Okema Cyber - Infrastructure Build Report

Oscar Capraro, Emmalee Carpenter, Marc Rosenthal, Kevin McCarthy, Anushka Tilara

December 8, 2025

Table of Contents

Basic Information

Organization Name

Okema Cyber

Mission Statement

At Okema Cyber, we stay ahead of tomorrow's threats today. Guided by urgency and diligent observation, our mission is to fuse cutting-edge technology with expert insight to deliver adaptive, proactive, and future-ready defenses in order to ensure our clients remain secure in an ever-changing digital landscape.

Group Members

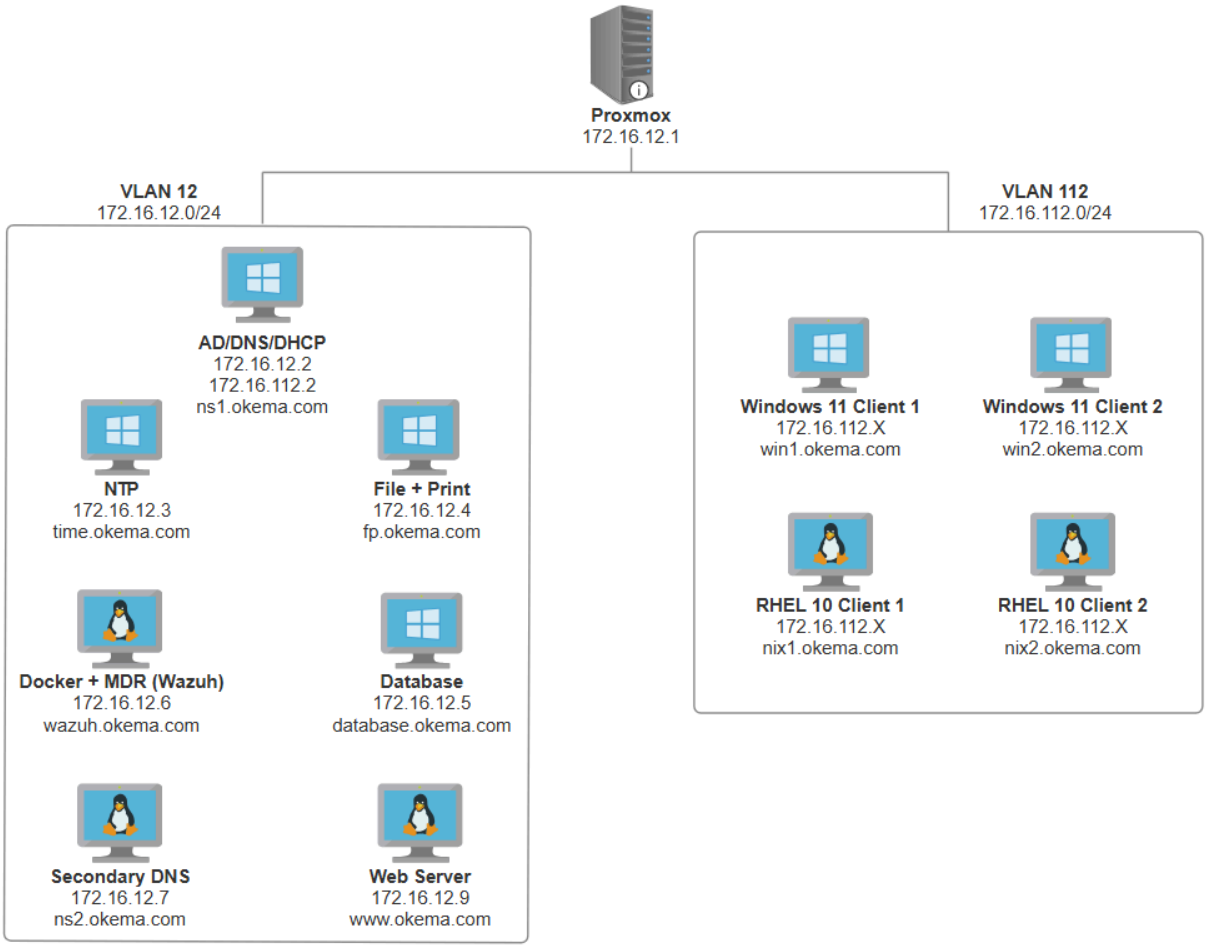
Name	Degree Program	Expected Graduation Year
Oscar Capraro	Cybersecurity	2027
Emmalee Carpenter	Cybersecurity	2027
Marc Rosenthal	Cybersecurity	2026
Kevin McCarthy	Cybersecurity	2026
Anushka Tilara	Cybersecurity	2026

