Pacific Northwest
NATIONAL LABORATORY

Risk-Informed Approach for Verification and Validation

Seemita Pal, Ph.D.

Team Leader, Systems Engineering Team,
Pacific Northwest National Laboratory

May 2022 Technical Talk with ReliabilityFirst

16th May 2022

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Let’s Start with a Question!

- What percentage of reported CISA security incidents result from exploits against defects in the design or code of software?
  - 10%
  - 30%
  - 60%
  - 90%

[1]https://us-cert.cisa.gov/sites/default/files/publications/infosheet_SoftwareAssurance.pdf

One More Question

- When purchasing an energy delivery system device what questions do you ask the vendor/manufacturer?

Challenges and Opportunities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips | Resources | Industrial Control Systems

Industrial Control Systems > ICS-CERT Alerts > Cyber-Attack Against Ukrainian Crit

ICS Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016 | Last revised: July 20, 2021

Print | Tweet | Send | Share

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purpo
regarding any information contained within. DHS does not endorse any commercial product or service, refe
Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp,

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-st
cyber campaign against Ukrainian critical infrastructure. For more information on Russi

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power ou
also been reports of malware found in Ukrainian companies in a variety of critical infras

U.S. GOVERNMENT ACCOUNTABILITY OFFICE: A Century of Non-Partisan Fact-Based Work

FOR CONGRESS | PRESS CENTER | CAREERS

GAO@100

REPORTS & TESTIMONIES | VIEW TOPICS | VIEW AGENCIES | BID PROTESTS & APPROPRIATIONS LAW | ABOUT

Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)

Posted on May 18, 2021

Share this Story:

The recent cybersecurity attack on the Colonial Pipeline Company has led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast United States.

In today's WatchBlog post, we look at this attack and the federal government and private-sector response. We here at GAO have been warning of cybersecurity threats to critical infrastructure for many years, and the need to strengthen the federal role in protecting critical infrastructure, which we reiterated in a report issued in March.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE: A Century of Non-Partisan Fact-Based Work

FOR CONGRESS | PRESS CENTER | CAREERS

GAO@100

REPORTS & TESTIMONIES | VIEW TOPICS | VIEW AGENCIES | BID PROTESTS & APPROPRIATIONS LAW | ABOUT

SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)

Posted on April 22, 2021

Share this Story:

The cybersecurity breach of SolarWinds' software is one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. In today's WatchBlog post, we look at this breach and the ongoing federal government and private-sector response. This information is based on publicly disclosed information from federal and private industry sources. We here at GAO are currently conducting a comprehensive review of the breach with plans to issue a public report later this year.

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

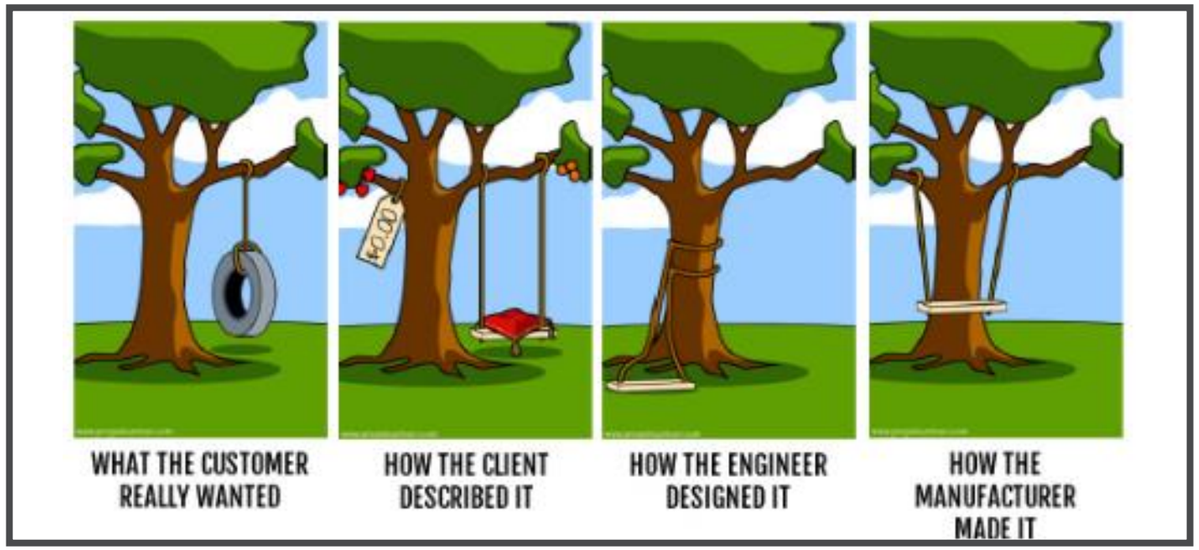
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the

Executive Order Link: https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity?utm_medium=email&utm_source=govDelivery

