Ana's Cloud
Specialists in Cloud and Management Services

Cybersecurity Vulnerability Executive Summary

Client A

July 15, 2025

Lawrence Furman
LarryF@AnasCloud.com
732-580-0024

Cybersecurity Vulnerability – Executive Summary

In May and June 2025, Ana's Cloud conducted a preliminary CyberSecurity assessment of Client_A's computers and network. We evaluated the computers in the network using a suite of tools, some commercial and others developed in-house. We also used Large Language Models, LLMs, and AI enabled tools including ChatGPT and Microsoft Copilot.

This document is a redacted and anonymized version of the report. All identifying information such as system names and IP addresses and explicit references to the Client have been deleted.

Our Process

Our process includes anonymizing identifying information such as system names and IP address when using MS Copilot and other AI enabled tools. IP addresses are anonymized by using the fourth or third and fourth octets of the IPv4 Address. So 192.168.0.16 would be rendered as x.y.0.16 or x.y.z.16.

The Results

The results of the security vulnerability reports are nuanced. The scans, whether Ana's Cloud's tools or the Greenbone analysis are based on both uncredentialed and credentialed scans of each endpoint within the networks we are allowed to scan. These are nodes or hosts on the network where the user account with which the scan is based has sufficient rights, not simply to log on to the host but also run the scan.

Recommendations

Based on the results of this survey, we recommend the following.

1. Maintain current and supported versions of MS Windows to allow new security patches from Microsoft on all computers within the network.

    1. PCs. Client_A has PCs running Windows 7 Enterprise, Windows 10 Pro, and Windows 11 Pro. Microsoft discontinued support for Windows 7 on January 14, 2020. Microsoft has also announced plans to discontinue support for Windows 10 on October 14, 2025.

        1. Client_A should replace all computers running Windows 7 with computers running Windows 11.

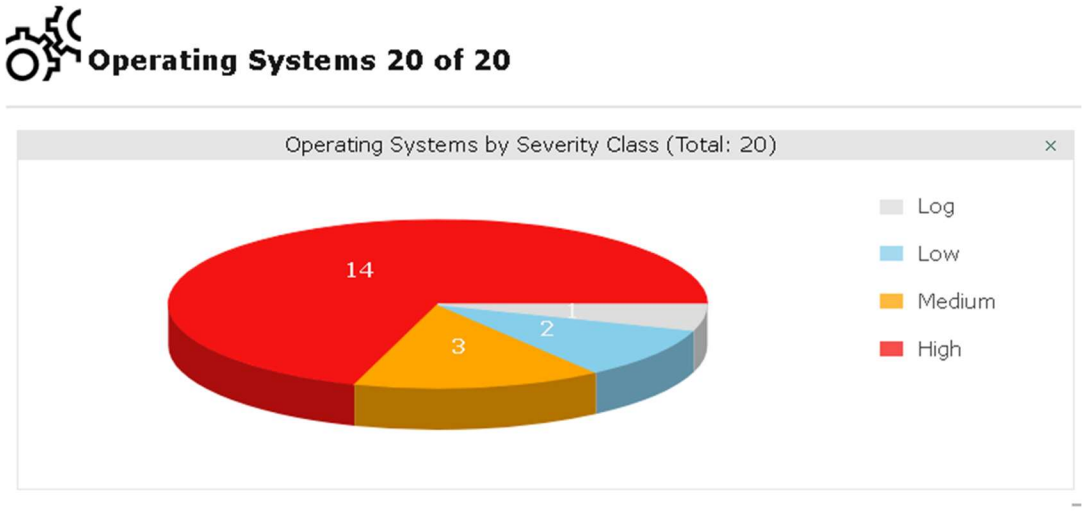
        2. Client_A should either replace the computers running Windows 10 with new computers running Windows 11 or upgrade Windows 10 to Windows 11. ***And it should do this before October 14, 2025.***

