Supply Chain Cybersecurity Risk Management

Sunny Jamwal
Director of CyberSecurity, **Dash Hudson**

The Basics

Supply Chain

“A supply chain is a linked set of resources and processes beginning at the origin of the product or service and ending at the consumer. A supply chain can be very complex. Everything from the food we eat, our medical and transportation systems, and our access to the internet rely on a supply chain.” **- NIST**

Supply Chain Risk

Risk that a malicious entity may disrupt the supply chain by introducing something malicious during;

- Design
- Manufacturing
- Production
- Distribution
- Installation
- Operation
- Maintenance

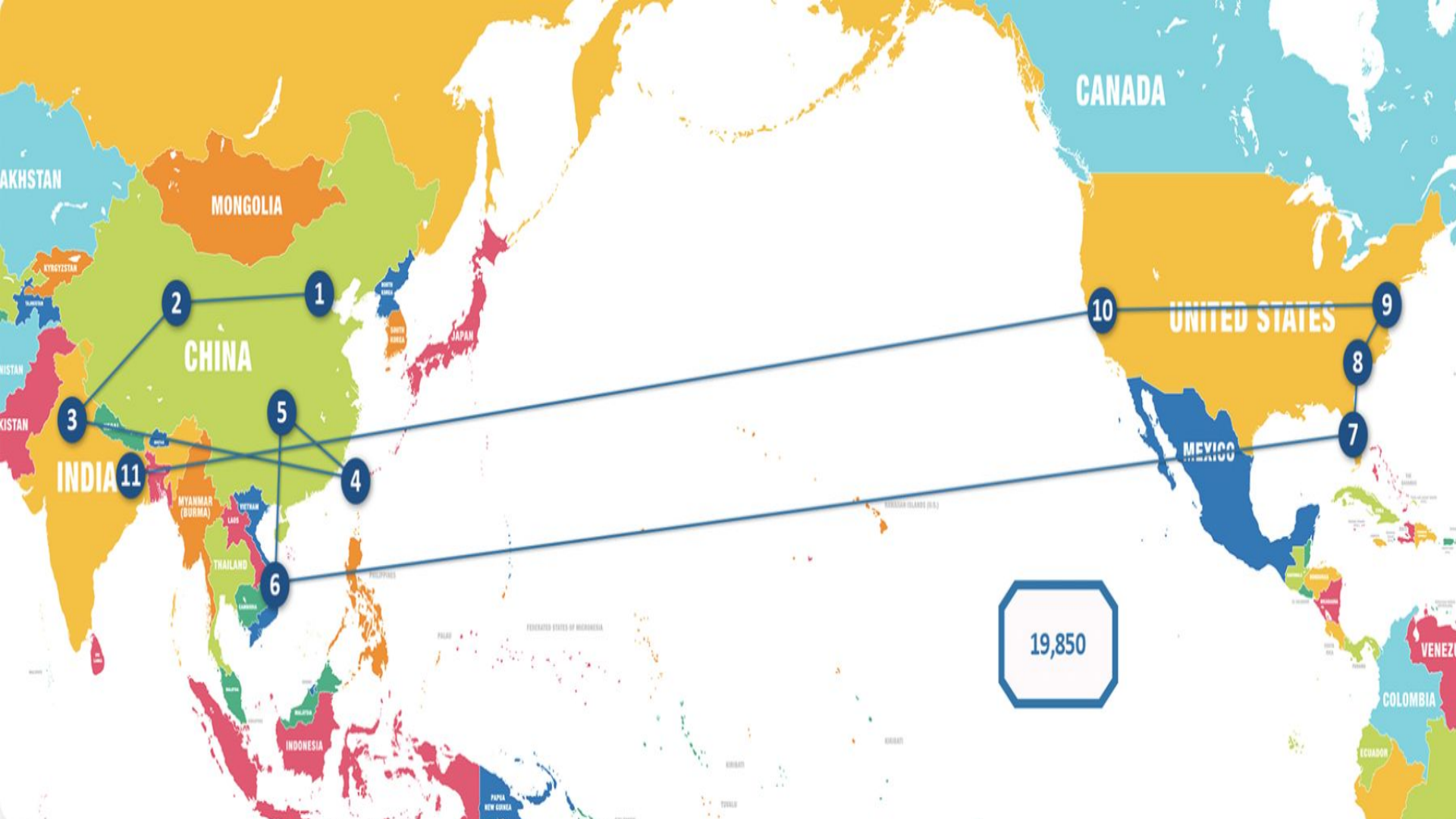
The Basics

Supply Chain Risk Management

“Supply Chain Risk Management (SCRM) involves monitoring all parts of a supply chain for vulnerabilities, disruptions of or lack of access to parts, and managing a wide variety of risks.” - **NIST**

Cyber Supply Risk Management

“Cyber Supply Chain Risk Management (C-SCRM) is the monitoring of a supply chain for an Information and Communication technology (ICT) product or service for any vulnerability that could introduce a risk to the end user of the product or service.” - **NIST**


CANADA
MONGOLIA
CHINA
JAPAN
UNITED STATES
MEXICO
INDIA
MYANMAR (BURMA)
THAILAND
INDONESIA
COLOMBIA
1
2
3
4
5
6
7
8
9
10
11
19,850

1. DESIGN

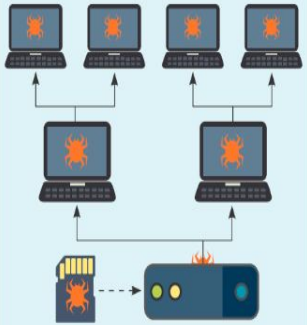
Vulnerabilities introduced during Design are often unintentional and can potentially affect all users of the components. Malicious actors could integrate vulnerabilities into components that may be installed in millions of pieces of equipment.

HIJACKED CELLULAR DEVICES

2016—A foreign company designed firmware used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

2. DEVELOPMENT AND PRODUCTION

Vulnerabilities introduced during this phase are often inadvertent and can be costly to fix if not identified when testing initial prototypes. Well-designed products may still have malicious components introduced during manufacturing and assembly in a way that is potentially difficult to identify.



INFECTED SWITCH FLASH CARDS

2012—A third party factory that produced switches designed by a U.S. company installed infected compact flash cards during production. The U.S. company warned that using an infected component could compromise the system and potentially spread the malware within the network.

