, ISO 30111 vulnerability handling processes, and ISO 27034 secure development. She is a visiting scholar with the MIT Sloan School and a cybersecurity fellow at New America and the National Security Institute.

- **Luta Security:** Luta Security is transforming the way governments and organizations are using process, people, and technology to improve vulnerability coordination and security investments in connecting vulnerability management to secure development. Luta Security advises organizations across all phases of vulnerability coordination, including smart roadmaps on how to comply with ISO standards 29147, 30111 and 27304.

Vulnerability Disclosure vs. Pen Test vs. Bug Bounty

Vulnerability Disclosure

- Anyone outside your org reporting vulns to you
- Should follow the ISO standards for vulnerability disclosure (**ISO 29147**) and vulnerability handling processes (**ISO 30111**).

Penetration Testing

- Hackers for hire via a consulting arrangement
- Consultants have passed employment background checks
- **Contracts and NDAs make this a planned process**

Bug Bounty Programs

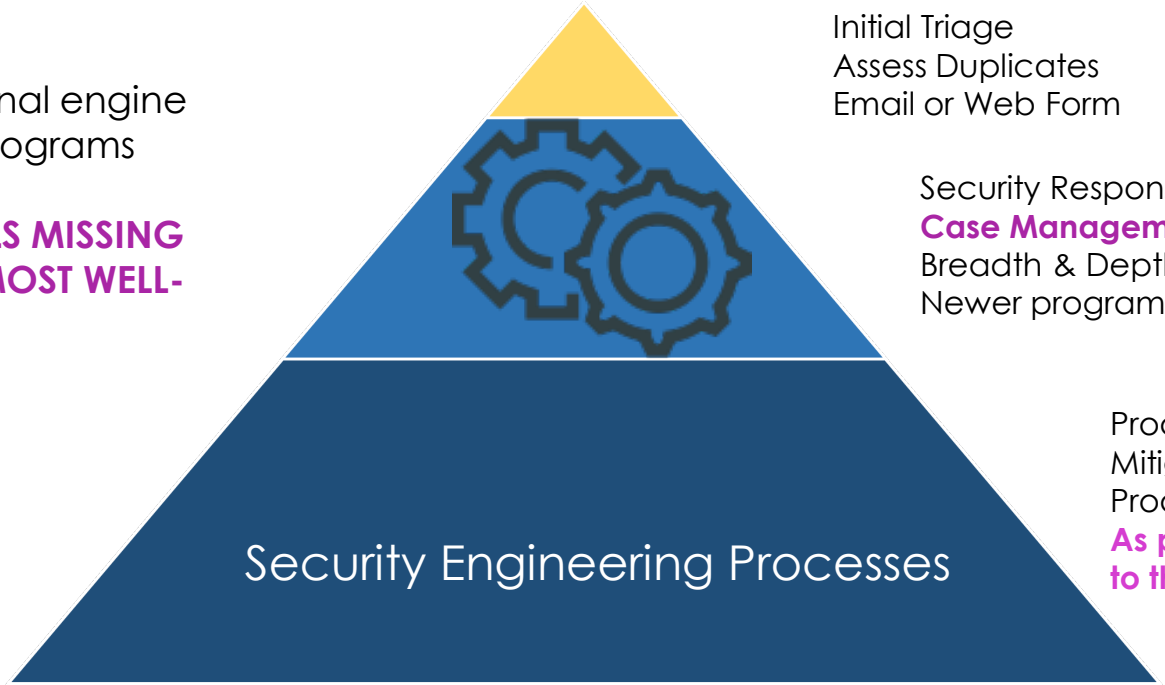
- Cash rewards for bugs
- Can be structured & targeted
- AVOID NDAs HERE!
- **Bug Bounties only work if you can fix the bugs!**

88% of the Forbes Global 2000 have NO PUBLISHED WAY to report a security vulnerability.

