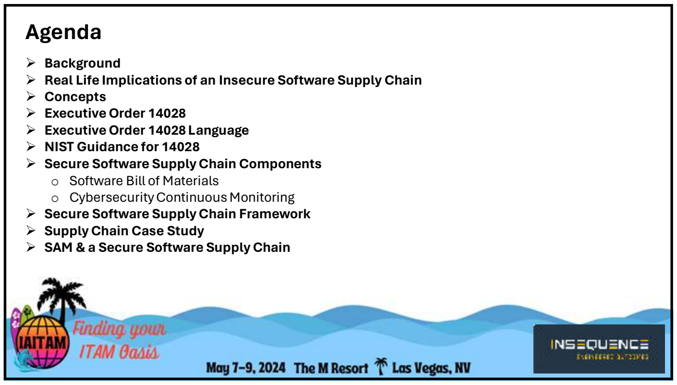
IAITAM ACE
May 7-9, 2024 The M Resort Las Vegas, NV
IAITAM

A Secure Software Supply Chain is Critical to Successful Federal SAM Programs

Andrew Filla
CEO, InSequence
afilla@insequenceinc.com

Finding your IAITAM Oasis

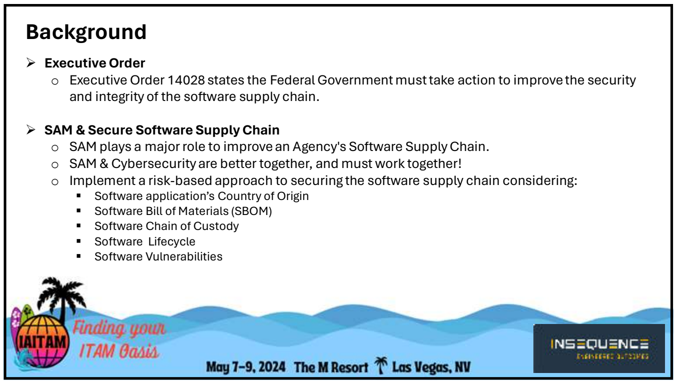
1



Agenda

- Background
- Real Life Implications of an Insecure Software Supply Chain
- Concepts
- Executive Order 14028
- Executive Order 14028 Language
- NIST Guidance for 14028
- Secure Software Supply Chain Components
  - Software Bill of Materials
  - Cybersecurity Continuous Monitoring
- Secure Software Supply Chain Framework
- Supply Chain Case Study
- SAM & a Secure Software Supply Chain

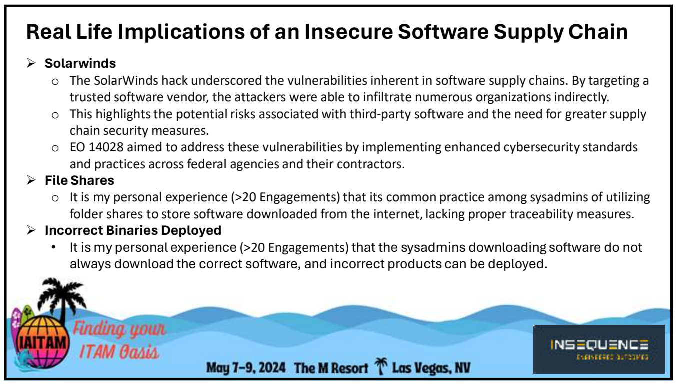
2



Background

- **Executive Order**
  - Executive Order 14028 states the Federal Government must take action to improve the security and integrity of the software supply chain.
- **SAM & Secure Software Supply Chain**
  - SAM plays a major role to improve an Agency's Software Supply Chain.
  - SAM & Cybersecurity are better together, and must work together!
  - Implement a risk-based approach to securing the software supply chain considering:
    - Software application's Country of Origin
    - Software Bill of Materials (SBOM)
    - Software Chain of Custody
    - Software Lifecycle
    - Software Vulnerabilities

