

Part 1: Vulnerability Management You Can  
Live With (And Might Even Like)

Part 2: Breathwork For Better... Everything

---

Robert Kerby - PancakesCon 2023



# April 5 1995...SATAN



## Quotes about SATAN

---

### Pre-release:

"It's like randomly mailing automatic rifles to 5,000 addresses. I hope some crazy teen doesn't get a hold of one." (Oakland tribune.)

"SATAN is like a gun, and this is like handing a gun to a 12-year-old." (LA times.)

"It's like distributing high-powered rocket launchers throughout the world, free of charge, available at your local library or school, and inviting people to try them out by shooting at somebody." (San jose mercury.)

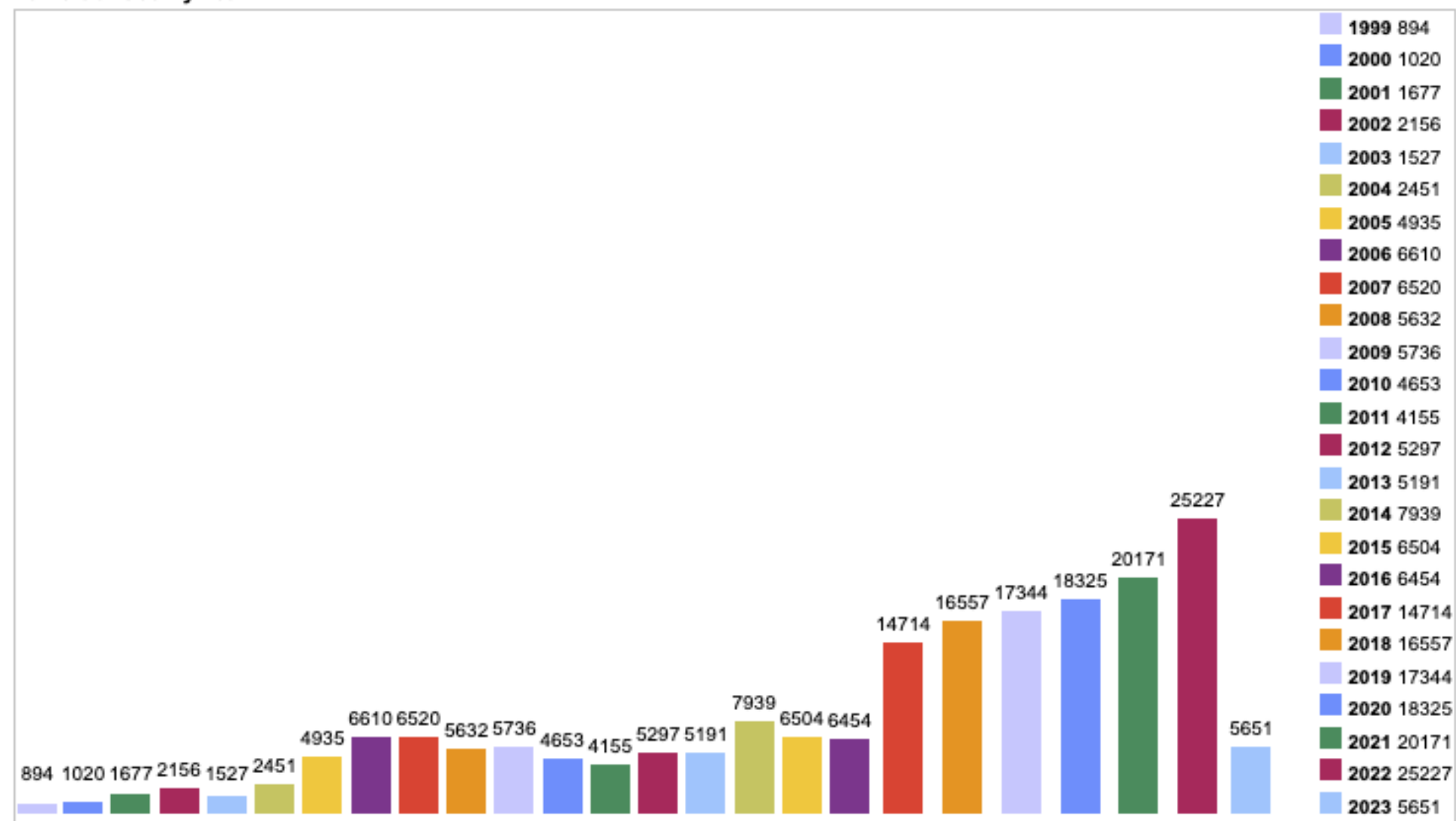
"It discovers vulnerabilities for which we have no solutions." (The New York Times.)

