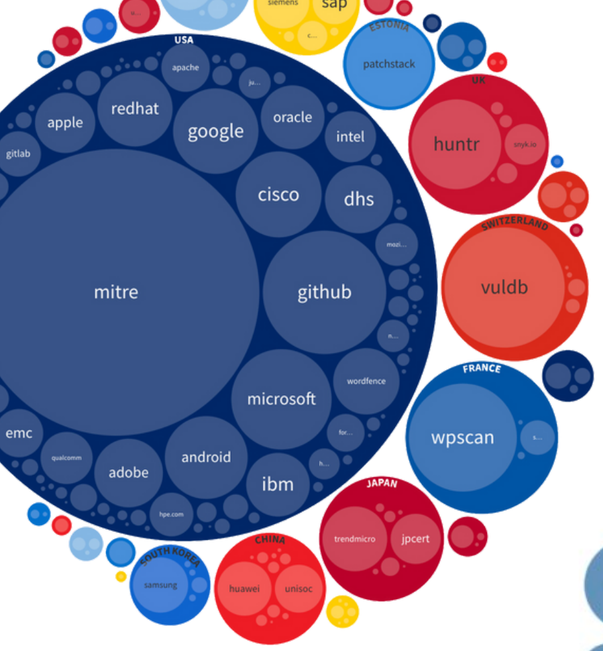
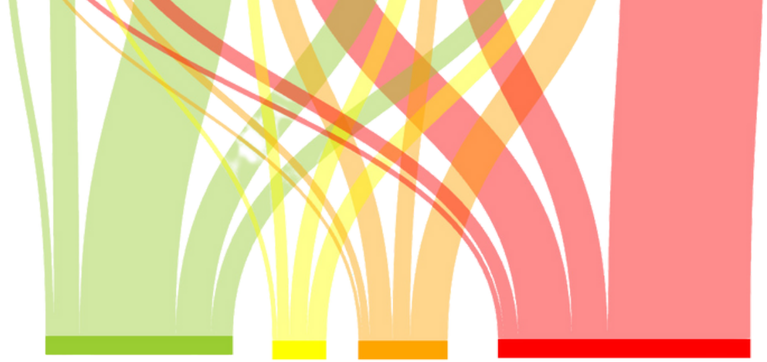
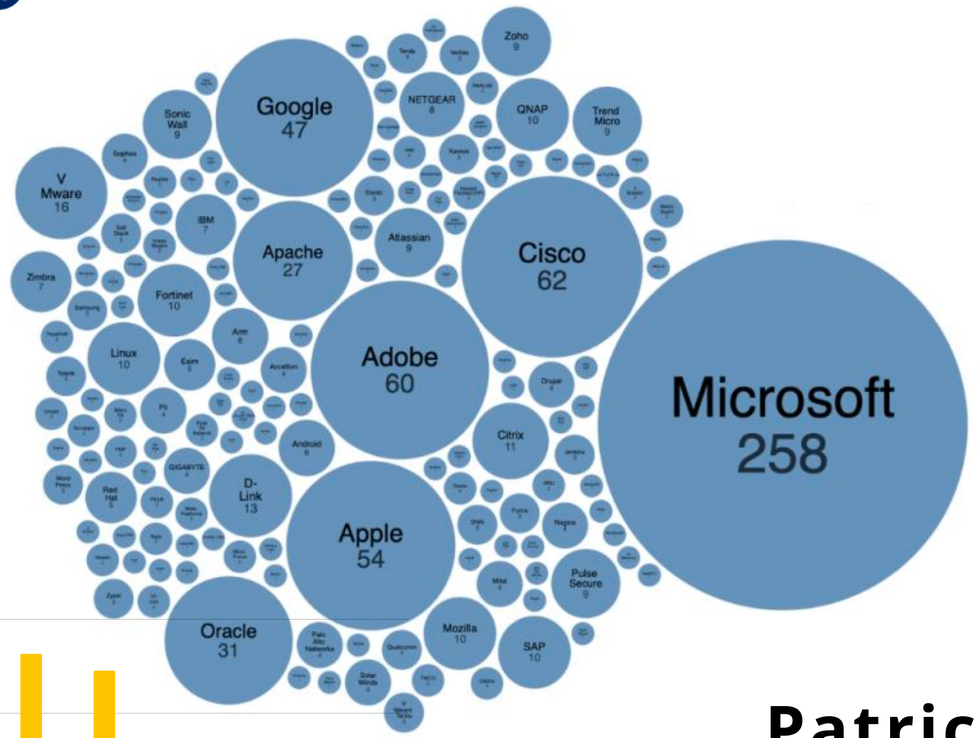
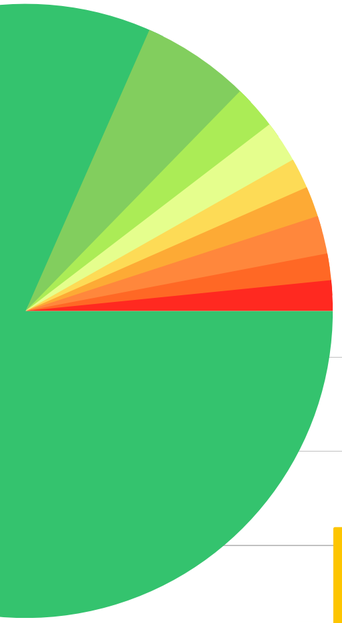








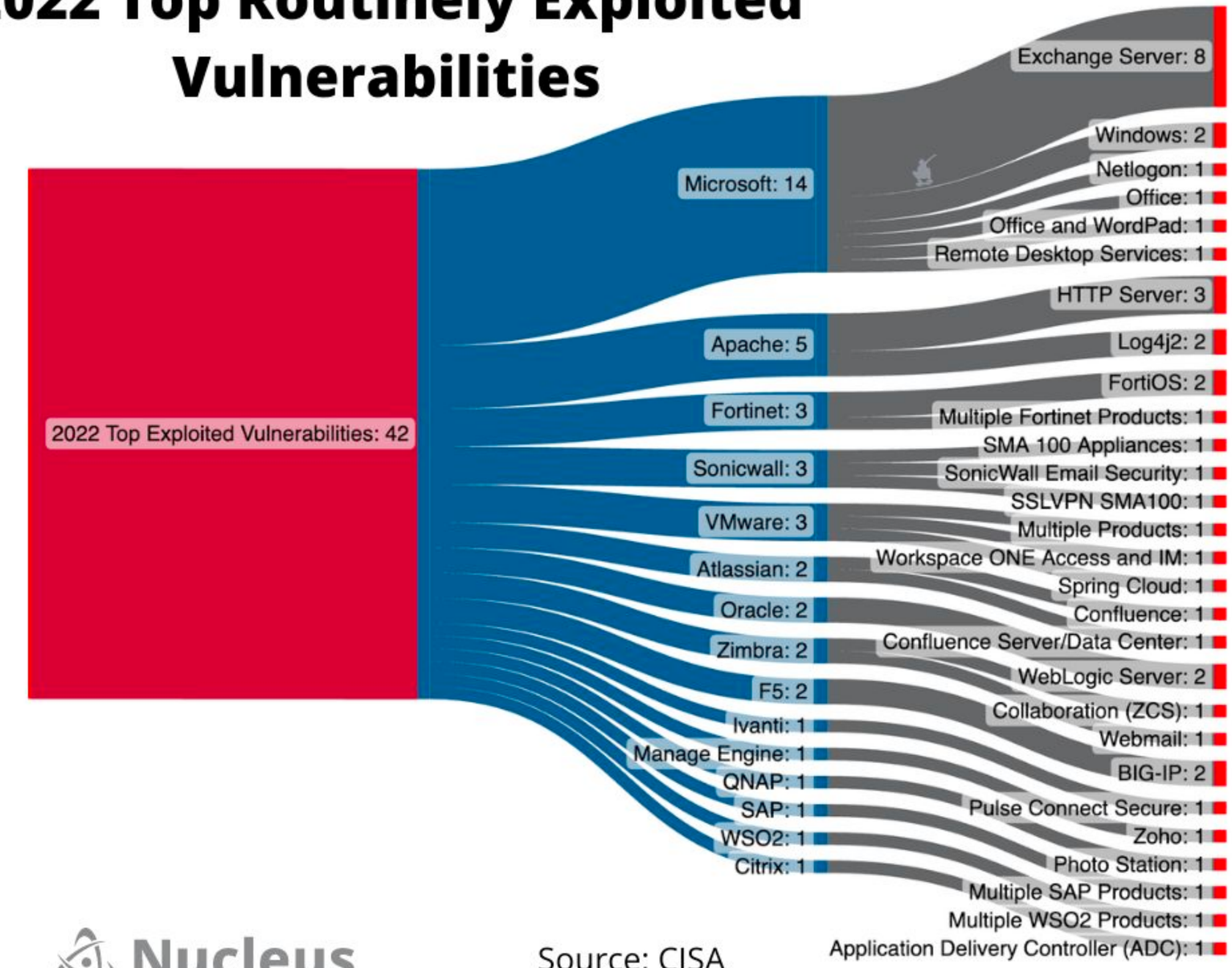
Nucleus

INSIGHTS INTO VULNERABILITY MANAGEMENT

Patrick Garrity
Security Researcher
/in/patrickmgarrity/


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA
KEV

2022 Top Routinely Exploited Vulnerabilities



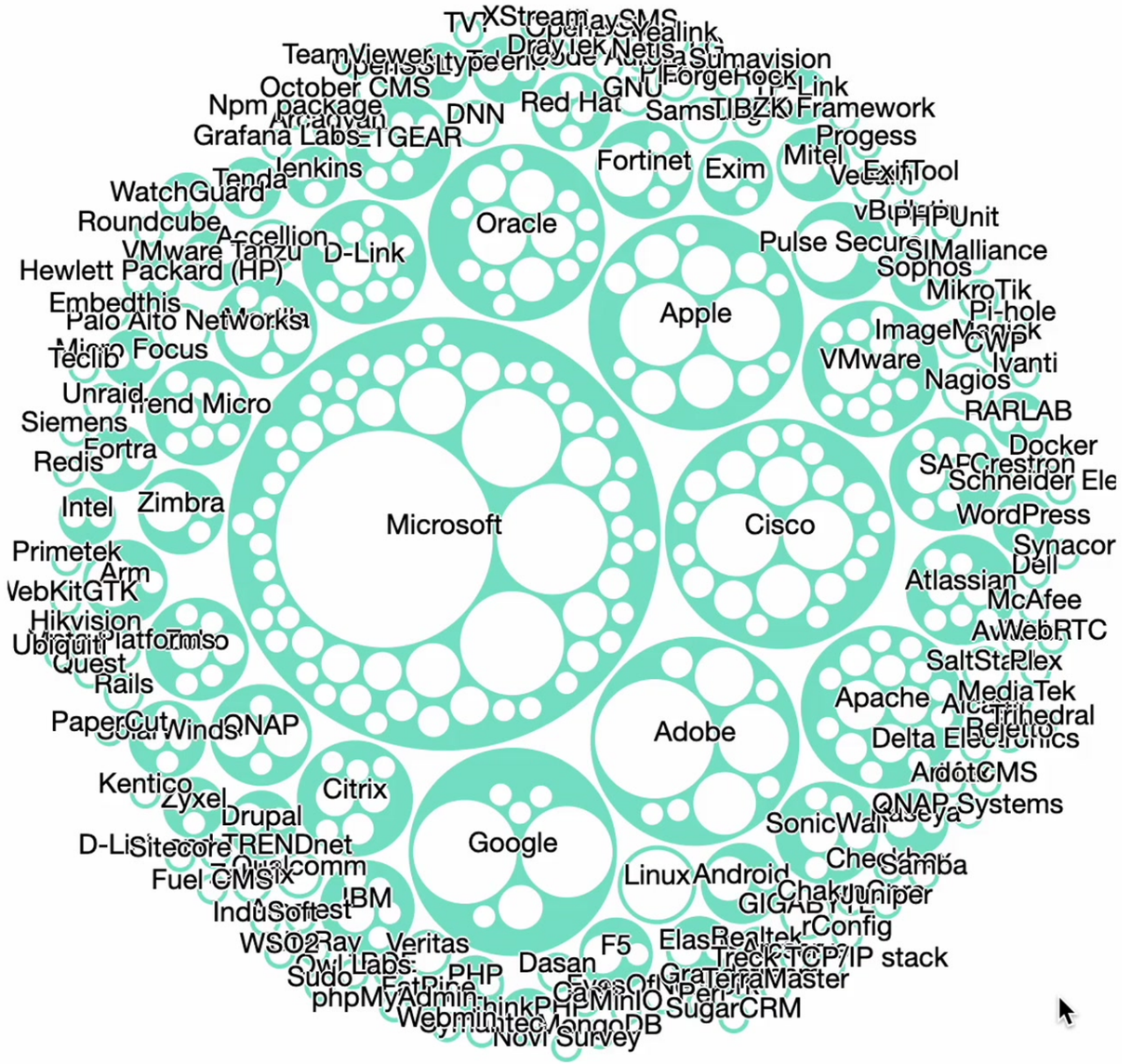
Nucleus

Source: CISA

Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

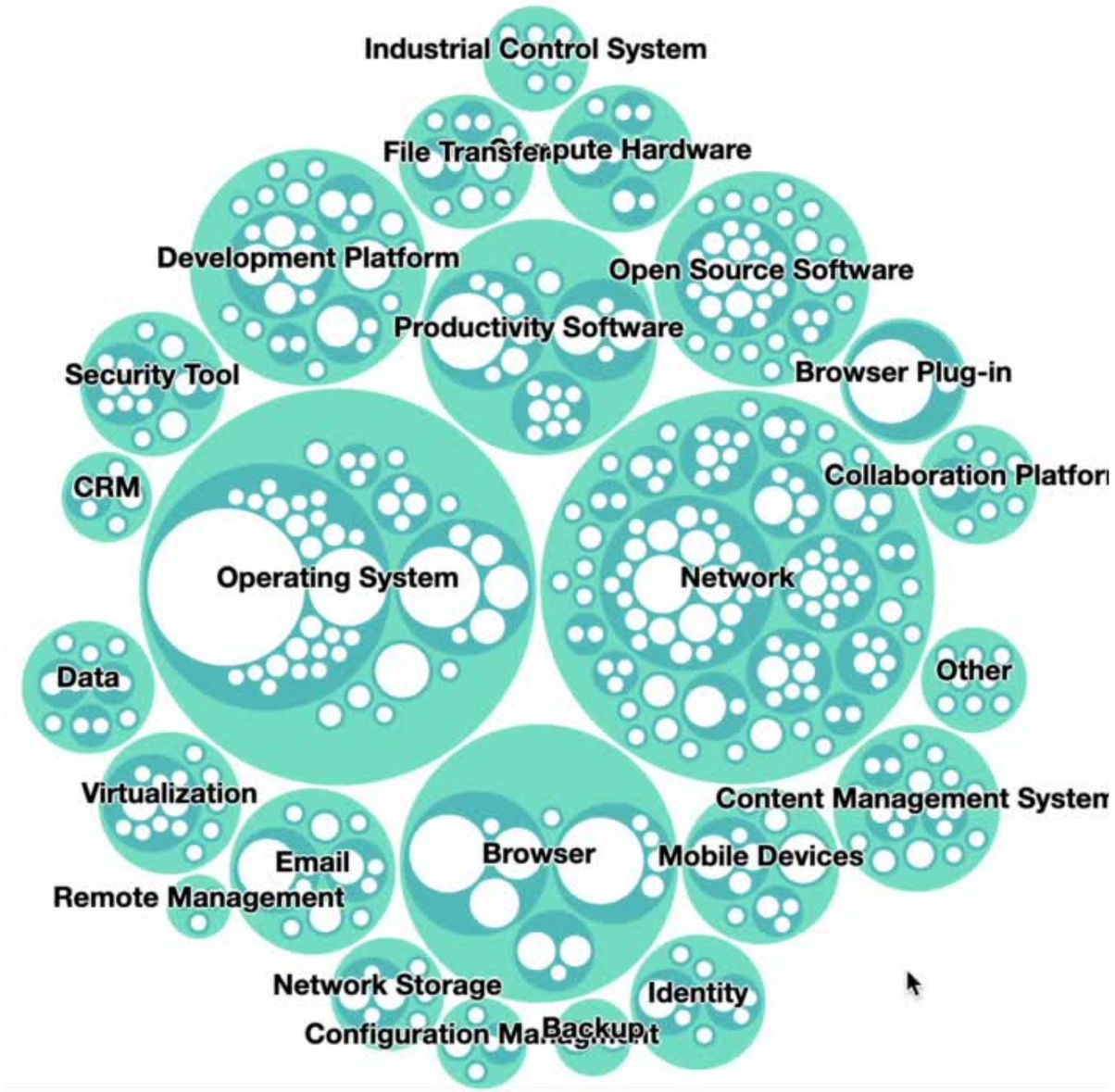
CISA Known Exploited Vulnerabilities (925)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