Best Practices: Resource Allocation for VDPs

The 2nd layer is the operational engine of Vulnerability Disclosure Programs

KEY PEOPLE, PROCESS, TOOLS MISSING IN MOST ORGS - EVEN THE MOST WELL-RESOURCED



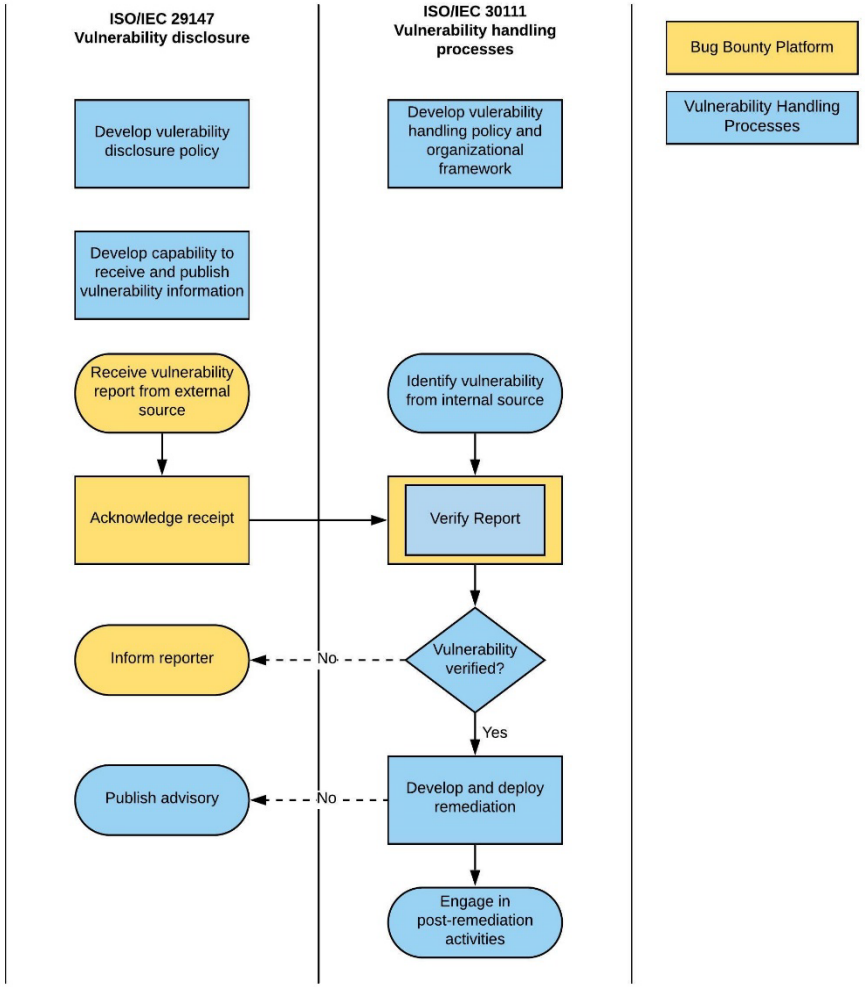
Initial Triage
Assess Duplicates
Email or Web Form

Security Response Center / Product Security
Case Management – Researcher interface
Breadth & Depth Analysis
Newer programs- the majority of work focused here

Product Engineering
Mitigation Strategy
Product roadmap evaluation
As programs mature- the majority of work shifts to this layer

VDPs accelerate the need to improve internal security engineering, secure development, and internal case management infrastructure

ISO Standards 29147 & 30111



Not everyone is ready to implement ISO 29147, Vulnerability Disclosure

Everyone should be ensuring vulnerability handling compliance with ISO 30111 first

Scalable VDPs require planning, training, & resources

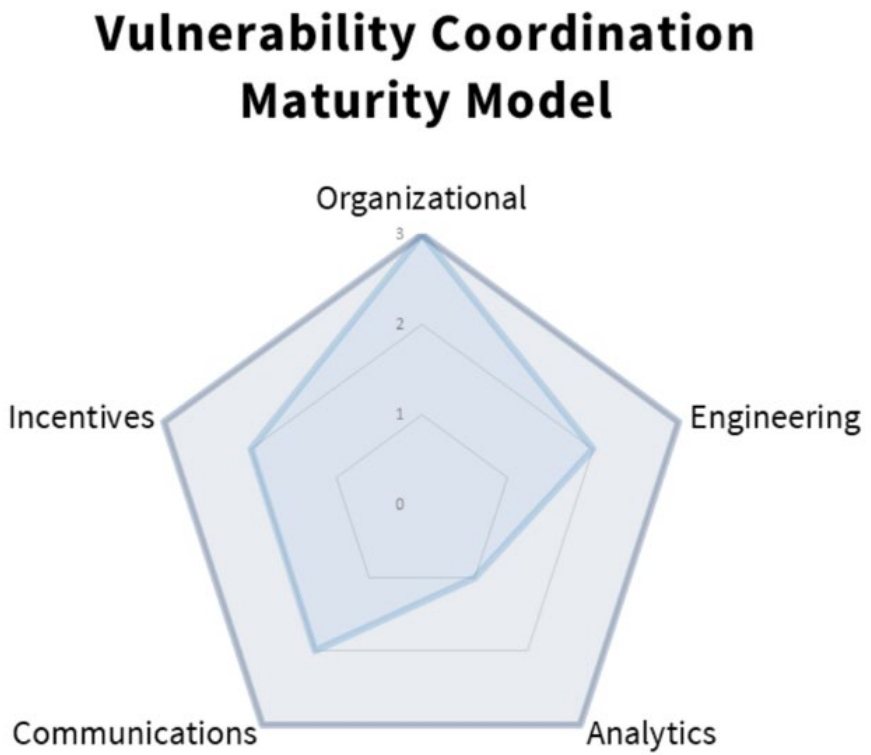
Commercial bug bounty platforms are not replacements for ISO 30111 or 29147