3. DISTRIBUTION

Components transported between production facilities and customers often do not fall under the purview of the personnel responsible for their design or production. Vulnerabilities introduced during Distribution are likely to be malicious and affect a limited number of components and customers compared to earlier phases.

END USER DEVICE MALWARE

2012—Researchers from a major U.S. software company investigating counterfeit software found malware pre-installed on 20% of devices they tested. The malware was installed in new desktops and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.

4. ACQUISITION AND DEPLOYMENT

Malicious insiders may insert vulnerabilities or replace equipment with vulnerable components during acquisition or installation. Vulnerabilities introduced during this phase likely affect only a limited number of customers.

COUNTERFEITS SOLD TO U.S. NAVY

2015—A U.S. citizen imported thousands of counterfeit integrated circuits from China and Hong Kong, and resold them to U.S. customers, including Defense contractors supplying them to the U.S. Navy for use in nuclear submarines.

5. MAINTENANCE

ICT components receiving Maintenance are susceptible to vulnerabilities introduced through physical or network access, and from exploitation of previously unknown or unpatched vulnerabilities. Vulnerabilities introduced during Maintenance might be targeted against specific entities, but can affect many customers in the case of software updates.

MALWARE EMBEDDED WITHIN SOFTWARE SECURITY TOOL

2017—Malicious actors attacked a security software company by infiltrating its network and inserting code into security software. Installs and updates to the application landed in millions of personal computers. The attack targeted predominant IT company networks.

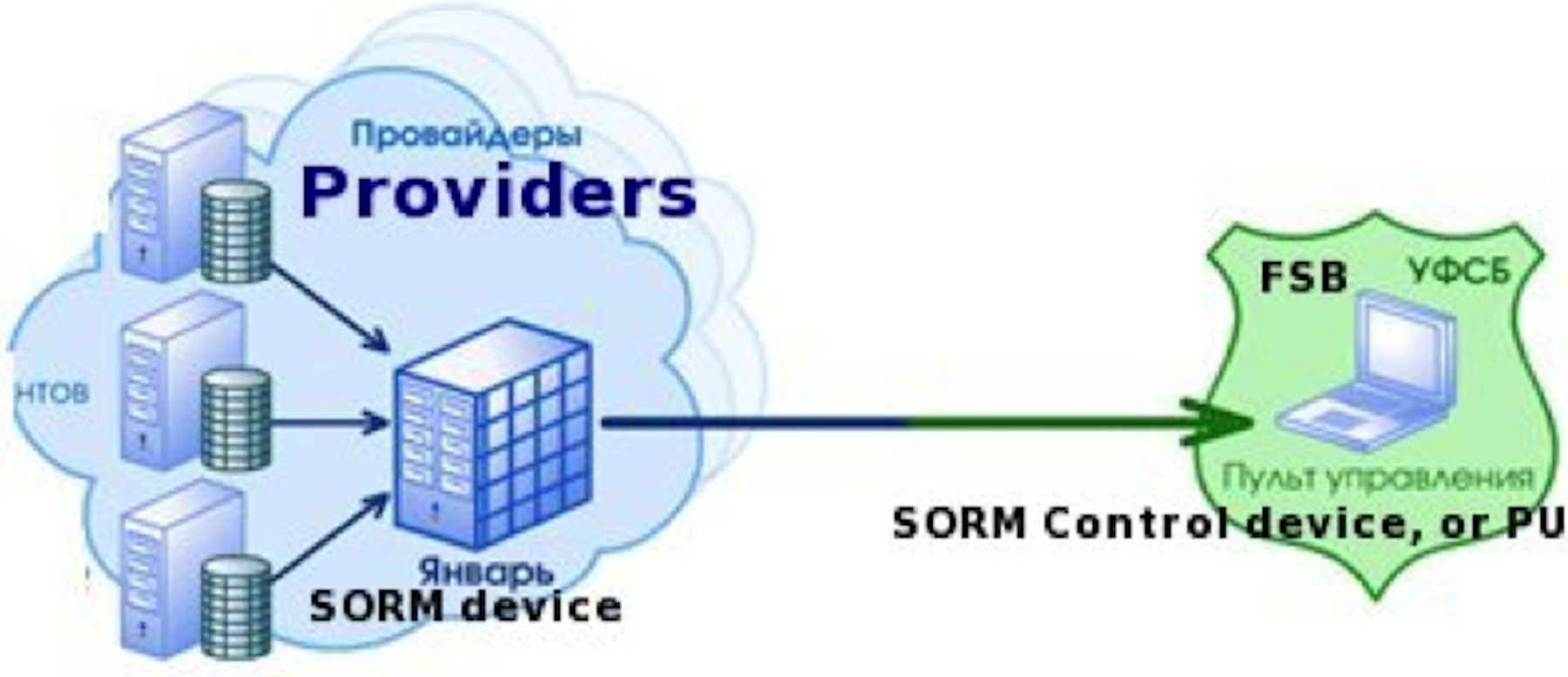
6. DISPOSAL

ICT components that are improperly disposed of can contain sensitive company or customer data. Malicious actors can also attempt to refurbish components and try to resell them as new. Used parts may be less reliable and prone to failure, or have malware installed.

SENSITIVE FEDERAL DATA LOSS

2010—An internal audit discovered that a federal agency was selling computers containing proprietary information. Certain devices failed sanitation verification tests and resulted in the release of sensitive federal agency data.


