Secure Acquisition Case Study 4: Supplier Capability Evaluation

Dan Shoemaker, University of Detroit Mercy

April 2021

Secure Acquisition Case Study 4: Supplier Capability Evaluation

Background

Systems are built out of components that are integrated from the lowest level of a supply chain up to a finished product. This creates a serious weakness in that malicious code, or counterfeit parts can be inserted at the bottom of the process without scrutiny and then integrated up into the end-product, as was demonstrated by the recent SolarWinds hack.

The possibility of such a thing occurring is so obvious that you would think that there have been practical efforts to address it. However, even though we've expended much time and effort to ensure robust, efficient and defect free code, we have done very little to ensure against compromises that could occur during the integration process. Thus, the aim of this project is to help the student understand the stages involved in establishing supply chain capability, as well as present a sample solution.

Case Study Overview

There are three communities of practice in the supply chain, the acquirers/customers, suppliers and integrators. Each one of these roles has different sets of responsibilities within the supply chain structure. In order to ensure a successful supply chain process, a clear line of communication must be established. The acquirer is the customer/entity in which the product is provided to. The supplier provides a product to a customer under a provision or a contract. The integrator receive parts from sub-contractors and integrate them into larger products that can then be passed up the supply chain to the next level.

The main challenge here is understanding how each of these roles communicate with each other to ensure the product that is being developed can be assembled/compiled and function as expected with no security flaws. In order to mitigate this, the acquisition managers work with suppliers and integrators to establish a line of communication up and down the supply chain. This allows the managers to track performance of the suppliers and their adherence to the requirements. Therefore, once the student has determined the capability maturity of their organization with respect to the requirements of NIST 800-161. It is time to make a concrete plan to achieve the requisite level of capability for the supply chain.

Student Instructions

Once you have determined the capability maturity of your organization with respect to the requirements of NIST 800-161, it is time to make a concrete plan to achieve the requisite level of capability for each community of practice within the supply chain.

So, using the Case, please provide a complete set of steps that you feel would be necessary to achieve level three (Managed) for each of the standard requirements of one of the principles in NIST 800-161. Ensure that the actions you specify will provide auditable evidence of achievement of the four necessary common features for each element.

The final product will be an action plan for achieving standard compliance with the Managed capability level. You must provide a complete plan as well as the outcome of the assessment (score). Maturity levels will be assessed using the scale provided across the top of the

instrument. For each practice please rate its execution as: Not Done Performed, Managed, Predictable, and Optimizing. The various common features of each capability level will help guide your decision in placing your response.

Incomplete: The Incomplete level has no common features. There is general failure to perform the base practices. There are no easily identifiable work products or outputs of the practice.

Performed: Base practices of the process are generally performed. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed when required. The performance of these base practices is ad-hoc and is not rigorously planned or tracked. Performance depends on individual knowledge and effort. There are identifiable work products for the process Work testify to the performance of the practice.

Managed: The performance of the process is planned and tracked and executed systematically within the organization. Base practices are performed according to a well-defined process using approved methods which are tailored versions of standard, documented processes.

Predictable: Execution of the process is fully reliable because detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed. The quality of work products is quantitatively known.

Optimizing: Quantitative process effectiveness and efficiency goals (targets) for performance are established, based on the business goals and system assurance case of the organization. Continuous process improvement against these goals is enforced by quantitative data that is obtained from the execution of the defined processes as well as from piloting innovative ideas and technologies.

Instructor notes

This is an individual assignment done during a live-lab session. The process steps are taken a step at a time as guided by the instructor. This is done in-class as a first of four lab projects done over the semester to illustrate an explicit process for risk mitigation in supply chains using NIST 800-161

Example solution

Acquirer –Programmatic Activities

Establish unique identification of roles …
Who: WBYT project manager/team.
When: Initiation of project and after any and all changes to process
Where: Within their own process and down the supply chain
What: establish and document the standards by which entities within supply chain are required to conduct business, including identifying roles, organizations, personnel, etc.