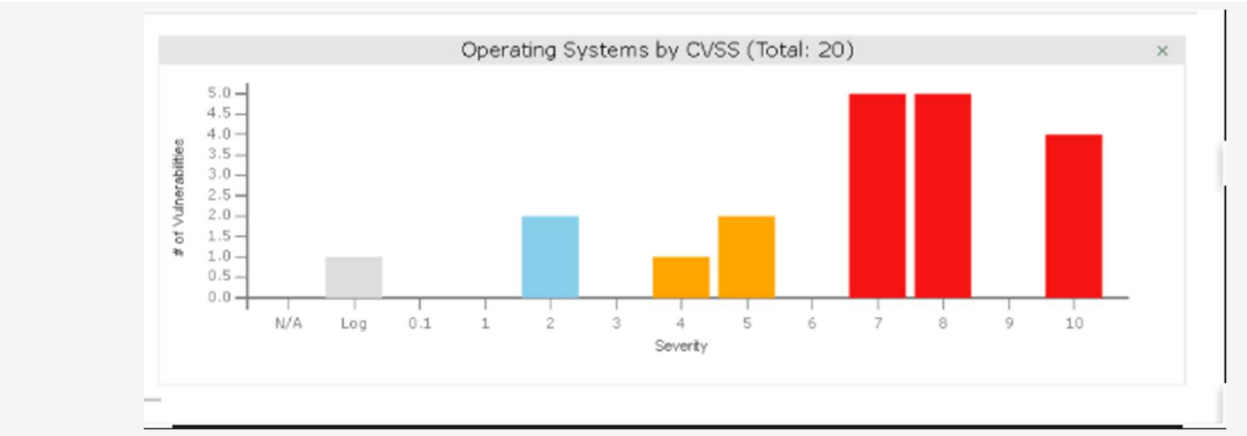
2. Servers. Client_A has computers running Windows Server versions 2003, 2008, 2012, 2016, 2019, and 2022.

    1. Microsoft has discontinued support for Windows Server versions 2003, 2008, and 2012. Therefore, Client_A should plan to migrate the applications on the computers running Windows Server versions 2003, 2008, and 2012, to computers running Windows Server 2022 as soon as possible. This includes SAS_SVR, running Windows 2003, eight servers running Windows Server 2008 R2. These are listed in Client_A-AD-local-Computers.xlsx and EOL-Online-Computers.PNG.

    2. Microsoft has also announced plans to discontinue support for Windows 2016 on January 12, 2027. Therefore, Client_A should also plan to migrate the applications on computers running Windows Server 2016 before January 12, 2027.

    3. Server operating systems. These graphs show server vulnerabilities by operating system. The images are taken from the attached file, "CLIENT_A-x.y.z-distribution-image.png".





1. In both graphs above, "Log" represented in gray, indicates one server with a current and supported operating system. a severity of less than 0.1.

2. "Low," a severity of 2, represented by light blue, shows two servers with a severity of 2.

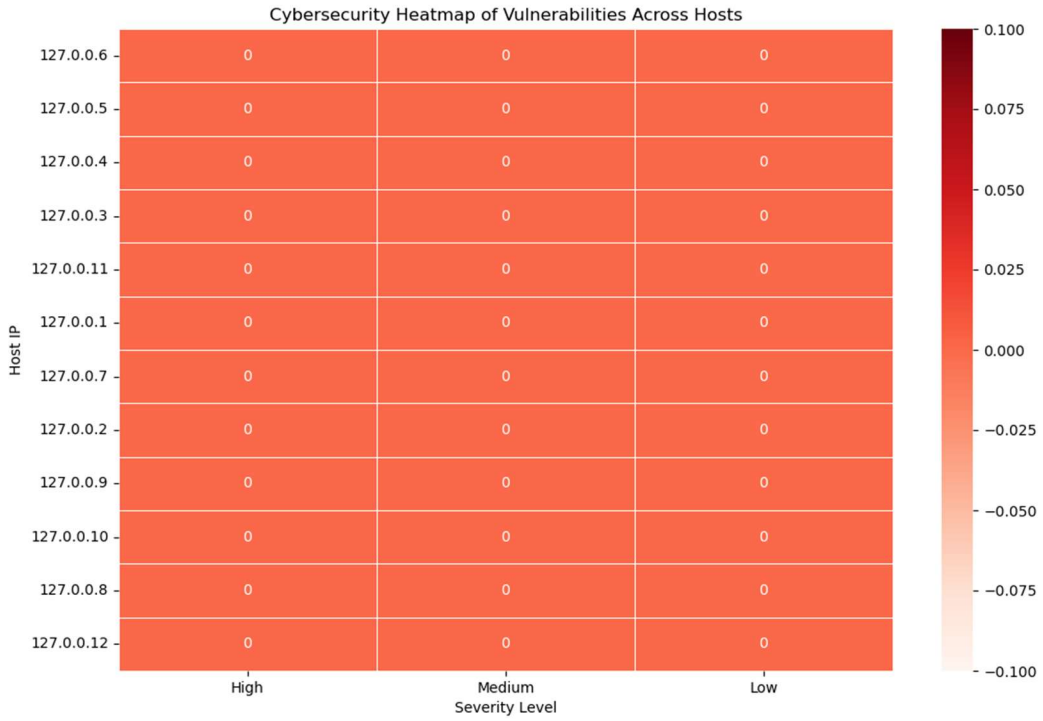
3. "Medium," in orange, shows one server with a severity of 4 and two servers with a severity of 5.

