Final Project Report

ENABLING CYBERSECURITY FOR THE DIGITAL MANUFACTURING SUPPLY CHAIN

Principal Investigator / Email Address	Radu Pavel, Ph.D. / pavel@techsolve.org
Project Team Lead	TechSolve, Inc.
Project Designation	Cybersecurity
MxD Contract Number	19-12-02
Project Participants	TechSolve, Inc.; Siemens Corporation, Corporate Technology; University of Cincinnati, General Tool Co., Magna Machine Co., Cleaning Technologies Group LLC, Midwest Filtration LLC, Wulco Inc.
MxD Funding Value	$200,000
Project Team Cost Share	$262,500
Award Date	November 12, 2020
Completion Date	October 31, 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
This project was completed under the Technology Investment Agreement W15QKN-19-3-0003, between Army Contracting Command – New Jersey and MxD. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The scale and speed of digitalization and growth of connectivity networks in manufacturing are leading to an increase in cybersecurity risks. Cyber-attacks have the potential to affect confidentiality, integrity, and availability in a manufacturing setting. They can lead to loss of product and process IP, production losses, and even injury and loss of life. Compared to manufacturing assets (known as operational technology – OT), the information technology (IT) systems and related business processes are more established and more focused on end-user support and efficiency. The OT systems are developed with a different philosophy than the typical IT infrastructure, they follow different standards, and have different goals and priorities. Therefore, manufacturers are seeing additional challenges due to the need to protect not only the information technology (IT) systems but also the operational technology (OT).

While large organizations have made significant strides on identifying ways to protect their manufacturing operations, the small and medium size manufacturers (SMMs) lack the resources that big companies have to research and implement tools that can help them understand and mitigate their vulnerabilities. There is a lack of tools and expertise needed to identify and mitigate cyberattack vulnerabilities for small and medium manufacturers in the supply chain.

This project was conducted to address these challenges and provide manufacturers with best practice considerations for identifying and selecting tools for asset inventory and vulnerability scanning, and for conducting internal assessments. The project had the following main goals:
1) To create awareness and inform manufacturers of the importance of conducting vulnerability scans and keeping an asset inventory.
2) To be a reference for manufacturers regarding how to select the necessary cybersecurity tools, and how to utilize them.
3) To provide representative examples using the tools selected based on the criteria and considerations developed during the project.

The approach was to explore current cybersecurity solution offerings relative to a minimum set of requirements, establish benchmarking and tool selection criteria, select a set of representative tools for testing and demonstration, deploy pilot implementations and create a guide of best practices for small and medium size manufacturers.

The deliverables of the project include:

- Criteria for benchmarking of existing cybersecurity solutions
- Guidelines for best practices for the adoption and use of such tools
- Guidelines that enable manufacturers to determine the total cost of ownership
- Considerations for assessment tool deployment and required expertise
- Examples of the application and results of utilization of such tools

The guide can be utilized by the person responsible for implementing the cybersecurity program at a small manufacturer, who needs guidance and information for selecting and utilizing an effective cyber-solution for uncovering and mitigating vulnerabilities. Future directions of investigation associate with de-risking the OT scans to avoid slowdowns or crippling the operation, exploring differences between scanning outputs and standardization opportunities, and development of a Cybersecurity test-bed to support experimentation and data benchmarks to research cybersecurity issues for small and medium size manufacturers.

II. PROJECT DELIVERABLES

The following list includes all deliverables created through this project. These deliverables will be referenced throughout this report and should be accessible on the MxD membership portal in accordance with the rights defined by the Membership Agreement. Specific deliverable types include, but are not limited to, the items listed in Table 1.

Table 1. Project deliverables

#	DELIVERABLE NAME	DESCRIPTION	FORMAT OF DELIVERY
1	Manufacturer Profile	Documented profiles for the manufacturers included in the pilot to help manufacturers with assessment of adoption decisions.	Excel and pdf file
2	Defined/documented criteria for Benchmarking of Existing Cybersecurity Solutions	Documented set of criteria that is vital to an effective SMM cyber solution and benchmark tools on the listed functional/technical evaluation factors.	Excel and pdf file
3	List of tools evaluated	A list of tools evaluated according to the established criteria.	Pdf file
4	Criteria for selection of evaluated tool(s)	Description of criteria used for the determination of the tool(s) selected for use in the evaluation exercise.	Pdf file
5	Report(s) on performance of benchmarked tool(s) based on established criteria	Report on performance of selected cybersecurity tools for pilot implementation. The performance was evaluated based on technical literature review, conversations with the providers, tests conducted at TechSolve, and observations from the pilot implementations.	Pdf file
6	De-Identified/Anonymized Results of vulnerability assessment and penetration test(s)	Summary of anonymized (de-identified) results from instances of vulnerability assessment exercises.	csv files
7	Prioritized recommendations	Report with prioritized recommendations for the remediation of identified vulnerabilities.	Pdf file(s)
8	Evaluation Scorecard	Results from the team's evaluation of tool(s) based on established criteria.	Pdf file(s)
9	Due Diligence Report	A report of due diligence performed to assess the longer-term viability of vendor(s) for selected tools	Pdf file
10	Installation and configuration guide for SiESTA	Document how we configure and use the SiESTA for the purposes of the project activities	Pdf file
11	Software guide for SiESTA	Document how we configure and use the SiESTA for the purposes of the project activities	Pdf file

12	User guide for SiESTA	Document how we configure and use the SiESTA for the purposes of the project activities	Pdf file
13	User training and DEMO for SiESTA	Document how we configure and use the SiESTA for the purposes of the project activities	Pdf file
14	Guide for the SMMs regarding best practice considerations	A guide for the SMMs regarding best practice considerations for adopting cybersecurity technologies, criteria for benchmarking cybersecurity solutions meeting the minimum requirements listed in MxD-19-12 RFP, and examples based on the tools adopted for this project.	Pdf file
15	Presentation slides	Include presentation slides (i.e. PowerPoint) suitable for seminar presentations, live webinars, and train-the-trainer workshops. The slide-deck is based on the outcomes of the project and includes the guidelines for SMMs.	PowerPoint and pdf files
16	Recorded Presentation	The recorded presentation can be used in combination with the other guide materials to transition the research results to inform the SMMs looking to invest in cybersecurity.	Video file (mp4 format)
17	Final Report	A report describing all the tasks of the project and their results, delivered at the completion of the project.	Pdf file

III. PROJECT REVIEW

Manufacturing has become an increasing critical industry sector for reported cyber incidents. Cyberattacks have the potential to affect confidentiality, integrity, and availability in a manufacturing setting. They can lead to loss of product and process IP, production losses due to destroying, modifying, reprogramming parts and processes, damage to reputation, and even injury and loss of life. Data and cyber-physical system availability are also critical to manufacturing productivity. The scale and speed of digitalization and growth of connectivity networks are leading to an increase in cybersecurity risks. It is not just that scale of exposure, that is, increase in number of network nodes, it is also the vulnerability of the cyber-physical systems being connected.

Compared to manufacturing assets (known as operational technology – OT), the information technology (IT) systems and related business processes are more established and more focused on end-user support and efficiency. The OT systems are developed with a different philosophy than the typical IT infrastructure, they follow different standards, and have different goals and priorities. Legacy or orphaned hardware and software systems are commonly used in manufacturing processes and some of these OT systems were not designed with cybersecurity or the IoT in mind. Therefore, manufacturers are seeing additional challenges due to the need to protect not only the information technology (IT) systems but also the operational technology (OT), which can span from sensors to PLCs, robot controllers, machine tools and other operational equipment.

While large organizations have made significant strides on identifying ways to protect their manufacturing operations, the small and medium size manufacturers (SMMs) lack the cybersecurity resources of large corporations. This makes it difficult for SMMs to research and implement tools that can help them understand and mitigate their vulnerabilities. There is a lack of tools and expertise needed to identify and mitigate vulnerabilities for small and medium manufacturers in the supply chain. A lot of businesses are not fully aware of everything that resides on their network, and the potential risks they pose.

With technology constantly evolving, there are more than just IT assets that need to be protected. The cybersecurity tools need to be able to work for both IT and OT devices, as both perform crucial functionality for manufacturers, and pose risk to the manufacturing environment. Solutions to be tested therefore must have capabilities that allow for testing of operations technology and information technology (OT/IT) components of manufacturing entities.

To address these challenges, the project was focused on identifying, benchmarking and evaluating user-friendly (consumer-grade), intuitive and effective cybersecurity tools for cataloguing and assessing vulnerabilities of IT/OT assets for small and medium-sized manufacturers (SMM).

The purpose was to

- Create awareness and inform decisions regarding adoption, augmenting/enhancing, or integrating capabilities within a tool or collection of tools.
- Conduct a pilot implementation and test of the top cybersecurity tools, and
- Create an example packet that can be used by SMMs as reference for their own learning and scanning needs.

Use Cases & Problem Statement

Digital transformation of manufacturing processes leaves it vulnerable to cyber-attack. There is a lack of tools and expertise needed to identify and mitigate cyberattacks for small and medium size manufacturers. A lot of businesses are not fully aware of everything that resides on their network, and the potential risks they pose. If an attacker can gain a foothold on a network, these vulnerabilities are what threat actors are looking for to gain persistence, pivot around the network, perform lateral movement, and ultimately fulfil their objective.

It is difficult for businesses to understand what the impact of each vulnerability is, and how to fix it. With technology constantly evolving, there are more than just IT assets that need to be protected. These tools need to be able to work against IT and OT devices, as both perform crucial functionality for manufacturers, and pose risk to the environment.

Currently there are no clear guidelines and criteria for selecting tools needed to identify and mitigate cyberattacks on SMMs. There is limited understanding of the ability of the tools to address not only IT but also OT, and relate to NIS 800-171 controls. There is no guidance or criteria for selecting such tools and there are no examples the SMMs could relate to.

The use case scenarios considered when developing the scope and goals of the project are listed below:

- As the person responsible for implementing our cybersecurity program at a small manufacturer, I want a resource that will not only tell me I have a problem but also point me in the right direction for how to address the issue so I can be confident that the risk has been reduced.
- As the person responsible for implementing our cybersecurity program at a small manufacturer, I want easy-to-use tools that can be easily understood without taking too much time away from my day job.
- As the supply chain manager at a large manufacturer, I want to be confident that my suppliers are improving their cybersecurity practices to reduce cybersecurity risks across my supply chain(s).
- As the person responsible for implementing our cybersecurity program at a small manufacturer, I want guidance and information for selecting & utilizing an effective cyber-solution that will enable me to uncover and mitigate vulnerabilities.

Scope & Objectives

The scope of the project was to identify, evaluate, deploy pilot implementations and create a guide of best practices for small and medium size manufacturers. The main objectives set for this project are summarized below.

- Develop a self-assessment Cybersecurity Profile for Manufacturers that helps them understand their current cybersecurity readiness / status and their unique needs relating to cybersecurity toolsets with respect to asset discovery and inventory and vulnerability scanning.
- Define & document criteria for benchmarking of existing Cybersecurity solutions – which is a set of criteria for an effective cyber-solution for the small and mid-size manufacturers
- Report on performance of benchmarked tools based on established criteria - Conduct a pilot implementation and test of the top cybersecurity tools at TechSolve and the 5 manufacturers that were members of our project team
- Generate examples and technical lessons learned from the pilot implementations, including de-identified/anonymized data (which are the scan results).
- Create a guide with best practice considerations for adopting cybersecurity technologies

Planned Benefits

The outcomes of the project provide guidelines and criteria for selecting appropriate cybersecurity tools, and provide procedures and examples. The project is also introducing SiESTA as a new tool designed for the manufacturing environment and actual requirements of the cybersecurity ecosystem. The key benefits are:

- The creation of a documented set of criteria that is vital to an effective SMM cyber solution and benchmark tools on the listed functional/technical evaluation factors,
- Reporting from pilot implementation detailing analysis to validate the effectiveness of the benchmarking, identify solution gaps, and provide guidance for implementation that will help maximize ROI for SMMs,

which, in turn, will support the efforts to

- Reduce cybersecurity attack risks
- Efficiently select cybersecurity tools for asset discovery and vulnerability assessment
- Validate compliance with specific controls of NIST 800-171 standard
- Understand and reduce efforts and costs associated with the identification, selection and utilization of cybersecurity tools.

This is the first effort of its kind, which not only provides awareness and guidelines for manufactures, but also highlights gaps and opportunities for research and development to enable further improvement of the tools and practices enabling to better secure the digital manufacturing supply chain against cyber-attacks.

IV. TECHNICAL APPROACH

The following technical approach was adopted to complete the project goals and objectives.

- Build a team that besides TechSolve included five small and medium size manufacturers, a large manufacturer and technology provider, and a university (academe)
- Develop cybersecurity profiles for the manufacturers included in the pilot to help manufacturers with assessment of adoption decisions.
- Conduct a state-of the art study to identify tools, capabilities and limitations
- Develop the criteria for benchmarking of existing cybersecurity solutions
- Select a representative set of tools to conduct assessments (list of tools and criteria for selection)
- Conduct tests in TechSolve’s cybersecurity lab and on TechSolve’s IT and OT network(s) – The Machining Lab is a shop floor environment with machine tools and instrumentation similar to a small manufacturer environment
- Report on performance of evaluated tools and develop testing protocol

- Develop Test Plan for conducting assessments at manufacturers with selected cybersecurity solutions
- Conduct pilot implementations at manufacturers and collect de-identified/anonymized results of asset inventory and vulnerability assessments
- Review results with manufacturers and generate prioritized recommendations
- Create evaluation scorecards for the tools selected for pilot implementations to provide examples and considerations
- Create a report of due diligence performed to assess the longer-term viability of vendor(s) for selected tools
- Develop a guide for the SMMs regarding best practice considerations for adopting cybersecurity technologies, criteria for benchmarking cybersecurity solutions meeting the minimum requirements, and examples based on the tools adopted for this project. The guide package includes:
    - Written guide
    - Summary slides
    - Recorded presentation
    - Template tools (e.g. manufacturer profile, criteria for benchmarking)
    - Guides for SiESTA
    - Sample results, including de-identified/anonymized data
- Generate final report and presentation

A transition plan for the developed materials and lessons learned has been created to disseminate the information to MxD members and to small and medium size manufacturers in general. As an MEP organization, TechSolve is committed to supporting the SMM community and the deliverables of this MxD project boost the efforts to improve cybersecurity resilience of the manufacturing supply chain.

The team organization and roles have been divided as shown in Table 2.

Table 2. Team organization and roles

Team Organization	Role
TechSolve	- Project management - On-site test bed - Documentation tasks - Tool integration at SMM sites - Cybersecurity subject matter expertise - Lead integration team - Deliverable development - Transition management
Siemens	- Cybersecurity subject matter expertise - Provide SiESTA tools - Provide SiESTA training to integration team

	- Documentation tasks - Deliverable development
University of Cincinnati (UC)	- Cybersecurity subject matter expertise - Metrics development - Documentation tasks - Member integration team
Small and Mid-size Manufacturers (SMMs)	- Provide SMM test bed environments - Member integration team for their own site

TechSolve and Siemens have partnered in this project in a complimentary way. TechSolve has well-established relationships with SMMs as well as MxD institute. Siemens has expertise in cybersecurity as well as developing new, innovative digital manufacturing products and solutions. TechSolve's expertise in empowering SMMs to learn about and adopt emerging technologies aligned with the goal of evaluating and selecting cybersecurity tools that would best serve SMMs. The SMMs were specifically selected to represent a variety of manufacturing process types. Additionally, some of the SMMs have supply chain relationships. Overall the selected SMMs represent a cross-section of the manufacturing community typically supported through the Manufacturing Extension Partnership (MEP) program. The team aimed to blend new and existing tools to address the goals of this project. Since TechSolve and the manufacturing partners were new to the Siemens SiESTA solution, there was truly an opportunity to evaluate a cybersecurity solution that the SMMs have not yet seen or experienced.

The team included the University of Cincinnati as an academic partner, to bring a scientific and academic mindset to design the metrics, format and methodology. University of Cincinnati provided insights that supported a well-balanced execution, meaningful evaluation of the tools with metrics that matter, and documentation providing clear, understandable deliverables. We also relied on our academic partner to identify future research ideas and opportunities that could further the results of this project after its completion.

This project aimed to provide a repeatable process for selecting cybersecurity tools and conducting meaningful assessments. These assessments address operational cybersecurity as well as regulatory compliance. To accomplish this goal, the team started by conducting a state-of-the-art study of existing commercial solutions to select representative tools. The team also investigated if solutions are already in use at the SMMs, and to what extent those fit the benchmarking criteria. A new product from Siemens specifically designed to provide turn-key cybersecurity assessments, SiESTA, was one of the main tools used in this project. All of the cybersecurity solutions were tested using a set of predefined metrics aligned to the project KPIs.

Siemen's SiESTA (Siemens Extensible Security Testing Appliance) incorporates existing security tools into a system that also hosts a web interface which acts as a level of abstraction between the cybersecurity tools and the user. The existing application also enables the definition of specific test cases in an easy to understand format that does not require much knowledge about the security applications themselves. It is possible to configure the security applications and perform the assessment without the user directly configuring and operating the cybersecurity tools.

In parallel with the state of the art study, the team began developing a self-assessment tool focused on capturing the cybersecurity profiles for manufacturers (the "Manufacturer Profile").

The purpose of this self-assessment tool is to provide the manufacturer a template that helps understand their current cybersecurity readiness/status and their unique needs relating to cybersecurity toolsets.

After completion of the State-of-the-Art study, the team was ready to create the Criteria for Benchmarking of Cybersecurity Solutions. The criteria was primarily derived from the documentation provided by MxD with respect to minimum requirements, and the key performance indicators (KPIs) for cybersecurity tools. From the State-of-the-Art study, additional criteria were further compiled and utilized to capture characteristics of cybersecurity tools. Another source that was leveraged for criteria selection was a checklist developed at TechSolve, prior to this project, providing considerations for manufacturers looking to select suppliers for technology needs. Eventually, the benchmarking criteria was created and a template and examples were included in the Guide Package for manufacturers.