INN BANK
LAS VEGAS

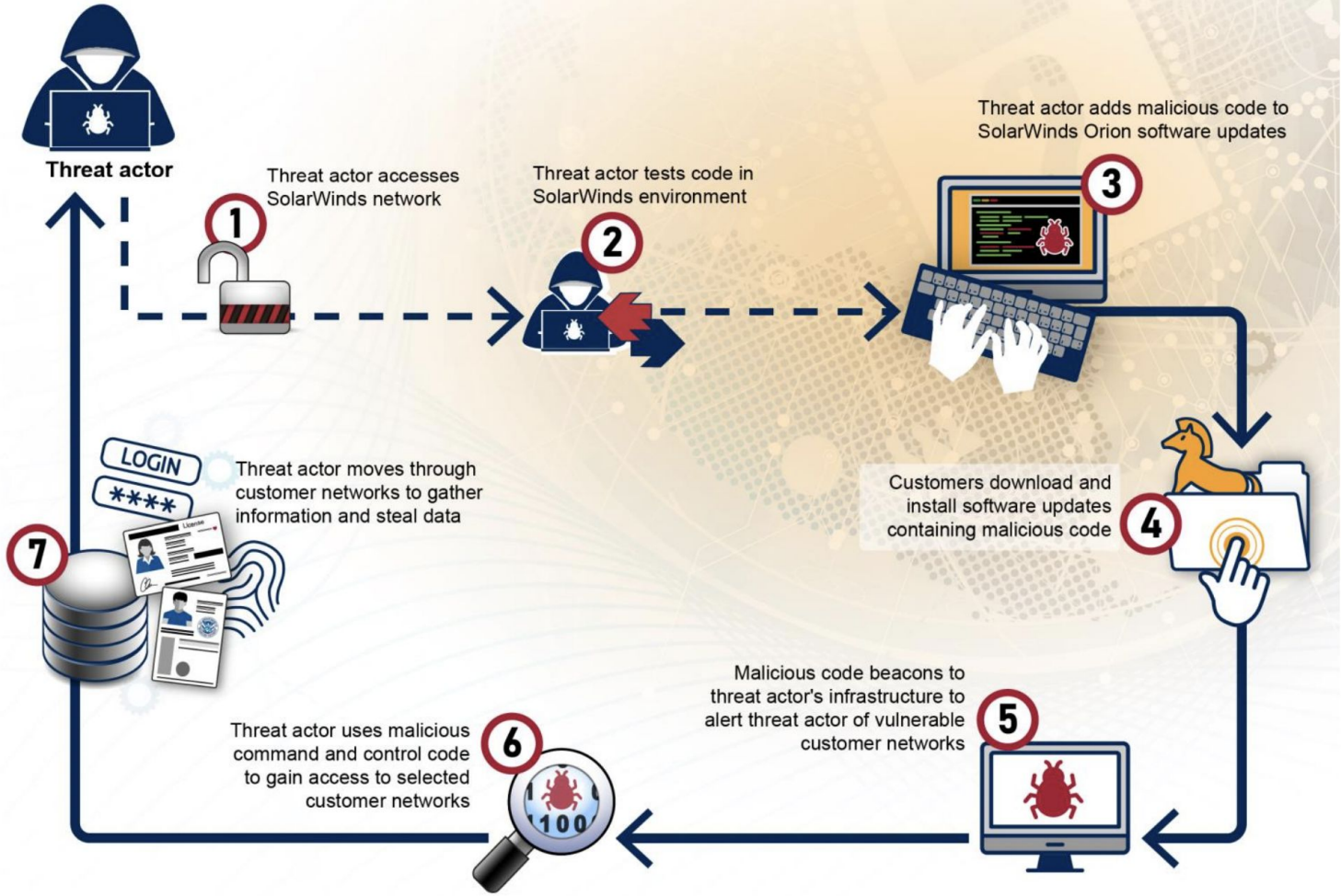

Провайдеры
Providers
НТОВ
Январь
SORM device
FSB
УФСБ
Пульт управления
SORM Control device, or PU

Threat Actor Accesses SolarWinds

- September 4, 2019: unknown attackers access SolarWinds.

- September 12, 2019: The attackers use a sophisticated injection source to insert the SUNBURST malicious code into the company's Orion Platform software.

- February 20, 2020: Hackers compile and deploy the SUNBURST attack. This is an updated variant of the malicious code inserted into the Orion Platform released from February 20, 2020, and beyond.


Threat actor
Threat actor accesses SolarWinds network
1
Threat actor tests code in SolarWinds environment
2
Threat actor adds malicious code to SolarWinds Orion software updates
3
Customers download and install software updates containing malicious code
4
Malicious code beacons to threat actor's infrastructure to alert threat actor of vulnerable customer networks
5
Threat actor uses malicious command and control code to gain access to selected customer networks
6
100
Threat actor moves through customer networks to gather information and steal data
7
LOGIN
****


THE DEPARTMENT OF THE TREASURY
1789


U.S. DEPARTMENT OF HOMELAND SECURITY


CROWDSTRIKE


solarwinds

In Germany, the head of the cybersecurity agency fired for its links with a company suspected of being close to Russia

The company in question would have had contacts with Russian intelligence circles.

The World with AFP

Posted today at 12:40 p.m., updated at 2:37 p.m. • Reading 1 min.

Tesla employee bribed with US$1 million helps FBI arrest Russian hackers

The hackers' scheme to hold Tesla's private data for ransom was exposed by their contact, who even wore a wire to help catch the criminals

David Booth
Aug 27, 2020 • May 20, 2021 • 2 minute read • Join the conversation

C-SCRM Frameworks

- **CISA** - Information and communications technology supply chain risk management.
- **CISA** -*Vendor supply chain risk management (SCRM) Template*
- **NIST** - *NIST SP 800-161r*
- **Canada** - *Cyber supply chain: An approach to assessing risk - ITSAP.10.070*
- **UK** - *Supply chain security guidance*

UK National Cyber Security centre

Principal of Supply Chain Security

Understand the Risk

1/12 Understand what needs to be protected and Why.

2/12 Know who your Supplier are and build an understanding of their security measures.

3/12 Understand the Risk posed by your Supply chain.

Establish Control

4/12 Communicate your view of Security needs to your supplier.

5/12 Set and communicate minimum security requirements for your supplier.

6/12 Build security requirements into your contracting process and require your supplier to do the same.