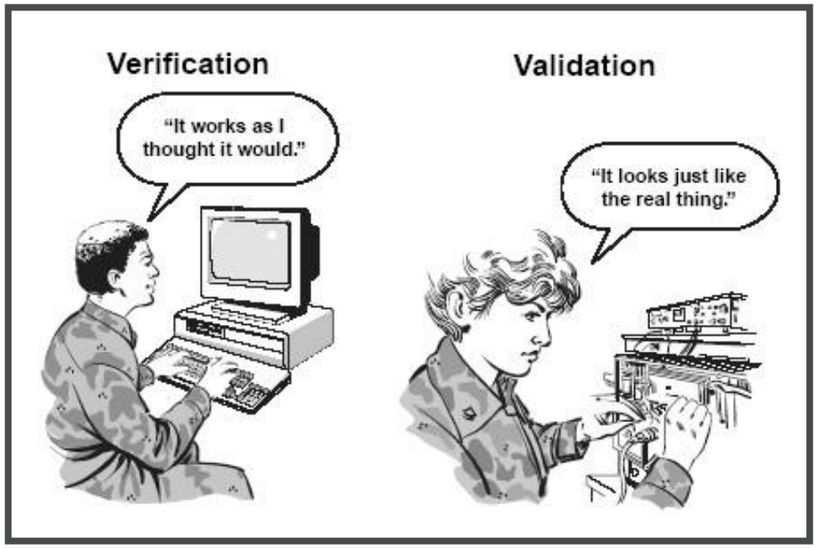
Verification and Validation (V&V)

- **Verification** – have you built something correctly *(does it meet spec?)*
- **Validation** – have you built the right thing *(does it meet user needs?)*



Avoid

Image Source: https://miro.medium.com/max/996/1*nhVE3RkKyhk2kEh3nuk3Lw.png, Last accessed: 03/13/22



Achieve

Image Source: https://commons.wikimedia.org/wiki/File:Verification_Validation_Accreditation.jpg, Last accessed: 03/13/2022

Challenge 1: Verification and Validation (V&V) Throughout the Lifecycle

Different lifecycle phases, and different stakeholders

Challenge 2: Different Devices Mean Different Risks

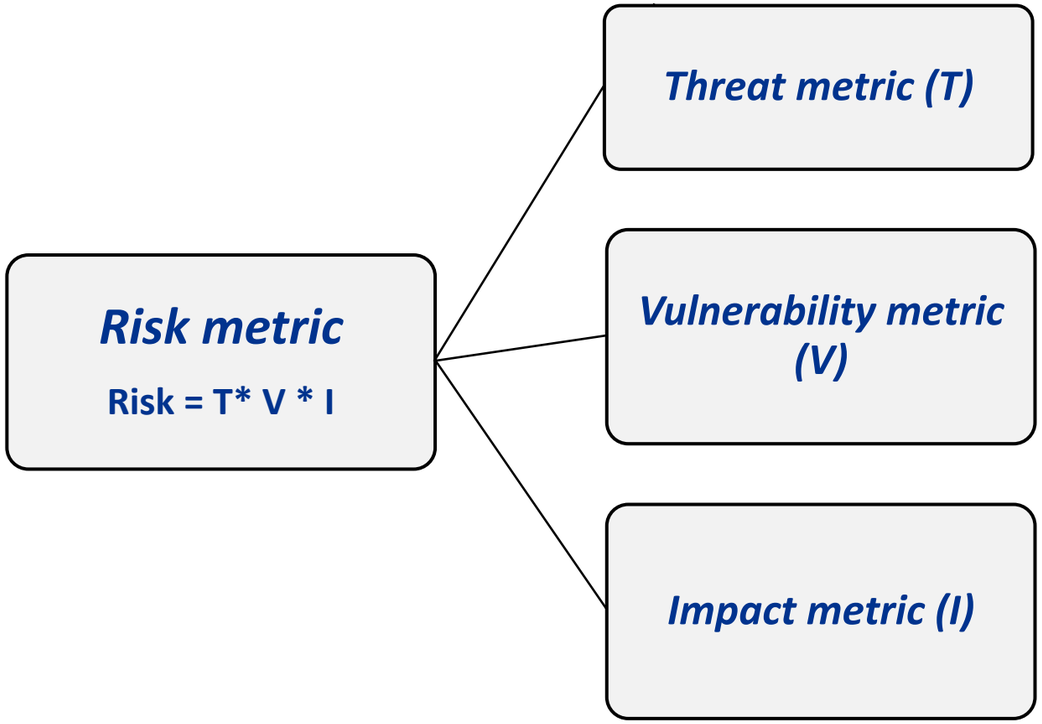
Image Source: https://image.shutterstock.com/image-photo/indoor-medium-voltage-metal-enclosed-260nw-1288606204.jpg Last Accessed: 03/13/2022

Image Source: https://www.shutterstock.com/image-photo/wifi-smart-plug-on-white-background-1805313235 Last Accessed: 03/13/2022