Based on the established criteria, a number of tools have been selected for performance evaluation tests. Considering the scope of the project, as well as the resources and time constraints, four tools have been selected, including:

- SiESTA, by Siemens Corporation, is a solution that has the capability to integrate various tools (such as Kali Linux, Nessus and Nmap), and it is using software developed by Siemens to effectively and efficiently conduct asset discovery and vulnerability scanning for both IT and OT.
- Qualys Vulnerability Management Detection and Response (VMDR) & Web Application Scanning (WAS), by Qualys – a cloud based tool that has full capability associated with the goals of the project and the benchmarking criteria developed by the project team
- OpenVAS Community Edition– which is a no-cost option provided by Greenbone Networks. A more comprehensive, at cost solution is available from Greenbone but the team wanted to explore to what extent the no-cost option was a good starting point for manufacturers that look for an inexpensive option or initial, quick assessment
- SolarWinds Network Configuration Manager (NCM) (runs on an On-Premises Server), by SolarWinds - which was selected based on feedback from the provider and the fact that the team learned some manufacturers use SolarWinds software for network monitoring. From SolarWinds options at the time of selection, Network Configuration Manager appeared to be the closest to the needs of the project.

The selected tools have been first tested on TechSolve's cybersecurity lab and IT and OT network(s). TechSolve has a Machining Lab that emulates the shop floor of a small manufacturer with machine tools, metrology equipment and associated instrumentation. This working industrial manufacturing facility includes data-connected industrial machining centers, additive manufacturing machines, collaborative robot systems, and IIoT sensors and devices.

Based on these tests, an initial evaluation of the tools has been conducted and the results have been captured in a performance evaluation report. The lessons learned have been used to establish a testing protocol and a test plan for the pilot implementations at the manufacturers.

The University of Cincinnati designed a rigorous assessment protocol so that each tool is applied and evaluated in an objective manner. The initial version has been reviewed and refined with contributions from TechSolve and Siemens. A high level view sample of this protocol is provided in Table 3.

Table 3. Testing Protocol

Status Prior to application helps determine expectations from applying the tool (along specific criteria)
• SMMs identify zone that represent IT and OT technologies to be used for the pilot
• Each toolset will run against the same equipment in the defined zone to get a repeatable and easily comparable set of test results
Document steps for applying the tool
• Issues that are faced and how it was addressed
• Impact on the manufacturer during the application
Set Up
• Set up the process
• Process to roll back if something goes wrong
Results
• Did the result match the expectation
• Was the status prior to application accurate
• What were the differences between the expectations and the actual
• Why was there a difference
• What could the manufacturer have done to match the results?
Verify
• Apply the steps and reach a new manufacturer state
• Did the results match expectations?
Repeat

Based on the results of the tests conducted at TechSolve and the testing protocol, a test plan has been developed for assessment of cybersecurity tools at manufacturers. The test plan has been provided in a report to MxD, and a summarized version is presented in Appendix B. The test plan was presented to and discussed with the manufacturers that were part of the project prior to conducting the assessments. These communications were very useful for scheduling and conducting the assessments in an efficient manner.

Once the test plan has been established, TechSolve and Siemens conducted pilot implementations at manufacturers, and collected the results of asset inventory and vulnerability assessments. These results were reviewed with the manufacturers and prioritized recommendations have been generated. The results have been de-identified/anonymized to enable selecting examples for manufacturers.

Each SMM was requested to define a scope or zone of devices that represent IT and OT technologies to be used for the pilot. Each toolset was then run against the same equipment in the defined scope, to get a repeatable and easily comparable set of test results.

The tests conducted at TechSolve and manufacturers enabled creation of evaluation scorecards for the selected tools, which are provided as part of the deliverables for this project. It should be noted here that the intent was not to grade the tools but rather to establish the evaluation scorecards/criteria and provide examples for the selected tools and their configuration. A report of due diligence performed to assess the longer-term viability of vendor(s) for selected tools has also been developed. The goal was to create awareness that beyond the technical part and cost, the viability of the provider is also important and should be carefully evaluated based on certain criteria and considerations provided in the guide for manufacturers.

The main lessons learned and best practice considerations captured during the project have been compiled into a package that includes the written guide, summary slides, recorded guide presentation, template tools (e.g. manufacturer profile, criteria for benchmarking), guides for SiESTA, and sample results including de-identified/anonymized data.

V. RESULTS

This section presents the results and deliverables generated during the project.

Manufacturer Profile

The purpose of this self-assessment tool is to provide the manufacturer a template that helps understand their current cybersecurity readiness/status and their unique needs relating to cybersecurity toolsets. According to the MxD institute recommendations, the following characteristics have been considered when developing the manufacturer profile:

i. The self-assessment should be able to be completed by an IT professional with assistance from manufacturing, ops, etc.

ii. The manufacturing profile should take no longer than 4 hours to complete.

iii. The profile should consider the number of employees, device types, and other factors each team deems necessary.

The document was created by TechSolve and was subjected to reviews from Siemens and University of Cincinnati. Assessment meetings with each manufacturer participating in the project have been completed to validate the approach and create examples for this guide.

This document presents a list of the selected characteristics of the profile as well as the reasoning behind the proposed formulation. The profile has two main sections: one focused on general characteristics of the manufacturer, and the second focused on characteristics associated with NIST 800-171 controls. For quick reference, Appendix C presents the line items for the general characteristics of the manufacturer.

The Manufacturer Profile tool is provided in an Excel file that includes 2 tabs and accompanies this guide. The first tab represents the Self-Assessment Questionnaire, and the second tab presents the Relevant Controls and to which minimum requirement (according to MxD recommendations) they correspond, as well as best practice implementation recommendations. For quick reference, the minimum requirements to which the controls were mapped are listed below:

> **Asset Discovery and Inventory**
> Inventory/catalog client technology (IT/OT) assets and resources (e.g., applications, database, endpoint devices, network appliances, OT equipment/appliances, and servers), as required for assessment/testing scope determination.
>
> **Network Vulnerability Assessment/Test**
> Assess current network (including wireless) security measures to identify any vulnerability that exists in the Client's network infrastructure. Conduct external and/or internal scans/tests to identify any security vulnerability that exists in the client's assets and resources.
>
> **Application Vulnerability Assessment/Test**
> Conduct web application security assessment.
>
> **Automated Report Creation**
> Create an automated report of security findings with assessed criticality ratings and recommendations for remediation.

To get the benefits of this tool, a manufacturer should answer the self-assessment questionnaire, map the responses to the controls tab and then check their responses versus the best practice. Doing so will help them to identify where they may have gaps as it pertains to the controls relevant to the asset inventory and cybersecurity vulnerabilities.

Criteria for Benchmarking of Existing Cybersecurity Solutions

The criteria for benchmarking of existing cybersecurity solutions include a set of decision factors that are essential for identifying an effective solution for the manufacturer. These criteria contain a set of minimum requirements and a set of key performance indicators (KPIs) as defined by the MxD institute. Another source that was leveraged for criteria selection was a checklist developed at TechSolve, prior to this project, providing considerations for manufacturers looking to select suppliers for technology needs. A third source of information were the findings of a state-of-the-art study focused on identifying cybersecurity tools satisfying the minimum requirements. The team conducted internet searches to identify multiple tools with the ability to satisfy the minimum requirements listed in the following subsection. For this guide, the list of identified tools is provided in Appendix D.

Details of these studies referenced above are not provided in this guide as it was considered out of scope; however, the MxD institute members can find such details in the 19-12-02 project deliverables.

Minimum Requirements

***Asset Discovery and Inventory* –** The ability to conduct asset discovery and inventory is one of the key necessities of a cyber-secure manufacturing environment. It provides visibility of all devices located within an organization, preferably with limited or no human interaction. A tool capable to provide asset discovery and inventory should allow to inventory/catalog technology (IT/OT) assets and resources (e.g., applications, database, endpoint devices, network appliances, OT equipment/appliances, and servers), as required for assessment/testing scope determination.

***Network/Wireless Vulnerability Assessment* –** This allows organizations to test the devices on their network for known vulnerabilities. Tools could be used to conduct external and/or internal scans/tests to identify any security vulnerability that exists in the Client's assets and resources. The Wireless Security Assessment helps with the prevention of unauthorized access or damage to devices on wireless networks. This helps ensure up-to-date secure encryption is used, check for default credentials on devices, check for firmware vulnerabilities, and verify the segregation of guest access from the company's internal network.

***Application Vulnerability Assessment* –** The focus is on Web Application Scanning. The Web Application Scan should be able to scan a URL and identify any Web Application vulnerabilities. This can help identify vulnerabilities in public facing applications that could lead to an internal network compromise, or find vulnerabilities on internal applications.

***Automated Report Creation* –** It refers to the ability to create automated reports of security findings with assessed criticality ratings and recommendations for remediation. Reporting is an important feature to view and keep track of assets and assessments.

Key Performance Indicators (KPIs)

Total Cost of Ownership – The total cost of ownership includes the stated license or acquisition costs of the tool as well as any other costs that can be associated with its use, maintenance, training, update of the tool, necessary hardware, additional software licenses (e.g. database), time of IT professionals using the tool or cost of the IT service, annual renewal fees and other elements that may be specific to the organization. Such elements may include (but are not limited to): accessibility of external contractors, solution being deployed on-premises vs. a cloud platform, and the troubleshooting time in case certain OT technology becomes crippled by the cybersecurity tool. The downtime associated with pausing the production during OT scanning to avoid affecting/scrapping the products, can also add to the total cost of ownership.

Ease of Deployment – The ease of deployment criteria refers to how difficult it is to set up the environment for the tool, install the tool, and maintain the tool. It can also include characteristics such as platform compatibility, associated development tasks and average time to install and configure. According to MxD documentation, the ease of deployment was also regarded from the perspective of availability of cloud-based solutions of the assessment tool(s) for users with minimal technical expertise. Therefore, the set of considerations for assessing the ease of tool deployment include:

- Hardware required and lifecycle
- Software required
- Connectivity (i.e. connectivity to the networks and IT/OT being scanned)
- Licensing requirements and installation
- Require software agents or not
- On-premises or in the cloud
- Cybersecurity-tool maintenance and upgrades

- Ongoing support cost – IT expertise in house or at managed service provider (MSP)

Ease of Use – The ease of use criteria relates to how difficult it is to learn and use the tool. For example, how difficult it is to setup a discovery event or scan, how difficult the results are to interpret, how difficult it is to move to the next step, etc. It also includes how well developed training materials are, support options and how much prerequisite knowledge is required. The following criteria is recommended for evaluating the ease of use of a tool:

- Friendly user interface
- Easy to get started
- Ability to store and manage results
- Technical Knowledge needed
- Intuitiveness of installation, conducting scanning
- Intuitive and easy interpretation of results
- Ability to schedule scans
- Learning curve
- Availability of technical support
- Necessary Ports and Protocols
- Associated development tasks, if any
- Average time to install, configure and schedule

Effectiveness – This involves the scope of options the tool provides and how well they complete the stated tasks. This includes the range of vulnerabilities that can be tested, alternative installation models for different environments and adaptability to regulatory requirements. The effectiveness is also a function of the ability to fulfill the minimum requirements and the reporting capabilities (automation level).

Intuitiveness – This characteristic relates to how user-friendly the interface of the tool is, and how automated the solution is. The criteria for evaluating the intuitiveness of the tools includes

- User interface ease of use
- Scheduling the tool
- Report generation
- Reading and interpreting the results
- Ease of understanding of patching recommendations
- Technical knowledge needed to run and interpret the results
- Efficiency - Time it takes to complete a scan and completeness of results

Non-intrusiveness – This criterion relates to how much the tool utilizes the overall network and system resources, and if installation of agents or other software modules becomes necessary on the scanned assets. It also refers to the ability to scan IT and OT equipment with minimal or no disruptions or slowing down of the processes. A summary of the non-intrusiveness considerations include:

- Platform compatibility
- To what extent the tool require installation of agents or clients
- Ability to conduct credentialed and uncredentialed scanning without agents
- Tools does not use brute-forcing by default
- Penetration testing is not utilized by default
- Industrial environment compatibility for hardware (Tool would not cripple the IT or OT systems being scanned)

Provider Viability Assessment

Regarding the ***Provider Viability Assessment***, several sub-criteria relating to the sustainability of business model and practices of the solution provider were selected as follows:

Location of headquarters – By identifying the location of headquarters, an SMM should be able to filter out the products as a function of the country of provenience.

Year the company was established (time in business) – While recognizing that newer organizations are often founded on new technologies and most recent trends, an older organization with a longer business experience would more likely have experience, proven implementations, and references/ clients that can vouch for its effectiveness and quality of services and products.

Size of company (number of people) – This criterion will inform if the company has a sufficient employee head count that provides credibility to the ability to provide services and products in a sustainable manner.

Public financials (i.e. annual sales or revenue) – This criterion will inform on the size and business capability of the organization

Reputation/notable clients – This criterion is a balance between public customer reviews, press releases, and reputation of clients of the company providing the cybersecurity solution

Training / Guides – Availability of training and guides is critical for reducing the learning period for a new cybersecurity tool. The training can be on-line, in person or based on videos and documentation provided by the supplier.

Customer support availability – The responsiveness and availability of customer support is important considering at least the following scenarios: support to learn the system, utilize the system, and troubleshoot the system. 24 hours/7 days support is preferred, considering an attack can happen at any time.

An example of long-term viability assessment considerations for the vendors of the tools is presented in Appendix E. It is important to note that when assessing the long-term viability of a provider, the user should look beyond the individual indicators, and rather consider an overview of all characteristics and inter-relationships. Also, the users should consider their priorities or preferences regarding the type of provider and technology they need and would like to work with. As a rule of thumb, companies that have been more than ten years in business, and have a large infrastructure, tend to have longer viability. However, small companies that managed to evolve beyond the status of a start-up, tend to be nimble and leverage newer technologies, which may be attractive for smaller organizations.

The benchmarking criteria template is provided as a table in Excel format; an example presented for the tools utilized in the MxD project is also provided as part of the deliverables package. In addition, a summary of the tools evaluated at TechSolve and at the manufacturers that participated in the MxD-19-12-02 project, is provided below, after the next paragraph. The criteria for selection of evaluated tools follows the criteria for benchmarking. It should be noted that the costs listed for these tools were approximate and at the time when the evaluation was conducted. The actual costs may be different for the specific configurations and capabilities of the same tools at the time when the user is reading this guide.

TechSolve's testing process included conducting the same structured asset discovery and vulnerability scans against targets with each tool. The TechSolve team conducted an asset discovery scan against its entire internal network, consisting of servers, workstations, laptops, printers, cameras, projectors, cellphones, routers, switches, firewalls, and OT devices. The OT devices consisted of multiple Siemens PLC's, different types of machine tools with Fanuc, Siemens, and Mazak controls (vertical and horizontal machining centers and a mill-turn machine), and a Feed Axis testbed run by a Siemens control. TechSolve conducted vulnerability scans against workstations, laptops, virtual machines, and the OT equipment listed. Once these scans were complete, the devices were checked to ensure they did not crash, and that no services running on the devices crashed. A report was generated from each type of scan documenting the findings. These tests were conducted multiple times to ensure consistency in the process, findings, and reports.

SiESTA

- SiESTA is a new technology with a high readiness level, which was developed to address operational technology (OT) cybersecurity vulnerability testing needs. SiESTA can also be leveraged for IT scanning and is configured to use a set of tools (e.g. Kali Linux, Nmap, and Nessus) that address the minimum requirements of the criteria set.
- SiESTA was attractive for this project due to its novelty and proximity to a market mature solution. SiESTA was in great alignment with MxD's efforts to identify new technologies that can tackle the needs of the ever-changing digital manufacturing supply chain ecosystem.
- Since we are introducing the SiESTA and its application interface as a new toolset, the deliverables will serve to enable further research and development of the SiESTA platform as a turnkey industrial security assessment solution.
- Since TechSolve, University of Cincinnati, and the manufacturing partners are new to the Siemens SiESTA solution, the MxD project was a good opportunity to evaluate a cybersecurity solution that the SMMs have not yet seen or experienced.

SiESTA fully satisfies all four minimum requirements. The tool uses Nmap for asset discovery and inventory, as well as a Siemens specific OT scanner. SiESTA will also use Nessus to scan for vulnerabilities internally / externally in the manufacturer's environment. Nessus has excellent reporting capabilities. SiESTA will require the user to plug the box into an active Ethernet port. The tool operates with a web facing GUI so that a non-technical individual could operate the tool. It is effective at identifying vulnerabilities and ranking findings for remediation. The SiESTA tool will also provide a great explanation on how to remediate the vulnerability. SiESTA will have a minimal impact on day-to-day operations unless a Nessus scan is running. In case of Nessus scanning, there could be some disruptions to certain devices, such as stopping services on the system or causing an unintended Denial of Service against the system, although we did not experience this over the course of our assessments. SiESTA provides test cases which minimize the possibility of disruptions. The cost of the SiESTA tool was estimated to approximately $7,000 yearly at the time of the evaluation. The tool will take up space in the environment. At the present time, operation of the SiESTA will require an individual from Siemens to update and operate the tool.

Qualys VMDR and WAS

Qualys tools fully satisfy all four minimum technical requirements with both modules Vulnerability Management Detection and Response (VMDR) and Web Application Scanning (WAS), included in the platform. The VMDR tool will automatically discover and categorize known and unknown assets. VMDR can also complete network vulnerability assessments and WAS can conduct application vulnerability assessments, consisting of URLs or internal/external servers hosting web applications. The last requirement of automating report creation is satisfied fully because the user does not have to generate reports. Qualys is a cloud-based tool that requires a virtual scanner to be installed on a hypervisor - a software that allows for the creation and management of virtual machines, which can access the internet. Qualys is easy to use because the GUI is simplistic and clean. Qualys also offers a lot of videos and step by step documentation on how to use the application. If the customer requires a more specialized scan, a technically trained individual will be needed to help run the scan. The tool is effective at identifying vulnerabilities and ranking findings for remediation. It will also give remediation help to fix a vulnerability and will show status updates on how vulnerable the node still is or was. Qualys is non-intrusive with its scanning and deployment unless a brute force scan is deployed. Like Nessus, if a machine has a vulnerability where running a port/vulnerability scan against it can cause a denial of service, this can take that system offline. This was not experienced from Qualys in any of the testing, but it does not rule out the possibility. Qualys' license will cost approximately $5,000 for 128 IPs and $13,500 for 512 IPs added to the account annually, which allows for unlimited scanning. You can get 256 or IPs as well, the price will fall in the middle. On top of that, there is another $1,000 fee annually for the virtual scanner and will require updating from the individual responsible for the tool. WAS will be an extra cost.