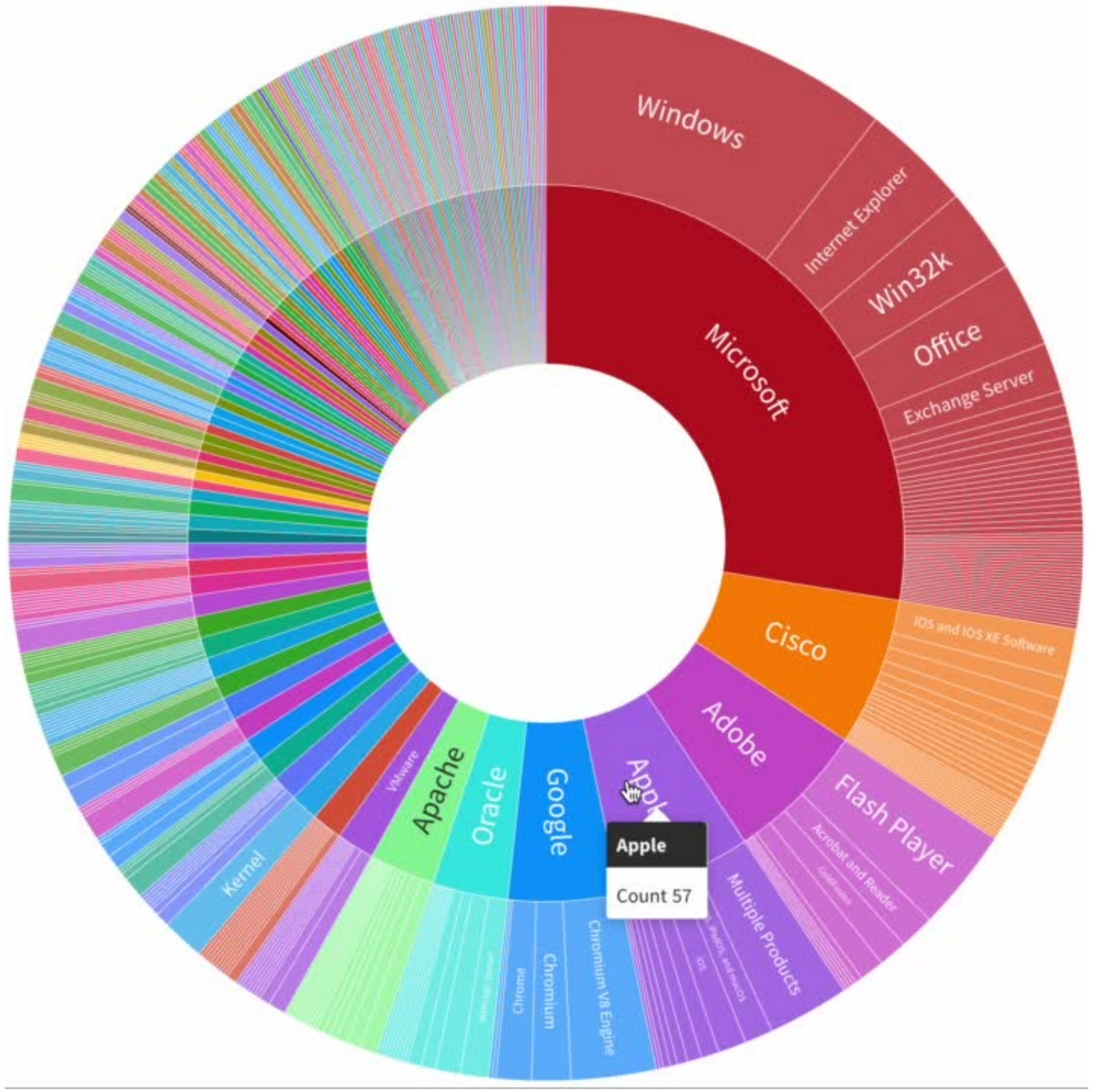
CISA Known Exploited Vulnerabilities Categorized by Type (977)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

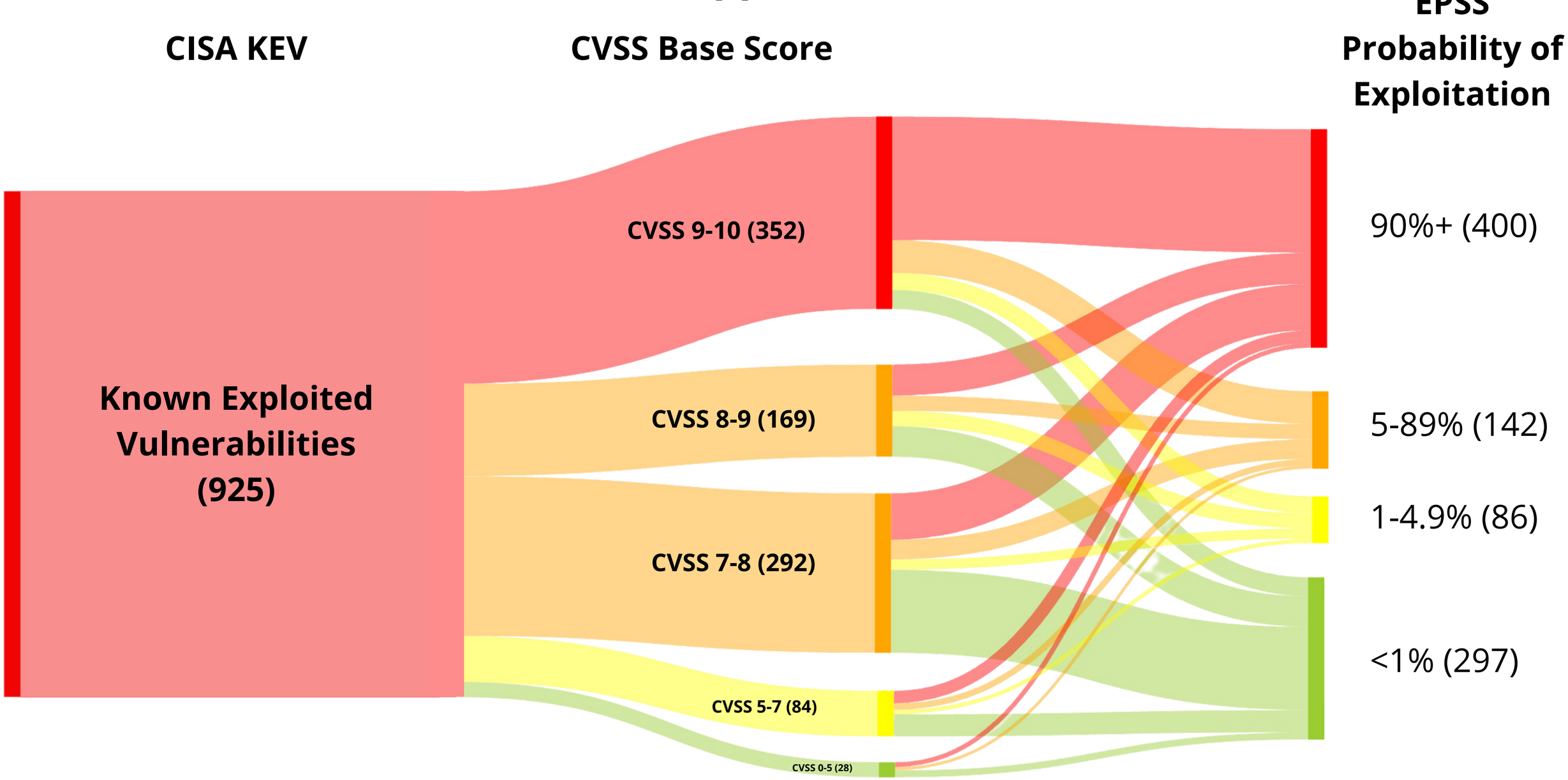
Interactive CISA KEV Vendor > Product Mapping to CVSS & EPSS



