

## Control Implementation Write-Up

Danny Rangel-Rios

Department of Cybersecurity, Collin College

CYBR-4350.200: Senior Project

December 9, 2023

## Table of Contents

1. Overview .....	4
2. Topology.....	4
3. Inclusion of a Secured Routed and Switched Environment.....	5
3.1. Create Port Rules for Ports That are Heavily Targeted in Attacks.....	6
3.2. Lockdown of Unauthorized Internet Protocol (IP) Ranges .....	8
3.3. Lockdown of Unauthorized Port Ranges.....	9
3.4. Limiting Software Installation .....	11
3.5. Use Virtual Local Area Networks for Management.....	12
3.5.1. Implementation.....	12
3.6. Implement Encryption Policy .....	13
4. Domain Name Service (DNS).....	14
4.1. Deployment.....	14
5. Dynamic Host Configuration Protocol (DHCP) .....	17
6. Network Time Protocol (NTP).....	17
7. Database .....	18
8. Endpoint Detection and Response.....	18
8.1. Deployment.....	18
9. Data Inspection.....	26
10. DLP Analysis .....	30

11.	Vulnerability Scanning .....	33
12.	Business Continuity and Disaster Recovery (BCDR) Strategy .....	36
13.	Detecting Unauthorized Changes .....	36
14.	References .....	37

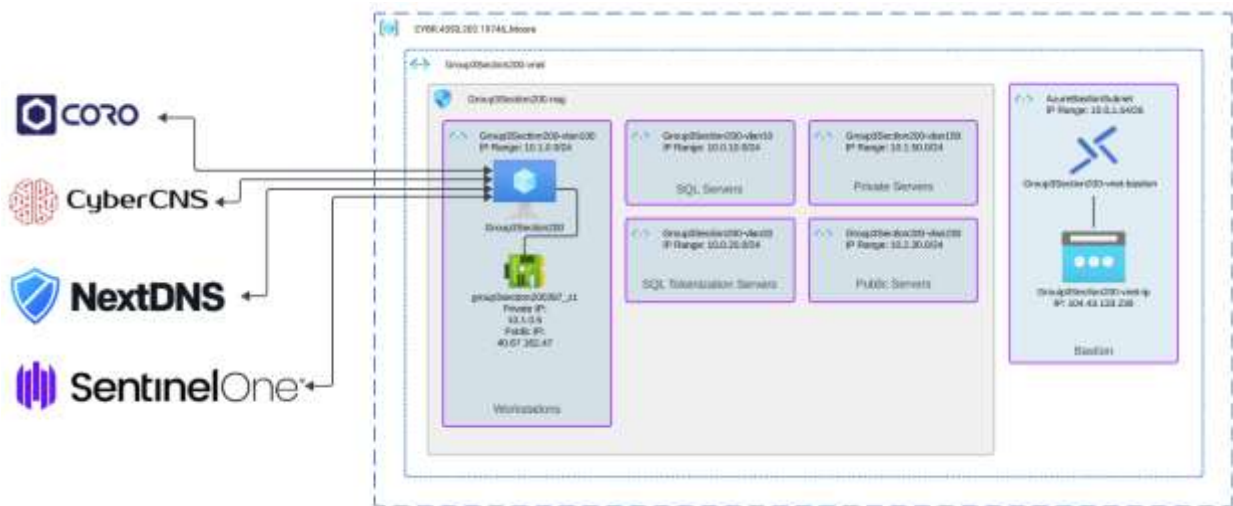
## Phase IIA - Design Statement of Work

## 1. Overview

As outlined in our Business Case for Alpha Community College, the purpose of this design plan is to address the improper storage and access of electronic patient records and private health information along with implementing data loss protection to prevent the improper storage and sharing of said data. The initial proposal included multiple servers and technologies in AWS. After the requirements changed the scope was reduced to a single server hosted in Azure. Portions of the following design discuss how the solutions were implemented, while other sections discuss how they would be implemented within Azure if permission levels were correct, or in AWS with the original scope.

## 2. Topology

The following topology provides an overview of the final design and configuration deployed within Azure. While there was only one system deployed, the subnets that were part of the original plan were included in the network security group. This provides insight into the overall design vision, and allows for security rules to be implemented as originally planned.



### Current Design within Azure

### **3. Inclusion of a Secured Routed and Switched Environment**

When using Microsoft Azure cloud services the customer uses a shared responsibility model where the customer is responsible for customer facing services in securing their assets. Microsoft also provides documentation for security best practices that provides benchmarks for establishing a security best practice baseline in securing the Azure cloud service. These controls can be tailored for the unique needs of an organization. No system is completely secure and if these best practices are left unchecked can lead to weaknesses or vulnerabilities that can make an organization's cloud services more susceptible to attack. Therefore, this section shall focus on establishing a baseline of controls for network security specifically using principles such as least privilege access controls and the zero-trust model.

When it comes to network security it's important to control and monitor the flow of communications through the network as well as access to resources and services within the network. Once a baseline of security controls is established these controls must be continuously assessed for effectiveness and also the fact that the security posture as well as the attack surface can change over time. Attackers are always finding new and creative ways to break into systems and controls that may be effective today may not be in the future.

Microsoft provides several tools for implementing network security controls that shall be used here for locking down unauthorized port ranges, IP ranges, and addressing common vulnerabilities and well-known attacks. These services include creating Network Security Groups and using Azure Firewall for establishing rules to block or allow specific ports and IP ranges, and utilizing Role Based-Access Control (RBAC) for implementing only necessary permissions for users to control access to resources.

It is also a best practice and assists in management of a network to segment the network into subnets. A virtual network or V-net is similar to a local area network (LAN) that allows for routing connections and communications between different services and virtual machines. Network segmentation also helps isolate and better control access to services that do not require to be public facing or accessible from the internet. This is essential for better security and management of the network. The forementioned best practices and controls will ensure access to the network and services running on the network as well as communication traffic that flows through the network are secure from unauthorized parties or users.

### **3.1. Create Port Rules for Ports That are Heavily Targeted in Attacks**

This section will define well known attacks and vulnerable ports that are commonly exploited by attackers. Ports are linked to different services and protocols and can be a common attack vector for attackers if they are not sufficiently protected. Any port can be a way into a network, but the ones defined here are most common due to weaknesses in the protocol, service, or due to misconfiguration of these services. As a general rule of thumb it is best practice to use a deny by default rule that blocks and closes all ports while creating allow rules for only necessary ports and services. It is important to ensure that all services in use are updated and patched while running the latest version of the services. Azure provides a set of default rules already in place for virtual machines and services although these rules can be overridden by setting a higher priority to custom rules.