4. "High," in red, shows five servers with a severity of 7, five with a severity of 8, and four with a severity of 10.

4. The file EOL-Online-Computers.png, part of which is reproduced below shows:

    1. The rows in a regular, non-bolded type, shows the one server running Windows Server 2016 and 2022.

    2. The rows with a yellow background show computers running Windows Server versions 2008 R2, 2012 R2, 2016, and 2022.
        1. Server versions 2016 and 2022 are current and supported.
        2. Server 2008 and 2012 are obsolete and should be phased out as soon as possible. AA_ mission critical applications on these servers should be moved to physical or virtual servers running modern, supported operating systems.



3. The eight (8) rows in bold-faced type show computers running Windows Server 2012 R2. These may be upgradable to Windows Server 2016, and potentially to Windows Server 2019. Note that Microsoft will end "Extended Support" for Server 2016 on January 12, 2027. However, they may be very old and fragile hardware, which use significantly more power and require more air conditioning capacity than contemporary physical or virtual servers. They also may also have relatively slow processors with few cores, low capacity hard drives, less than optimal RAM. It may be easier and more cost effective to migrate the applications to several virtualization hosts.

Server Data

Name	OS Name	OS Ver	IP v4
A_SQL11	Windows Server 2022 Datacenter	10.0 (20348)	x.y.z.15
A_Web16	Windows Server 2016 Datacenter	10.0 (14393)	x.y.z.16
A_SAS09	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.96**
A_WSUS04	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.55**
A_PYTHN06	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.97**
A_STAF10	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.3**
A_CYBER05	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.40**

A_Web17	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.17**
A_Web18	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.25**
A_Web19	**Windows Server 2012 R2 Standard**	**6.3 (9600)**	**x.y.z.20**
EU_B01	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.35
A_SQL06	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.9
A_Web04	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.12
A_QL03	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.14
A_TS14	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.24
A_TS15	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.21
A_Web06	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.13
A_SQL07	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.17
A_SAS08	Windows Server 2008 R2 Standard	6.1 (7601)	x.y.z.95

Table 1, Servers

2. Clean up Active Directory.
    1. Remove accounts that are no longer in use.
    2. Verify that users can only access the systems and data they need.
    3. Annual audits of user permissions and administrative access.

3. Local Administrator's Groups.

    1. Client_A should audit Local Administrator's Groups on all servers,
    2. Client_A should restrict Administrative access to Domain Administrators.

4. Server Message Block, SMB.

    1. There are three (3) versions of the SMB file sharing protocol, SMB 1, SMB 2, and SMB 3. SMB 1 and SMB 2 are not secure communications protocols. SMB 3 is a secure communications protocol when encryption and signing are enabled.
    2. Various servers at Client_A have SMB 1, SMB 2 and SMB 3enabled, however do not have encryption or signing enabled.
    3. Refer to A_SAS.SystemInfoAndUpdates.txt and A_Solm01.old.SystemInfoAndUpdates.txt.

