PATCH YOUR SH!!

(Or, as it appears on the program:
A Comprehensive Approach to IT Vulnerability Management
In case you were wondering if you came to the wrong room)

David C. Frier, RIMS-CRMP, CISM, etc.
Rochester Security Summit 2024

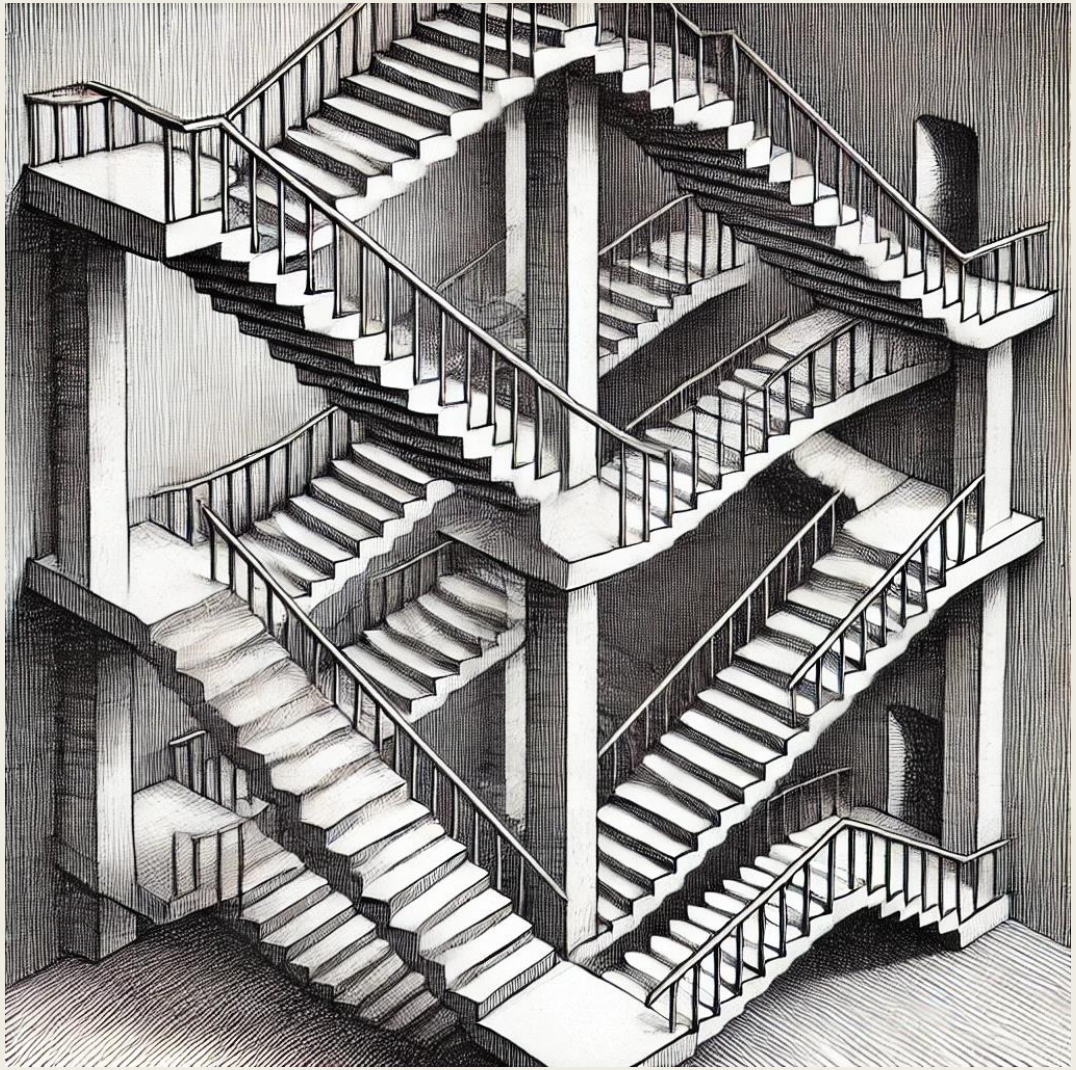
overview

- This is an Introduction to Vulnerability Management
- Spiced with some tips from my sliver of experience with VM
- VM is a continuous, proactive process

