Naval Surface Warfare Center Dahlgren Division
Fiscal Year 2024 University Challenge
Cyber Resiliency and Measurement Challenge
Smaller System Under Evaluation

Rev. 0.1

24 September 2024

Prepared by:

Naval Surface Warfare Center, Dahlgren Division
A Department
Dahlgren, Virginia 22448

Page left blank.

Table of Contents

List of Tables

List of Figures

1.0 Introduction.

This document describes the second System Under Evaluation (SUE) that will be used for the Cyber Resiliency and Measurement Challenge, Phase 3 Demonstration. It is intended to assist in evaluating how well the submissions can be adapted to a new SUE. Challenge teams may develop additional SUE configurations to further demonstrate their solution capability within the timeframe assigned for the Phase 3 Demonstration Brief presentation and solution demonstration.

To further illustrate the intent of the challenge objectives, this document will present a fictional scenario based on a small business company named "Working Software as a Service" (WSAAS) that develops, delivers, maintains software deployments for their customers. WSAAS customers are extremely satisfied with the products, and they have become key components within the critical missions for these customer organizations. This requires WSAAS to maintain certain critical functions for internal operations at all times in order to meet the customer's needs. Figure 1.0-1 illustrates the WSAAS facility layout. It consists of discrete spaces for the work areas: (a) Software Development, (b) Quality Assurance, (c) Information Technology and Cybersecurity, and (d) Company Management. The facility also has a Main Lobby area for visitors and during normal business hours there is a Security Guard to control visitor access to the facility. There may be some problems with the facility layout that could impact the company's cyber resiliency in the event of an outsider threat or insider threat event. Competitor companies and foreign governments very much want access to WSAAS's products design artifacts and test data as well as the unique Intellectual Property (IP) information that the company has created.

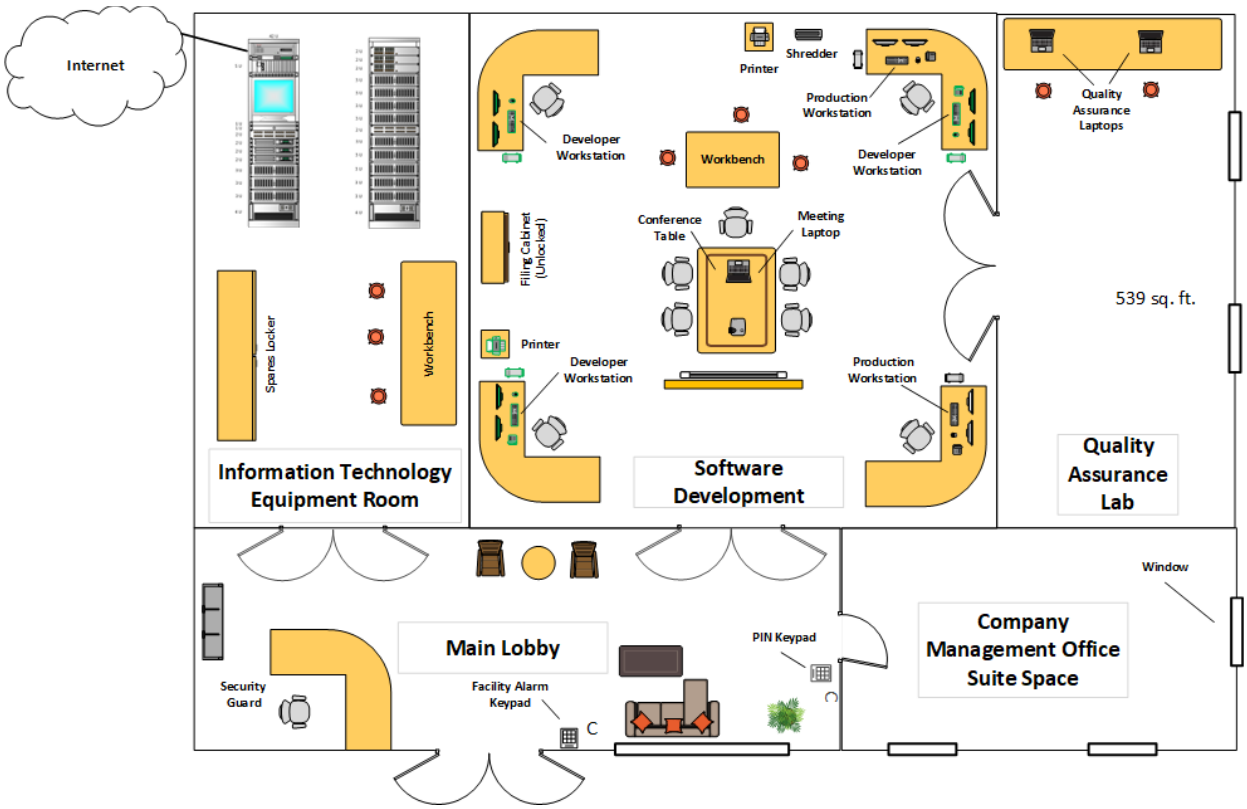


Figure 1.0-1. Company WSAAS Facility Layout

Some additional company facility and information system characteristics to consider are:

a. Company facility is in a shared building in a busy city district with lots of foot traffic.

b. Company facility implements some physical security measures to include a Security Guard desk at the main entrance that is staffed Monday-Friday 8:00 AM to 5:00 PM. The main entrance is locked when the Guard is not on duty but allows employees to exit if they work late (sometimes the door does not close all the way if employees do not make sure it catches). An after-hours alarm system that only monitors the main entrance door is implemented and it is monitored by a commercial service over a telephone line link. All employees know the alarm code in the event they need to work late or have to come into work over the weekend. The last employee leaving the facility in the evening is responsible for activating the alarm.

c. Company has an equipment room that contains all the Information Technology (IT) equipment racks, and the room has a single door with an August Smart Lock Pro. The IT staff have their phones configured to control the lock and the door is usually left unlocked during normal business hours, but it is supposed to be locked whenever there is no IT staff present in the room per the company policy. The IT staff does not always lock the door if they step out and "expect" to be back in 15 minutes or less. The equipment racks in the space do not have locks and neither does the equipment spares cabinet.