3



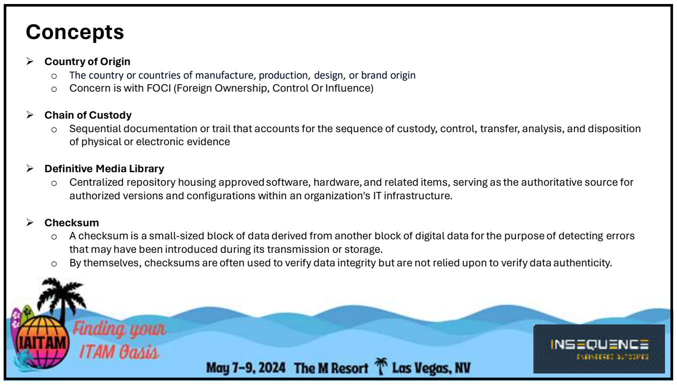
Real Life Implications of an Insecure Software Supply Chain

- **Solarwinds**
  - The SolarWinds hack underscored the vulnerabilities inherent in software supply chains. By targeting a trusted software vendor, the attackers were able to infiltrate numerous organizations indirectly.
  - This highlights the potential risks associated with third-party software and the need for greater supply chain security measures.
  - EO 14028 aimed to address these vulnerabilities by implementing enhanced cybersecurity standards and practices across federal agencies and their contractors.
- **File Shares**
  - It is my personal experience (>20 Engagements) that its common practice among sysadmins of utilizing folder shares to store software downloaded from the internet, lacking proper traceability measures.
- **Incorrect Binaries Deployed**
  - It is my personal experience (>20 Engagements) that the sysadmins downloading software do not always download the correct software, and incorrect products can be deployed.

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

4



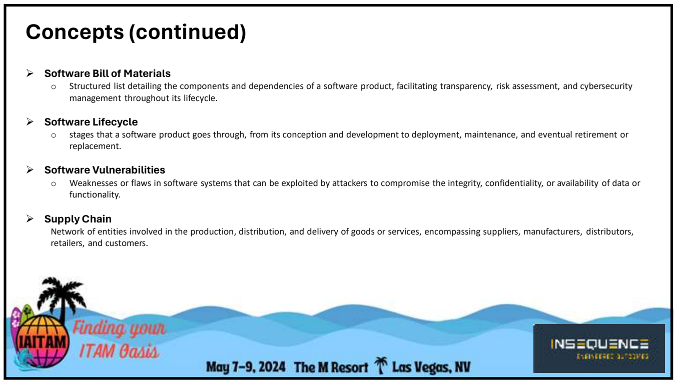
Concepts

- **Country of Origin**
  - The country or countries of manufacture, production, design, or brand origin
  - Concern is with FOCI (Foreign Ownership, Control Or Influence)
- **Chain of Custody**
  - Sequential documentation or trail that accounts for the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence
- **Definitive Media Library**
  - Centralized repository housing approved software, hardware, and related items, serving as the authoritative source for authorized versions and configurations within an organization's IT infrastructure.
- **Checksum**
  - A checksum is a small-sized block of data derived from another block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage.
  - By themselves, checksums are often used to verify data integrity but are not relied upon to verify data authenticity.

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

5



Concepts (continued)

- **Software Bill of Materials**
  - Structured list detailing the components and dependencies of a software product, facilitating transparency, risk assessment, and cybersecurity management throughout its lifecycle.
- **Software Lifecycle**
  - stages that a software product goes through, from its conception and development to deployment, maintenance, and eventual retirement or replacement.
- **Software Vulnerabilities**
  - Weaknesses or flaws in software systems that can be exploited by attackers to compromise the integrity, confidentiality, or availability of data or functionality.
- **Supply Chain**

  Network of entities involved in the production, distribution, and delivery of goods or services, encompassing suppliers, manufacturers, distributors, retailers, and customers.

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

6

Executive Order 14028

- **Executive Order (EO) 14028**
  - Executive Order on Improving the Nation’s Cybersecurity
  - MAY 12, 2021