SolarWinds Network Configuration Manager (NCM)

The SolarWinds NCM product can partially fulfill three of the four minimum requirements: Asset Discovery, Network Vulnerability Assessment, and Automated Report Generation. The tool can scan the network with SNMP, WMI, and ICMP to discover network devices such as switches, routers, and firewalls. It can partially fulfill the network vulnerability assessment requirement by identifying firmware vulnerabilities in the devices that have agents installed on them. However, the tool does not have the capability to scan internally / externally for vulnerabilities. The tool can generate reports, but the user must manually select which type of report they would like to generate. The tool does not fulfill the application vulnerability assessment requirement. SolarWinds NCM requires an Orion and a SQL server to be installed on site to run the tool. The SolarWinds SAM and the NCM will run on the same server if the user has both. NCM will require a technically trained individual to operate the tool effectively. NCM is effective at finding firmware vulnerabilities in network devices but will not rank them for prioritization of remediation efforts. The tool will provide a link to the Common Vulnerability and Exposures (CVE) located under the firmware vulnerabilities section within the NCM dashboard to provide their explanation for remediation. The NCM tool is non-intrusive because it does not require agents to be installed on the network devices. The SolarWinds NCM product will cost $1687 for 50 nodes and will require the Orion and SQL servers. It will also require a technically trained individual to monitor, update and configure the tool.

OpenVAS by Greenbone GMBH

OpenVAS fully satisfies two minimum requirements - Network Based Vulnerability Assessment/Asset Discovery, and partially satisfies one other minimum requirement - Automated Report Creation. The other minimum requirement, Application Based Vulnerability Assessment is not satisfied. OpenVAS can perform unauthenticated testing, authenticated testing, various high level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test. The partially satisfied requirement is automated report creation. OpenVAS can generate reports, but the user is the one that must initiate the generation. OpenVAS is not easy to use at first, but the GUI interface is straightforward after you read documentation. OpenVAS is effective at identifying vulnerabilities and ranking findings for remediation. The tool will also offer help to remediate the vulnerability with just one or two sentences. OpenVAS is non-intrusive as it does not try to exploit the vulnerability, instead it will only identify and report the vulnerabilities. Like the other vulnerability scanners, it has the potential to stop services or cause a Denial of Service against the devices, in which case we experienced twice from this tool in our testing. The software version is free of charge but will require updating from the individual responsible for the tool.

Utilizing the Cybersecurity Tools

Considerations Prior to Utilizing the Tools

Prior to purchasing or using one of these tools, it is important to ensure proper equipment and software are available. Considerations will start with simple items such as availability of a power source to connect the physical devices, whether it is a standalone system with the tool built in, or a host system such as a server to run the tools from. If the tool is going to be run on a virtual machine, it is crucial to have the appropriate resources available to allocate to these machines for optimal performance. In that regard, it is imperative to establish which hypervisor can be used with each tool, so the appropriate hypervisor can be installed on the host machine prior to downloading the ISO image – the file that is to be used with the hypervisor that will create a virtual instance of the tool. RJ-45 connectors are required for SiESTA and it is highly recommended to use these over WiFi with the other tools for better stability and speed. Lastly, but nonetheless important, a manufacturer will have to determine who will manage the tool(s) and could interpret the results. While these tools are relatively easy to learn, and the default settings allow starting ‘out of the box’; understanding ports, protocols, services, 3-way handshakes, and subnets will play an important role in customizing your scans. It is also important to be able to interpret the results. These tools are great at identifying and providing details about vulnerabilities, such as the impact and solution, but having a more intermediate IT knowledge base will help in fixing vulnerabilities that are not simply resolved by patching.

The next section present example prerequisites for the tools used during the MxD project.

Qualys

1. **Hardware** – One of the following systems will be needed to install the virtual scanner.
    a. Desktop/Laptop VMware Workstation, Player, Workstation Player, Fusion
    b. Client/Server VMware vSphere: vCenter Server, ESXi Citrix XenServer Microsoft Windows Server (Microsoft Hyper-V)
    c. Cloud Amazon EC2-Classic Amazon EC2-VPC Microsoft Azure Cloud Platform (ARM) Google Cloud Platform OpenStack OCI and OCI-Classic Alibaba Cloud Computer
2. **Virtual Scanner VM Requirements**
    a. Minimum- 1 x vCPU | 1.5 GB RAM | 1 x 40GB virtual HDD
    b. Recommended- 8 x vCPU | 16GB RAM | 1 x 40GB virtual HDD
    c. Internet connection to contact the Qualys server
3. **Qualys Account**
    a. The Virtual Scanner option must be turned on for your account.
    b. The user must be a Manager or sub-user with the “Manage virtual scanner appliances” permission.

SiESTA

1. **Hardware**
    a. Have a physical SiESTA box at the location
    b. Have at least two Ethernet cables, one for the management interface and one for scanning
    c. Have an open power outlet to plug in the SiESTA box
    d. Monitor and USB keyboard for initial network setup

Regarding SiESTA utilization, separate guidelines have been prepared by Siemens and have been attached to the Guide package in the folder named SiESTA-Guides.

SolarWinds NCM

1. **Hardware**
    a. Windows Server 2016/2019 Server. Windows 10 can be used for evaluation purposes only. This can be a VM.
        i. Minimum Requirements: CPU Speed: 3GHz dual core processor | 6GB RAM | 30GB HDD Space

ii. A separate SQL Server 2014/2016/2017/2019 or Azure SQL Database. The SQL Server needs to be on a separate physical drive. If you select the Lightweight Installation option, SQL Server Express 2017 is installed locally. This option should be used only for evaluating NCM.

OpenVAS – Community Edition

1. **Hardware**
   a. A physical laptop, Desktop, or Server on your network to setup a virtual machine
      i. This system needs to have a hypervisor installed to setup a virtual appliance scanner
2. **Virtual Scanner Requirements**
   a. This system should be able to allocate at least 2 Processor Cores, 2 GB RAM, and 10 GB HD space. For better performance, you may want to double or triple that.

MANUFACTURER PREPARATION

After the hardware and software prerequisites are satisfied, the user will need to determine where will the tool connect and “sit” on your network. The following content presents the examples for the tools used during the project. At least two IP addresses will be required for each tool: One for the host machine and one for the virtual machine, or in SiESTA’s case; one for the management Ethernet interface and one for the scanning interface. SiESTA will require at least one static address for the scanning interface, while the others can be issued via DHCP or statically assigned. It is also important to determine the IP scope when conducting these scans, if there are some devices that you don’t want to scan, these can be excluded in the scan configuration. Credentialed scans are highly recommended as this will give more accurate results, find more vulnerabilities, and reduce the number of false positives. To run a credentialed scan, an administrative account would need to be created and added to the authentication record of each tool. This will only work on devices in which that account has access, so if it is a domain account, it will authenticate to devices on the domain.

Qualys

1. Have two IP addresses ready: One for the Laptop/Desktop/Server and the second for the Virtual Scanner. (This can be issued via DHCP)
2. Have a list of IP addresses that are in Scope/Out of Scope.
3. Have an Administrator account ready (This is only necessary for a credentialed scan, i.e. a scan that can run as a logged in user. A credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.

SiESTA

1. Have an open port to plug the SiESTA box in to obtain an IP address. This can be a DHCP address.
2. Have an IP to assign to each Ethernet interface you want to use for scanning. These need to be statically assigned.
3. Have a separate computer on the same network that can browse to SiESTA’s web interface.
4. Have a list of IP addresses that are In Scope/Out of Scope.

5. Have an Admin Account ready (This is only necessary for a credentialed scan; a credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.

SolarWinds NCM

1. Have two IP addresses ready: One for the Laptop/Desktop/Server and the second for the Virtual Scanner. (This can be issued via DHCP)
2. Have a list of IP addresses that are in Scope/Out of Scope.
3. Have an Administrator account ready (This is only necessary for a credentialed scan, a credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.

OpenVAS – Community Edition

1. Have two IP addresses ready: One for the host machine and the other for the virtual scanner appliance (These can be issued via DHCP)
2. Have a list of IP addresses that are in and out of scope.
3. Have an Administrator account ready (This is only necessary for a credentialed scan, i.e. a scan that can run as a logged in user. A credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.

Expected Tasks

With each of the tools selected, the user should be able to perform asset discovery, network/wireless vulnerability scans, web application vulnerability scans, and automatic report generation. It is more common for a vendor to have specific (i.e., separate) modules or tools for web application vulnerability scans. Also, certain tools may enable scheduling scans at desired times, while others may not have that capability. This could be very useful, as the user will not need to take the time out of the daily work to setup and conduct scans whenever needed. Regarding the tools selected for this project, with Qualys WAS and SiESTA, the user can conduct web application vulnerability scans. Except for the community edition of OpenVAS (the professional edition can do this), scans that will run without user interaction can be scheduled. Running these scans can help identify new devices (asset discovery scan) and detect new vulnerabilities as the vendors update their tools frequently. All these tools can be setup to send an email to a user or group of users before the scan will take place, and once the scans are finished. Once the scans are complete, the results can be exported and saved to compare against previous scans or use them as a document to conduct vulnerability management tasks. As new vulnerabilities are discovered each day, it is recommended to conduct such scans at least once a month.

Using the Results - Prioritization

The vulnerability scanning results will list each IP address, the vulnerabilities associated, and a severity rating. Each tool has a slightly different scale in their severity rating, but they rate the vulnerabilities in a similar manner, based on their own scoring system. Qualys has a severity rating of 1-5, SiESTA has a rating of 0-4, OpenVAS and SolarWinds NCM have a rating of low, medium, and high. These severities are rated based on how easy they are to exploit, and the Common Vulnerability Scoring System (CVSS) scores. The CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. Originally developed by the National Infrastructure Advisory Council (NIAC), this system is now maintained by the Forum of Incident Response and Security Teams (FIRST), which is a US based nonprofit: https://www.first.org/

In the web interface of these tools, the user can filter by various queries and export those specific results. Similar sorting can be conducted in the exported CSV file from the scan results. To get started remediating the most critical vulnerabilities, the user should filter those results and only show the severity “4 and 5” vulnerabilities for Qualys, “3 and 4” for SiESTA, and the “High” for OpenVAS or NCM. These results will provide a great foundation to start remediating vulnerabilities. Once the most critical vulnerabilities are addressed, whether that would be by fixing the vulnerability or accepting the risk and controlling/monitoring that device as well as possible, the user can start to filter by a lower number.

Sample Results – Overview and Interpretation

Discovery Reports

A discovery scan will examine the network and identify devices based on open ports and protocols. The user can gather information such as IP address, Operating System, MAC address, open ports, and hostname. This will enable identifying nodes in the network that may be intentional or unintentional, and isolate those that create vulnerabilities. Brief samples of network discovery and inventory outputs generated with each tool used in this study are presented in Appendix F.

Vulnerability Assessment

Every manufacturer that was scanned had vulnerabilities in their environment which could have detrimental effects. Almost all these vulnerabilities have been known about for over at least two years and can be resolved by patching or upgrading end of life (EOL) systems and software. We saw many vulnerabilities related to Server Message Block (SMB) protocol, Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), Secure Shell (SSH), Virtual Network Computing (VNC), and system misconfigurations – see next subsection. To guarantee a correct comparison and to provide non-skewed results, these scans have all been un-credentialed. As we had no guarantee credentialed scans could be run at all manufacturers, for the scope of the project only uncredentialed scans were run first. Running credentialed scans increase the findings, as the tools can authenticate to the devices, looking for vulnerabilities in software, misconfigurations, malicious files or services, registry entries, web extensions, and much more. However, it was uncertain all manufacturers will allow that level of investigation in their network for the purpose of the project. Eventually, the investigative team was able to run credentialed scans at two manufacturers to explore the differences, and the expectation of increased level of results was proven to be accurate.

Table 4 presents the total number of vulnerabilities found using uncredentialed scans (not including informational or potential) with the four tools selected for the project.

Table 4. Total number of vulnerabilities found using uncredentialed scans

	Qualys	SiESTA	OpenVAS	SolarWinds NCM*
Manufacturer1	695	597	566	0
Manufacturer2	768	787	361	0
Manufacturer3	320	214	194	0
Manufacturer4	491	321	247	0
Manufacturer5	1554	1223	808	0
Total	3828	3142	2276	0

* SolarWinds Network Configuration Manager was mainly designed to help customers manage their network switch configurations. It does have a feature to check for firmware vulnerabilities in network devices, such as switches, firewalls, and routers. In testing, this tool did not find any firmware vulneraries in any environment. While other tools were able to identify some, this is not the main feature of SolarWinds NCM, and it seems to lack the amount of time and resources dedicated to maintaining this feature.

TOP 10 CRITICAL/URGENT VULNERABILITIES COMMONLY SHARED

1. EOL/Obsolete Software: SNMP Protocol Version Detected / Writeable SNMP Information / SNMP Agent Default Community Name (public)

   Simple Network Management Protocol (SNMP) is used to collect information about devices and can be modified to change device behavior

2. End of Life (EOL)/Unsupported Operating Systems

   Systems that no longer receive vendor support

3. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)

   Remote Desktop Protocol vulnerability that can allow an attacker to execute code remotely

4. MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (WannaCry) (Petya)

   Network File Sharing Protocol vulnerability that allows for remote code execution, used in previous ransomware attacks

5. Unauthenticated Access to FTP Server Allowed

   File Transfer Protocol, Anonymous logins are allowed

6. VNC Server Unauthenticated Access

   VNC allows remote access to a graphical user interface (GUI), and no authentication is required to connect with this vulnerability

7. Remote User List Disclosure Using NetBIOS

Usernames can be gathered, and an attacker can use these for a password brute force attack

8. SMB Signing Disabled or SMB Signing Not Required

   Server Message Block is a protocol used for file sharing and to request services, not requiring a signature or being disabled can allow attackers to conduct a man-in-the-middle attack against the SMB server

9. SSH User Login Brute forced (SSH Layer Authentication)

   Secure Shell is used to remotely access another device, not limiting failed password attempts will allow for password brute forcing

10. Microsoft Windows SMB NULL Session Authentication

   SMB vulnerability that can allow unauthorized users to obtain sensitive information about local resources and the user may be able to access/modify the registry

VULNERABILITY REPORTS

Once a vulnerability scan is complete, there will be an option to view or download the report. These reports are automatically generated, and can be downloaded in multiple format types, with the most popular being CSV and PDF. SiESTA will create a ZIP file with all the necessary documents, so selecting the type of file won't be needed. We found that a copy of both CSV and PDF are great to have, as the CSV will make sorting and managing much easier, and the PDF is more descriptive. Each report will list each vulnerability found for each IP address, the severity rating, CVSS score, threat, impact, and solution. This is crucial for remediation as these details will help identify the most critical assets that need to be addressed, and how to fix the vulnerabilities. Appendix G presents sample outputs of the vulnerability reports for each tool. For SIESTA, additional information is provided in its guides attached as part of this Guide Package.

CREDENTIALED VERSUS UNCREDENTIALED SCANS – COMPARISON

Credentialed scans use an admin account to authenticate to the devices allowing it access to more information, such as the registry, processes, software, services, ACLs, and files. This allows for a reduction in false positives and can detect more vulnerabilities in the devices. Uncredentialed scans have a higher chance of false positives, can still identify a lot of vulnerabilities, but must identify them based on open ports, the services running on them, how the devices respond to specific packets, and operating system. Number of vulnerabilities found are based on the scan type. Tables 5 and 6 show the results of both types of scans on the same target.

Table 5. Sample of credentialed scan output

Credentialed
Petya Ransomware Detected (Pre-Reboot)
Microsoft Internet Explorer Cumulative Security Update (MS15-124)
EOL/Obsolete Software: Microsoft .NET Framework 3.5 Service Pack 0 (SP0) Detected
EOL/Obsolete Software: Microsoft XML Parser and Microsoft XML Core Services (MSXML) 4.0 Detected

Credentialed
EOL/Obsolete Software: Oracle Java Standard Edition (SE) Java Runtime Environment (JRE) Java Development Kit (JDK) 7 (1.7) Detected
Oracle Java SE Critical Patch Update - October 2012 (ROBOT)
Oracle Java Runtime Environment Remote Code Execution Vulnerabilities
Oracle Java SE Critical Patch Update - February 2013
Oracle Java SE JVM 2D Subcomponent Remote Code Execution Vulnerability (Oracle Security Alert for CVE-2013-1493)
Oracle Java SE Critical Patch Update - July 2018
Oracle Java SE Critical Patch Update - October 2018
Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4)
Microsoft Malicious Software Removal Tool (MSRT) Privilege Escalation Vulnerability - February 2020
Microsoft Internet Explorer Security Update for September 2017
Oracle Java Runtime Environment Remote Code Execution Vulnerability
Intel Graphics Driver Type Confusion vulnerability in Content Protection HECI Service (INTEL-SA-00095)
Oracle Java SE Critical Patch Update - January 2020
Oracle Java SE Critical Patch Update - April 2020
Oracle Java SE Critical Patch Update - July 2020(CPUJUL2020)
SMB Signing Disabled or SMB Signing Not Required
Microsoft XML Core Services XMLHttpRequest "SetCookie2" Header Information Disclosure Vulnerability - Zero Day
Microsoft .NET Framework 3.5 Service Pack 1 Not Installed
Built-in Guest Account Not Renamed at Windows Target System
SAP Crystal Reports Print ActiveX Control Buffer Overflow Vulnerability
Intel Graphics Driver Multiple Vulnerabilities(INTEL-SA-00166)
Intel Graphics Driver Multiple Vulnerabilities(INTEL-SA-00189)
Windows Service Weak Permissions detected
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
NetBIOS Name Accessible
Enabled Cached Logon Credential
Allowed Null Session
Default Windows Administrator Account Name Present
Microsoft Windows Explorer AutoPlay Not Disabled
Windows Explorer Autoplay Not Disabled for Default User
SSL Certificate - Signature Verification Failed Vulnerability
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)
Oracle Java Input Validation Code Execution Vulnerability (Oracle Security Alert for CVE-2016-0603)

Table 6. Sample of uncredentialed scan output for same target as Table 4

Uncredentialed
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
NetBIOS Name Accessible
SSL Certificate - Signature Verification Failed Vulnerability
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)
SMB Signing Disabled or SMB Signing Not Required

System Overview

A Guide Package was developed to provide manufacturers with best practice considerations for identifying and selecting tools for asset inventory and vulnerability scanning, and for conducting internal assessments. The guide presents vulnerability scanning examples, considerations for patch management, and results generated using tools and approach referenced in this document. The guide also illustrates how these tools fit into the CMMC level 3 cybersecurity framework, which is going to be required for all manufacturers who need to handle Controlled Unclassified Information (CUI) when working as a prime or subcontractor in the Department of Defense (DoD) supply chain.