d. Company has a room for the Software Development staff, and it has a single entrance door with an August Smart Lock Pro. All the staff have their phones configured to control the lock. The belief is that the Security Guard at the main entrance will control visitors and all the company staff is trusted.

e. Company has a room for Quality Assurance testing, and it has a single door, but it is accessed through the Software Development room. It also does not have a key lock or any other physical access control mechanism.

f. Company Management offices are comprised of a suite of rooms that are accessed from a single door. That door has a key lock to secure the office space after hours. The door is unlocked during normal business hours, but a PIN keypad is used to gain access. The individual offices in the management suite do not have locks on their doors.

g. The company uses proprietary application software for all the Software Development, Quality Assurance, and company management functions. This proprietary application software will not be part of the system under evaluation for this challenge.

h. There is one IT staff member. They have years of IT and cybersecurity experience, formal technical education, and a number of IT and cybersecurity certifications. They were hired into the company within the past 6 months to improve the information system security, but the system architecture is already deployed and there is no funding to make improvements until next year.

i. Information system boundary Firewall Intrusion Prevention System (IPS) rulesets are not up to date.

j. Some of the hardware and software components within the company information system have reached "end-of-life". This means that the component manufacturer no longer supports the hardware or software item, and as a result will not provide security patches to firmware or software for any newly discovered vulnerabilities.

k. Nodes within the company information system have not had the latest security patches installed leaving open vulnerabilities. Some vulnerabilities have been known for some time but cannot be patched since some of the application software providing critical functions will stop working.

l. Nessus vulnerability scanner has not been updated with the latest plugins, where a single plugin performs an automated test to detect the presence of a specific known vulnerability on a commercial hardware or software item. This has resulted in the IT staff performing vulnerability scans on the system in compliance with company policy but are not detecting the new vulnerabilities on the information system.

m. The IT staff has implemented user accounts processes and monitoring procedures and have implemented Role Based Access Control (RBAC) with four defined roles:

- System Administrator (SA) – The SA role has "root" level privileges to all IT equipment, cybersecurity capability and tools, and all data stored on the workstations and laptops, servers, and SANS storage locations to include the Archive and Archive Backup locations. IT staff is assigned the SA role, and the IT staff is responsible for performing all cybersecurity tasks and data management tasks.

- Software Developer (Dev) – The Dev role has "owner" privileges to all software applications and tools used during product and system development, configuration management, integration, production, fielding, and sustainment. This role also has access to all the engineering and production data for all the company projects. All the company software developer staff are assigned the Dev role.
- Quality Assurance (QA) – The QA role has "owner" privileges to all the software applications used to test the company products during development and integration as well as the production units. The QA role also has "owner" privileges to all test plans, test procedures, product under test configuration information, and test data. All company Quality Assurance staff are assigned the TE role.
- Company Management (CMgmt) – The CMgmt role has "owner" privileges to all the company sensitive information to include Human Resources records, Payroll records, Project Management records, Legal records, and personnel managers records to include the company Vice President and President records. All company management staff are assigned the CMgmt role.

2.0 References.

The following list of references is just some of the many available resources that are available to characterize information system vulnerabilities, threats, adversary tactics, techniques, and procedures, and methods for assessing cyber resiliency. It is not intended to be a complete list of references and each participant team should perform additional research when developing their challenge solution.

a. Cyber Resiliency and Measurement Challenge
(available at: https://www.challenge.gov)

b. MITRE Common Vulnerability and Exposure (CVE) Listing
(available at: https://cve.mitre.org/cve/search_cve_list.html)

c. miter Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
(available at: https://attack.mitre.org/)

d. MITRE ATT&CK Groups
(available at: https://attack.mitre.org/groups/)

e. miter ATT&CK Enterprise Tactics
(available at: https://attack.mitre.org/tactics/enterprise/)

f. MITRE Common Attack Pattern Enumeration and Classification (CAPEC)
(available at: https://capec.mitre.org/data/definitions/1000.html)

g. miter Common Weakness Enumeration (CWE)
(available at: https://cwe.mitre.org/index.html)

h. National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD)
(available at: https://nvd.nist.gov/)

i. NIST NVD Common Vulnerability Scoring System (CVSS)
(available at: https://nvd.nist.gov/vuln-metrics/cvss#)

j. NIST NVD CVSS Calculator
(available at: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator#)

k. Cybersecurity Infrastructure & Infrastructure Security Agency, Know Exploited Vulnerabilities Catalog
(available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

l. MTR180314, Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring, MITRE, September 2018
(available at: https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-measures-effectiveness-and-scoring)

m. MP190668, Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes, miter, September 2019

(available at: https://www.mitre.org/news-insights/publication/relationships-between-cyber-resiliency-constructs-and-cyber-survivability)

n. MTR180449, Cyber Resiliency Metrics and Scoring in Practice, Use Case Methodology and Examples, MITRE, September 2018
(available at: https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-and-scoring-practice-use-case-methodology)

o. MTR180450, Cyber Resiliency Metrics Catalog, miter, September 2018
(available at: https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-catalog)

p. MTR200286R2, Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs), Mapping Cyber Resiliency to ATT&CK Framework, Revision 2, MITRE, December 2021
(available at: https://www.mitre.org/news-insights/publication/cyber-resiliency-approaches-controls-mitigate-tactics-rev2)

q. SP 800-160, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, Volume 2, Revision 1, National Institute of Standards and Technology (NIST), December 2021
(available at: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final)

r. RR-2703-AF, Measuring Cybersecurity and Cyber Resiliency, RAND Corporation, 2020
(available at: https://www.rand.org/pubs/research_reports/RR2703.html)

s. Cyber Resilience Review (CRR), Method Description and Self Assessment User Guide, U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), April 2020
(available at: https://www.cisa.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf)

t. Cyber Resilience Review Downloadable Resources, U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), 17 December 2020
(available at: https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-downloadable-resources)

u. Cyber Resilience Review Fact Sheet, U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)
(available at: https://www.cisa.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf)

v. Cybersecurity Architecture, Part 1: Cyber Resilience and Critical Service, Carnegie Mellon University, Software Engineering Institute
(available at: https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-1-cyber-resilience-and-critical-service/)