7/12 Meet your own security requirements as consumer and supplier

8/12 Raise awareness of security within your supply chain

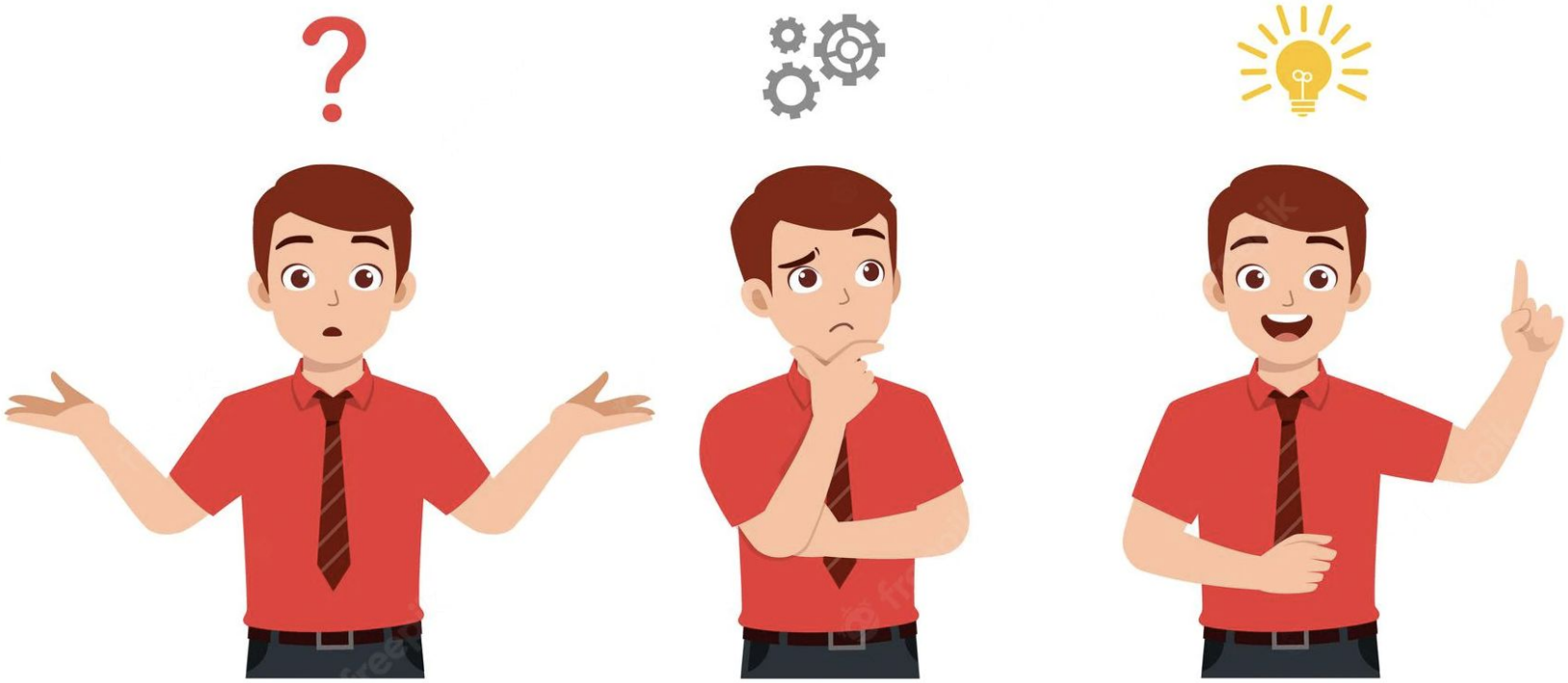
Check Your Arrangements

10/12 Build assurance activities into your supply chain management

Seek Continuous Improvement

11/12 Encourage continuous improvement of security within the supply chain.

12/12 Build trust with suppliers.



Build Cyber Supply Chain Risk Management Program

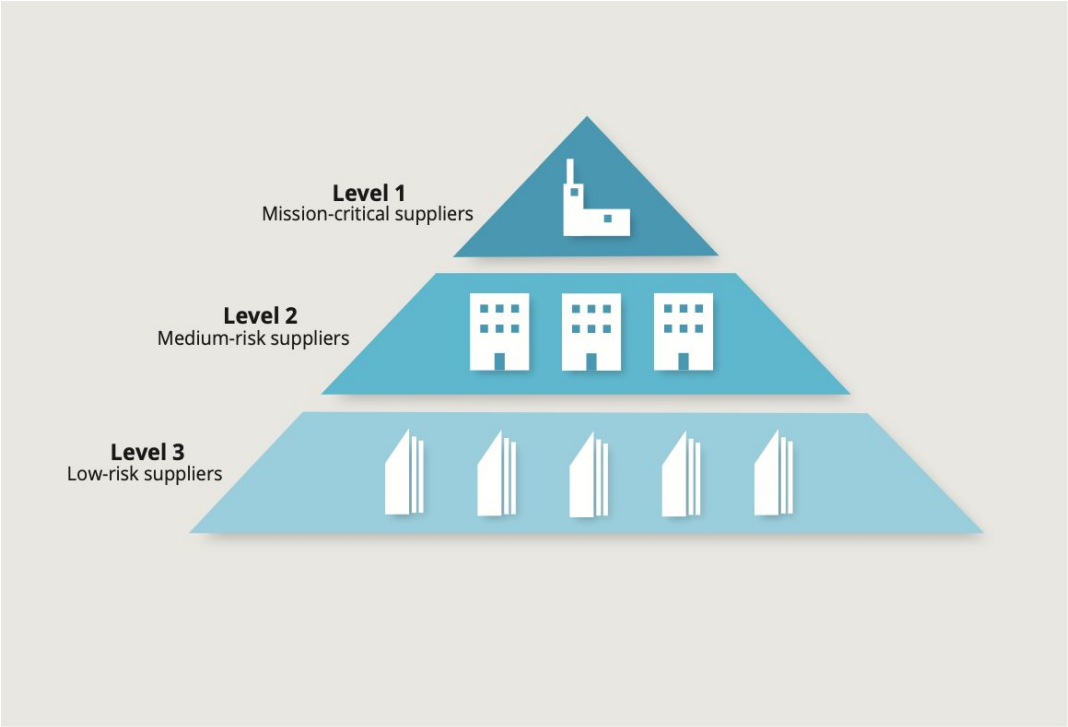
Step 1: Categorize Vendors based on business

- ***Service/Software Provider***
- ***Third Party Libraries***

Step 2: Categorize Vendors based on criticality to the business

- ***Type of Data***
- ***Criticality to the business***
- ***Operational environment***

*****Essentially set up the Context*****



Build Cyber Supply Chain Risk Management Program

Perform Risk assessment

Evaluate and Review

1. Team Structure.
2. Security Policies.
3. Endpoint protection solution.
4. Identity and Access Management solution.
5. External/Internal Audit and Compliance reports.
6. Penetration test reports.
7. Data lifecycle management;
8. External Vendors.

