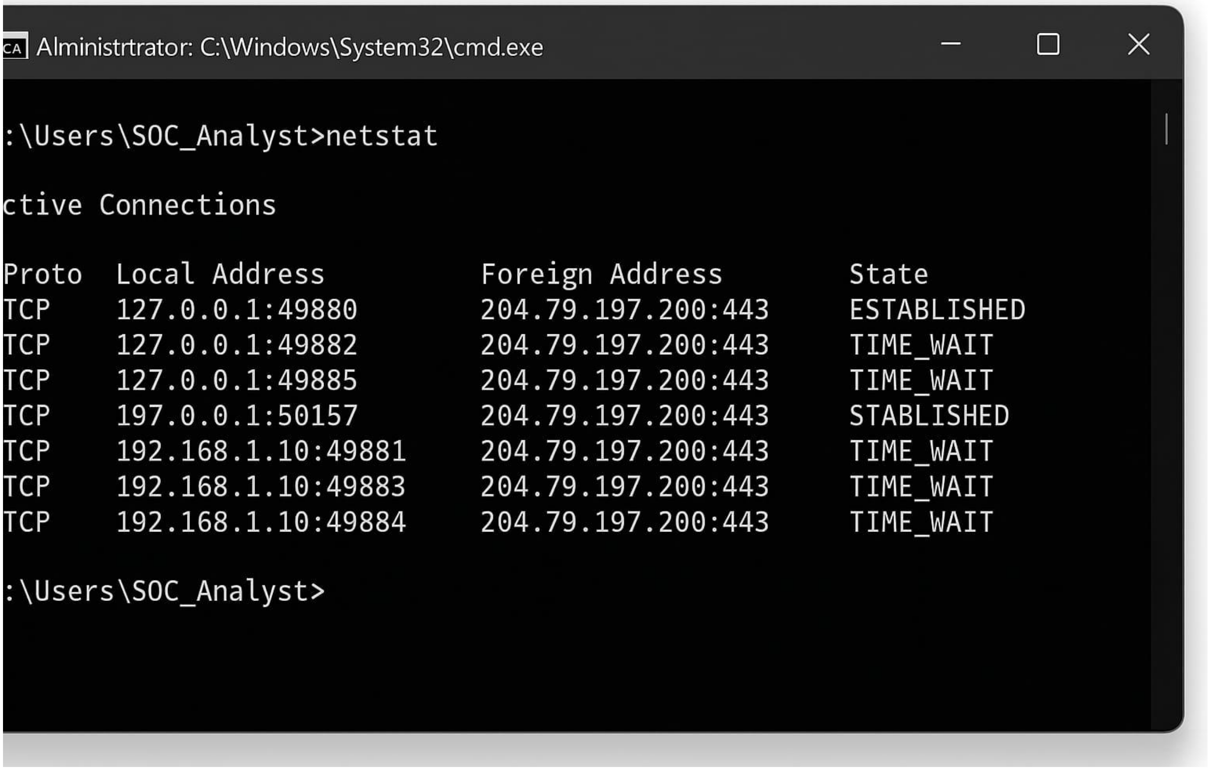
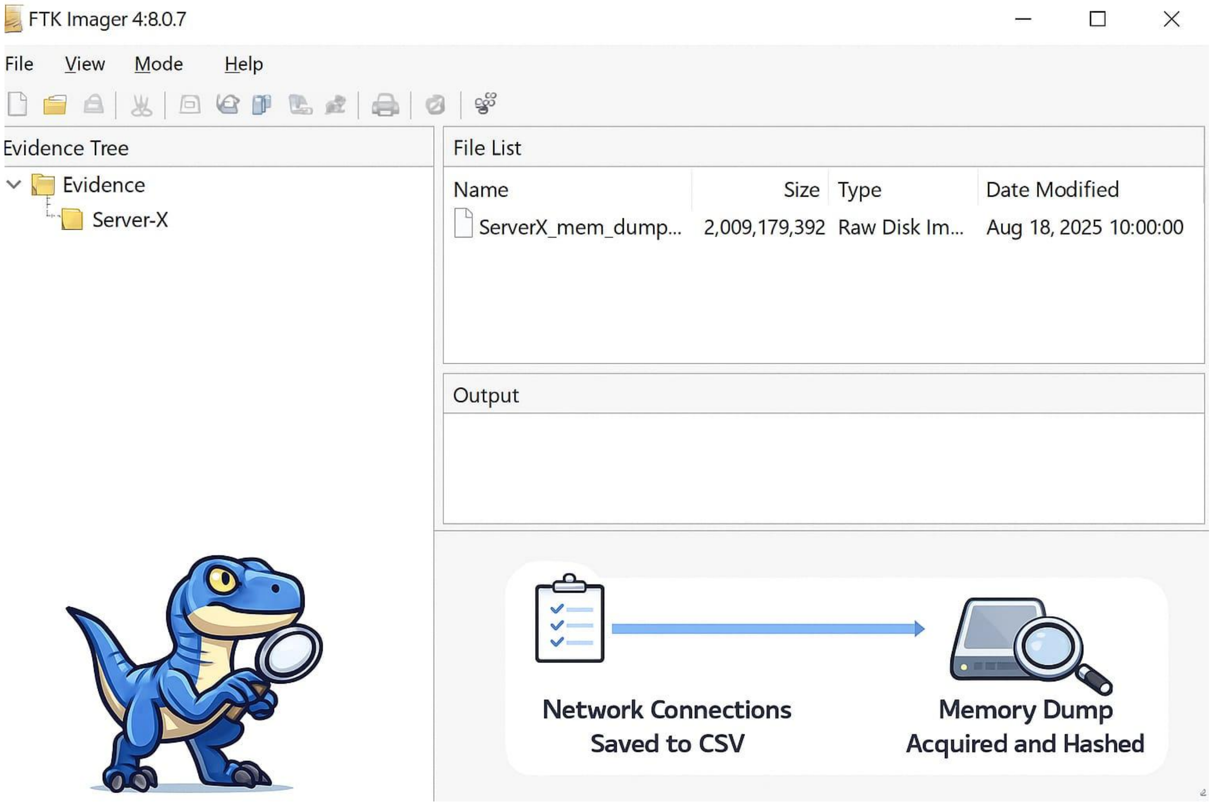
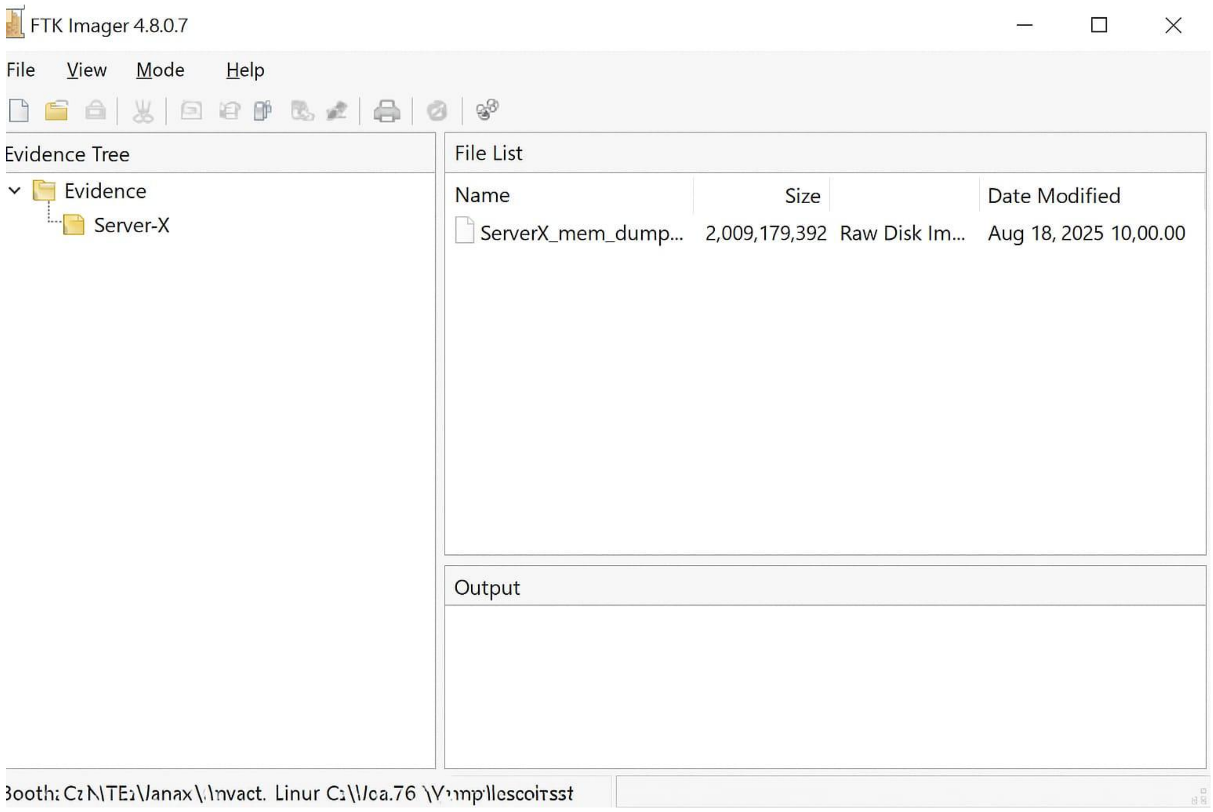


```
:\Users\SOC_Analyst>netstat

ctive Connections

Proto  Local Address          Foreign Address        State
TCP    127.0.0.1:49880        204.79.197.200:443     ESTABLISHED
TCP    127.0.0.1:49882        204.79.197.200:443     TIME_WAIT
TCP    127.0.0.1:49885        204.79.197.200:443     TIME_WAIT
TCP    197.0.0.1:50157        204.79.197.200:443     STABLISHED
TCP    192.168.1.10:49881     204.79.197.200:443     TIME_WAIT
TCP    192.168.1.10:49883     204.79.197.200:443     TIME_WAIT
TCP    192.168.1.10:49884     204.79.197.200:443     TIME_WAIT

:\Users\SOC_Analyst>
```