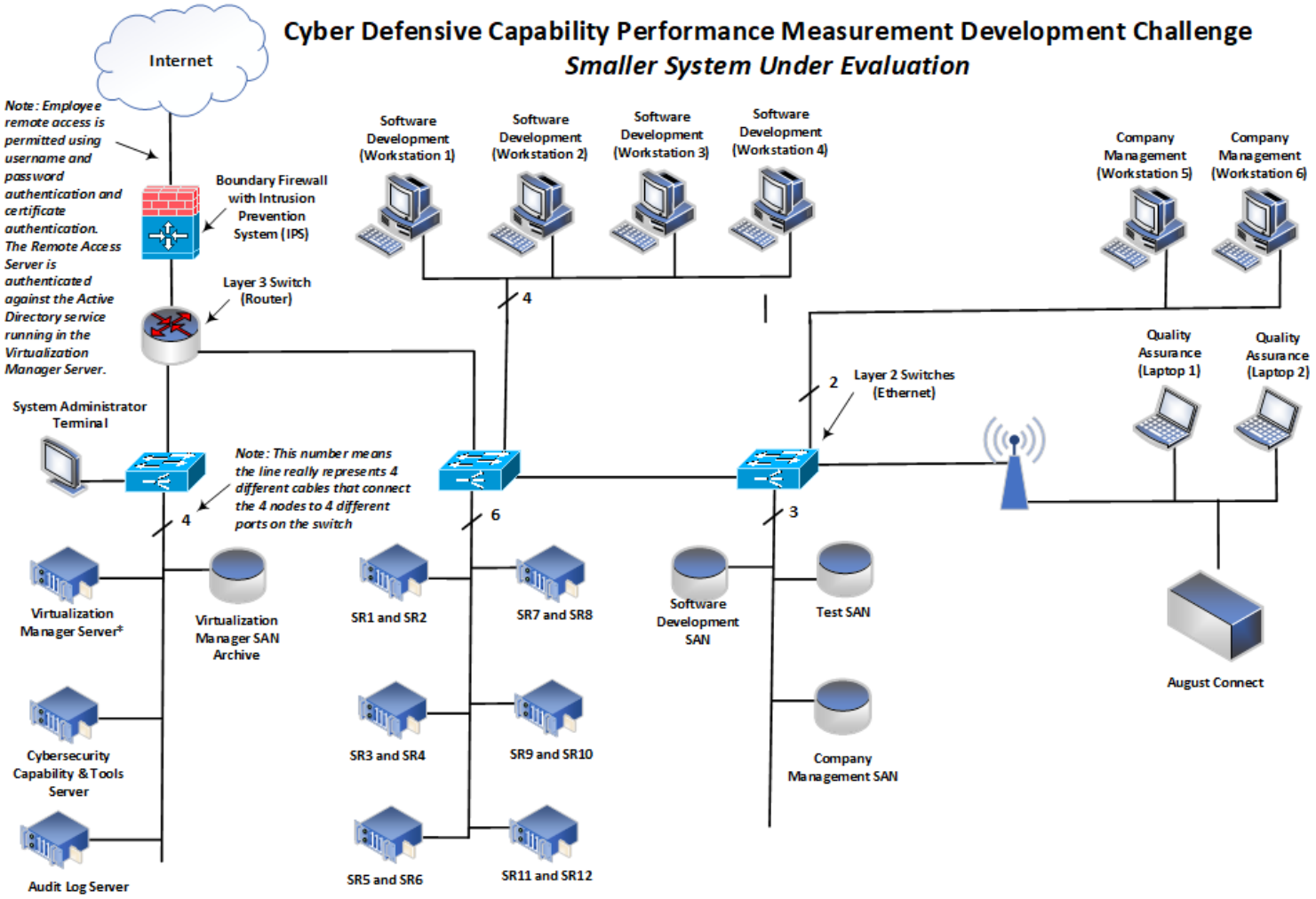
w. Cybersecurity Architecture, Part 2: System Boundary and Boundary Protection, Carnegie Mellon University, Software Engineering Institute
(available at: https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection/)

3.0 System Under Evaluation Description.

The following subsections describe the company information system details. Part of the company cyber resiliency assessment could also include physical security, personnel training and level of experience, operational policies and procedures, and other factors in additional to the information system technical details.

3.1 Company Information System Architecture.

Figure 3.1-1 provides an architecture view for the company's information system that is under evaluation during this challenge. Note that there may be architecture design flaws that could impact the company's cyber resilience.



*Note: The company mail, active directory, webserver, customer database, Gitlab, and Jenkins CI servers are on the Virtualization Manager Server inside the information system perimeter and there is no Demilitarized Zone (DMZ) implemented between the Internet and the Boundary Firewall. This was done to save money and because the Virtualization Manager Server had a spare processing resources.

DISTRIBUTION A: Approved for public release: distribution unlimited.

DISTRIBUTION A. Approved for public release: distribution unlimited.

Figure 3.1-1. Information System Architecture

3.2 Information System Components Description.

The following subsections describe the information system equipment racks and the hardware and software installed in the racks that will be part of the system under evaluation for this challenge. The company has developed a suite of proprietary application software for their software development, quality assurance, and company management work areas. The company asserts that the application software does not have any vulnerabilities, so the application software will not be part of the system under evaluation for this challenge other than evaluating the criticality of the functions the software performs. The challenge will be limited in scope to just the operating systems and specific commercial tools used for cybersecurity.

3.2.1 Boundary Defense and System Administration Rack.

As illustrated in Figure 3.2.1-1, the company facility will have a Boundary Defense and System Administration Rack that will include a Cisco Firepower Firewall with an Intrusion Prevention System (IPS). All external network traffic passing into or out of the facility will be routed through the Firewall and rulesets will be developed to only permit the required data flows. The IPS will be updated periodically with the latest Cisco signatures in order to detect well known cyber attacks, and specific alert types and automated response actions will be configured on the IPS by the facility IT System Administrator for each signature category. The rack will include a Cisco Layer 3 Switch that will interconnect the internal rack components as well as provide the interface to the other equipment racks within the facility. External network traffic that successfully passes through the Firewall will then be routed through the Layer 3 Switch to the end node destination. The rack will include PowerEdge Servers with a dedicated server for the Virtualization Management, Cybersecurity Capability and Tools, and Computer and Network Audit Log Server functions. The Virtualization Management Server will have a bulk data Storage Area Network (SAN) location. A built-in monitor, keyboard, and track ball will be part of the equipment rack and will provide the location where the System Administrator will configure and monitor the IT internal to the facility, perform cybersecurity tasks, and manage the user accounts. It will also be the location where the Virtualization Management will be performed when virtual machines are instantiated on the Server Racks for the production and test activities. A patch panel will provide a central cable management point for all the internal equipment interconnection in the rack. It will also allow for easier reconfiguration of the rack interconnect if it becomes necessary. The rack will include an Uninterruptible Power Supply with a power conditioner that will provide emergency power backup in the event of a primary facility power interruption.

