DevSecOps Days 2023

Washington, D.C.

Modern Vulnerability Management: Separating Signal from the Noise

OCTOBER 12, 2023

Chris Hughes
President @ Aquia
Dr. Nikki Robinson
Security Architect @ IBM

Agenda

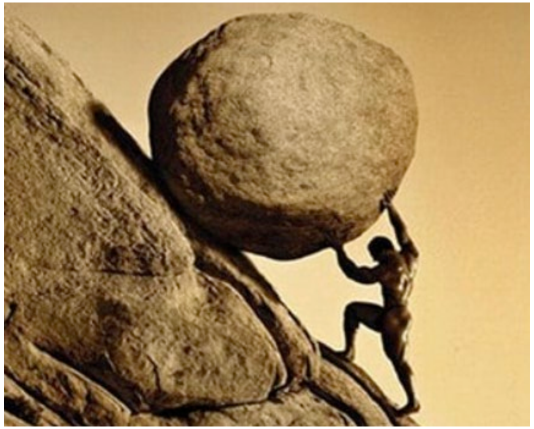
- Modern Vulnerability Management
- Current Challenges in Vulnerability Management
- Vulnerability Chaining
- The Human Component
- Building a Modern Vulnerability Management Program

Section 1:

Modern Vulnerability Management

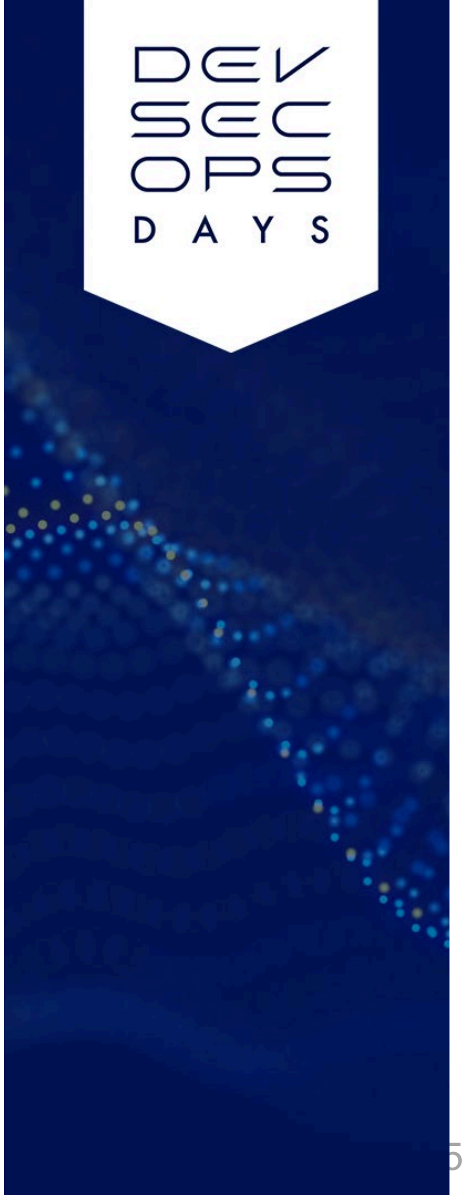
State of Vulnerability Backlogs

- 2022 saw a record 26,558 CVE's reported in NVD
- "Critical" vulnerabilities up 59% from 2021
- Report from Rezilion/Ponemon
  - 66% have a backlog of more than 100,000 vulnerabilities
  - Average number of vulnerabilities in backlog is *1.1 million*
- Cyentia Institute found:
  - Organizations typically have the capacity to remediate 1 out of 10 vulnerabilities in their environment in a given month



Section 2:

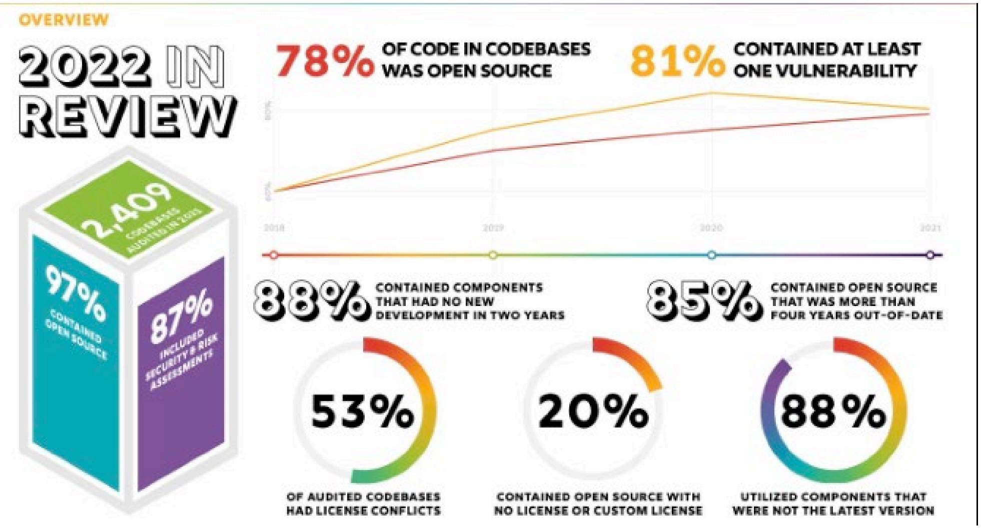
Current Challenges in VulnMgmt



Expansive Growth of Open Source Software (OSS)

We've tremendous growth of OSS adoption/use:

- 60-80% of modern codebases contain OSS
- 91% of those codebases are comprised of OSS
- Accelerates time
- Saves cost
- Fosters a thriving ecosystem and community
- High Bus Factor:
    - 25% of projects have ONE developer contributing code
    - 94% have 10 or fewer



OVERVIEW

2022 IN REVIEW

2,409 CODEBASES AUDITED IN 2021

97% CONTAINED OPEN SOURCE

87% INCLUDED SECURITY & RISK ASSESSMENTS

78% OF CODE IN CODEBASES WAS OPEN SOURCE

81% CONTAINED AT LEAST ONE VULNERABILITY

88% CONTAINED COMPONENTS THAT HAD NO NEW DEVELOPMENT IN TWO YEARS

85% CONTAINED OPEN SOURCE THAT WAS MORE THAN FOUR YEARS OUT-OF-DATE

53% OF AUDITED CODEBASES HAD LICENSE CONFLICTS

20% CONTAINED OPEN SOURCE WITH NO LICENSE OR CUSTOM LICENSE

88% UTILIZED COMPONENTS THAT WERE NOT THE LATEST VERSION

Source: Synopsys Open Source Security and Risk Analysis Report 2022

Continued adoption of Cloud and SaaS

- Organizations continue to make increased use of cloud
- Hyper-focus on IaaS, but organizations are consuming 200+ SaaS apps on average
- Misconfigurations and vulnerabilities continue to spiral – continued data breaches
- Cloud Security tool sprawl/acronym soup
  - Cloud Security Posture Management (CSPM)
  - Cloud Workload Protection Platform (CWPP)
  - Cloud Access Security Broker (CASB)
  - Cloud Infrastructure Entitlements Management (CIEM)
  - Cloud Native Application Protection Platform (CNAPP)

Vulnerability Scoring and Prioritization Struggles

- CVE Growth in NVD
  - 200,000+
  - 20,000+ in 2023 alone
  - Almost 15% YoY growth
- Historically, organizations have used CVSS Severity Scores to prioritize vulnerabilities
- This is problematic, because less than 5% of *all* known CVE's are ever exploited
- Organizations are wasting tremendous time, effort and energy prioritizing vulnerabilities that are unlikely to ever be exploited and present little risk