Network Topology Overview

The Okema Cyber environment is designed as a segmented, security-focused enterprise network consisting of centralized virtualization infrastructure hosted on Proxmox. All core services including identity and authentication, DNS, DHCP, NTP, web hosting, file services, printing, MDR, and logging operate on dedicated virtual machines.

Clients reside on a separate subnet (172.16.112.0/24), divided via VLANs to separate administrative systems from standard user endpoints, reducing lateral movement opportunities. MDR, DNS redundancy, centralized authentication, and a hardened security stack ensure monitoring, availability, and resilience across the environment.

Visualized Topology



System List

All systems except the Hypervisor were joined to the Active Directory and share the domain users: Emmalee, Oscar, Kevin, Anushka, Marc, and Administrator.

System/Service	OS Version	IPv4 address	Local Users	hostname	Purpose & Notes
Hypervisor	Proxmox	172.16.12.1	root	proxmox	Central virtualization platform hosting all VMs
Active Directory Domain Controller	Windows Server 2022	172.16.12.2 172.16.112.2	administrator	ns1.okema.com	AD DS, Group Policy, Primary DNS, DHCP
Secondary DNS	Red Hat Enterprise Linux 10	172.16.12.7	dnssecondary	ns2.okema.com	DNS redundancy and failover
NTP Server	Red Hat Enterprise Linux 10	172.16.12.3	root	time.okema.com	Time synchronization for all hosts
Web Server	Red Hat Enterprise Linux 10	172.16.12.9	webserver administrator	www.okema.com	Hosts organizational website
Docker Container (Wazuh)	Linux Containers on Red Hat Enterprise Linux 10	172.16.12.6	wazuh administrator	wazuh.okema.com	MDR, SIEM, log aggregation
File Server	Windows Server 2022	172.16.12.4	administrator	fp.okema.com	File and Storage Services
Print Server					Print and Document Services
Database Server	Windows Server 2022	172.16.12.5	administrator	database.okema.com	SQL database for applications
Windows Client 1	Windows 11 Education N,	172.16.112.X	Emmalee	win1.okema.com	End-user and administrative

	version 25H2				workstation access
Windows Client 2	Windows 11 Education N, version 25H2	172.16.112.X	Emmalee	win2.okema.com	
*NIX Client 1	Red Hat Enterprise Linux 10	172.16.112.X	nixclient1	nix1.okema.com	
*NIX Client 2	Red Hat Enterprise Linux 10	172.16.112.X	nixclient2	nix2.okema.com	

Applications/Services

- Windows Server 2022
  - All boxes
    - Wazuh Agent 4.14.1
    - RDP
  - ns1.okema.com
    - AD, DNS, DHCP
  - database.okema.com
    - Microsoft SQL 2025 Express Edition
  - fp.okema.com
    - File and Storage Services, Print and Document Services, Windows Print Spooler, SMB 3.1.1
- RHEL 10
  - All boxes
    - Realmd 0.17.1 , sssd 2.9.4, adcli 0.9.2, oddjob 0.34.7, oddjob-mkhomedir 0.34.7, samba-common 4.22.4, samba-common-tools 4.22.3, krb5-workstation 1.21.3, git 2.47, wazuh-agent 4.14.1, nano 8.1
    - SSH 9.9
    - Python 3.14
    - https://github.com/ocapraro/cis-benchmark-macos-audit/tree/rhel
  - time.okema.com
    - Chrony 4.8
  - www.okema.com
    - Httpd 2.4.66 , openssl 3.6.0, mod_ssl 2.4.63

    - wazuh.okema.com
        - Docker 29.0, docker-compose v2
        - wazuh docker container v4.14.1
    - ns2.okema.com
        - Bind 9.18.22
    - RHEL Clients
        - cif-utils, cups, samba-client, samba-common, msodbcsql18-18.3.3.1-1.x86_64.rpm, mssql-tools18-18.2.1.1-1.x86_64.rpm, unixODBC, unixODBC-devel
- Windows 11 Education N, version 25H2
    - All boxes
        - Wazuh Agent 4.14.1
        - RDP

Subnet/VLAN Structure

Okema was supplied with the 172.16.12.0/24 and 172.16.112.0/24 subnets as well as VLAN 12 and VLAN 112. We decided that it would be best to separate our servers from our clients using these VLANs. Our servers were on VLAN 12 with IP addresses in the 172.16.12.0/24 subnet. Our clients were on VLAN 112 with IP addresses in the 172.16.112.0/24 subnet.