Build Cyber Supply Chain Risk Management Program

Perform Risk assessment

Report Structure

1. <Vendor Name> - Vendor Risk and Compliance Assessment
2. Scope of Service(s)
3. Observations
4. Recommendations
5. Business Owner
6. Conclusion
7. Vendor Profile

Build Cyber Supply Chain Risk Management Program

Monitor the Vendors

- **Key Metrics to monitor:**
  - **Incident response times**
  - **Patching cycles**
  - **Maintenance schedules.**

- **Regular validation**
  - **Internal or external audits,**
  - **Self-assessment using questionnaires**

- **The results of testing and validation should input into the supplier performance plan as well as guiding further investment in the organisation’s cyber security programme.**

Build Cyber Supply Chain Risk Management Program

Maintain

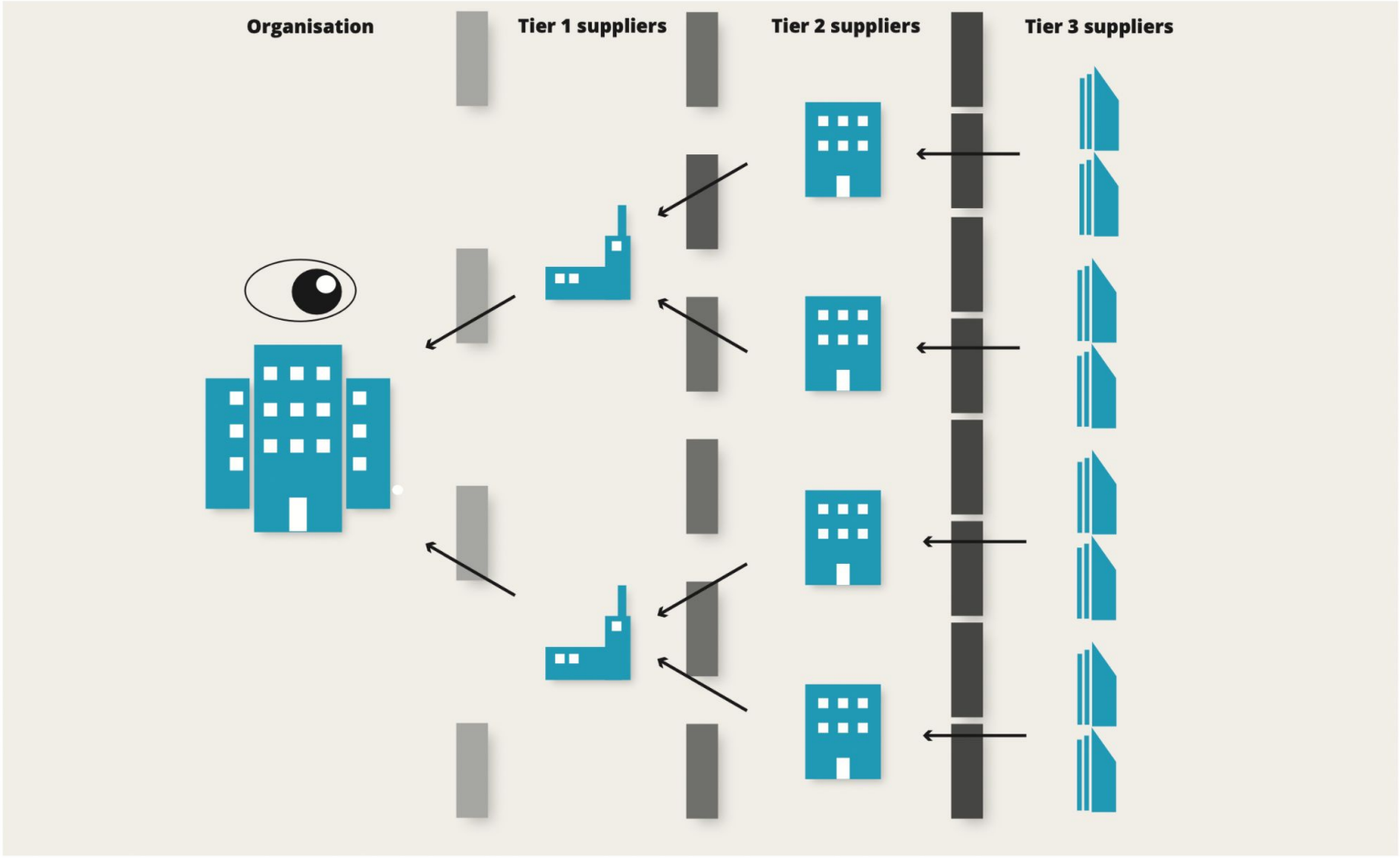
- **Schedule periodic reviews.**
- **Maintain and update Supplier registers.**
- **Ensure the register is updated when changes occur.**
- **Regularly review the criticality status of each supplier.**
- **Keep a schedule for conducting regular security reviews of your supplier.**
- **Record any status changes or deviations from their contractual obligations.**
- **Reviews should ideally be overseen by a group of stakeholders within your organisation.**

