CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

WHAT IT TAKES TO RUN AMERICA'S VULNERABILITY MANAGEMENT TEAM

Panelists: Sandy Radesky (moderator), Chris Hughes (co-moderator), Bob Lord, Lindsey Cerkovnik, Pat Garrity

TLP CLEAR

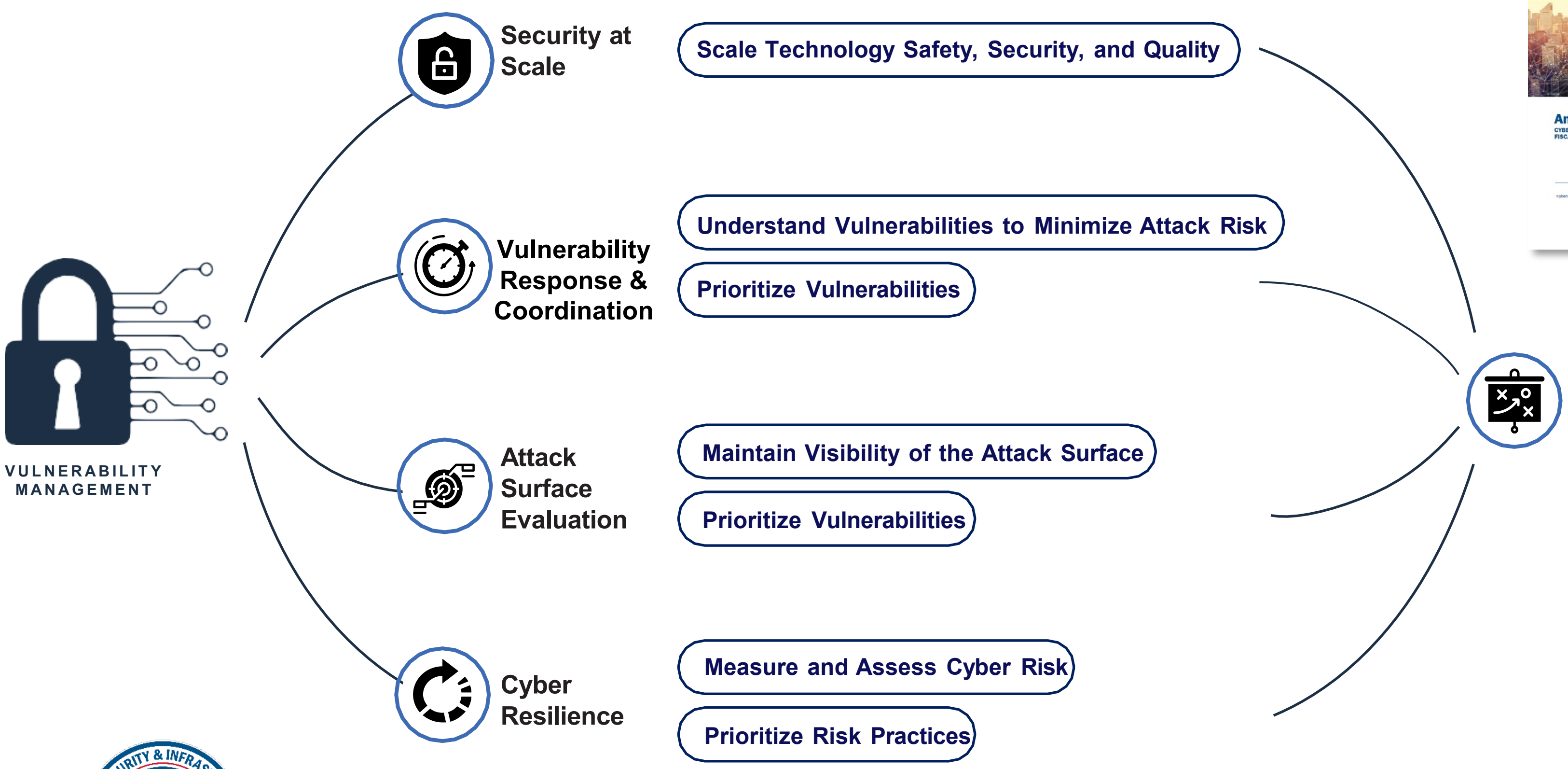
March 26, 2024

VM Operational Design | What We Do

VM Mission | Enable cyber risk reduction to proactively strengthen national infrastructure resilience.