These IP addresses were distributed via DHCP by the DHCP server. The DHCP server was assigned two NICs in order to allow clients and servers to talk to each other from different subnets. All systems were on DHCP and were assigned their IP by the combined domain controller, DNS server, and DHCP server (172.16.12.2, 172.16.112.2, ns1.okema.com). The servers have reservations within the DHCP server to ensure their IPs stay the same, while the clients do not and have dynamic addresses in the 172.16.112.0/24 subnet. VLANs were assigned in the Proxmox GUI using VLAN tags. This directs the DHCP server to know which VMs to assign 172.16.12.0/24 addresses and which to assign 172.16.112.0/24 addresses.

Technical Rationale

Windows Server 2022

Windows Server 2022 was chosen for core infrastructure roles, including the Active Directory Domain Controller, database, file, and print servers, due to its robust security, enterprise support, and operational resilience. It provides multi-layered protections such as Credential Guard, Secure Boot enhancements, and improved Kerberos authentication to safeguard credentials and prevent unauthorized access. Full Active Directory and Group Policy support enables centralized identity management, policy enforcement, and consistent configuration across the network. Compatibility with SQL Server, IIS, and other enterprise applications allows seamless integration for database and application services. Built-in features like failover clustering and storage spaces ensure high availability and disaster recovery readiness, while its alignment with CIS Benchmarks and Microsoft security guidance supports compliance and audit readiness.

Windows 11 Education N, version 25H2

Windows 11 Education N, version 25H2 was selected for client endpoints to provide a modern, secure, and manageable environment. The education version of Windows 11 builds off of Windows 11 Enterprise. The system does not include media technology apps like camera, music, movies, and other entertainment services unnecessary to our company. Integration with Active Directory and Group Policy allows centralized management, policy enforcement, and configuration compliance checks. Windows 11 supports remote work capabilities, regular updates, extended support, and automated security patches to reduce vulnerability exposure. This combination ensures a consistent, secure, and user-friendly client environment across the organization.

Red Hat Enterprise Linux 10 (RHEL 10)

RHEL 10 was picked for infrastructure services such as DNS, NTP, and web hosting servers along with linux endpoints due to its enterprise stability, security, and long-term support. SELinux provides mandatory access control to protect critical services even in the event of compromise, and regular patches with kernel hardening reduce exposure to vulnerabilities. RHEL supports a wide range of services, including containerized workloads, webserves, and monitoring agents,

providing operational flexibility. Robust networking, process management, and high-availability features ensure reliable service delivery. Enterprise support through Red Hat subscriptions provide access to tested updates, expert technical support, and official documentation, helping organizations keep systems secure, reliable, and easy to manage while supporting long-term planning. Access to CIS Benchmarks further allows security settings to be tailored to the environment, balancing robust protection with operational flexibility.

AD, Primary DNS, DHCP

Windows Server 2022 was selected to host the AD, DNS, and DHCP services due to its built-in Server Manager application. This application hosts roles and features that align with the aforementioned services. The 2022 version was specifically selected as it is the most recent version of Windows Server that still supports a 2012 R2 domain functional level. Windows Server 2022 is still supported until 2032 and has proven reliability. As well as more documented security controls that can be implemented to harden the system.

Security Implementations:

- Enabled AD DS, DNS, DHCP roles in Server Manager.
- Installed Wazuh agent for log collection.
- Used ChatGPT to reference CIS Benchmarks that were most important to the security of the environment and applied them in the categories below.
- Implemented CIS Benchmarks in categories like authentication, lateral movement, privilege abuse, network exposure, logging integrity, domain compromise.