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

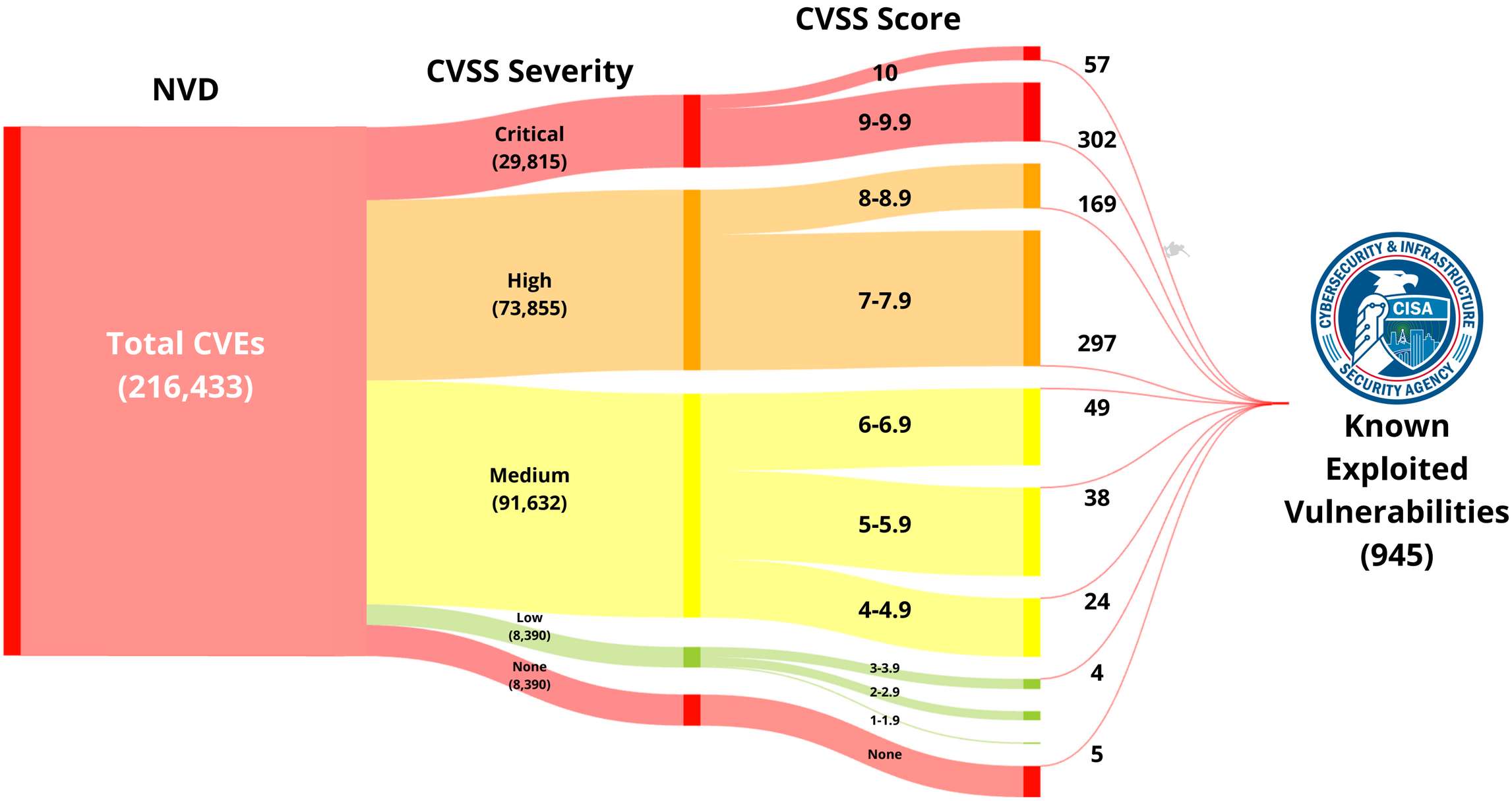
CISA KEV Mapped to CVSS & EPSS



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

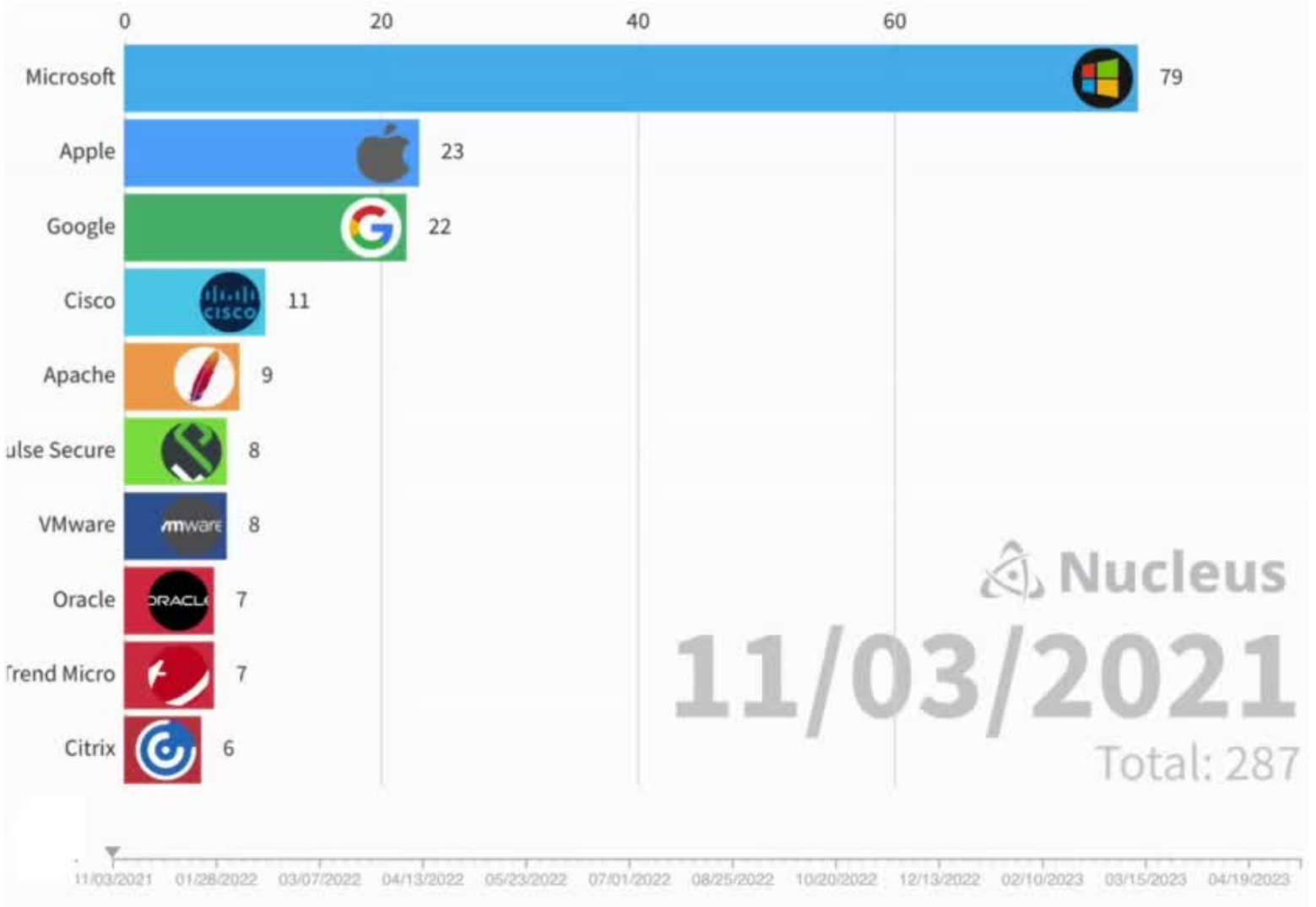
NVD Mapped to CVSS & CISA KEV



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

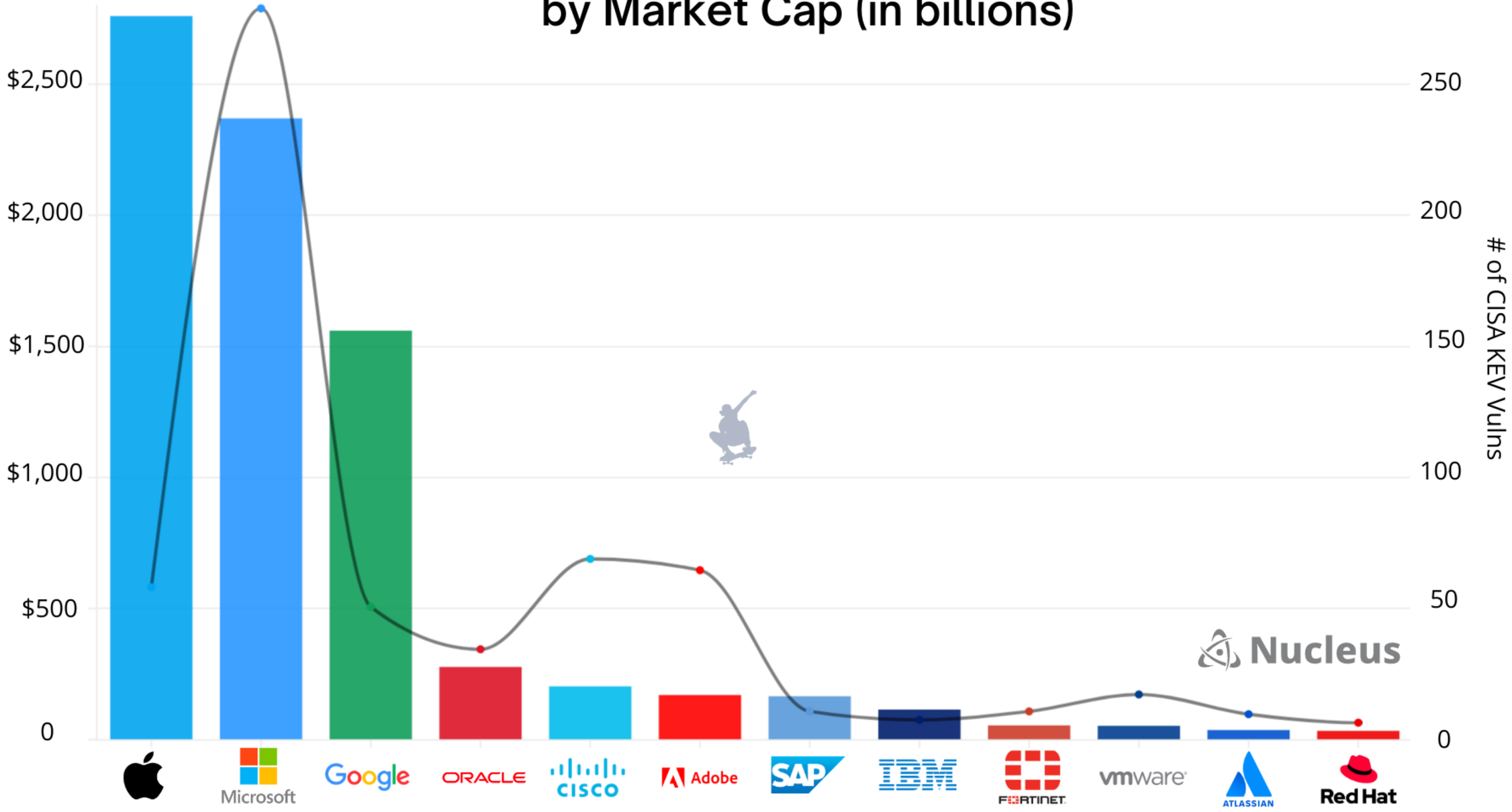
CISA Known Exploited Vulnerabilities (933)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

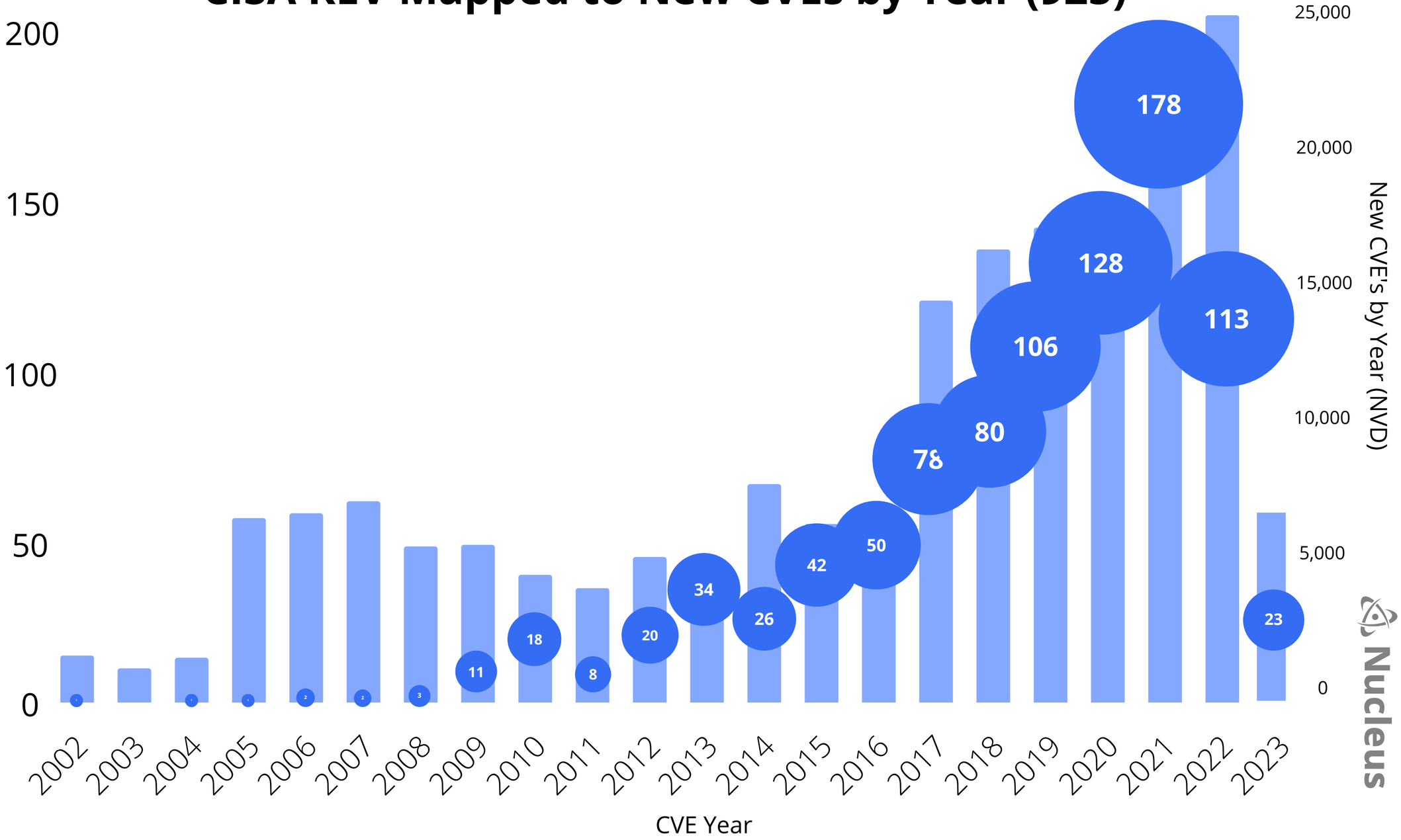
CISA Known Exploited Vulnerabilities by Market Cap (in billions)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

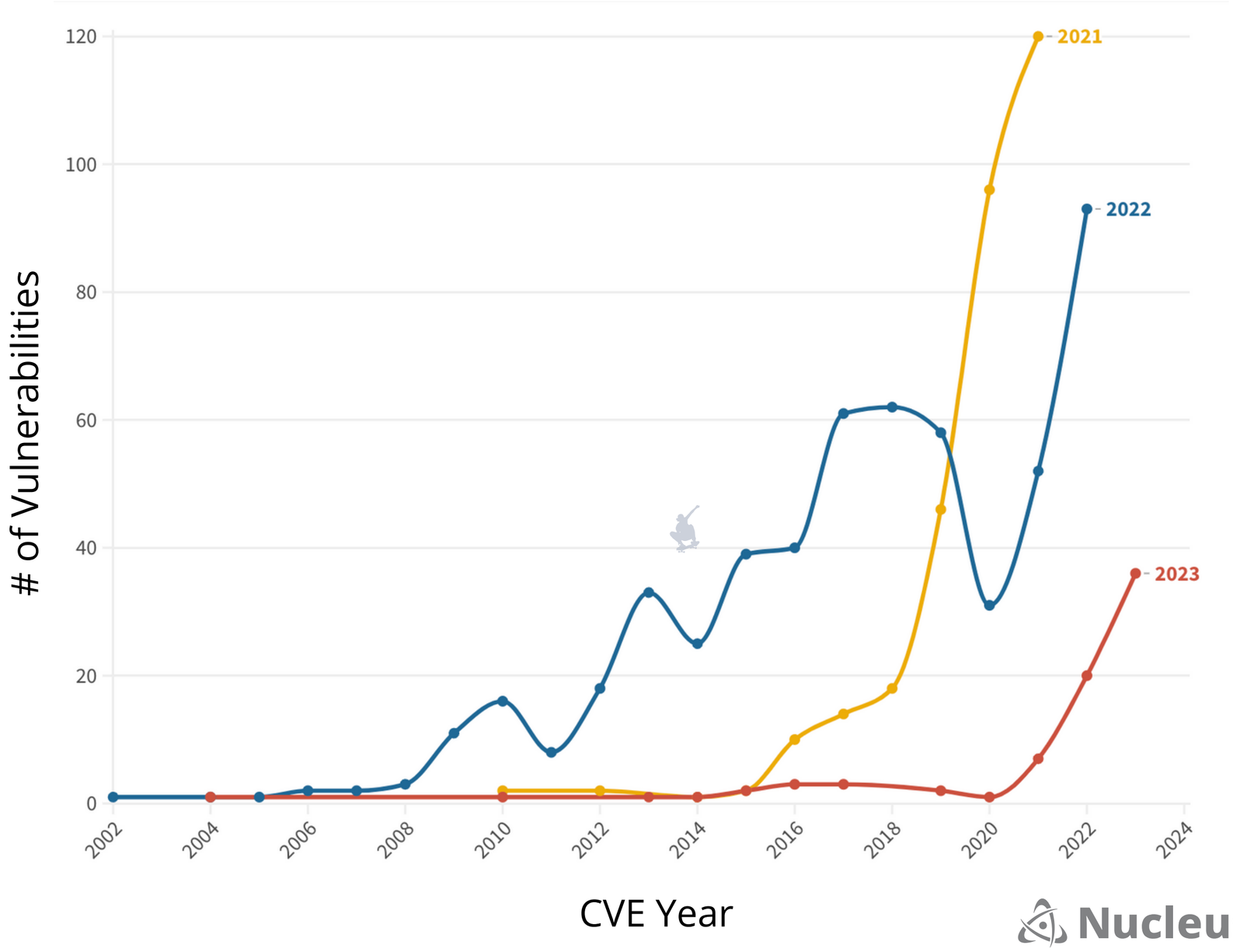
CISA KEV Mapped to New CVEs by Year (925)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