about this guy

- David C Frier, RIMS-CRMP, CISM, CISSP, CRISC, CCSK
- vCISO and Senior Cybersecurity Program Manager at Sedara… ***but I speak only for myself, not for Sedara!***
- 0x2d years into IT, 0x13 years into Infosec
- Avid player of poker… Orioles and Cubs fan… enthusiastic-if-slow rider of a Trek.
- None of the “usual” social media aside from LinkeDin, but I can be sighted in the Fediverse (#checkin)
- about.me or wheretofind.me

geekosaurus



steps in vulnerability management

- Asset Inventory
- Network Scoping
- Internal and External Scanning
- Classifying Results
- Prioritizing Vulnerabilities
- Remediation Assignment
- Measuring & Reporting

asset inventory (1/2)

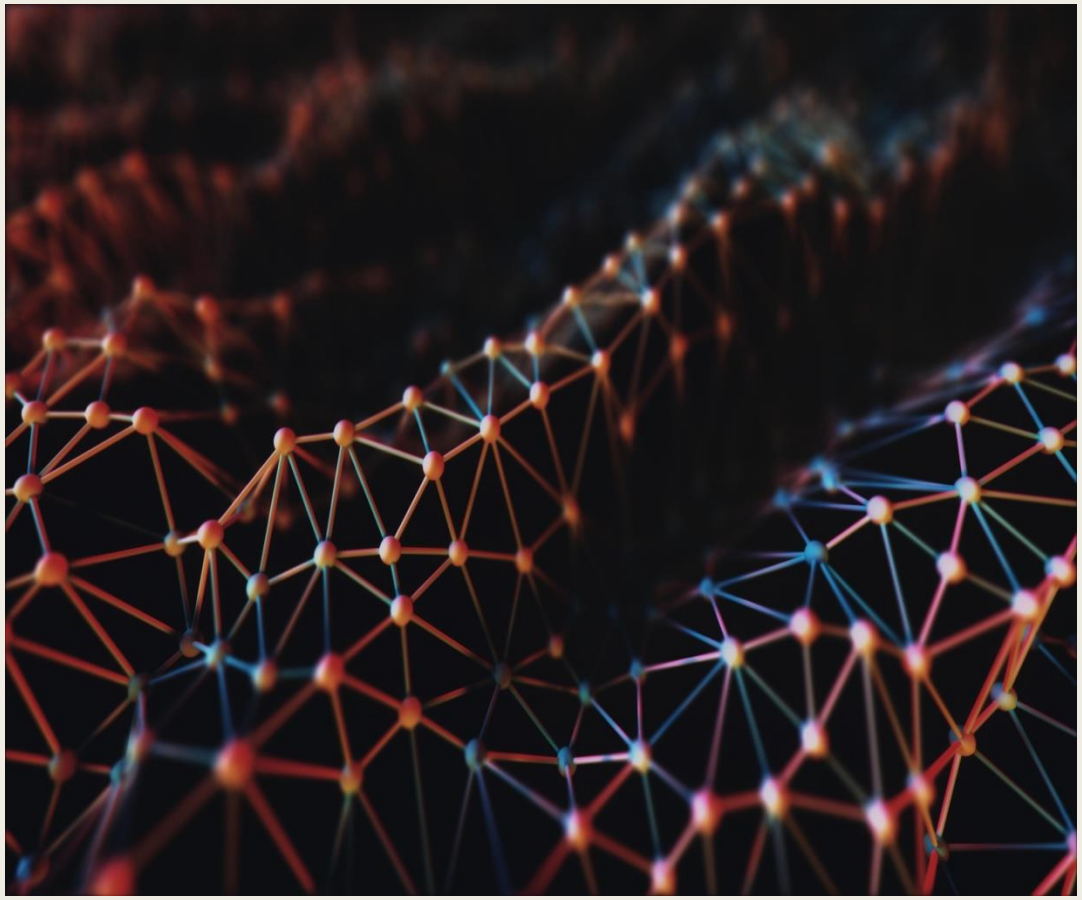
- Identify all hardware and software
- Document asset types and locations
- Asset discovery tools
  - *CMDB*
  - *Nmap, etc.*
  - *Discovery scans*

asset inventory (2/2)