"...people could die." (vikr@aol.com (VikR))

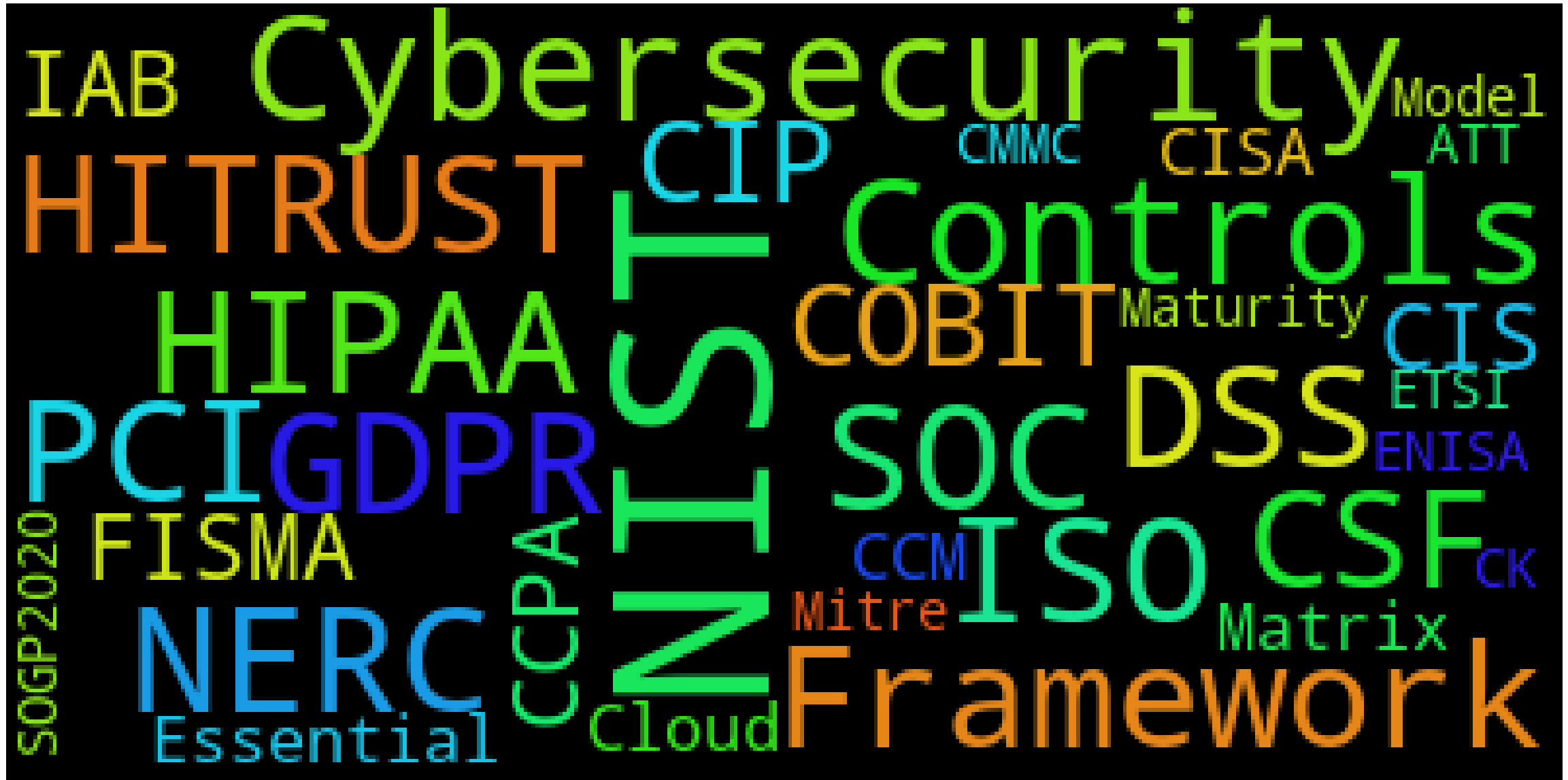
### Post-release:

"...there is no obscuring its presence. It announces itself like a rock concert to the scanned machine's log file." (Nick Christenson, npc@minotaur.jpl.nasa.gov)