VM Vision | Trusted, credible, and timely vulnerability ecosystem management advantages for the nation.

VM Essential Tasks



VULNERABILITY MANAGEMENT

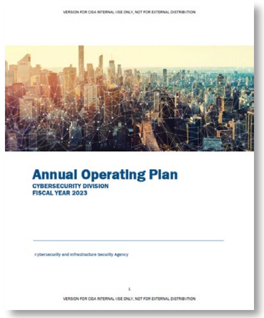
Security at Scale
- Scale Technology Safety, Security, and Quality

Vulnerability Response & Coordination
- Understand Vulnerabilities to Minimize Attack Risk
- Prioritize Vulnerabilities

Attack Surface Evaluation
- Maintain Visibility of the Attack Surface
- Prioritize Vulnerabilities

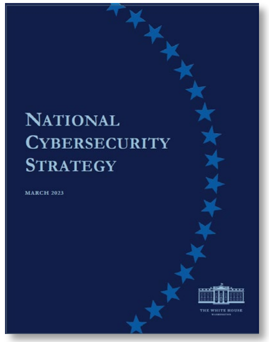
Cyber Resilience
- Measure and Assess Cyber Risk
- Prioritize Risk Practices

Insights

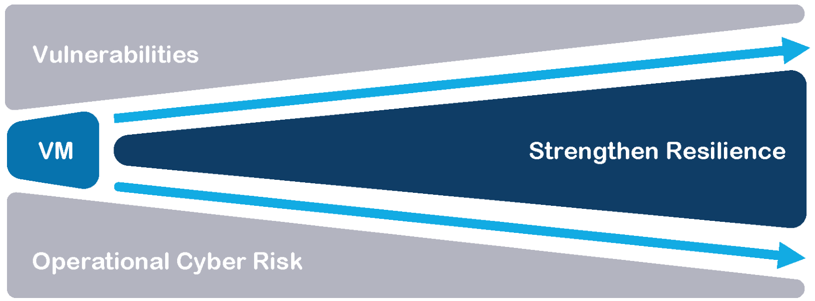


Annual Operating Plan
CYBERSECURITY DIVISION
FISCAL YEAR 2023

CISA
STRATEGIC PLAN
2023–2025



NATIONAL CYBERSECURITY STRATEGY
MARCH 2023



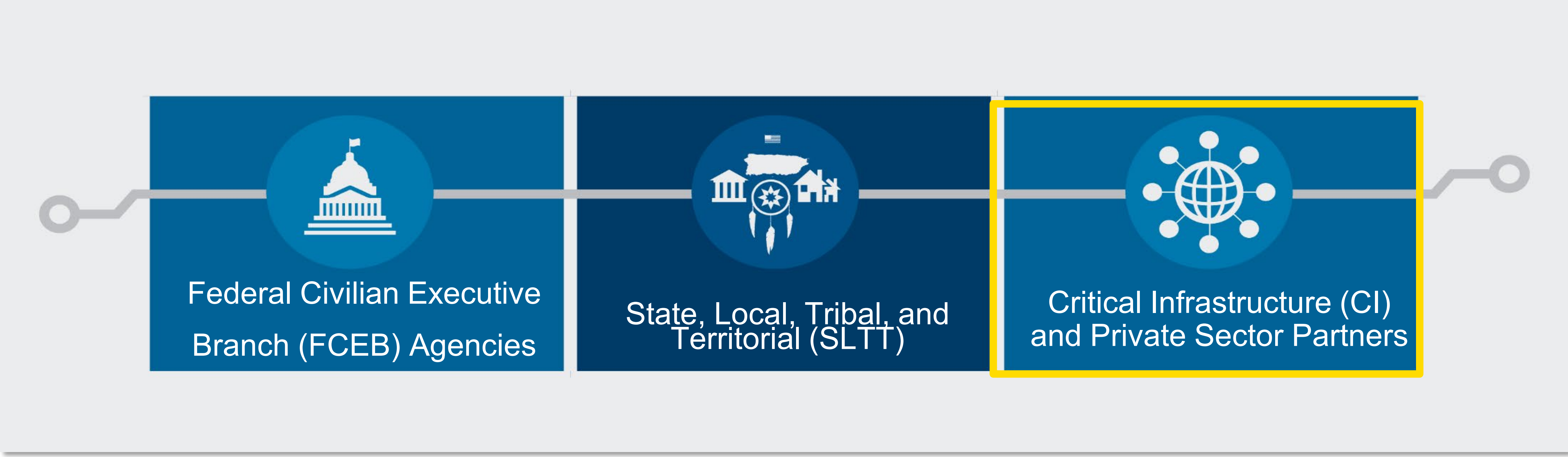
Scale Technology Safety, Security, and Quality