- Criticality ranking (business impact)
- Regular updates for accuracy
- Ensuring full scope for scanning

network scoping (1/2)

- Define internal/external network boundaries
- Identify critical systems for scanning
- Include servers, endpoints, network devices
- Segment your network…
  - *…however it makes sense for your org*
  - *Staff/team scope, or locations, or functions*



network scoping (2/2)

- Avoid unnecessary scans (non-critical assets)
  - *About end-user computers…*
- Consider network segments, subnets, firewalls
  - *Make sure your scanner can access everything*
- Key decisions: what to scan and when

internal scanning

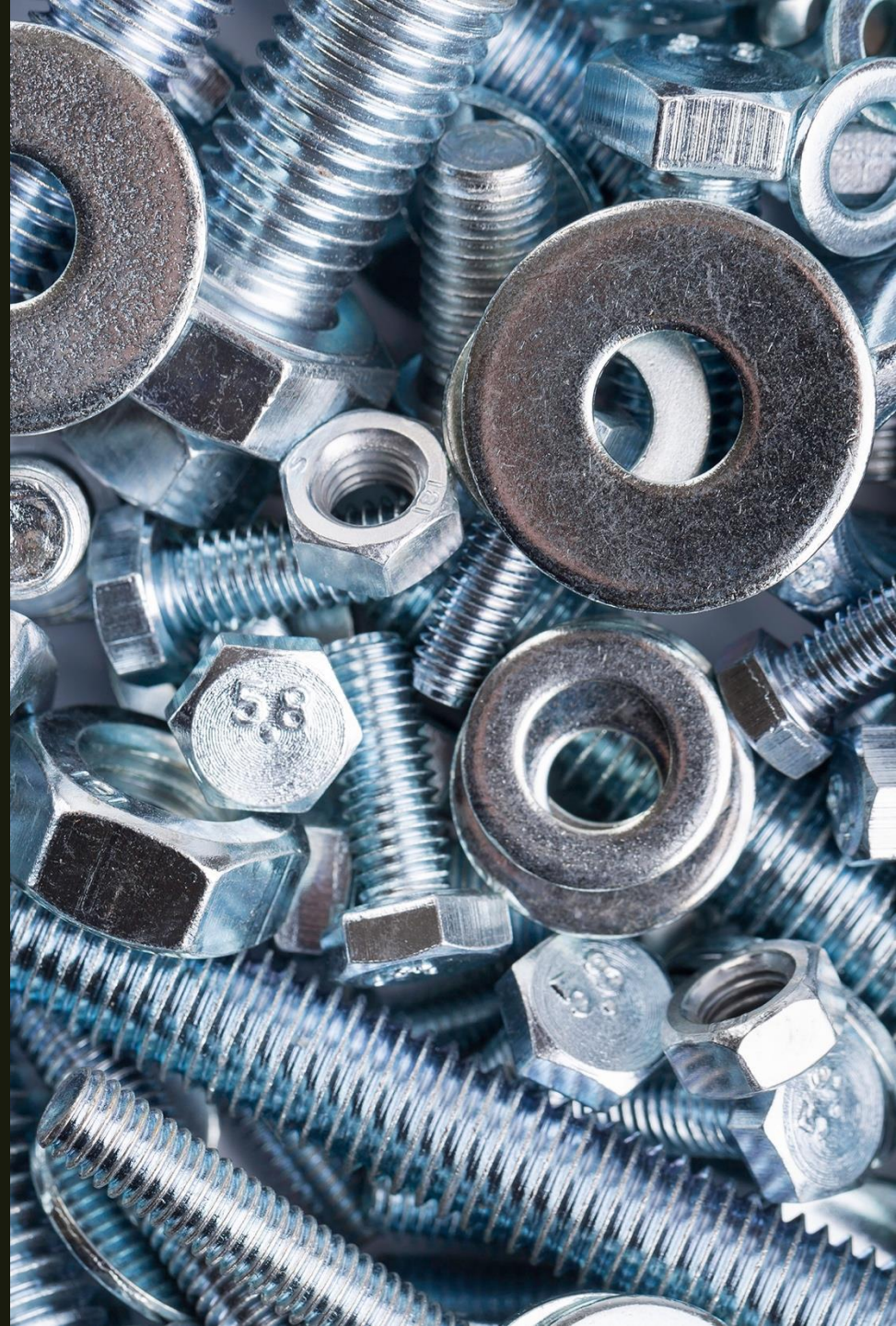
- Focus on vulnerabilities within the internal network
- Detect misconfigurations, outdated software, missing patches
- Regular scans (weekly/monthly)