**Vulnerabilities By Year**







# PR.IP-12: A vulnerability management plan is developed and implemented

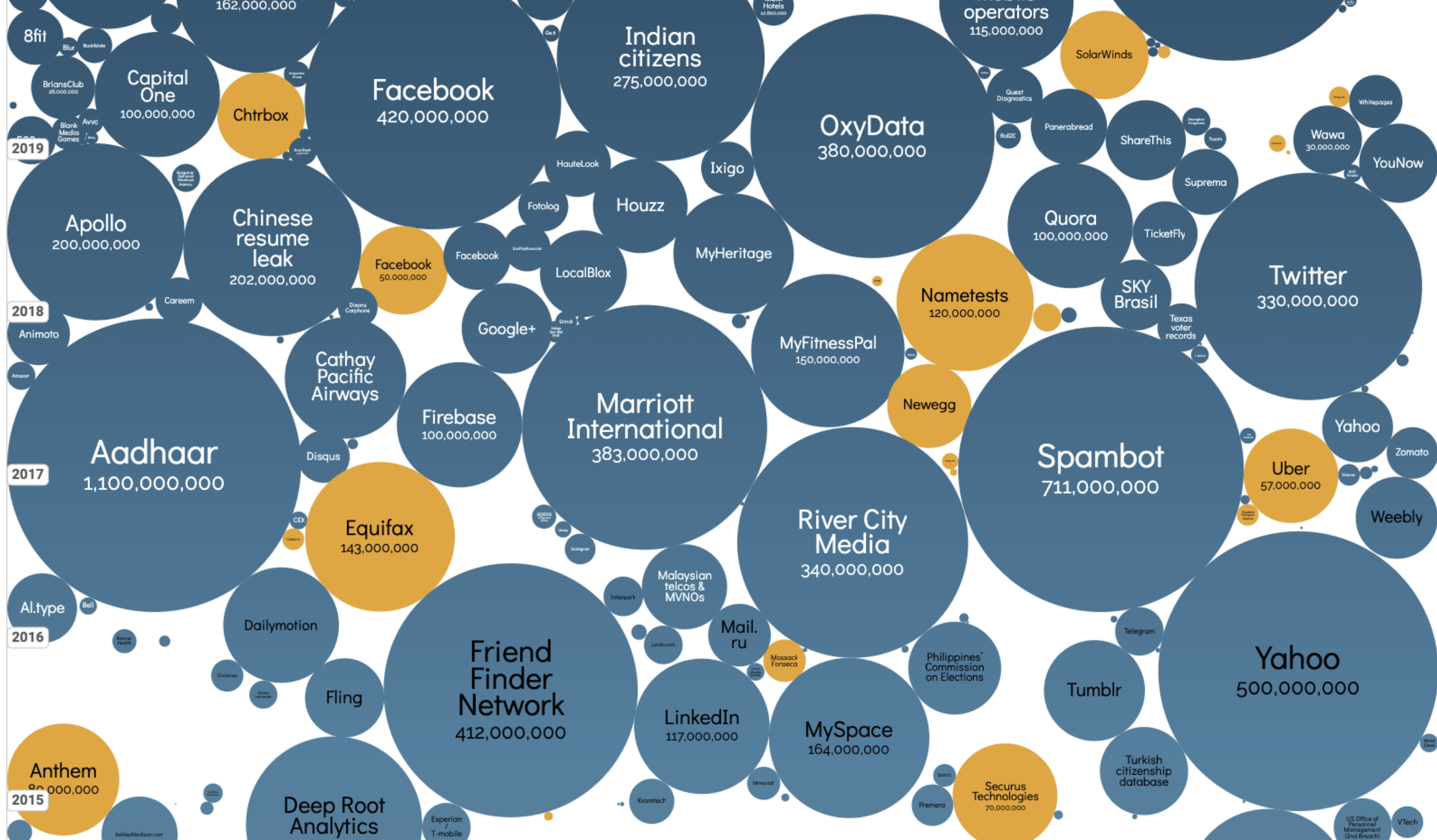
- RA-1: Policy and Procedures
- RA-3: Risk Assessment
- RA-5: Vulnerability Monitoring and Scanning
- SI-2: Flaw Remediation
- 3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified
- 3.11.3: Remediate vulnerabilities in accordance with risk assessments
- 3.12.2: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems
- .....



