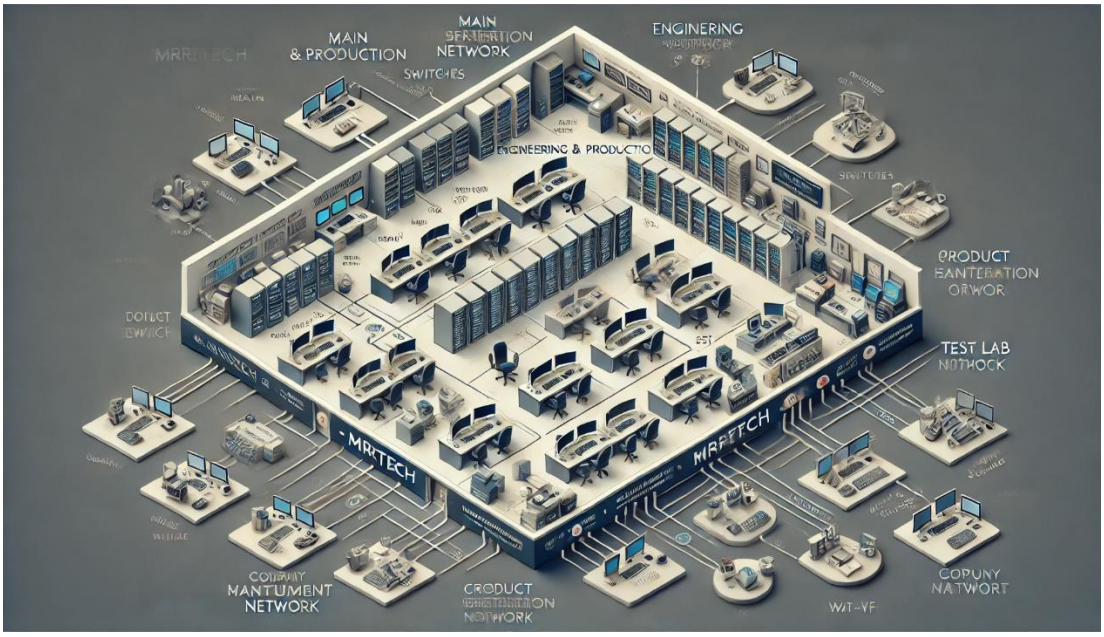
SYSTEM A

This document outlines the System Under Evaluation (SUE) that will be utilized for the Cyber Defensive Capability Performance Measurement Development Challenge, Phase 3 Demonstration. It serves as a reference for participants as they develop and test their solutions during Phase 2 of the challenge. The goal is to establish a baseline SUE configuration that all teams will use for their solution demonstrations. Participants are also encouraged to create additional SUE configurations to further showcase their solution capabilities within the timeframe allocated for the Phase 3 Demonstration Brief and solution demonstration.

To further clarify the challenge objectives, this document presents a fictional scenario involving a small business, "MRZTech." MRZTech is a company that develops, tests, fields, and supports advanced technology products that meet a unique market demand. Customers of MRZTech are highly satisfied with its products, which have become critical components in the customers' essential missions. As a result, MRZTech must maintain certain core internal operations to continuously meet customer requirements. Figure 1.0-1 depicts the MRZTech facility layout, which includes separate areas for (a) Engineering and Production Management, (b) Test Engineering, (c) Production (excluded from this challenge evaluation), (d) Information Technology and Cybersecurity, and (e) Company Management. Additionally, the facility has a Main Lobby for visitors, with a Security Guard controlling access during normal business hours. Potential vulnerabilities in the facility layout could impact MRZTech's cyber resilience in the event of an external or internal threat. Competitors and foreign entities have a keen interest in obtaining MRZTech's product designs, test data, and unique Intellectual Property (IP).



The company has implemented a comprehensive suite of physical and cybersecurity measures to ensure a highly secure operational environment:

Facility and Environmental Security

1. Flood Risk Mitigation: The facility is equipped with flood barriers and water detection systems, given its proximity to a river and location within a floodplain. A regularly updated flood response and evacuation plan is in place to maintain preparedness.

2. Main Entrance Security:

- The Security Guard desk at the main entrance is staffed 24/7, including weekends, with security personnel controlling access and ensuring doors are securely closed at all times.

- Automatic locking systems are installed on all doors, with controlled access for employees, and a policy is enforced to verify that doors are fully closed and locked after hours.