The Virtualization Manager Server will host the team's Gitlab server for version control of the software they develop. It also hosts virtual machines accessible to the public internet to serve the developed software for their customers. WSAAS's website advertising their services and allowing customers to log into accounts to manage payment information is also hosted on the Virtualization Manager Server as website hosted via Microsoft Internet Information Services (IIS) on a Windows Server 2008 virtual machine. The customer account login is verified against a plaintext Microsoft SQL Server database hosted on the same virtual machine. Customer financial information is stored in the same database. That same Windows Server 2008 machine is also the domain controller for WSAAS's internal Active Directory identity management.

The Cybersecurity Tools will consist of a Splunk Security Information and Event Manager (SIEM), McAfee Anti-Virus scanner, and Nessus vulnerability scanner to monitor the facility operations and ensure the information systems are secure. The facility IT System Administrator will routinely monitor the SIEM for cybersecurity alerts and will initiate internal cybersecurity tests, such as Anti-Virus scans and Nessus vulnerability scans, of all installed IT in compliance with the company cybersecurity policy and procedures. The facility System Administrator will also perform user account management from the Boundary Defense and System Management rack through the IdM service. The System Administrator will validate all user accounts are still valid and that each user has the appropriate roles assigned at least monthly per the company cybersecurity policy and procedures.

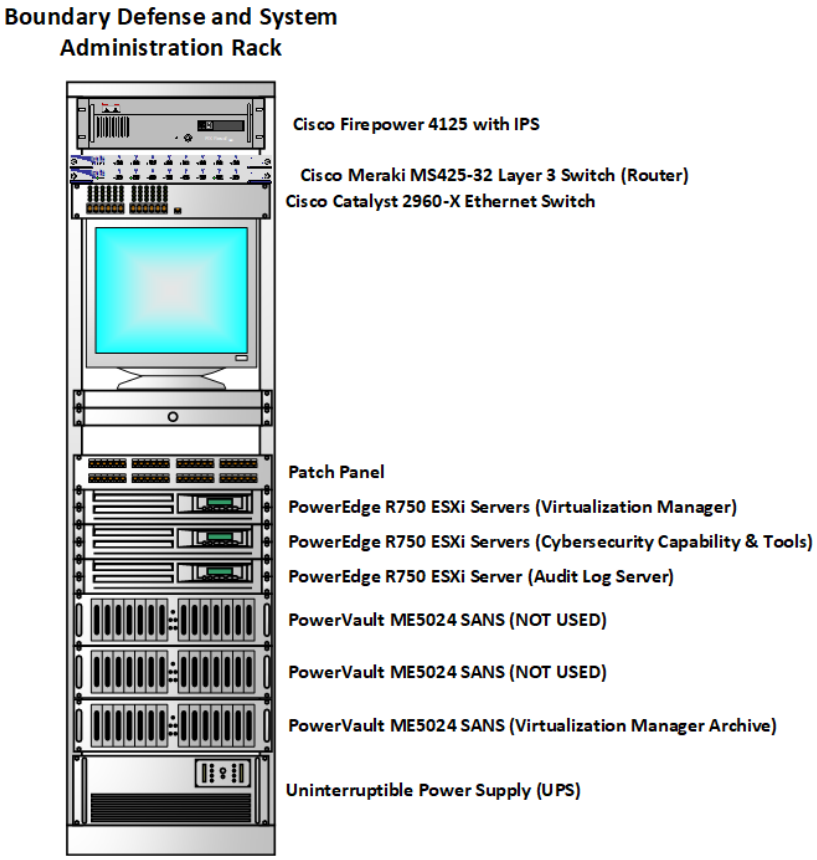


Figure 3.2.1-1. Boundary Defense and System Administration Rack Layout

The Boundary Defense and System Administrator Rack hardware and software list is provided in Tables 3.2.1-1 and 3.2.1-2, respectively.

Table 3.2.1-1. Boundary Defense and System Administrator Rack Hardware

Make	Model No.	Description
Cisco	4125 NGFW	Next Generation Firewall (NGFW) with Intrusion Protection Systems (IPS), rack mountable, 1U
Cisco	MS425-32	Meraki Layer 3 Switch (Router)
Cisco	Catalyst 2960-X	Layer 2 Gigabit Ethernet Network Switch
Tripp Lite	B030-008-17-IP	Rack Mounted Monitor, Keyboard, and Touchpad
Dell	PowerEdge R750	Rack Server (2U, Intel C620 series chipset, up to two 3rd Generation Intel Xeon processors with up to 40 cores per processor)
Dell	PowerVault ME5024	Storage Area Network (SAN)
Tripp Lite	N052-048-1U	48-Port Patch Panel (1U Rack-Mount, 558B, Cat6/Cat5, RJ45)
APC	SMT3000RM2UC	Uninterruptible Power Supply (3kVA, 2U rackmount, Smart-UPS)

Make	Model No.	Description
Miscellaneous	Miscellaneous	Miscellaneous Components (e.g., rack cables, equipment rails, cable retractors, power strip, screws, etc.)