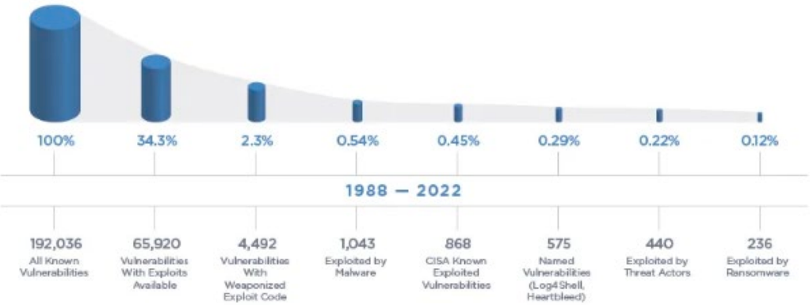


Figure 2: Evolution of vulnerability threat landscape, 1988 – 2022

Source: Qualys TruRisk Report 2022

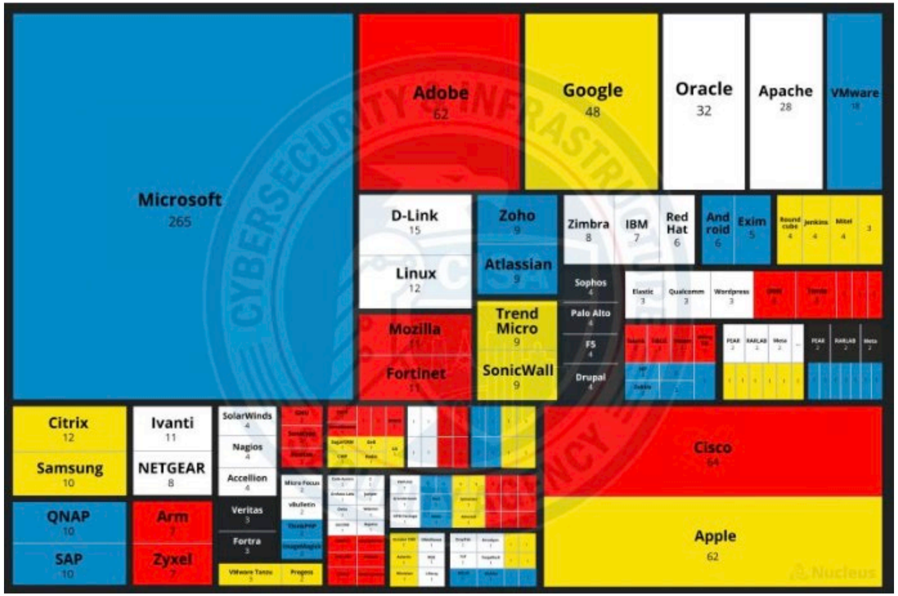
Emerging Vulnerability Scoring and Prioritization Systems

- As we now realize the challenges of legacy/traditional scoring and prioritization, several others have emerged:
  - CISA Known Exploited Vulnerability (KEV) catalogue
  - Exploit Prediction Scoring System (EPSS)
  - Stakeholder Specific Vulnerability Categorization (SSCV)

Emerging Vulnerability Scoring and Prioritization Systems – CISA KEV

- Launched November 2021 as part of Binding Operational Directive (BOD) 22-01
- Helps Federal agencies (and commercial entities) prioritize ***known exploited*** vulnerabilities
- Recently hit 1,000 vulnerabilities listed
- To appear on the KEV, must:
  - Be assigned a CVE identifier
  - Be under active or attempted success exploitation
  - Has *clear* remediation guidance (e.g. patches/mitigations)

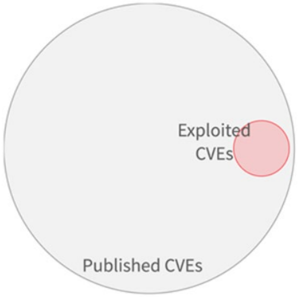
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

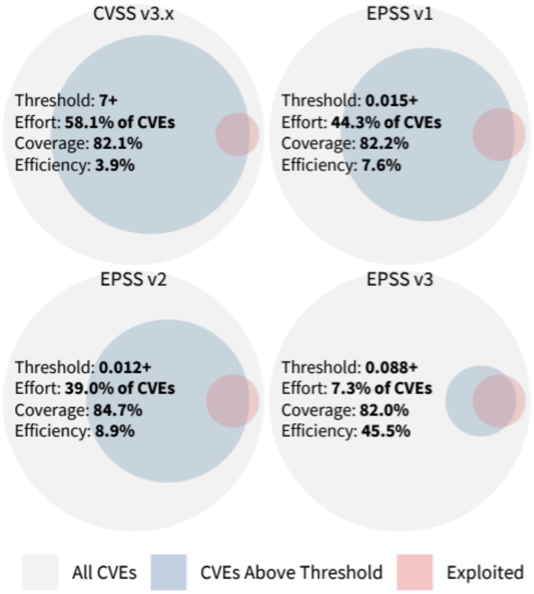


Source: Patrick Garrity @ Nucleus Security

Emerging Vulnerability Scoring and Prioritization Systems – Exploit Prediction Scoring System (EPSS)

- As discussed, only 2-7% of vulnerabilities are ***ever*** seen to be exploited in the wild
- EPSS produces a probability score between 0 and 1 (0% and 100%) that a vulnerability will be exploited in the next 30 days
- Uses a variety of data sources, such as:
  - Published CVE's
  - Published exploit code
  - Exploitation-in-the-wild activity
  - And more