THE WHITE HOUSE

Executive Order on Improving the Nation’s Cybersecurity

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

  - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

7

Executive Order 14028 Language

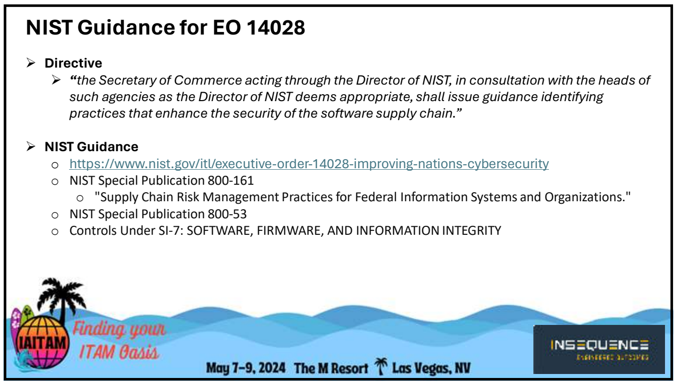
- **Executive Order (EO) 14028**
  - *“The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended.”*
  - *The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices*

8

Executive Order 14028 Language (Continued)

- include standards, procedures, or criteria regarding:
  - (i) secure software development environments, including such actions as:
    - (A) using **administratively separate build environments**;
    - (B) **auditing trust relationships**;
    - (C) establishing **multi-factor, risk-based authentication and conditional access** across the enterprise;
    - (D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
    - (E) employing **encryption for data**; and
    - (F) monitoring operations and alerts and responding to attempted and actual cyber incidents;
  - (ii) generating and, when requested by a purchaser, **providing artifacts that demonstrate conformance** to the processes set forth in subsection (e)(i) of this section;
  - (iii) employing automated tools, or comparable processes, to **maintain trusted source code supply chains**, thereby ensuring the integrity of the code;
  - (iv) employing automated tools, or comparable processes, that **check for known and potential vulnerabilities and remediate them,** which shall operate regularly, or at a minimum prior to product, version, or update release;
  - (v) providing, when requested by a purchaser, **artifacts of the execution of the tools and processes** described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;
  - (vi) maintaining accurate and up-to-date data**, provenance (i.e., origin) of software code or components**, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;
  - (vii) providing a purchaser a **Software Bill of Materials (SBOM)** for each product directly or by publishing it on a public website;
  - (viii) participating in a **vulnerability disclosure program** that includes a reporting and disclosure process;
  - (ix) attesting to conformity with **secure software development practices**; and
  - (x) ensuring and attesting, to the extent practicable, to the **integrity and provenance of open source software used within any portion of a product**.

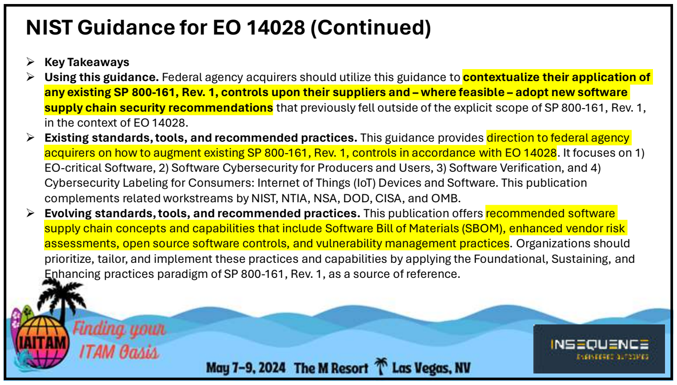
9



NIST Guidance for EO 14028

- **Directive**
  - ***“****the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain.”*
- **NIST Guidance**
  - https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
  - NIST Special Publication 800-161
    - "Supply Chain Risk Management Practices for Federal Information Systems and Organizations."
  - NIST Special Publication 800-53
  - Controls Under SI-7: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

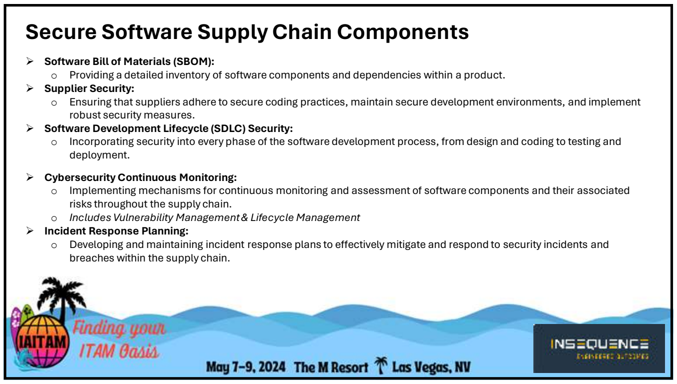
10



NIST Guidance for EO 14028 (Continued)