Utilizing these tools will help manufacturers learn what is connected to their network and identify vulnerabilities to be remediated. An asset discovery tool is essential for finding new devices that may not be listed in the asset inventory. Being able to identify critical vulnerabilities early is vital. If an attacker manages to gain initial access to a network, these vulnerabilities can quickly be identified and potentially allow attackers to gain control over the entire network. Remediating these vulnerabilities is going to give bad actors a much more difficult time to move around or control a network, buying enough time to identify a threat or push the attackers to a dead end all together. With new vulnerabilities being discovered each day, it is important to utilize these tools frequently.

This guide is part of a Guide Package that contains templates and examples accompanying each section as listed below.

- Manufacturer Profile – a self-assessment tool that includes best practice recommendations associated with the NIST 800-171 controls related to asset discovery and vulnerability scanning. The guide section includes the rationale and an overview of the tool, which is provided attached as an excel files named, ManufacturerProfile_Template.xlsx and ManufacturerProfile_Example.xlsx
- Criteria for Benchmarking of Existing Cybersecurity Solutions – This section includes the description of a set of decision factors that are essential for identifying an effective cybersecurity solution for the manufacturer. A template and examples are provided in the Guide Package (see BenchmarkingCriteria_TemplateWithExample.xlsx).
- Utilizing the Cybersecurity Tools – This section presents the main considerations that a user has to account for when utilizing the tools. Examples for each of the tool utilized

during the MxD-19-12-02 project are summarized. Additional guiding information for SiESTA is included in the Guide Package.

- Sample Results – Overview and Interpretation – includes examples of asset discovery and vulnerability scanning conducted with the cybersecurity tools selected for the MxD project. Samples of anonymized/de-identified data from manufacturers are included as part of the Guide Package, in folder 04_SampleResults.
- CMMC/NIST 800-171 Controls related to Vulnerability Scanning - This is a short section that highlights the usefulness of vulnerability scanning as part of compliance measures to the CMMC/NIST 800-171 controls.

System Requirements

No specific system requirements are necessary for the users to be able to access and use the results of this project. Generic system characteristics enabling readout of pdf, Excel, and csv files should be sufficient.

System Architecture

The project was focused on development of templates, criteria, guides and example results of asset inventory and vulnerability scanning. One of the main objectives was to test technology rather than develop technology. Therefore, no specific system architecture had to be developed.

Features & Attributes

Due to the fact that the project was not focused on technology development, this section did not have to be completed. Regarding the new technology leveraged by Siemens Corporation for this project, SiESTA, information regarding its features and attributes can be found in the guides provided as deliverables for this project.

Target Users & Modes of Operation

The project deliverables are mainly intended for the small and medium size manufacturers. The main goal is to provide best practice considerations on how to select the necessary cybersecurity tools, and utilize them. A written guide, examples, and template tools are provided in a Guide Package. The guide aims to create awareness and inform manufacturers of the importance of conducting vulnerability scans and keeping an asset inventory.

As the technology advances and the threat space changes, the users should carefully consider the recommendations provided in the guide as a function of the newest trends and evolving needs of the manufacturing ecosystem.

Software Development/Design Documentation

This project did not require software development and design documentation. As mentioned previously in this report, information about the novel software tool utilized by Siemens Corporation for this project, SiESTA, can be found in the guides provided as part of the project deliverables.

VI. DISCUSSION & ANALYSIS

Work on this project has revealed limited awareness in the manufacturing domain about the existence and characteristics of cybersecurity tools for asset discovery and inventory, and for vulnerability scanning. Therefore, the situation found in industry confirmed the importance and the timeliness of the project. Another realization that surprised the team was the extent of the vulnerabilities found during the scanning tests. This highlighted the importance of the vulnerability scans as well as understanding the needs for mitigating such vulnerabilities. This also revealed the challenges that exist in most manufacturing environments to protect not only the IT but also the OT, and created a first view of the potential future directions of investigations and R&D associated with protecting the shop floor.

The results of this project create awareness and educate the small and medium size manufacturers, as well as the OEMs, with regard to our findings and tools related to selecting cybersecurity solutions for proper asset inventory and vulnerability scanning. Template tools and associated examples have been developed to address some of the existent shortcomings:

- Manufacturer Profile – a self-assessment tool that includes best practice recommendations associated with the NIST 800-171 controls related to asset discovery and vulnerability scanning.
- Criteria for Benchmarking of Existing Cybersecurity Solutions – this includes a set of decision factors that are essential for identifying an effective cybersecurity solution.
- Utilizing the Cybersecurity Tools – a guide has been developed to highlight the main considerations that a user has to account for when utilizing the tools. Examples for each of the tool utilized during the MxD-19-12-02 project have been summarized.
- Sample Results – Overview and Interpretation – includes examples of asset discovery and vulnerability scanning conducted with the cybersecurity tools selected for the MxD project. Samples of anonymized/de-identified data from manufacturers are being provided as a relatable reference.
- CMMC/NIST 800-171 Controls related to Vulnerability Scanning – brief section that highlights the usefulness of vulnerability scanning as part of compliance measures to the CMMC/NIST 800-171 controls.

Industry Impact

The results of this project will help identify and reduce the risks in a manufacturing environment through guidance in best practices for selecting and utilizing asset discovery/inventory and vulnerability scanning tools. For those manufacturers in the Department of Defense supply chain, obtaining a Cybersecurity Maturity Model Certification (CMMC) may be a requirement. Vulnerability scanning is a requirement in CMMC, so implementing one of these tools will meet the requirements for those controls and assist in satisfying other controls. To achieve this impact, a manufacturer must first determine who is best suited to run, manage, and interpret the tool. This will require a fundamental IT background to run the tools, but interpreting the results will require an intermediate background in IT. After identifying who will operate the tool, it is important to understand which tool works best for the business. Whether that would be a cloud-based tool, open-source tool, or on premises. The budget and type of IT/OT environment will be primary considerations in selection of the tool.

Any business can benefit from such cybersecurity tools. Cyber-attacks increase every day, and no business is out of scope for one of these attacks. Vulnerability scanning is going to help any business to identify their risks, so they can be remediated, greatly reducing the risks. Running these tools and remediating all the vulnerabilities found does not mean the system cannot be hacked, but it will help reduce the risk and attack surface. For those businesses abiding by a specific cybersecurity framework or plan to adopt one, vulnerability scanning may be a control listed and is very important to adopt early.

The project is addressing the issue of cybersecurity of the manufacturing supply chain. The outcomes of the project best apply to SMMs. However, the outcomes can be used by organizations of various types and sizes – e.g. government, academia and industry.

CMMC/NIST 800-171 Controls related to Vulnerability Scanning

Manufacturers in the Department of Defense (DoD) supply chain will be required to hold a CMMC L-3 certification by October 1st, 2025. Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity framework that is meant to safeguard Controlled Unclassified Information (CUI)/Federal Contract Information (FCI). CMMC has five levels of certifications; while most manufacturers in this chain will need to comply with CMMC level 3, depending on the type of data developed and received on behalf of the U.S. Government, will determine the level on compliance necessary for the organization. These are some of the controls in which vulnerability scanning can contribute to or satisfy:

CMMC: RM.2.141 | NIST 800-171: 3.11.1 - *Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. Vulnerability scanning helps identify the risks that are in an organization. This can include vulnerabilities in the operating system, software, hardware, or misconfigurations of the system.*

CMMC: RM.2.142 | NIST 800-171: 3.11.2 - *Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Vulnerability scanning is required to satisfy this control. It allows you to identify the vulnerabilities in systems and applications.*

CMMC: RM.2.143 | NIST 800-171: 3.11.3 - *Remediate vulnerabilities in accordance with risk assessments. You can't remediate vulnerabilities if you don't know what they are. Vulnerability scanning identifies those and offers remediation advice, which will tell you the solution to fix the vulnerability. Qualys also has a remediation feature built in which will allow you to track which vulnerabilities you close. If you were to install agents on devices with Qualys, you could push out patches that would remediate the vulnerability.*

CMMC: RM.3.146 - *Develop and implement risk mitigation plans. It's crucial to know what types of vulnerabilities are in your environment as you create this plan.*

CMMC: RM.3.147 - *Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. Asset discovery and vulnerability scanning will help identify the types of devices that are in your environment. This can help you identify non-vendor supported products.*

CMMC: IR.2.093 – *Detect and report events. Vulnerability scanning can find traces of malware breadcrumbs, open ports known to host malware, and misconfigurations using a credentialed scan. This can contribute to the detection of potentially compromised systems.*

CMMC: CA.3.162 - *Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.* *Vulnerability scanning can help if the software is a web application. Using the specific Web*

Application module, this can check software for specific vulnerabilities related to web applications, such as SQL Injection, Cross-Site Scripting, Command Injection, and much more.

Key Performance Indicators & Metrics

Table 7 lists the key performance indicators (KPIs) that were selected for this project.

Table 7: KPI's and Metrics

KPIs	BASELINE	GOAL	RESULTS	VALIDATION METHOD
Total cost of ownership	No clear understanding or guidance for evaluating the total cost of ownership	Set of guidelines that enable manufacturers to determine the total cost of ownership	Set of guidelines included in the written guide and criteria for benchmarking report	The team purchased and implemented pilots at TechSolve and manufacturers that were part of the team
Ease of deployment	Limited information on the applicability of tools to the IT/OT environment and pre-requisite knowledge	Clear set of considerations for assessment tool deployment and required expertise	Set of considerations included in the written guide and criteria for benchmarking report	The team implemented and tested the tools at TechSolve and the manufacturers that were part of the team, which enabled the validation of the considerations included in the written guide
Ease of use	Limited knowledge and criteria on identifying and selecting tools	Criteria that help evaluate ease of use of cybersecurity tools	Set of criteria included in the written guide and criteria for benchmarking report	The team implemented and tested the tools at TechSolve and the manufacturers that were part of the team, which enabled the validation of the criteria
Effectiveness of tools	No clear guidelines for aligning the needs of the manufacturer with the capabilities of the tools	Criteria for benchmarking of existing cybersecurity solutions	Set of criteria included in the written guide and criteria for benchmarking report	The team implemented and tested the tools at TechSolve and the manufacturers that were part of the team, which enabled the validation of the criteria
Intuitiveness / Efficiency	No clear baseline for evaluating the Intuitiveness/Efficiency of the cybersecurity tools	Chart with basic criteria for evaluating the intuitiveness of the tools	Set of criteria included in the written guide and criteria for benchmarking report	The team implemented and tested the tools at TechSolve and the manufacturers that were part of the team, which enabled the validation of the criteria
Non-Intrusiveness of Solution(s)	No state-of-the-art knowledge for minimizing potential disruptive behavior or inconvenient form factors	Guidelines that enable manufacturers to assess the capabilities of a technology relative to its own infrastructure	Guidelines provided in the written guide and criteria for benchmarking report	The team implemented and tested the tools at TechSolve and the manufacturers that were part of the team, which enabled the validation of the guidelines.
Provider Viability Assessment	Generic set of rules not fine-tuned for cybersecurity assessment technologies	Criteria specifically designed to enable assessing viability of the cybersecurity technology providers for manufacturing	Set of criteria included in the written guide and criteria for benchmarking report	The team had to purchase the tools and assessed multiple vendors, which enabled the validation of the criteria

The metrics for evaluating tools were developed and used in collaboration with University of Cincinnati (UC). UC reviewed over 45 tools and conducted evaluation using data collected by Gartner Peer Insights on each of the tools. The evaluation summary is included in the State-of-the-Art excel file. Furthermore, the UC team reviewed 120 user evaluations of various tools and conducted thematic analysis to validate the metrics. Using tools in the Asset Discovery, Application Vulnerability, and Network Vulnerability categories, it was found that users are concerned with the criteria in Table 8.

Table 8. Criteria and Definition

Criteria	Definition
Cost	Determination if the quality of the product matches the cost or the affordability of the product
User Friendly	The level of ease or difficulty a user experiences, whether it be installation, deployment, updates, or everyday usage.
User Support	Any support available to users through different means of communication and resources provided by the company. Examples are documentation, technical, installation support, etc.
Effectiveness	The overall performance of a product including functionality and capability
Flexibility	Users are able to use a product for multiple functions
Non-Intrusiveness	When you run the tool, it should have no impact or minimal impact on the general operations or on the already existing software
Time efficiency	The time taken by the tool to finish the task. Generally, users prefer the tools that can finish the task in less time
Powerfulness	The strength and capacity a tool has to operate and level of performance.

The team found that users are looking for a tool that is effective. The user friendliness of the tools came next in importance as shown in Table 9, followed by user support. In Table 9, the frequency is defined as the number of users that mentioned a criterion as important in their review. Often, a review will indicate more than one criterion.

Table 9. Number of users identifying each criterion as important

Theme	Overall Frequency	Frequency for Asset Discovery tools	Frequency for Application Vulnerability tools	Frequency of Network Vulnerability tools
Effectiveness	63	26	17	20
Cost	7	1	4	2
User Friendly	37	9	15	13
User Support	28	11	8	9
Flexibility	13	4	0	6
Time Efficiency	4	0	3	1
Non-Intrusiveness	2	1	0	1
Powerfulness	13	3	4	6

Table 1 Number of users identifying each criterion as important

Accessing the Technology

The MxD Members will have access to the developed Guide Package and tools through MxD institute portal. No Background Intellectual Property (software, designs, data, etc.) is needed to use or modify the project deliverables. The Guide Package and project deliverables include file formats that are generally available to the public such as Microsoft Excel, and Adobe Acrobat Reader pdf formats.

The team considers there is no support needed to make use of the project deliverables. The users have the option to contact TechSolve for any additional information or support. For matters related to SiESTA, the users should contact Siemens Technology.

Workforce Development

This project was conducted to provide manufacturers with best practice considerations for identifying and selecting tools for asset inventory and vulnerability scanning, and for conducting internal assessments. The outcomes were templates, criteria, guides and example results of asset inventory and vulnerability scanning. While the main objective of the project was not workforce development, the outcomes of the project do provide documentation and examples that create awareness and educate the manufacturers relative to the selection and use of cybersecurity solutions for asset inventory and vulnerability scanning. The target audience are the small and medium size manufacturers; however, the results and findings can be very useful for managed service providers (MSP) organizations providing services to SMMs, as well as larger organizations seeking to increase the cybersecurity of their supply chain(s). More information about the contribution to workforce development can be found in the Transition Plan section of this report.

Lessons Learned

There were multiple lessons learned throughout the project. A summary of the technical lessons learned and overall, project lessons learned are summarized below. One of the first learnings of the project was that there is very limited knowledge of such tools and practices among manufacturers, hence the timeliness of the project. One other important fact was that most tools identified during the state of the art study were not developed with the ability to scan OT in mind. Therefore, it was important to have SiESTA as one of the main tools tested during the project.

The learnings from the project activities helped outline some of the gaps and opportunities for future direction of investigation and developments, as listed in the Next Steps & Challenges section of this report. Such directions refer to the need to be able to scan OT while operating, application of patches for the discovered vulnerabilities, need for use of a standard score, and reducing the gap/differences between the outputs of various technologies.

The amount of vulnerabilities discovered from the pilot implementations appear to be common amongst manufacturers. Therefore, it is important to utilize such tools to maintain awareness of ones vulnerabilities and protect against intrusions that could easily allow a bad actor to exploit such vulnerabilities.

Technical Lessons Learned

- Each vulnerability scanning tool has a different grading scale.

- Each tool had a different output in the results, making it so vulnerabilities couldn't be identified by Common Vulnerability and Exposures (CVE), but rather vulnerability title.
- SiESTA appeared to be the most accurate at identifying OT devices.
- Qualys does not scan port 0, which is known to host backdoors.
- OpenVAS crashed two servers running a vulnerability scan, the servers had a vulnerability that running a port scan/vulnerability scan against it could cause a denial of service. Given the vulnerability of the servers, all other tools tested would have resulted in such effect, should they have been run first.
- Always test the authentication credentials prior to running a full vulnerability scan.
- Credentialed scans find a significant amount more vulnerabilities.
- SiESTA failed to generate the results checker file with large amounts of data to be processed. However, this is being addressed by Siemens for future versions.
- OpenVAS had issues downloading result files with large amounts of data.