Discussion: Was This What You Were Expecting?

Maturity Assessment -VCMM

To improve overall security, every organization needs to benchmark its capabilities and identify and prioritize areas that need improvement.

The Vulnerability Coordination Maturity Model (VCMM) provides a framework that evaluates five key areas to help organizations measure and evolve their vulnerability management capabilities.



www.lutasecurity/vcmm

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. **Learn from mistakes to mature.**

Analytics:

Data analysis of vulnerabilities to identify trends and improve processes

Level -- Capability

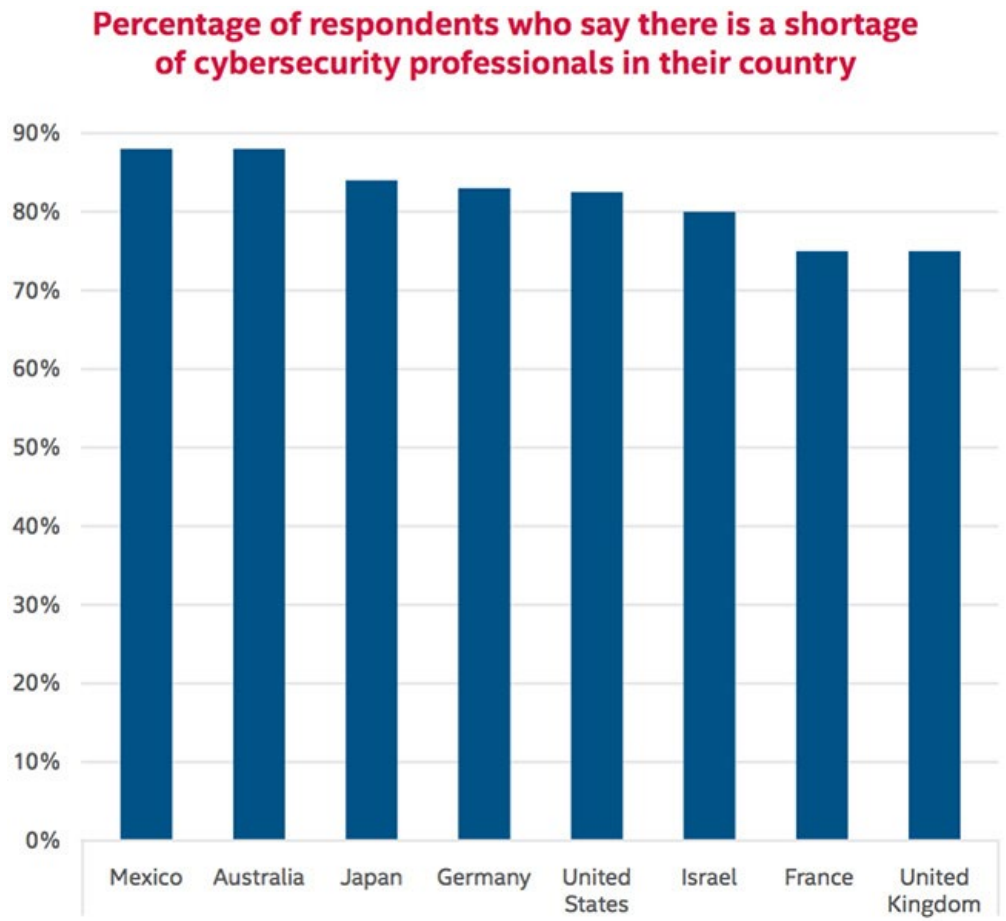
- **Basic:** Track the number and severity of vulnerabilities over time to **measure improvements in code quality**.
- **Advanced:** Use root cause analysis to **feed back into your software development lifecycle.** See ISOs 29147, 30111, 27034.
- **Expert:** Track **real-time telemetry of active exploitation** 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.