5. Multiple issues with various computers, described in the file "Client_A-x.y.z-report-ef829fc6.txt"

    1. A_SAS09, 173 high issues.
    2. A_STAF10, 135 high issues
    3. A_Python06, 179 high issues.
    4. A_WSUS04, 254 high issues.
    5. A_CYBER05, 253 high issues.
    6. A_WEB18, 2 high issues.

7. A_DC02, 2 high issues.
8. A_SQL07, 1 high issue.

6. A subset of workstations are listed in Table 2, Basic Workstation Details, and Table 3, Windows 11 Compatibility for a subset of computers. Full test results include basic data and Windows 11 compatibility for all workstations in the environment.

    1. Table 2 shows the workstation name, current operating system, computer model, processor, number of CPUs, CPU Cores, amount of RAM, whether the drive is a spinning disk, or hard Disk, or Solid State Drive, and the drive capacity. Serial Numbers, User Names, and IPv4 addresses are redacted.

Basic Details

Name	Current OS	Model	Processor	CPUs	Cores	RAM	HD/SSD	Disk Size
WKS-02	W 10 Pro 22H	OptiPlex 9020	i7-4790 3.60GHz	1	4	8	SSD	465.76
WKS-03	W 10 Pro 22H	OptiPlex 9020	i5-4590 3.30GHz	1	4	8	SSD	465.76
WKS-17	W 10 Pro 22H	OptiPlex 9020	i7-4790 3.60GHz	1	4	8	SSD	931
WKS-18	W 10 Pro 22H	OptiPlex 9020	i7-4790 3.60GHz	1	4	8	SSD	465.76
WKS-26	W 10 Pro 22H	OptiPlex 9020	i7-4790 3.60GHz	1	4	8	SSD	465.76
WKS-27	W 7 Pro 6.1	OptiPlex 3010	i5-3450 3.10GHz	1	4	8	HD	465.76
WKS-01	W 10 Pro 22H	OptiPlex 7090	i7-11700 @ 2.50GHz	1	8	16	SSD	931.51
WKS-04	W 10 Pro 22H	OptiPlex 7000	i7-12700T	1	12	16	SSD	476.94
WKS-08	W 10 Pro 22H	OptiPlex 7000	i7-12700	1	12	16	SSD	476.94
WKS-11	W 10 Pro 22H	OptiPlex 3000	i7-4790 3.60GHz	1	6	16	SSD	238.47
WKS-15	W 10 Pro 22H	OptiPlex 9020	i7-4790 3.60GHz	1	4	8	SSD	256.17
WKS-16	W 10 Pro 22H	Inspiron 3793	i7-1065G7 1.30GHz	1	4	16	SSD	476.94
WKS-23	W 10 Pro 22H	OptiPlex 3080	i5-10500 3.10GHz	1	6	32	SSD	465.76

Table 2, Workstations, Basic Data

    2. Table 3 shows the results of the Windows 11 Compatibility test for the same set of workstations. The test looks at CPU, Disk, Disk free space, RAM, the presence of a TPM chip, the capability of Secure Boot, and suggests next steps.

        1. The computers in green passed the compatibility test, and can be upgraded to Windows Pro 11.

        2. The computers in red are not compatible with Windows 11 and must be replaced. In one case, WKS-17 has a 1 TB SSD which can be reused.

        3. The computers in yellow did not pass the test, but can be retested after certain actions are taken. These include reseting the system clock, turning on secure boot, and freeing space on the disk or replacing the disk with one with greater capacity.

Windows 11 Compatibility

Name	Compatible	CPU	Disk	Free Space	RAM	TPM	Sec boot	Recommendations
WKS-02	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-03	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-17	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace and reuse disk.
WKS-18	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-26	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-27	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-01	No	Fail	Pass	Pass	Pass	Fail	Fail	Replace
WKS-04	Yes	Pass	Pass	Pass	Pass	Pass	Pass	Upgrade
WKS-08	Yes	Pass	Pass	Pass	Pass	Pass	Pass	Upgrade
WKS-11	Unknown	Pass	Pass	Fail	Pass	Pass	Pass	Free space or replace disk, retest
WKS-15	Unknown	Pass	Pass	Fail	Pass	Pass	Pass	Free space or replace disk, retest
WKS-16	Unknown							Reset system clock, retest
WKS-23	Unknown	Pass	Pass	Fail	Pass	Pass	Fail	Turn on secure boot, retest

Table 3, Windows 11 Compatibility

7. Other issues, listed in the files embedded in CLIENT_A-SecurityReports.zip. These files are all named <computer name>.SecurityReports.txt.