General Lessons Learned

- What went well?
  - Good cohesion/collaboration of the team
  - High interest from manufacturers
  - Good and helpful communications with MxD
  - The state-of-the-art was very useful for technology identification, evaluation and selection process
  - The tests conducted at TechSolve prior to deployment to manufacturers were very useful
  - The tests run at manufacturers went very well
- What went poorly? And associated learnings
  - COVID-19 Pandemic had an impact on the ability to interact with the team members (i.e. in person visits) and reach out to the vendors.
  - The performance of one of the software packages selected for trials did not match the minimum requirements as we were initially led to believe. The evaluation trials at TechSolve and the state-of-the-art study were vital to identify the shortcomings and identify alternative solutions.
  - Due to accessibility and availability at manufacturer's sites, the testing process went longer than initially envisioned
- What do you want to do differently?
  - The team would have liked to run similar tests after a certain duration of time (e.g. min. 3 or 6 months) and changes implemented at sites

- Testing more tools using credentialed scans and understand the differences (why some tools find certain vulnerabilities other don't)
- Create a website that would allow on-line access to the templates and the guide package.

VII. CONCLUSIONS & FUTURE WORK

This project is addressing the issue of cybersecurity of the manufacturing supply chain. There is a lack of tools and expertise needed to identify and mitigate the cybersecurity attack risks, especially for SMMs in the supply chain.

The project's objective was to evaluate vulnerability assessment tools with a focus on total cost of ownership, ease of deployment and use, effectiveness, and efficiency, and to generate criteria and guidelines for selecting such tools. The project deliverables provide a documented set of criteria that is vital to an effective SMM cyber solution, guide for the SMMs regarding best practice considerations, and sample (de-identified/anonymized) results of the of vulnerability assessment tests.

Two typical use cases addressed by this project are as follows:

- As the person responsible for implementing our cybersecurity program at a small manufacturer, I want easy-to-use tools that can be easily understood without taking too much time away from my day job.
- As the person responsible for implementing our cybersecurity program at a small manufacturer, I want a resource that will not only tell me I have a problem but also point me in the right direction for how to address the issue.

These use cases apply to SMMs or managed service providers for SMMs. The user role is associated with cybersecurity and/or IT (Cybersecurity or IT Manager, CISO or similar roles, depending on the size of the company). The user would periodically check the SMM's IT/OT network and systems for vulnerabilities and/or as part of the compliance with NIST800-171 and CMMC. The user would need to interact with the leadership team, various sector managers and, where the case the MSP.

The solution generated by this project is a set of guidelines, criteria and examples that can help a manufacturer or its service provider to identify and utilize cybersecurity solutions/tools that enable asset discovery and inventory, vulnerability assessment, and reporting.

The outcomes of the project will be disseminated in common file formats such as pdf and Excel. The potential follow-up work after completion of the project would be associated with commercialization, and periodical review/upgrade of state-of-the-art and criteria for benchmarking / minimum requirements.

Although the outcomes of the project best apply to SMMs, they can be used by organizations of various types and sizes – e.g. government, academia and industry.

The user position is related to cybersecurity and/or IT (Cybersecurity or IT Manager, CISO or similar roles, depending on the size of the company – e.g. owner or IT tech)

The outcomes of the project will have impact on various industries and their supply chains such as aerospace, automotive, continuous and batch processing.

Next Steps & Challenges

The recommended next steps for deploying the project outcomes are the dissemination of information through webinars, presentations, and social media posts, as listed in the Transition Plan section below. MxD members will have access to the materials through their membership. TechSolve will seek to leverage the NIST MEP network they are part of, the Ohio Department of Development and Ohio MEP to disseminate the results of the project.

TechSolve will seek to integrate the knowledge and information generated during the project into their cybersecurity service providing business. Examples include awareness and education events designed for manufacturers, compliance support, and vulnerability scanning services.

The risks and challenges that need to be overcome in order to deploy the project outcomes are mainly related to the ability of the technologies to operate efficiently both for IT and OT, without slowing down or crippling the operations. Other challenges are associated with the fact that identification of vulnerabilities cannot always result in a complete elimination of such vulnerabilities or cyber-attack risks.

Siemens can leverage the lessons learned from the pilot implementations of SiESTA to further improve the technology and make it more useful and appealing to small and medium size manufacturers.

2 – 5 years after the completion of this project, it is envisioned that the findings and lessons learned would have contributed to an increase of utilization of cybersecurity solutions by the manufacturers for vulnerability assessment and mitigation. It will also lead to the development and adoption of a new category of tools, with better application to OT (not just IT), and added capabilities for patch management.

Future research ideas and opportunities that could further the results of this project include

- Develop and operate a Cybersecurity testbed to support experimentation and data benchmarks to research cybersecurity issues for small and medium size manufacturers. This includes, but is not limited to:
    - Development and operation of a digital model of a small or medium size manufacturer (e.g. on the Ohio Cyber Range.)
    - Development and operation of a management protocol to allow running various experiments on the model. For instance,
        - Collect benchmark normal data flow on the model as well as data for various types of cyber-attacks.
        - Compare risk assessment models for manufacturing
        - Compare effectiveness of tools for various cyber defense.
        - Research and test protocols and models for cyber defense.
    - Development and operation of benchmark data dissemination to support researchers around the country.
- Explore current capabilities and future needs of the cybersecurity solutions for vulnerability assessment of operational technology (OT). One challenge is avoiding slowdown or crippling of the OT while scanning, hence ability to run these tools during production.

- Further research and development of the SiESTA platform as a turnkey industrial security assessment solution.
- Considering the number and importance of vulnerabilities determined during scans, it would be helpful if a playbook or guide will be developed to instruct manufacturers on how to protect against such vulnerabilities in the hypothesis that not all of them could be eliminated. Such use case would be: if a critical manufacturing asset is using an outdated operating system, which however the manufacturer cannot replace due to the cost and implications of that change, what are some of the best practices to address that vulnerability.
- Explore opportunities for standardization such that vulnerability scans with cybersecurity tools provide a minimum requirement or vulnerabilities, particularly for the critical vulnerabilities. Use of a standardized score would also enable better assessment and comparison amongst multiple tools

Transition Plan

The table below provides a catalog of all of the project deliverables and their respective transition routes. Deliverables can transition through deployment at an industry member's site, as an educational reference or through a commercialization effort. Each of these transition routes are detailed below, in Table 10.

Table 10. Transition route

#	DELIVERABLE FILE NAME	TECHNOLOGY INTEGRATION	EDUCATION	COMMERCIALIZE
1	Manufacturer Profile		X	
2	Defined/documented criteria for Benchmarking of Existing Cybersecurity Solutions		X	
3	List of tools evaluated		X	
4	Criteria for selection of evaluated tool(s)		X	
5	Report(s) on performance of benchmarked tool(s) based on established criteria		X	
6	De-Identified/Anonymized Results of vulnerability assessment and penetration test(s)		X	
7	Prioritized recommendations		X	
8	Evaluation Scorecard		X	
9	Due Diligence Report		X	
10	Installation and configuration guide for SiESTA		X	
11	Software guide for SiESTA		X	
12	User guide for SiESTA		X	

13	User training and DEMO for SiESTA		X	
14	Guide for the SMMs regarding best practice considerations		X	
15	Presentation slides		X	
16	Recorded Presentation		X	
17	Final Report		X	

TechSolve and the Manufacturers of the project team will use the deliverables at their sites to select tools and apply best practices that will enable them to identify and mitigate efficiently cybersecurity vulnerabilities of their IT/OT systems. Based on the outcomes of these implementations, the scaling strategy will leverage various channels such as MxD membership, MEP network and other organizations to deploy the outcomes into industry.

A one sentence summary of the transition activities that describes how the deliverable will be deployed or consumed is presented below.

Deliverable 1 – Manufacturer Profile

- Education: Manufacturer Profile will be used to educate small and medium size manufacturers (SMMs) so that they can learn and relate to the type of manufacturers that participated in this study.

Deliverable 2 – Defined/documented criteria for Benchmarking of Existing Cybersecurity Solutions

- Education: Defined/documented criteria for Benchmarking of Existing Cybersecurity Solutions will be used to educate SMMs and MxD community so that they can understand what needs to be considered and what criteria needs to be used to select cybersecurity tools that meet minimum criteria outlined by MxD institute

Deliverable 3 – List of tools evaluated

- Education: The list of tools evaluated will be used to educate SMMs and MxD community so that they can be aware of various commercial tools that can be leveraged to enable cybersecurity and maintain compliance with DFARS requirements and CMMC

Deliverable 4 – Criteria for selection of evaluated tool(s)

- Education: Criteria for selection of evaluated tool(s) will be used to educate SMMs and MxD community so that they can use appropriate criteria for selecting cybersecurity tools that meet minimum requirements as defined by MxD

Deliverable 5 – Report(s) on performance of benchmarked tool(s) based on established criteria

- Education: Report(s) on performance of benchmarked tool(s) based on established criteria will be used to educate SMMs and MxD community with example on how the developed criteria can be used to evaluate the performance of selected tools.

Deliverable 6 – De-Identified/Anonymized Results of vulnerability assessment and penetration test(s)

- Education: De-Identified/Anonymized Results of vulnerability assessment and penetration test(s) will be used to educate SMMs so that they can understand what type of outputs they should see from the cybersecurity tools evaluated in this project

Deliverable 7 – Prioritized recommendations

- Education: Prioritized recommendations will be used to educate SMMs on the type of recommendations they could see as a result of running such tools.

Deliverable 8 – Evaluation Scorecard

- Education: The Evaluation Scorecard will be used to provide examples to SMMs and MxD community regarding the results from the team's evaluation of tool(s) based on established criteria.

Deliverable 9 – Due Diligence Report

- Education: Due Diligence Report will be used to educate SMMs and MxD community with regard to the longer-term viability of vendor(s) for selected tools of this project.

Deliverable 10 – Installation and configuration guide for SiESTA

- Education: Installation and configuration guide for SiESTA will be used to educate SMMs and MxD community on the high level steps necessary for the installation and configuration of SiESTA

Deliverable 11 – Software guide for SiESTA

- Education: Software guide for SiESTA will be used to educate SMMs and MxD community so that they can understand SiESTA's software components.

Deliverable 12 – User guide for SiESTA

- Education: User guide for SiESTA will be used to educate SMMs and MxD community so that they can understand how to configure and use SiESTA.

Deliverable 13 – User training and DEMO for SiESTA

- Education: User training and DEMO for SiESTA will be used to educate SMMs and MxD community so that they can understand the operation and capabilities of SiESTA

Deliverable 14 – Guide for the SMMs regarding best practice considerations

- Education: Guide regarding best practice considerations will be used to educate SMMs so that they can select tools and develop or hire expertise needed to identify and mitigate cyberattacks

Deliverable 15 – Presentation slidedeck

- Education: The presentation slidedeck will be used to educate SMMs and MxD community about the scope, approach and lessons learned of the project

Deliverable 16 – Recorded Presentation

- Education: The recorded presentation will be used to educate SMMs and MxD community about the scope, approach and lessons learned of the project

Deliverable 17 – Final Report

- Education: The final report will be used to educate SMMs with regard to project roadmap, problems being tackled, goals and objectives, approach, results and lessons learned, including future areas of interest and research.

The deliverables and lessons learned will be transitioned using a series of venues including:

- Website and Social Media Posts
- Blogs
- White Papers
- Slide Decks
- Press Releases
- Webinars
- Presentations
- Testimonials
- Case Studies

To broaden the outreach of the transition, TechSolve will seek to leverage a number of partners such as

- Ohio MEP Cyber Work Group
- Ohio Cyber Collaboration Committee (OC3)
- NIST MEP Cyber Work Group
- National Cybersecurity Center of Excellence
- MEP Connect
- MEP University
- University of Cincinnati

VIII. ACKNOWLEDGEMENTS & DISCLAIMER

The Project Team would like to acknowledge the financial support and guidance received from the MxD Institute and the State of Ohio (Ohio Department of Development and Ohio MEP).

This effort was sponsored by the U.S. Government under Agreement number W15QKN19-3-0003 between the MXD USA and the Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

Although this project work was prepared with financial support from the State of Ohio, the content of this guide reflects the views of TechSolve and does not purport to reflect the views of Grantor and/or that of the State of Ohio.

IX. APPENDICES

Appendix A: Definitions

CMMC – Cybersecurity Maturity Model Certification

CUI – Controlled Unclassified Information

CVE – Common Vulnerability and Exposures

CSV file – delimited text file that uses a comma to separate values

EOL – End of Life

FCI – Federal Contract Information

FTP – File Transfer Protocol

GUI – Graphical User Interface

IIoT – Industrial Internet of Things

IT – Information Technology

MEP – Manufacturing Extension Partnership

NetBIOS – Network Basic Input/Output System

NIST – National Institute of Standards and Technology

OT – Operational Technology

PDF or Pdf or pdf file - portable document format file

PLC – Programmable Logic Controller

RCE – Remote Code Execution

RDP – Remote Desktop Protocol

SiESTA – Siemens Extensible Security Testing Appliance

SMB – Server Message Block

SMM – Small and Medium-size Manufacturer

SNMP – Simple Network Management Protocol

SSH – Secure Shell

SSL – Secure Sockets Layer

TLS – Transport Layer Security

VNC – Virtual Network Connection

Appendix B: Test Plan

Test Requirements

The test requirements have been outlined by the project goals and the capabilities of the selected cybersecurity tools. The following list summarizes the main considerations:

- Conduct tests that enable assessing the capabilities of the cybersecurity tools with regard to the minimum requirements outlined by MxD. The assessment will be run to validate the effectiveness of the benchmarking, identify solution gaps, and create best practice guidance.
- The tests will target both IT and OT. The team will carefully select the OT equipment, in agreement with the participating manufacturers, such that on one hand it is representative for this work, and on the other hand it will not jeopardize production or lead to losses due to (potential) temporary slowing down or disabling the equipment.
- It is preferable that connectivity exists between the IT and OT equipment. In case such connectivity does not exist, the team may temporarily connect to select OT equipment to perform individual scanning for assets with such connectivity capabilities.
- The test results will be captured in reports and will be de-identified and anonymized.
- The test results will be evaluated from the perspective of the NIST 800-171 controls identified as part of the Manufacturer Profile assessment tool development.

Prerequisites

Qualys

4. **Hardware** – One of the following systems will be needed in order to install the virtual scanner.
   d. Desktop/Laptop VMware Workstation, Player, Workstation Player, Fusion
   e. Client/Server VMware vSphere: vCenter Server, ESXi Citrix XenServer Microsoft Windows Server (Microsoft Hyper-V)
   f. Cloud Amazon EC2-Classic Amazon EC2-VPC Microsoft Azure Cloud Platform (ARM) Google Cloud Platform OpenStack OCI and OCI-Classic Alibaba Cloud Computer
5. **Virtual Scanner VM Requirements**
   d. Minimum- 1 x vCPU | 1.5 GB RAM | 1 x 40GB virtual HDD
   e. Recommended- 8 x vCPU | 16GB RAM | 1 x 40GB virtual HDD
   f. Internet connection to contact the Qualys server
6. **Qualys Account**
   c. The Virtual Scanner option must be turned on for your account.
   d. The user must be a Manager or sub-user with the “Manage virtual scanner appliances” permission.

SiESTA

2. **Hardware**
   e. Have a physical SiESTA box at the location
   f. Have at least two Ethernet cables, one for the management interface and one for scanning

g. Have an open power outlet to plug in the SiESTA box
h. Monitor and USB keyboard for initial network setup

SolarWinds NCM

2. **Hardware**
   b. Windows Server 2016/2019 Server. Windows 10 can be used for evaluation purposes only. This can be a VM.
      iii. Minimum Requirements: CPU Speed: 3GHz dual core processor | 6GB RAM | 30GB HDD Space
      iv. A separate SQL Server 2014/2016/2017/2019 or Azure SQL Database. The SQL Server needs to be on a separate physical drive. If you select the Lightweight Installation option, SQL Server Express 2017 is installed locally. This option should be used only for evaluating NCM.

Manufacturer Preparation

Qualys

4. Have two IP addresses ready for the TechSolve Employee's Laptop and Virtual Scanner. (This can be issued via DHCP)
5. Have a list of IP addresses that are in Scope/Out of Scope.
6. Have an Administrator Account ready (This is only necessary for a credentialed scan, i.e. a scan that can run as a logged in user. A credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.
7. Have an IT staff member available to assist with any technical issues related to accessing the SMM network.

SiESTA

6. Have an open port to plug the SiESTA box in to obtain an IP address. This can be a DHCP address.
7. Have an IP to assign to each Ethernet interface you want to use for scanning. These need to be statically assigned.
8. Have an IP address ready for the TechSolve Employee Laptop, which will be used to access the SiESTA.
9. Have a list of IP addresses that are in Scope/Out of Scope.
10. Have an Admin Account ready (This is only necessary for a credentialed scan, a credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.
11. Have an IT staff member available to assist with any technical issues related to accessing the SMM network.

SolarWinds NCM

4. Have two IP addresses ready for the TechSolve Employee's Laptop and Virtual Scanner. (This can be issued via DHCP)

5. Have a list of IP addresses that are in Scope/Out of Scope.
6. Have an Administrator Account ready (This is only necessary for a credentialed scan, a credentialed scan will provide more detailed information). The account would need to have elevated access to each asset being scanned.
7. Have an IT staff member available to assist with any technical issues related to accessing the SMM network.

TechSolve Preparation

Qualys

1. Have Qualys account setup and ready.
2. Have a Virtual Scanner Appliance Installed on a VM or the ISO for the SMM to setup the VM.
    - Refer to Qualys Application Scanner Installation Guide document

SiESTA

1. Connect SiESTA to network, monitor, keyboard, and power.
2. Confirm SiESTA gets an IP address for the management interface after boot completes. If static assignment is necessary, follow Setup Guide and on screen prompts to configure a static IP address.