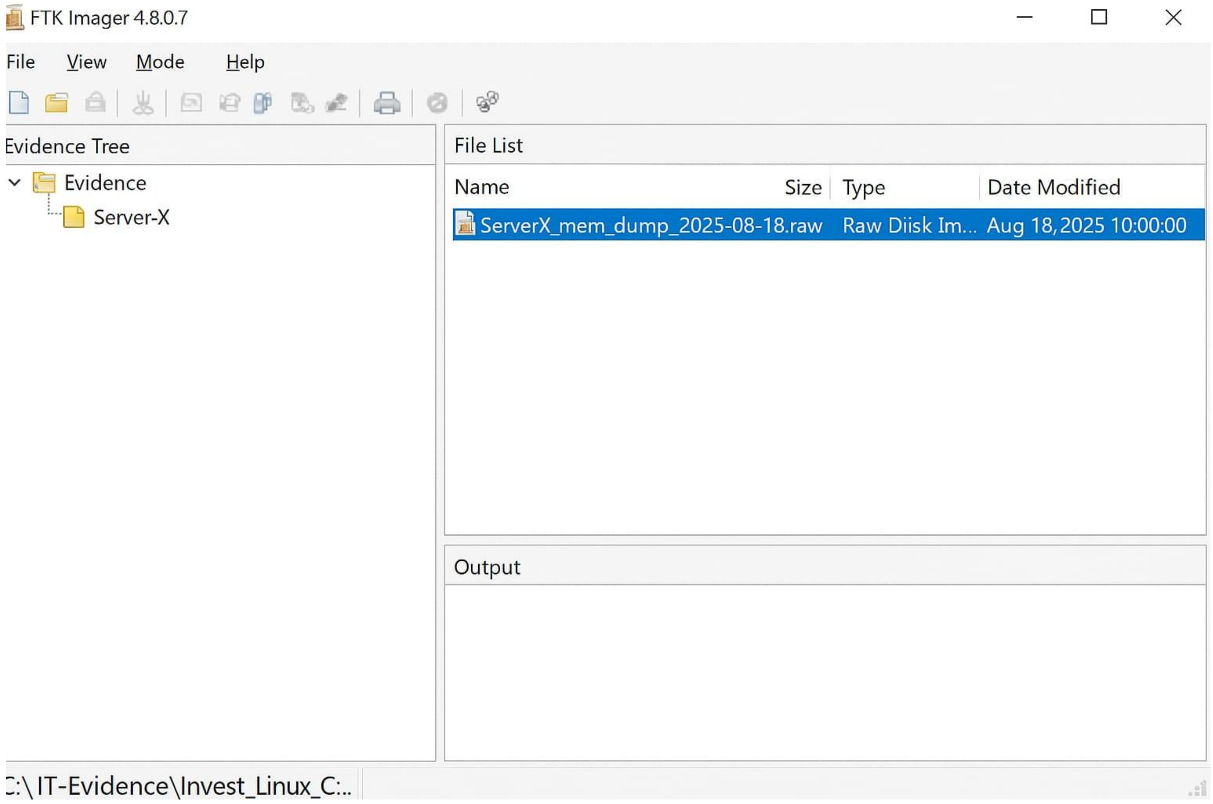


Name	Size	Type	Date Modified
ServerX_mem_dump...	2,009,179,392	Raw Disk Im...	Aug 18, 2025 10:00:00