Common vulnerable ports		Common Attacks
20, 21	FTP	Brute-forcing passwords, Authentication with default log in credentials, cross-site scripting, directory traversal attacks.
22	SSH	Brute-forcing credentials, Using leaked SSH keys.
3389	RDP	Weak or leaked log in credentials, BlueKeep Vulnerability.
445	SMB	EternalBlue exploit, capturing NTLM hashes, brute-forcing login credentials.
137, 139	NetBIOS over TCP	
443, 80, 8080, 8443	HTTP / HTTPS	SQL injections, cross-site request forgeries, cross-site scripting, DDoS attacks.
23	Telnet	Spoofing and spamming, credential brute-forcing, outdated and insecure.
25	SMTP	Spoofing and spamming with TCP
69	TFTP	Lack of built in encryption and access control or authentication.
1433,1434,3306	Databases	Unprotected databases with default log in credentials, SQL injections, Malware distribution, DDoS attacks.
389	LADP	LADP injection
53	DNS	DDoS attacks

### 3.2. Lockdown of Unauthorized Internet Protocol (IP) Ranges

To protect the network from malicious or unauthorized IP ranges Azure firewall shall be implemented. Network Manager is used primarily as a centralized service for managing multiple networks. Since we are only working with one network particularly Network Security Groups are better for segmentation of our network and controlling traffic internally between different subnets within the network. Azure Firewall is more of an endpoint device at the edge of our network to monitor and protect inbound and outbound traffic from the public facing internet and access to the resources within the network. While NSG's can be finely tuned to secure network traffic and connections that flow internally within our network, Azure Firewall is a more robust security solution for addressing the wide range of threats that exist outside and beyond our network.

Azure Firewall also utilizes threat intelligence from Microsoft Web Security which assists to automate the process by cross-examining well-known threats with over 58,000 signatures across 50+ categories that are continuously updated in real time. Azure Firewall also allows for Network Address Translation to mask the networks public facing IP address. Along with threat intel network and application traffic can also be filtered with custom rule configurations. Using Azure Firewall in conjunction with NSG's is in accordance with a defense in depth approach.

**Note:** As a disclaimer, we have restricted permissions for implementing the firewall plan and at this current point in time during the design phase it is unnecessary while the network is offline and not public facing the internet. However, we highly recommend the approval from the board of trustees and executive officials of ACC for the planned firewall implementation before finalizing the project and bringing it online and into production.



### 3.3. Lockdown of Unauthorized Port Ranges

Within a virtual network, Network Security Groups define how resources and subnets can connect and access each other. You can assign NSG's to one or multiple subnets. A NSG acts as a basic firewall between other NSG's , resources, and subnets within the virtual network. Custom rules can be created to filter inbound and outbound traffic between these resources. This helps to secure access control between resources and only allow authorized users to connect to these resources. This helps to implement a zero trust policy to verify users and devices and limit lateral movement within the local network.

Security rules are applied based on what is called the five-tuple and is defined as such:

**1. Source, 2. Source Port, 3. Destination, 4. Destination Port, 5. Protocol**

The following inbound rules shall be defined and implemented using the Network Security Group named Group3Section200-nsg. These rules will segment and restrict traffic to secure the private or backend databases that store sensitive PI and PHI. These rules also control the flow of access and how the services connect and communicate to provide more secure access control. These rules are defined as follows by priority where the highest priority is checked first. Using a tokenized database also helps in anonymizing PI and PHI so information that can be linked to an individual's identity is not stored in the same place for better security and privacy.

When creating the inbound rules it's necessary to create the outbound rules on the opposite end to allow access to and from as opposed to only a one way connection. This allows the flow of network traffic to send and also receive when transmitting read and write transactions.

#### Inbound Security Rules

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action
105	10.0.10.5/32		10.0.20.6/32	1433	TCP	Allow
201	Any		10.0.20.0/24	0-65535	TCP	Deny

**Priority 105** - Allows the primary database server access to the secure database which holds the token to PII/PHI data sets. The primary database SQL Server falls within the 10.0.10.0/24 subnet range and is given a single IP address of 10.0.10.5/32. This is the source address that is defined and given access to the 10.0.20.0/24 subnet range where the SQL Tokenized Server resides, where the SQL Tokenized Server is given a single IP address 10.0.20.6/32 as the destination for the inbound traffic that is sent from the primary SQL server. The protocol defined is TCP on port 443. This rule will allow only access from the specified IP, port, and protocol with other rules denying any other access.

**Priority 201** – This rule blocks all network access from any source IP to the SQL Tokenized Server within the subnet 10.0.20.0/24. The exception to this rule is the first rule with a higher priority of 105.

#### Outbound Security Rules

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action
106	10.0.20.6/32	1433	10.0.10.5/32	49152-65535	TCP	Allow
108	10.0.10.5/32	1433	10.1.0.0/24, 10.1.50.0/24, 10.2.30.5/32	49152-65535	TCP	Allow
201	10.0.20.0/24		Any	0-65535	Any	Deny

**Priority 106** – This rule is the opposite end of the first inbound rule allowing the SQL Tokenized Server to respond to requests made from the primary server. The SQL Tokenized server uses it's IP address 10.0.20.6/32 as the source and the IP address of the primary server 10.0.10.5/32 as the destination. This allows the secure database to access and respond to requests made by the primary database from source port 443 and destination port ranges 49152-65535 using TCP.

These VLAN's include workstations and internal servers but not the SQL Tokenized database which only grants access to the primary database.

**Priority 108** – This rule allows the private database to respond to requests from the VLAN's 100, 150, and a public server with a single IP address of 10.2.30.5.

**Priority 201** – This rule blocks all other outbound traffic if it does not match the first rule allowing the SQL Tokenized Server to respond to requests made from the primary server. The source IP address is the 10.0.20.0/24 subnet where the SQL Tokenized database resides.

The rules for inbound and outbound traffic shall also include default rules that are necessary for connection with a lower priority and also a final rule that denies all traffic by default other than the exception of the allow rules which only permit specific access.

### **3.4. Limiting Software Installation**

To enhance the security of the virtual machine (VM), Software Restriction Policies (SRP) will be enforced via the Local Group Policy in order to restrict software installation. This is a crucial component of cybersecurity efforts, aimed at reducing risks associated with malicious software by allowing only the execution of software that meets strict security protocols. The Remote Desktop Protocol (RDP) is used to configure SRP by accessing the operating system of the VM. This process involves creating a new Group Policy Object (GPO) and setting up SRP within it. A GPO is a set of configurations made via the Group Policy Editor in the Microsoft Management Console (MMC), which directs the working environment for user and computer accounts. Once created, the GPO is linked to the Organizational Unit that includes the VMs. The SRP configuration involves setting security levels and establishing path and hash rules to block software. These rules identify which software should be restricted and determine the conditions under which software can execute. The implementation of SRP aims to support organizational

security by managing software execution, ensuring that only approved applications are allowed to operate on company systems.

### 3.5. Use Virtual Local Area Networks for Management

The use of subnets in conjunction with virtual local area networks (VLANs) provides a logical segregation of network traffic into individual broadcast and security zones. Our solution will utilize public and private subnets in Azure to create security zones in order to granularly control the flow of traffic between systems, services, and users. Our design will group systems with identical security requirements together into subnets, which will provide the VLAN segregation needed to meet security requirements.

