Team members:
Jyothish Sai Talagadadeevi
Gopi Krishna Muppineni
Hemanth Chowdary Vallabhaneni
Sree Charan Sai Manne

Mitigation:

We are using the command **pkill** to terminate the process by name and -f flag to ensure it matches with the entire command line and to find identify the process the system administrator get the alert of the process which is document.py then it will execute to terminate the process

pkill -f document.py.

in next will use the chmod 000 /path/to/document.py to lock the file were attacker cannot execute the script again this will quarantine the malicious script.

summary:The reason we using the pkill is for immediate threat neutralization and focusing on killing the malware spread and it is one the first step in the incident response