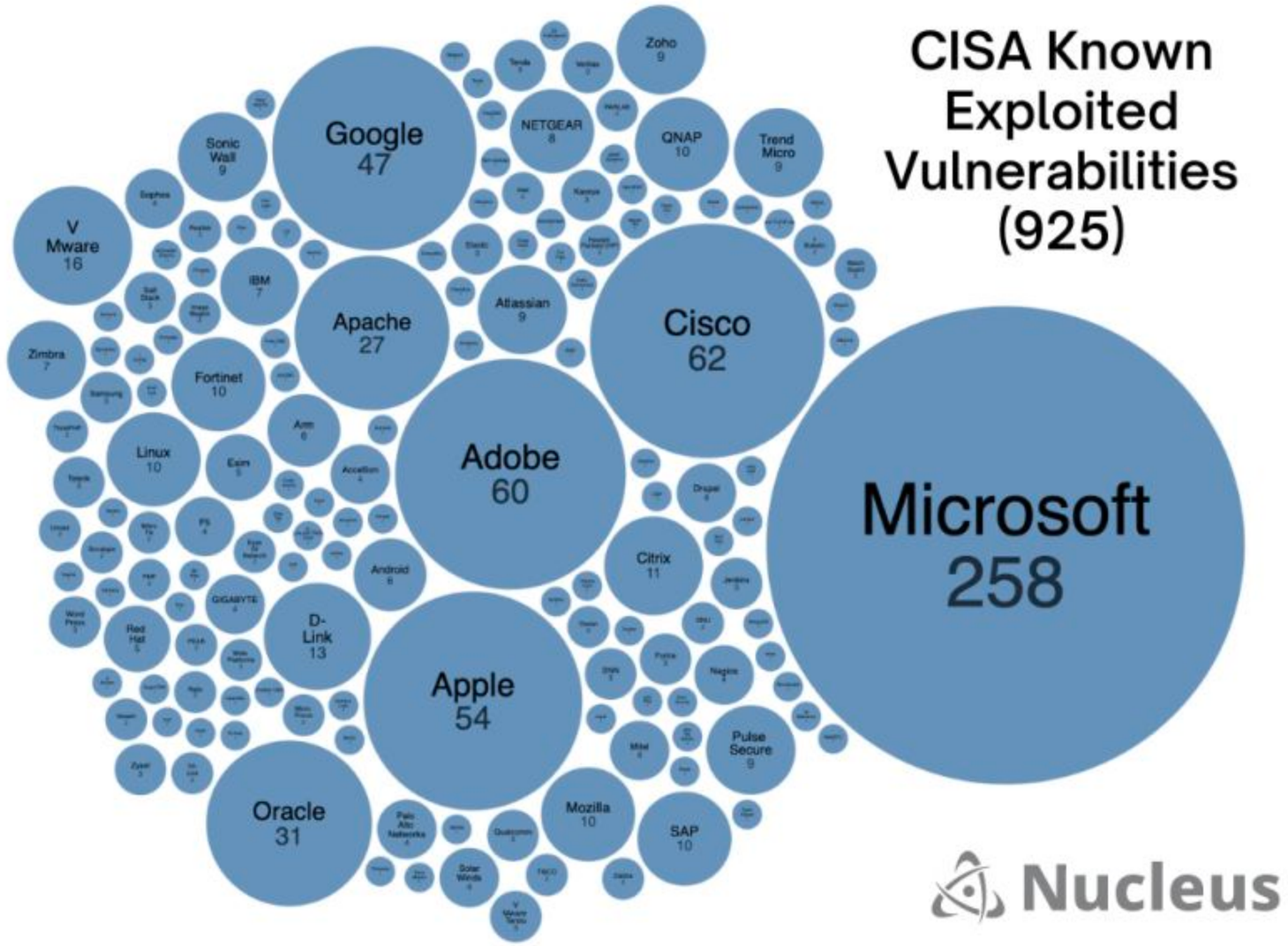
CISA KEV (YEAR ADDED TO KEV)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

CISA Known Exploited Vulnerabilities by Vendor

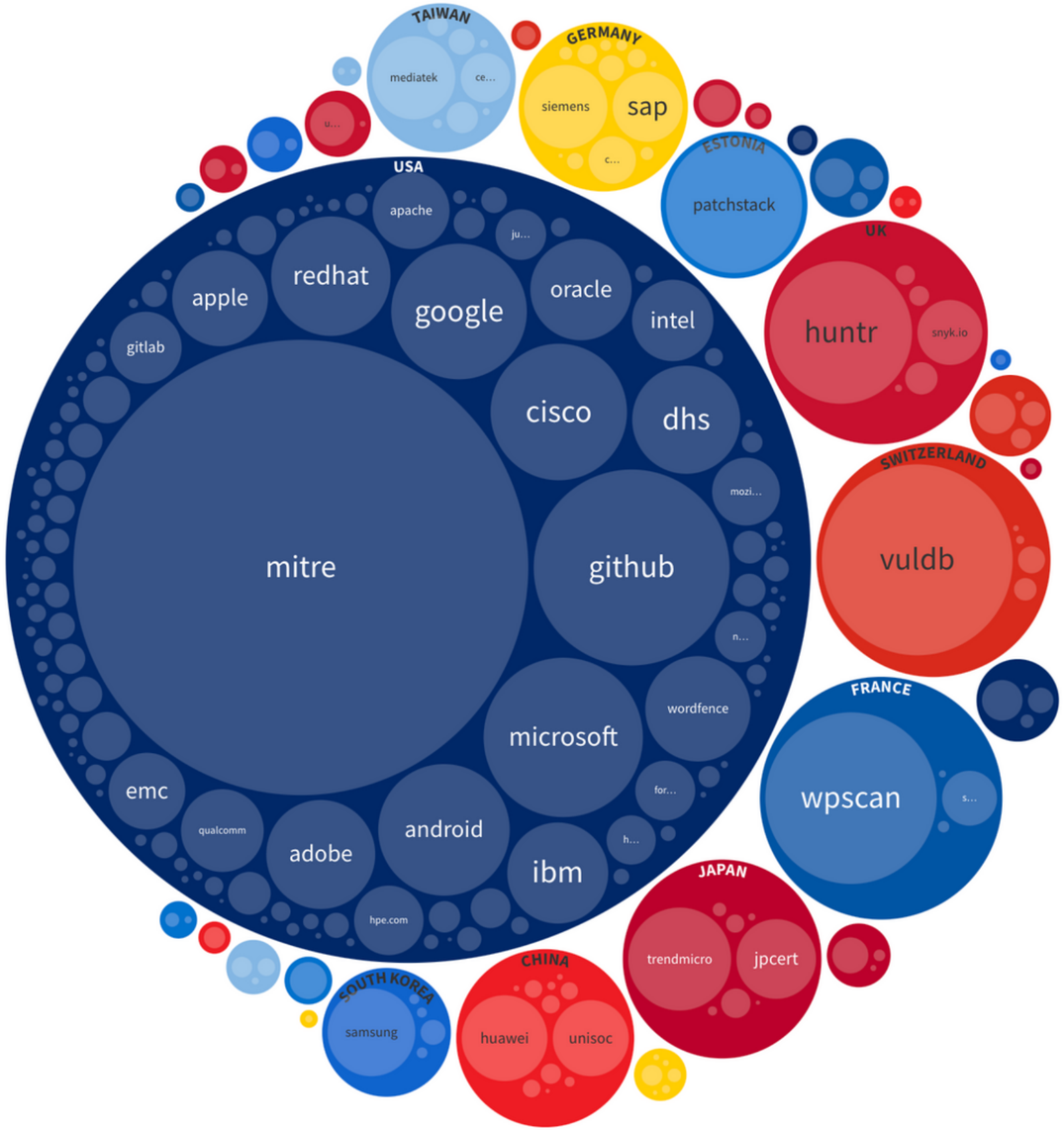


Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

National Vulnerability Database (NVD)

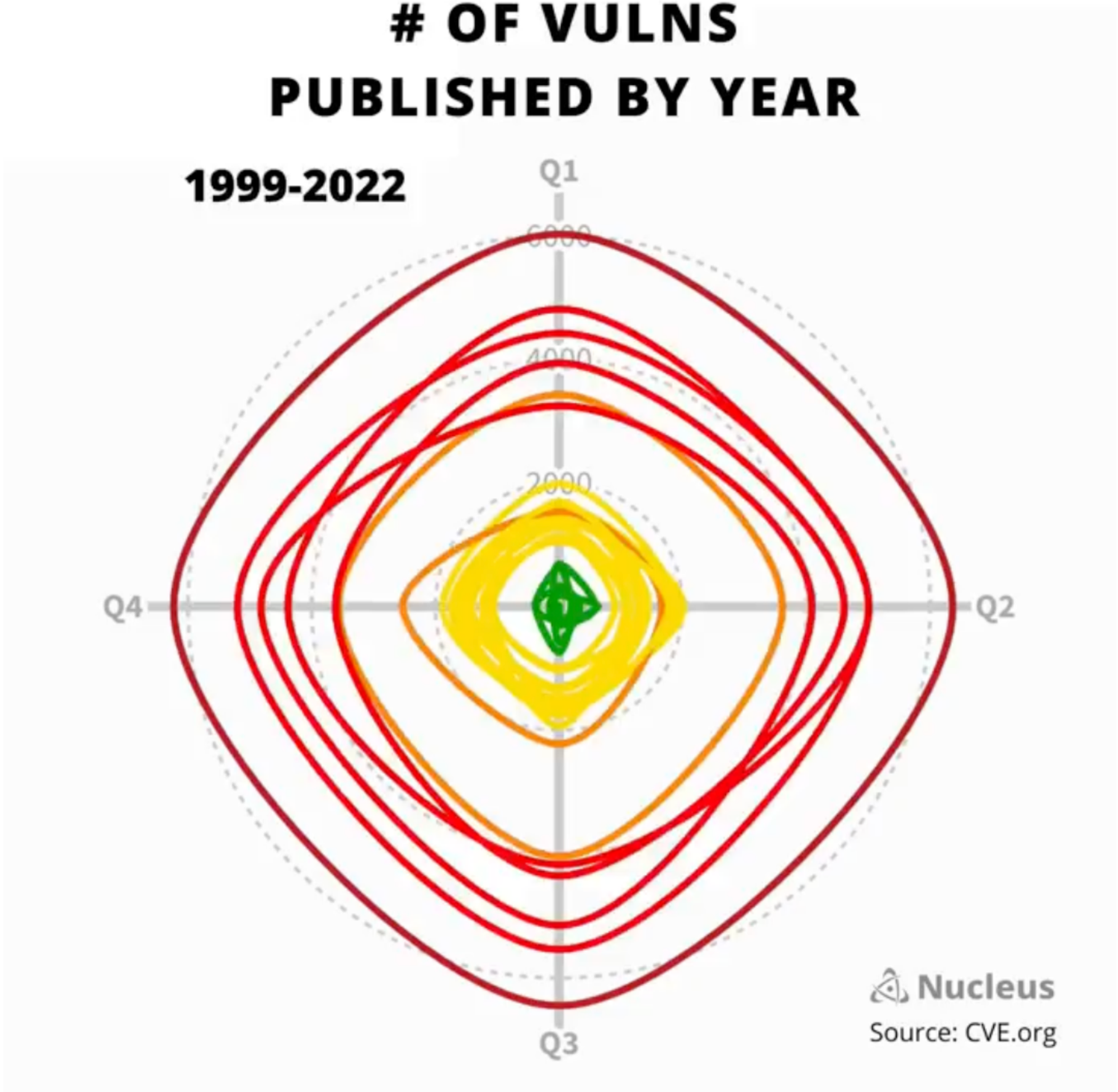
CVE Distribution by CNA (2022-1H2023)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

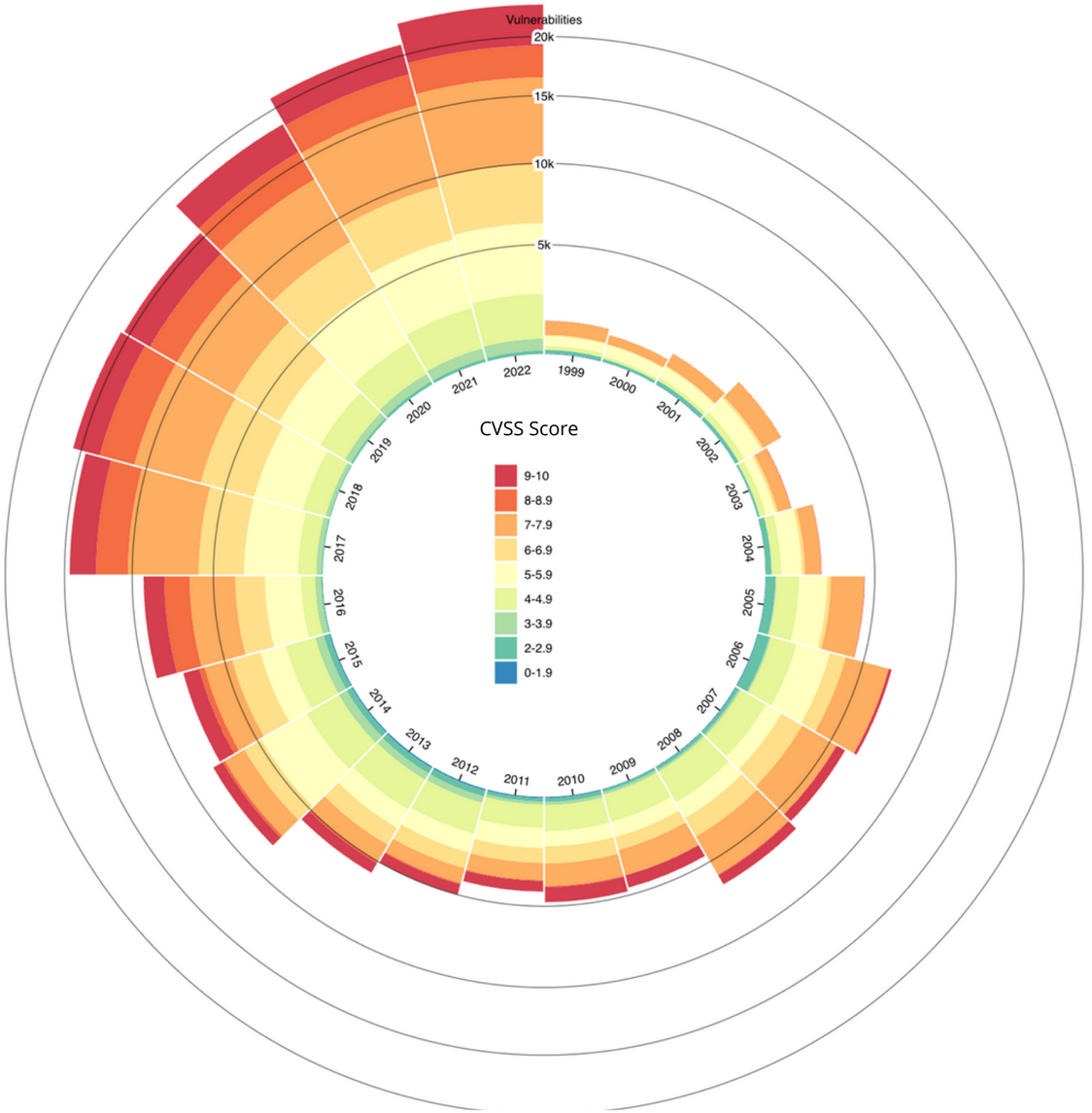
OF VULNS PUBLISHED BY YEAR



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

CVE Vulnerability Distribution Overtime by CVSS Score

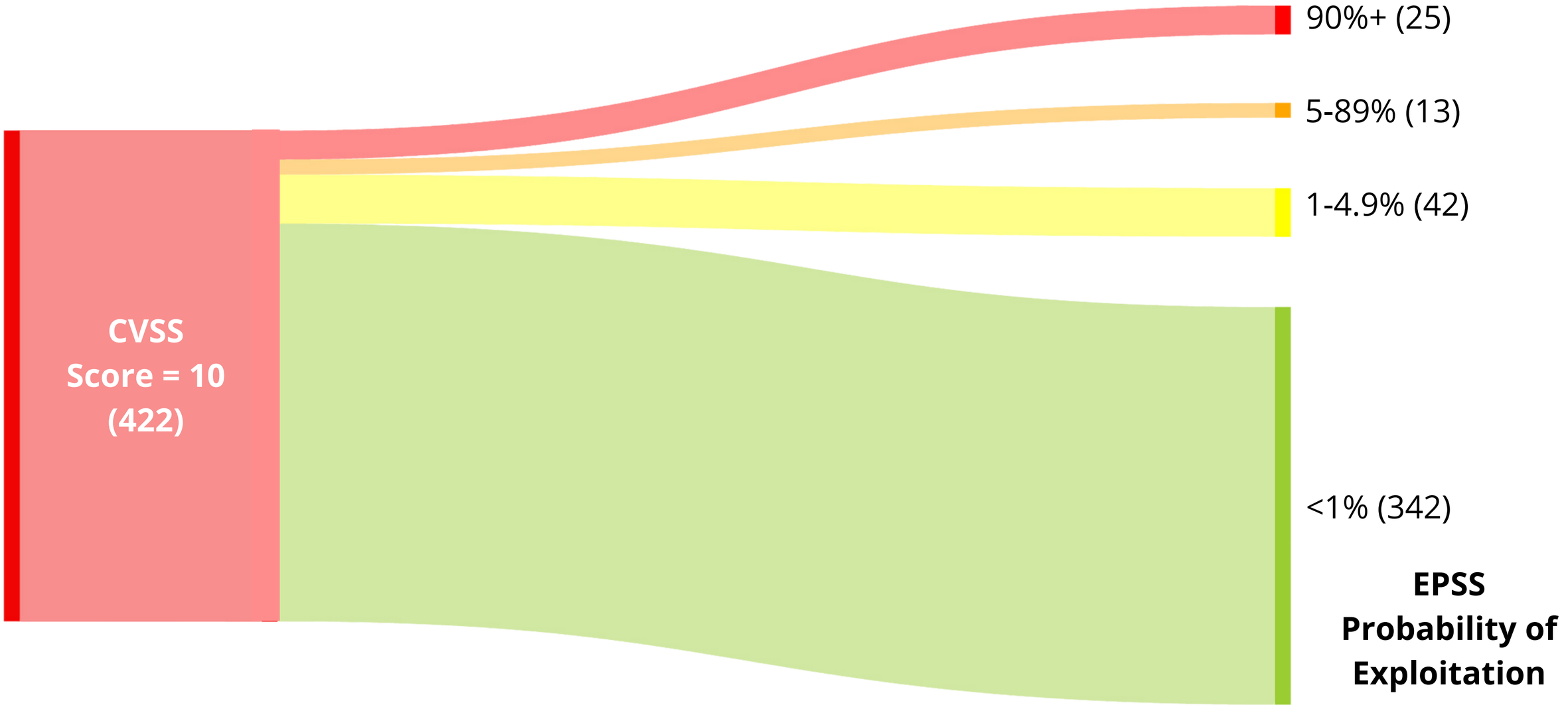


Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Exploit Prediction Scoring System (EPSS)