- The production floor door has been upgraded with a secure electronic access control system, which replaces the previous key-based system, limiting access to authorized personnel only.

3. After-Hours Alarm System:

- A comprehensive alarm system now monitors all facility entry points, managed by a professional security service over a secure, encrypted connection.

- Each employee has a unique access code, and the system alerts security personnel immediately upon after-hours entry, ensuring prompt response.

Information Technology (IT) Equipment Room Security

4. Controlled IT Room Access:

- Biometric access controls and electronic locks have been installed on the IT equipment room door, limiting entry to authorized IT staff only.

- The door is equipped with an automatic locking mechanism that activates after 5 minutes of inactivity.

- All equipment racks and storage cabinets are secured with individual locks, preventing unauthorized access.

5. Enhanced Physical Security for Engineering and Production Areas:

- Keycard access control has been installed on the Engineering and Production room door, restricting entry to authorized personnel.

- CCTV monitoring covers all employee and visitor-accessible areas, with secure storage of video recordings.

6. Secured Product Testing Room:

- The Product Testing room door now features electronic access controls, accessible only by authorized staff from the Engineering and Production team.

- Motion detectors and surveillance cameras continuously monitor activity within the room for enhanced security.

7. Restricted Access to Management Offices:

- The Company Management Office suite is secured with a PIN keypad access system that logs entries and alerts security personnel to any unauthorized access attempts.

- Individual offices within the suite are now equipped with electronic locks, providing additional protection for sensitive areas.

8. Controlled Access to Production Floor:

- An electronic access control system secures the door between the Engineering and Production areas and the Production floor, limiting entry to designated personnel. A new key has been procured and is securely managed.

- Physical access control policies and procedures are regularly reviewed and reinforced.

Information System and Cybersecurity Policies

9. IT Staff Training and Certification:

- All IT staff have obtained and are maintaining up-to-date cybersecurity certifications relevant to their roles.

- Ongoing cybersecurity training programs and periodic refresher courses are in place, ensuring staff are informed of the latest security protocols and threats.

10. Firewall and Intrusion Prevention System (IPS):

- Firewall IPS rulesets are routinely updated, ensuring continuous protection against emerging threats.

- Regular audits and reviews are conducted to maintain an optimal network security posture.

11. End-of-Life Equipment and Vulnerability Patching:

- All hardware and software components that reached end-of-life have been replaced with supported versions to guarantee the availability of security patches.

- A strict patch management schedule ensures that all systems are regularly updated with the latest security patches.