Table 3.2.1-2. Boundary Defense and System Administrator Rack Software

Node	SW Make	Software (SW) Description	Software Version
Firewall	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software	6.6.7
Layer 3 Switch (Router)	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23) – search for "Meraki")	2014-09-23
Layer 2 Switch (Ethernet)	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E
Virtualization Manager Server	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0
	Gitlab	Gitlab Enterprise Edition	v13.7.0
	Microsoft	Microsoft SQL Server	SQL Server 2008 SP2
	Microsoft	IIS	IIS 7.5
	OpenVPN	VPN Server	v2.3
	Jenkins	CI/CD pipeline	v2.32.3 LTS
Cybersecurity Capability & Tools Server	RedHat	RedHat Enterprise Linux	RHEL 7.1
	McAfee	VirusScan Enterprise	2.0
	Tenable	Nessus Vulnerability Scanner	8.10.0
	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6
Audit Log Server	RedHat	RedHat Enterprise Linux	RHEL 7.1
Virtualization Manager SANS	RedHat	RedHat Enterprise Linux	RHEL 6.0
Cybersecurity Capability & Tools SANS	RedHat	RedHat Enterprise Linux	RHEL 7.1
Audit Log SANS	RedHat	RedHat Enterprise Linux	RHEL 7.1

3.2.2 Server Rack.

The Server Rack is illustrated in Figure 3.2.2-1, and it provides the common computing resources for the entire company to include the software development, quality assurance, and company management work areas. The IT and cybersecurity work area separated and is implemented on a dedicated Boundary Defense and System Administration Rack (section 3.2.1). The Server Rack contains multiple PowerEdge R750 Servers and PowerVault Storage Area Network (SANS) servers and they will be used within the facility to:

a. Provide the product design, development, and test tools.
b. Process and display technical data library artifacts that describe the systems and products under development and test within the organization to include sensitive Intellectual Property (IP) information.
c. Product Help Desk Response Ticketing System application software and record database software. The software development work area will provide a Help Desk to respond to customer questions and comments. The Help Desk operators will access the Ticketing System from their workstations.
d. Virtualized product under development Test and Analysis Environment for software products.
e. Company training environment that will be used to develop workforce knowledge and skills.
f. Provide computer resources for company management functions (e.g., Human Resources, Payroll, Legal, Contracts, project managers, personnel managers, company vice president, and company president).

The rack also includes Cisco Catalyst Ethernet Switches that will interconnect the servers and SANS storage servers and a Cisco Meraki Layer 3 network switch will connect the server rack to any other server racks if they are installed in the future (not currently used). A patch panel is provided to allow for easier reconfiguration of the rack interconnect if it becomes necessary. An Uninterruptible Power Supply (UPS) will be included within the Server Rack that will provide temporary emergency power when the primary facility power circuit is interrupted allowing for a graceful shutdown or until any backup emergency power source is engaged. Tables 3.2.2-1 and 3.2.2-2 provide the hardware and software list, respectively, for the Server Rack.

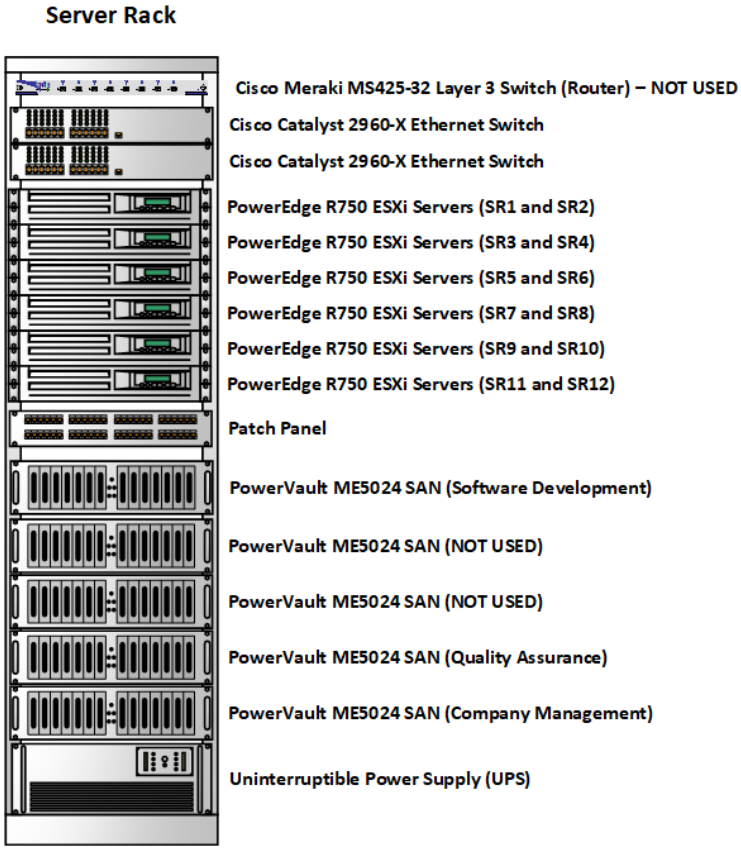


Figure 3.2.2-1. Server Rack Layout

Table 3.2.2-1. Server Rack Hardware

Make	Model No.	Description
Cisco	Catalyst 2960-X	Layer 2 Gigabit Ethernet Network Switch
Dell	PowerEdge R750	Rack Server (2U, Intel C620 series chipset, up to two 3rd Generation Intel Xeon processors with up to 40 cores per processor)
Tripp Lite	N052-048-1U	48-Port Patch Panel (1U Rack-Mount, 558B, Cat6/Cat5, RJ45)
Cisco	MS425-32	Cisco Meraki Layer 3 Switch (32 ports, 10 Gb)
Dell	PowerVault ME5024	Storage Area Network (SAN)
APC	SMT3000RM2UC	Uninterruptible Power Supply (3kVA, 2U rackmount, Smart-UPS)
Miscellaneous	Miscellaneous	Miscellaneous Components (e.g., rack cables, equipment rails, cable retractors, power strip, screws, etc.)

Table 3.2.2-2. Server Rack Software

Node	SW Make	Software (SW) Description	Software Version
Layer 2 Switches (Ethernet), Qty. 2	Cisco	Catalyst 2960-X IOS	IOS 15.2(1)E
Servers SR1 and SR2	RedHat	RedHat Enterprise Linux	RHEL 5.0
Servers SR3 and SR4	RedHat	RedHat Enterprise Linux	RHEL 7.1
Servers SR5 and SR6	RedHat	RedHat Enterprise Linux	RHEL 6.0
Servers SR7 and SR8	RedHat	RedHat Enterprise Linux	RHEL 7.1
Severs SR9 and SR10	RedHat	RedHat Enterprise Linux	RHEL 7.1
Severs SR11 and SR12	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2
Software Development SAN	RedHat	RedHat Enterprise Linux	RHEL 5.0
Quality Assurance SAN	RedHat	RedHat Enterprise Linux	RHEL 7.1
Company Management SAN	RedHat	RedHat Enterprise Linux	RHEL 5.0

3.2.3 Smart Locks

Table 3.2.3-1. Smart Lock Software

Node	SW Make	Software (SW) Description	Software Version
August Connect App	August	August Connect Wi-Fi Bridge phone application	v10.11.0
August Connect Device	August	August Connect device firmware	v2.2.12

3.2.4 Wireless Network

The company also has a wireless network that is being broadcast. The Quality Assurance laptops connect to this network for all their network access. The network utilizes WPA2 encryption to protect communications, but all the staff know the password and a piece of paper with the network information is taped to the wall in the Software Development work area.