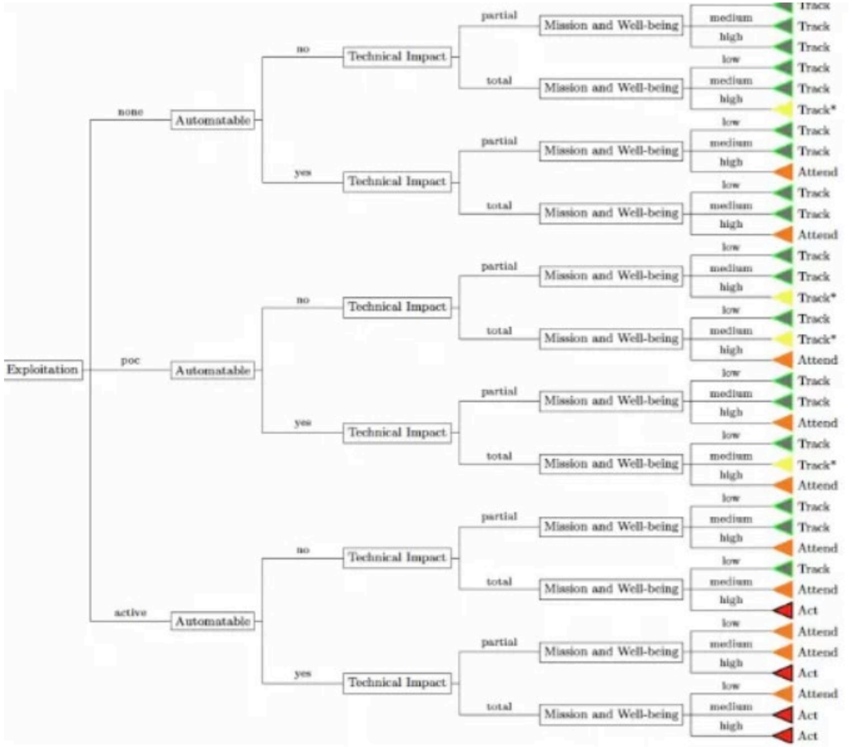




Source: EPSS 3.0 whitepaper

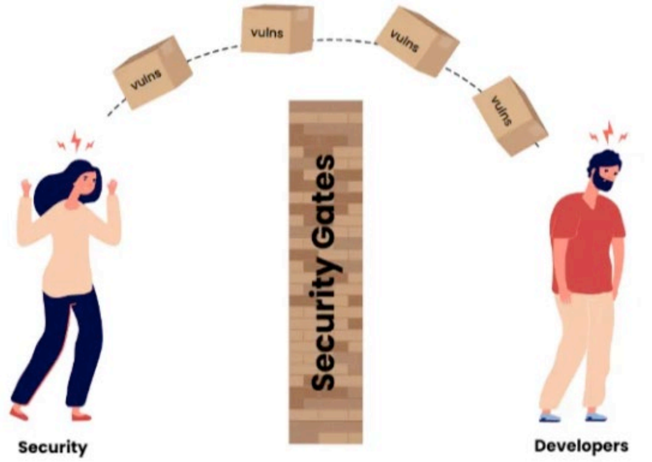
Emerging Vulnerability Scoring and Prioritization Systems - SSVC

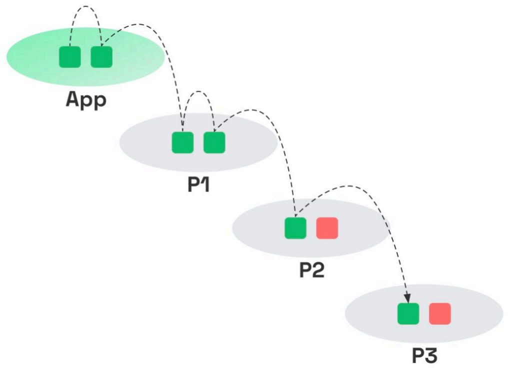
- Uses decision trees to prioritize relevant vulnerabilities into four possible decisions
  - Track – Does not require action – monitor & reassess
  - Attend – Requires attention (e.g. remediating sooner than standard timelines), may need assistance/publishing notification
  - Act – Remediate as soon as possible, does require assistance and publishing notification
- Looks at factors such as:
  - Exploitation Status
  - Technical Impact
  - Automatable
  - Mission Prevalence
  - Public Well-Being/Impact



Throwing Toil and Building Silos

- Despite all of the talk of "breaking down silos" and DevSecOps, we (Security) are generally throwing toil over the fence
- Vulnerability with little to no context
- "guilty until proven innocent" mindset
- Erecting "gates" with little context into key things we've discussed
- We've shifted toil left (e.g. SAST, DAST, IaC, SCA et al)
- Many organizations still primarily use CVSS for prioritization, without taking into consideration:
  - Known Exploitation (e.g. CISA KEV)
  - Exploitation Probability (e.g. EPSS)
  - Exploitability (e.g. Reachability Analysis, Architecture etc.)
  - Business Context/Criticality (e.g. data sensitivity, mission essentiality)