12. Regular Vulnerability Scanning and Monitoring:

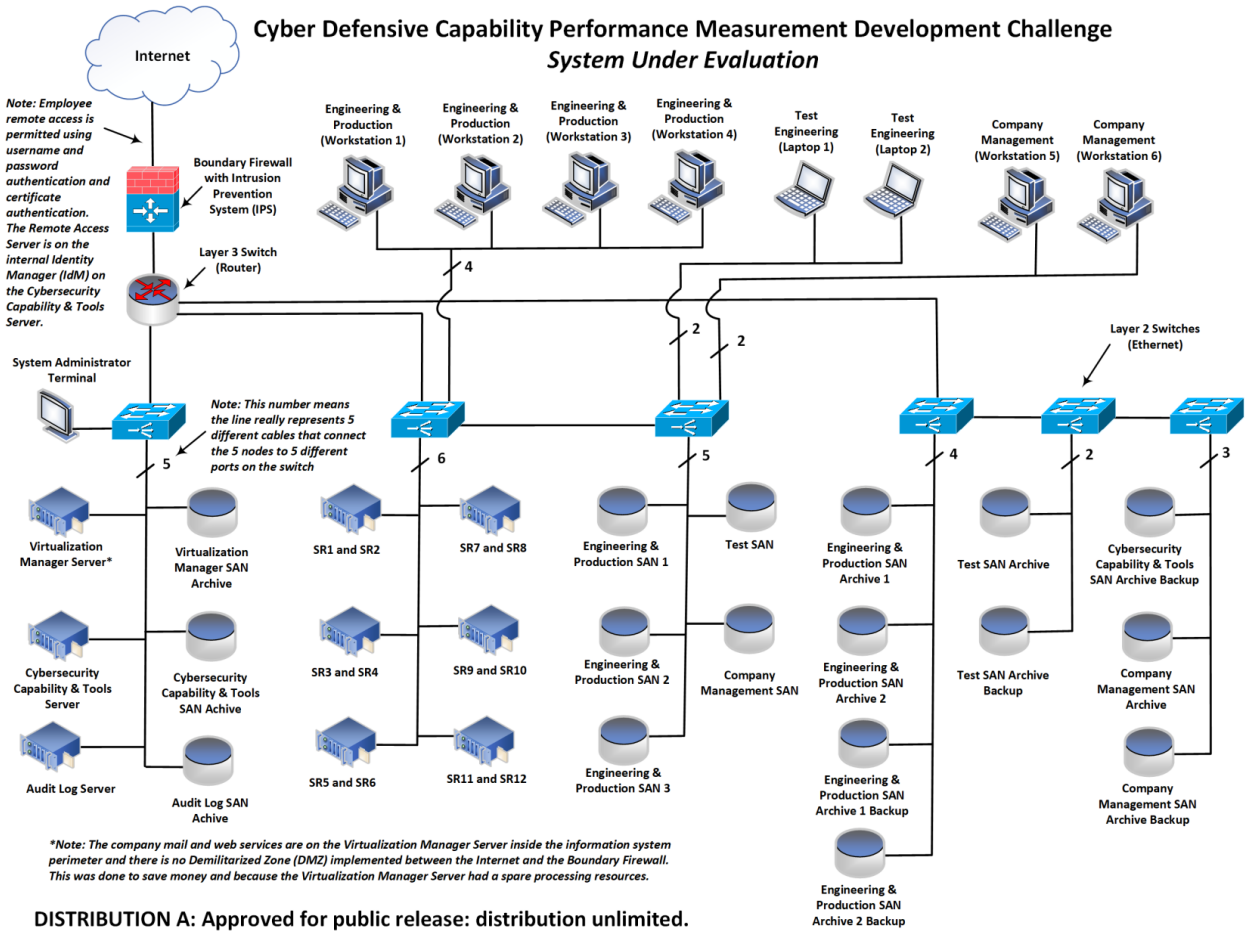
- The Nessus vulnerability scanner is kept up-to-date with the latest plugins, and regular vulnerability scans are conducted.

- A designated team member reviews scan results and promptly addresses vulnerabilities, including applying alternative security measures where necessary.

13. Role-Based Access Control (RBAC) Enforcement:

- Stringent role-based access control (RBAC) policies are enforced, with privileges restricted based on roles and responsibilities.

- Regular access reviews and audits are conducted to ensure compliance with RBAC policies, with adjustments made as necessary to reflect any changes in staff duties.



The following sections describe the highly secure configuration of the information system equipment racks, including hardware and software, that will form part of the system under evaluation. Proprietary application software developed by the company for engineering, production, test engineering, and management functions will not be directly evaluated, as the company asserts it is free of vulnerabilities. Instead, the challenge will focus on the critical functions supported by the software, as well as the operating systems and commercial cybersecurity tools in use.

3.2.1 Boundary Defense and System Administration Rack

As depicted in Figure 3.2.1-1, the facility includes a highly secure Boundary Defense and System Administration Rack, featuring a Cisco Firepower Firewall with an integrated Intrusion Prevention System (IPS). All inbound and outbound network traffic is routed through the firewall, with customized rulesets ensuring only essential data flows are permitted. The IPS is continually updated with the latest Cisco threat signatures to detect known cyber attacks. Specific alert types and automated response protocols are configured by the IT System Administrator for each category of threat, providing robust and dynamic defense.

The rack also includes a Cisco Layer 3 Switch, which securely interconnects all internal rack components and interfaces with other facility equipment racks. Network traffic that successfully passes through the firewall is subsequently routed via the Layer 3 Switch to its designated endpoint, ensuring streamlined and secure data transmission.

Additionally, the rack hosts Dell PowerEdge Servers, each dedicated to specific functions: Virtualization Management, Cybersecurity Tools and Capabilities, and a Computer and Network Audit Log Server. Each server is linked to a dedicated, high-capacity Storage Area Network (SAN) for data storage and backup. These servers are designed to handle critical operational loads, while ensuring secure data storage and access.

For on-site management, the rack is equipped with an integrated monitor, keyboard, and trackball, providing a secure workstation for the System Administrator. This setup enables configuration, cybersecurity monitoring, user account management, and virtualization

tasks, with virtual machines dynamically managed for production and testing. A central patch panel is also installed for cable management and allows quick reconfiguration if needed. An Uninterruptible Power Supply (UPS) with a power conditioner provides emergency backup power to maintain operations during power outages, ensuring resilience.