- **Key Takeaways**
- **Using this guidance.** Federal agency acquirers should utilize this guidance to **contextualize their application of any existing SP 800-161, Rev. 1, controls upon their suppliers and – where feasible – adopt new software supply chain security recommendations** that previously fell outside of the explicit scope of SP 800-161, Rev. 1, in the context of EO 14028.
- **Existing standards, tools, and recommended practices.** This guidance provides direction to federal agency acquirers on how to augment existing SP 800-161, Rev. 1, controls in accordance with EO 14028. It focuses on 1) EO-critical Software, 2) Software Cybersecurity for Producers and Users, 3) Software Verification, and 4) Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software. This publication complements related workstreams by NIST, NTIA, NSA, DOD, CISA, and OMB.
- **Evolving standards, tools, and recommended practices.** This publication offers recommended software supply chain concepts and capabilities that include Software Bill of Materials (SBOM), enhanced vendor risk assessments, open source software controls, and vulnerability management practices. Organizations should prioritize, tailor, and implement these practices and capabilities by applying the Foundational, Sustaining, and Enhancing practices paradigm of SP 800-161, Rev. 1, as a source of reference.

11



Secure Software Supply Chain Components

- **Software Bill of Materials (SBOM):**
  - Providing a detailed inventory of software components and dependencies within a product.
- **Supplier Security:**
  - Ensuring that suppliers adhere to secure coding practices, maintain secure development environments, and implement robust security measures.
- **Software Development Lifecycle (SDLC) Security:**
  - Incorporating security into every phase of the software development process, from design and coding to testing and deployment.
- **Cybersecurity Continuous Monitoring:**
  - Implementing mechanisms for continuous monitoring and assessment of software components and their associated risks throughout the supply chain.
  - *Includes Vulnerability Management & Lifecycle Management*
- **Incident Response Planning:**
  - Developing and maintaining incident response plans to effectively mitigate and respond to security incidents and breaches within the supply chain.

12

Secure Software Supply Chain Components

Artifact Requirements of Your Vendors

- **Software Bill of Materials (SBOM):**
  - Providing a detailed inventory of software components and dependencies within a product.
- **Supplier Security:**
  - Ensuring that suppliers adhere to secure coding practices, maintain secure development environments, and implement robust security measures.
- **Software Development Lifecycle (SDLC) Security:**
  - Incorporating security into every phase of the software development process, from design and coding to testing and deployment.

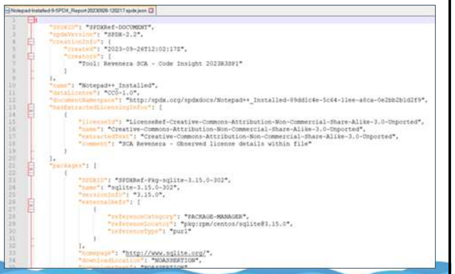
Capabilities Agencies Must Implement

- **Cybersecurity Continuous Monitoring:**
  - Implementing mechanisms for continuous monitoring and assessment of software components and their associated risks throughout the supply chain.
  - *Includes Vulnerability Management & Lifecycle Management*
- **Incident Response Planning:**
  - Developing and maintaining incident response plans to effectively mitigate and respond to security incidents and breaches within the supply chain.

13

Software Bill of Materials

- **Generation**
  - Ideally by Vendor
  - Can be generated later
- **Example**
  - Example: Notepad++
  - .SPDX File Format
  - Generated by Revenera SCA Code Insight