Our Azure deployment will consist of five VLANs: VLAN 10, VLAN 20, VLAN 100, VLAN 150, and VLAN 230. The follow table details the configuration:

<b>VLAN ID</b>	<b>Purpose</b>	<b>IP Range</b>	<b>Members</b>
<b>10</b>	SQL Servers	10.0.10.0/24	
<b>20</b>	SQL Tokenization Mapping Servers	10.0.20.0/24	
<b>100</b>	Workstations	10.1.0.0/24	Group3Section200
<b>150</b>	Non-sql, non-public servers	10.1.50.0/24	
<b>230</b>	Public servers (DMZ)	10.2.30.0/24	

#### 3.5.1. Implementation

Within Azure, subnets must be created within a virtual network. The Group3Section200-vnet virtual network was created with the address space of 10.0.0.0/8 in order to provide the ability to utilize the desired IP ranges for each subnet. Additionally, encryption was enabled on the virtual

network to encrypt all data while in transit. Next, in the subnets section of the Group3Section200-vnet settings the subnets were created as Group3Section200-vlan<ID> with the assigned IP range and Group3Section200-nsg selected as their security group. Lastly, a Gateway Subnet was created with the IP range of 10.0.1.0/28 to allow for connections over a VPN connection.

### **3.6. Implement Encryption Policy**

To ensure the safety of the data that is kept on Virtual Machines (VMs), it is extremely important to enable disk encryption. The process of handling keys centrally for numerous virtual machine drives is facilitated by Azure Disk Encryption. To begin the procedure, navigates to the virtual machine's settings, on the left click "Disks". To configure disk encryption, select "Additional Settings" at the top of this section. Following this, the operating system disk or all disks should to be chosen in accordance with particular specifications. For the purpose of encryption, the operating system disk is selected in this specific implementation.

The establishment of a new Key Vault is an essential procedure due to its role as a safe storage for sensitive data, such as encryption keys and certificates. In the absence of an existing Key Vault, it is necessary to generate one by assigning it a designated name. The subsequent method involves the configuration of an access policy within the Key Vault. This involves the allocation of permissions for keys and certificates, along with the inclusion of necessary accounts. Utilizing an existing network infrastructure is advantageous when Key Vaults necessitate network connectivity.

Prior to commencing the Key Vault, it is imperative to perform a thorough analysis of all configurations in order to validate their ability to withstand validation tests. If a key has not been generated, it is necessary to create, assign a name to, and configure the key within the Key Vault.

Preservation of the current iteration of this key is of utmost importance, as it plays a vital part in the encryption process. Upon successful insertion of the key, the encryption process begins, potentially requiring a restart of the virtual machine. Continuous monitoring of the encryption state is crucial in order to ascertain the successful completion of the encryption process.

#### **4. Domain Name Service (DNS)**

Each system in the environment will be configured to use NextDNS to provide a secure DNS service with auditing and reporting functionality. NextDNS provides encrypted transport of DNS queries using DNS-over-HTTPS, DNS-over-TLS, or the NextDNS client. For this environment, the NextDNS client was chosen for its simpler deployment, that does not require the modification of any DHCP or local DNS settings.

##### **4.1. Deployment**

The first step in deploying NextDNS is to create a deployment profile at [my.nextdns.io](https://my.nextdns.io). The profile was named “Collin College Project (Do NOT Delete)”. Then under the under the Security options, the following protections were enabled:

- Threat Intelligence Feeds
- AI-Driven Threat Detection
- Google Safe Browsing
- Cryptojacking Protection
- IDN Homograph Attacks Protection
- Typosquatting Protection
- Domain Generation Algorithms (DGAs) Protection
- Block Newly Registered Domains (NRDs)
- Block Dynamic DNS Hostnames

- Block Parked Domains
- Block Child Sexual Abuse Material
- Block Top-Level Domains (TLDs)
  - Blocked .xyz, .fun, .top, .ru, .br, .cn, .se, .zip, .mov, .hk, .gq, .ga, .cf, .tk, .ml, and .icu as these are commonly used for malicious attacks, phishing, malware, grayware, and command and control connections (Toulas, 2021; , Watchguard, 2023).

Next under the Privacy options, the following protections were enabled:


- Blocklists
  - Added NextNDS Ads & Trackers Blocklist
  - Added AdGuard DNS filter
  - Added OISD
  - Added Steven Black
  - Added HaGeZi – Multi ULTIMATE
- Block Disguised Third-Party Trackers
- Allow Affiliate & Tracking Links

After the profile is setup up, the client was installed on Group3Section200 virtual machine using the following script in and administrator PowerShell session:


```
Invoke-WebRequest -Uri "https://nextdns.io/download/windows/stable.msi" -OutFile
"$env:TEMP\NextDNSSetup.msi"

msiexec /qn /i "$env:TEMP\NextDNSSetup.msi" PROFILE=a233a6
```

After the installation was completed, the application was tested for functionality by confirming that DNS queries were appearing in the NextDNS logs.



 **NextDNS**

Collin College Project (Do NOT Delete) EDITOR ▾









[Setup](#) [Security](#) [Privacy](#) [Parental Control](#) [Denylist](#) [Allowlist](#) [Analytics](#) [Logs](#) [Settings](#)

All devices ▾

☒ Blocked Queries Only

☐ Raw DNS logs

 portal.mycybercns.com	 Group3Section20 Tuesday, October 31, 2023 11:59 PM
 agentv3.myconnectsecure.com	 Group3Section20 Tuesday, October 31, 2023 11:59 PM
 portaluseast2.mycybercns.com	 Group3Section20 Tuesday, October 31, 2023 11:59 PM

*Allowed DNS responses*



The screenshot shows the NextDNS web interface for the 'Collin College Project (Do NOT Delete)' account. The 'Logs' tab is selected, displaying a list of blocked queries. The interface includes a search bar, filters for 'Blocked Queries Only' (selected) and 'Raw DNS logs', and a table of blocked queries with domain names, icons, and timestamps.

Domain	Icon	Group	Time
self.events.data.microsoft.com	Microsoft	Group3Section20	9 minutes ago
srtb.msn.com	MSN	Group3Section20	11 minutes ago
functional.events.data.microsoft.com	Microsoft	Group3Section20	11 minutes ago
browser.pipe.aria.microsoft.com	Microsoft	Group3Section20	12 minutes ago
c.bing.com	Bing	Group3Section20	14 minutes ago
c.msn.com	MSN	Group3Section20	14 minutes ago
sb.scorecardresearch.com	Scorecard Research	Group3Section20	14 minutes ago
self.events.data.microsoft.com	Microsoft	Group3Section20	14 minutes ago

### ***Blocked DNS Responses***

## **5. Dynamic Host Configuration Protocol (DHCP)**

VLAN 100 will utilize the DHCP services built in to Azure subnets to provide IP addresses for workstation level machines. However, each of the servers in our deployment will have static IP address assignment.

## **6. Network Time Protocol (NTP)**

Our deployment will utilize the NTP Pool Project's NTP servers. The use of pool.ntp.org will provide automatic redundancy and direct the systems to the nearest regional NTP member server.

## **7. Database**

The original design deployment would have consisted of two Microsoft SQL database servers with sample data. SQL01, located in VLAN 10, would have the primary database with the patient records minus any PII that would directly correlate an individual to the record. SQL02, located in VLAN 20, would provide the mapping to match the individual's PII with the patient records. Our sample data would have been provided from a dental application vendor which provides a test database to test their application without live data. However, due to technical and permission issues, only the subnets were created in the network security group to simulate as if the servers existed.

## **8. Endpoint Detection and Response**

There are multiple endpoint protection solutions available, including Microsoft Defender for Endpoint. However, decided to use SentinelOne Singularity Complete. While this is a third-party solution, it has a higher industry ranking based on Gartner Peer Insights reports and includes managed detection and response to provide a 24x7 security operations center (SOC) (Gartner, Inc., n.d.).