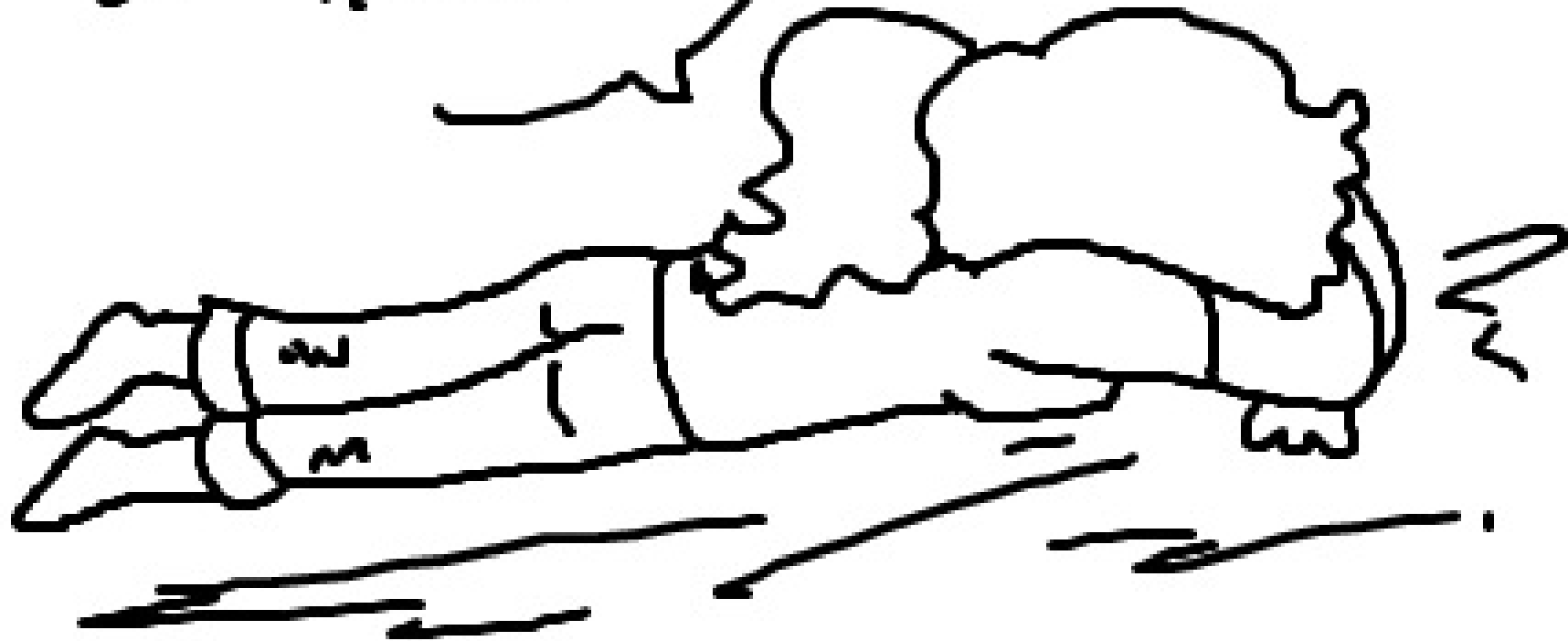


and  
then  
what?





Why is everything  
so hard...?



# Vulnerability Management Challenges



**Incomplete Asset Inventory** – I've scanned all 10 things I know about



**Overwhelming Scope** – Yeah, the last scan has been running for 6 days and we need to start the next one



**What to Work on First** – This all seems important to me



**Manual Processes** – Hold on one minute, I'm starting the  $10^5$  scan of the week



**Reporting** – Numbers are Hard



**Lack of Resources** – I'll take 10 additional headcount please

Maybe...