Understand Vulnerabilities to Minimize Attack Risk

TLP:CLEAR

March 26, 2024

VM Customers equal “America”

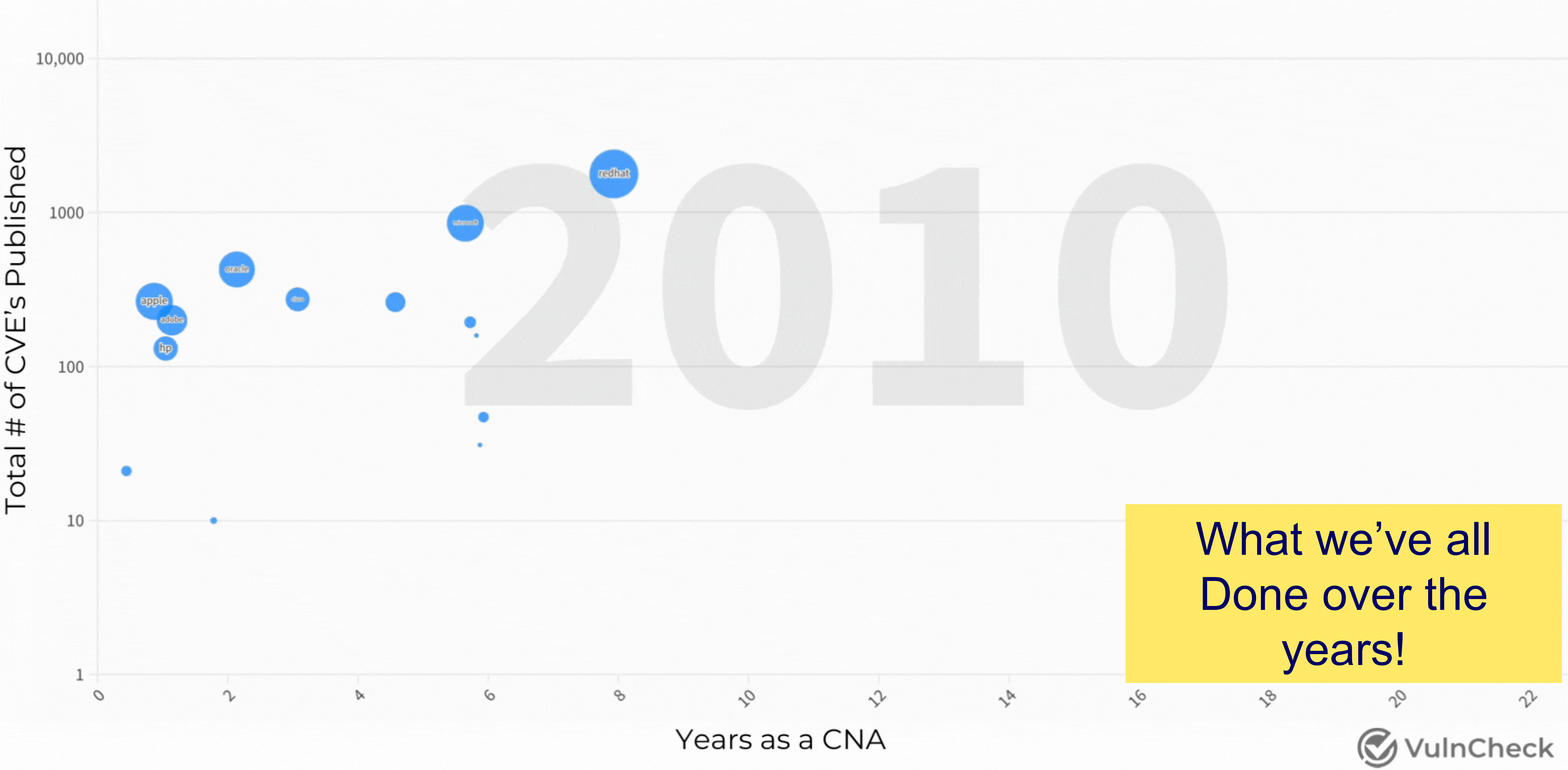


Federal Civilian Executive Branch (FCEB) Agencies

State, Local, Tribal, and Territorial (SLTT)