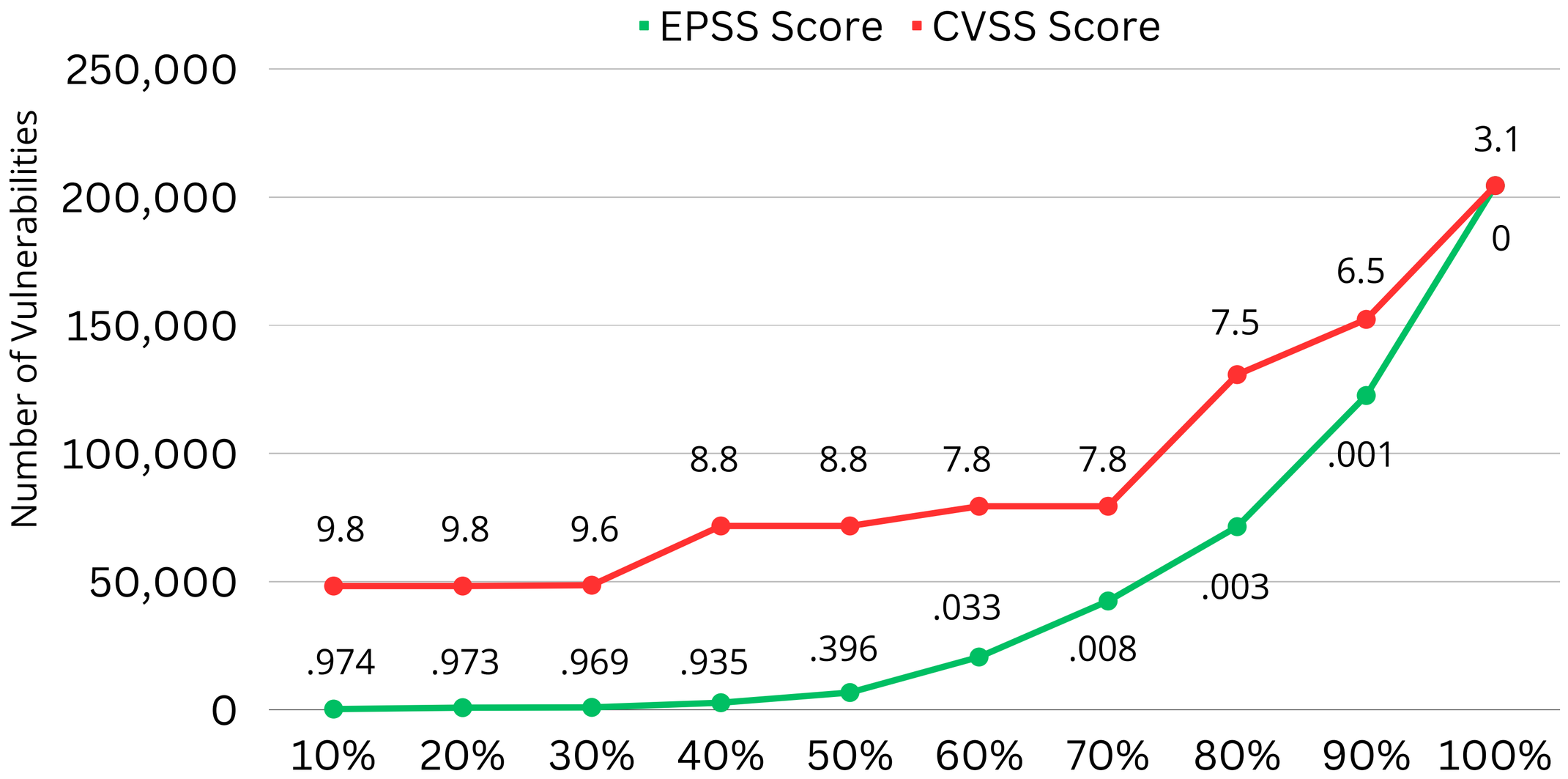
CVSS 10 Vulnerabilities Mapped to EPSS



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

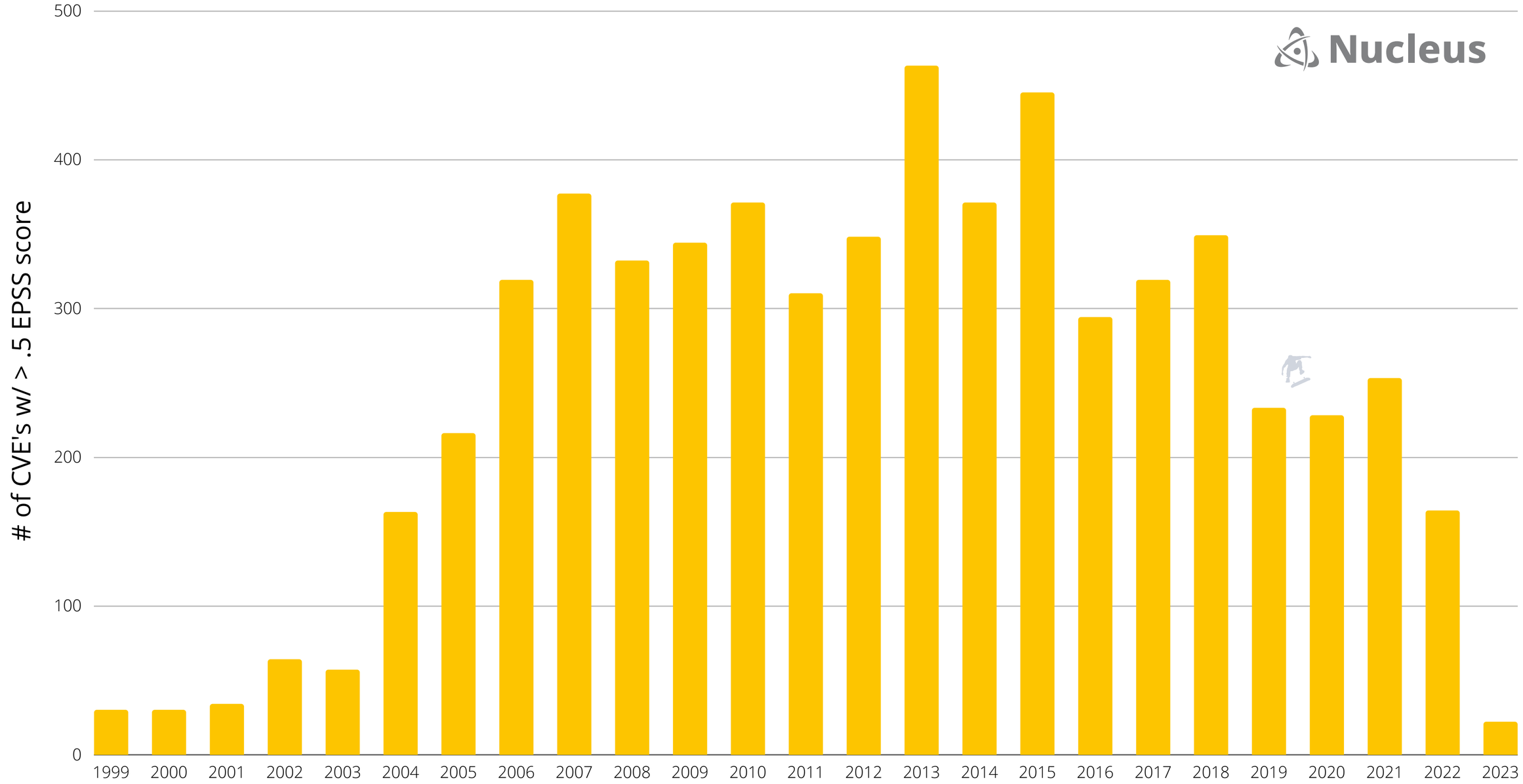
CISA KEV COVERAGE COMPARISON (CVSS / EPSS)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

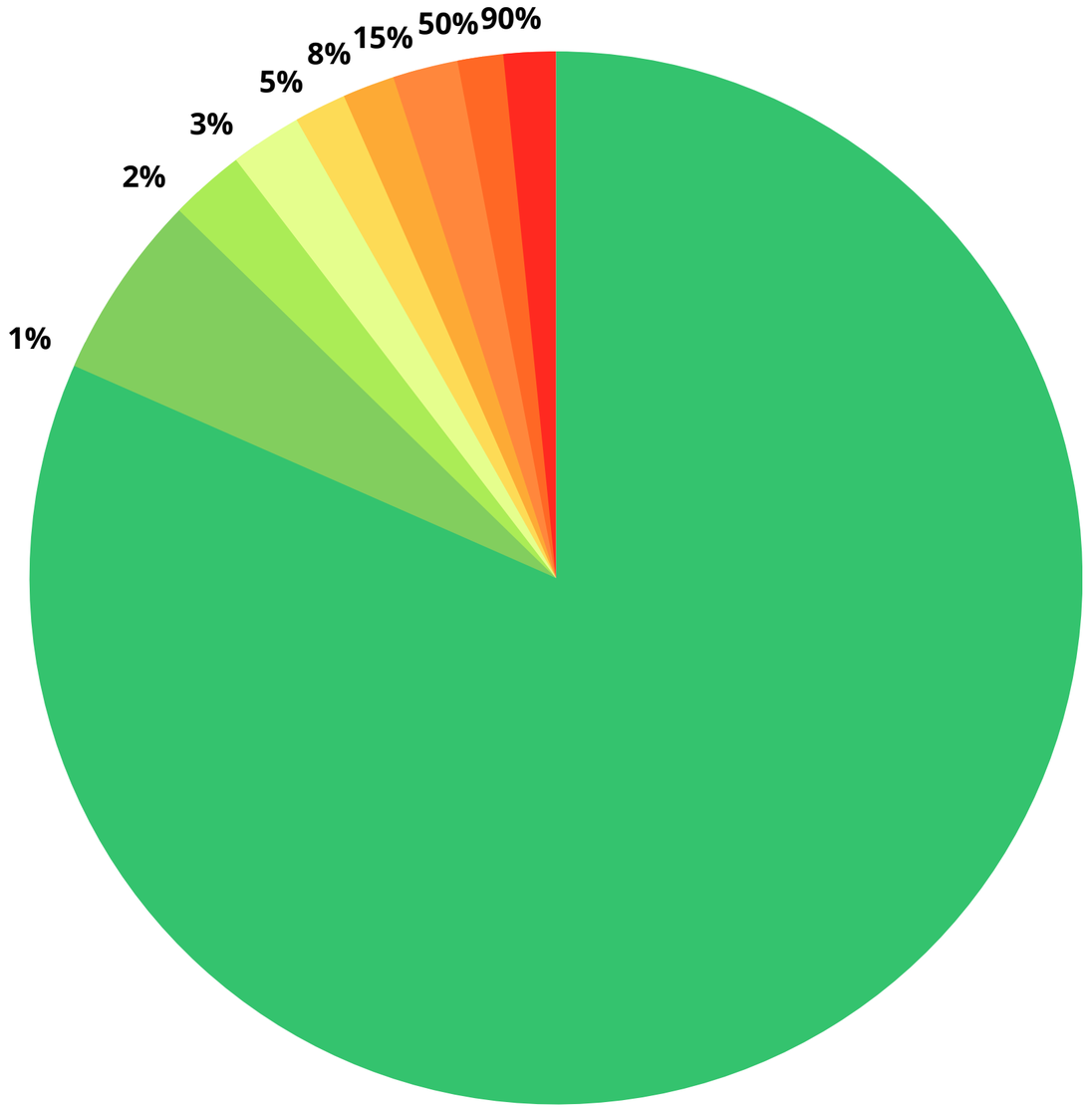
> 50% probability of exploitation in the next 30-days (Source: EPSS)



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Exploit Prediction Scoring System Probability Distribution (NVD)