Cybersecurity Tools and Capabilities

The Cybersecurity Suite is comprehensive, including an Identity Management (IdM) Server, Splunk Security Information and Event Management (SIEM) system, McAfee Anti-Virus, and Nessus Vulnerability Scanner. These tools enable continuous monitoring and protection of facility operations:

- The SIEM aggregates security events, providing real-time analysis for early threat detection. The IT System Administrator continuously monitors this system and responds to alerts as per the cybersecurity policy.

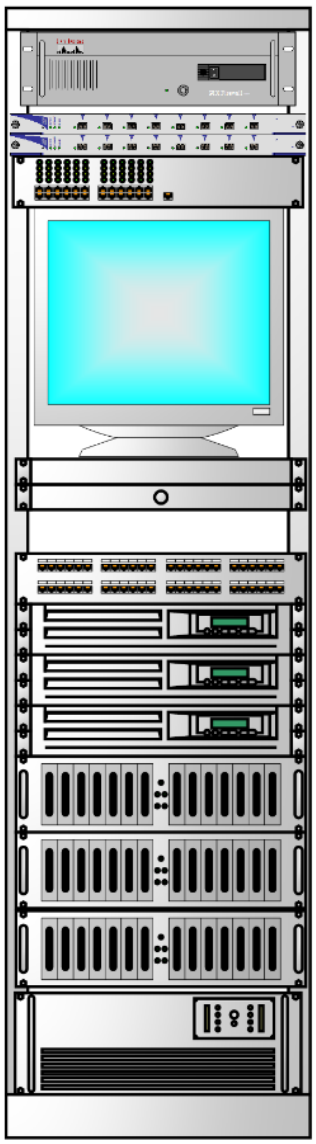
- McAfee Anti-Virus and Nessus scans are regularly performed across all systems, ensuring comprehensive threat detection and compliance with the company’s cybersecurity protocols.

- The Identity Management (IdM) server enforces role-based access control, managing user identities and ensuring only authorized personnel have access to specific resources.

The System Administrator performs monthly audits of user accounts, verifying role assignments and access permissions in line with cybersecurity policies. This rigorous process ensures that access remains restricted to authorized users, supporting the company’s commitment to the highest levels of cybersecurity and data integrity.

In summary, this secure and redundant system architecture underpins the facility's cyber defense strategy, combining advanced hardware, industry-leading software tools, and rigorous operational policies to protect against a wide array of threats while ensuring operational resilience and data integrity.

Boundary Defense and System Administration Rack



Cisco Firepower 4125 with IPS

Cisco Meraki MS425-32 Layer 3 Switch (Router)

Cisco Catalyst 2960-X Ethernet Switch

Patch Panel

PowerEdge R750 ESXi Servers (Virtualization Manager)

PowerEdge R750 ESXi Servers (Cybersecurity Capability & Tools)

PowerEdge R750 ESXi Server (Audit Log Server)

PowerVault ME5024 SANS (Audit Log Archive)

PowerVault ME5024 SANS (Cyber Capability & Tools Data Archive)

PowerVault ME5024 SANS (Virtualization Manager Archive)

Uninterruptible Power Supply (UPS)

Node	Make	Hardware Description	Software Node	Software Make	Software Description	Software Version
Firewall	Cisco	Cisco Firepower 4200 NGFW with Threat Defense (1U, rack mountable)	Firewall			