Estimated risk ← → V&V Testing Rigor

Risk-Informed Approach

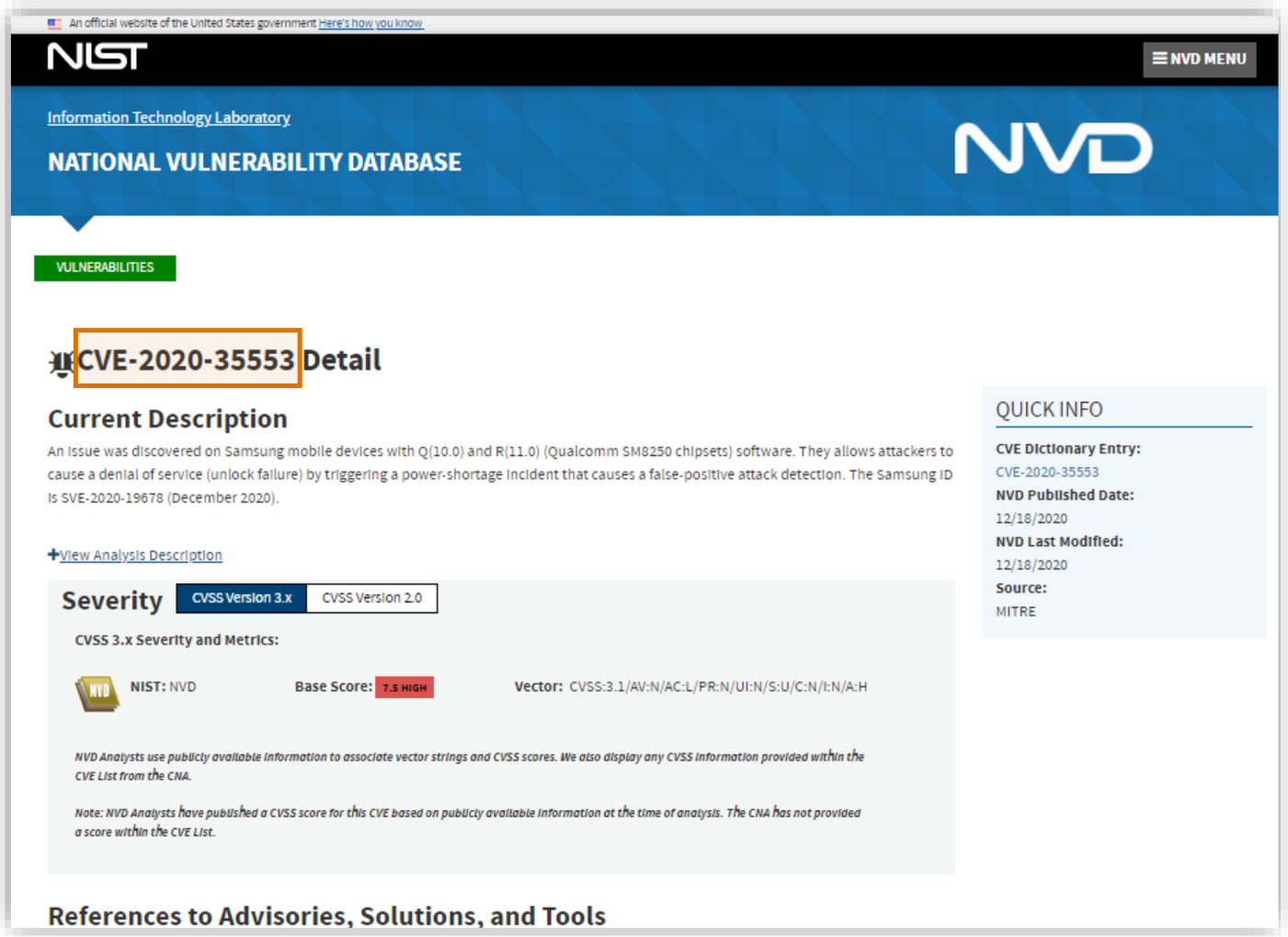
- *Risk* is potential loss or harm related to technical infrastructure, use of technology or reputation of an organization due to exposure or loss resulting from a cyber attack or data breach on organization
- *Risk metric* measures extent to which vulnerabilities in a product could be exploited or triggered by an adversary
- Why do we need *risk-metric*?
  - Basis for proactive security
  - Risk-informed prioritization of V&V
  - Efficient utilization of resources



Glyn A. Holton (2004) Defining Risk, Financial Analysts Journal, 60:6, 19-25, DOI: 10.2469/faj.v60.n6.2669

Introduction to Common Vulnerabilities and Exposures (CVEs)

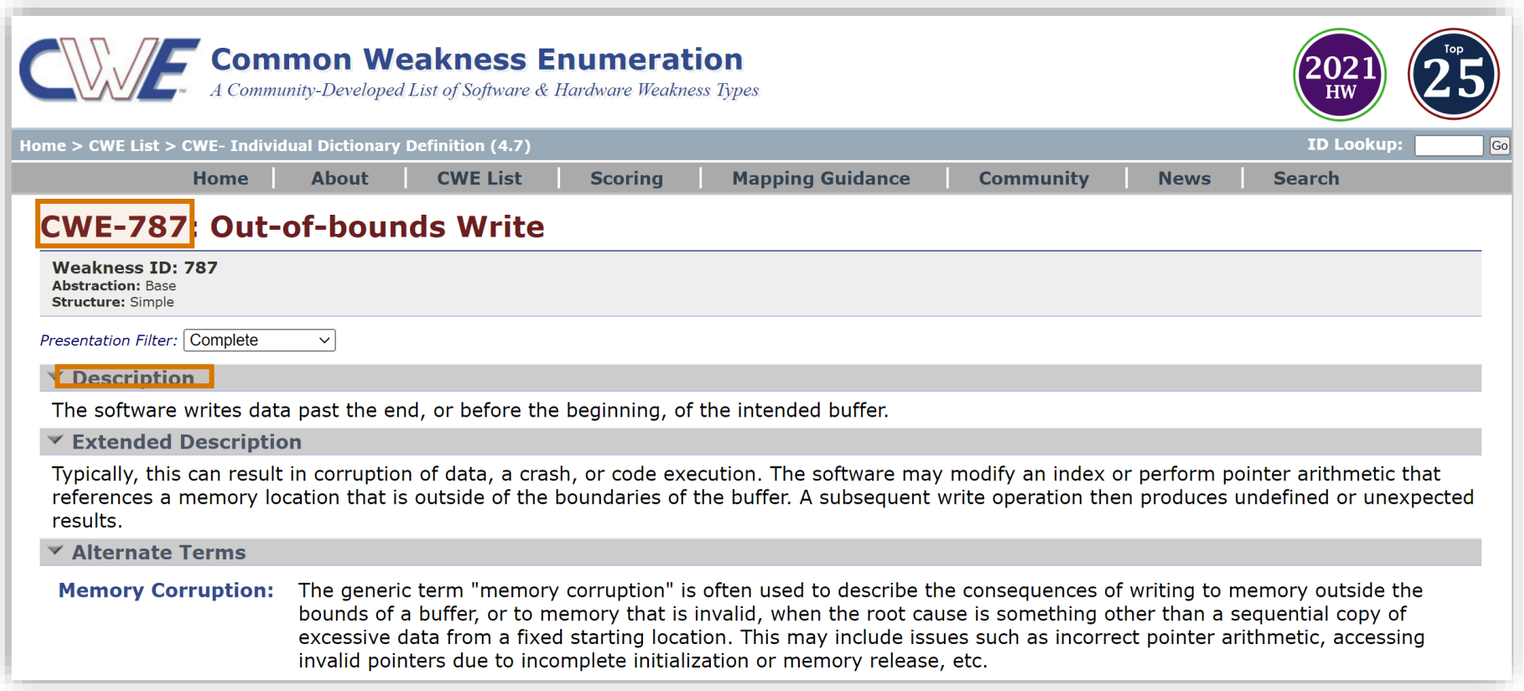
- Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities
- CVE ID is a unique, alphanumeric identifier referencing a specific vulnerability



Source: https://nvd.nist.gov/vuln/detail/CVE-2020-35553

Introduction to Common Weakness Enumeration (CWE™)

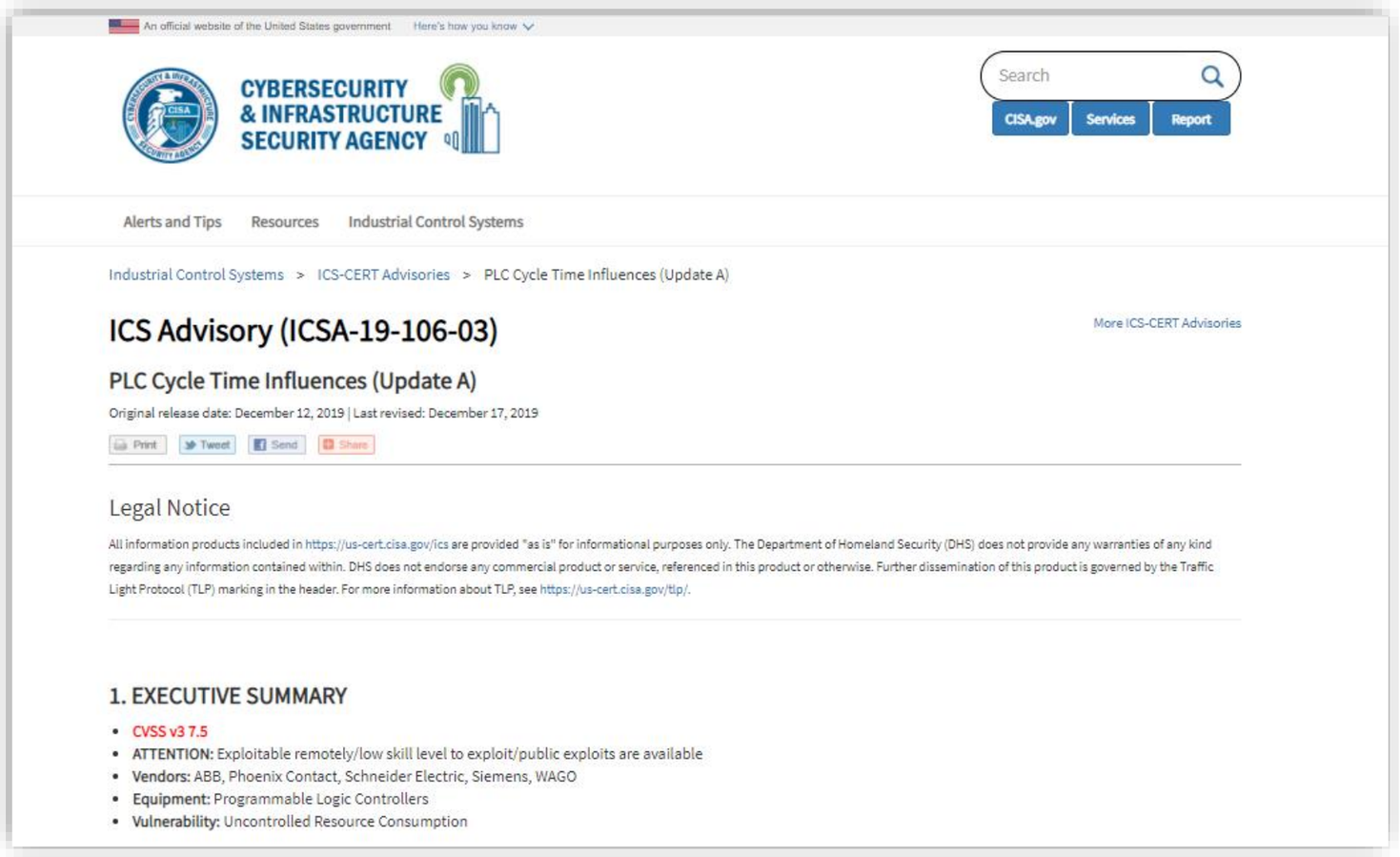
- Formal list or dictionary of common *software and hardware weaknesses* that can occur in architecture, design, code, or implementation that can lead to exploitable security vulnerabilities
- Includes *Weakness ID, description, applicable platforms, common consequence* and other relevant information



Source: https://cwe.mitre.org/data/definitions/787.html

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Advisory

- Conduct vulnerability and malware analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations

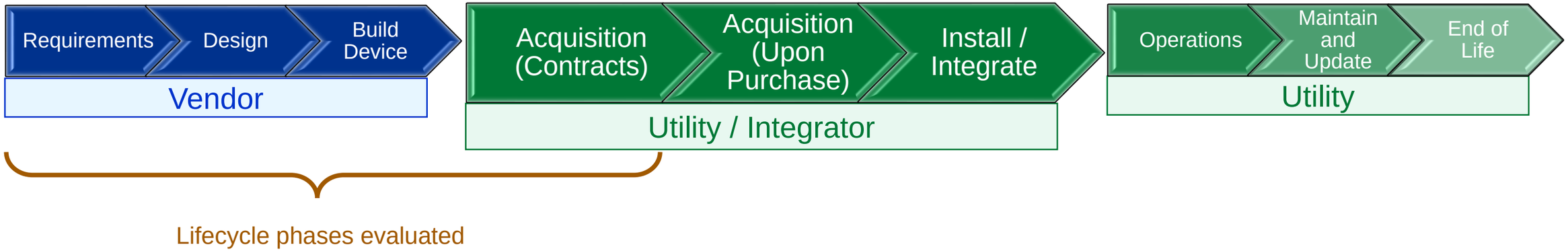


https://www.cisa.gov/uscert/ics/advisories/ICSA-19-106-03

Risk-Informed V&V Approach: Getting Started

1	• User wants to assess a specific product	Product model ‘XYZ’ from fictional vendor ‘ABC’
2	• Perform a search of the ICS-CERT, NIST and MITRE databases to identify any relevant CVEs and corresponding CWEs	Returns a series of weaknesses (for example): 1. "CWE-22” 2. "CWE-787”
4	• User sends list to vendor to determine patching/mitigation status	Send list of vulnerabilities (for example): 1. "CVE-2021-xxxxx” 2. "CVE-2019-xxxxx”
5	• Appropriate testing techniques are determined	1. Dynamic code analysis 2. Static code analysis

Pre-Procurement Guidance



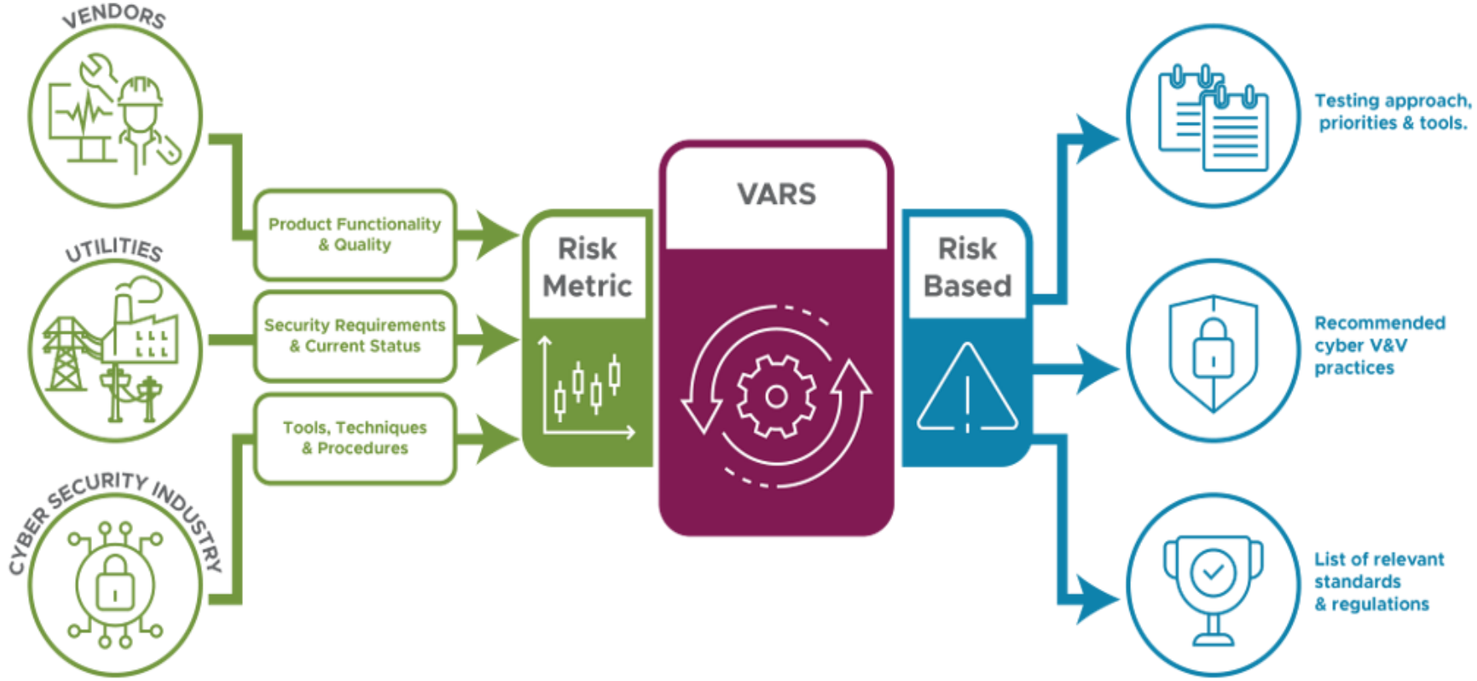
1. U.S. Department of Homeland Security (2009). "Cyber Security Procurement Language for Control Systems." Accessed April 11, 2022
2. Energy Sector Control Systems Working Group (ESCSWG) (April 2014). "Cybersecurity Procurement Language for Energy Delivery Systems." Accessed April 11, 2022:
3. "IEC 62443-4-2: Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components"
4. "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities," in IEEE Std 1686-2013 (Revision of IEEE Std 1686-2007), vol., no., pp.1-29, 13 Jan. 2014.
5. "NATF Supply Chain Security Criteria Version 2.0", Accessed April 11, 2022: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Product-specific information and vendor organizational level practices together determine security maturity

Risk-Informed Verification and Validation Recommendation (RIVVR)

RIVVR tool for organizations to determine risk-informed Verification and Validation (V&V) approaches

- Tool will be ready for pilot testing by June 2022
- Target users:
  - Primary: Asset owners – Energy utilities
  - Secondary: Vendor & OEM – EDS hardware/software vendors, integrators

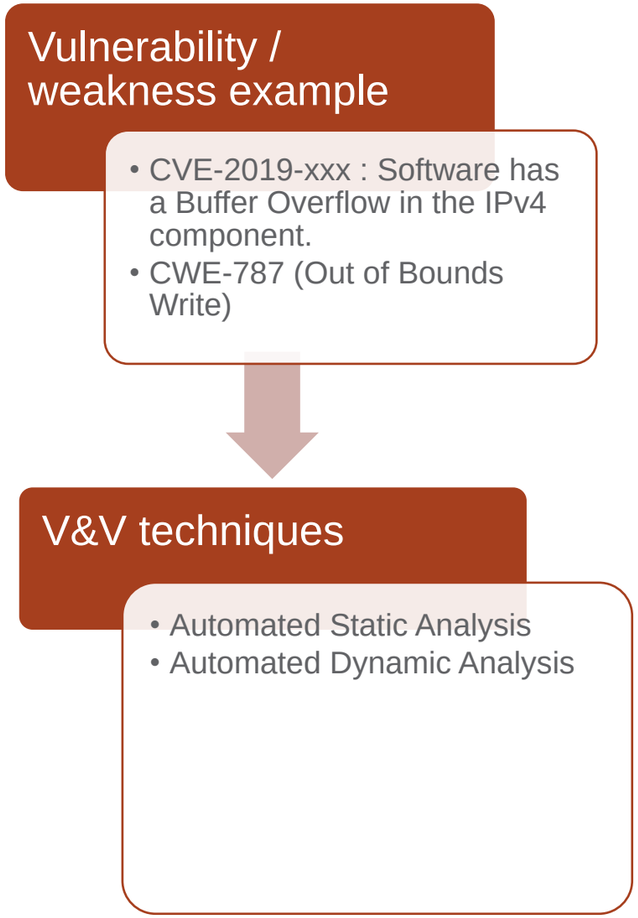


Consultant
Shabbir Shamsuddin

Weaknesses to Techniques to Standards and Tools

STANDARDS

IEEE 1686-2013
IEEE 1012-2016
IEEE C37.1
IEEE C37.238-2017
CIP-007-6
CIP-010-3
CIP-013-1
ANSI/ISA-62443-2-4-2018
ANSI/ISA-62443-4-1-2018
ANSI/ISA-62443-4-2-2018
NIST SP 800-30 Rev. 1
NIST SP 800-82
NIST SP 800-160
NIST SP 1800-2
API Standard 1164
…

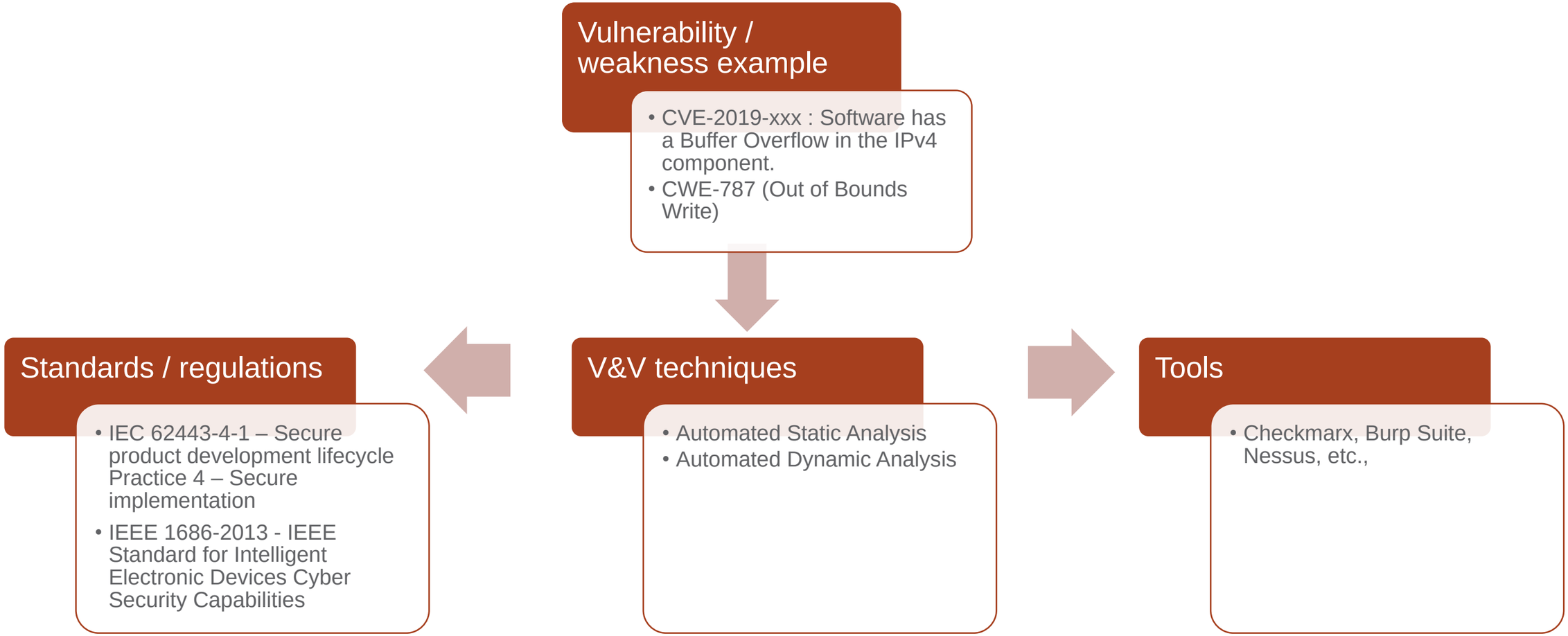


TOOLS

AMD CodeAnalyst
Checkmarx
FlawFinder
Ghidra
GNU Debugger
Lint
Metasploit Framework
MOPS
Nmap
RATS
SonarQube
SSASS-E
Tenable Nessus
WhatsUp Gold
…

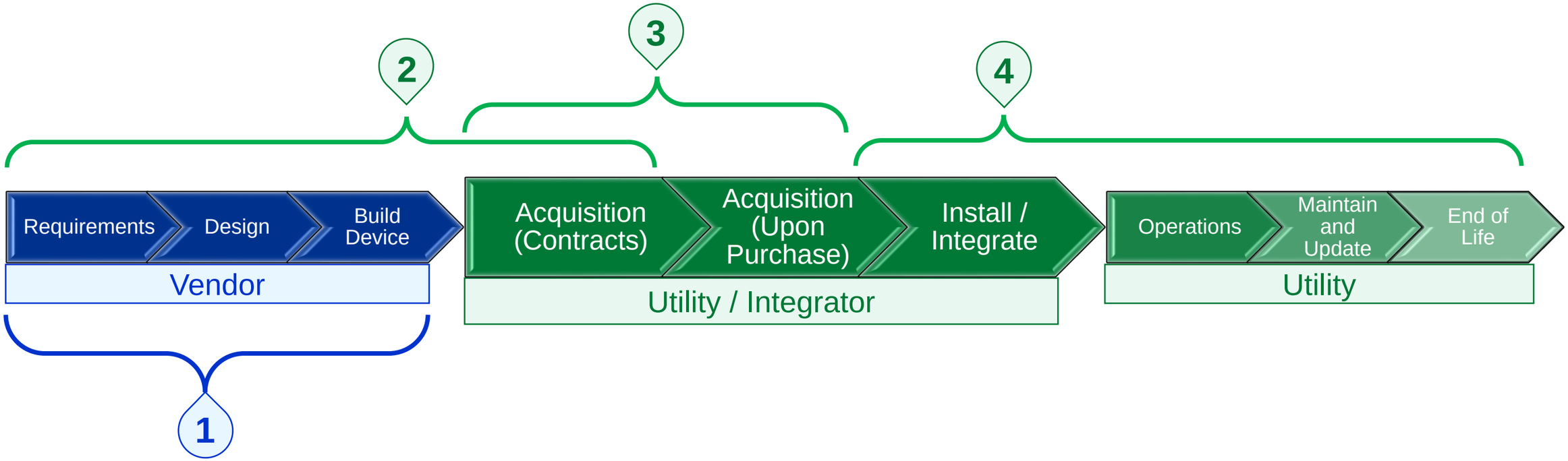
Recommendations of V&V prioritized according to risk type

Weaknesses to Techniques to Standards and Tools



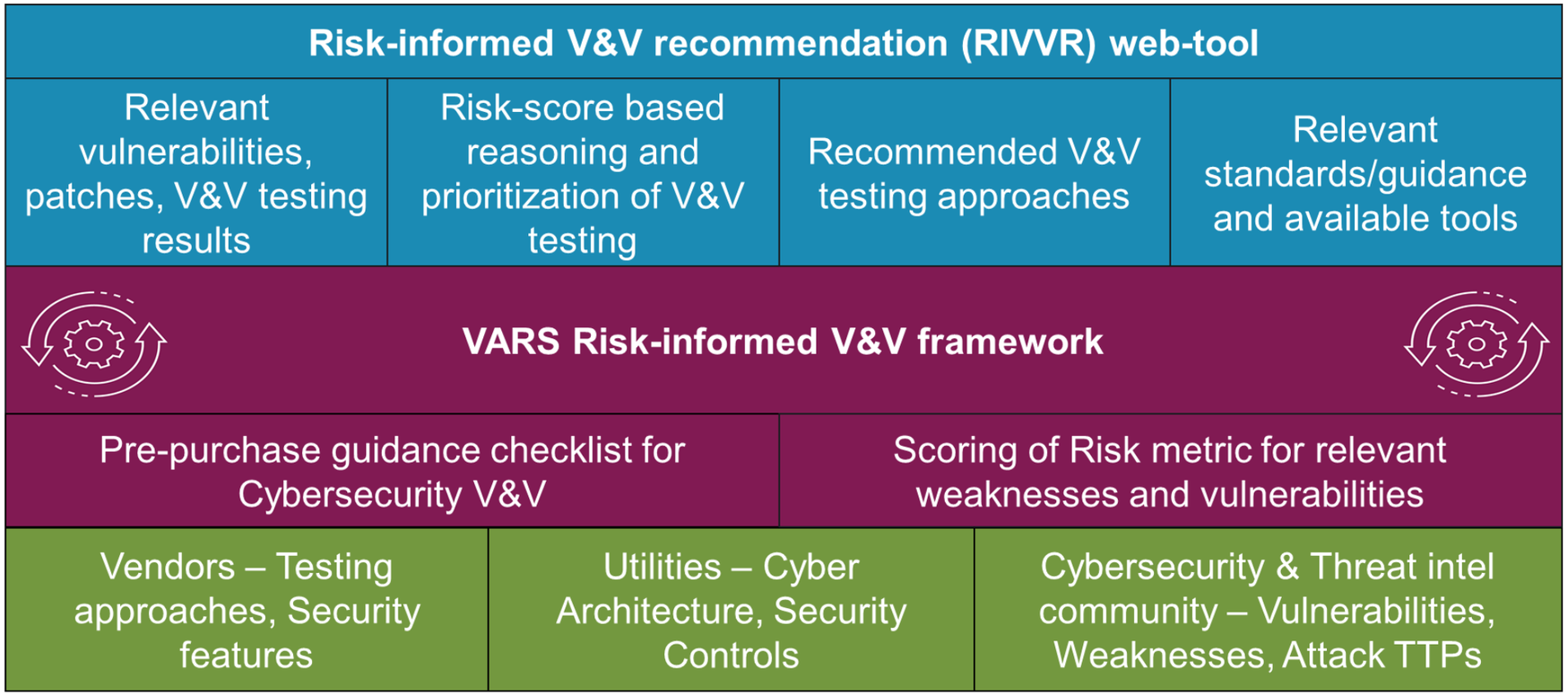
Recommendations of V&V prioritized according to risk type

Major Benefits



1 Standards, techniques and tools for vendors
2 Pre-procurement guidance checklist for utilities
3 Risk scoring for resource prioritization/planning/replacement
4 Standards, techniques and tools for utilities

Thank You



Seemita Pal
seemita.pal@pnnl.gov