Secondary DNS

Red Hat Enterprise Linux 10, or RHEL 10, was selected for our secondary DNS server to provide utmost security to this machine. With its built-in support for DNS encryption, this operating system can prevent potential attackers from accessing data within our network via DNS lookup requests. Similar to previous RHEL versions, RHEL 10 enforces strict access controls through SELinux to enhance the overall security posture of the server. Beyond everything, Red Hat Software is particularly known for their thorough lifecycle management cycle, ensuring that potential vulnerabilities found in the wild are protected against through their patch updates.

Security Implementations:

- Only subnets 172.16.12.0/24 and 172.16.112.0/24 are within scope of the configurations.
- System hardening done with CIS RHEL 10 benchmarks to ensure account policies are maintained, services are installed and removed as needed, and baseline configurations are maintained.
- Wazuh Agent installation for logging and visibility purposes.

NTP

Chrony was selected as the service to run our NTP server on. We choose Chrony due to it being specifically optimized for running on virtual machines with internal LAN segments. Using Chrony's configuration file, we can easily dictate which subnets are allowed to use our particular server for time, and block all others. Being built specifically for virtual machines, if any machine goes offline then back online later on, Chrony has no problem re-syncing their clock, coming to be even more accurate than traditional NTP services. It's also free to use and lightweight, great for our expanding workforce.

Security Implementations:

- Only our subnet is allowed to get time from this service. All other connections are blocked.
- Comes with tracking to see exactly what boxes are using the server.
- Pools can be reconfigured with a singular command.

Webserver

RHEL 10 was picked to run the webserver since, as was mentioned earlier, the Red Hat environment provides many baked-in security features via SELinux. The webserver itself was hosted using apache2, allowing for seamless setup, and after joining the webserver to the domain and allocating it a static ip, it could be accessed from anywhere on our network at www.okema.com. The webserver is hosted on its own VM rather than doubling up with any of the other RHEL services, as in a production environment, the webserver would be the most public facing endpoint, and therefore the one most accessible to an attacker. Because of this, this box is isolated so that in the case of a breach, the attacker would not have immediate access to any other services, and the threat could be easily quarantined without requiring the disruption of any other server. To further shore up this service, an automated script was run which, to the best of our abilities, implemented all automateable RHEL 10 CIS benchmark

controls up to server level implementation, with the exception of 1.2.1.3: Ensure repo_gpgcheck is globally activated. This control was left off, as RHEL 10 is quite new, and not all of its repositories have the required .asc signature files yet, so when this control is in place, none of the package managers will work. The built in security of Red Hat, along with the additional hardening is sufficient to make the webserver a public facing application, without the fear of immediate breach.

Security Implementations:

- Enabled httpd to be run in a SELinux environment.
- HTTPS enabled with private CA.
- CA distributed through GPO.
- Redirecting from http to https by default.
- Enabled auditing for remote access and system health through Wazuh.
- Enabled vulnerability detection through Wazuh.
- Disabled default root account.
- Implemented CIS L3 RHEL 10 benchmark controls.

Docker Container (Wazuh)

The Docker VM is also run on RHEL 10 for all the previously mentioned reasons, and because Docker is built for a linux environment, so running it on a Windows machine would have been needlessly complex. Wazuh was chosen as the service to be run using Docker. Some form of centralized logs was required, and Wazuh provides that along with real-time vulnerability protection, and XDR services. All of the devices on our network were connected to Wazuh as agents, so it could provide constant monitoring of all of our endpoints. Configuring Wazuh using Docker makes for a much cleaner environment, as Wazuh is broken up into 3 different services, the Dashboard, Manager, and Indexer. Docker allows these to each be in their own container, which keeps our services separated. This machine also has no other services on it, since Wazuh is such an important part of our security system that creating any more access points than necessary would leave us vulnerable.

Security Implementations:

- All services are run through docker containers to reduce access points.
- Enabled auditing for remote access and system health through Wazuh.
- Enabled vulnerability detection through Wazuh.
- Disabled default root account.
- Implemented CIS L3 RHEL 10 benchmark controls.
- Disabled GUI to limit attack surfaces.

File & Print Server

Windows Server 2022 was selected to host both file and print services due to its strong integration with Active Directory, reliable SMB 3.1.1 file sharing, and built-in Print and Document Services. Using Windows Server allows centralized management of shared folders, NTFS permissions, and printer deployment through Group Policy. The platform supports secure access control, consistent configuration, and straightforward administration through Server Manager. Together, these features provide a stable and manageable environment for shared storage and organizational printing needs.