#NotAllBugs Are Created (or Fixed) Equally

Creating a Vulnerability Typology

Vulnerability Characteristics	Quantity of Vulnerabilities	➢	Scarce - Numerous
	Ease of Vulnerability Discovery	➢	Easy - Difficult to Find
	Likelihood of Vulnerability Rediscovery	➢	Low - High
Patching Dynamics	Technical Difficulty of Remediation	➢	Easy - Hard to Fix
	Logistical Difficulty of Remediation	➢	Easy - Hard to Access
	Average Life of a Vulnerability	➢	Short - Long
Market Dynamics	Third Party Market for Vulnerability	➢	Offensive, Defensive, Mixed, Etc.
	Market Size	➢	Small - Large
	Bug Bounty Program	➢	Yes, No
Human Dynamics	Attackers	➢	Criminals, States, Patriots, Etc.
	Researcher Pool	➢	Small - Large
	Attacker Motivation	➢	Political, Financial, Reputational

Cyber Workforce Shortage = Opportunity



82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations.[1]

Unfilled cybersecurity jobs has grown by more than 50 percent since 2015.[3]

By 2022, the global cybersecurity workforce shortage is predicted to exceed 1.8 million unfilled positions.[4]

https://www.csis.org/analysis/cybersecurity-workforce-gap

https://www.helpnetsecurity.com/2016/07/28/cybersecurity-talent-crisis/

Triage Labor – The Job You'll Never Love

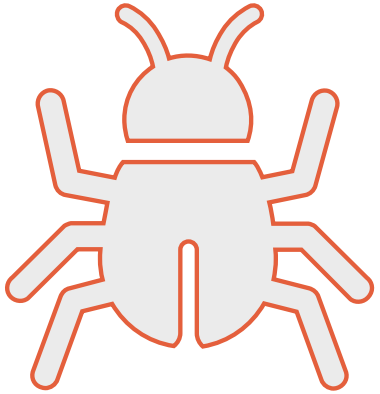
Microsoft receives between 150,000-200,000 non-spam email messages per year to secure@Microsoft .

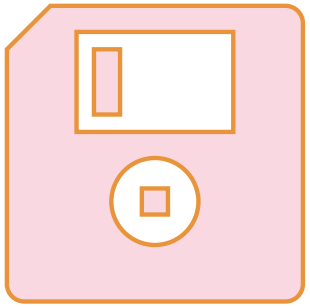
In 2007, Popular Science named "**Microsoft Security Grunt**" among the **Top 10 Worst Jobs in Science**.

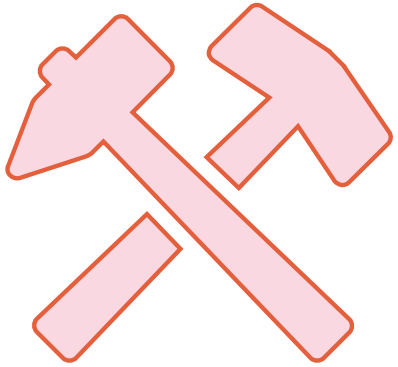
- This lands the triage/case management job between "**Whale Feces Researcher**" and "**Elephant Vasectomist**"
- This role is full-time, **pays six figures plus full benefits**, is held by several team members, & has the **highest turnover** of any job in the Microsoft Security Response Center

Labor Market for Bug Hunting vs. Issue Remediation & Incident Response /Investigation

- The [bug hunting] labor market is **highly-stratified**…characterized by a minority of…lucrative workers and a majority of low-volume…low-earning workers"[2]
- Tiny fraction of talent; Majority generate **noise**
- Bug bounty hunting celebrated for outpacing median developer salaries (16x in India, 40x in Argentina)?!
- Top 10 CS programs in US universities don't require security to graduate. 3/10 lack security electives.
- **We are cranking out more bug writers than software developers & building a permanently indefensible ecosystem**







Vital Metrics for Best Security Outcomes

(cannot get this data from current BB platforms)

- Code quality & vulnerability handling maturity indicators
  - Granular duplicate rates
  - Vulnerability taxonomy
- Cyber workforce preparedness & labor market
  - Assess personnel needs in anticipation of shortages in the labor market for cyber security
  - Use VCMM to identify gaps in people, process, technology

Indicators with data we have now spanning the past several years shows:

Poorly designed VDPs & BBs are not efficient at reducing risk or increasing skilled domestic labor.