### **8.1. Deployment**

The first part of the deployment is to create the protection policy. The policy is broken in to six sections:

- Protection Mode
- Detection Engines
- Agent
- Deep Visibility
- Binary Vault

- More Options

Under the Protection Mode settings we kept the default for malicious threats to “Protect”, which is determined by the protection level, and suspicious threats to “Detect”, which alerts only. The protection level is also set to the default of kill and quarantine, with the other options being to remediate or rollback. We then set it to remove malicious macros from Office files and disconnect from the network upon threat detection.

## Protection Mode

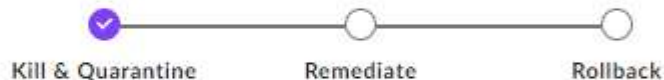
### Malicious Threat

Kill &amp; Quarantine

### Suspicious Threat

Alerts Only

### Protect Level



### Malicious Macros Mitigation ?

This only applies when the Static AI detection engine is On, and the Protection Mode of Malicious Threats is set to Protect.

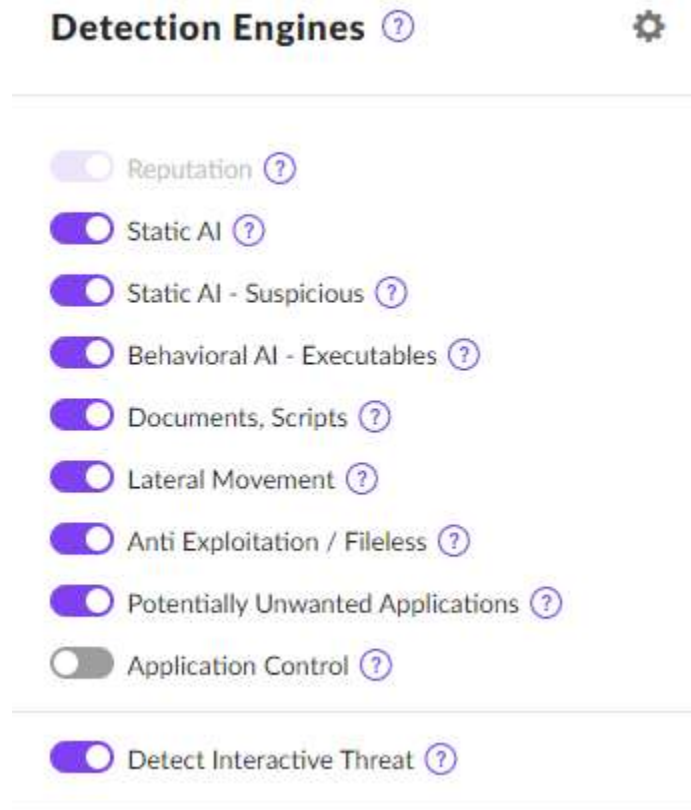
☒ Remove malicious macros from the Office file instead of placing the file in quarantine.

### Containment

Disconnect from network ?

### *Protection Mode settings*

For the Detection Engine settings we kept the defaults, with the exception of enabling the detection of interactive threats to detect insider threats with the behavioral AI analysis.



### ***Detection Engine settings***

For the Agent settings we went with the defaults.

Agent

Security Settings

☒ Snapshots [?](#)

☒ Anti Tamper [?](#)

☒ Scan New Agents [?](#)

☒ Suspicious Driver Blocking All Drivers [?](#)

☒ Logging [?](#)

Agent UI

☒ Show Agent UI & tray icon on endpoints [?](#)

Set which information and notifications to show for end-users

Show pop-up notifications for:

☒ Threats and Mitigation [?](#)

☒ Blocked Devices [?](#)

Show suspicious events in the UI:

☒ Include Suspicious [?](#)

Show warning in case of Agent errors:

☐ Include Warnings [?](#)

Show in the UI events from the last:

days [?](#)

Show these menu items in the UI:

☐ Blocked Devices

☒ Quarantined Files

☒ Contact Support

### *Agent settings*

We also kept the defaults for the Deep Visibility settings. The deep visibility options improve threat hunting capabilities.

## Deep Visibility

### Deep Visibility Configuration

Collect this Deep Visibility data

☒ Enable Deep Visibility ?

[Event Type Configuration](#)

<input checked="" type="checkbox"/> Process ?	<input checked="" type="checkbox"/> File 5/5 ?	<input checked="" type="checkbox"/> URL ?
<input checked="" type="checkbox"/> DNS ?	<input checked="" type="checkbox"/> IP 2/2 ?	<input checked="" type="checkbox"/> Login 2/2 ?
<input checked="" type="checkbox"/> Registry Keys 8/8 ?	<input checked="" type="checkbox"/> Scheduled Tasks 5/5 ?	<input checked="" type="checkbox"/> Behavioral Indicators ?
<input checked="" type="checkbox"/> Command Scripts ?	<input checked="" type="checkbox"/> Cross Process 4/4 ?	<input checked="" type="checkbox"/> Driver Load ?

☐ Data Masking ? ☒ Focused File Monitoring ?

☒ Automatically install Deep Visibility browser extensions

☐ Do not select if your organization uses Google Workspace (formerly G Suite) to manage browser extensions

This overrides other browser extensions deployed with Google Workspace. If your organization uses Google Workspace to deploy browser extensions, deselect this option and deploy the SentinelOne browser extension in the same way you deploy other extensions. This option requires Windows Agent 4.7+.

### *Deep Visibility settings*

For the Binary Vault settings, we enabled this setting and kept the default file size limits to provide automatic file uploads of files related to an incident for further forensic examination.

## Binary Vault

### Enable Automatic File Upload

☒ Enable Automatic File Upload ?

Exclude Path	<input type="text" value="New Path"/>
Exclude File Type	<input type="text" value="New File Type"/>
Maximum file size Upload (Max 250MB)	<input type="text" value="250"/> MB
Total Upload per Agent per day (Max 500MB)	<input type="text" value="500"/> MB
Offline cache size (Max 2048MB)	<input type="text" value="2048"/> MB

### *Binary Vault settings*

In the last section of the policy, More Options, we turned off the auto decommission option. We did this to prevent the logs from being removed the system if the agent does not check in

within the default 21 days. Additionally, we kept the default to leave the remote shell disabled. This should setting should be enabled as needed to reduce the system's exposure.

**More Options**

Decommissioning

☒ Auto decommission after 21 days offline ?

Remote Shell


☐ Enable Remote Shell

### *More Options settings*

To deploy SentinelOne Singularity, we downloaded the most recent Windows agent, version 23.2.2.358, and installed locally on the virtual machine. Once completed, the agent performs an inventory of the system including the system details, cloud details, and application inventory. The following images show the successful inventory of the system.

