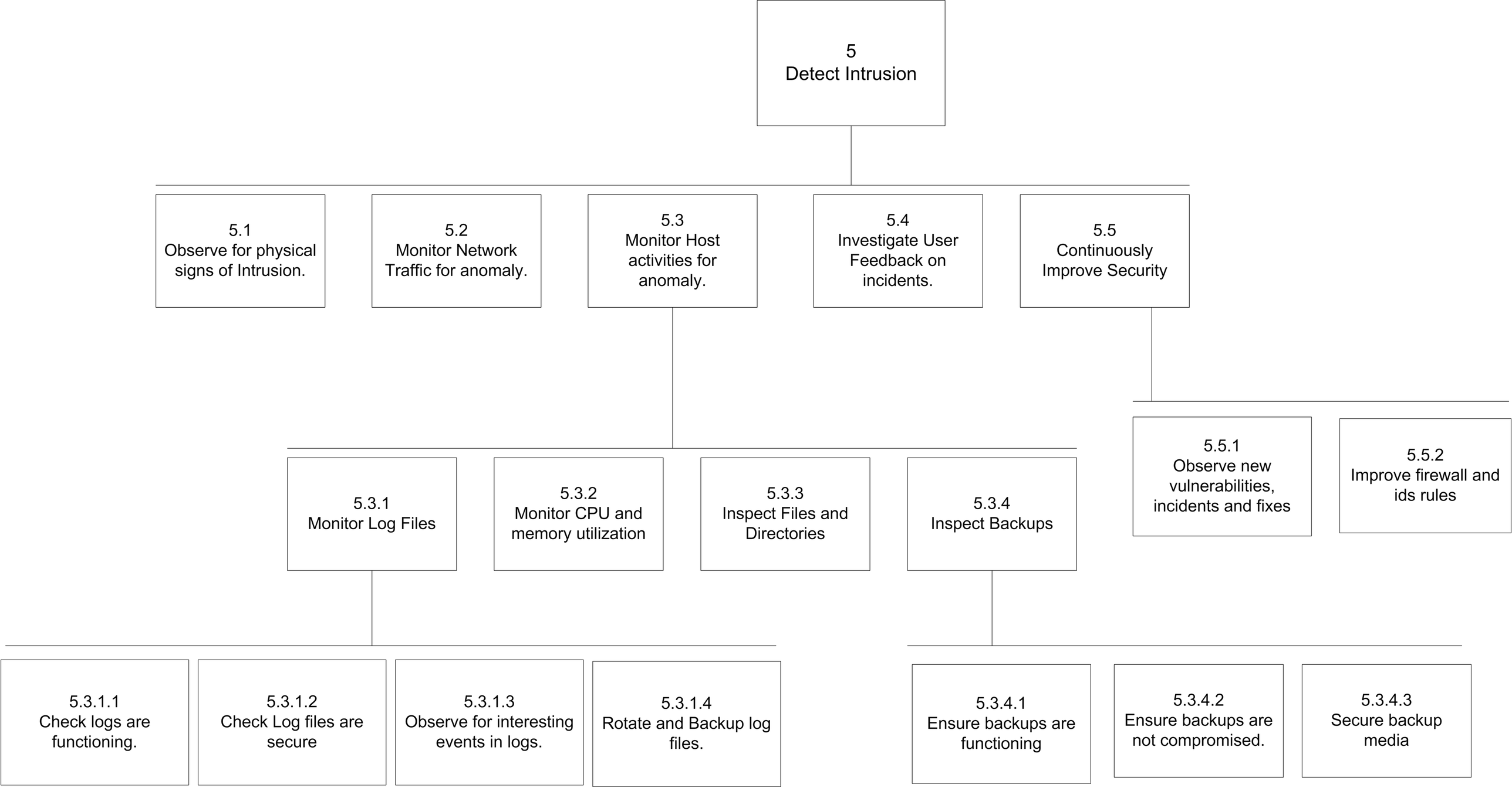
5
Detect Intrusion
5.1
Observe for physical signs of Intrusion.
5.2
Monitor Network Traffic for anomaly.
5.3
Monitor Host activities for anomaly.
5.4
Investigate User Feedback on incidents.
5.5
Continuously Improve Security
5.5.1
Observe new vulnerabilities, incidents and fixes
5.5.2
Improve firewall and ids rules
5.3.1
Monitor Log Files
5.3.2
Monitor CPU and memory utilization
5.3.3
Inspect Files and Directories
5.3.4
Inspect Backups
5.3.1.1
Check logs are functioning.
5.3.1.2
Check Log files are secure
5.3.1.3
Observe for interesting events in logs.
5.3.1.4
Rotate and Backup log files.
5.3.4.1
Ensure backups are functioning
5.3.4.2
Ensure backups are not compromised.
5.3.4.3
Secure backup media