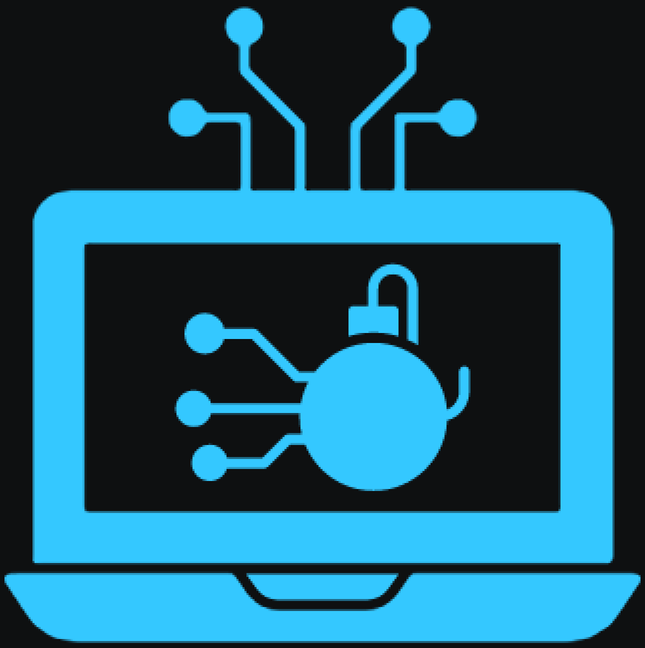
Section 1: Threat Detection



What Happened?

Task 1: ClamAV scan

As a first threat detection measure, you will have to perform an antivirus scan on the system to determine the malware files planted by the National Peace Agency on the processing plant's server. Launch ClamAV malware scanner and perform a scan on the 'Downloads' directory (*/home/ubuntu/Downloads/*). Report all detections in the `clamAV_report.txt` file.

Note: *The VM has an older version ClamAV 0.100.3 installed, which is inherently blocked from downloading new updates. See this [End of Life]() policy for specific details. Therefore, you cannot update the virus database using the `freshclam` command. However, you can still complete the task above without updating the ClamAV.*

Task 2: Suspicious File Identification

You know that the National Peace Agency has an advanced infiltration group. As a curious investigator, you still want to explore other files available in the Downloads folder, despite the ClamAV scan detecting some files as malware. Can you spot *one more suspicious file* which should have been a cause of infection but managed to defeat your ClamAV scan? Find this filename and the embedded callout URLs hardcoded in this file. This callout domain is the Command & control server of the National Peace agency. Report this finding in the file `suspicious_file_report.txt`.

Task 3: Yara Rule Creation

Once you have ensured the presence of a unique malware file that could not be detected through ClamAV scan, you also want to ensure that there is a signature or rule in place so that you can scan your other servers for the presence of the same file. Create a Yara rule file named `unknown_threat.yara` which can be compiled with ClamAV to detect the unique malware you have identified in the task above.