Security Implementations:

- Enabled File and Storage Services role for file sharing.
- Enabled Print and Document Services role for centralized printer management.
- Configured SMB 3.1.1 file sharing for network access.
- Applied NTFS permissions to secure shared folders.
- Restricted access to authorized users and groups only.
- Enabled Windows Print Spooler for print job handling.
- Enabled auditing for file access and print job activity through Wazuh.
- Hardened the system following CIS Level 1 (L1) benchmarks, including account policies, service restrictions, and system configuration baselines.

Microsoft SQL Server 2025 Express Edition

Microsoft SQL Server 2025 Express Edition was chosen because it holds all the core functionality and features of the newest Microsoft SQL server, while also coming in a free package, yet still offers enough functionality for our small team. Express edition comes with SQL Server Data Tools, full text to speech, and the new Microsoft SQL Server 2025 machine learning integration. Alongside this, as our company expands, we can easily upgrade Express Edition to higher end editions of SQL Server, to accommodate for higher database strain and an increased workforce. Lastly, by using SQL Server 2025 instead of prior versions, we have an increased relational database size, and it comes with all advanced features that in previous editions cost extra.

Security Implementations:

- Installed Wazuh for log collection and database visibility.
- Windows Firewall configured for Database Engine Access.
- Configured to force all connections to be encrypted.

- Drive level Bitlocker in case of database takeover.
- CIS Benchmarks implemented via GPO (See AD technical rationale).

Windows 11 Clients

Please refer to the above Windows 11 OS technical rationale. The Windows 11 Clients were joined to the Active Directory Domain and received their IP addresses from the DHCP server. They were assigned IP addresses on the 172.16.112.0/24 subnet to separate them from the servers on our infrastructure. This prevents lateral movement, protects critical infrastructure, implements least privilege, and reduces the attack surface.

Security Implementations:

- Installed Wazuh agent for log collection.
- Hardened the system following CIS Level 1 (L1) benchmarks, including account policies, service restrictions, and system configuration baselines.
- Assigned VLAN 112 (Client-only network) and 172.16.112.0/24 IP address.

*NIX Clients

The Red Hat Enterprise Linux 10 (RHEL 10) clients were integrated into the Active Directory (AD) domain and provisioned IP addresses via the enterprise DHCP server. These clients were assigned to the 172.16.112.0/24 subnet on VLAN 112, a client-only network segment designed to isolate endpoints from core infrastructure systems. This segmentation strategy reduces the attack surface, limits lateral movement opportunities, enforces least privilege, and helps preserve the integrity of critical services.

Security Implementations:

- Wazuh agent installed for endpoint monitoring and centralized log collection.
- System hardened using CIS RHEL 10 Benchmarks, including strengthened account policies, restricted unnecessary services, and baseline configuration enforcement.
- Placed on VLAN 112 with addresses in the 172.16.112.0/24 network to ensure strict separation from server infrastructure.

MITRE ATT&CK Technique Analysis

T1190- Exploit Public Facing Application. This technique is when attackers exploit internet-facing hosts to initially breach a network. The takeover of these internet-facing hosts are then used to attack the rest of the network, affecting computers and networks that adversaries might not even know about. Our environment would be able to prevent this from happening, or at least detect if it was. Our reasoning behind this is as follows:

- Our environment is hardened with CIS benchmarks, preventing any easy, open exploits from being available.
- Wazuh's logging could see any suspicious activity going on inside of our network, and aggregate that information so we could quickly detect its presence.
- Wazuh's vulnerability detection aggregates known CVE's and tests our network against them, ensuring we stay protected.
- Each part of the network is segmented, meaning initial compromise of an internet-facing application wouldn't lead to any more takeover.
- Our environment is completely isolated from the internet, with all connections outside of our internal LAN being blocked.