| Cisco | Cisco FirePower 4200 with Firepower Threat Defense (FTD) | 7.0
Layer 3 Switch (Router) | Cisco | Cisco Meraki MS450-48 Layer 3 Cloud Managed Switch | Layer 3 Switch (Router)
| Cisco | Cisco Meraki MS450-48 Layer 3 Switch Firmware | 2023-04-15
Layer 2 Switch (Ethernet) | Cisco | Cisco Catalyst 9300 Series Layer 2 Switch (Gigabit Ethernet) | Layer 2 Switch (Ethernet)
| Cisco | Cisco Catalyst IOS XE
| 17.3.4
Rack Monitor/Keyboard | Dell | Dell KM713 Rack Mounted Monitor, Keyboard, and Mouse | Virtualization Manager Server
| VMware | VMware vSphere Hypervisor (ESXi)
| 7.0
Rack Server | Dell | Dell PowerEdge R760 (2U, 4th Gen Intel Xeon Scalable processors, up to 60 cores per processor) |
Cybersecurity Capability & Tools Server | RedHat | RedHat Enterprise Linux (RHEL) | 9.2
Storage Area Network (SAN) | Dell | Dell PowerVault ME5084 Storage Area Network (SAN) | Cybersecurity Capability & Tools Server | Trellix | Trellix (formerly McAfee) Endpoint Security | 10.7.0
Patch Panel | Panduit | Panduit DP245E88TGY 48-Port Patch Panel (Cat6A, 1U Rack-Mount) | Cybersecurity Capability & Tools Server | Tenable | Nessus Vulnerability Scanner
| 10.5.1
Uninterruptible Power Supply | APC | APC Smart-UPS SRT3000RMXLA (3kVA, 2U Rackmount, Lithium-Ion) | Audit Log Server
| Splunk | Splunk Enterprise Security (SIEM)
| 9.0
Miscellaneous | Miscellaneous | Miscellaneous Components (cables, rails, retractors, power strip, etc.) | Audit Log Server
| RedHat | RedHat Enterprise Linux (RHEL)
| 9.2

The Server Rack, as illustrated in Figure 3.2.2-1, is a critical infrastructure component that provides secure, centralized computing resources for all company functions, including engineering, production, test engineering, and management. The IT and cybersecurity systems are isolated on a dedicated Boundary Defense and System Administration Rack (Section 3.2.1) to ensure robust security controls. The Server Rack houses multiple Dell PowerEdge R750 ESXi Servers and Dell PowerVault Storage Area Network (SAN) servers, which are utilized within the facility to:

a. Deliver secure access to product design, development, and testing tools, ensuring that proprietary methodologies are protected.

b. Process and securely display technical data library artifacts that describe systems and products under development, including sensitive Intellectual Property (IP) information critical to company operations.

c. Operate the Help Desk Response Ticketing System, which includes software for tracking customer inquiries and comments. Help Desk operators in the engineering and production areas securely access the system from authorized workstations.

d. Support a virtualized Test and Analysis Environment for the secure development, testing, and analysis of software products.

e. Host a secure training environment designed to enhance workforce knowledge and skill development across the organization.

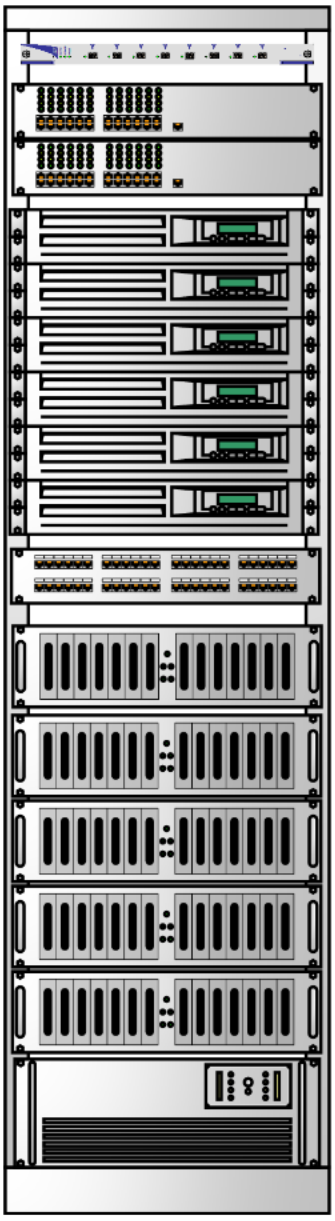
f. Provide protected computing resources for critical company management functions, including Human Resources, Payroll, Legal, Contracts, and executive operations.

The Server Rack also includes Cisco Catalyst Ethernet Switches, which securely interconnect the servers and SAN units, along with a Cisco Meraki Layer 3 switch that enables secure scalability by connecting to additional server racks as needed. The patch panel facilitates efficient and secure reconfiguration of connections within the rack when adjustments are required.

An Uninterruptible Power Supply (UPS) with advanced surge protection and power conditioning is integrated into the Server Rack, providing emergency power during primary power disruptions. This setup enables a controlled shutdown of systems or continuous operation until backup power sources are activated. Tables 3.2.2-1 and 3.2.2-2 list the

hardware and software components within the Server Rack, ensuring a comprehensive and secure solution for the company's critical computing needs.