Critical Infrastructure (CI) and Private Sector Partners

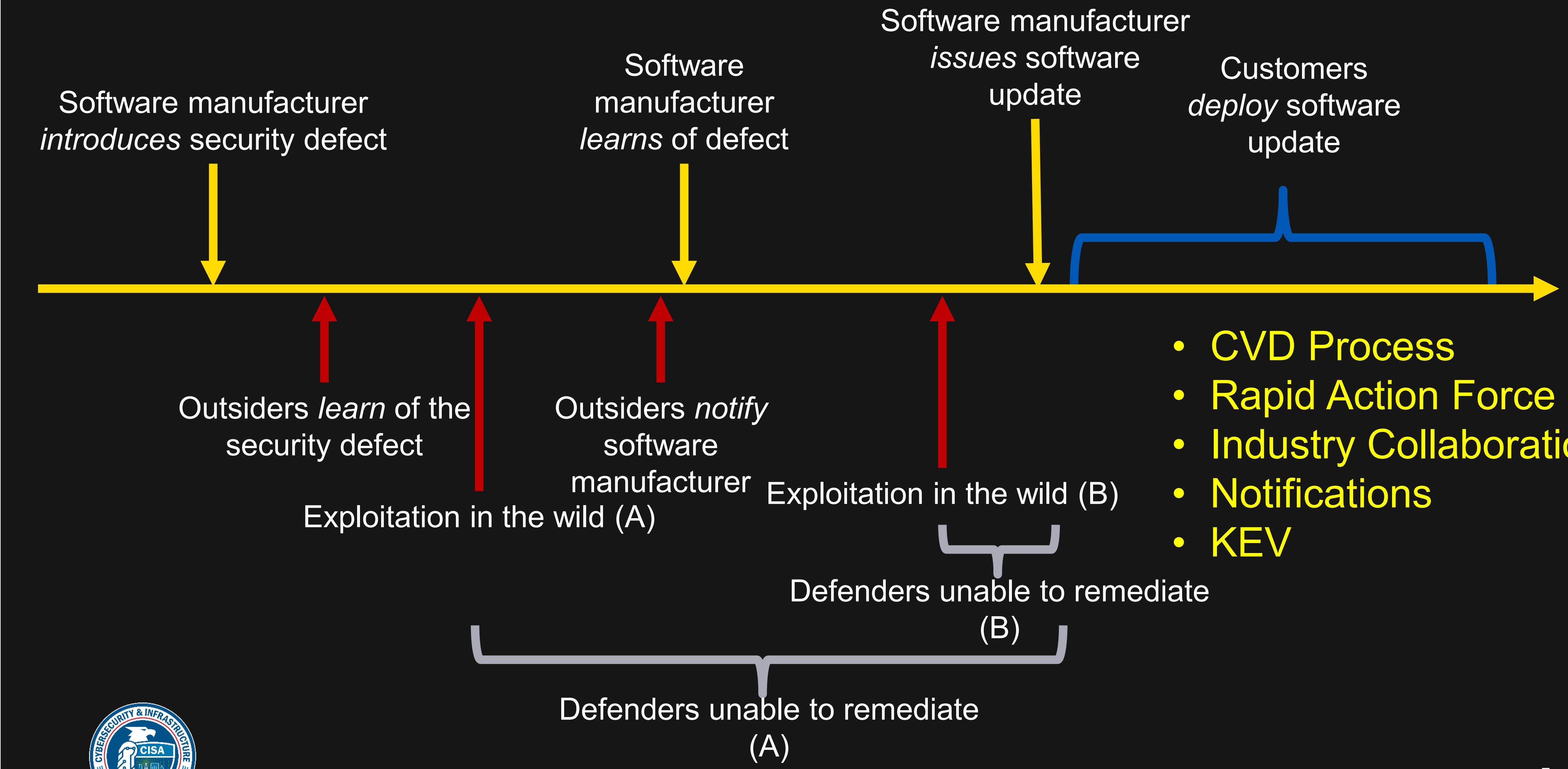
CVEs Published by CNAs Over Time



What we've all Done over the years!

VulnCheck

Topic 1: Vulnerability Response Life Cycle (Today)



Software manufacturer *introduces* security defect

Outsiders *learn* of the security defect

Exploitation in the wild (A)

Outsiders *notify* software manufacturer

Software manufacturer *learns* of defect

Exploitation in the wild (B)

