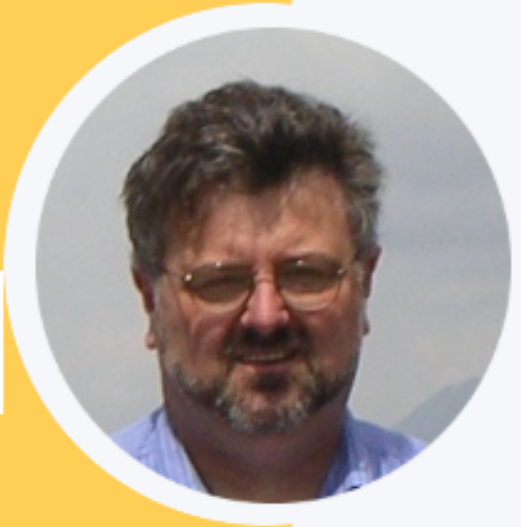
energycentral.

Power Talks™

CIP-010-3 Software Verification for Compliance and Supply Chain Security Controls



with Dick Brooks
Co-Founder and Lead Software Engineer,
Reliable Energy Analytics LLC

NERC Supply Chain Standards

- CIP-013-1
- CIP-010-3
- CIP-010-3 R1 Part 1.6 – Software Verification Requirements

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-3&title=Cyber%20Security%20%E2%80%94%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&Jurisdiction=United%20States

NERC/NATF Guidance

Endorsed Implementation Guides

Cyber Security Supply Chain Risk Management Plans

CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)

Executive Order 13873 of May 15, 2019

Securing the Information and Communications Technology and Services Supply Chain

Implementation Guidance for Verifying the Identity of the Software Source and the Integrity of the Software with a Single Method

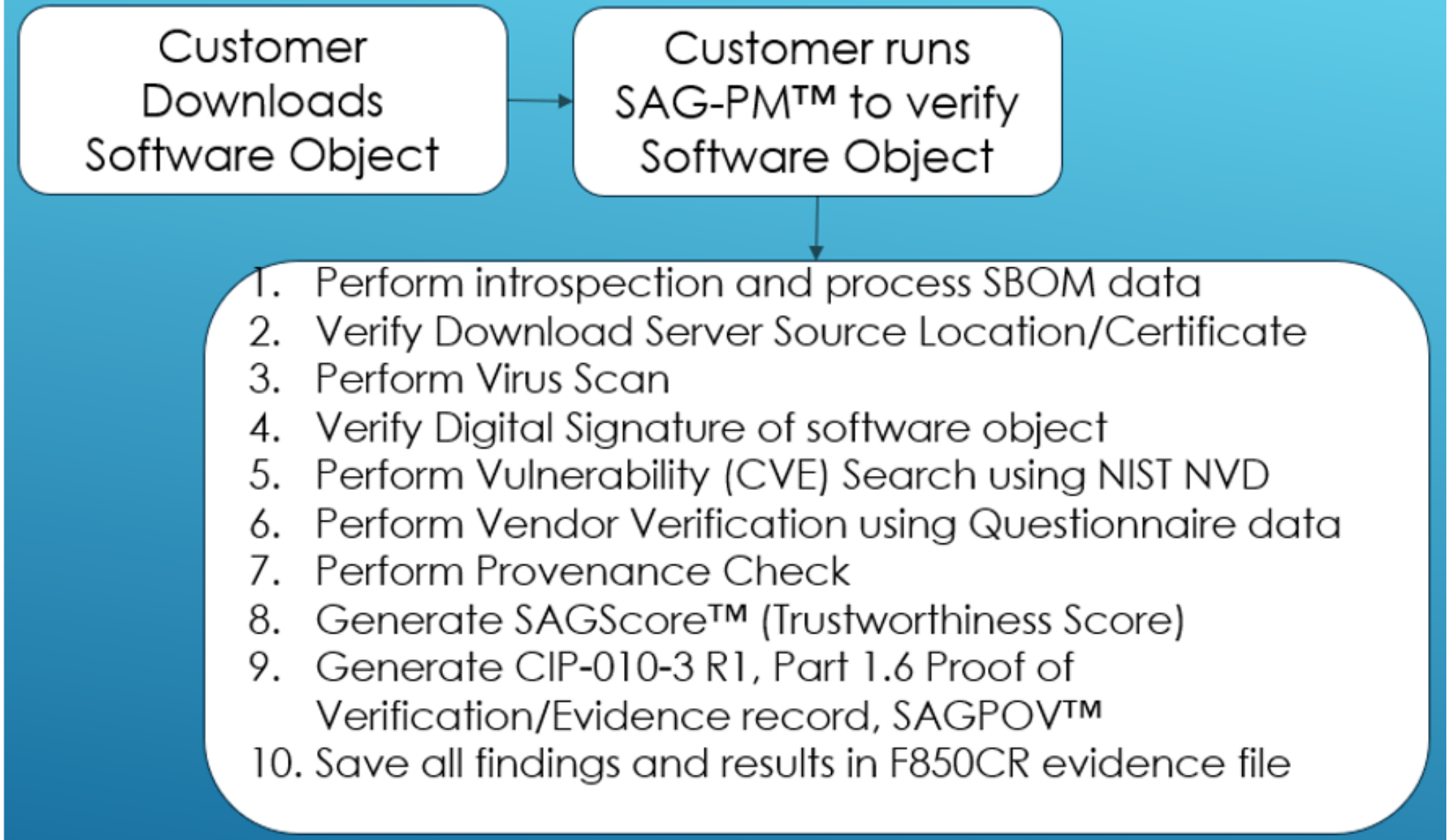
Some methods may complete both the verification of the identity of the software source and the verification of the integrity of the software obtained from the software source. Validation of digitally signed software is an example of a method that accomplishes both obligations required in CIP-010-3 Requirement 1, Part 1.6. Further, some processes may handle this in an automated fashion. One example of this is the Microsoft update process using Windows Server Update Services (WSUS) as described in the article found at the following link:

https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-010-3%20R1.6%20Software%20Integrity%20and%20Authenticity.pdf

Is this Guidance Accurate?

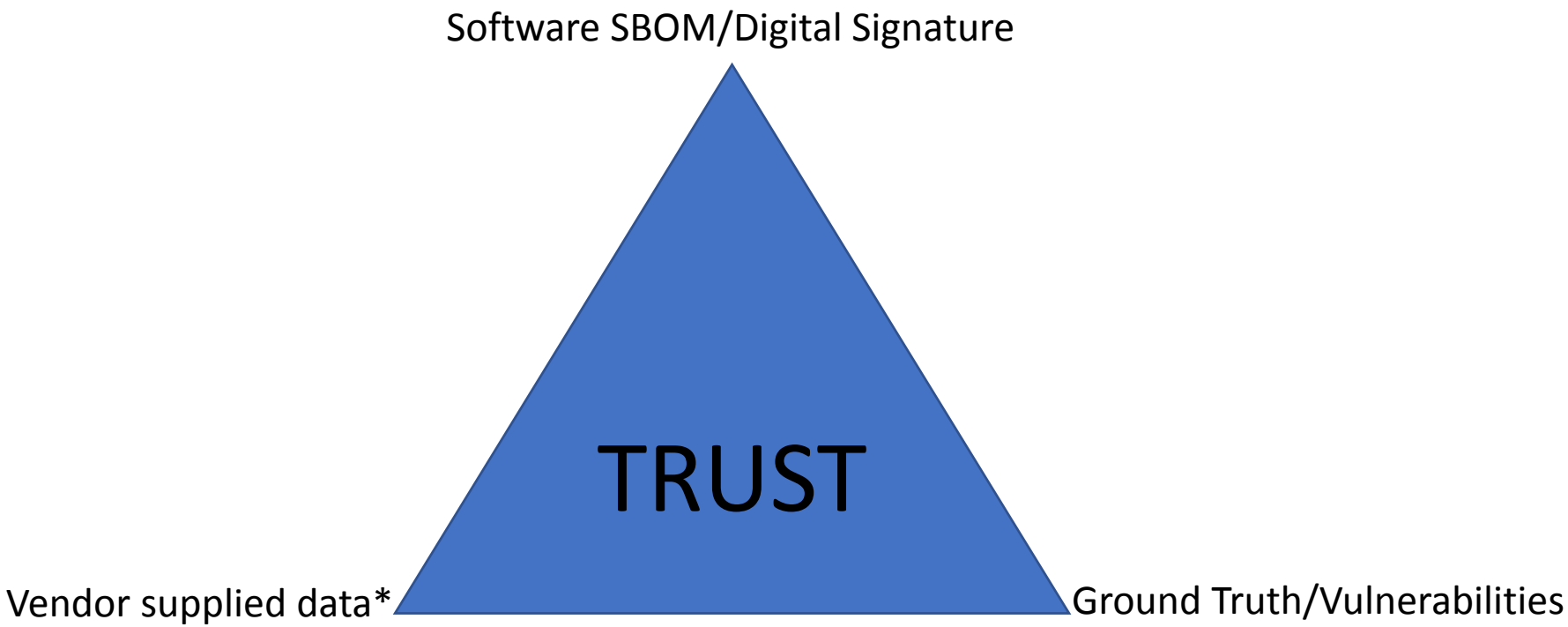
- NO
- A Digital Signature alone will not verify the identity of the party that produced the software
- Verification of identity requires two steps:
  1. Identify the party that produced the software
  2. Verify that the digital signature matches the name of the party that produced the software

SAG-PM™ PROCESS FLOW



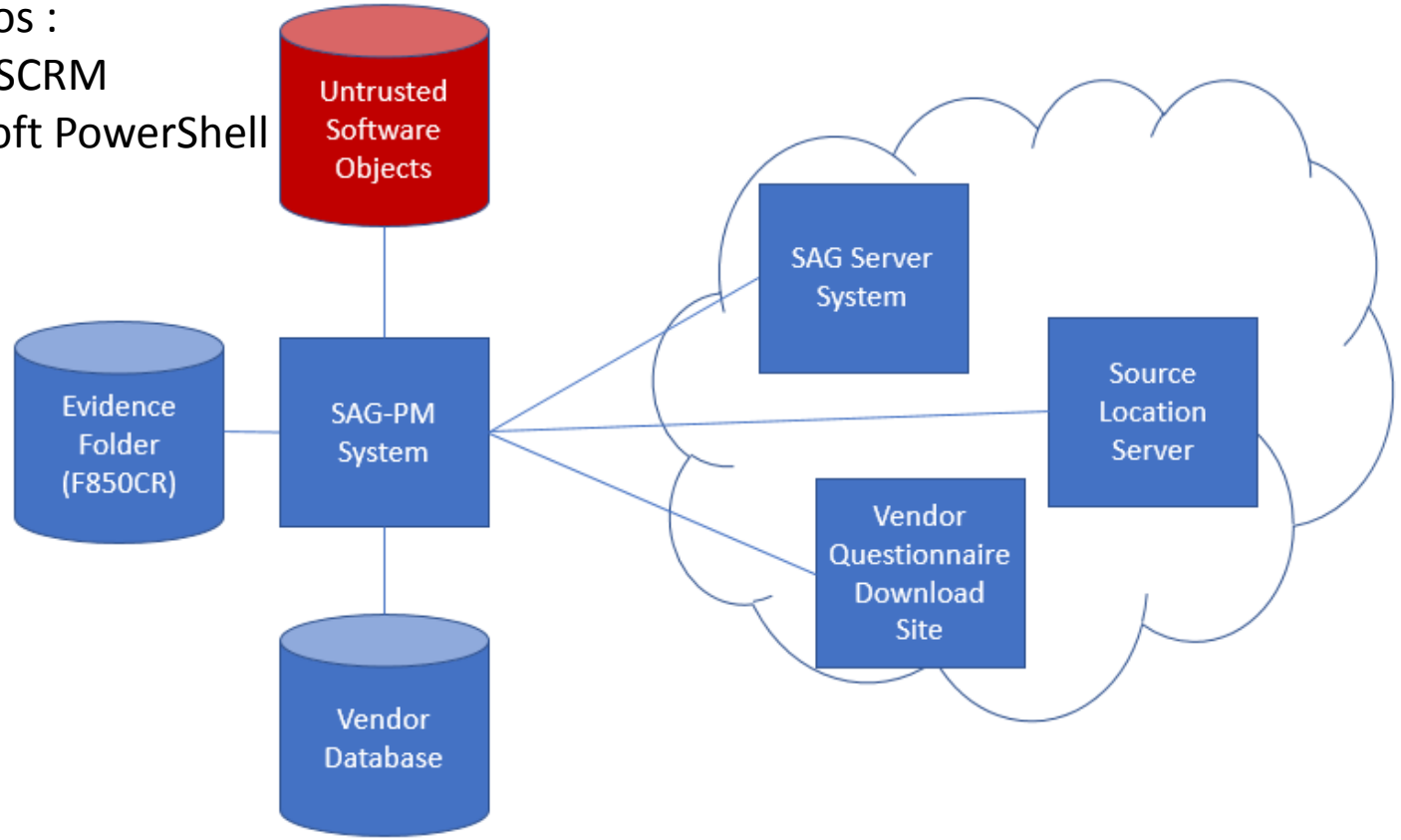
SAG-PM™ Methodology

- *Never trust software, always verify and report!*™
- Corroborating evidence is key to establishing trust
- Even today some malware scanning engines fail to detect the malware used against Solarwinds



SAG-PM™ Components

Two Demos :
1. NIST C-SCRM
2. Microsoft PowerShell



SAG-PM™ Demonstration

- Create a SPDX SBOM when no SBOM is provided by a Vendor
- Demonstrate a suspicious digital signature and the Warning issued by SAG-PM ™
- Demonstrate Evidence data (3 files)
  1. F850CR Evidence Data for Risk Assessment (all 7 steps)
  2. SBOM created by SAG-PM™
  3. Malware scanning results – Microsoft Defender

Demonstrate NIST C-SCRM

- Shows warning for digital signature mismatch

Demonstrate Microsoft PowerShell

- SBOM creation

Questions?

energycentral™

Power Talks

Dick Brooks
Co-Founder and Lead Software Engineer,
Reliable Energy Analytics LLC

ENERGY CENTRAL | COMMUNITY@ENERGYCENTRAL.COM