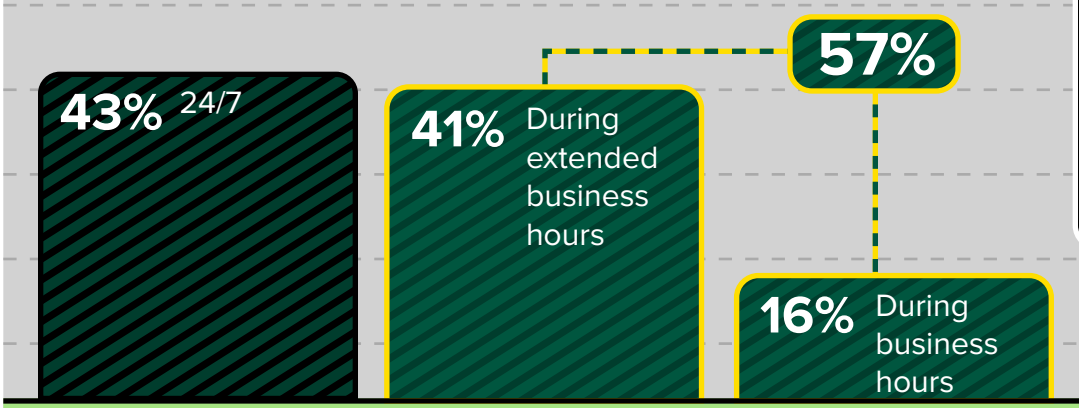
Threat Actors Work Around The Clock, But Most SMBs Don't

FORRESTER®

MOST SMBs LACK A 24/7 SECURITY OPERATION CENTER

64% of SMBs with purely internal SOCs have 10 or fewer employees*

When do SMB security operation centers (SOCs) operate?



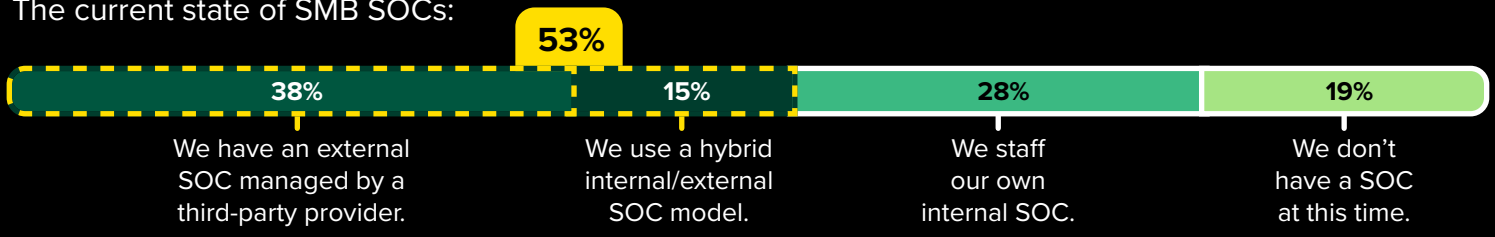
WHAT IS A SOC?

A centralized function operating as first responders for attempted intrusions with responsibilities that include detection, analysis, investigation, and response on a 24/7 basis.

These are **NOT** enough resources to run a 24/7 SOC without exhausting employees.

EXTERNAL PARTNERS HELP EXTEND THE REACH OF SECURITY OPERATIONS TEAMS

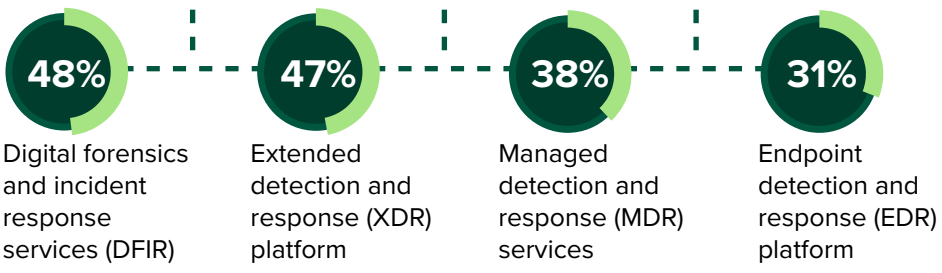
The current state of SMB SOCs:



EXTERNAL SERVICES AND TOOLS FILL SKILL AND RESOURCE GAPS

Respondents plan to invest **60%** in managed and/or consulting services and **40%** in platforms.

Top services and tools SMBs plan to implement in the next 12 months:



Base: 232 IT and security operations strategy decision-makers in the US
*Base: 66 IT and security operations strategy decision-makers in the US whose organizations have a purely internal SOC
Source: A study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Read the full study