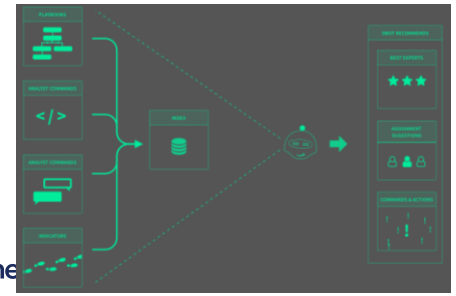
S1 NEXUS SOLUTION BRIEF

Shorten the time from detection to orchestrated response

DEMISTO

Integration Benefits

- Automate incident response and security policy through playbooks and actions
- Reduce time spent investigating threats
- Improve security analyst productivity by automating key tasks and shortening times to resolution



SOC teams find themselves drowning in constant streams of alerts, logs, and data in managing incident response lifecycles. Automation is increasingly the answer in complex security environments to enhance analyst productivity.

Leveraging **SentinelOne EPP** and **Demisto**, practitioners can combine the pre-execution, on-execution, and post-execution threat convictions and response actions of SentinelOne with the automation and orchestration of Demisto into one scalable workflow.

- Ingest activity, event, and alert data from S1 into Demisto
- Run interactive commands and automate tasks for agent lifecycle management and diagnostics: quarantine, decommission, software upgrades etc.
- Enrich incident data like hashes using S1 Deep Visibility telemetry
- Respond by orchestrating S1 convictions, including system rollback, in conjunction with other Demisto security solution apps