Name	Size		Date Modified
ServerX_mem_dump...	2,009,179,392	Raw Disk Im...	Aug 18, 2025 10,00.00

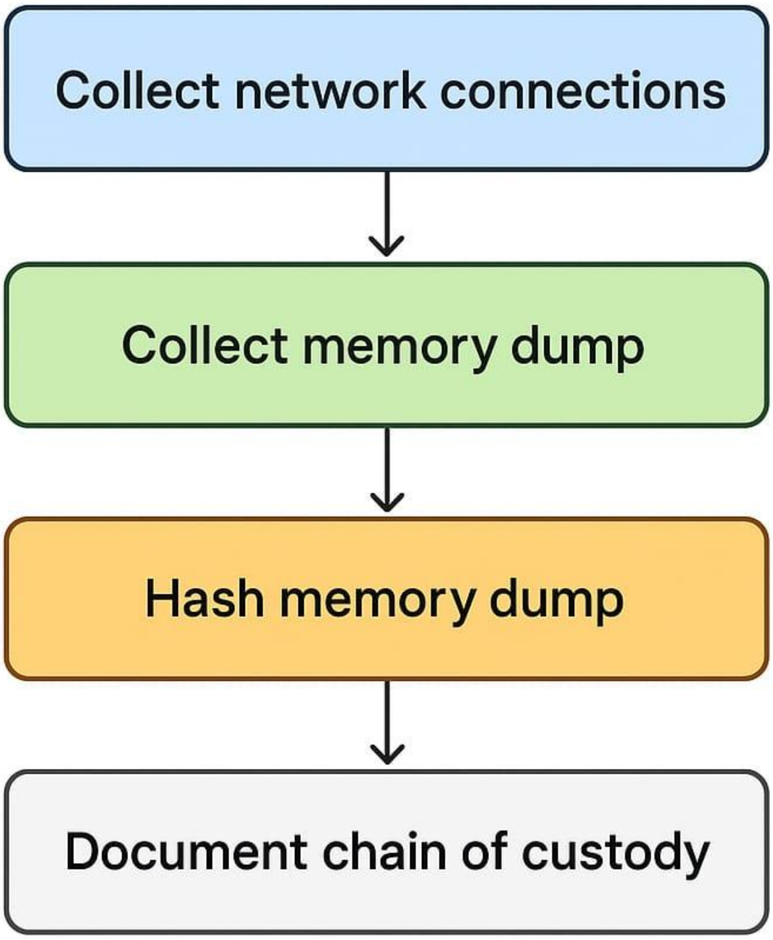
Booth: C:\ITE:\Janax\.\nvact. Linur C:\\ca.76 \V:mp\lescoirsst



Name	Size	Type	Date Modified
ServerX_mem_dump_2025-08-18.raw		Raw Diisk Im...	Aug 18,2025 10:00:00

C:\ IT-Evidence\Invest_Linux_C:..