T1548.003- Abuse Elevation Control Mechanism: Sudo and Sudo Caching. This technique is when attackers abuse the sudo command via sudo caching or changing the sudoers file to elevate privileges. These escalated privileges are then used to create persistence on a network, spawn processes with higher privileges, or modify/read data that they shouldn't have access to. Our environment would be able to prevent this from happening, or at least detect if it was. Our reasoning behind this is as follows:

- Due to following the CIS L3 RHEL 10 Benchmark Controls, our Linux systems automatically have NOPASSWD entries disabled and sudo audit logging, as well as disabling the sudo timestamp timeout, making this attack much harder to execute.
- Wazuh's File Integrity Monitoring watches /etc/sudoers and /etc/sudoers.d, meaning any change to these files would create an alert.
- Wazuh automatically captures all sudo or su executions, ensuring any executions are logged, and the path can be detected.

T1566.001-Phishing: Spearphishing Attachment. This technique is when attackers send emails with malicious attachments to attempt to take over a victim's computer when they are opened or executed. Given that these attacks rely on social engineering tactics to try and manipulate the user into believing that they are valid, they are frequently successful in penetrating internal systems. It is our belief that our environment does not have sufficient permissions to prevent this attack, or detect if it was happening. We do not have any specific phishing training that our employees must take, and we don't have any attachment scanning software installed that would first ensure that an attachment is valid and doesn't contain malware before opening. We do have auditing software that could log if any malicious attachment was run, but we can't be positive that it would properly catch this.

T1053.005- Scheduled Task/Job: Scheduled Task. This technique is when attackers abuse the Windows Task Scheduler to perform scheduling of malicious code. This can be used as a form of persistence, as part of lateral movement, to run a process under a different account or to mask execution under trusted system processes. Our environment would be able to prevent this from happening, or at least detect if it was. Our reasoning behind this is as follows:

- By following the CIS benchmarks, our system limits who can create tasks, and every task that is created is logged.
- Wazuh constantly monitors these logs and file changes. Any creation of a task with an unfamiliar name, strange path, or running as SYSTEM, would create an alert within Wazuh for us to see.
- Because of our segmented system, it is impossible to create a scheduled task remotely, which would make the execution of this vulnerability much harder. An attacker would already have to have access to our physical location as well as proper administrative permissions.

T1055- Process Injection. This technique is when attackers inject malicious code into processes. This allows them to evade defenses, escalate privileges, and hide for longer periods of time, masking as important system executables. This method of executing arbitrary code in other live processes allows attackers access to the processes memory, resources and privileges. Given our current protections and hardening of systems, we are still vulnerable to this attack. While Wazuh can collect logs and analyze events, it doesn't have the capability to inspect running memory, which is what would detect this type of attack. Once the process is injected, Wazuh will see the legitimate process functioning as normal. We need to implement EDR systems.

Applicable CTI Analysis

One CTI report that is applicable to our environment would be CRON#TRAP, as written about on here:
https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/
This attack campaign targets Windows clients, leveraging malicious .lnk files delivered through phishing to extract and initiate a custom Linux environment with QEMU. Once the phishing link is clicked, firstly it uses explorer.exe to say that there is a server error (to dismiss suspicion of the link not doing anything) and secondly executes the QEMU process (renamed to avoid suspicion) which holds the malware. Once the QEMU process is started, it opens a Linux environment which is already pre-configured with a backdoor that automatically connects to the attacker's C2 server. The C2 server has many functions, including checking for network connectivity, loading additional tools/malware, establishing further persistence and even enabling further remote access. Here is the full list of MITRE ATT&CK Techniques identified in the report, and how Okema Cyber would measure up to all of them:

T1566.001: Phishing: Spearphishing Attachment - Okema Cyber would not be able to protect this from happening, nor detect if it was happening. Okema Cyber doesn't have any specific email attachment scanning software that would detect if an attachment was malicious. In addition to this, we don't have any specific mandatory phishing training for employees to go through.

T1071.001: Application Layer Protocol: Web Protocols - Okema Cyber would be able to protect this from happening, as well as detect if it was happening. For protecting it from happening, because Okema is inside of an environment that cannot connect to the internet, it is impossible to communicate with outbound C2 servers. In addition to this, Wazuh includes outbound connection monitoring, and if we saw this as suspicious, we would stop the communication.

T1132: Data Encoding - Okema Cyber would be able to protect this from happening, however we would not be able to detect this if it was happening. We would be able to protect it from happening because we are in an airgapped environment, meaning that all external C2

connections aren't possible. However, we wouldn't be able to detect it if it was happening, because none of the security software used checks outgoing traffic, or disallows encoded traffic.

