Security Operations Maturity

Where Do You Stand?

An IDC infographic, sponsored by Symantec

Risky
Low maturity
High maturity
Routine
Re/f_ined
Robust

Security Self-Assessments May Not Be Accurate

Recent IDC research of more than 300 organizations worldwide showed that many companies operate under false assumptions when it comes to the maturity of their security operations centers (SOCs). Gain key insights from the study, as well as how to determine whether a SOC is Risky or Routine (at the lower end of the maturity scale) versus Re/f_ined or Robust (at the highest end). Also, find out where companies have made the greatest progress in maturing their security operations.

Spending Alone Doesn’t Improve Security

Although at different ends of the maturity scale, Robust organizations invest about the same percent of IT budget on SOCs as Risky ones.

Threat Intelligence, Detection Are Integral to Mature SOCs

Sophisticated security solutions are rare among companies surveyed; only robust performers deploy big data analytics; threat detection at the network, host, database, and endpoint; and threat hunting—which together are classified as advanced analytics.

Major Investments in SOC Staffing Are Planned

43% companies that have 24x7 coverage today; 16% more that plan to expand SOC coverage to 24x7 within a year.

59% organizations have higher turnover rates than the industry average; 15% less or less.

Where Do You Stand?

Is your SOC mature? Would it rate as Risky or Routine, or as Re/f_ined or Robust? Take a quick online assessment at SymantecSecOpsScorecard.com.

To learn more, visit Symantec Cyber Security Services.

All IDC research is © 2017 by IDC. All rights reserved. All IDC materials are licensed with IDC’s permission and in no way does the use or publication of IDC research indicate IDC’s endorsement of Symantec’s products or strategies.