SolarWinds NCM

1. Have a VM setup with NCM installed on laptop
2. Have an SQL Express Database setup on laptop

Onsite Tasks

Qualys

1. Gather networking information from the manufacturer
    a. IP addresses that are in scope/out of scope
    b. IP information for TechSolve’s laptop and Virtual Scanner
    c. Domain name
    d. Privileged account credentials that has elevated permissions to each asset that is being scanned (If SMM wants to do a credentialed scan)
2. Setup a Virtual Scanner Appliance for internal scanning
3. Complete the test scenarios in the Testing Protocol Document under Active Asset Discovery
4. Complete the test scenarios in the Testing Protocol Document under Network/Host Based Vulnerability Assessment scan
5. Complete the test scenarios in the Testing Protocol Document under Web Application Based Vulnerability Assessment scan (if you are testing a web app)
6. Complete the test scenarios in the Testing Protocol Document under Comprehensive Reporting capability

SiESTA

1. Gather networking information from the manufacturer
2. IP addresses that are in scope/out of scope
3. Connect the SiESTA box to the network and verify it has an IP address
4. Navigate to the web interface of the SiESTA via your laptop
5. Click Advanced and Continue to access the login portal
6. Complete the test scenarios in the Testing Protocol Document under Active Asset Discovery
7. Complete the test scenarios in the Testing Protocol Document under Comprehensive Reporting capability

SolarWinds NCM

1. Gather networking information from the manufacturer
    a. IP addresses that are in scope/out of scope
    b. IP information for TechSolve's laptop and SW Orion Server
    c. Domain name
    d. Privileged account credentials that has elevated permissions to each asset that is being scanned (If SMM wants to do a credentialed scan)
2. Setup the Orion Server/SQL Express Server
3. Complete the test scenarios in the Testing Protocol Document under Active Asset Discovery
4. Complete the test scenario in the Testing Protocol Document under Wireless Assessment
5. Complete the test scenarios in the Testing Protocol Document under Comprehensive Reporting capability.

What happens when we leave the site?

Qualys

1. If the Virtual Scanner Appliance is setup on one of TechSolve's laptops, this will need to remain secured on site (If the scan did not complete). If a SMM has setup the Virtual Scanner Appliance in their own VM, this will need to remain active over night while the scan takes place.

SolarwWinds NCM

1. Since Techsolve is not continuously monitoring the SMM's environment the laptop will be taken when the test is over.

SiESTA

1. Download all test results from SiESTA onto the TechSolve laptop.

Final Steps

Qualys

1. TechSolve will collect their equipment
2. Anonymize data
3. Remove agents on any devices if installed
4. TechSolve will provide the customer with a report of the scan
5. TechSolve will explain the details of the report
6. TechSolve will go over next steps.

SiESTA

1. Siemens will wipe the data from the SiESTA.
2. Siemens will power down SiESTA when complete.
3. TechSolve will collect the SiESTA equipment.
4. Siemens will collate the SiESTA reports on the TechSolve laptop.
5. TechSolve will provide the SiESTA report(s) to the customer.
6. Siemens and/or TechSolve will anonymize the data it retains.

SolarWinds NCM

1. TechSolve will collect their equipment
2. Anonymize data
3. Remove agents on any devices if installed
4. TechSolve will provide the customer with a report of the scan
5. TechSolve will explain the details of the report
6. TechSolve will go over next steps.

Appendix C: Manufacturer Profile Self-Assessment Line Items

Company	Associated Controls
Hires IT services (external)	N/A
Hires cybersecurity services (external)	N/A
Company is using own Cybersecurity tools (list them)	N/A
Hired Cybersecurity firm is using cybersecurity tools	N/A
Company follows one or more established frameworks or standards for cybersecurity	N/A
Company has conducted the NIST 800-171 assessment (Yes/No)	N/A
Company will need the CMMC certification	N/A
IT network is connected to OT network	N/A
Type of network segmentation	N/A
Company had significant cybersecurity incidents (Yes/No)	N/A

Technical Tools related to each of the following: please list all that are used	**Associated Controls**
Asset inventory and discovery (both HW and SW)	This is a CMMC 3 control, not in NIST 800-171
Endpoint protection / antivirus	3.14.1, 3.14.2, 3.14.4, 3.14.5
Firewall	3.13.6, 3.13.7, 3.13.15, 3.14.2, 3.14.6, 3.14.7
Identity and Access Management	3.3.2
- Do you allow the sharing of accounts between individuals?	3.3.2
VPN or other remote access capability	3.1.12, 3.1.13, 3.1.14, 3.1.15
Networking equipment and wireless access points	3.1.16, 3.1.17, 3.13.5
- Do you prevent access to Wifi before authorizing?	3.1.16
- Do you used authentication and encryption for Wi-Fi access?	3.1.17
SIEM, IPS, IDS or other monitoring tools	3.3.1, 3.14.7
- Do you analyze and review the logging results periodically?	3.3.1
- Do you retain logs for at least 30 days?	3.3.1
- Do you limit access to logs and to changing logs?	3.3.2, 3.3.8, 3.3.9
- Do you log changes to logs?	3.3.2
- Do you periodically review your logging policies and procedures?	3.3.3
- Are you alerted to logging failures?	3.3.4
- Do you have a process for reporting and investigation based on suspicious or unusual activity within logs?	3.3.5
- Do you have automated analysis and reporting of logs?	3.3.6
- Do you implement Network Time Protocol (NTP) or otherwise synchronize all system clocks to a standard time?	3.3.7
Allow or Denylisting software	3.4.8
Provide process documentation or description for each of these areas	**Associated Controls**
Configuration management tools	3.4.1, 3.4.2
- Are only those ports and protocols necessary to provide the service of the information system configured for that system?	3.4.7

- Are only applications and services that are needed for the function of the system configured and enabled?	3.4.7
- Are systems services reviewed to determine what is essential for the function of that system?	3.4.7
Baseline establishment tools	3.4.1, 3.4.5, 3.4.6
Change management	3.4.3, 3.4.4, 3.4.5, 3.4.9
Patch Management	3.14.1, 3.14.3, 3.14.4
- Do you install patches in a timely manner?	3.14.1, 3.14.4
Risk Management	3.11.1
- Do you periodically assess security controls to determine their effectiveness?	3.12.1
- Do you have a Plan of Action and Milestones (PoAM)	3.12.2
- Do you monitor security controls on an ongoing basis?	3.12.3
- Do you have a System Security Plan?	3.12.4
Vulnerability assessments	3.11.2
- Do you conduct vulnerability scans of your systems and network at a defined frequency?	3.11.2
- Do you prioritize remediation of vulnerabilities found during assessments?	3.11.3
- Do you correct flaws in a timely manner?	3.14.1

Appendix D: List of Tools

	Tool	**Company Information**	**Website**
1	SiESTA	Siemens 300 New Jersey Avenue, Suite 1000 Washington, D.C. 20001 United States 1-800-SIEMENS	https://new.siemens.com/
2	Solarwinds (SAM)	Solarwinds 7171 Southwest Parkway, Bldg 400 Austin, Texas 78735 1-866-530-8100	https://www.solarwinds.com/
3	Solarwinds (NCM)		https://www.solarwinds.com/
4	Solarwinds (SEM + NPM)		https://www.solarwinds.com/

5	Tenable OT	Tenable 7021 Columbia Gateway Drive Suite 500 Columbia, MD 21046 1-410-872-0555	https://www.tenable.com/
6	Nessus	Tenable 7021 Columbia Gateway Drive Suite 500 Columbia, MD 21046 1-410-872-0555	https://www.tenable.com/
7	Nmap	Nmap No Address fyodor@nmap.org	https://nmap.org/
8	OpenVAS	Greenbone Networks GmbH Neumarkt 12 49074 Osnabrück Germany	https://www.openvas.org/
9	Nikto	Cirt No Address Contact through site	https://cirt.net/
10	Continuous Threat Detection	Claroty 488 Madison, 11th Floor New York, NY 10022 Contact through site	https://www.claroty.com/
11	Guardian	Nozomi Networks 575 Market Street, Suite 3650 San Francisco, CA 94105 1-800-314-6114	https://www.nozominetworks.com/
12	beSecure	Beyond Security 2267 Lava Ridge Ct, Suite 100 Roseville, CA 95661 1-279-201-7150	https://beyondsecurity.com/
13	Vulnerability Manager Plus	ManageEngine 4141 Hacienda Drive, Pleasanton, CA 94588 1-925-924-9500	https://www.manageengine.com/
14	Intruder	Intruder 1-15 Clere St, London, EC2A 4UY, UK Contact through site	https://www.intruder.io/

15	Vulnerability Management Detection and Response	Qualys 919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 1-800-745-4355	https://www.qualys.com/
16	Netsparker Standard	Netsparker 220 Industrial Blvd Ste 102 Austin, TX 78745 Contact through site	https://www.netsparker.com/
17	PRTG Monitor	Paessler Thurn-und-Taxis-Str. 14, 90411 Nuremberg, Germany 49 911 93775-0	https://www.paessler.com/
18	Tripwire Industrial Visibility	Tripwire 308 SW Second Ave, Suite 400 Portland, OR 97204 503-276-7500	https://www.tripwire.com/
19	Verve	Verve Industrial 4124 Seven Hills Dr. Florissant, Missouri 63033, US 888-756-3251	https://verveindustrial.com/
20	Rapid7 Nexpose	GLOBAL HEADQUARTERS 120 Causeway Street Suite 400 Boston, MA 02114 1-617-247-1717	https://www.rapid7.com/
21	Acunetix	220 Industrial Blvd Suite 102 Austin, TX 78745 USA	https://www.acunetix.com/
22	CrowdStrike Falcon	150 Mathilda Place Sunnyvale, CA 94068 United States 1-888-512-8906	https://www.crowdstrike.com
23	Qualys Cloud platform (Qualysguard)	919 E Hillsdale Blvd, 4th Floor Foster City, CA 94404 1 (800) 745-4355	https://www.qualys.com/
24	Metasploit	GLOBAL HEADQUARTERS 120 Causeway Street Suite 400 Boston, MA 02114 1-866-772-7437	https://www.rapid7.com/

25	AlienVault USM	208 South Akard Street Dallas, TX 75201 1-214-666-8510	https://cybersecurity.att.com/
26	Tenable.io	7021 Columbia Gateway Drive Suite 500 Columbia, MD 21046 1 (410) 872-0555	https://www.tenable.com
27	LogicMonitor	820 State St. Floor 1 Santa Barbara, CA 93101 1-888-415-6442	https://www.logicmonitor.com/
28	Cisco DNA Center	170 West Tasman Dr. San Jose, CA 95134 USA 800-553-2447	https://www.cisco.com
29	ManageEngine OpManager	No Address 888-270-9500	https://www.manageengine.com/
30	Zabbix	4638 Bedford Ave, Brooklyn, NY 11235-2612, USA 877-4-ZABBIX	https://www.zabbix.com/
31	BreachLock	BreachLock Inc. 276 5th Avenue Suite 704 – 3031 New York NY 10001 1 917-779-0009	https://www.breachlock.com
32	Arctic Wolf	8939 Columbine Rd, Suite 150 Eden Prairie, MN 55347 888-272-8429	https://arcticwolf.com/
33	Wapiti	Nicolas Surribas http://devloop.users.sf.net/	https://wapiti.sourceforge.io

34	InsightVM	120 Causeway Street Suite 400 Boston, MA 02114 866-772-7437	https://www.rapid7.com/
35	Greenbone Vulnerability Manager	Greenbone Networks GmbH Neumarkt 12 49074 Osnabrück Germany 49-541-760278-0	https://www.greenbone.net/en/
36	MaxPatrol	8 Preobrazhenskaya Square, Moscow, 1070618 +7 495 744 01 44	https://www.ptsecurity.com/
37	Whitehat Sentinal Dynamic	1741 Technology Drive Suite #300 San Jose, CA 95110 408) 343-8350	https://www.whitehatsec.com/
38	GFI Langaurd	GFI Software 401 Congress Avenue Austin, Texas, US 78701 888-243-4329	https://www.gfi.com/
39	KICS	39A/2 Leningradskoe Shosse Moscow, 125212 Russian Federation 7-495-797-8700	https://ics.kaspersky.com/
40	FortiClient	No Address 408 542 7780	https://www.forticlient.com/
41	Outpost24 outscan	Sweden Skeppsbrokajen 8 371 33 Karlskrona 46 455 612 300	https://outpost24.com/
42	F-secure Radar	25 Independence Boulevard Suite 203 Warren, NJ 07059 USA 866 476 0216	https://www.f-secure.com/

43	Titania Nipper	Titania Security House Barbourne Road Worcester, WR1 1RS United Kingdom 44 (0)1905 888785	https://www.titania.com/
44	Kentik	Kentik Technologies, Inc. 548 Market St PMB 78595 San Francisco, CA 94104-5401 844-356-3278	https://www.kentik.com/
45	Catchpoint	150 West 30th Street, 3rd Floor New York, NY 10001 877-240-4450	https://www.catchpoint.com/
46	Sinefa	2445 Augustine Dr, Suite 150 Santa Clara, CA 95054 650 618 0183	https://www.sinefa.com/
47	Accedian Skylight	No Address Contact through site	https://go.accedian.com/
48	Camel360	CamelSecure 8600 NW 17th St # 140, Doral, FL 33126, EE. UU. +1 (786) 785-4654	https://camelsecure.com/
49	Armis	Armis Inc. 300 Hamilton, Suite500, Palo Alto, CA 94301	www.armis.com

Appendix E: Long-Term Vendor Viability Assessment Considerations

Year the company was established

All technology providers selected for this project have been in business for at least 13 years, with Siemens being the oldest (approx.1973) and Greenbone Networks GmbH being the youngest (2008). The time in business denotes a good level of maturity for each of the companies selected, which nevertheless should be considered relative to the other KPIs discussed next. For example, Greenbone has been in business for approximately 8 years; however, this is a 5 people company with two locations – one in Germany and one in UK.

Nevertheless, the reputation of their cybersecurity tool (OpenVAS) is very good and it provides a capable version free of charge.

Size of Company (no. of people)

The number of people at each company had significant variation. Qualys, SolarWinds, and Tenable Holdings have between approximately 900 and 2500 employees, which is a relatively large number, suggesting good business capabilities, infrastructure, and customer support.

Siemens Corporation had the highest number, significantly larger than any other provider selected for this project, with significant international presence.

Greenbone Networks GmbH has a small number of employees (5), which may be regarded as challenging for long-term viability. However, considering the relatively young age of the organization and the effectiveness of the tool, Greenbone may see a growth in the following years.

Nmap, a no-cost tool, has only 2 people listed so its ability to continue developing and maintaining their software is subject to risks. For this project, Nmap is part of SiESTA, which has a modular structure and can integrate various tools. Therefore, if one tool becomes obsolete or undesirable, it can be replaced with alternatives.

Public financials

Except for Nmap and Greenbone, all other providers displayed a high annual revenue. In case of Greenbone, although the total annual revenue was significantly smaller comparing with the other providers, the normalized amount ($/no. of people) was considered competitive.

In general, it is expected that larger companies will have a relatively large annual revenue. However, the balance between the number of people and revenue is usually preferred when estimating the long-term viability of a company.

Publicly Traded

The fact that a company is publicly traded is considered a relevant indicator because it provides an understanding of the level of maturity and business capabilities of that company. For example, Qualys, SolarWinds, Siemens and Tenable Holdings are all publicly traded companies, which in addition to the other characteristics suggests an increased level of maturity and sustainability. On the other hand, Greenbone Networks, is not publicly traded and it is smaller in size, which may result in a lower confidence for longer term viability.

Corporate Family

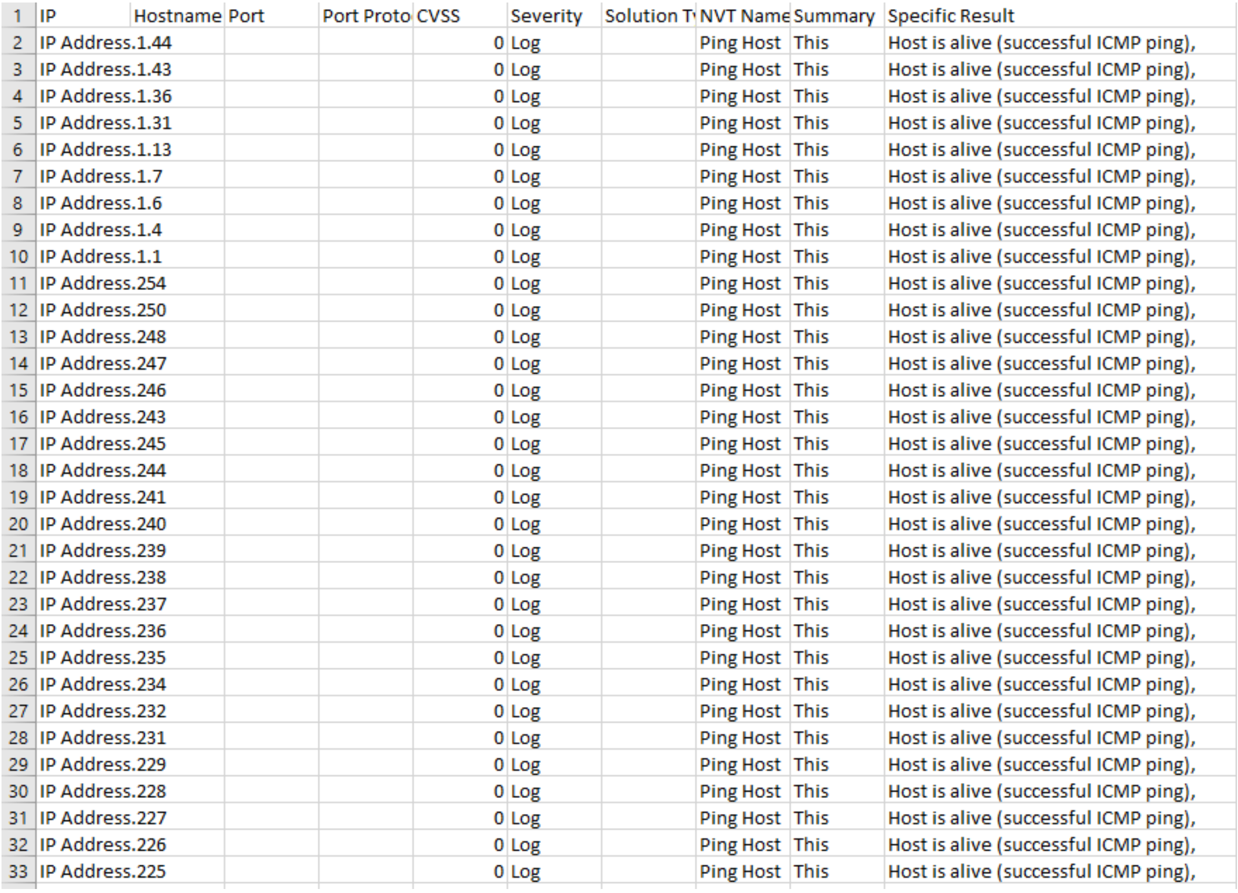
This indicator relates to the size of the organization and its presence nationally and internationally. For this project, with the exception of Nmap and Greenbone, all other companies have multiple branches. The availability of multiple branches nationally is related to the size of the company and suggest an increased ability to provide customer support throughout the country. Correlated with the age and the size of the company, multiple branches also suggest good business practice, services, and products and hence, long term viability.