T1572: Protocol Tunneling - Okema Cyber would be able to protect this from happening, and we would be able to detect if this was happening. We would be able to protect it from happening because we are in an airgapped environment, meaning that all external C2 connections aren't possible. We would be able to detect if this was happening because Wazuh includes outbound connection monitoring, meaning when Wazuh sees that a strange protocol is making outbound traffic, it would create an alert.

T1027: Obfuscated Files or Information - We wouldn't be able to protect this from happening, however we may be able to detect if it was happening. Our hardened systems from benchmarks wouldn't stop obfuscated files from being run, but every executable run is logged in Wazuh, and depending on the level of obfuscation, we would be able to see it.

T1036: Masquerading - We wouldn't be able to protect this from happening, however we may be able to detect if it was happening. None of our protections prevent files or executables from being run, but it would still be logged in Wazuh, and depending on the level of masquerading and how skillful we are at viewing the logs, we may be able to catch it.

T1218: System Binary Proxy Execution - We wouldn't be able to protect this from happening, however we would be able to detect if it was happening. None of our protections prevent binary proxy executions, however because of Wazuh's monitoring, we would be able to see that this was happening within our system.

T1564.006: Hide Artifacts: Run Virtual Instance - We would not be able to protect this from happening, nor would we be able to detect if it was happening. Our CIS benchmarks don't prevent virtual instances from running, and because of the highly unique nature, it also wouldn't show up on Wazuh.

T1059.001: Command and Scripting Interpreter: PowerShell - We would not be able to prevent this from happening, however we would be able to detect if it was happening. None of our CIS benchmarks or software disallows PowerShell from running, however everytime PowerShell is

run, it generates Wazuh logs. So, we would see that PowerShell was spawned from a .lnk file, and detect that it's malicious.

T1059.003: Command and Scripting Interpreter: Windows Command Shell - We would not be able to prevent this from happening, however we would be able to detect if it was happening. None of our CIS benchmarks or software disallows Windows Command Shell from running, however everytime it is run, it generates Wazuh logs. So, we would see that Shell was spawned from a .lnk file, and detect that it's malicious.

T1204.001: User Execution: Malicious Link - We would not be able to prevent this from happening, however we would be able to detect if it was happening. None of our CIS benchmarks or software disallows malicious links from running, but we would see through Wazuh that the resulting process chain is suspicious, and detect that it's malicious.

T1204.002: User Execution: Malicious File - We would not be able to prevent this from happening, however we would be able to detect if it was happening. None of our CIS benchmarks or software disallows malicious files from running, but we would see through Wazuh that the resulting process chain is suspicious, and detect that it's malicious.

T1072: Software Deployment Tools - We would be able to protect this from happening, and we would be able to detect if it was happening. Okema Cyber doesn't have any centralized software suites installed that could be used to execute commands and move laterally though the network. In addition, Wazuh would detect unauthorized software deployment tools being used to move across the network, and would create alerts.

T1041: Exfiltration Over C2 Channel - We would be able to protect this from happening, and we would be able to detect if it was happening. Because Okema Cyber uses an airgapped environment, it is impossible to establish a connection to a C2 channel, let alone exfiltrate data over to it. In addition, Wazuh would show the suspicious outbound connection for us to see.

Works Cited

Center for Internet Security. (n.d.). CISsecurity.org. CIS Benchmarks List. Retrieved Dec 8, 2025, From https://www.cisecurity.org/cis-benchmarks?gad_source=1&gad_campaignid=1751678049&gbraid=0AAAADLJ4LKkOp8NZ0Fxk_5bIK8bL6rWD&gclid=Cj0KCQiAi9rJBhCYARIsALyPDttFWIA0KEA_vNLUsSRuSGzA4kOd7CTi3i2IHMZE_P-uDVbTj8suQtwaAvYLEALw_wcB

MITRE. (n.d.). MITRE ATT&CK®. Retrieved Dec 8, 2025, from https://attack.mitre.org/

Securonix. (2024, Nov 04). securonix.com. CRON#TRAP: Emulated Linux Environments as the Latest Tactic in Malware Staging. Retrieved 12 08, 2025, from https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/

SmartDraw. (n.d.). Document Your Cloud Infrastructure Automatically. Retrieved Dec 8, 2025, from https://www.smartdraw.com/it/it-infrastructure.htm