SECURITY DOCUMENTATION

Team ID: ____

Documentation file name must include your team ID.

Do not reference your College/University.

SYSTEM OVERVIEW

Briefly describe the overall system and its purpose (in 250 words or less).

One cannot secure a system when its purpose and scope are unknown.
[Note: The audience for this section is "senior leadership", so please write accordingly.]

LunarQuest Family Fun Zone is an amusement park that is part of a trio of amusement parks serving the local area. The park was a recent victim of a cybersecurity and physical security-related attacks in which customer credit card information was stolen from several POS terminals in the park. The security team at the park is working to remediate these attacks and secure the property to prevent future incidents.

The physical system at the park consists of several elements – the fenceline, an NVR system and cameras located in strategic areas of the park, a team of security guards, a set of walkie-talkies, the POS terminals in the food court and gift shop, a webserver, ticket scanner, and access to the AP-ISAC systems. The fence line prevents park-goers from accessing the park without a ticket. The ticket scanner verifies the ticket the park-goer has purchased. The NVR system and cameras record activity in the park. The team of security guards is to make sure park-goers are enjoying the park in a safe and responsible manner. The walkie-talkie's allow the security guards to contact one another. The PoS terminals in the food court and gift shop facilitate sales. The webserver coordinates ticket, food, and merchandise sales. The AP-ISAC services allows LunarQuest Family Fun Zone to keep up to date with potential threats to the security of the park.

Observations

- Jargon is used (AP-ISAC)
- The system's purpose is clear and targets senior leadership.
- The system is defined, but there are discrepancies between this summary and the asset inventory.
- POS is inconsistently capitalized.
- Does not explain acronyms (POS, AP-ISAC, etc.)
- Minor spelling and grammatical errors (fence line is two words, walkie-talkies should not have an apostrophe).

ASSET INVENTORY

List all of the system's devices, by name, and their key attributes in the following table.

Asset management is a critical component of operational technology security. One cannot secure a network when one does not know what devices and services are running on the network.

Host	OS	IP Address	Port	Service
ACME Walkie-Talkie	Proprietary	404 MHz	n/a	radio
POS Mobile terminal	Proprietary	1.2.3.4	4321	DigitalCash
PoS Gift Shop Terminal	ACME Proprietary		4321	DigitalCash
POS Food Court Terminal	ACME Proprietary		57005 48879	Deadbeef Protocol
Ticket Scanner				
Cameras & NVR…	Debian			
Security golf cart	N/A			transportation
Fence Line	N/A	N/A	N/A	Physical security
Drones	Proprietary			

Observations

- Asset discrepancy between this inventory, the network diagram, and the vulnerability list. (e.g., restrooms and the supply cabinet are shown in the network diagram, but they are not listed here; the radio supply cabinet is only listed on the vulnerability list).
- Inconsistent capitalization of POS, which indicates a lack of document copy editing.
- The table is not completely filled out (e.g., no details are provided for the Ticket Scanner).
- Ellipses after cameras and NVR