Software manufacturer *issues* software update

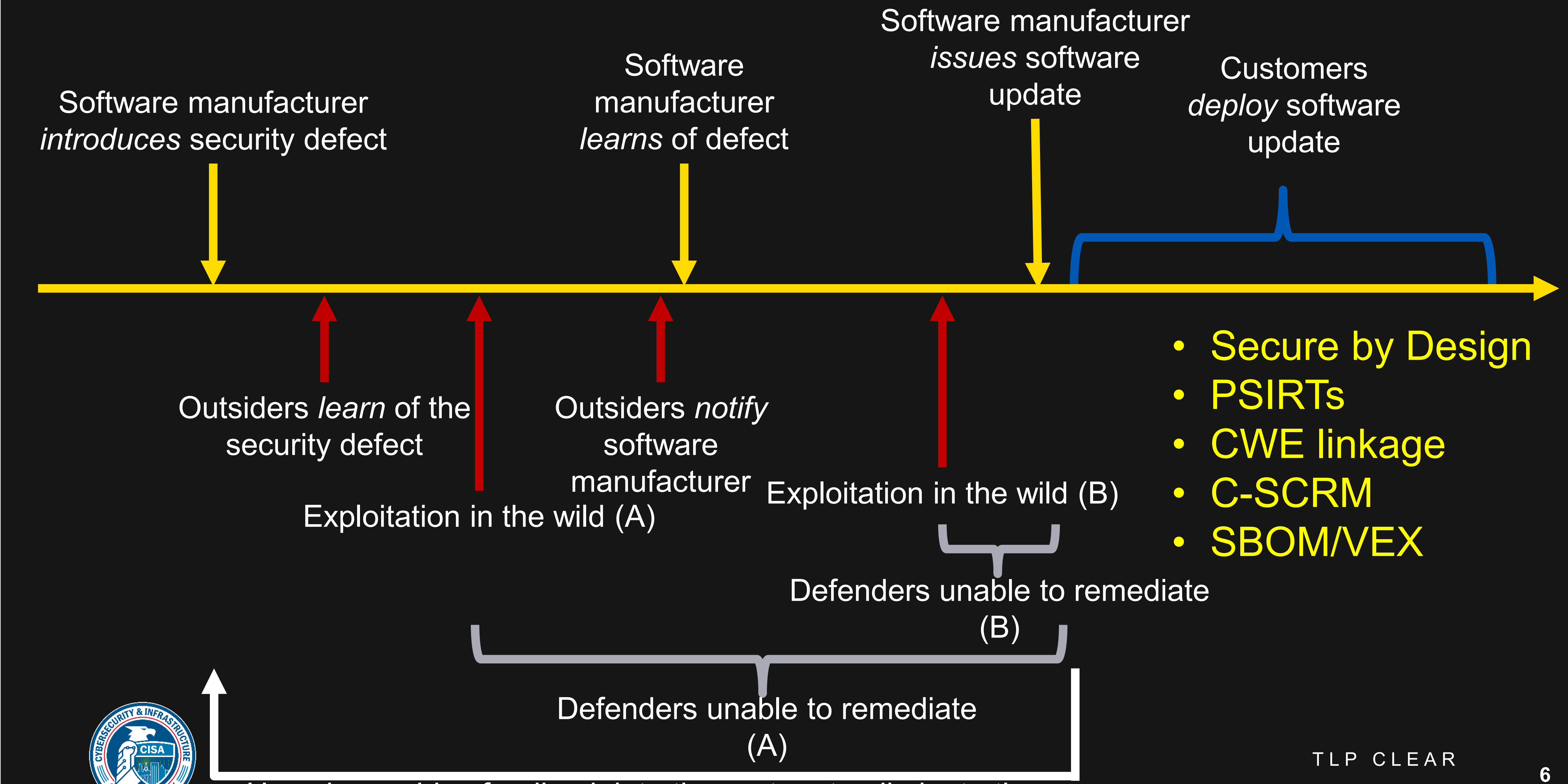
Customers *deploy* software update

Defenders unable to remediate (B)

Defenders unable to remediate (A)

- CVD Process
- Rapid Action Force
- Industry Collaboration
- Notifications
- KEV

Topic 2: Move to the Left



Software manufacturer *introduces* security defect

Outsiders *learn* of the security defect

Exploitation in the wild (A)

Software manufacturer *learns* of defect

Outsiders *notify* software manufacturer

Exploitation in the wild (B)