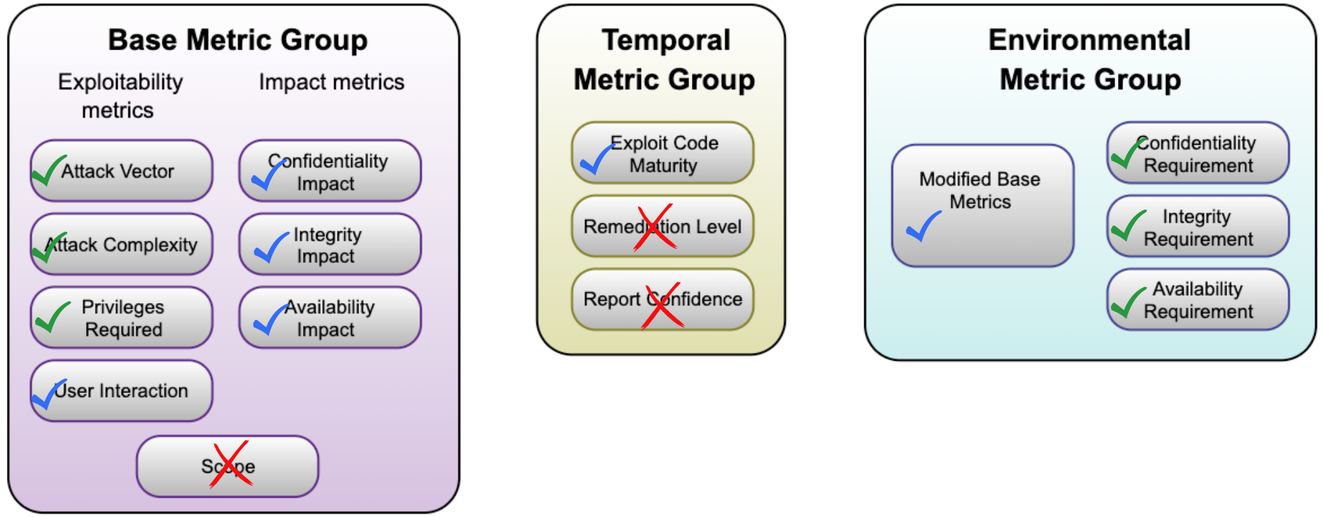


Created By: Patrick Garrity, Security Researcher, Nucleus Security

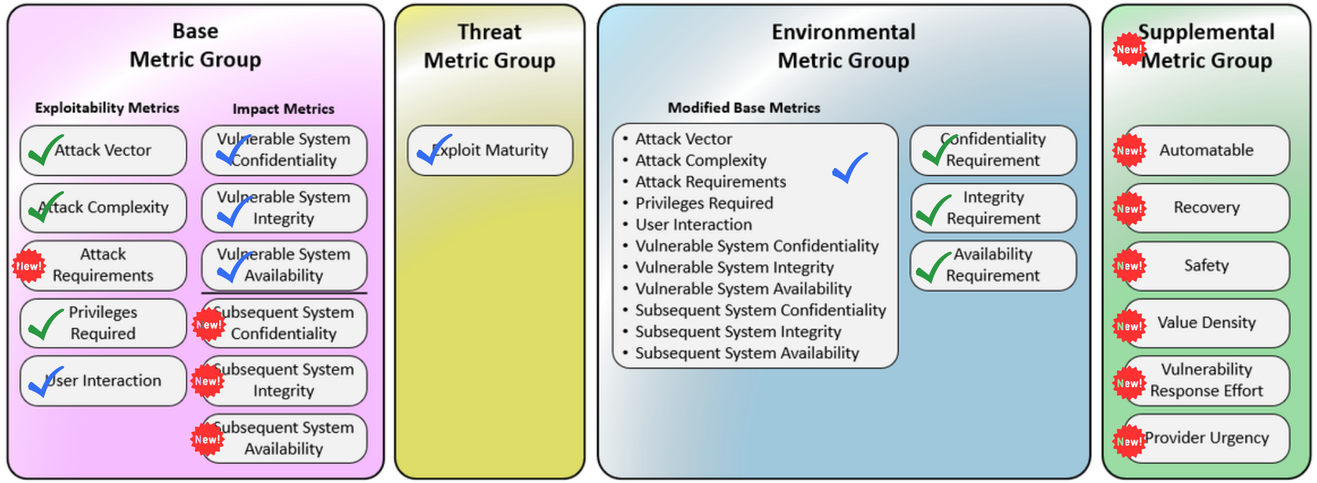
Nucleus

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System v3.1



Common Vulnerability Scoring System v4

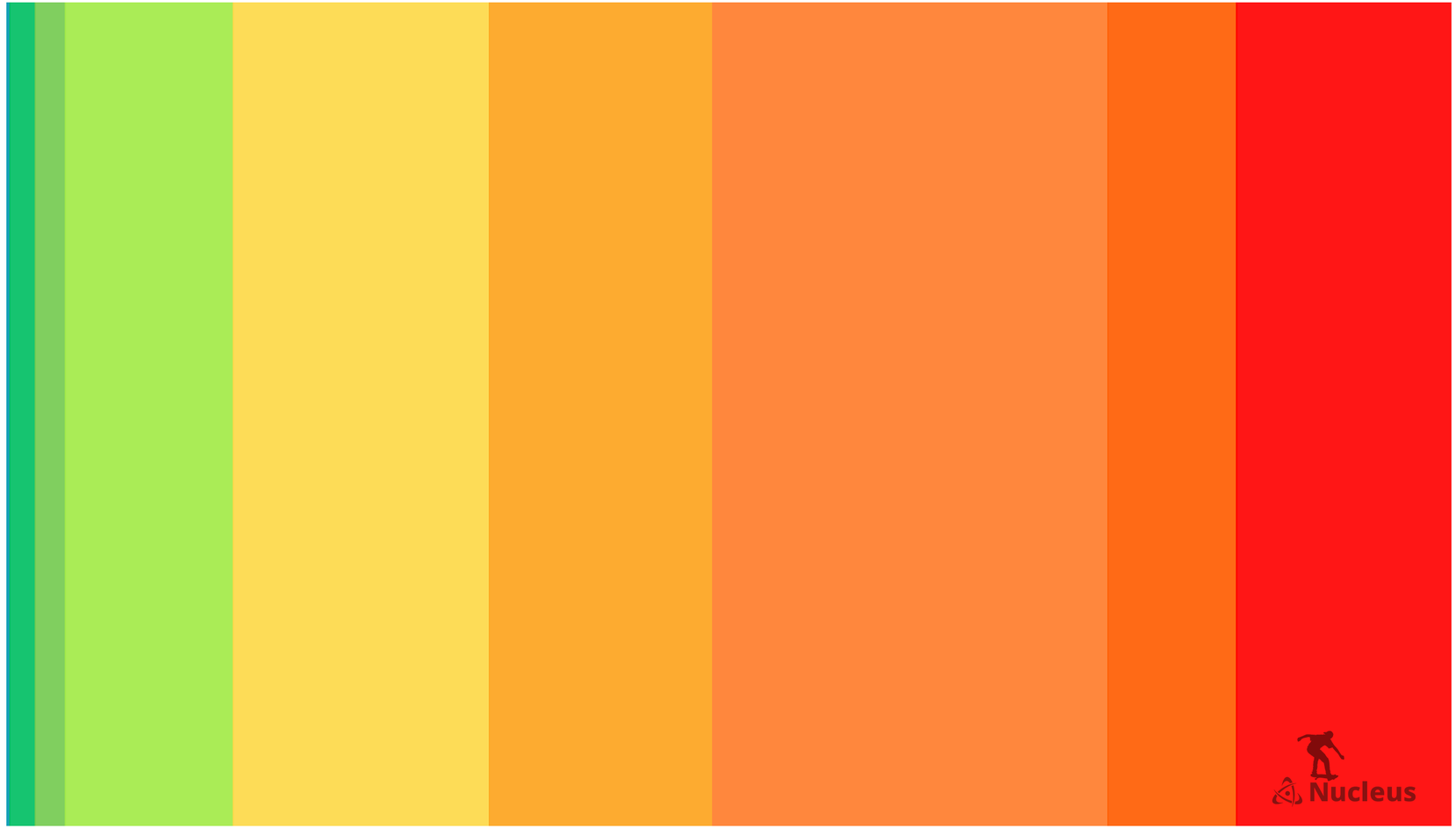


Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

CVSS Base Score Distribution

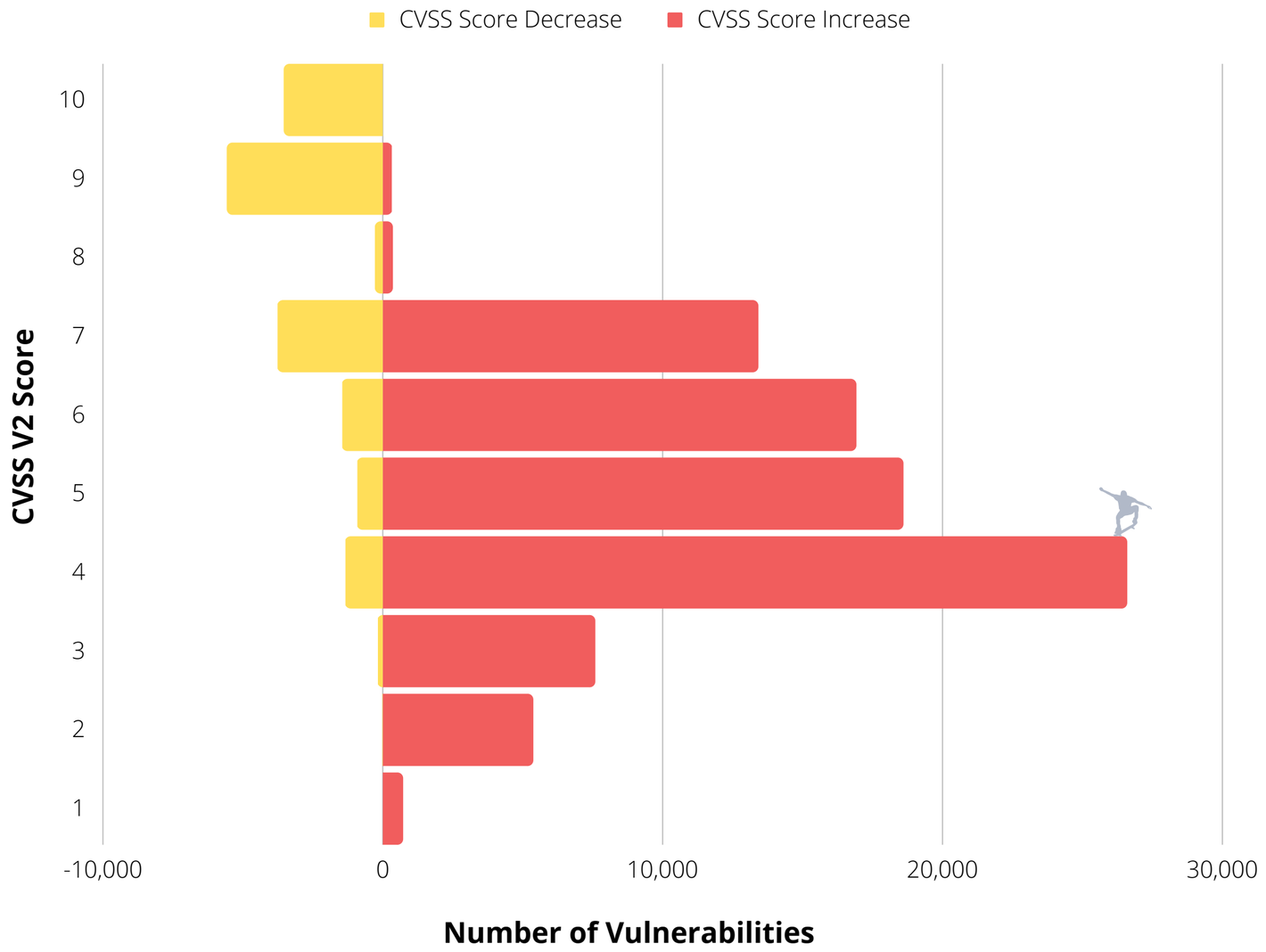
TURN UP THE BASE



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

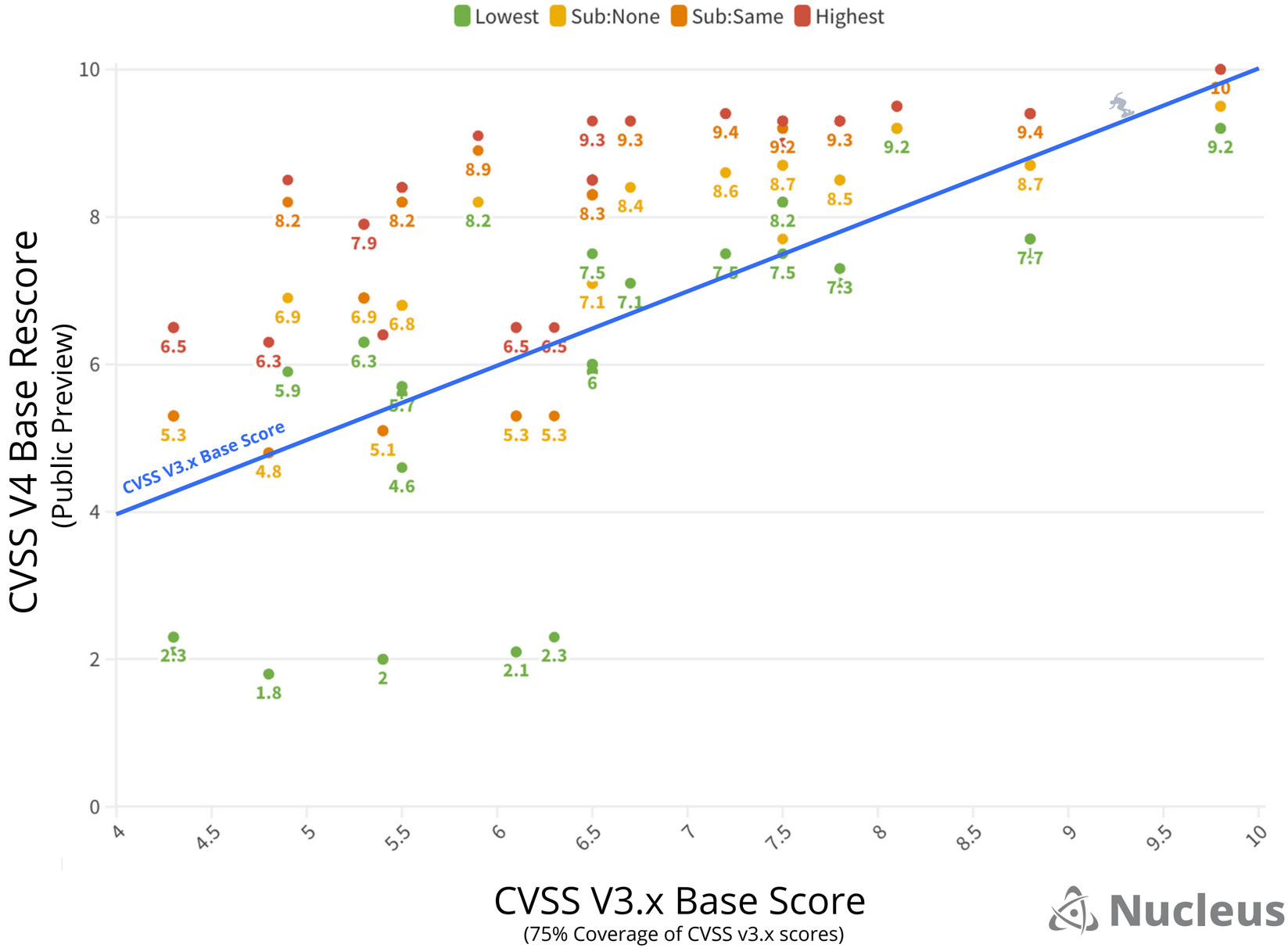
CVSS BASE SCORE CHANGE
CVSSv2 > CVSSv3.x