external scanning

- Assess external-facing assets (e.g., web servers)
- Look for rogue connections
- Verify firewall effectiveness and correct rule-set

scanning tools

- Examples: Nessus/Tenable, Qualys, OpenVAS
  - ***Must*** *be able to emit well-formed, fully-detailed CSVs of scan results*
- Automation for continuous scanning
- Set schedules for regular scans and changes

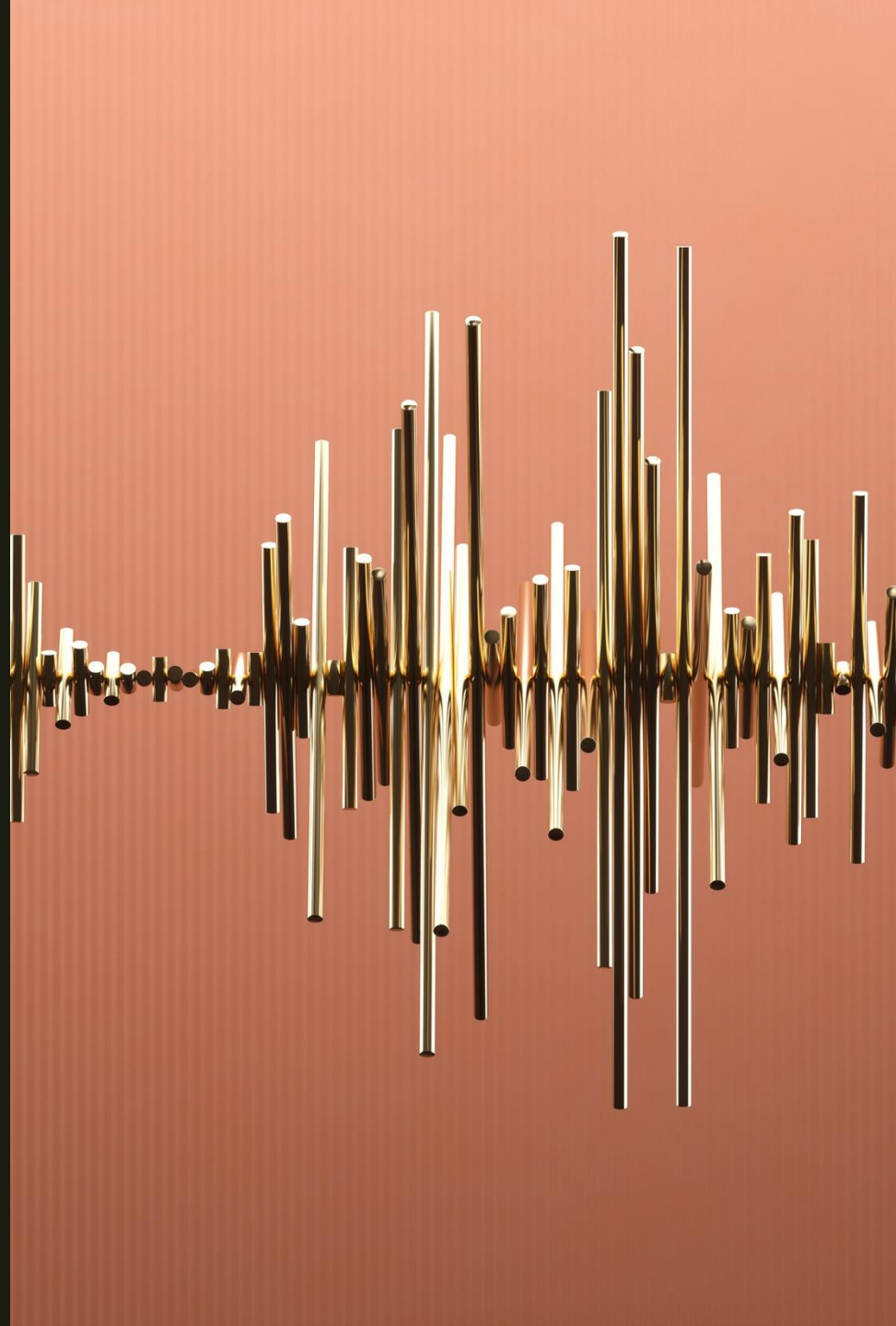


classifying scan results (1/3)

- Categorize by risk level (high, medium, low)
- Use CVSS (Common Vulnerability Scoring System)
- Enrich with EPSS, KEV *(more about this in a sec)*
- Factors: exploitability, impact, asset criticality
- Good idea: database of results over time

classifying scan results (2/3)

- **Enriching** scan results helps with prioritization
- EPSS *(see: https://www.first.org/epss/)*