Reputation / Notable Clients

The reputation of a company is important for the selection process with respect to its capabilities, customer support, and the customer base. For this project, all providers had good reputation at the time of selecting their respective tools. The news about SolarWinds hacks occurred later. Nevertheless, the selected SolarWinds tool continued to be used for the project considering the company has provided patches to address their platform's vulnerabilities.

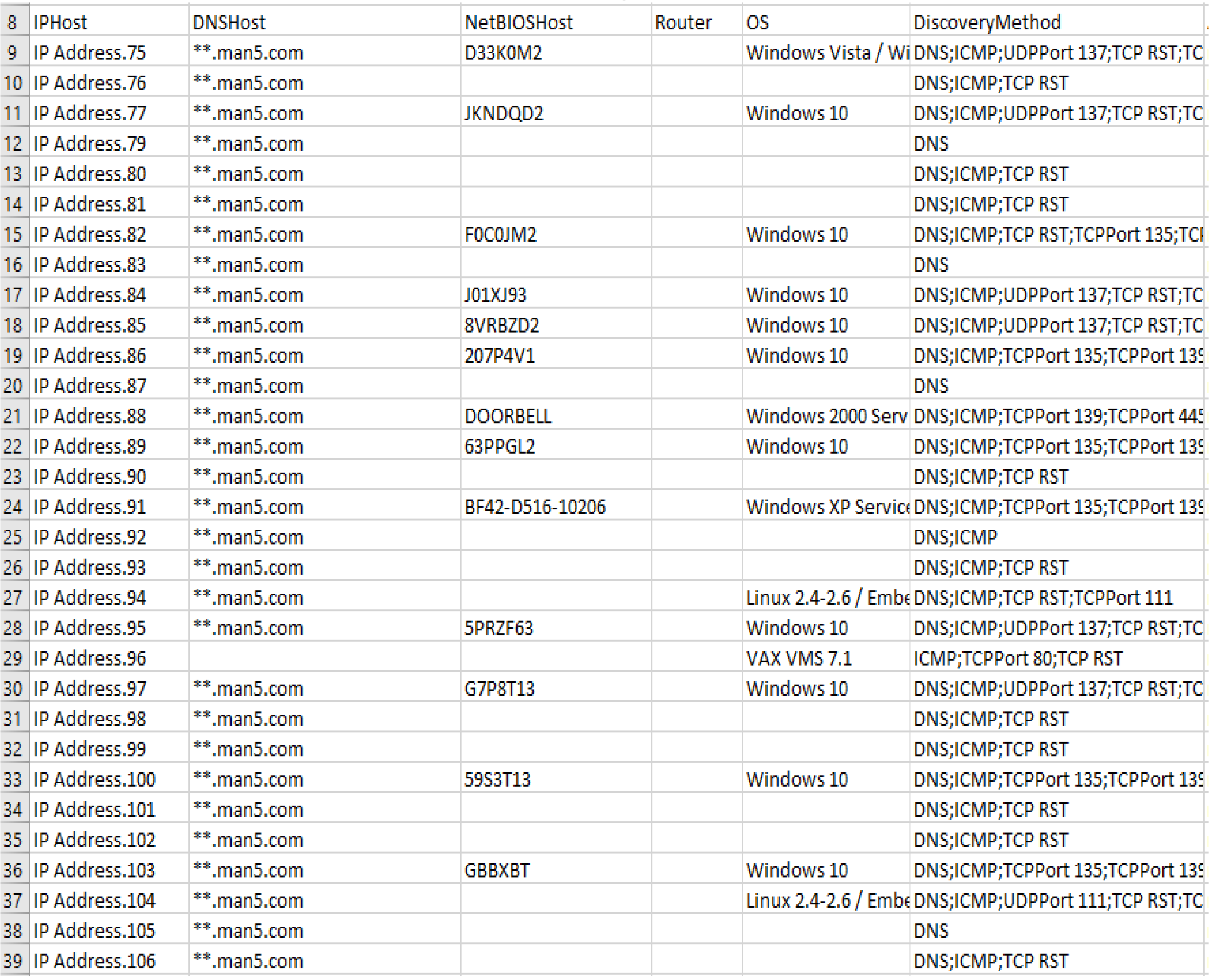
Appendix F: Samples of Asset Discovery Scan Results

OpenVAS



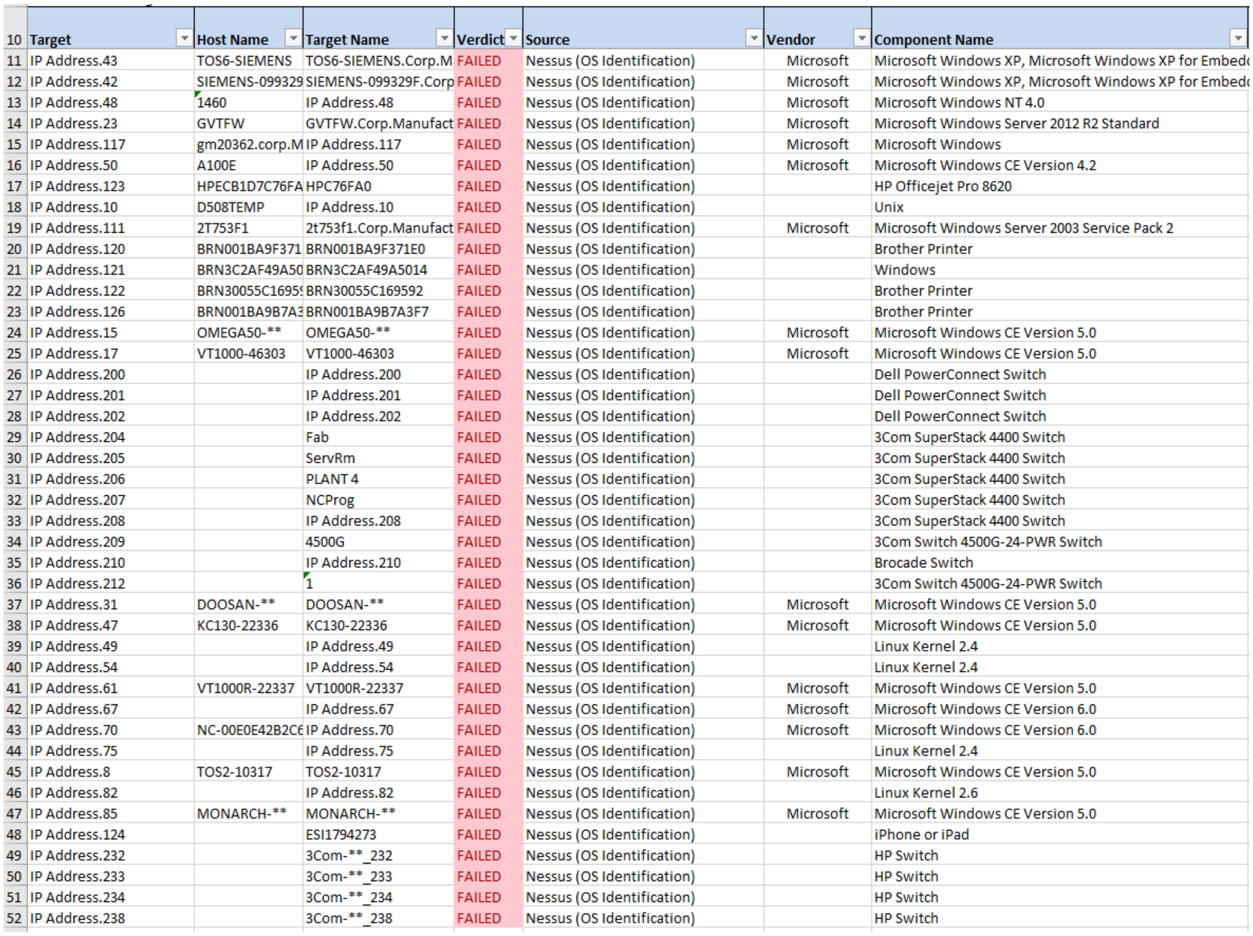
1	IP	Hostname	Port	Port Proto	CVSS	Severity	Solution T	NVT Name	Summary	Specific Result
2	IP Address.1.44				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
3	IP Address.1.43				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
4	IP Address.1.36				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
5	IP Address.1.31				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
6	IP Address.1.13				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
7	IP Address.1.7				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
8	IP Address.1.6				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
9	IP Address.1.4				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
10	IP Address.1.1				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
11	IP Address.254				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
12	IP Address.250				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
13	IP Address.248				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
14	IP Address.247				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
15	IP Address.246				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
16	IP Address.243				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
17	IP Address.245				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
18	IP Address.244				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
19	IP Address.241				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
20	IP Address.240				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
21	IP Address.239				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
22	IP Address.238				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
23	IP Address.237				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
24	IP Address.236				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
25	IP Address.235				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
26	IP Address.234				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
27	IP Address.232				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
28	IP Address.231				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
29	IP Address.229				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
30	IP Address.228				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
31	IP Address.227				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
32	IP Address.226				0	Log		Ping Host	This	Host is alive (successful ICMP ping),
33	IP Address.225				0	Log		Ping Host	This	Host is alive (successful ICMP ping),

Qualys



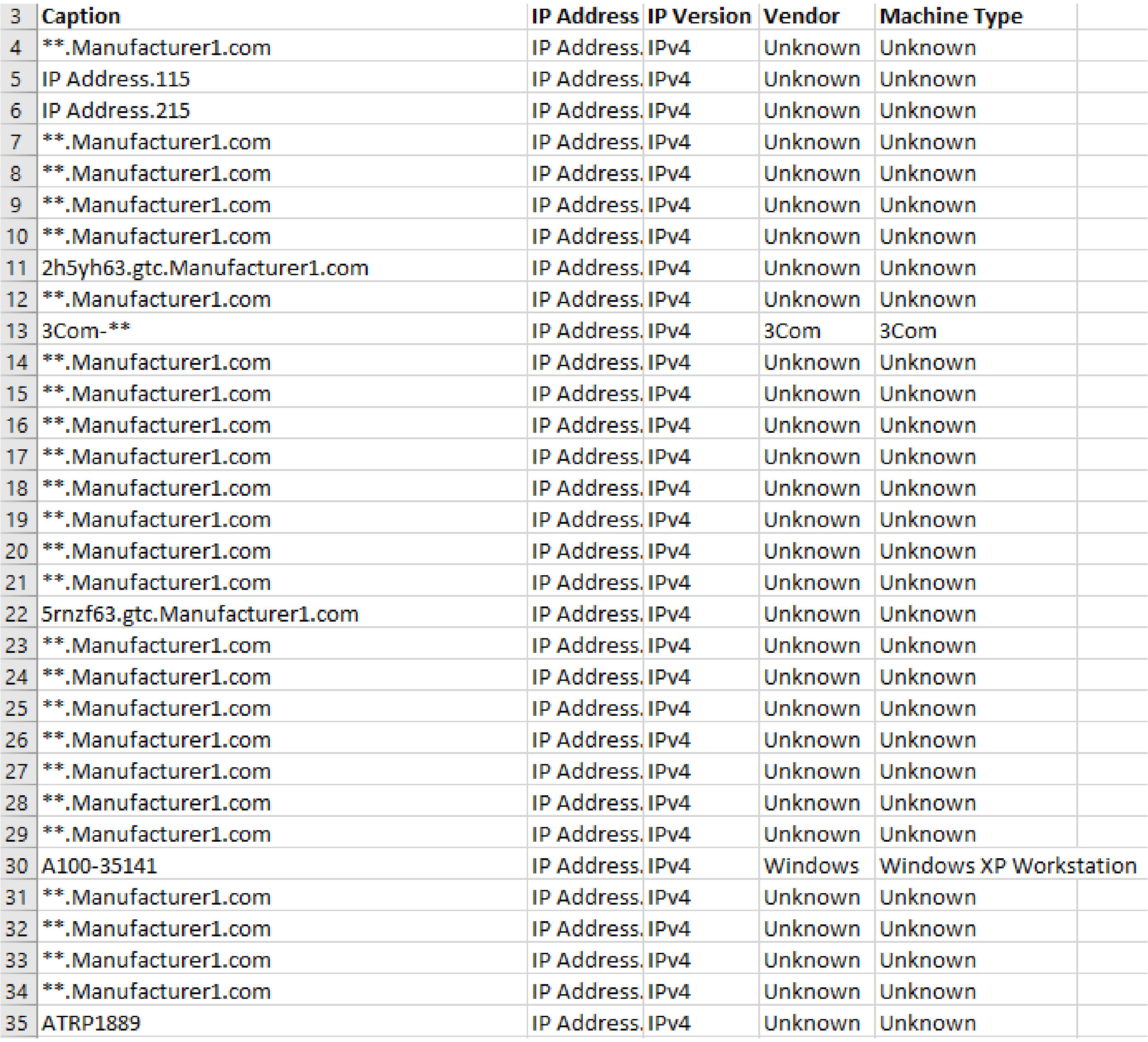
8	IPHost	DNSHost	NetBIOSHost	Router	OS	DiscoveryMethod
9	IP Address.75	**.man5.com	D33K0M2		Windows Vista / Wi	DNS;ICMP;UDPPort 137;TCP RST;TC
10	IP Address.76	**.man5.com				DNS;ICMP;TCP RST
11	IP Address.77	**.man5.com	JKNDQD2		Windows 10	DNS;ICMP;UDPPort 137;TCP RST;TC
12	IP Address.79	**.man5.com				DNS
13	IP Address.80	**.man5.com				DNS;ICMP;TCP RST
14	IP Address.81	**.man5.com				DNS;ICMP;TCP RST
15	IP Address.82	**.man5.com	F0C0JM2		Windows 10	DNS;ICMP;TCP RST;TCPPort 135;TCP
16	IP Address.83	**.man5.com				DNS
17	IP Address.84	**.man5.com	J01XJ93		Windows 10	DNS;ICMP;UDPPort 137;TCP RST;TC
18	IP Address.85	**.man5.com	8VRBZD2		Windows 10	DNS;ICMP;UDPPort 137;TCP RST;TC
19	IP Address.86	**.man5.com	207P4V1		Windows 10	DNS;ICMP;TCPPort 135;TCPPort 139
20	IP Address.87	**.man5.com				DNS
21	IP Address.88	**.man5.com	DOORBELL		Windows 2000 Serv	DNS;ICMP;TCPPort 139;TCPPort 445
22	IP Address.89	**.man5.com	63PPGL2		Windows 10	DNS;ICMP;TCPPort 135;TCPPort 139
23	IP Address.90	**.man5.com				DNS;ICMP;TCP RST
24	IP Address.91	**.man5.com	BF42-D516-10206		Windows XP Service	DNS;ICMP;TCPPort 135;TCPPort 139
25	IP Address.92	**.man5.com				DNS;ICMP
26	IP Address.93	**.man5.com				DNS;ICMP;TCP RST
27	IP Address.94	**.man5.com			Linux 2.4-2.6 / Embe	DNS;ICMP;TCP RST;TCPPort 111
28	IP Address.95	**.man5.com	5PRZF63		Windows 10	DNS;ICMP;UDPPort 137;TCP RST;TC
29	IP Address.96				VAX VMS 7.1	ICMP;TCPPort 80;TCP RST
30	IP Address.97	**.man5.com	G7P8T13		Windows 10	DNS;ICMP;UDPPort 137;TCP RST;TC
31	IP Address.98	**.man5.com				DNS;ICMP;TCP RST
32	IP Address.99	**.man5.com				DNS;ICMP;TCP RST
33	IP Address.100	**.man5.com	59S3T13		Windows 10	DNS;ICMP;TCPPort 135;TCPPort 139
34	IP Address.101	**.man5.com				DNS;ICMP;TCP RST
35	IP Address.102	**.man5.com				DNS;ICMP;TCP RST
36	IP Address.103	**.man5.com	GBBXBT		Windows 10	DNS;ICMP;TCPPort 135;TCPPort 139
37	IP Address.104	**.man5.com			Linux 2.4-2.6 / Embe	DNS;ICMP;UDPPort 111;TCP RST;TC
38	IP Address.105	**.man5.com				DNS
39	IP Address.106	**.man5.com				DNS;ICMP;TCP RST

