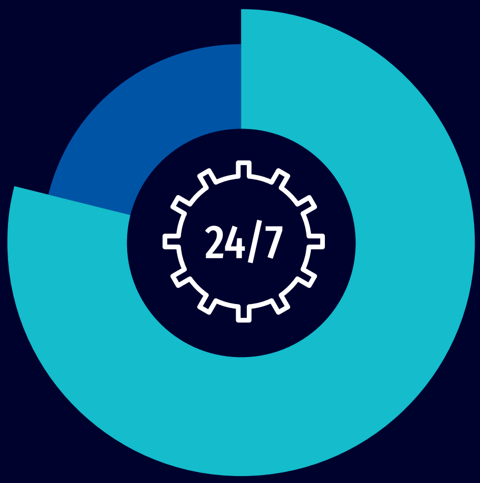
SANS | Research Program

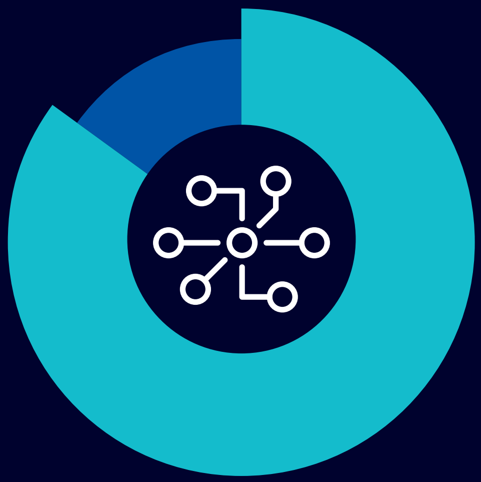
Dropzone AI

SANS 2025 SOC SURVEY
Key Findings

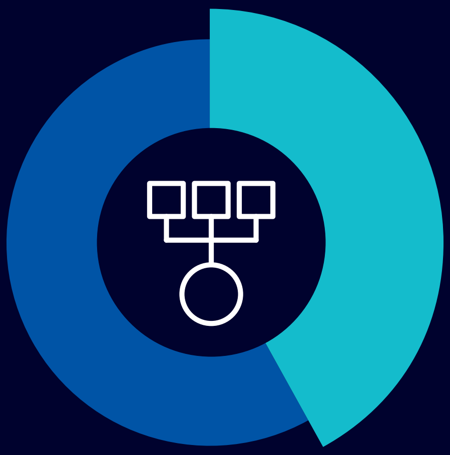
Operations and Technology Use



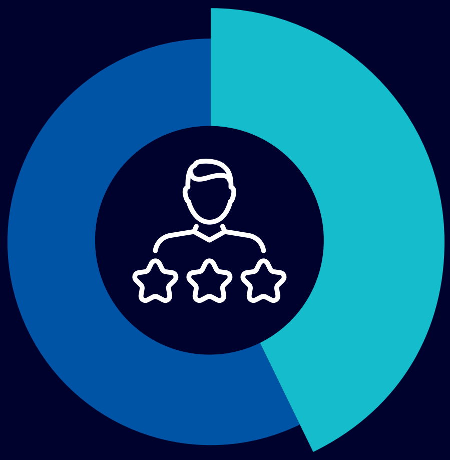
79% of SOCs are operational **24/7.**



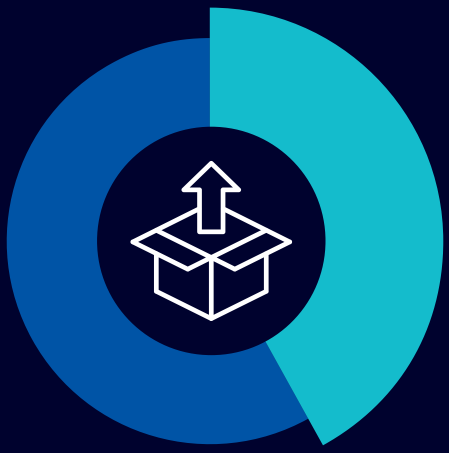
85% of respondents say **endpoint security alerts** are their **primary trigger for response.**



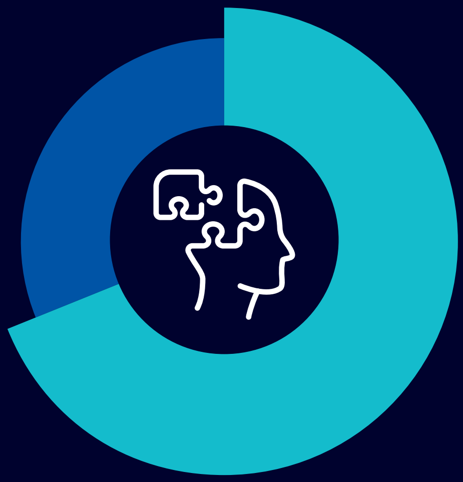
42% of SOCs **dump all incoming data into a SIEM**, often without a retrieval or management plan.



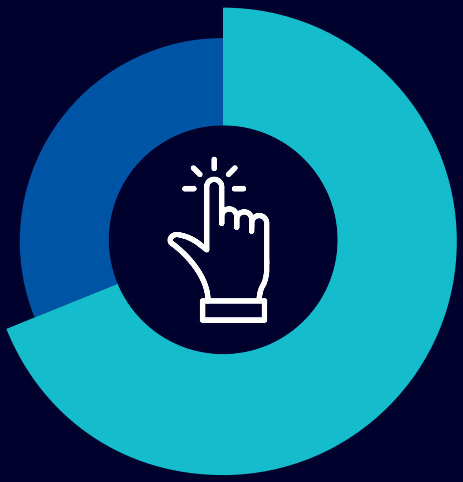
43% of respondents say **SIEM** is the **top tech skill** they seek when hiring—**more than double** the next highest response.



42% of SOCs use **AI/ML tools "out of the box"** with **no customization.**



69% of SOCs use **cyber threat intelligence (CTI)** data primarily for **incident response.**



69% of SOCs still rely on **manual or mostly manual processes** to report metrics.

Staffing and Workforce Dynamics

2–10 people is the most common size for a fully staffed SOC.

3–5 years is the most common tenure for SOC staff.

73% of organizations allow remote work for SOC team members at least some of the time.

62% of SOC professionals say their organization isn't doing enough to retain top talent.

42% of SOC staff don't know the SOC's budget, indicating a disconnect between technical and business teams.