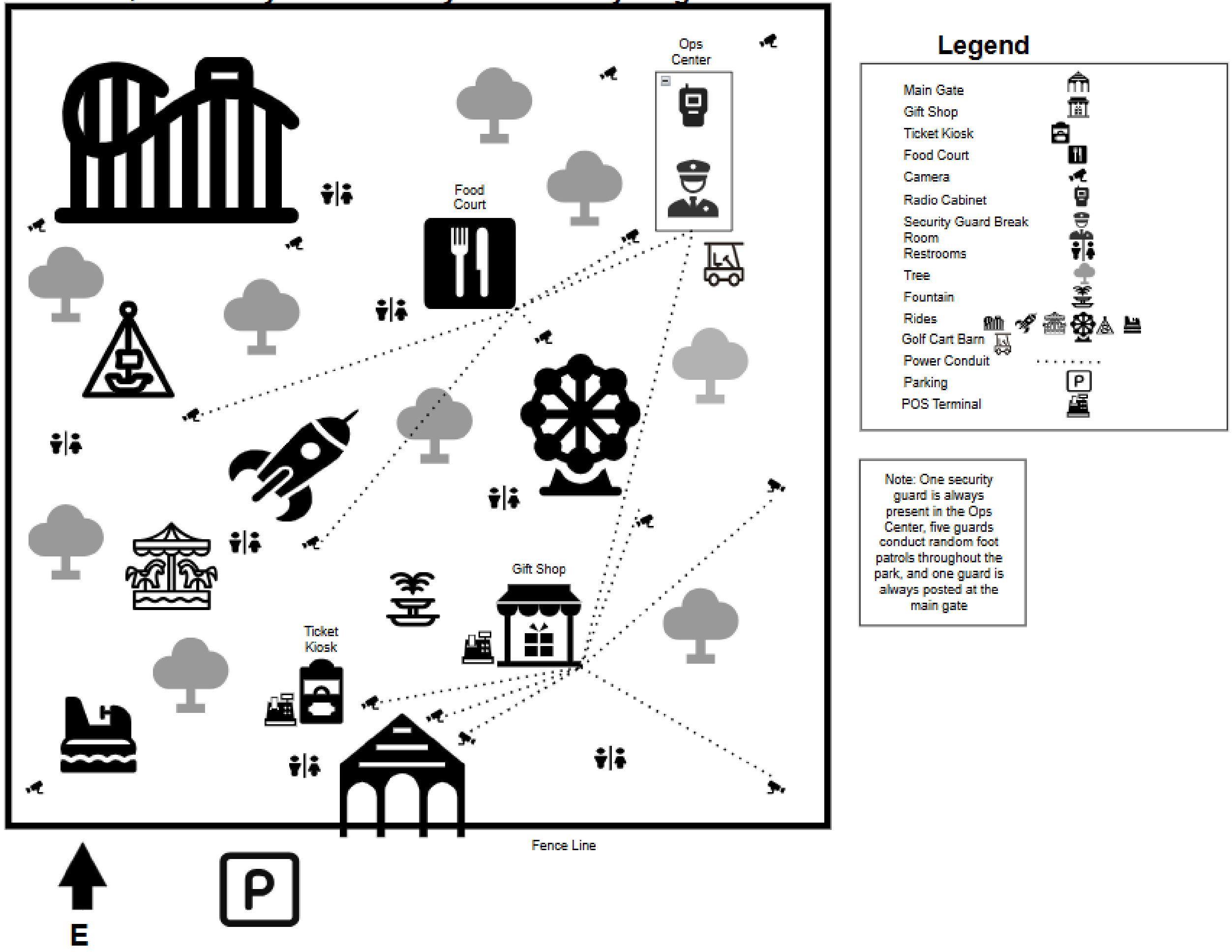
NETWORK DIAGRAM

Provide a network diagram for your system. All hosts, network appliances, and services should be identified.

Current and detailed network diagrams facilitate enhanced situational awareness, especially for new staff that may be responding to a cyber security incident.

[Note: Focus on the information content—a thorough, hand-drawn diagram will score higher than an incomplete “visio” diagram.]

LunarQuest Family Fun Zone Physical Security Diagram



Note: One security guard is always present in the Ops Center, five guards conduct random foot patrols throughout the park, and one guard is always posted at the main gate

Observations

- Includes a POS terminal at the ticket kiosk and gift shop but not at the food court.
- Does not reference the mobile POS terminals included in the asset inventory.
- Inconsistent layout (e.g., some cameras have their physical connections shows, others do not).
- Includes a legend that explains the various symbols used in the diagram.
- The diagram is missing walkways.
- The geographic layout of the diagram makes logical sense. Orienting East as up does not make sense.

PLEASE LIST ALL VULNERABILITIES YOU FOUND AND THE MITIGATIONS YOU TOOK FOR EACH

The CyberForce Competition environment was “seeded” with many vulnerabilities. List each vulnerability that you were able to identify. For each vulnerability, also list the mitigation(s) that you were able to enact (e.g., system hardening, software patch, compensating control, operational procedure).

[Note: Add a row to the table for each unique vulnerability per host. For example, if Alice, Bob, and Carol all have weak passwords on host Foo, this merits one line in the table. If Alice, a network admin, has weak passwords on three hosts, then three lines should be added to this table.]

[Note2: Security documents often include a section of known issues—both those that have been resolved as well as open issues that may or may not yet have mitigating controls.]

[Note3: The audience for this section includes “senior leadership”. Please summarize your results as appropriate. Including “raw” vulnerability report(s) in this section does not meet the senior leadership audience requirement.]