Table 3.2.4-1. Wireless Access Point Software

Node	SW Make	Software (SW) Description	Software Version
WAC510 Wireless Access Point	Netgear	Netgear WAC510 Wireless Access Point Firmware	v5.0.0.16

3.2.5 Workstations and Laptops.

The company implements the common workstation configuration depicted in Figure 3.2.4-1 for the software development and company management work areas. The quality assurance work area uses the laptop configuration depicted in Figure 3.2.4-2. Laptops are used to allow for testing of the product from the Quality Assurance Lab table as well as in the field. The laptops will use a direct attached bulk storage tower when testing on the production floor or in the field. The collected test data will then be transferred onto the Quality Assurance SAN once the laptops are reconnected to the company information system. The company does not have any kind of asset control process for the hard drives used within the direct attached bulk storage tower. Tables 3.2.4-1 and 3.2.4-2 provide the company workstation hardware and software configuration, respectively. Tables 3.2.4-3 and 3.2.4-4 provide the test laptop hardware and software configuration, respectively.

Figure 3.2.5-1. Company Common Workstation Configuration

Figure 3.2.5-2. Company Quality Assurance Laptop Configuration

Table 3.2.5-1. Workstation Hardware

Make	Model No.	Description
Dell	Precision 5820	Computer Tower with Keyboard and Mouse
Samsung	S24C450DL	24” Widescreen LCD Display

Table 3.2.5-2. Workstation Software

Make	Description	Software Version
RedHat	Red Hat Enterprise Linux (RHEL)	RHEL 6.0
OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4

Table 3.2.5-3. Quality Assurance Laptop Hardware

Make	Model No.	Description
Dell	7330	Rugged Latitude Extreme Laptop
Gator	None	ATA TSA Molded Laptop Travel Case (Hard Shell, Exterior Dimensions: 19.38” W x 14.5” D x 9.75” H)

Make	Model No.	Description
Miscellaneous	Miscellaneous	Miscellaneous Equipment (e.g., industrial grade power strip and power cord, various computer network cable types, cable adapters, etc.)

Table 3.2.5-4. Quality Assurance Laptop Software

Make	Description	Software Version
RedHat	Red Hat Enterprise Linux (RHEL)	RHEL 5.0
OpenOffice	Apache OpenOffice (Open Source)	4.1.1.4

3.3 System Critical Functions and Mapping.

The company information system provides fifteen functions that the software development, quality assurance, IT and cybersecurity, and company management work areas use. The criticality levels that are used within this example are listed below but challenge participants may derive their own criticality scale and weighting values.

- **High Criticality** – The company must maintain all High criticality functions at all times to meeting vital product development, test, and delivery to customers and to maintain timely customer support for fielded products. There are also contractual and safety reasons for having to maintain all High criticality functions. No interruption in critical functions is acceptable during cyber attacks on the company information system from external threats or internal threats or during natural disasters. IT and cybersecurity services within the company information system are considered High criticality.
- **Medium Criticality** – The company can accept partial or complete interruption of Medium criticality functions for no longer than 1 month before it will begin impacting operations. Product development, test, production, and fielding can still be completed but the process is slowed down and is more expensive when medium criticality functions are degraded or denied for an extended period of time. Work arounds are defined to continue company operations when Medium criticality functions are disrupted.
- **Low Criticality** – The company can accept long term degradation or denial of Low criticality functions. It is considered a nuisance if Low criticality functions are not available, but it will not impact product development, test, production, and fielding in any way and will have minimum impact on company management.

Table 3.3-1 lists the company critical functions that is provided by the company's proprietary application software that is installed on the workstations, laptops, and servers. A given function may execute on a single endpoint node within the information system, or it may be distributed across multiple nodes as illustrated in Table 3.3-2. The computer network infrastructure components that interconnect all the nodes will also be critical for the distributed functions to the highest criticality value of the functions that rely on the network components. Table 3.3-2 maps the software functions to the information system endpoint nodes that are required to execute those functions. An "X" in the matrix indicates that all or a portion of the function is executed on an endpoint. Once simple method for assessing the criticality of an endpoint node (hardware and software) using the matrix mapping is to apply the "highwater mark" technique. For a given node in Table 3-3-2, scan the row to find the "X" that is in the highest criticality column, and that would be considered the highwater mark. For example, the Server Rack, Server #4 executes functions F4, F8, and F9, and since F4 has a criticality value of "High" in Table 3.3-1, then the Server #4 criticality is also considered "High". Likewise, the Software Development (Workstation 4) executes functions F7 and F11, and since function F7 is assessed as Medium criticality in Table 3.3-1 while function F11 is assessed as Low criticality, the criticality of Workstation 4 is Medium. There are ae other techniques that can be used, so participants are encouraged to use their preferred methods.

Table 3.3-1. Company Critical Functions Definition

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

Table 3.3-2. Company Critical Functions Mapping Across Information System Endpoints

	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	X							
Cybersecurity Capability & Tools Server					X	X									
Audit Log Server					X	X									
Server Rack, Server #1 (SR1)	X		X												
Server Rack, Server #2 (SR2)	X	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			X		
Server Rack, Server #7 (SR7)												X		X	
Server Rack, Server #8 (SR8)															X
Server Rack, Server #9 (SR9)				X					X			X			
Server Rack, Server #10 (SR10)							X								
Server Rack, Server #11 (SR11)		X													
Server Rack, Server #12 (SR12)										X					
Software Development SAN 1	X	X	X												
Quality Assurance SAN				X				X	X						
Company Management SAN										X			X	X	X
Software Development (Workstation 1)	X	X													