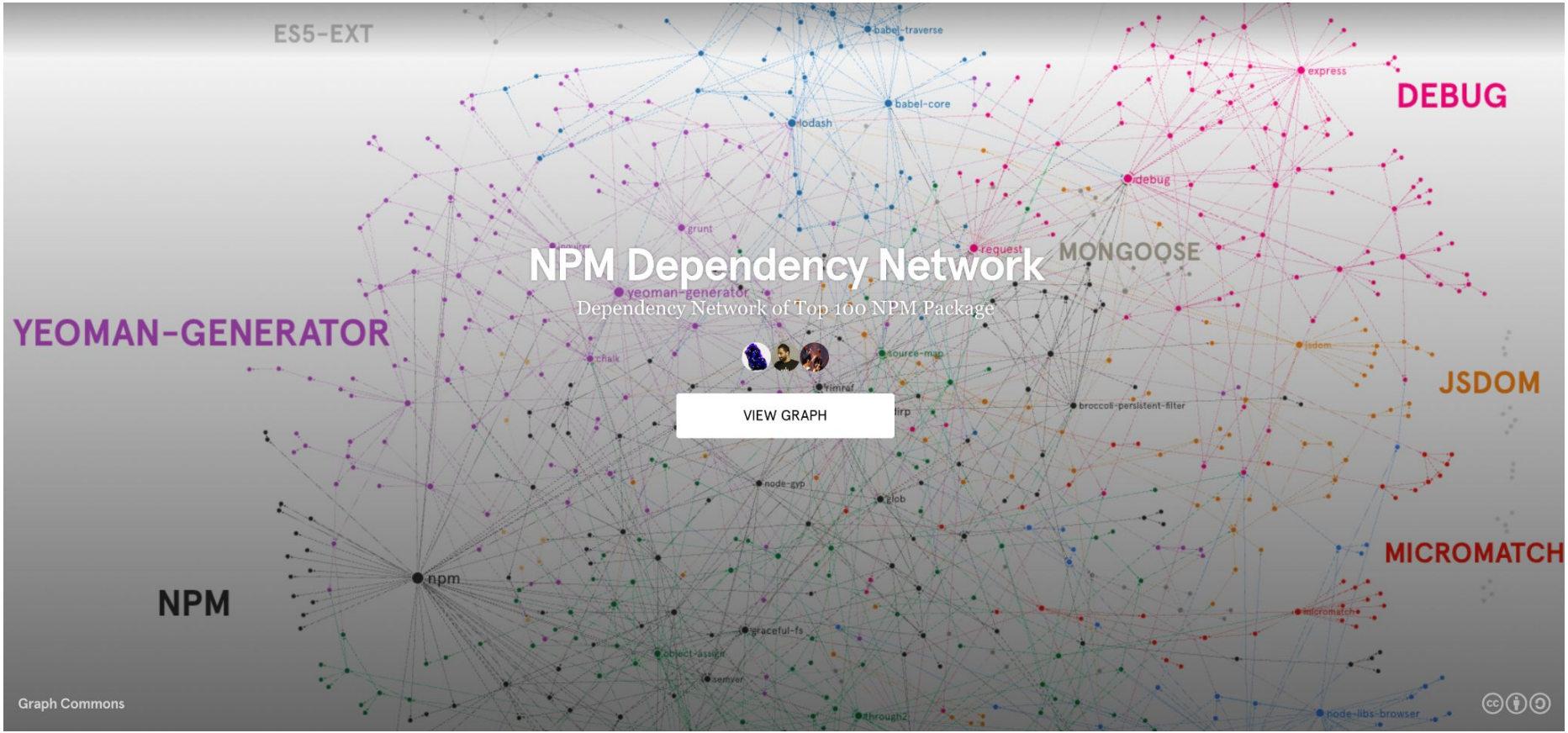
Build Cyber Supply Chain Risk Management Program

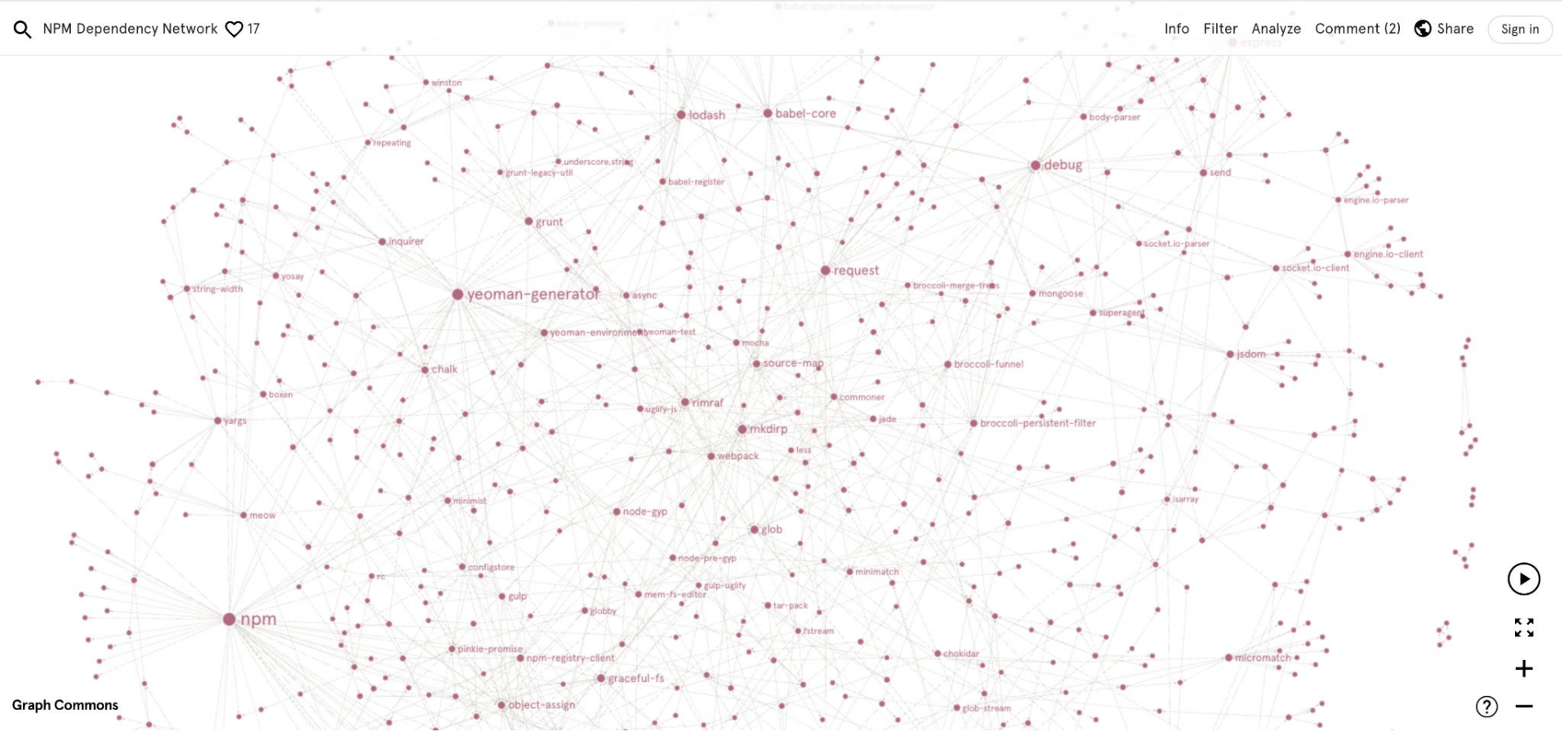
Maintain

- **Encourage a flow of security information between you and your suppliers, and view supply chain security as a mutual concern.**
- **Communicate regularly with your suppliers on security issues, such as emerging cyber risks. Consider utilising technology solutions that streamline collaboration without elevating risk.**
- **Be open to receiving feedback from suppliers about your own security. Be willing to address any legitimate concerns they have about your security procedures.**