Server Rack



Cisco Meraki MS425-32 Layer 3 Switch (Router) – NOT USED

Cisco Catalyst 2960-X Ethernet Switch

Cisco Catalyst 2960-X Ethernet Switch

PowerEdge R750 ESXi Servers (SR1 and SR2)

PowerEdge R750 ESXi Servers (SR3 and SR4)

PowerEdge R750 ESXi Servers (SR5 and SR6)

PowerEdge R750 ESXi Servers (SR7 and SR8)

PowerEdge R750 ESXi Servers (SR9 and SR10)

PowerEdge R750 ESXi Servers (SR11 and SR12)

Patch Panel

PowerVault ME5024 SAN (Engineering & Production 1)

PowerVault ME5024 SAN (Engineering & Production 2)

PowerVault ME5024 SAN (Engineering & Production 3)

PowerVault ME5024 SAN (Test)

PowerVault ME5024 SAN (Company Management)

Uninterruptible Power Supply (UPS)

Make	Hardware Description

Cisco	Cisco Catalyst 9300 Series Layer 2 Gigabit Ethernet Network Switch	
Dell	Dell PowerEdge R760 (2U, Intel C741 chipset, up to two 4th Gen Intel Xeon processors with up to 60 cores)	
Panduit	Panduit DP245E88TGY 48-Port Patch Panel (1U Rack-Mount, Cat6A, RJ45)	
Cisco	Cisco Meraki MS450-48 Layer 3 Switch (48 ports, 10 Gb)	
Dell	Dell PowerVault ME5084 Storage Area Network (SAN)	
APC	APC Smart-UPS SRT3000RMXLA (3kVA, 2U rackmount, Lithium-Ion)	
Miscellaneous	Miscellaneous Components (rack cables, equipment rails, cable retractors, power strip, screws, etc.)	

Node	Software Make	Software Description	Software Version
Layer 2 Switches (Ethernet)	Cisco	Cisco Catalyst IOS XE	17.3.4
Servers SR1 and SR2	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Servers SR3 and SR4	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Servers SR5 and SR6	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Servers SR7 and SR8	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Servers SR9 and SR10	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Servers SR11 and SR12	Microsoft	Windows Server 2022	Windows Server 2022
Engineering & Production SAN 1	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Engineering & Production SAN 2	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Engineering & Production SAN 3	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Test SAN	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Company Management SAN	RedHat	RedHat Enterprise Linux (RHEL)	9.2

3.2.3 Secure Bulk Data Storage Rack

The Secure Bulk Data Storage Rack, depicted in Figure 3.2.3-1, includes multiple Dell PowerVault Storage Area Network (SAN) units, designed to provide robust, encrypted archive storage for all facility areas, including engineering, production, test engineering, IT, cybersecurity, and management. Advanced encryption protocols ensure that all data is securely stored at rest, with separate, dedicated SAN drives assigned to each functional area for enhanced data segregation and security.

Sensitive data, such as technical product data, test results, Intellectual Property (IP), and other critical business information, is encrypted using AES-256 encryption, both at rest and during transmission. Additionally, automatic archive replication to a redundant backup SAN unit within the same rack ensures immediate failover capabilities in the event of primary archive failure, maintaining data integrity and availability.

The SAN units provide secure storage for the following data categories:

a. IT Operations and Cybersecurity Data: All data from IT operations, cybersecurity monitoring, and cyber incident response activities is stored securely, with strict access controls in place.

b. Product IP and Sensitive Corporate Data: Proprietary product designs, Intellectual Property, financial records, and contract agreements are securely stored and protected against unauthorized access.

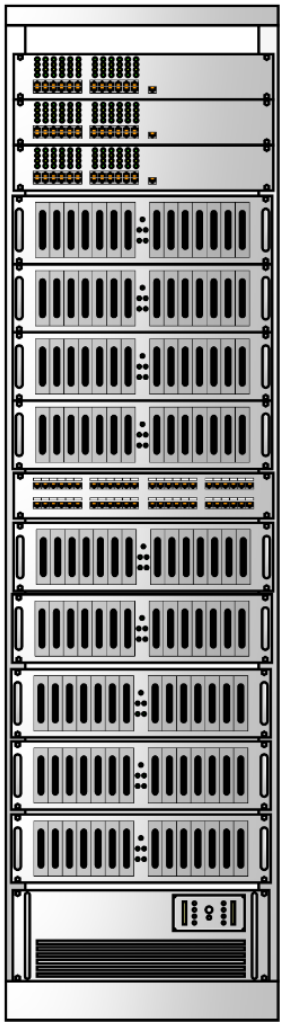
c. Test and Analysis Data: Critical test and analysis data, including test reports, are securely archived to support product validation and regulatory compliance.

d. Corporate Sensitive Information: Financial records, legal documents, contract data, HR information, payroll, and other sensitive corporate data are stored in a segregated, encrypted SAN environment, ensuring confidentiality and compliance with data protection regulations.