Group3Section20
⊖ ×

GENERAL
CLOUD
APP INVENTORY
TASKS
UPDATES
TAGS
Actions



Group3Section20
Windows 11 Pro (64 bit)
  
Republic Elite / CYBR4350 / Default Group

Last active	Last 4 minutes	Disk encryption	Off
Health status	Healthy	UUID	a5ac38d9d6fc4300be4d...
Last logged in	Group3Section200	Console connectivity	Online
Agent version	23.2.3.358 <span>UPDATED</span>	Network status	Connected
Full Disk Scan	Completed ( Oct 25, 2023 ...	Configurable Netw...	Disabled
Memory	3.50 GB	Domain	WORKGROUP
CPU	1 X Intel(R) Xeon(R) Platinu...	Subscribed on	Oct 25, 2023 20:02
Core count	1	Last Reboot	Nov 18, 2023 18:52
Customer identifier	N/A	Console visible IP	40.67.162.47
Ranger Version	21.11.0.123	IP Address	10.1.0.5
Installer Type	MSI	Locations	fallback
Firewall status	Disabled	Serial Number	0000-0004-7666-7124-...

Network Adapters:


Name	IP	Mac Address
Ethernet	10.1.0.5	00:22:48:4a:85:5e

***Singularity agent details, General tab***



Group3Section20 ⊖ ×

GENERAL CLOUD APP INVENTORY TASKS UPDATES TAGS **Actions** ⌵


**Microsoft Azure**

Account ID d0ef3921-dd6d-4902-b4e0-1383f52c614c  
Location centralus  
Resource Group cybr.4350.202.19746\_moore  
Instance ID 42269e3d-8e5f-46be-adde-48fdad112b01  
Image win11-22h2-pro  
Tags  
Instance Size Standard\_DS1\_v2

*Singularity agent details, Cloud tab*

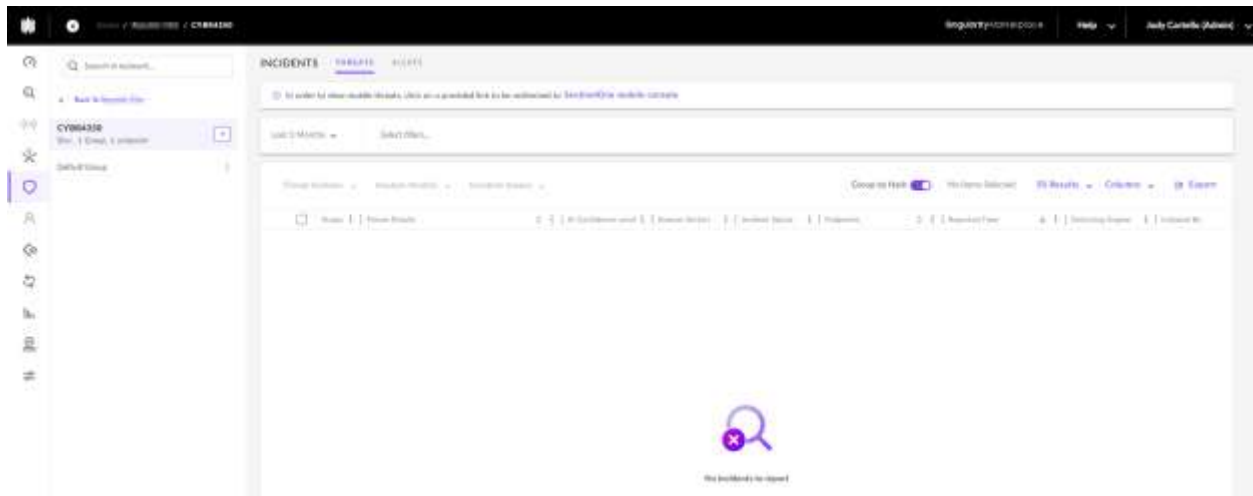
Group3Section20 ⊖ ×

GENERAL CLOUD APP INVENTORY TASKS UPDATES TAGS **Actions** ⌵

Name	Installed Date	Size	Version	Publisher
CyberCNS LightWei...	11/17/23	0.00 B	2.1.8	CyberCNS Inc.
Microsoft Update H...	11/18/23	1.02 KB	5.72.0.0	Microsoft Co...
Coro	11/18/23	219.36 KB	2.0.53.1	Coro Cyber S...
Microsoft OneDrive	11/18/23	299.23 KB	23.226.1031...	Microsoft Co...
Microsoft Edge Web...	11/17/23	0.00 B	119.0.2151.72	Microsoft Co...
Microsoft Edge	11/17/23	0.00 B	119.0.2151.72	Microsoft Co...
Npcap OEM	10/25/23	0.00 B	1.50	Nmap Project
Microsoft Visual C+...	10/25/23	17.91 KB	14.29.30040.0	Microsoft Co...
NextDNS	10/25/23	0.00 B	3.0.12	NextDNS
Sentinel Agent	10/25/23	250.66 KB	23.2.358	Sentinel Labs...

### *Singularity agent details, App Inventory tab*

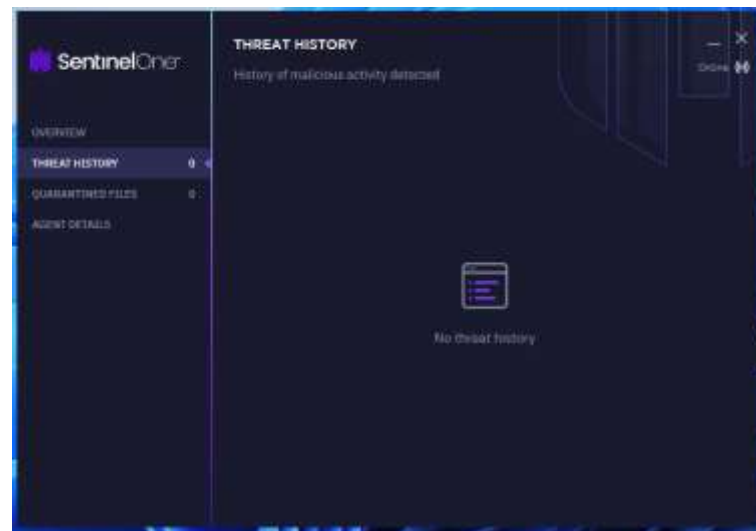
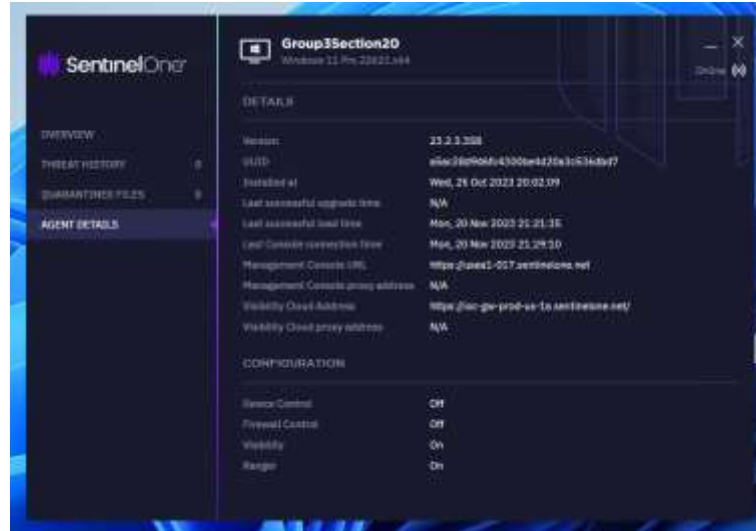
The Incidents section of the Singularity portal provides details on detected threats, including the threat details, incident status, and the verdict of the SOC analyst. At this time, no threats have been detected.