Software manufacturer *issues* software update

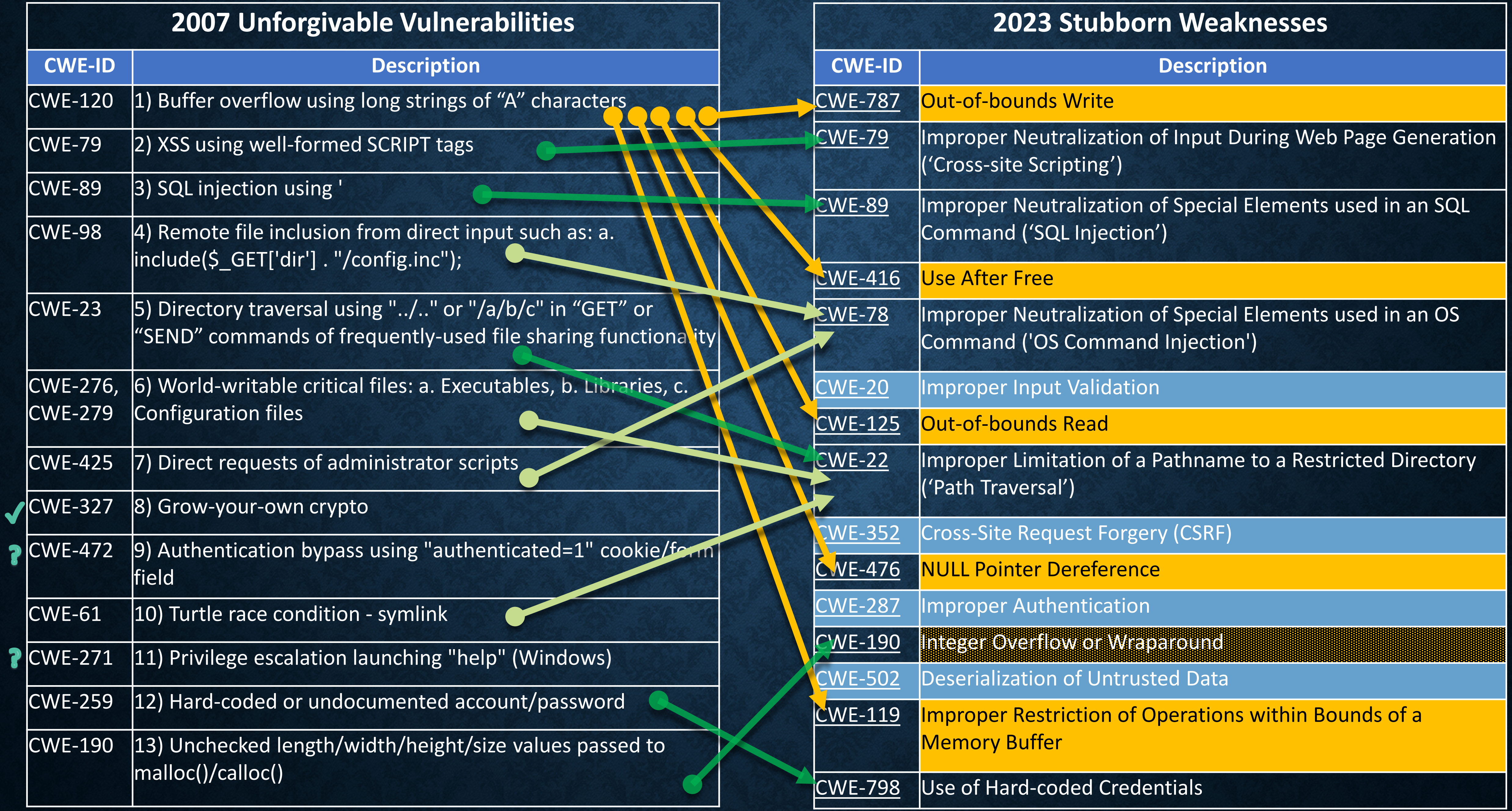
Customers *deploy* software update

Defenders unable to remediate (B)

Defenders unable to remediate (A)

- Secure by Design
- PSIRTs
- CWE linkage
- C-SCRM
- SBOM/VEX

How do we drive feedback into the system to eliminate the unforgivable vulnerabilities?



2007 Unforgivable Vulnerabilities

CWE-ID	Description
CWE-120	1) Buffer overflow using long strings of "A" characters
CWE-79	2) XSS using well-formed SCRIPT tags
CWE-89	3) SQL injection using '
CWE-98	4) Remote file inclusion from direct input such as: a. include($_GET['dir'] . "/config.inc");
CWE-23	5) Directory traversal using "../.." or "/a/b/c" in "GET" or "SEND" commands of frequently-used file sharing functionality
CWE-276, CWE-279	6) World-writable critical files: a. Executables, b. Libraries, c. Configuration files
CWE-425	7) Direct requests of administrator scripts
✓ CWE-327	8) Grow-your-own crypto
? CWE-472	9) Authentication bypass using "authenticated=1" cookie/form field
CWE-61	10) Turtle race condition - symlink
? CWE-271	11) Privilege escalation launching "help" (Windows)
CWE-259	12) Hard-coded or undocumented account/password
CWE-190	13) Unchecked length/width/height/size values passed to malloc()/calloc()

2023 Stubborn Weaknesses

CWE-ID	Description
CWE-787	Out-of-bounds Write
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-416	Use After Free
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-20	Improper Input Validation
CWE-125	Out-of-bounds Read
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-476	NULL Pointer Dereference
CWE-287	Improper Authentication
CWE-190	Integer Overflow or Wraparound
CWE-502	Deserialization of Untrusted Data
CWE-119	Improper Restriction of Operations within Bounds of a Memory Buffer
CWE-798	Use of Hard-coded Credentials

Memory safety CWEs

Thoughts on Next Steps

- How do we get to actual risk reduction ?
- How can this group become a catalyst for change ?
- What do we think software companies need to do make safer higher quality software ?

TLP CLEAR

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA