RELIABLE ENERGY ANALYTICS (REA™) SOFTWARE ASSURANCE GUARDIAN POINT MAN (SAG-PM™)

APRIL 4, 2022

ACRONYMS

Acronym	Description
CISA	Cybersecurity & Infrastructure Security Agency
FERC	Federal Energy Regulatory Commission
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
SBOM	Software Bill of Materials
SPDX	A US Government endorsed SBOM standard

ABOUT REA

- Software Developer of Cybersecurity Supply Chain Risk Management (C-SCRM) tools, SAG-PM™
- Gatekeeper for the Software Assurance Guardian Community Trust Registry™ SAG-CTR ™
- Inventor of Patent 11,374,961 Methods For Verification Of Software Object Authenticity And Integrity
- Influential in the development of SBOM and Supply Chain standards at NTIA, NIST and CISA
- Influential in the development of Industry Standards (FERC regulations) and SPDX SBOM

SUPPLY CHAIN CYBERSECURITY BUSINESS DRIVERS

- US Government Driving Demand
  - Executive Order 14028, May 2021
  - Cybersecurity Reporting Law, March 2022
- Ransomware Pandemic
- New Laws requiring evidence of controls
- Regulatory Changes Forthcoming (SEC October NOPR)
- Cyber Insurance and Credit Rating Agencies demanding proof of cybersecurity practices
- Shareholder lawsuits against BoD members and C-Level Executives for cybersecurity failures

THE SOFTWARE SUPPLY CHAIN DILEMMA

Hackers want something from you

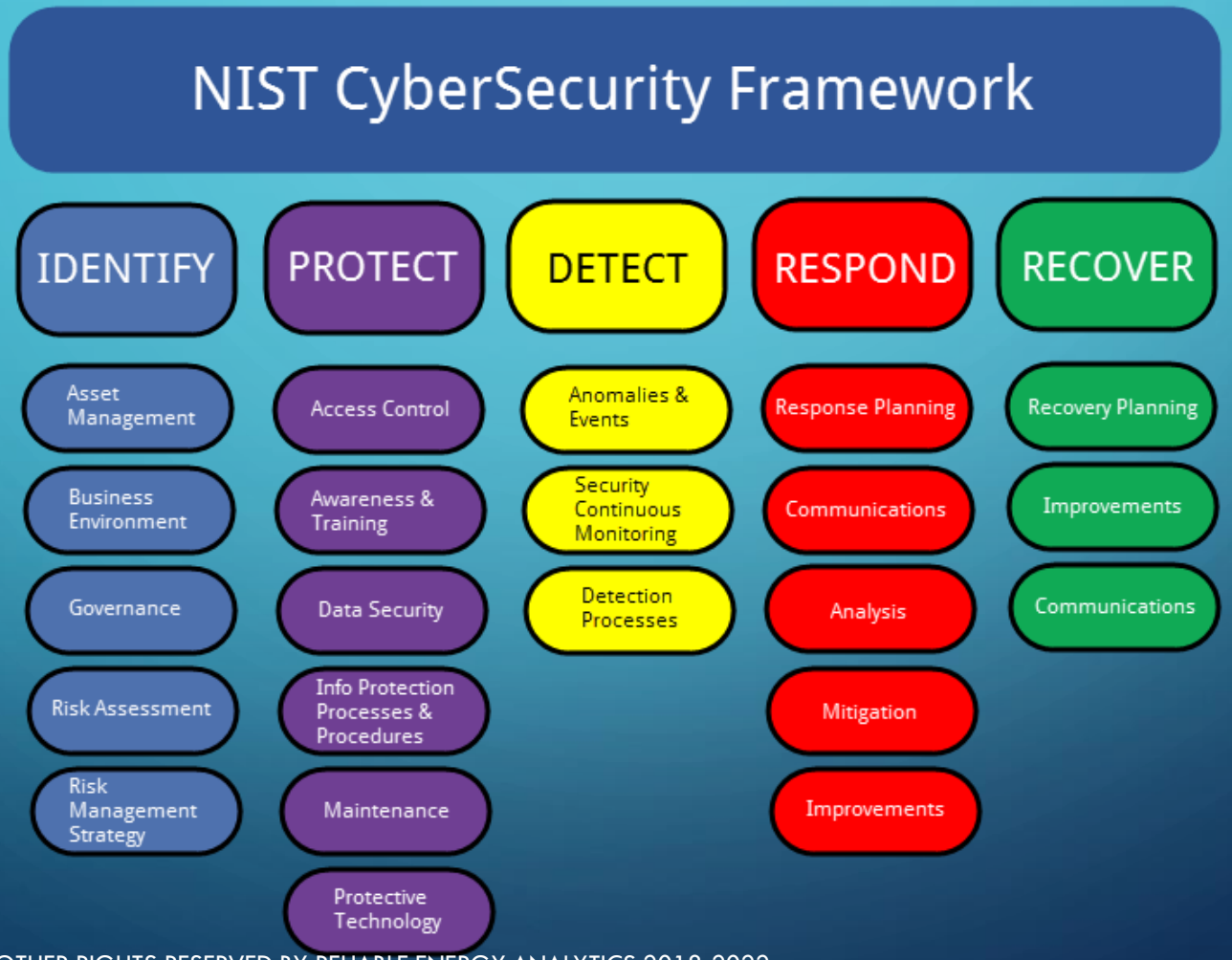
- Money
- Data
- Intellectual Property
- Trade Secrets
- Destroy Reputation
- Bragging Rights
- Peer Recognition

How they succeed (at your expense)

- Downloadable Software
- Deceptive Emails
- Vulnerable Software
- Malware
- Human Trust
- Tenacity

STEPS TO PROTECT YOURSELF FROM HACKERS

- These are the best practices prescribed by the US Government Experts at NIST



WHAT YOU NEED TO KNOW

Would you eat what's in this can without knowing what you're eating?

This happens every day with software that is downloaded from the Internet.

GOAL: Determine if "this thing" is trustworthy

1. Identify what's inside
2. Identify who supplied it
3. Identify where it came from
4. Protect yourself from harm; make risk based decision to purchase AND install software
5. Detect risks, i.e., Food Recalls
6. Determine if others have established trust
7. Determine trustworthiness score
8. Save your evidence to prove due diligence

BUT HOW DOES THIS WORK IN PRACTICE?

- Imagine you go to your favorite app store to search for a calorie counting app – you do a search and 12 options are returned.
- How do you choose which one to install?
- What if each app result contained a TRUST next to the GET button?
- Pressing the TRUST button returns a Trust Score, called a SAGScore™ that indicates the level of trustworthiness for each app, similar to a FICO Score
- Now you can decide which app is the most trustworthy before installing in your phone

PROACTIVE VS REACTIVE ACTIVITIES

- Software is the root of all evil in digital ecosystems
- Proactive Activities: Look for Indicators of Threat (IOT)
  - Detect risk before a software product is purchased or installed
  - Prevent harmful software from being installed or executed
  - Avoids business disruption and costly recovery efforts, as well as other effects (reputational)
- Reactive Activities: Look for Indicators of Compromise (IOC)
  - Detect when hackers have already breached the wall
  - Too late to stop an attack, but can help limit damage
  - Indicator that Incident Response Plans need to be initiated
- You need BOTH

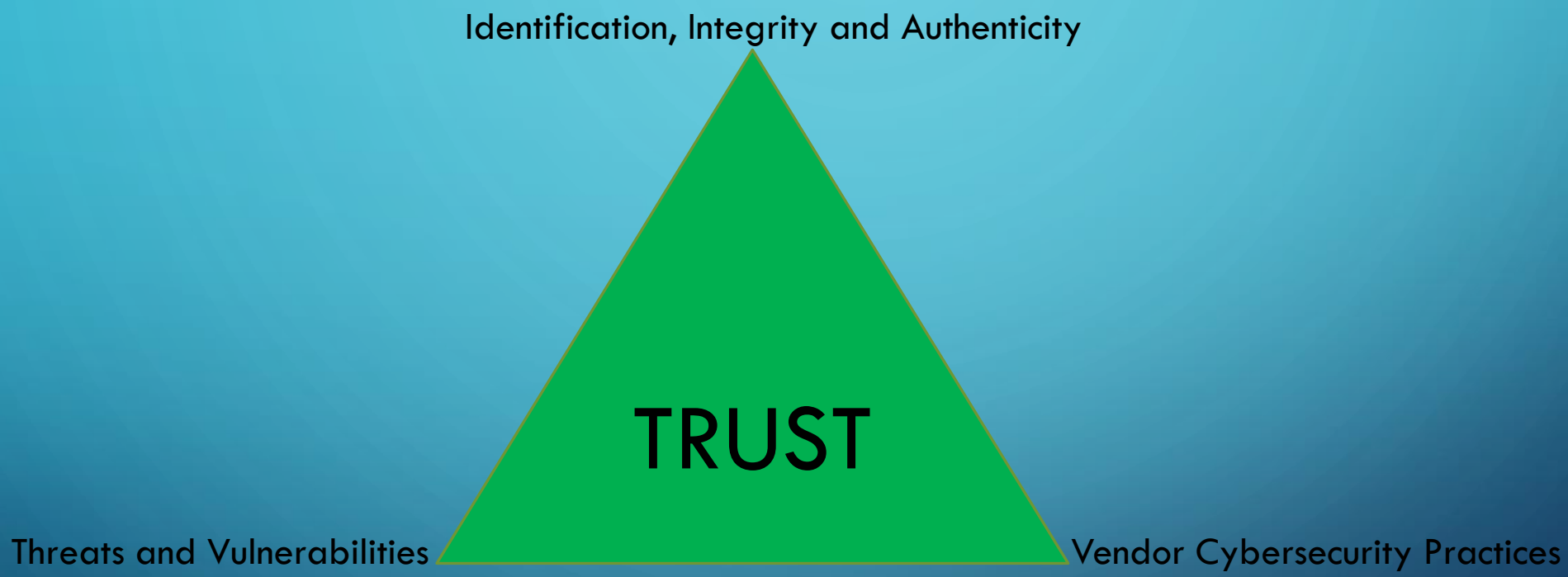
SAG-PM

- Assumes that all software is evil, until proven otherwise
- Need to determine if software is trustworthy before purchase and installation
- Need to determine trustworthiness score (SAGScore™) using a 7-step patent pending process (16/933161)
  - Similar to a FICO score in expressing trust
  - Ranges from 0 to 100
    - Zero equals NO TRUST
    - 100 equal COMPLETE TRUST
  - Statistically Calculated and Weighted
  - 20+ risk factors examined
- Make risk based decision to purchase/install based on SAGScore