Host/System	Vulnerability	Mitigation(s)
ACME Walkie-Talkie	Theft	Handcuff to security personnel and clerks
ACME Walkie-Talkie	No identity verification	Introduce identity verification policy or a policy where certain information or requests can not be done over Walkie-Talkie
Cameras & NVR	Blindspot in area near fence hole	Add additional security patrols in that area
Cameras & NVR	Blindspot in area to the left of Rocket Ride	Add additional security patrols in that area
Cameras & NVR	No tamper indicators	Attach security seal
Cameras & NVR	Unaccounted for video blackout in some of the camera footage	Send alerts when video is deleted or if NVR is not receiving the expected video stream
Fence Line	Hole in Fence	Fix fence
Fence Line	Weak fence	Reinforce fence
POS Mobile Terminals	No tamper indicators	Attach security seal
Key cards	Theft	Stored in secure area or handcuffed to personnel
POS clerk	Left station unsecured	Introduce policy to secure POS before leaving station
PoS clerk	Not trained to notice card skimmers	Introduce training to identify card skimmers and other similar devices
POS Food Court Terminal	No tamper indicators	Attach security seal
POS Gift Shop	Card skimmer attached	Remove card skimmer
PoS Gift Shop	No tamper indicators	Attach security seal
POS Mobile Terminal	No tamper indicators	Attach security seal
Radio/Supply Cabinet	Broken Lock	To be mitigated in the next cycle
Security Golf Cart	Theft	Keys stored in secure area or are handcuffed to security personnel
Security Golf Cart	Untrained personnel driving it	Introduce new policy where only those with drivers licenses may drive the golf cart
Security guard breakroom	Door left propped open	Training to not leave doors to secure areas open
Security guards	Long time between patrol of critical areas	Increased patrol frequency
Ticket Scanner	No tamper indicators	Attach security seal

Observations

- Inconsistent capitalization of POS terminal.
- There are only 22 vulnerabilities listed, which is not enough to get a “proficient” (3) rating.
- Accepting risk (i.e., postponing a mitigation) is acceptable for the Radio/Supply cabinet.
- Some hosts in this vulnerability table are missing from the asset inventory (e.g., POS clerk, Radio/Supply Cabinet, etc.).
- The names match the ones on the asset inventory.
- The mitigations for each vulnerability are reasonable.
- Common vulnerabilities are listed separately for each host as was specified in the instructions.

SYSTEM HARDENING

In 1250 words or less please describe and justify the procedures your team used to harden and defend your systems for the competition. This description should include a list of the tools that you used.
Cybersecurity professional must proactively harden and defend their systems. It is not enough to just mitigate known vulnerabilities, professionals establish and follow procedures that ensure consistent, day-to-day excellence.

POS Terminals

Several steps were taken to harden the systems primarily more security measures have been taken to protect the POS terminals, increased frequency of patrols by security guards, and personnel have been trained to recognize and prevent security incidents. The measures taken to protect the POS terminals were attaching security seals to all the POS terminals and putting the non-stationary terminals in a secure area when an employee is not present. The secure area is an employee area only accessible with the employee key cards. Putting the PoS terminals in a secure area when not in use if they can be moved makes it more difficult for unauthorized people to access the POS terminals. Attaching the security seals means that even if an adversary does access a terminal, it will be easier to identify that the terminal has been tampered with. The security seals can also be used to increase security for all the terminals, including the ones that cannot be easily moved. The materials necessary to do this were only 25 security seals, as the park already has secure employee areas that require a key card to access.

Security Patrols

The frequency of security patrols has also increased. Specifically, patrols around the fence line have increased from weekly to twice a day and low traffic areas and areas that have blind spots in the cameras have patrols twice as often. Increasing the frequency of walking the fence lines will help ensure that there are no more holes in the fence and that if an adversary does make a hole in the fence, then they are more likely to still be at the park as less time has passed. The increase in patrols in low traffic areas is so adversaries are less likely to do malicious activities in them and increase the chance of catching them if they do. There were no additional materials necessary for this, although it is recommended to consider hiring at least one more security guard due to the increase in workload.

Personal Training

The personal have also been trained in how to identify and prevent security incidents. This includes training on how to identify card skimmers and similar technology, how to recognize social engineering, and training on the policies associated with the new security measures. It also included refreshers on how to report security incidents, what counts as a security incident, how to identify suspicious behavior in guests and other employees, and policies like the one card, one entry policy into employee-only areas and to not leave doors propped open. This training is also set to be repeated every year and is now required for all employees. Because of this training the personnel are unlikely to repeat the mistakes they made.

Observations

- Inconsistent capitalization of POS terminal in first paragraph.
- Used the word personal instead of personnel.
- Personnel training section does not specify what materials were used.
- The explanation for personnel training could also be more specific.
- Needs another hardening step to earn an “exemplary” (4) rating.
- POS terminals and security patrols both have the necessary materials listed.
- POS terminals and security patrols both have at least adequate if not strong reasoning.
- All the steps taken are at least mostly reasonable.