	Function Number														
Endpoint Node Name	**F1**	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**	**F10**	**F11**	**F12**	**F13**	**F14**	**F15**
Software Development (Workstation 2)			X												
Software Development (Workstation 3)		X					X								
Software Development (Workstation 4)							X				X				
Quality Assurance (Laptop 1)				X											
Quality Assurance (Laptop 2)								X	X						
Company Management (Workstation 5)										X			X	X	X
Company Management (Workstation 6)													X		

3.4 Information System Cyber Vulnerabilities Lists.

Tables 3.4-1 through 3.4-5 list the vulnerabilities that are present on the company information system under evaluation. For the purpose of this challenge, assume that all computer Ports, Protocols, and Services (PPS) needed to exploit each listed vulnerability are enabled on the endpoint and network devices. Also assume that the company proprietary software applications that provide the functions described mapped in section 3.3 do not have any known vulnerabilities. The Common Vulnerability and Exposure (CVE) numbers provided in the table are reference numbers for a given vulnerability used on the MITRE CVE website. The National Institute of Standards and Technology (NIST) has a National Vulnerability Database (NVD) that includes the CVEs, and they assign a Common Vulnerability Scoring System (CVSS) score to each vulnerability to recommend a severity rating if the vulnerability were successfully exploited. The NVD also provides a CVSS Calculator to allow cybersecurity engineers to adjust the default NVD CVSS score for a given vulnerability if it is deemed appropriate. Some of the NVD CVSS scores use the Version 2 calculator while others use the Version 3.x calculator, so when both CVSS scores are provide for a given vulnerability the Version 3.x calculator value should be used for this exercise. Below are the links to the MITRE and NIST websites. The challenge participants may add additional vulnerabilities for any additional system configurations they would like to demonstrate, but the vulnerabilities listed in the tables should be demonstrated for the initial demonstration run. This initial demonstration run may also include removing one or more vulnerabilities from the assessment as would be done if the IT staff apply security software patches to the information system in order to remediate vulnerabilities, and then a new cyber resiliency assessment score will be calculated.

- MITRE CVE Search: https://cve.mitre.org/cve/search_cve_list.html
- NIST NVD Search: https://nvd.nist.gov/vuln/search
- NIST NVD CVSS Version 3.1 Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- NIST NVD CVSS Version 2 Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

Table 3.4-1. Boundary Defense and System Administrator Rack Vulnerabilities

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Firewall	Cisco	FirePower 4125 Next Generation Firewall with Firepower Threat Defense (FTD) Software	6.6.7	CVE-2023-20269; (NVD Score: 9.1) CVE-2023-20256; (NVD Score: 5.8) CVE-2023-20247; (NVD Score: 4.3) CVE-2023-20200; (NVD Score: 6.3) CVE-2023-20095; (NVD Score: 8.6) CVE-2023-20015; (NVD Score: 6.7) CVE-2023-20934; (NVD Score: 7.8)

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Router	Cisco	Meraki MS425-32 Layer 3 Switch (firmware 2014-09-23)	2014-09-23	CVE-2018-0284; (NVD Score: 6.5) CVE-2014-7999; (NVD Score: 7.7) CVE-2014-7993; (NVD Score: 3.3) CVE-2014-7994; (NVD Score: 5.4) CVE-2014-7995; (NVD Score: 7.2)
Ethernet Switch	Cisco	Catalyst 2960-X	IOS 15.2(1)E	CVE-2016-6473; (NVD Score 6.5) CVE-2017-6606; (NVD Score 6.4) CVE-2017-3803; (NVD Score 4.7) CVE-2016-1425; (NVD Score 6.5)
Virtualization Manager Server	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0	CVE-2012-2697; (NVD Score: 4.9) CVE-2012-3440; (NVD Score: 5.6) CVE-2010-0727; (NVD Score: 4.9)
	Gitlab	Gitlab Enterprise Edition	v13.7.0	CVE-2024-1495; (NVD Score: 6.5) CVE-2024-2743; (NVD Score: 9.1) CVE-2024-2576; (NVD Score: 4.3)
	Microsoft	Microsoft SQL Server	SQL Server 2008 SP2	CVE-2012-0158; (NVD Score: 8.8) CVE-2012-1856; (NVD Score: 8.8) CVE-2015-1762; (NVD Score: 7.1) CVE-2015-1763; (NVD Score: 8.5)
	Microsoft	IIS	IIS 7.5	CVE-2010-1256; (NVD Score: 8.5) CVE-2010-3972; (NVD Score: 10.0)
	OpenVPN	VPN Server	v2.3	CVE-2022-0547; (NVD Score: 9.8) CVE-2020-15078; (NVD Score: 7.5) CVE-2020-20813; (NVD Score: 7.5) CVE-2017-12166; (NVD Score: 9.8)
	Jenkins	CI/CD pipeline	v2.32.3 LTS	CVE-2017-1000353; (NVD Score: 9.8) CVE-2017-1000354; (NVD Score: 8.8) CVE-2017-1000356; (NVD Score: 8.8)

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Cybersecurity Capability & Tools Server	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
	McAfee	VirusScan Enterprise	2.0	CVE-2020-7337; (NVD Score: 6.7) CVE-2009-5118; (NVD Score: 9.3) CVE-2007-2152; (NVD Score: 7.9)
	Tenable	Nessus Vulnerability Scanner	8.10.0	CVE-2023-0101; (NVD Score: 8.8) CVE-2021-20135; (NVD Score: 6.7) CVE-2020-5765; (NVD Score: 5.4)
	Splunk	Enterprise Security Information and Event Manager (SIEM)	8.6	CVE-2024-23675; (NVD Score: 6.5) CVE-2024-23676; (NVD Score: 3.5) CVE-2023-40593; (NVD Score: 7.5) CVE-2023-40592; (NVD Score: 6.1)
Audit Log Server	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
Virtualization Manager SAN	RedHat	RedHat Enterprise Linux	RHEL 6.0	CVE-2013-1935; (NVD Score: 5.7) CVE-2013-2224; (NVD Score: 6.9) CVE-2013-2188; (NVD Score: 4.7)

Table 3.4-2. Server Rack Vulnerabilities

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Layer 2 Switches (Ethernet)	Cisco	Catalyst 2960-X	IOS 15.2(1)E	CVE-2016-6473; (NVD Score 6.5) CVE-2017-6606; (NVD Score 6.4) CVE-2017-3803; (NVD Score 4.7) CVE-2016-1425; (NVD Score 6.5)
Servers SR1 and SR2	RedHat	RedHat Enterprise Linux (RHEL)	RHEL 5.0	CVE-2012-2697; (NVD Score: 4.9) CVE-2012-3440; (NVD Score: 5.6)