### *Singularity Incidents dashboard*

## **9. Data Inspection**

There must be a way to inspect any and all data that comes in and resides in the network for malicious activity. The software "SentinelOne" was utilized to continuously monitor and check for infected files that could have potential harm to the sensitive data. An initial scan was done to the VM with SentinelOne after downloading it. Continuous scanning of the VM is done to alert if anything abnormal is found.



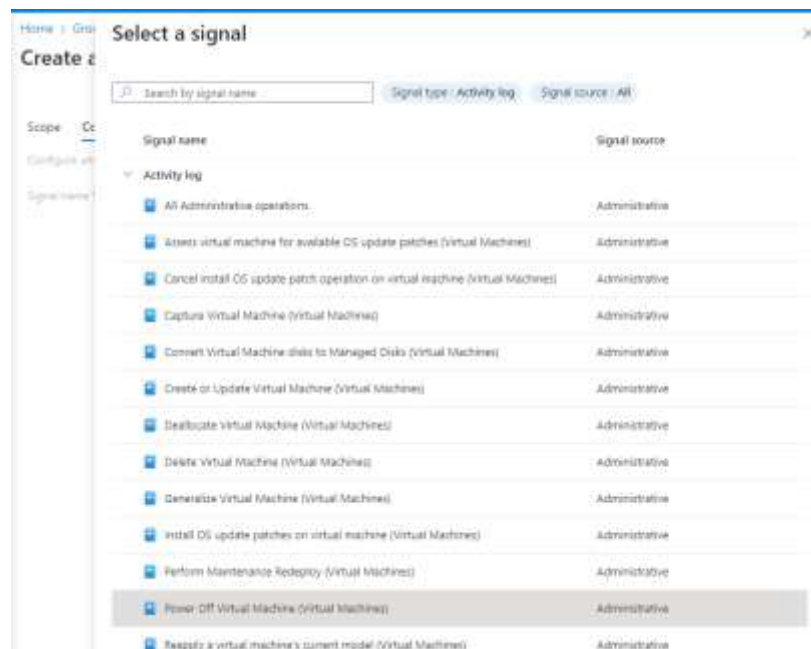
*Agent Details/Threat History, SentinelOne*

“Monitor” on Azure can be used to track what and when data was created, accessed, copied/moved, modified, deleted, and by who, through creating alerts.



*Alerts, Azure*

Alerts can be set up by creating “rules”. For example, a rule can be created to send out an alert to a specific person when the VM has been turned on or off. To do this, you first would click on “+ Create”, and then from the drop-down menu select “Alert rule”. By clicking on Scope, it will show you exactly what is being configured, which would be our class groups resource group and subscription. You then want to go to the “Conditions” tab to select a signal. There are many options to choose from in this step. The signal type drop-down menu has the options of metrics, log, or activity log. For the example, activity log would be selected, where a list of signal names from the activity log will be shown. The activity log name “Power Off Virtual Machine” and “Start Virtual Machine” would be chosen, as this will be the one that alerts when the VM has been shut down and powered on. Unfortunately, multiple signals for a rule cannot be chosen, so separate alerts will need to be created for each rule.



### *Selecting a Signal, Azure*

Once a signal has been selected, the event level should be chosen (verbose, informational, warning, error, critical) or a selection of all of them which would be the best idea. Then, the status should be selected. The options are failed, started, succeeded, or select all. For the event initiated by selection, all services and users are automatically chosen as the default option, which can be left as is.

### ***Alert Logic, Azure***

The next tab is to select an action group. Since there is no action group yet, one must be created. The Azure subscription being used will be selected, as well as the resource group, in this case it would be the VM. An action group name and display name can be chosen after. This is so Azure can charge the correct price for the subscription being utilized on the specific resource group. Notification type is the next tab, which is where someone can choose what type of notification they would like to receive if the alert is triggered. This can be either through SMS, Email, Push notification, or voice to a specific email or phone number, or the resource manager can be chosen as the designated person to receive alerts.

Home > All resources > Group3Section200 (Alerts) > Create an alert rule >

## Create action group

**Basics** Notifications Actions Tags Review + create

An action group invokes a defined set of notifications and actions when an alert is triggered. [Learn more](#)

### Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ CyberSecurity Faculty and Students

**Resource group \*** ⓘ CYBR4350.202.19746, Moore  
[Create new](#)

Region \* Global

### Instance details

Action group name \* ⓘ

Display name \* ⓘ   
The display name is limited to 12 characters

[Review + create](#) [Previous](#) [Next: Notifications >](#)

### *Action Group, Azure*

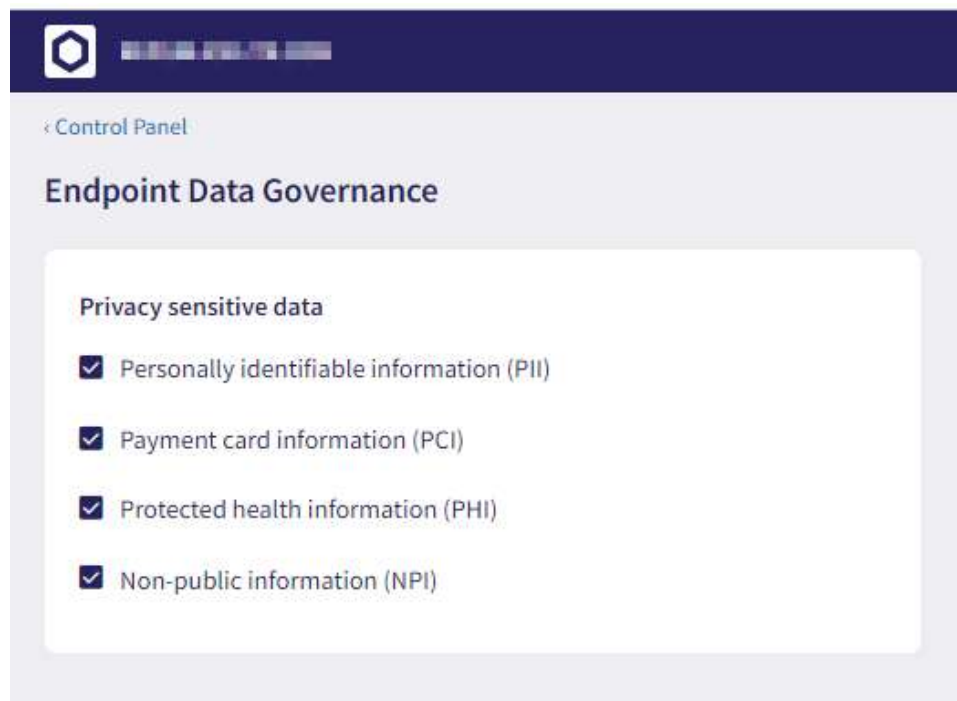
## 10. DLP Analysis

Data Loss Prevention is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data. It can help monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across folders, files, and software.

Microsoft Purview was going to be utilized to create DLP policies in Azure, but unfortunately was unable to do so due to permission issues. Instead, Coro, a third-party product free trial was downloaded onto the VM in place of Purview, which also has DLP tracking capabilities. Coro provides endpoint security, such as advanced threat protection, where both static files and running processes are analyzed for anomalies. Policies can be put in place for

users and groups, as well as allow/block lists of files, folders, and processes on those endpoints so that data such as PHI and PII can only be accessed by those who are authorized.