    1. A false positive identifies several servers as not having antivirus or anti-malware software or antivirus definitions however the servers are running Trend Micro Apex One.

    2. MSTAFS10 - 10 failed tests, including:
        1. No antivirus product installed and virus definitions missing – Note – false positive. See 6.1 above.
        2. Windows update services not running.
        3. 6 system updates pending.
        4. Account lockout policies need to be updated.
        5. Password policies need to be updated.
        6. Audit policies need adjustment or enhancement.
        7. Drive encryption error.

    3. A_DC01 – 11 failed tests, including:
        1. Firewall is disabled.
        2. No antivirus product installed Virus definitions missing – Note – false positive. See 6.1 above.
        3. 4 system updates pending.
        4. Account lockout policies need to be updated.
        5. Password policies need to be updated.

6. Google Chrome, and old version is installed. The current version should be installed.
7. Drive encryption error.

4. A_DC02 – 11 failed tests, including:
    1. Firewall is disabled.
    2. No antivirus product installed Virus definitions missing – Note – false positive. See 6.1 above.
    3. 4 system updates pending.
    4. Account lockout policies need to be updated.
    5. Password policies need to be updated.
    6. Google Chrome, and old version is installed. The current version should be installed.
    7. Drive encryption error.

5. The same tests were run on A_Python01, A_SAS, A_Solm01Old, Client_Cyb-1, Client_AWSUS. As noted above, the results are in the text tiles named <machine name>.SecurityReports.txt.

8. The Greenbone vulnerability scanning tool was run against all hosts in the 10.0 and the 10.30 subnets. The results are documented in the files Greenbone.Client_A-x.y.z-report-ef829fc6.pdf and Greenbone. Client_A-x.y.z-report.pdf.

    1. In 10.0, there are 1,000 vulnerabilities with a threat level of "High."
    2. In the 10.30 network there are 74 vulnerabilities, all listed as "Low Level."

Appendices

Appendix 1: Attached files

1. Client_A-SecurityReports1.zip; files named <computer name>.SecurityReports.txt.

2. Client_A-SecurityReports2.zip:
    1. AD-local-Computers.xlsx
    2. AD-local-Users.xlsx
    3. EOL_Computers.PNG
    4. Greenbone.CLIENT_A-X.Y.Z-report-ef829fc6.pdf.
    5. Greenbone.CLIENT_A-X.Y.Z -report.pdf.
    6. A_S01.SystemInfoAndUpdates.txt
    7. A_S02.SystemInfoAndUpdates.txt
    8. CLIENT_A_X.Y.Z.report-ef829fc6.txt
    9. CLIENT_A_X.Y.Z-distribution-image.png".

Appendix 2: How Greenbone works.

According to both ChatGPT and MS Copilot, Greenbone's scanning engine is based on the OpenVAS scanner.

The Topology Graphic Is based on

1. Subnet-Based Mapping:
    - The topology graph primarily shows hosts that are on the same subnet as the scanner.
    - These hosts are connected with lines to the scanner, and their nodes are color-coded based on vulnerability severity.
2. Unconnected Hosts:
    - Hosts that are reachable but on different subnets appear as grey, unconnected dots. This is a limitation of the current visualization.
3. Host Discovery:
    - The graph is built from the results of host discovery and scanning tasks.
    - If more than 100 hosts are discovered, the topology graph may be omitted from the report to maintain performance.

Greenbone uses a variety of network discovery and scanning techniques, including:

- Ping (ICMP Echo Requests): To check if a host is alive.
- TCP SYN Scans: To identify open ports and services.
- Traceroute: Sometimes used to map the path to a host, though not always included in the topology.
- ARP Scans: For local subnet discovery.
- Service Detection: Helps identify the role of each host (e.g., web server, database).