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. **Establish vulnerability disclosure handling processes.** 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 and VDPs won't replace other security testing.

Hackers can help you – if you let them!

References, Contact, & Questions
THANK YOU!

Katie at Lutasecurity dot com
Sign up for a Workshop LutaSecurity.com/workshops
VCMM@LutaSecurity.com
@LutaSecurity @k8em0

- [1]https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=E162FD54-F858-44AE-B25F-64E331C628AE
- [2]Ryan Ellis, Keman Huang, Michael Siegel, **Katie Moussouris**, and James Houghton. "Fixing a Hole: The Labor Market for Bugs." New Solutions for Cybersecurity. Howard Shrobe, David L. Shrier, and Alex Pentland, eds. Cambridge: MIT Press. In Press. ISBN: 9780262535373 https://mitpress.mit.edu/books/new-solutions-cybersecurity
- [3]https://www.rsaconference.com/writable/presentations/file_upload/ht-r04f-but_now_i_see_-_a_vulnerability_disclosure_maturity_model.pdf
- [4]https://www.rsaconference.com/writable/presentations/file_upload/ht-t08-the-wolves-of-vuln-street-the-1st-dynamic-systems-model-of-the-0day-market_final.pdf

Appendix

Vulnerability Coordination Maturity Model

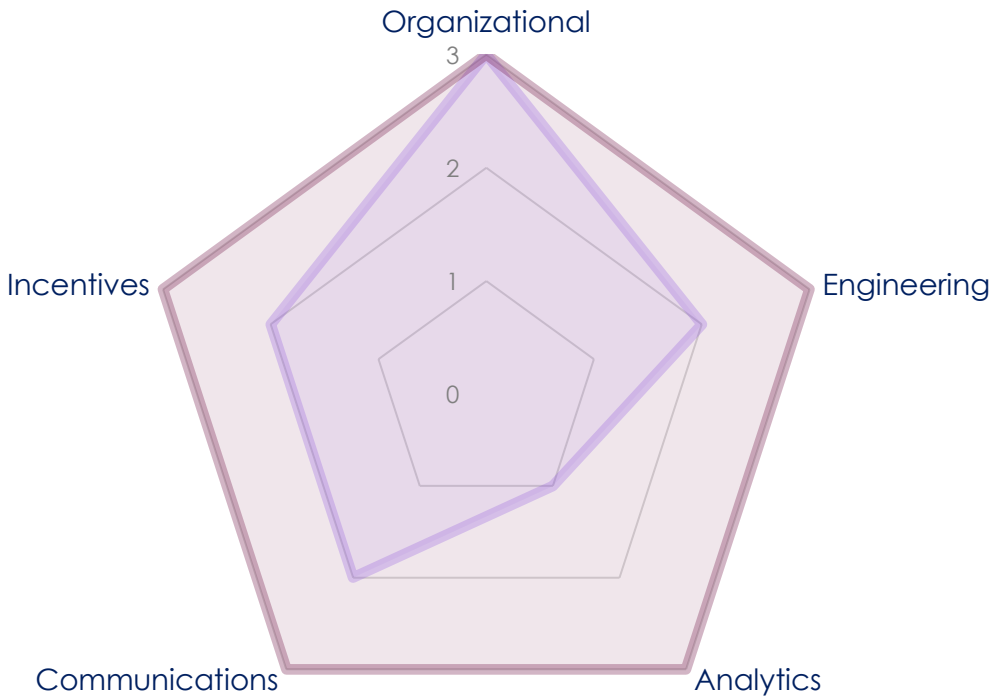
LUTA SECURITY

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.

Contact Luta Security

All code has vulnerabilities. We can help.

Contact: VCMM@LutaSecurity.com

www.LutaSecurity.com