The SAN components are interconnected through Cisco Catalyst Layer 2 Ethernet switches, which connect to the Layer 3 switch (router) in the Boundary Defense and System Administration Rack (Section 3.2.1) over a secure, encrypted VLAN. A central patch panel within the rack simplifies cable management and facilitates rapid reconfiguration when necessary, maintaining flexibility while ensuring a secure physical and logical layout.

An Uninterruptible Power Supply (UPS) with advanced power conditioning and surge protection is included in the rack. The UPS provides emergency power to ensure continuity during primary power outages, enabling a controlled shutdown or sustained operation until backup power is activated. Tables 3.2.3-1 and 3.2.3-2 provide a detailed inventory of the hardware and software used within the Secure Bulk Data Storage Rack, confirming the integration of high-assurance storage technologies to protect critical data assets.

Bulk Data Storage Rack



Cisco Catalyst 2960-X Ethernet Switch

Cisco Catalyst 2960-X Ethernet Switch

Cisco Catalyst 2960-X Ethernet Switch

Dell PowerVault ME5024 SAN (Engineering & Production Archive 1)

Dell PowerVault ME5024 SAN (Engineering & Production Archive 2)

Dell PowerVault ME5024 SAN (Engineering & Production Archive 1 Backup)

Dell PowerVault ME5024 SAN (Engineering & Production Archive 2 Backup)

Patch Panel

Dell PowerVault ME5024 SAN (Test Archive)

Dell PowerVault ME5024 SAN (Test Archive Backup)

Dell PowerVault ME5024 SAN (Cybersecurity Capability & Tools Archive Backup)

Dell PowerVault ME5024 SAN (Company Management Archive)

Dell PowerVault ME5024 SAN (Company Management Archive Backup)

Uninterruptible Power Supply (UPS)

Make	Hardware Description
Cisco	Cisco Catalyst 9300 Series Layer 2 Gigabit Ethernet Network Switch (AES-256 encrypted VLAN support)
Dell	Dell PowerVault ME5084 Storage Area Network (SAN) with secure AES-256 encryption at rest and replication
Panduit	Panduit DP245E88TGY 48-Port Patch Panel (1U Rack-Mount, Cat6A, RJ45)
Cisco	Cisco Meraki MS450-48 Layer 3 Switch (48 ports, 10 Gb) with full encryption support
APC	APC Smart-UPS SRT3000RMXLA (3kVA, 2U rackmount, Lithium-Ion, advanced surge protection)
Miscellaneous	Miscellaneous Components (rack cables, equipment rails, retractors, power strip, screws, etc.)

Node	Software Make	Software Description	Software Version
Layer 2 Switches (Ethernet), Qty. 3	Cisco	Cisco Catalyst IOS XE	17.3.4
Engineering & Production SAN Archive 1	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Engineering & Production SAN Archive 2	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Engineering & Production SAN Archive 1 Backup	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Engineering & Production SAN Archive 2 Backup	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Test SAN Archive	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Test SAN Archive Backup	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Cybersecurity Capability & Tools SAN Archive Backup	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Company Management SAN Archive	RedHat	RedHat Enterprise Linux (RHEL)	9.2
Company Management SAN Archive Backup	RedHat	RedHat Enterprise Linux (RHEL)	9.2

3.2.4 Secure Workstations and Laptops

The company has implemented a secure workstation configuration, as shown in Figure 3.2.4-1, for use in the engineering, production, and management work areas. The test engineering team utilizes a highly secure laptop configuration (Figure 3.2.4-2), designed to support flexible testing environments both within the Test Lab and in the field.

Laptops are equipped with robust security features, enabling secure data collection and storage across multiple locations, including the production floor and remote field sites. For testing on the production floor or in the field, laptops connect to encrypted, direct-attached bulk storage towers. All test data collected is securely transferred to the Test SANs when the laptops reconnect to the company’s secure information system, ensuring data integrity and confidentiality.