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

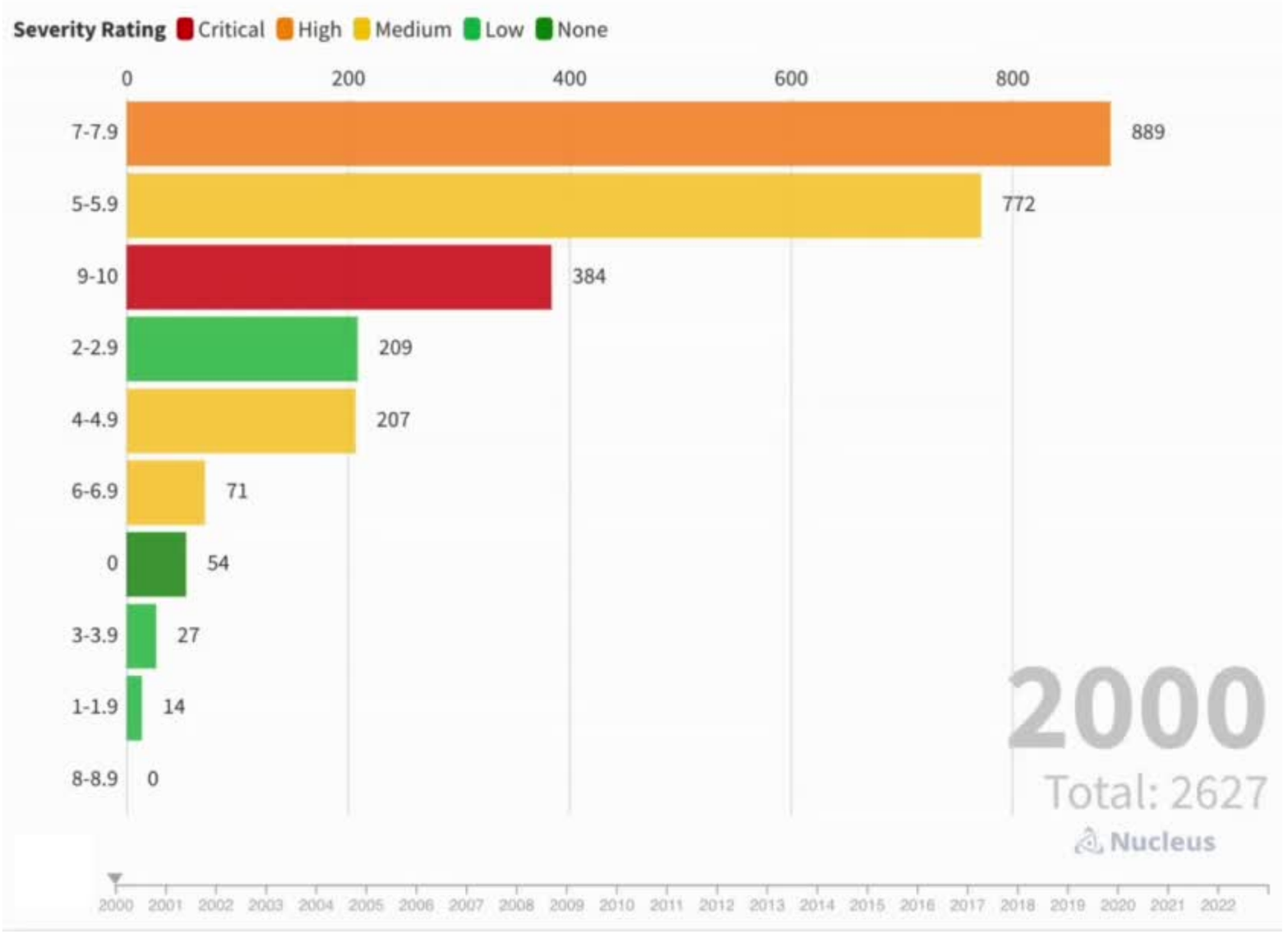
CVSS V4 BASE SCORE - RESCORING



Nucleus

Created By: Patrick Garrity, Security Researcher, Nucleus Security

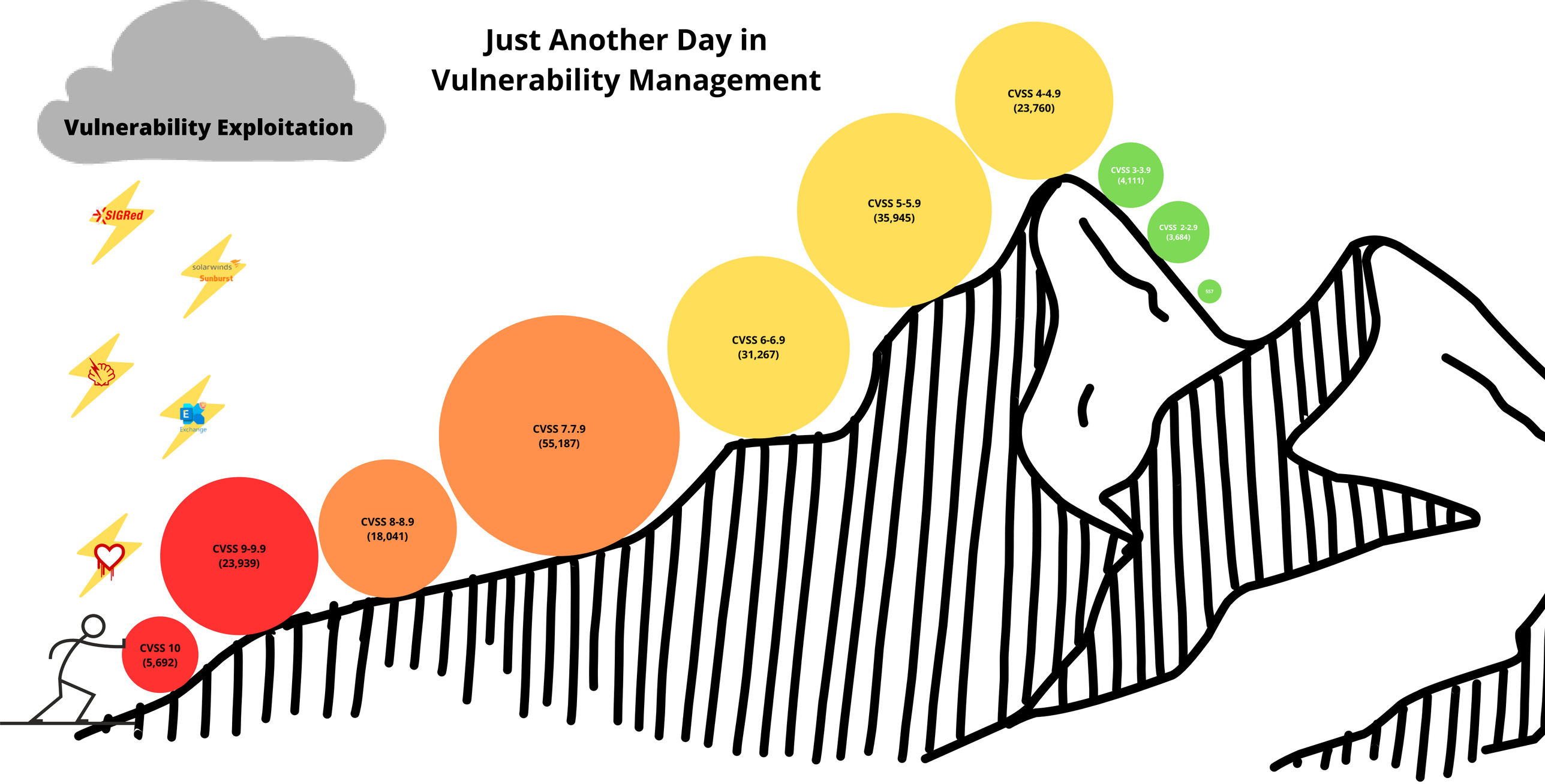
CVSS Scoring
Distribution Over Time



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Just Another Day in Vulnerability Management

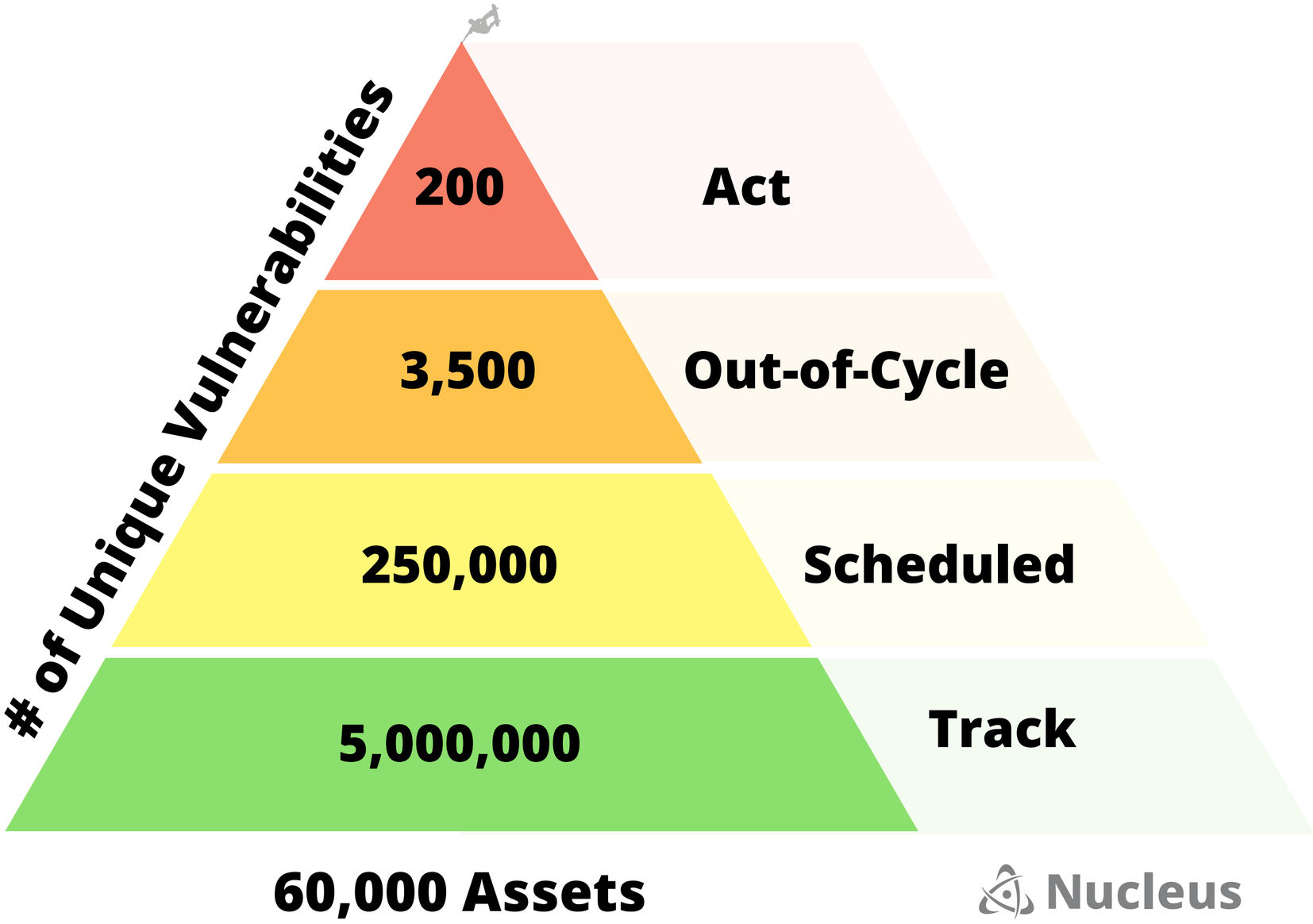


Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Stakeholder Specific Vulnerability Categorization (SSVC)

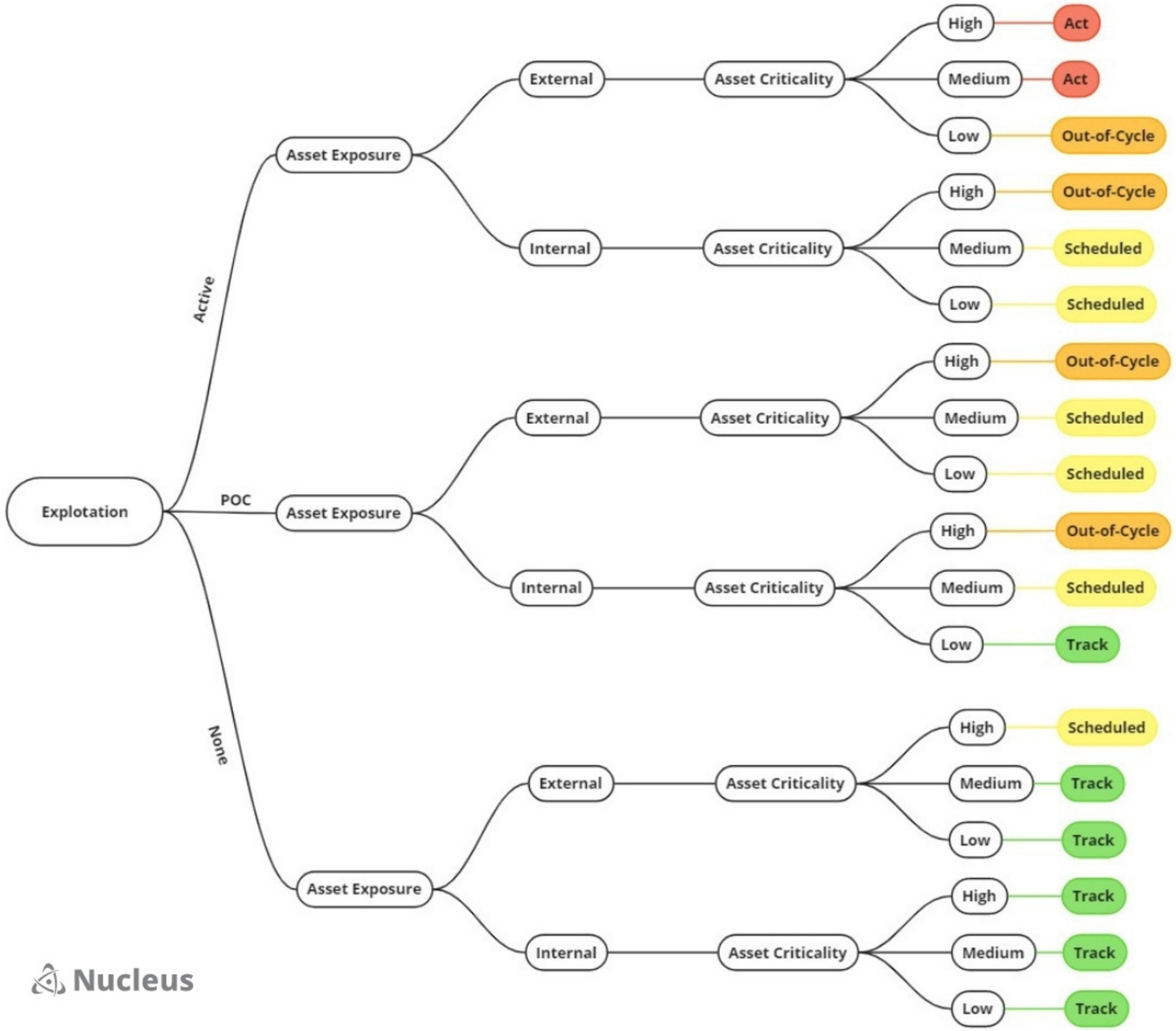
SSVC Vulnerability Prioritization Pyramid



