PHYSICAL SECURITY MODULE CHALLENGE

If you have any questions, please ask them in the “”physical-sec-module” channel, under the “Operation Chimera” category on the SBT Discord server.

If you feel you’re familiar with what Physical Security is, and different types of controls and their uses, then you may be ready for the Challenge! We suggest you still do some of your own research using the ‘Useful Links’ in the training material before attempting the Challenge.

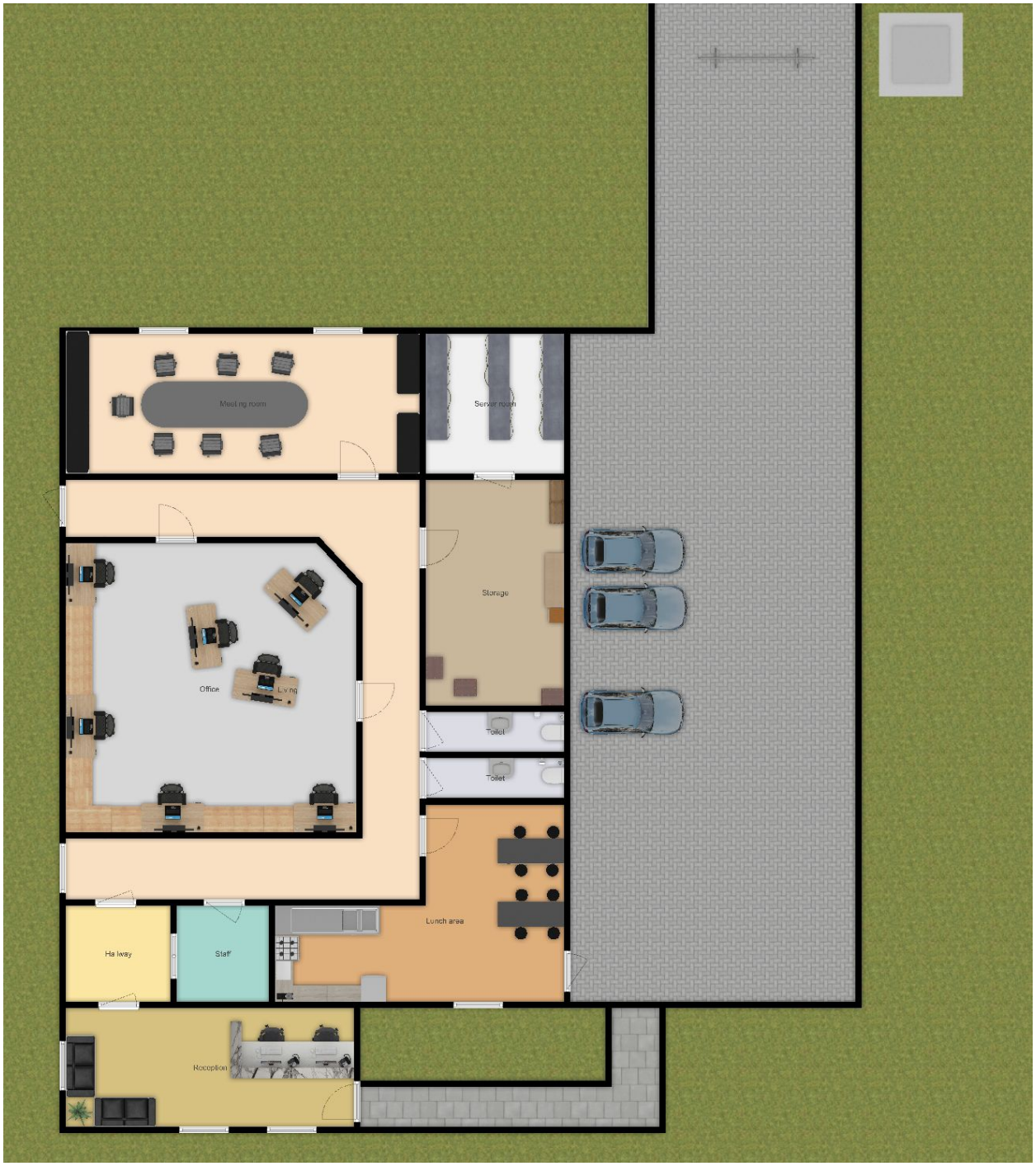
Challenge Brief:

You have been asked to refurbish a government-owned hot site for a SOC team, to make it more secure from physical attacks and intrusions. Consider how an attacker would attempt to enter the building, and what they might want to do when inside. You need to research and suggest appropriate controls including **deterrents**, **monitoring**, and **access controls**, and provide sufficient justification for your choices.. You will be graded based on your recommendations and how effective they would be given the scenario.

Please find the submission form with questions to be answered on the SBT website, under the Physical Security module:https://securityblue.team/operation-chimera

Challenge background information: (*This is a fictional challenge. Any relation to real-world events or locations is purely coincidental.*) There has been an increase in terrorist incidents recently, and the chance of physical attack is high. As a result, this backup site is being improved to withstand or at least slow down intruders until the authorities can arrive and take control of the situation.

The facility currently has no electronic doors, and they can all be opened by any employee. Fire doors (referenced in the images below) can only be open outwards, and are attached to the fire alarm system. The main access controls are a manned guard hut at the road entrance, with a simple metal barrier which needs to be moved manually. Inside the building, the main way for employees to enter the building is via the reception, into a holding room where security observe them, and then they enter the main corridor. Some employees have been seen skipping security, and entering or exiting via the kitchen door, which is unlocked. There is currently no CCTV system in place, and limited lights on the outside of the building and in the carpark.



There is currently no perimeter walls or fencing, no vehicle barricades, no CCTV, and no real lighting in the carpark, around the building, or on the path to reception.

The door on the left wall at the end of the corridor is an alarmed fire escape door, and is the only exit in the northern section of the facility.

The door on the right outer wall is a kitchen fire escape door and is alarmed. However, employees having been leaving it slightly open, allowing them to enter and exit for smoke breaks or fresh air. The room marked ‘Hallway’ is a holding room where employees or visitors talk to security (Staff room) through the window.

Physical Security Challenge Template	
Deterrent Security Controls	
What is your first deterrent control?	
Why do you think this is needed? Why will it make the facility more secure?	
What is your second deterrent control?	
Why do you think this is needed? Why will it make the facility more secure?	

Monitoring Security Controls	
What is your first monitoring control?	
Why do you think this is needed? Why will it make the facility more secure?	
What is your second monitoring control?	
Why do you think this is needed? Why will it make the facility more secure?	
Access Controls	
What is your first access control?	
Why do you think this is needed? Why will it make the facility more secure?	
What is your second access control?	
Why do you think this is needed? Why will it make the facility more secure?	