  - *Exploit Probability Scoring System*
  - *Gives a measure of how likely each CVE is to get an exploit developed against it*
  - *Changes over time*
  - *Has an easy-to-use API*
- KEV *(see: https://www.cisa.gov/known-exploited-vulnerabilities-catalog)*
  - *Known Exploited Vulnerability*
  - *Answers: Has this been used in a reported attack? Was it ransomware?*
  - *List is small-ish*
- With these elements, you can build a risk score formula to suit
  - *A* CVSS + B * EPSS + C if KEV is "Yes" + D if KEV is "Ransomware"*



classifying scan results (3/3)

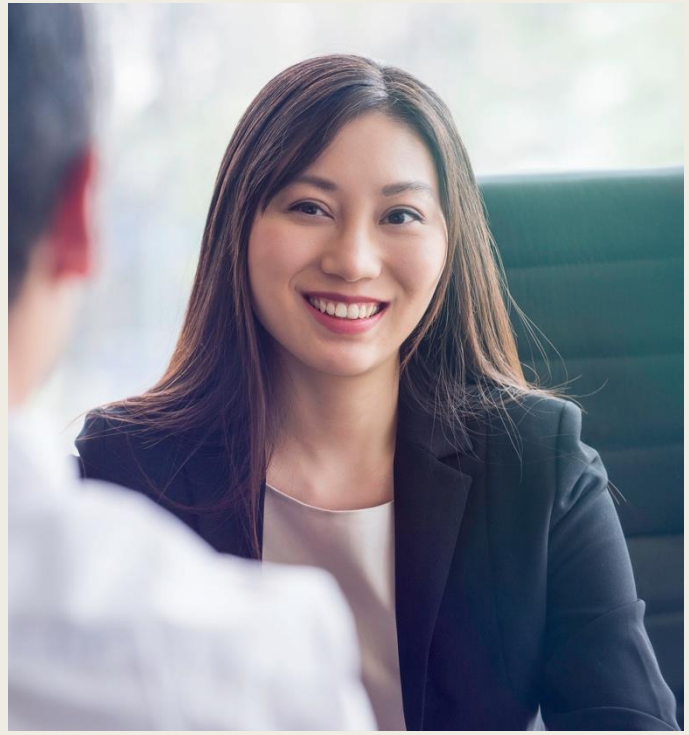
- Vulnerability types: bugs, misconfigurations, patches
- Define risk impact (business vs. operational)
- Streamline classification for faster remediation
  - *Quick way to do this: Excel pivot table!*

prioritizing vulnerabilities (1/2)