Evidence Preservation

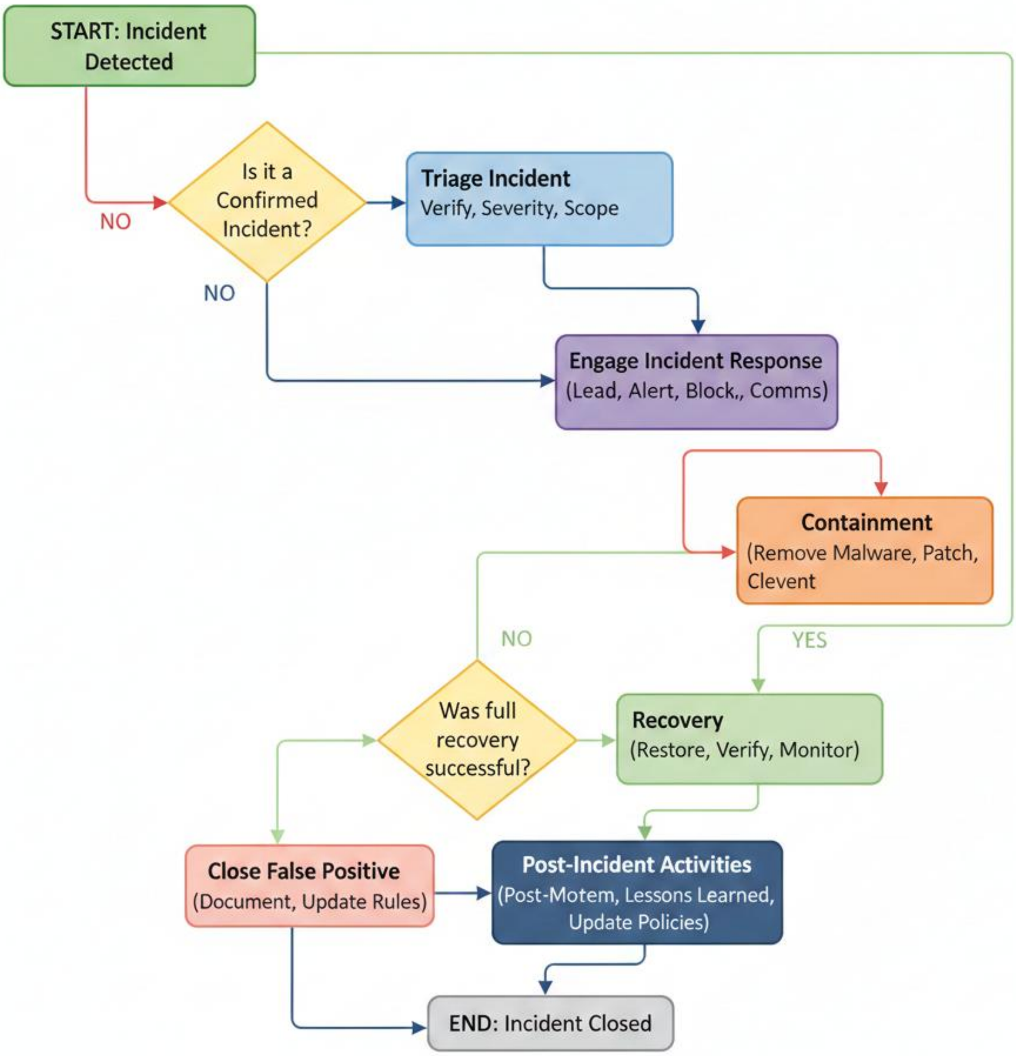


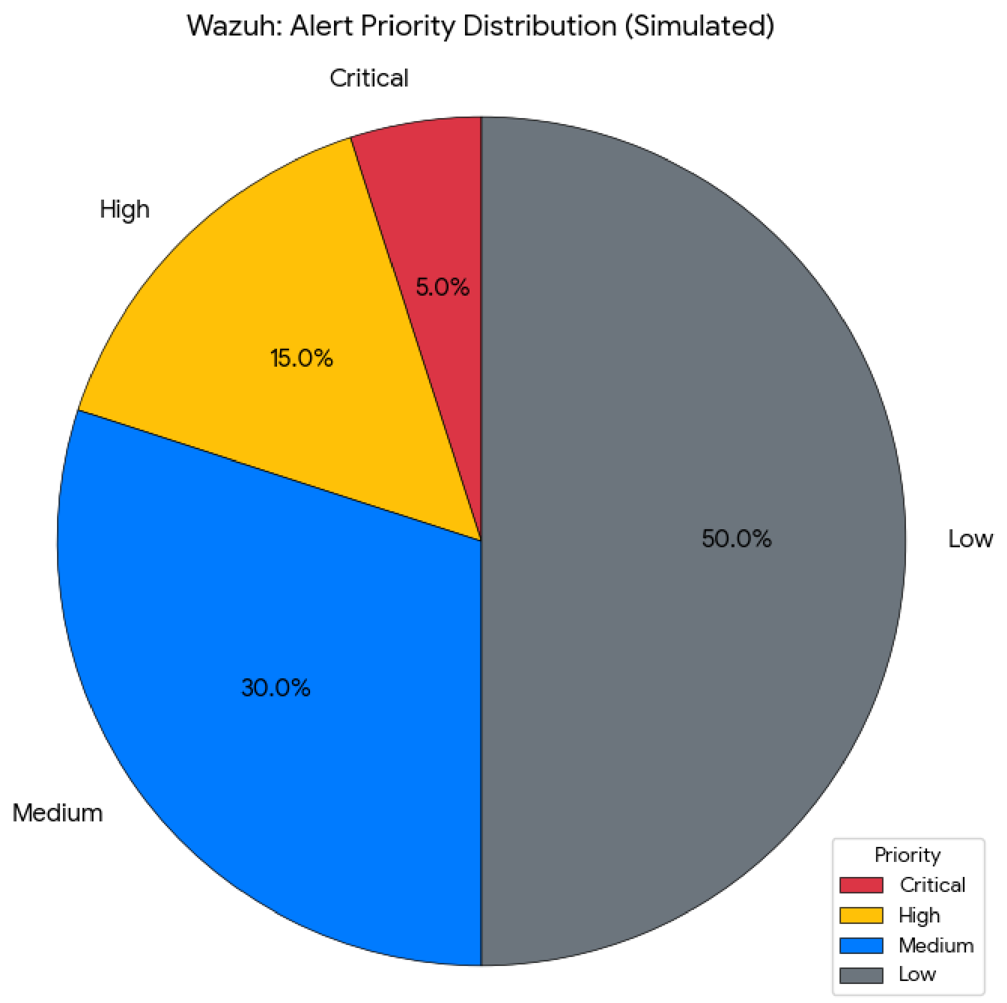
Collect network connections

Collect memory dump

Hash memory dump

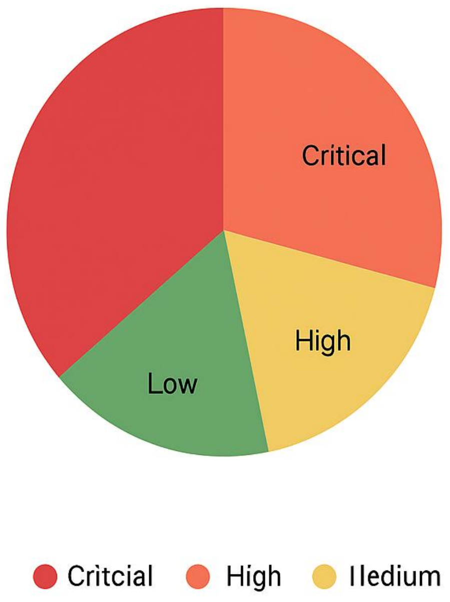
Document chain of custody


START: Incident Detected
NO
Is it a Confirmed Incident?
Triage Incident
Verify, Severity, Scope
NO
Engage Incident Response
(Lead, Alert, Block,, Comms)
Containment