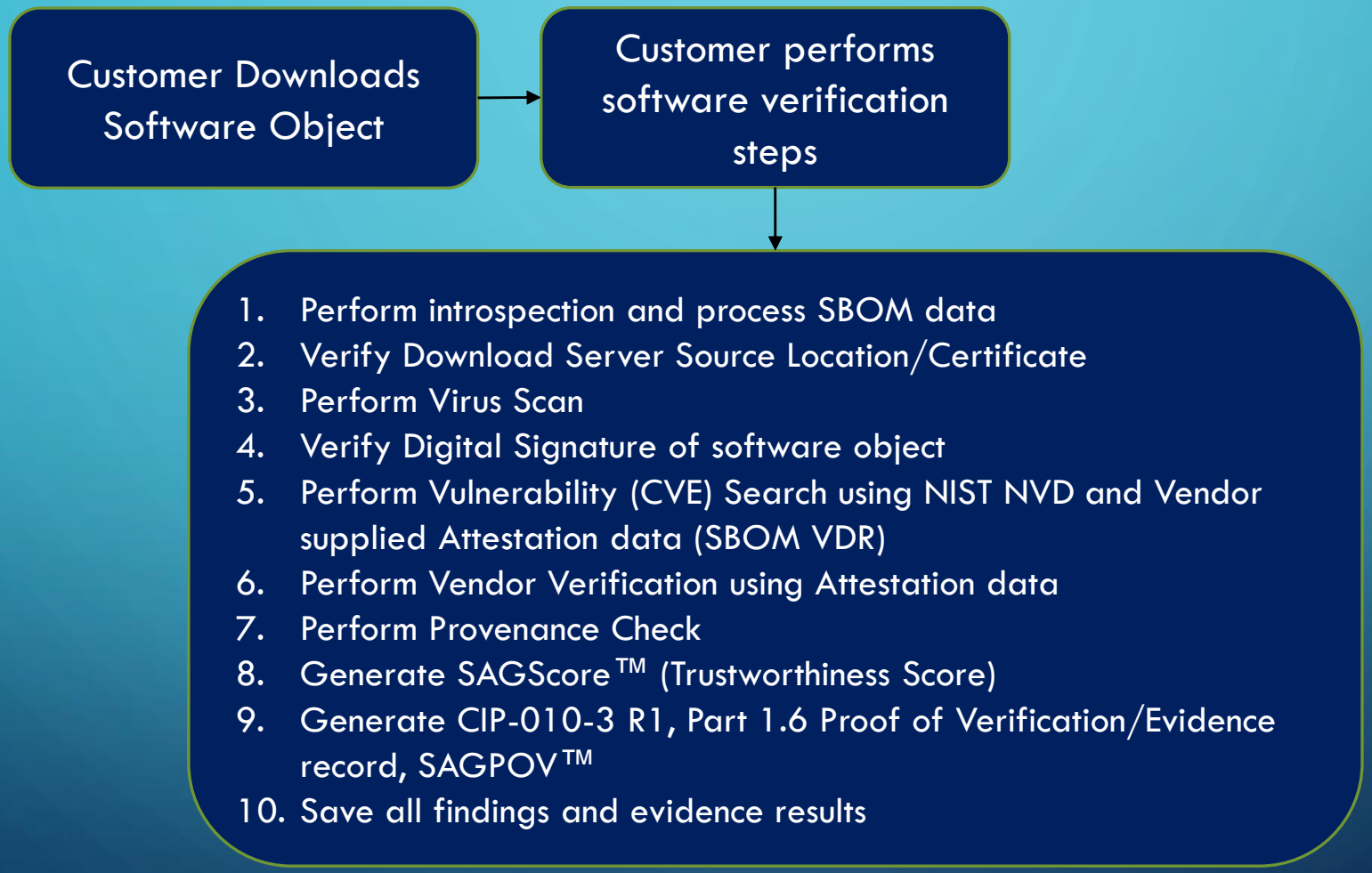
CORROBORATING EVIDENCE IS KEY

- Identify software packages and components (what's in the can)
- Identify and verify software supplier (who created the can)
- Determine risks based on contents (e.g. food recalls)
  - Search for malware and software vulnerabilities
- Determine trustworthiness of identified supplier
- Determine risks based on where software came from/has been
  - Referred to as provenance
- Look for anomalies in the evidence data; red flags

ESTABLISHING TRUSTWORTHINESS: VERIFY



Effective Software Verification Process Flow



PROTECT YOURSELF - SAVE THE EVIDENCE

- Collect and save all evidence data supplied by software vendor
- Save all evidence data from the risk assessment
- Consider saving tamperproof evidence data in a third party repository
- May need to show proof of cybersecurity controls during an audit or litigation

HELP OTHERS – SHARE YOUR TRUST DECLARATION

- After completing a SAG-PM ™ risk assessment the SAG-PM ™ software asks the user if they would like to submit a trust declaration into the SAG Community Trust Registry™, SAG-CTR ™
- If yes, SAG-PM ™ evidence data is submitted to REA for evaluation to include in the set of trusted software objects in the SAG-CTR database. REA serves as the Gatekeeper of the SAG-CTR ™
- The SAG-CTR ™ registry is used to determine trustworthiness, which impacts the final SAGScore ™ of a software object
- SAG-PM queries the SAG-CTR ™ for trusted software objects listed in the registry based on the SHA-256 hash value of a software object
- Software objects matching the hash value listed in the registry are retuned to the end user for examination, as part of a risk-based decision to procure or install a software object
- A separate "Trust inquiry" operation can be used to return a SAGScore for a software object, which may be used on App stores and other repositories, i.e. GitHub, where applications are available for download and installation

SHARE YOUR KNOWLEDGE

- Any identified risks or concerns should be shared with CISA
- Trust declarations for trusted software should be submitted to REA for inclusion in the SAG-CTR ™
- Never trust software, always verify and report! ™

SUMMARY

- Prevent harmful software from getting a foothold in your ecosystem using proactive measures and controls
  - Check each software object for risk before procurement and installation, think of the food recall scenario
- Contain the damaging effects of a cyber breach using reactive measures
- Follow best practices for software supply chain risk assessments provided by the US Government, CISA and NIST
- You cannot outsource the recovery effort and damage to reputation
- Save evidence data proving cybersecurity due diligence you may need this someday