- Rank vulnerabilities based on urgency, opportunity
- Use enrichment results if you have them
- Build and use your own risk-score formula
- Focus on severity and critical asset impact
- Use risk scores and asset importance

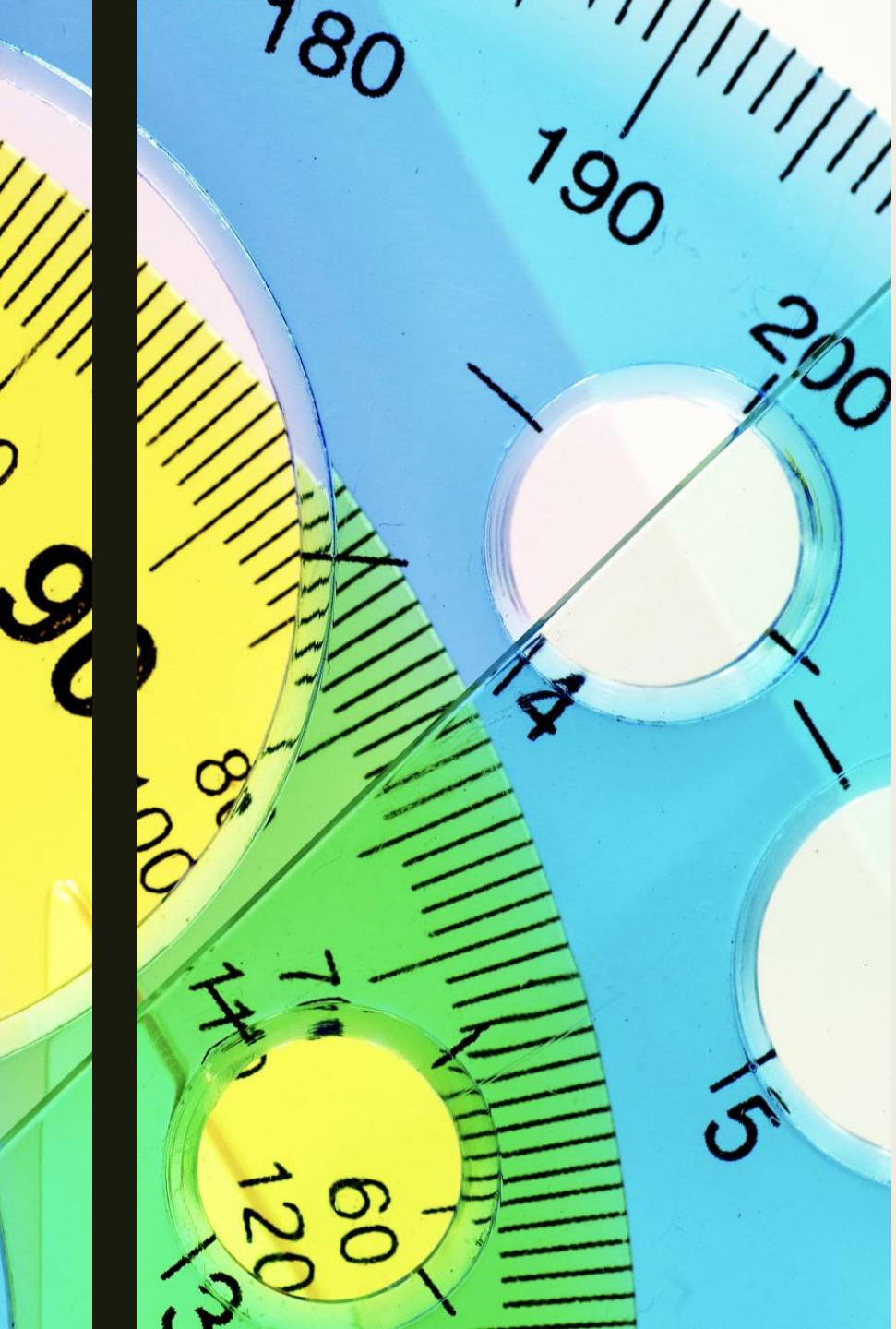
prioritizing vulnerabilities (2/2)