The Endpoint Data Governance module can be used to protect sensitive data such as PII, PHI, PCI, and NPI from unauthorized access, use, disclosure, modification, and destruction across endpoints. Selecting all of these options will provide the best protection available. This agent was installed on the VM.



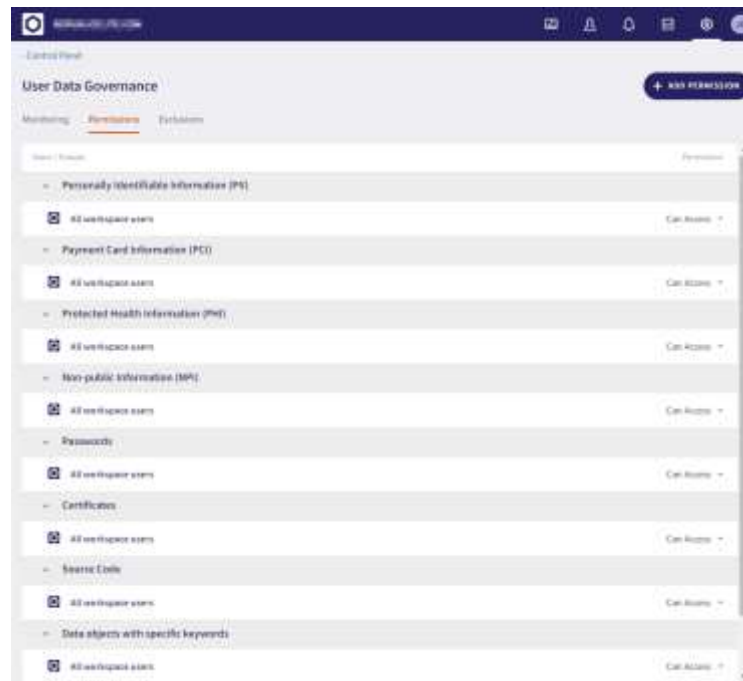
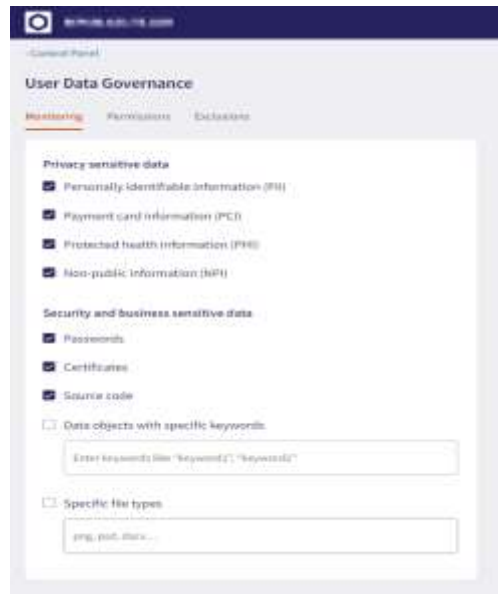
### ***Endpoint Data Governance, Coro***

The User Data Governance module is to help aid administrators in establishing a data handling strategy. With this, a list of users with permission violations, as well as the emails that have been flagged becomes available for review by scanning emails for unauthorized disclosure of that data such as:

- PII (Personally Identifiable Information)
- PHI (Protected Health Information)

- PCI (Payment Card Information)
- NPI (Non-Public Information)
- Passwords
- Source code
- Certificates
- Custom keywords



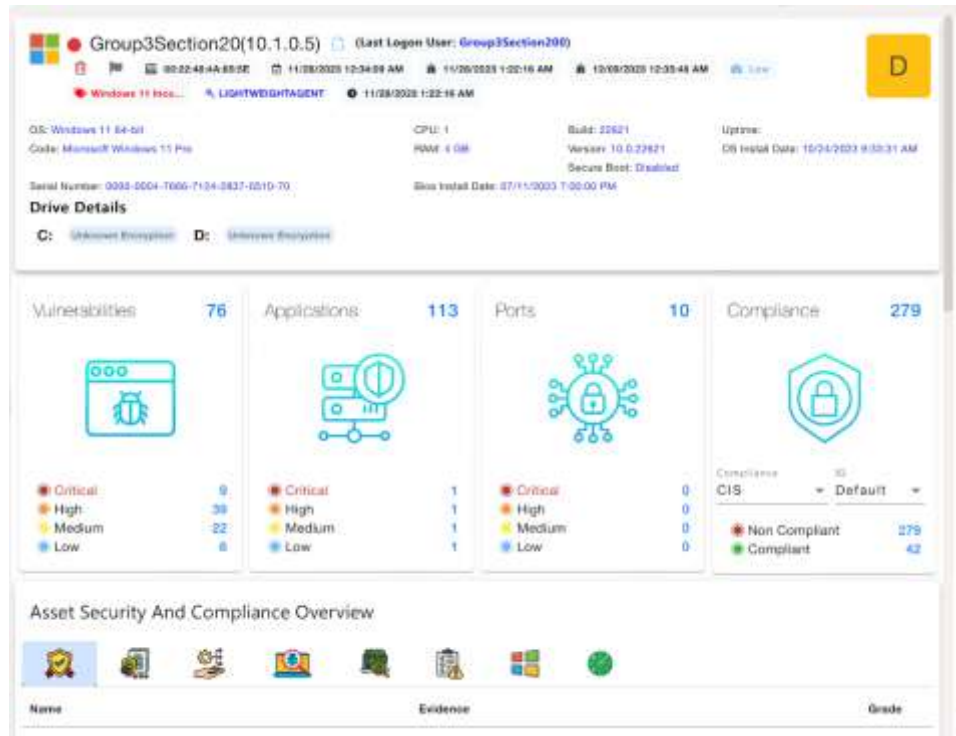


*User Data Governance, Coro*

## 11. Vulnerability Scanning

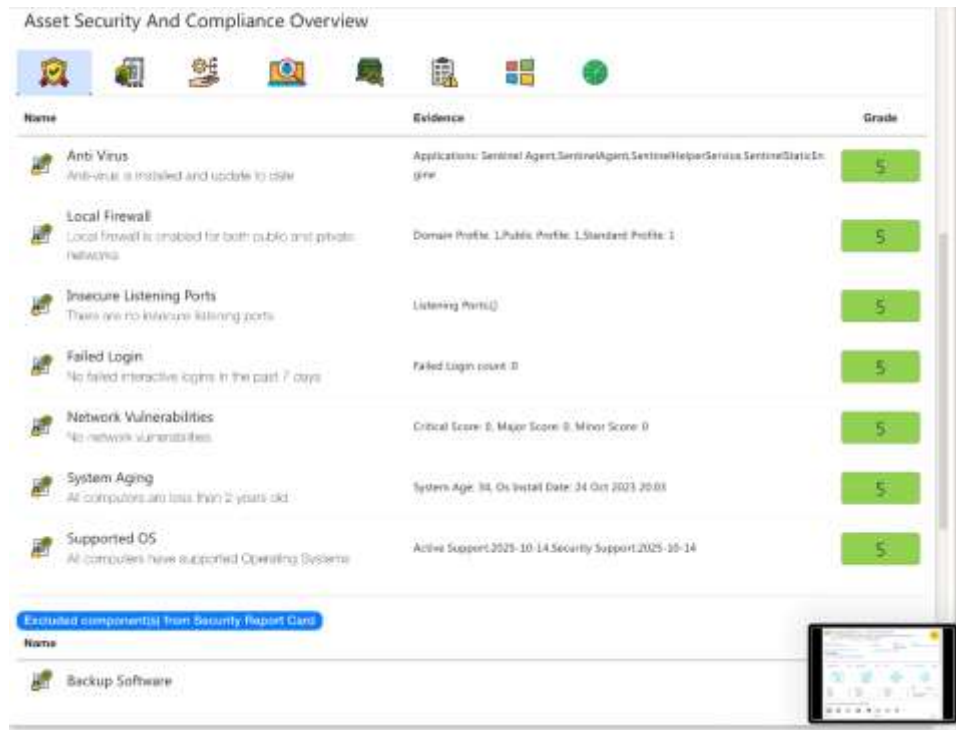
For our vulnerability scanner we will be using a third-party application called CyberCNS. CyberCNS has 2 types of agents. One is a probing agent that not only scans its host, but also any device on the network. Another is a lightweight agent, that runs only on the host and scans for