Require that unique identifiers and methods of identification be difficult or impossible to alter and that any alterations adhere to previously set, clearly defined criteria.

Who: WBYT project manager/team
When: Initiation
Where: throughout supply chain via standards outlined in contract
What: contractually require subcontractors adhere to unique identifiers

Require that identification methods are sufficient to support provenance in the event of a supply chain issue.
Who: PM / management teams
When: Initiation
Where: throughout supply chain via standards outlined in contract
What: ensure identification of all entities within supply chain adhere to strict documentation and tracking of purchases, shipping and receiving to ensure provenance

Use threat response practitioners to assist the systems engineering and the implementation, oversight, and compliance communities.
Who: WBYT is utilizing DUO security services for oversight of threat response
When: at Initiation and quarterly or after any changes to processes
Where: at affected supplier
What: Oversight and compliance confirmation for SCRM policies

Document that individuals are assigned appropriate roles throughout the supply chain and system/element life cycle, regardless of personnel turnover
Who: HR managers of involved companies
When: Initiation and Quarterly
Where: Supplier to conduct with their own organization
What: Produce personnel tracking and role assignment of personnel tasked to production of products/services for WBYT/ USAF projects

<u>Acquirer – Validation and Verification Activities</u>
Assess the effectiveness of acquirer and integrator identity management …
Who: DUO security as contracted by WBYT
When: Initiation, after any changes or minimally annually
Where: at supplier locations
What: conduct risk analysis and security assessments of access control policies and procedures

Perform audits on unique identification deficiencies and report up the supply chain for corrective action.
Who: DUO security as contracted by WBYT
When: initiation and quarterly
Where: supplier/integrator location
What: conduct quarterly reports on unique identification of roles, responsibilities, organization, people, etc.

Ensure that unique identifications are assigned to all actors/roles and to the tactics, techniques, procedures, and tools most associated with those actors
Who: DUO security as contracted by WBYT

When: initiation and quarterly during audit
Where: supplier/integrator location
What: audit and produce report detailing identifications assigned to all roles, techniques, procedures, etc.

Employ tools and techniques to determine if authenticators are sufficiently strong to resist attacks intended to discover or compromise authenticators
Who: DUO security as contracted by WBYT
When: Initiation and quarterly
Where: supplier / integrator location
What: conduct testing/auditing of controls in place to ensure adequate protection of authenticators.

Check for robustness of the infrastructure that manages unique identities.
Who: Duo Security
When: Initiation and during quarterly audit
Where: Supplier/integrator locations
What: audit for adequate resources and security controls of systems that manage identities.

Assess whether identities can be detected or altered (e.g., counterfeiting of identities/spoofing)
Who: Duo Security
When: initiation and quarterly
Where: supplier/integrator locations
What: audit for proper controls of supply chain process to evaluate potential for counterfeits and spoofing of trusted entities.

Recommendations: *In order to facilitate a more informed, secure supply chain, entities within supply chain are to conduct monthly meetings between the acquirer and their supplier. These meetings are to include documentation of all auditable activities as well as any documentation / tracking of processes to ensure provenance. Reports should be complied and separated according to activity (i.e. HR report, Security audits/report, progress report, purchasing/shipping/receiving report, etc.) and will be made available to the next entity directly up the chain. Integrators will be expected to supply their own reports, plus a second report documenting all the suppliers down chain from them.*

References

Sigler, Ken, Dan Shoemaker and, Anne Kohnke, Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product, Auerbach Publications; (Internal Audit and IT Audit) 1st Edition, November 3, 2017

Shoemaker, Dan, and Kenneth Sigler, "Cybersecurity: Engineering a More Secure IT Organization", Cengage Learning, 2014, Chapters 5 and 7
ISO 27001 and ISO 27002 (provided as BS7799)

IEEE 1028-1997 Standard for Software Reviews

ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)

IEEE 610 - Standard Glossary of Software Engineering Terminology

The Common Weakness Enumeration http://cwe.mitre.org/

Foreign Ownership, Influence or Control Investigations (FOCI)
http://www.dss.mil/isp/foci/foci_info.html