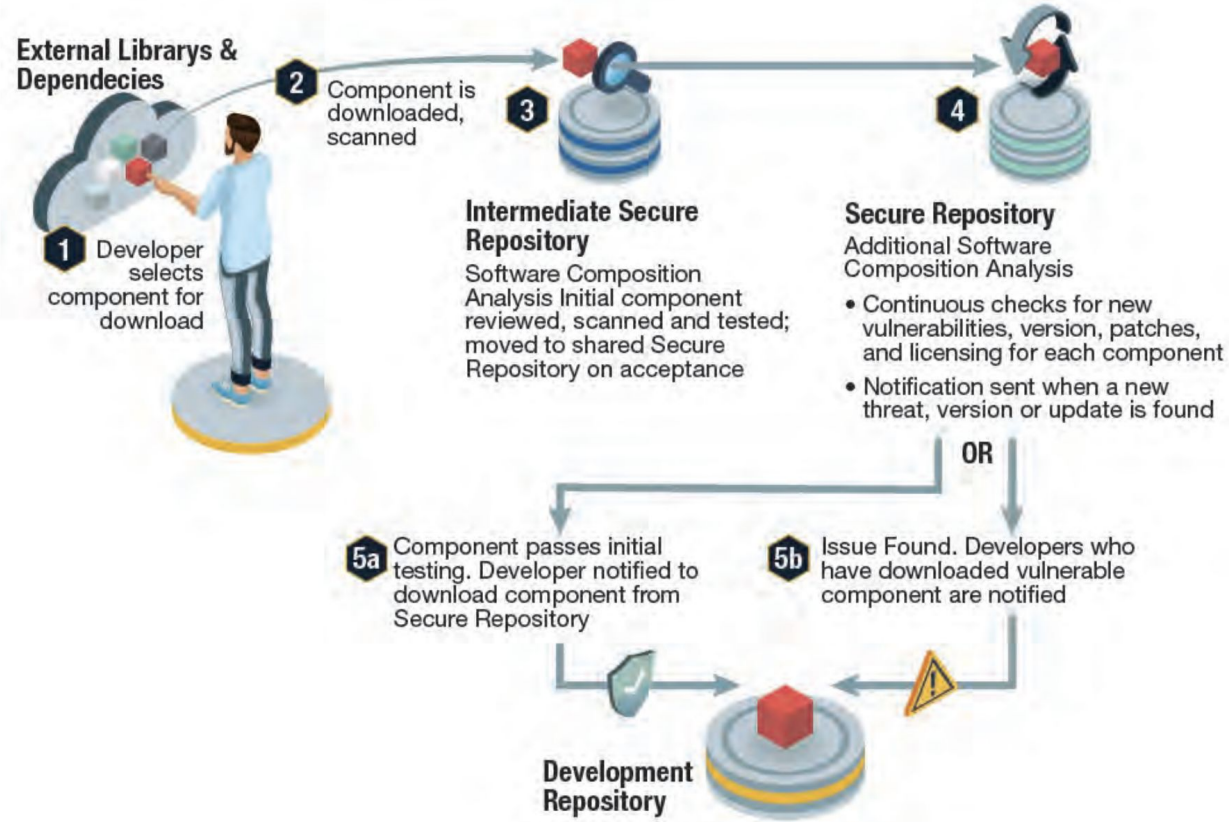
Supply chain visibility barriers




ES5-EXT
babel-traverse
express
DEBUG
babel-core
lodash
debug
grunt
request
MONGOOSE
NPM Dependency Network
yeoman-generator
Dependency Network of Top 100 NPM Package
YEOMAN-GENERATOR
source-map
jsdom
JSDOM
rimraf
VIEW GRAPH
broccoli-persistent-filter
node-gyp
glob
MICROMATCH
npm
NPM
micromatch
graceful-fs
object-assign
semver
through2
node-libs-browser
Graph Commons