Design Thinking +  
Architecture = 😊

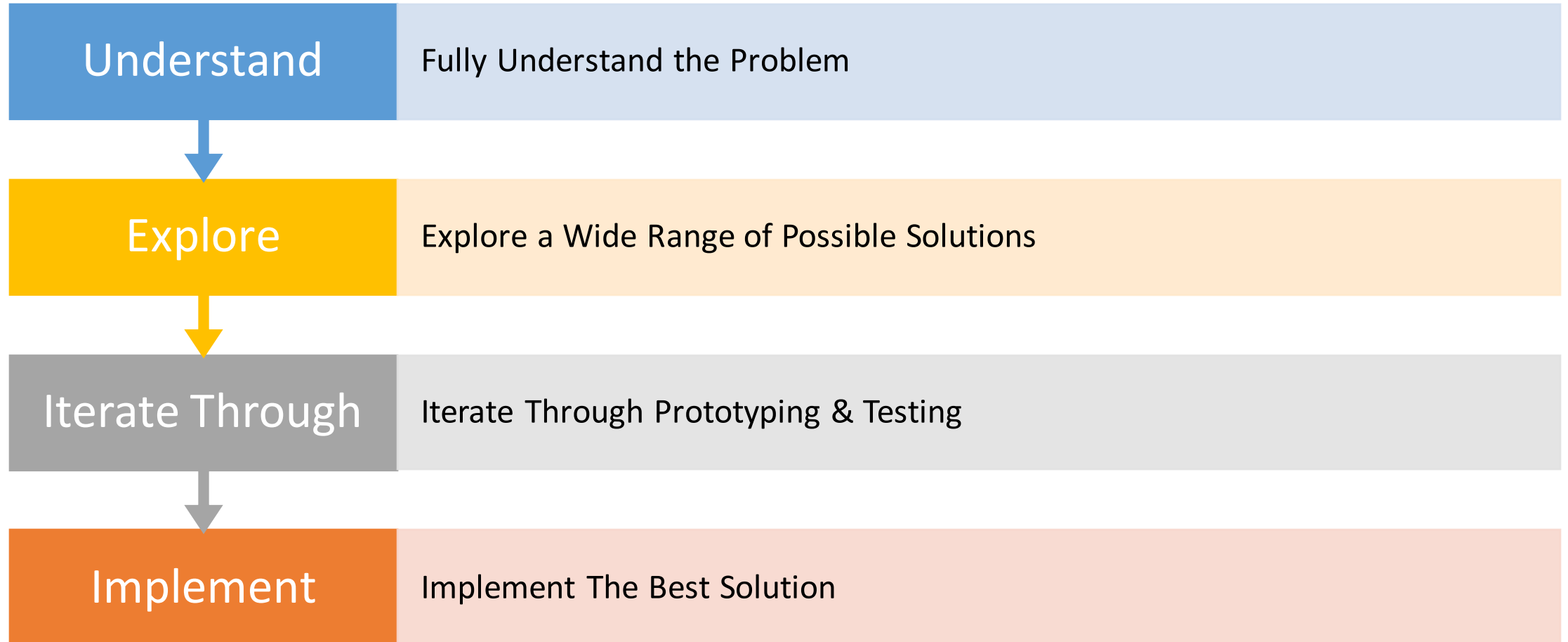


# What is Design Thinking?



With design thinking, throwing out what you think you know and starting from scratch opens all kinds of possibilities.

# Steps to Design Thinking





**pause**





What is  
Architecture?

A Shared Understanding of System Design



# Components of an Architecture

Requirements

"ilities"

Decisions

A Visual Structure

Design Thinking +  
Architecture = 😊



# From Design Thinking

- Who Will Be:
  - Using vulnerability scanners
  - Relying on vulnerability data
  - Building asset inventory
- What Will They:
  - Do with vulnerability information
  - Need to fix a vulnerability
  - Have to report to external entities
- Etc.



# From Architecture



Will I use the same tool for asset discovery and vulnerability scanning?



Can I show the life of a vulnerability from discovery to remediation?



How long can my vulnerability management process be unavailable?



Can I automate the end-to-end process?

# In Practice...

I want to be able to discover assets

I want to be able to import asset information programmatically

I want to be able to set different scopes for asset discovery

I want asset discovery to be separated from vulnerability scanning

I want to be able to deduplicate multiple sources of asset information

I want to be able scan multiple asset types including: physical machines (e.g., IoT devices), virtual machines, containers, applications, databases for vulnerabilities

I want to be able to scan multiple asset OS types including: Microsoft Windows, Linux, macOS, etc.

I want to be able to scan with different scan policies e.g., only high and critical vulnerabilities, only CVEs with known exploits, etc.



Discovery / Inventory

Scanning

Prioritization

Context / Attribution

Ticketing

Validation / Exceptions

Metrics / Reporting

# Easy Steps to Implementation



CREATE A LIST OF  
STAKEHOLDERS



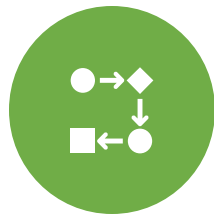
CREATE A LIST OF  
REQUIREMENTS



DRAW A PICTURE OF  
HOW YOU THINK  
THIS WILL WORK



CREATE A LIST OF  
USE CASES



TEST & ITERATE



# Resources

- Github: <https://github.com/beardedwanderer/VulnerabilityManagementStuff>
- Design Thinking: <https://mitsloan.mit.edu/ideas-made-to-matter/design-thinking-explained>
- Architecture: <https://nocomplexity.com/documents/arplaybook/introduction.html>
- Crayons: [https://www.amazon.com/Crayola-Ultra-Washable-Crayons-1-Pack/dp/B00N3K1SAK/ref=sr\\_1\\_8?crid=1352G93WUJL6T&keywords=crayons&qid=1679171952&srefix=crayons%2Caps%2C136&sr=8-8](https://www.amazon.com/Crayola-Ultra-Washable-Crayons-1-Pack/dp/B00N3K1SAK/ref=sr_1_8?crid=1352G93WUJL6T&keywords=crayons&qid=1679171952&srefix=crayons%2Caps%2C136&sr=8-8)