(Remove Malware, Patch, Clevent
NO
YES
Was full recovery successful?
Recovery
(Restore, Verify, Monitor)
Close False Positive
(Document, Update Rules)
Post-Incident Activities
(Post-Motem, Lessons Learned, Update Policies)
END: Incident Closed

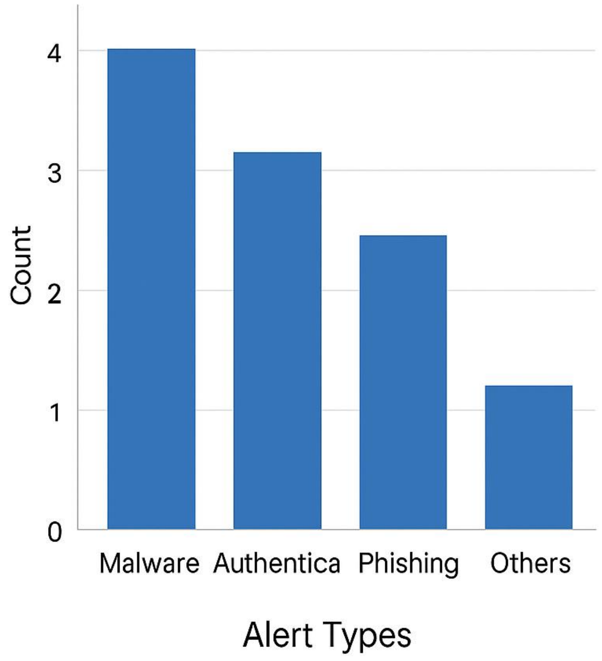


Wazuh: Alert Priority Distribution (Simulated)

Priority Distribution



Alert Types


Count
Malware
Authentica
Phishing
Others
Alert Types