Notepad-Installed-9-SPDX_Report-20230926-120217.spdx.json

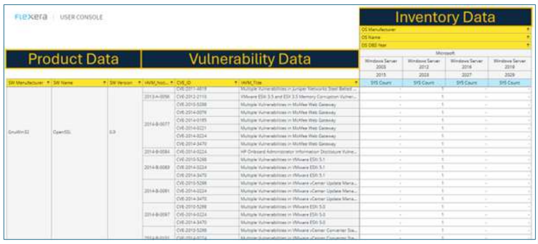
```
{
    "SPDXID": "SPDXRef-DOCUMENT",
    "spdxVersion": "SPDX-2.2",
    "creationInfo": {
        "created": "2023-09-26T12:02:17Z",
        "creators": [
            "Tool: Revenera SCA - Code Insight 2023R3SP1"
        ]
    },
    "name": "Notepad++_Installed",
    "dataLicense": "CC0-1.0",
    "documentNamespace": "http://spdx.org/spdxdocs/Notepad++_Installed-09dd1c4e-5c64-11ee-a8ca-0e2bb2b1d2f9",
    "hasExtractedLicensingInfos": [
        {
            "licenseId": "LicenseRef-Creative-Commons-Attribution-Non-Commercial-Share-Alike-3.0-Unported",
            "name": "Creative-Commons-Attribution-Non-Commercial-Share-Alike-3.0-Unported",
            "extractedText": "Creative-Commons-Attribution-Non-Commercial-Share-Alike-3.0-Unported",
            "comment": "SCA Revenera - Observed license details within file"
        }
    ],
    "packages": [
        {
            "SPDXID": "SPDXRef-Pkg-sqlite-3.15.0-302",
            "name": "sqlite-3.15.0-302",
            "versionInfo": "3.15.0",
            "externalRefs": [
                {
                    "referenceCategory": "PACKAGE-MANAGER",
                    "referenceLocator": "pkg:rpm/centos/sqlite@3.15.0",
                    "referenceType": "purl"
                }
            ],
            "homepage": "http://www.sqlite.org/",
            "downloadLocation": "NOASSERTION",
            "copyrightText": "NOASSERTION"
```

14

Cybersecurity Continuous Monitoring

- **Vulnerability Management**
  - Cyber Data and Asset Data coming together

Asset Mgmt Data
+ Cyber Security Data
Asset Risk Insight



Inventory Data: OS Manufacturer, OS Name, OS DBS Year

Product Data			Vulnerability Data			Inventory Data			
						Microsoft			
						Windows Server 2003	Windows Server 2012	Windows Server 2016	Windows Server 2019
						2015	2023	2027	2029
SW Manufacturer	SW Name	SW Version	IAVM_Noti...	CVE_ID	IAVM_Title	SYS Count	SYS Count	SYS Count	SYS Count
GnuWin32	OpenSSL	0.9		CVE-2011-4819	Multiple Vulnerabilities in Juniper Networks Steel Belted ...	-	1	-	-
			2013-A-0056	CVE-2012-2110	VMware ESX 3.5 and ESXi 3.5 Memory Corruption Vulner...	-	1	-	-
			2014-B-0077	CVE-2010-5298	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
				CVE-2014-0076	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
				CVE-2014-0195	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
				CVE-2014-0221	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
				CVE-2014-0224	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
				CVE-2014-3470	Multiple Vulnerabilities in McAfee Web Gateway	-	1	-	-
			2014-B-0084	CVE-2014-0224	HP Onboard Administrator Information Disclosure Vulne...	-	1	-	-
			2014-B-0083	CVE-2010-5298	Multiple Vulnerabilities in VMware ESXi 5.1	-	1	-	-
				CVE-2014-0224	Multiple Vulnerabilities in VMware ESXi 5.1	-	1	-	-
				CVE-2014-3470	Multiple Vulnerabilities in VMware ESXi 5.1	-	1	-	-
			2014-B-0081	CVE-2010-5298	Multiple Vulnerabilities in VMware vCenter Update Mana...	-	1	-	-
				CVE-2014-0224	Multiple Vulnerabilities in VMware vCenter Update Mana...	-	1	-	-
				CVE-2014-3470	Multiple Vulnerabilities in VMware vCenter Update Mana...	-	1	-	-
			2014-B-0087	CVE-2010-5298	Multiple Vulnerabilities in VMware ESXi 5.0	-	1	-	-
				CVE-2014-0224	Multiple Vulnerabilities in VMware ESXi 5.0	-	1	-	-
				CVE-2014-3470	Multiple Vulnerabilities in VMware ESXi 5.0	-	1	-	-
				CVE-2010-5298	Multiple Vulnerabilities in VMware vCenter Converter Sta...	-	1	-	-
			[illegible]	CVE-2014-0224	Multiple Vulnerabilities in VMware vCenter Converter Sta...	-	1	-	-

