Tools Used for Defense

SIEM: Splunk

IDS: Snort

EDR: LimaCharlie

Host-Based logging & Monitoring: Sysmon