To enhance security, the company has implemented a strict asset control process for all removable storage devices, including hard drives used within the bulk storage towers. This process includes:

- **Asset Tagging and Logging**: All storage devices are tagged, logged, and monitored within an asset management system.

- **Encryption and Access Control**: Drives are encrypted with AES-256 encryption, and access is restricted to authorized personnel only.

- **Audit and Tracking**: The company conducts regular audits of all storage devices to ensure they are accounted for and securely maintained.

The secure configurations for both workstations and laptops are outlined in Tables 3.2.4-1 through 3.2.4-4, detailing the specific hardware and software components used. These measures ensure that all devices adhere to the highest standards of security and data protection across all operational environments.

24" LCD Monitors

Computer Tower with Keyboard and Mouse

- RedHat Enterprise Linux Operating System
- Apache Open Office

- Direct Attached Storage tower
- Six 3.5" 10 TB SATA Hard Disk Drives
- USB C 3.2 (backwards compatible to USB 3.0 or older versions)

Hard Shell Equipment Travel Case

Miscellaneous Equipment

Make	Model No.	Description
Dell	Precision 5820	Computer Tower with Keyboard and Mouse, encrypted with AES-256 for local data protection
Samsung	S24C450DL	24” Widescreen LCD Display with anti-glare and privacy filter

Make	Description	Software Version
RedHat	Red Hat Enterprise Linux (RHEL)	RHEL 9.2
LibreOffice	LibreOffice Suite (Open Source)	7.0.4

Make	Model No.	Description
Dell	7330	Rugged Latitude Extreme Laptop with secure SSD and biometric authentication
Gator	None	ATA TSA Molded Laptop Travel Case (Hard Shell, with built-in cable lock and tamper-evident seals)
Miscellaneous	Miscellaneous	Industrial-grade power strip, encrypted external storage, various network cables and adapters

Make	Description	Software Version
RedHat	Red Hat Enterprise Linux (RHEL)	RHEL 9.2
LibreOffice	LibreOffice Suite (Open Source)	7.0.4

Critical Services:

Function Number	Company Work Area	Criticality (Weight)
F1	Engineering & Production	High (3)
F2	Engineering & Production	High (3)
F3	Engineering & Production	High (3)
F4	Test Engineering	High (3)
F5	IT & Cybersecurity	High (3)
F6	IT & Cybersecurity	High (3)
F7	Engineering & Production	Medium (2)
F8	Test Engineering	Medium (2)
F9	Test Engineering	Medium (2)
F10	Company Management	Medium (2)
F11	Engineering & Production	Low (1)
F12	Test Engineering	Low (1)
F13	Company Management	Low (1)
F14	Company Management	Low (1)
F15	Company Management	Low (1)

Function Number	Endpoint Node Name	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15
System Administrator Terminal		X	X													
Virtualization Manager Server		X	X	X												
Virtualization Manager SAN Archive				X												
Cybersecurity Capability & Tools Server						X	X									
Cybersecurity Capability & Tools SAN Archive						X	X									
Cybersecurity Capability & Tools SAN Archive Backup							X									
Audit Log Server								X								
Audit Log SAN Archive									X							
Server Rack, Server #1 (SR1)		X														
Server Rack, Server #2 (SR2)			X													
Server Rack, Server #3 (SR3)				X												
Server Rack, Server #4 (SR4)					X			X	X							
Server Rack, Server #5 (SR5)							X									
Server Rack, Server #6 (SR6)										X						
Server Rack, Server #7 (SR7)										X						

Server Rack, Server #8 (SR8)
| | | | | | | | | | X | | | |
|
Engineering & Production (Workstation 1)
| | | | | | | | | | | X | | |
|
Engineering & Production SAN 1
| | | | | | | | X | | | | | X | | X
|

Node | SW Make | Software Description | SW Version | CVEs List (NVD Score)

Firewall | Microsoft | Windows NT Account Policy Configuration | NT 4.0 | CVE-1999-0582; (3.0)
Router | Microsoft | LSASS.EXE Access Control Configuration | NT 4.0 | CVE-1999-0227; (2.8)
Virtualization Manager Server | Microsoft | Windows NT 4.0 Security Patch (Denial of Service Mitigation) | NT 4.0 | CVE-1999-1387; (2.7)