vulnerabilities on the device. What CyberCNS does is after it scans, it will link the vulnerabilities to their respective CVE. It also pulls an inventory of any installed applications and finds software vulnerabilities as well.



***Vulnerability Report, CyberCNS***

**Asset Security And Compliance Overview**



Name	Evidence	Grade
<b>Anti Virus</b> Anti-virus is installed and update to date	Applications: Sentinel Agent, SentinelAgent, SentinelHelperService, SentinelStaticEngine	5
<b>Local Firewall</b> Local firewall is enabled for both public and private networks	Domain Profile: 1, Public Profile: 1, Standard Profile: 1	5
<b>Insecure Listening Ports</b> There are no insecure listening ports	Listening Port(s)	5
<b>Failed Login</b> No failed interactive logins in the past 7 days	Failed Login count: 0	5
<b>Network Vulnerabilities</b> No network vulnerabilities	Critical Score: 0, Major Score: 0, Minor Score: 0	5
<b>System Aging</b> All computers are less than 2 years old	System Age: 34, Os Install Date: 34 Oct 2023 20:03	5
<b>Supported OS</b> All computers have supported Operating Systems	Active Support: 2025-10-14, Security Support: 2025-10-14	5

**Excluded components from Security Report Card**

Name
Backup Software

### *Asset Security and Compliance Overview, CyberCNS*

**Asset Inventory Overview**



Name	Version	Path	Arch
Microsoft Edge	118.0.2151.72	C:\Program Files (x86)\Microsoft\Edge\Application	
Windows PrintDialog	8.7.2.0	C:\Windows\PrintDialog	
SecHealthUI	1000.25873.9301.0	C:\Program Files\WindowsApps\Microsoft.SecHealthUI_1000.25873.9301.0_x64__8wekyb3d8bbwe	
NET.Native.Runtime.2.2	2.2.28604.0	C:\Program Files\WindowsApps\Microsoft.NET.Native.Runtime.2.2_2.2.28604.0_x64__8wekyb3d8bbwe	
XboxGameOverlay	1.54.4001.0	C:\Program Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_x64__8wekyb3d8bbwe	

Items per page: 5 | 1 - 5 of 103

Name	Version	Path	Arch	Uninstall String
CyberCNS LightWeight Agent	2.1.8			C:\PROGRAMS\2\CyberCNSAgent\2\uninstall.bat
Microsoft Edge Update	1.3.181.0			
Npcap OEM	1.50			"C:\Program Files\Npcap\uninstall.exe"
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30040	14.29.30040			MsExec.exe /I{3093CC13-DF27-4036-A072-A7593002}
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30040	14.29.30040			"C:\ProgramData\Package Cache\ca868509-65be-4c09"

Items per page: 5 | 1 - 5 of 8

### *Asset Inventory, CyberCNS*

## **12. Business Continuity and Disaster Recovery (BCDR) Strategy**

For the business continuity and disaster recovery strategy we will be keeping it simple and using what Azure Health Data Services to guarantee the robustness, dependability, and ability to recover your health data and applications in the event of a disruption. Azure Health Data Services is typically able to manage unexpected occurrences within the cloud environment and is proficient at maintaining the operation of your applications and business processes. However, with that being said there are a few things that it cannot help with like accidental/purposeful deletions, a natural disaster or any other event that that requires cross region failover.

For this reason, ensuring that there is a proper backup strategy in place is an essential component of any organization's AWS infrastructure strategy to ensure data reliability and resilience. For the backup solution we will still be within Azure and use Azure backup. This will allow us to configure it to automatically perform backups along with the frequency as which it is done and how long Azure retains it for. Implementing a robust backup solution within Azure will offer numerous benefits including data protection, business continuity, compliance adherence, cost optimization and enhanced operational efficiency.

## **13. Detecting Unauthorized Changes**

By implementing effective logging and monitoring practices we can ensure that unauthorized changes are detected before major damage is done. In order to accomplish this, the use of AWS CloudTrail and AWS config will be put to use. AWS Config will allow us to document alterations in the configurations of software running on EC2 instances within your AWS account, as well as virtual machines (VMs) or servers in our on-premises environment. AWS CloudTrail maintains continuous logs of account activity associated with actions across your AWS infrastructure, providing you with authority over storage, analysis, and corrective actions.

## 14. References

- Baldwin, M. (2023, January 5). *Enable Azure disk encryption for Windows VMS - Azure virtual machines*. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview>
- Fox, C., Koenen, K., & Mazzoli, R. (2023, September 29). *Learn about data loss prevention*. Microsoft Learn. <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
- Gartner Inc. (n.d.). *Microsoft vs SentinelOne 2023: Gartner Peer insights*. Gartner. <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions/compare/microsoft-vs-sentinelone>
- Gerend, J. (2021, July 29). *Software restriction policies technical overview*. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies-technical-overview>
- How Azure firewall works - training*. Microsoft Learn. (n.d.). <https://learn.microsoft.com/en-us/training/modules/introduction-azure-firewall/3-how-azure-firewall-works>
- How network security groups filter network traffic - training*. Microsoft Learn. (n.d.-b). <https://learn.microsoft.com/en-us/training/modules/filter-network-traffic-network-security-group-using-azure-portal/4-create-network-security-group>
- Microsoft Operating Systems bluekeep vulnerability*. Cybersecurity and Infrastructure Security Agency. (2019, June 17). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-168a>
- SentinelOne. (2019, May 27). *EternalBlue exploit: What it is and how it works*. <https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>

Sudbring, A. (2023, April 24). *Create, change, or delete an Azure Network Security Group.*

Microsoft Learn. <https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group?tabs=network-security-group-ports>

Toulas, B. (2021, November 12). These are the top-level domains threat actors like the most.

Bleeping Computer. <https://www.bleepingcomputer.com/news/security/these-are-the-top-level-domains-threat-actors-like-the-most/>

Watchguard. (2023). *Use WatchGuard products to block access to a top-level domain.*

Watchguard Support Center.

<https://techsearch.watchguard.com/KB?type=Article&SFDCID=kA16S00000110tgSAA>