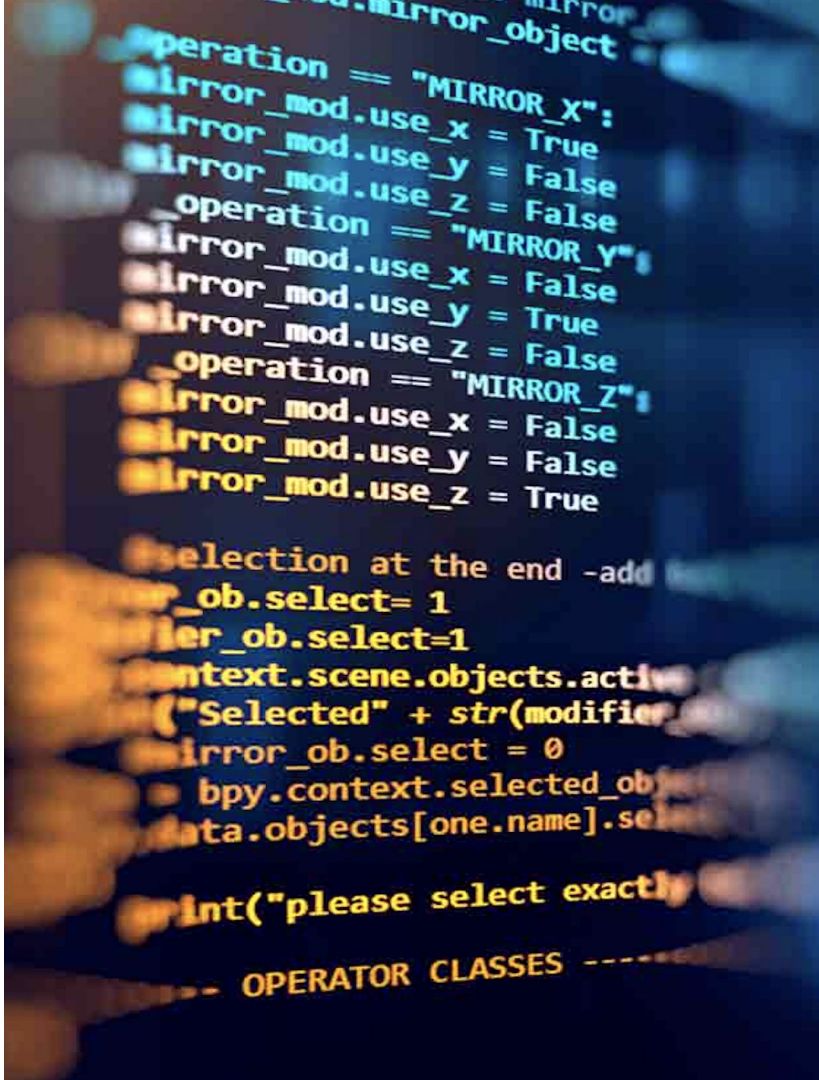

winston
lodash
babel-core
body-parser
repeating
underscore.string
grunt-legacy-util
babel-register
debug
send
engine.io-parser
grunt
inquirer
socket.io-parser
engine.io-client
request
socket.io-client
yosay
string-width
yeoman-generator
async
broccoli-merge-trees
mongoose
superagent
yeoman-environment
yeoman-test
mocha
jsdom
source-map
broccoli-funnel
chalk
boxen
rimraf
commoner
uglify-js
jade
yargs
mkdirp
broccoli-persistent-filter
less
webpack
minimist
isarray
meow
node-gyp
glob
node-pre-gyp
configstore
rc
minimatch
gulp-uglify
gulp
mem-fs-editor
tar-pack
globby
npm
fstream
pinkie-promise
chokidar
micromatch
npm-registry-client
graceful-fs
object-assign
glob-stream

Build Cyber Supply Chain Risk Management Program



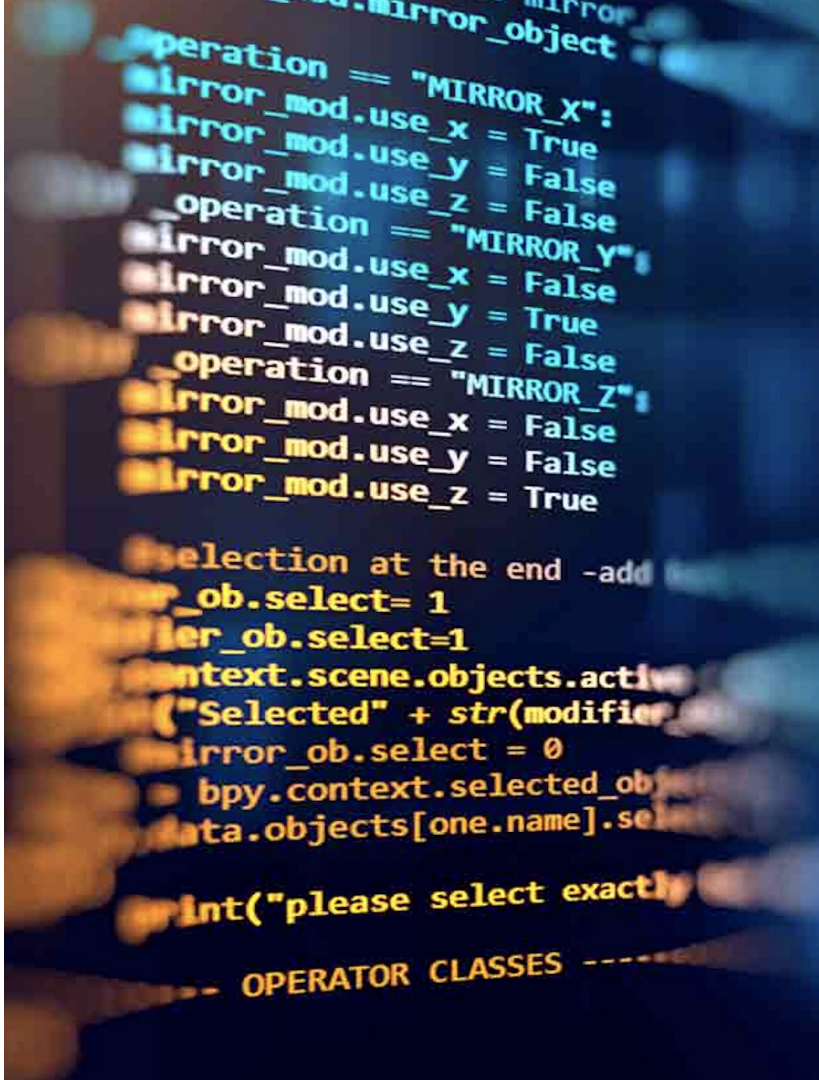
Build Cyber Supply Chain Risk Management Program

- **Track all third-party components you use directly and all internal components in a secure and persistent repository**
- **Implement an open source review board to approve third-party libraries included in a product and audit approved third party libraries for version adherence and vulnerabilities.**
- **Remove or mitigate critical known vulnerabilities or end of life issues of third party components before each release.**
- **Use a known and trusted supplier that has a proven record for secure coding practices and quality delivery of their components.**
- **Monitor and approve of all IDEs and third-party development/debugging extensions to ensure their adoption does not weaken the security posture of the local development environment.**



Build Cyber Supply Chain Risk Management Program

- **Have a trusted repository to support ongoing software composition analysis and security testing for all external and downloaded modules.**
- **Perform binary composition analysis of the final package.**
- **Have a Software Bill of Materials (SBOM) that satisfies the contracts.**



C-SCRM Program Benefits:

- Help enterprises understand which critical assets are most susceptible to supply chain weaknesses and vulnerabilities.
- Enhances an enterprise’s ability to effectively detect, respond, and recover from events that result in significant business disruptions should a supply chain compromise occur.
- Greater assurance that acquired products are of high quality, authentic, reliable, resilient, maintainable, secure, and safe.
- Greater assurance that suppliers, service providers, and the technology products and services that they provide are trustworthy and can be relied upon to meet performance requirements.

Thanks

https://www.linkedin.com/in/sunny-jamwal-058a65236/

https://twitter.com/browninfosecguy

Resources

ACSC: Cyber Supply Chain Guidance

https://www.cyber.gov.au/acsc/government/cyber-supply-chain- guidance

CISA: ICT Supply Chain Risk Management

https://www.cisa.gov/supply-chain

CISA: Supply Chain Risk Management Fact Sheet

https://www.cisa.gov/publication/ict-scrm-fact-sheet

Centre for the Protection of National Infrastructure: Supply Chain Guidance

https://www.cpni.gov.uk/supply-chain

NCSC (UK): Supply Chain Security Guidance

https://www.ncsc.gov.uk/collection/supply-chain-security

NZISM: Supply Chain Security
https://www.nzism.gcsb.govt.nz/ism-document#3574