- Factors: threat landscape, active exploits
- Compliance requirements
  - *e.g., PCI, HIPAA*
  - *More generally, business requirements*
- Production schedules
- Automate prioritization if possible



assigning remediation tasks

- Delegating tasks to teams (IT, security)
- If scan jobs align to team responsibilities, this is a natural split
- Use your ticketing systems (e.g., JIRA, ServiceNow)
- Accountability for each vulnerability
- Set deadlines based on priority
  - *Use SLAs where possible*
- Communication of criticality of vulnerabilities to stakeholders
- Automate workflows for patching and updates



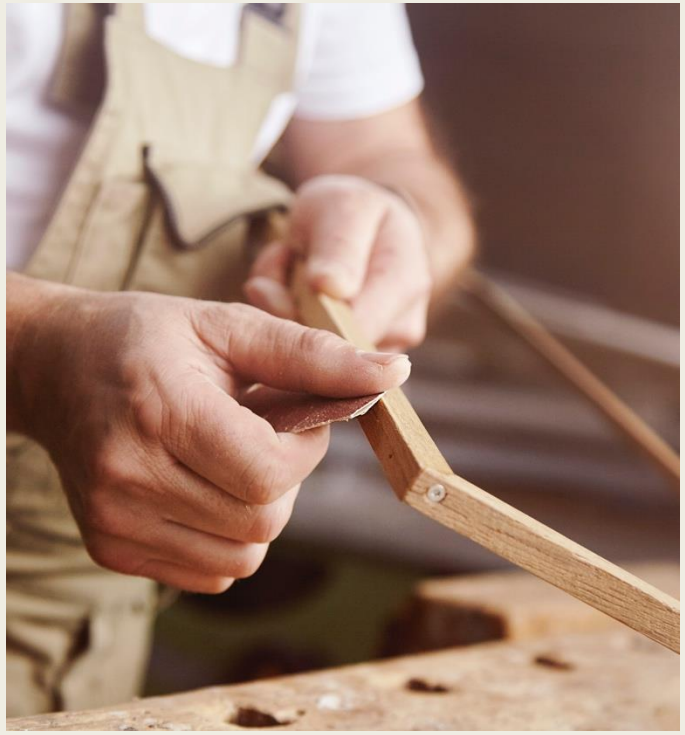
measuring results

- Metrics: vulnerabilities found vs. remediated
- Time to remediation (MTTR)
- Percentage of high-risk vulnerabilities closed within SLAs
- Track aggregate risk scores and %age reduction

reporting results

- Tailor reports for different audiences (IT vs. execs)
- Trends: reduction in vulnerabilities and aggregate risk over time
  - *But make sure to point out, new vulns pop up almost continuously*
- Visualize data (charts, graphs) for clarity
  - *But don't obfuscate with them*

continuous improvement



- Vulnerability management is an ongoing process
- Adjust processes based on:
  - *New threats*
  - *New technology*
  - *New techniques*
  - *Changing business requirements*
- Regular re-assessment and improvement

conclusion

Remember key steps in the vulnerability management cycle

Asset Inventory

Network Scoping

Internal and External Scanning

Classifying Results

Prioritizing Vulnerabilities

Remediation Assignment

Measuring & Reporting

Importance of prioritization using risk

Automation where possible

Continuing Improvement

Q&A

Yes, these slides will be available after the conference, on the RSS website

I can be reached at $FIRST.$LAST (at) rocinfosec (dot) com