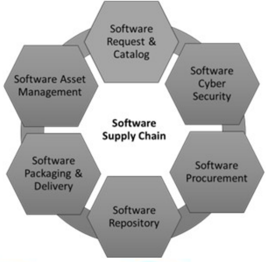
15

Cybersecurity Continuous Monitoring

- **Lifecycle Management**
  - End of Life
  - End of Service
  - Version Depth

16

Secure Software Supply Chain Framework



Software Supply Chain

Software Request & Catalog

Software Cyber Security

Software Procurement

Software Repository

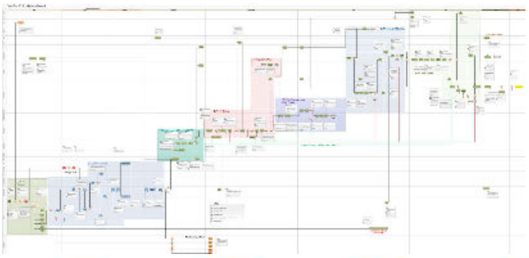
Software Packaging & Delivery

Software Asset Management

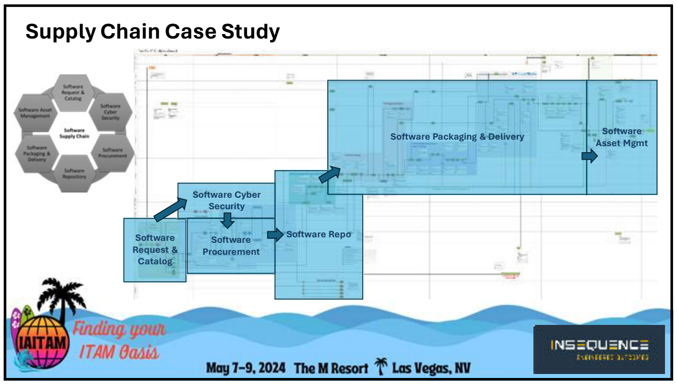
17

Supply Chain Case Study

- **Request > Retirement**
- **67 Steps**
- **6 Systems of Record**
- **6 Disciplines**



18



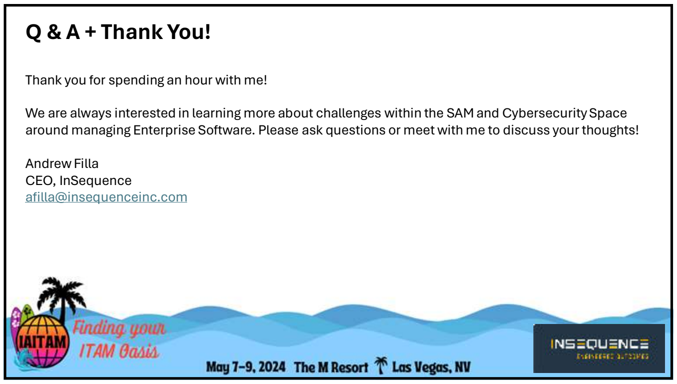
Supply Chain Case Study

19

SAM & a Secure Software Supply Chain

- SAM plays a major role to improve an Agency's Software Supply Chain.
  - Like it or not, SAM and Cybersecurity play in similar space and can help each other!
  - SAM and Cybersecurity must work together within:
    - Vendor Management
      - Define and Manage Definitive Media Libraries (Software Repositories)
      - Mandate Vendors to Provide Software Bill of Materials (SBOM)
      - Track and Managed Software Bill of Materials (SBOM)
      - Evaluate & Track Software application's country of origin
      - Evaluate & Track Vendor Development Practices
    - Internal Controls
      - Track Chain of Custody of Software Binaries
      - Provide Continuous Visibility into Software Lifecycle
      - Provide Continuous Visibility into Software Vulnerabilities
- Strong Relationships w/ Cyber Help SAM
  - Inventory Data, Gap Analysis, Policy Enforcement

20



Q & A + Thank You!

Thank you for spending an hour with me!

We are always interested in learning more about challenges within the SAM and Cybersecurity Space around managing Enterprise Software. Please ask questions or meet with me to discuss your thoughts!

Andrew Filla
CEO, InSequence
afilla@insequenceinc.com

IAITAM
Finding your ITAM Oasis
May 7-9, 2024 The M Resort Las Vegas, NV
INSEQUENCE

21