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

SSVC Decision Tree Example



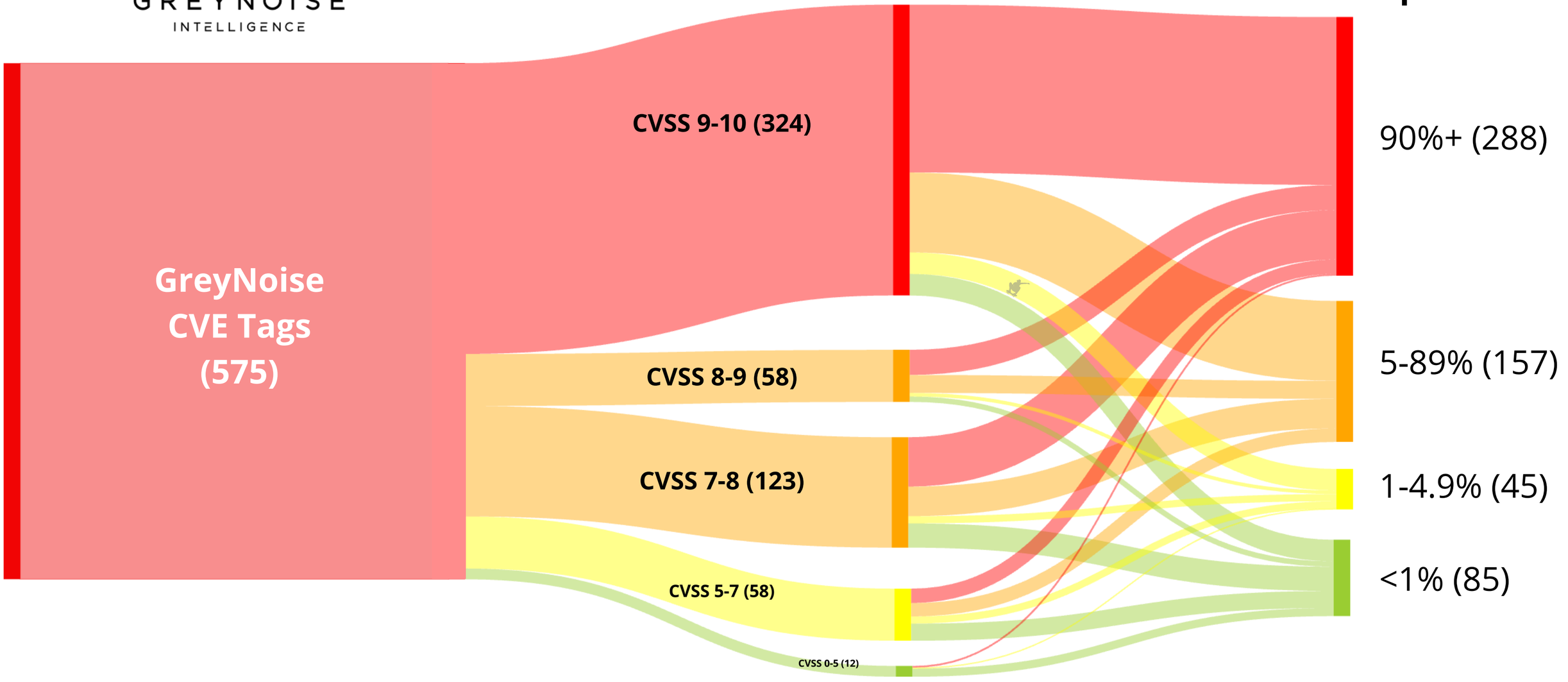
Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

GreyNoise

GreyNoise Mapped to CVSS & EPSS

GREYNOISE
INTELLIGENCE



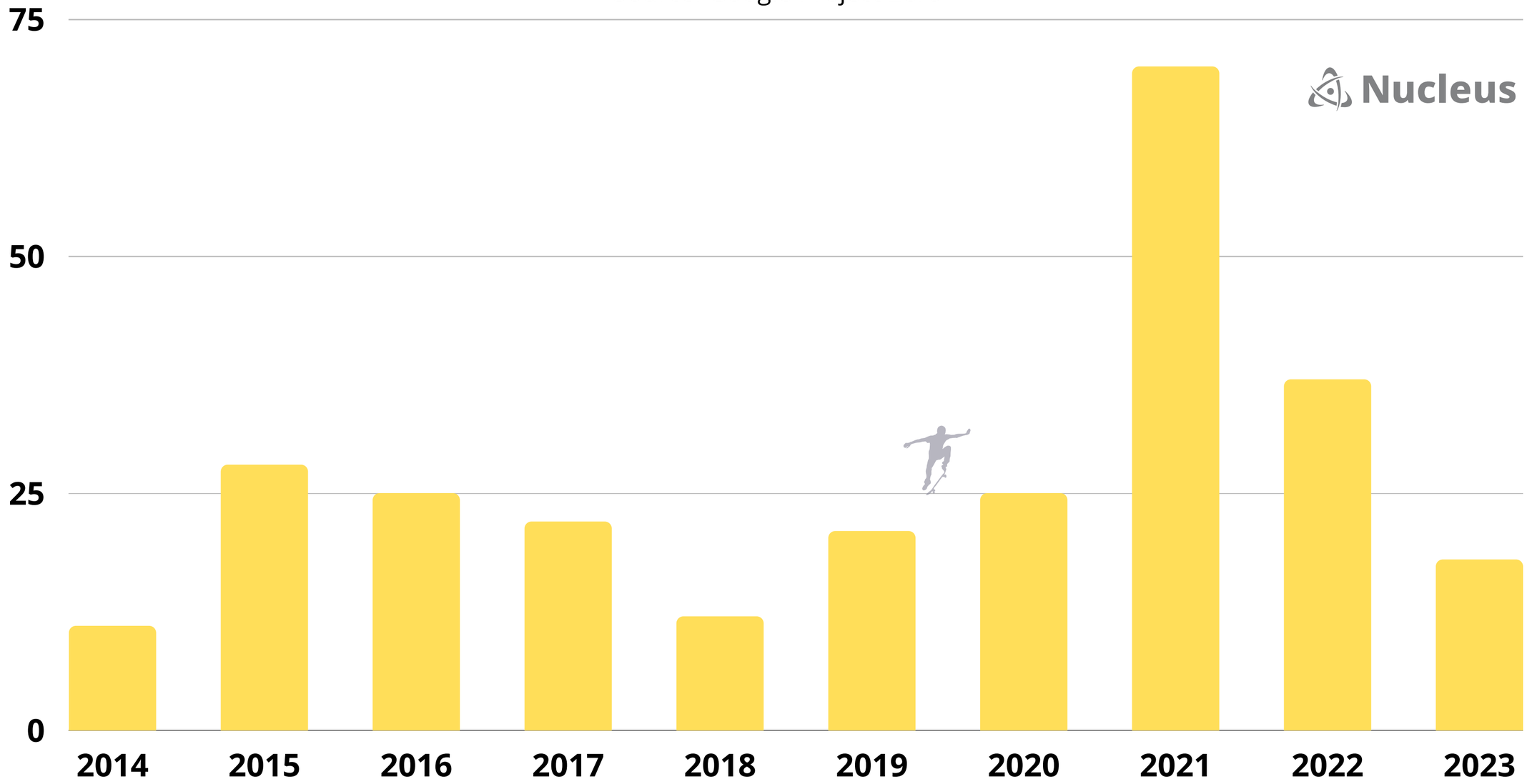
Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Zero Days

Zero-Day Vulnerabilities by Year (269)

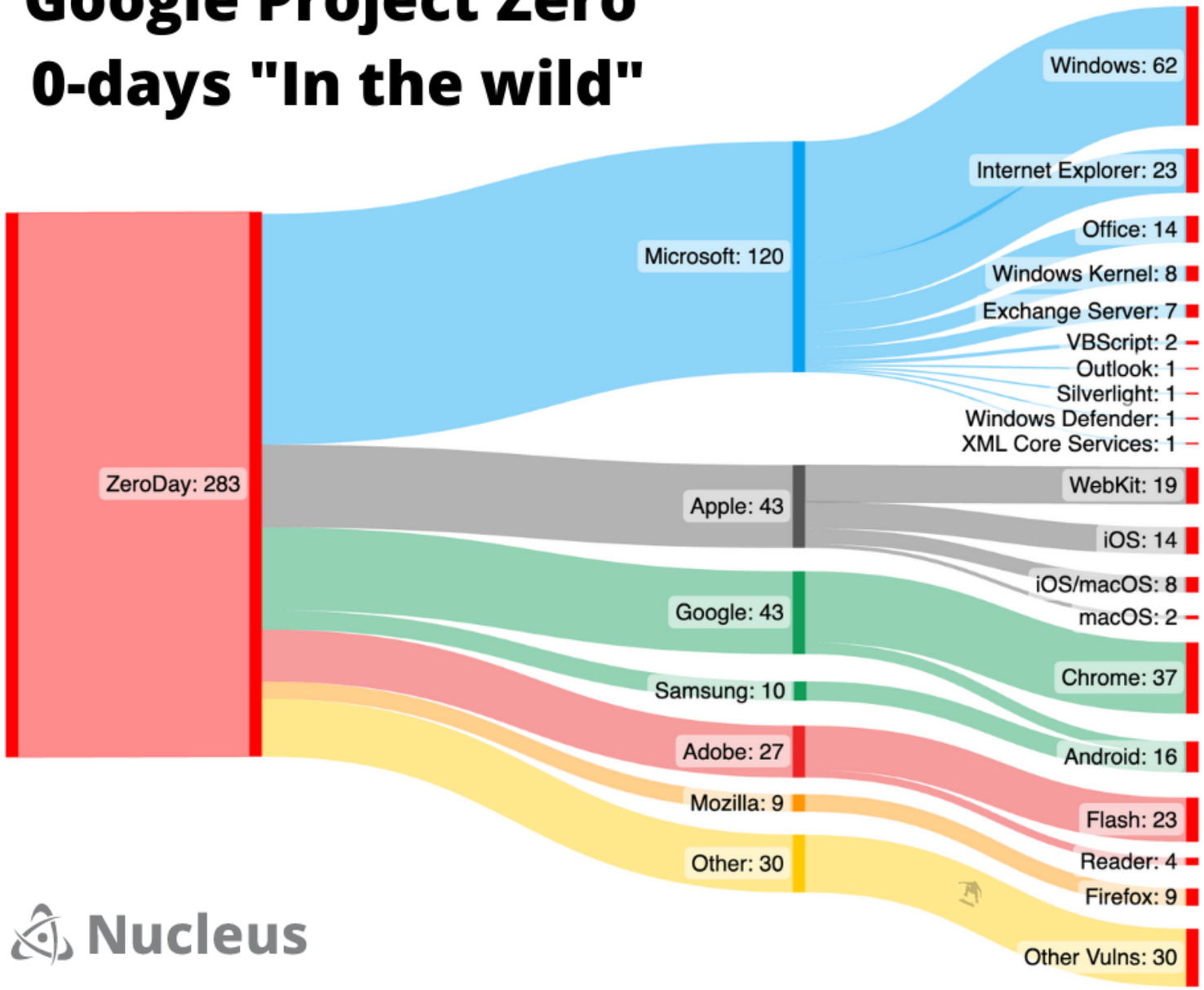
Source: Google Project Zero



Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Google Project Zero
0-days "In the wild"



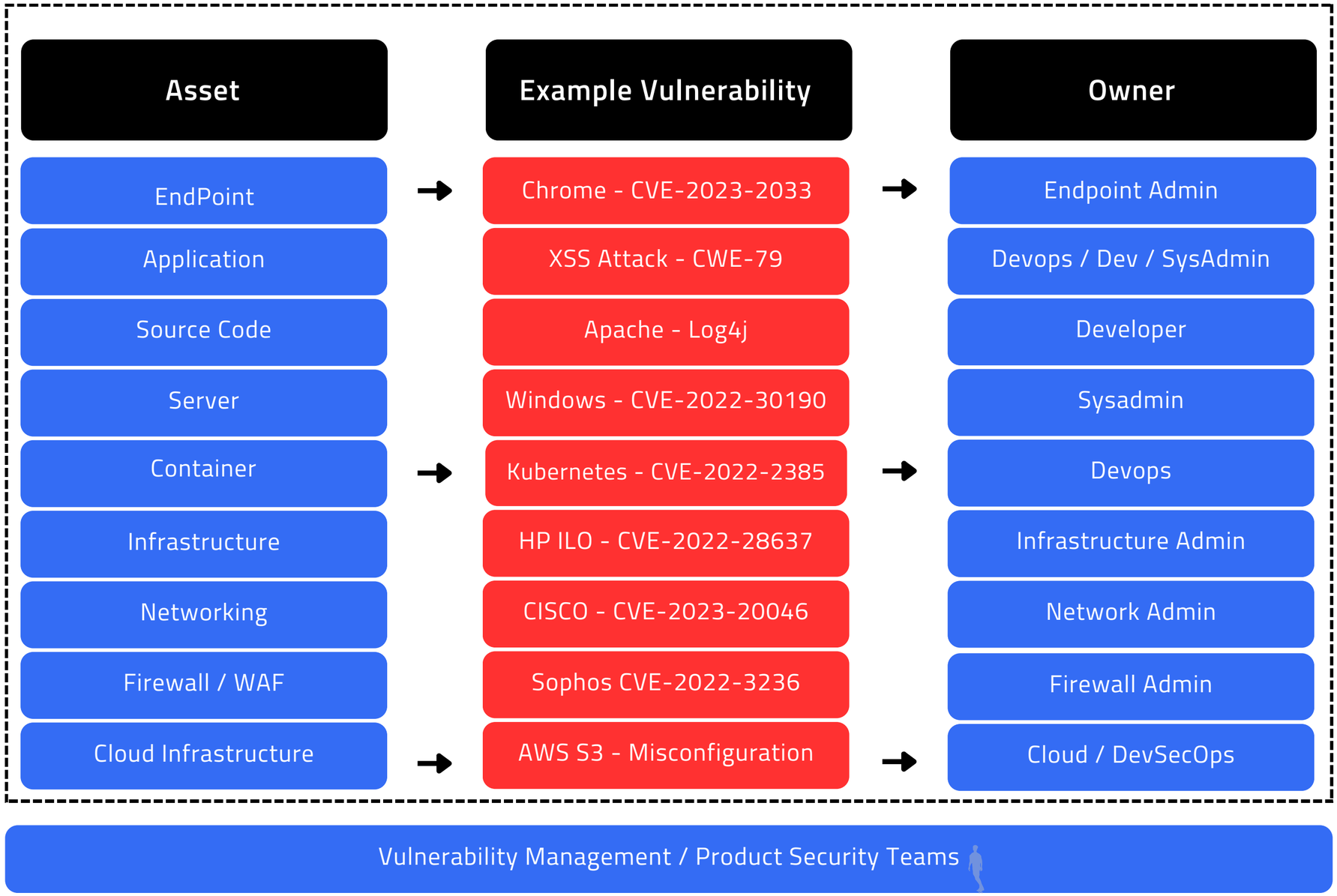
Nucleus

Created By: Patrick Garrity, Security Researcher, Nucleus Security

Nucleus

Security Team Considerations / Processes

Enterprise Vulnerability Management Responsibility Matrix



Created By: Patrick Garrity, Security Researcher, Nucleus Security