SiESTA



10	Target	Host Name	Target Name	Verdict	Source	Vendor	Component Name
11	IP Address.43	TOS6-SIEMENS	TOS6-SIEMENS.Corp.M	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows XP, Microsoft Windows XP for Embed
12	IP Address.42	SIEMENS-099329	SIEMENS-099329F.Corp	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows XP, Microsoft Windows XP for Embed
13	IP Address.48	1460	IP Address.48	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows NT 4.0
14	IP Address.23	GVTFW	GVTFW.Corp.Manufact	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows Server 2012 R2 Standard
15	IP Address.117	gm20362.corp.M	IP Address.117	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows
16	IP Address.50	A100E	IP Address.50	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 4.2
17	IP Address.123	HPECB1D7C76FA	HPC76FA0	FAILED	Nessus (OS Identification)		HP Officejet Pro 8620
18	IP Address.10	D508TEMP	IP Address.10	FAILED	Nessus (OS Identification)		Unix
19	IP Address.111	2T753F1	2t753f1.Corp.Manufact	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows Server 2003 Service Pack 2
20	IP Address.120	BRN001BA9F371	BRN001BA9F371E0	FAILED	Nessus (OS Identification)		Brother Printer
21	IP Address.121	BRN3C2AF49A50	BRN3C2AF49A5014	FAILED	Nessus (OS Identification)		Windows
22	IP Address.122	BRN30055C1695	BRN30055C169592	FAILED	Nessus (OS Identification)		Brother Printer
23	IP Address.126	BRN001BA9B7A3	BRN001BA9B7A3F7	FAILED	Nessus (OS Identification)		Brother Printer
24	IP Address.15	OMEGA50-**	OMEGA50-**	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
25	IP Address.17	VT1000-46303	VT1000-46303	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
26	IP Address.200		IP Address.200	FAILED	Nessus (OS Identification)		Dell PowerConnect Switch
27	IP Address.201		IP Address.201	FAILED	Nessus (OS Identification)		Dell PowerConnect Switch
28	IP Address.202		IP Address.202	FAILED	Nessus (OS Identification)		Dell PowerConnect Switch
29	IP Address.204		Fab	FAILED	Nessus (OS Identification)		3Com SuperStack 4400 Switch
30	IP Address.205		ServRm	FAILED	Nessus (OS Identification)		3Com SuperStack 4400 Switch
31	IP Address.206		PLANT 4	FAILED	Nessus (OS Identification)		3Com SuperStack 4400 Switch
32	IP Address.207		NCProg	FAILED	Nessus (OS Identification)		3Com SuperStack 4400 Switch
33	IP Address.208		IP Address.208	FAILED	Nessus (OS Identification)		3Com SuperStack 4400 Switch
34	IP Address.209		4500G	FAILED	Nessus (OS Identification)		3Com Switch 4500G-24-PWR Switch
35	IP Address.210		IP Address.210	FAILED	Nessus (OS Identification)		Brocade Switch
36	IP Address.212		1	FAILED	Nessus (OS Identification)		3Com Switch 4500G-24-PWR Switch
37	IP Address.31	DOOSAN-**	DOOSAN-**	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
38	IP Address.47	KC130-22336	KC130-22336	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
39	IP Address.49		IP Address.49	FAILED	Nessus (OS Identification)		Linux Kernel 2.4
40	IP Address.54		IP Address.54	FAILED	Nessus (OS Identification)		Linux Kernel 2.4
41	IP Address.61	VT1000R-22337	VT1000R-22337	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
42	IP Address.67		IP Address.67	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 6.0
43	IP Address.70	NC-00E0E42B2C	IP Address.70	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 6.0
44	IP Address.75		IP Address.75	FAILED	Nessus (OS Identification)		Linux Kernel 2.4
45	IP Address.8	TOS2-10317	TOS2-10317	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
46	IP Address.82		IP Address.82	FAILED	Nessus (OS Identification)		Linux Kernel 2.6
47	IP Address.85	MONARCH-**	MONARCH-**	FAILED	Nessus (OS Identification)	Microsoft	Microsoft Windows CE Version 5.0
48	IP Address.124		ESI1794273	FAILED	Nessus (OS Identification)		iPhone or iPad
49	IP Address.232		3Com-**_232	FAILED	Nessus (OS Identification)		HP Switch
50	IP Address.233		3Com-**_233	FAILED	Nessus (OS Identification)		HP Switch
51	IP Address.234		3Com-**_234	FAILED	Nessus (OS Identification)		HP Switch
52	IP Address.238		3Com-**_238	FAILED	Nessus (OS Identification)		HP Switch

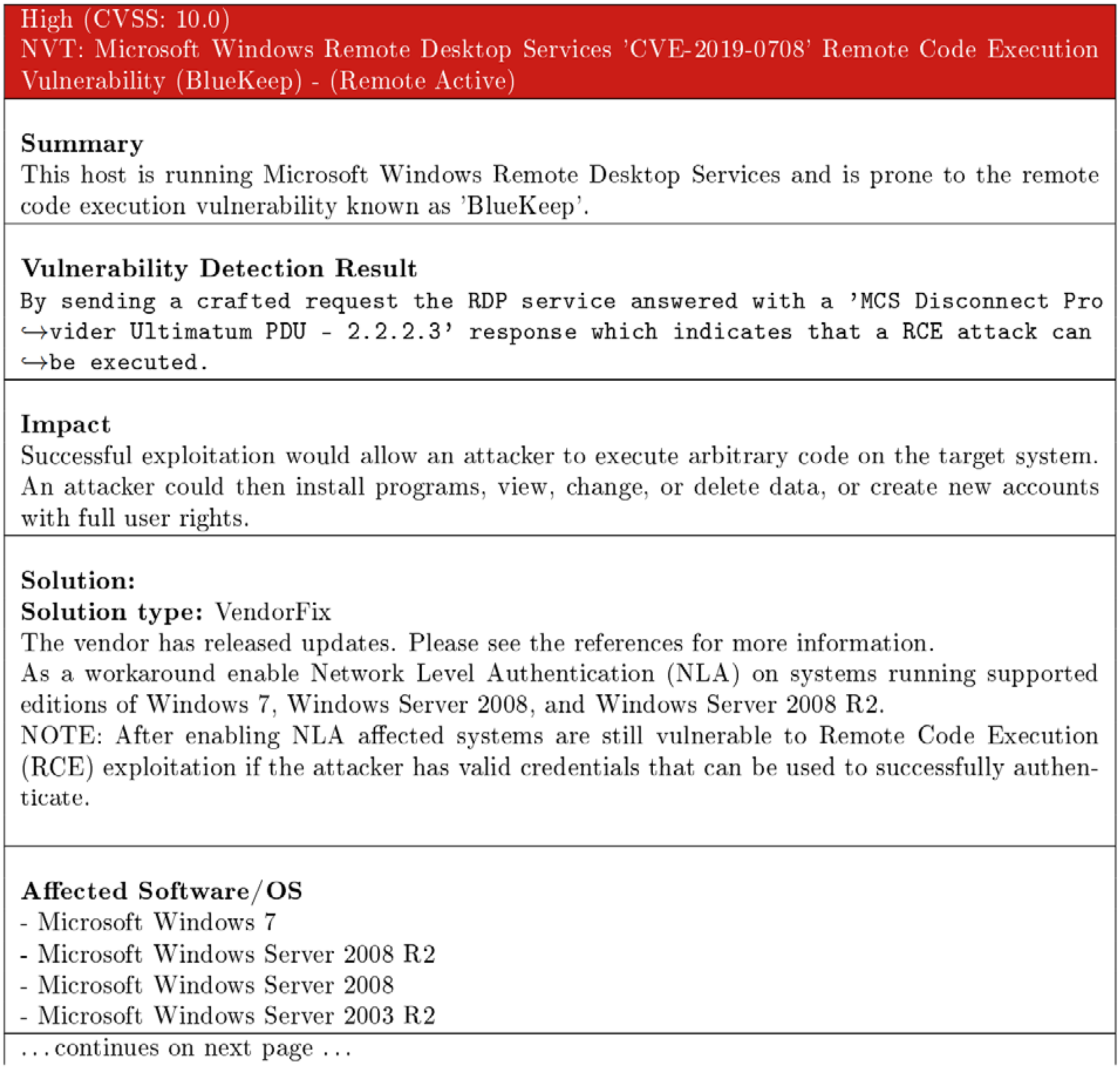
Solarwinds NCM



3	Caption	IP Address	IP Version	Vendor	Machine Type
4	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
5	IP Address.115	IP Address.	IPv4	Unknown	Unknown
6	IP Address.215	IP Address.	IPv4	Unknown	Unknown
7	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
8	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
9	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
10	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
11	2h5yh63.gtc.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
12	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
13	3Com-**	IP Address.	IPv4	3Com	3Com
14	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
15	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
16	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
17	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
18	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
19	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
20	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
21	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
22	5rnzf63.gtc.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
23	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
24	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
25	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
26	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
27	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
28	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
29	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
30	A100-35141	IP Address.	IPv4	Windows	Windows XP Workstation
31	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
32	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
33	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
34	**.Manufacturer1.com	IP Address.	IPv4	Unknown	Unknown
35	ATRP1889	IP Address.	IPv4	Unknown	Unknown

Appendix G: Vulnerability Details Sample

OpenVAS



High (CVSS: 10.0)
NVT: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)

Summary
This host is running Microsoft Windows Remote Desktop Services and is prone to the remote code execution vulnerability known as 'BlueKeep'.

Vulnerability Detection Result

```
By sending a crafted request the RDP service answered with a 'MCS Disconnect Pro
↪vider Ultimatum PDU - 2.2.2.3' response which indicates that a RCE attack can
↪be executed.
```

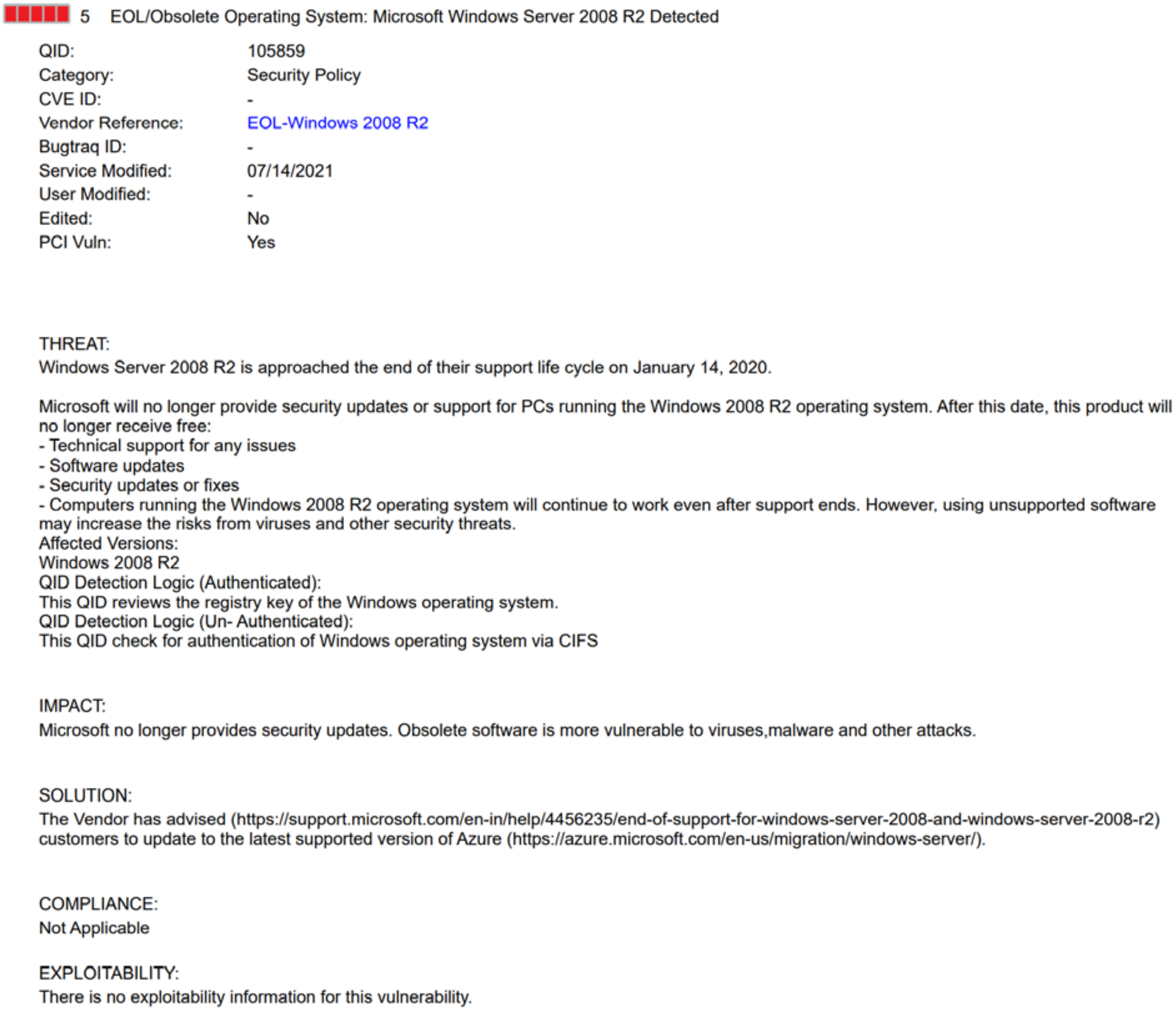
Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.
As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.
NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Affected Software/OS
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 R2

. . . continues on next page . . .

Qualys



🟥🟥🟥🟥🟥 5 EOL/Obsolete Operating System: Microsoft Windows Server 2008 R2 Detected

QID:	105859
Category:	Security Policy
CVE ID:	-
Vendor Reference:	EOL-Windows 2008 R2
Bugtraq ID:	-
Service Modified:	07/14/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Windows Server 2008 R2 is approached the end of their support life cycle on January 14, 2020.

Microsoft will no longer provide security updates or support for PCs running the Windows 2008 R2 operating system. After this date, this product will no longer receive free:
- Technical support for any issues
- Software updates
- Security updates or fixes
- Computers running the Windows 2008 R2 operating system will continue to work even after support ends. However, using unsupported software may increase the risks from viruses and other security threats.
Affected Versions:
Windows 2008 R2
QID Detection Logic (Authenticated):
This QID reviews the registry key of the Windows operating system.
QID Detection Logic (Un- Authenticated):
This QID check for authentication of Windows operating system via CIFS

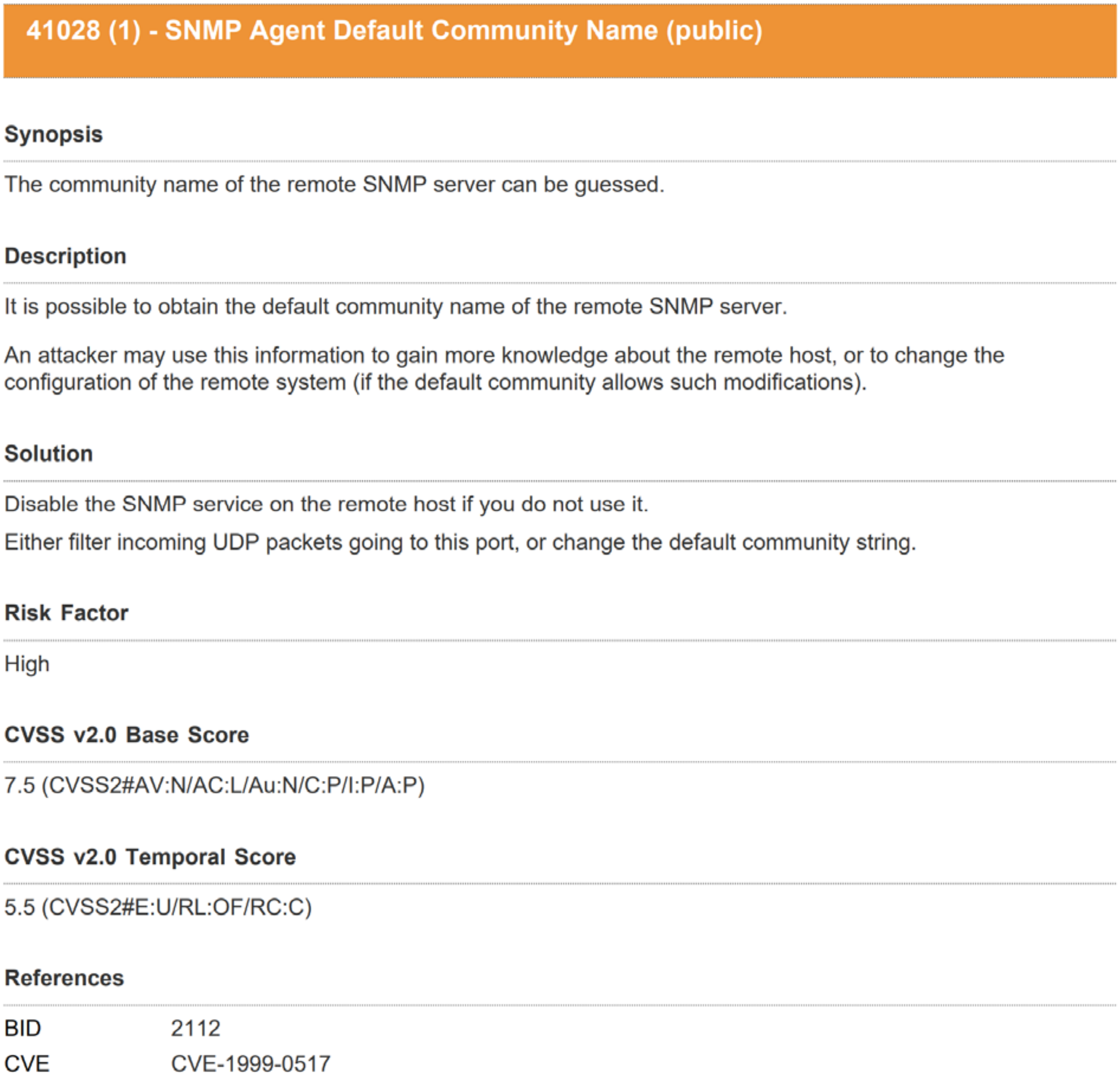
IMPACT:
Microsoft no longer provides security updates. Obsolete software is more vulnerable to viruses,malware and other attacks.

SOLUTION:
The Vendor has advised (https://support.microsoft.com/en-in/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2) customers to update to the latest supported version of Azure (https://azure.microsoft.com/en-us/migration/windows-server/).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

SiESTA (Raw Report from Nessus)



41028 (1) - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2112
CVE	CVE-1999-0517

Note: SolarWinds NCM did not find any vulnerabilities in the testing and therefore has no output to display.