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
				CVE-2010-0727; (NVD Score: 4.9)
Servers SR3 and SR4	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
Servers SR5 and SR6	RedHat	RedHat Enterprise Linux	RHEL 6.0	CVE-2013-1935; (NVD Score: 5.7) CVE-2013-2224; (NVD Score: 6.9) CVE-2013-2188; (NVD Score: 4.7)
Servers SR7 and SR8	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
Severs SR9 and SR10	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
Severs SR11 and SR12	Microsoft	Windows Server 2008 Service Pack 2	Windows Server 2008 SP2	CVE-2017-8543; (NVD Score: 9.8) CVE-2014-0301; (NVD Score: 9.3) CVE-2014-0323; (NVD Score: 6.6) CVE-2014-0315; (NVD Score: 6.9) CVE-2013-5058; (NVD Score: 6.9) CVE-2013-5056; (NVD Score: 9.3)
Software Development SAN	RedHat	RedHat Enterprise Linux	RHEL 5.0	CVE-2012-2697; (NVD Score: 4.9) CVE-2012-3440; (NVD Score: 5.6) CVE-2010-0727; (NVD Score: 4.9)
Quality Assurance SAN	RedHat	RedHat Enterprise Linux	RHEL 7.1	CVE-2015-7833; (NVD Score: 4.9)
Company Management SAN	RedHat	RedHat Enterprise Linux	RHEL 5.0	CVE-2012-2697; (NVD Score: 4.9) CVE-2012-3440; (NVD Score: 5.6) CVE-2010-0727; (NVD Score: 4.9)

Table 3.4-3. Company Workstations Vulnerabilities

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Software Development (Workstations 1 thru 4)	RedHat	RedHat Enterprise Linux	RHEL 6.0	CVE-2013-1935; (NVD Score: 5.7) CVE-2013-2224; (NVD Score: 6.9) CVE-2013-2188; (NVD Score: 4.7)
	OpenOffice	Apache OpenOffice	4.1.1.4	CVE-2023-47804; (NVD Score: 8.8) CVE-2022-37401; (NVD Score: 8.8) CVE-2021-33035; (NVD Score: 7.8) CVE-2020-13958; (NVD Score: 7.8) CVE-2017-12607; (NVD Score: 7.8)
Company Management (Workstations 5 and 6)	RedHat	RedHat Enterprise Linux	RHEL 6.0	CVE-2013-1935; (NVD Score: 5.7) CVE-2013-2224; (NVD Score: 6.9) CVE-2013-2188; (NVD Score: 4.7)
	OpenOffice	Apache OpenOffice	4.1.1.4	CVE-2023-47804; (NVD Score: 8.8) CVE-2022-37401; (NVD Score: 8.8) CVE-2021-33035; (NVD Score: 7.8) CVE-2020-13958; (NVD Score: 7.8) CVE-2017-12607; (NVD Score: 7.8)

Table 3.4-4. Company Laptops Vulnerabilities

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
Quality Assurance (Laptops 1 and 2)	RedHat	RedHat Enterprise Linux	RHEL 5.0	CVE-2012-2697; (NVD Score: 4.9) CVE-2012-3440; (NVD Score: 5.6) CVE-2010-0727; (NVD Score: 4.9)
	OpenOffice	Apache OpenOffice	4.1.1.4	CVE-2023-47804; (NVD Score: 8.8) CVE-2022-37401; (NVD Score: 8.8)

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
				CVE-2021-33035; (NVD Score: 7.8) CVE-2020-13958; (NVD Score: 7.8) CVE-2017-12607; (NVD Score: 7.8)

Table 3.4-5. Company Smart Locks

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
August Smart Lock Pro	August	August Connect Wi-Fi Bridge phone application	v10.11.0	CVE-2019-17098; (NVD Score: 3.1)
	August	August Connect device firmware	v2.2.12	CVE-2019-17098; (NVD Score: 3.1) CVE-2019-17518; (NVD Score: 6.5)

Table 3.4-6. Wireless Access Point

Node	SW Make	Software (SW) Description	Software Version	CVEs List; (NVD Score)
WAC510 Wireless Access Point	Netgear	Netgear WAC510 Wireless Access Point Firmware	v5.0.0.16	CVE-2018-21133; (NVD Score: 9.8) CVE-2018-21132; (NVD Score: 9.8) CVE-2018-21131; (NVD Score: 9.1) CVE-2018-21130; (NVD Score: 8.8) CVE-2018-21129; (NVD Score: 6.5) CVE-2018-21128; (NVD Score: 8.8) CVE-2018-21127; (NVD Score: 8.8) CVE-2018-21126; (NVD Score: 8.8) CVE-2018-21125; (NVD Score: 8.8) CVE-2018-21124; (NVD Score: 8.8)

3.5 Example Advanced Persistent Threats (APTs)

Participants can choose to include any desired information on APTs that is publicly available. MITRE hosts a list of APTs at Groups | MITRE ATT&CK® and details known tactics, techniques, and procedures (TTPs). An example list of possibly applicable APTs is provided below, but the list of possibly applicable APTs is not exhaustive. The APTs selected do not represent specific areas of concern, and no specific interest in the SUE is expected. However, information from these APTs should be included as examples of commonly known TTPs. As such, the initial demonstration run should include at a minimum TTPs from these groups. The initial demonstration run may also include adding or removing an APT and their TTPs.

- APT1 - APT1, Comment Crew, Comment Group, Comment Panda, Group G0006 | MITRE ATT&CK®
- Sandworm Team - Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Group G0034 | MITRE ATT&CK®
- APT28 - APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Group G0007 | MITRE ATT&CK®
- Windigo- Windigo, Group G0124 | MITRE ATT&CK®

MITRE makes the Cyber Threat Intelligence (CTI) from the ATT&CK knowledge base available in JSON and Excel formats. The links above include TTP information for each of the referenced APTs. Further information and resources, including a python library, on how to pull CTI from MITRE's ATT&CK Framework can be found at ATT&CK Data & Tools | MITRE ATT&CK®.