Source: Endor Labs State of Dependency Management 2022

Section 3:

Vulnerability Chaining

Vulnerability Chaining

- Combination of lower scored vulnerabilities - "Medium" and "Low" vulns to create Critical attacks
- Common attack method used by APT groups and malicious actors
- Leveraging open-source products, SSL/TLS vulnerabilities, and older or EOL software

Newer examples of vulnerability chaining released from vendors:

- Microsoft Active Directory / Domain Controller compromise
- VMware vRealize products – privilege escalation
- Software supply chain attacks like Log4j/Log4shell

Section 4:

The Human Element in VMPs

The Human Element

Complexity in infrastructure:

- Multi-cloud
- Hybrid cloud
- On-premise and cloud migrations
- Infrastructure as Code
- Digital transformation
- Combination of open-source and vendor solutions

Complexity in teaming:

- DevOps
- DevSecOps
- Software Development
- Project Management
- Program Management
- Security Operations
- Security Engineering
- Security Architecture
- Infrastructure Operations

Psychological Factors:

- Cognitive Overload
- Alert Fatigue
- Decision Fatigue
- Unconscious Bias
- Perception vs Intention
- Social Engineering
- Behavioral Analysis

Section 5:

Building a Modern VMP

Building a Modern Vulnerability Management Program

1. **Identify the level of maturity in the current program**
   a) Do you have vulnerability management experts?
   b) What are the biggest gaps in your VMP
   c) Does your VMP assist in managing risk across the enterprise?

2. What automation is currently in place

a) Evaluate the current security tooling in place and what automation exists for patching activities

b) Is there continuous monitoring in place for reviewing secure configurations / open vulnerabilities for tracking?

3. Does your VMP account for the human element of vuln mgmt?

a) Complexity in relationships and responsibilities between teams

b) How does perception impact the risk management activities in the program

c) Unconscious bias related to remediation activities

4. Evaluate the backlog of vulnerabilities for context

a) Why does the backlog exist – is it people, process, or technology driven

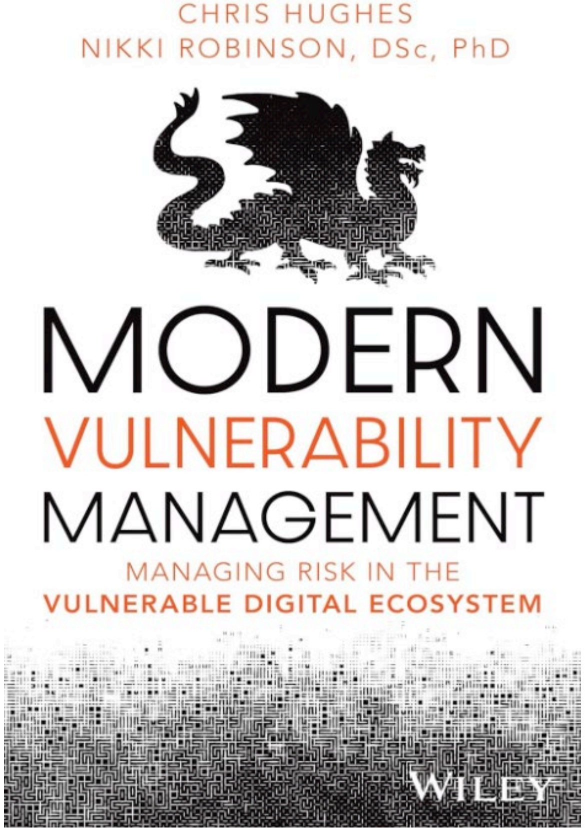
b) Find a starting point – evaluate which activities knock out the most vulns with the least amount of effort

Contact

Nikki Robinson
Security Architect / PoP

LInkedIn: www.linkedin.com/in/dr-nikki-robinson
Email: dr.nikki.robinson@gmail.com

Chris Hughes
President @ Aquia
CISA Cyber Innovation Fellow (CIF)
LinkedIn:
www.linkedin.com/in/resilientcyber
Email: chris.hughes@aquia.io



CHRIS HUGHES
NIKKI ROBINSON, DSc, PhD

MODERN VULNERABILITY MANAGEMENT

MANAGING RISK IN THE VULNERABLE DIGITAL ECOSYSTEM

WILEY

Released – May 2024
Available on Amazon for Pre-Order now