## IDC Security Response Readiness Summary Report





## **Executive Summary**

Thank you for completing the IDC Security Response Readiness Assessment, sponsored by Splunk. This tool has been developed to provide companies with comparative information regarding their security response readiness – backed up by independent, research. The survey collected responses from security influencers or budget holders across 600 organizations globally to understand how advanced different companies are when it comes to security strategy, incident detection and incident response.

Based on this survey, IDC has scored the individual responses and created a comparison framework based on grouping organizations into five different levels of Security Response Readiness based on their approach to security strategy, and incident detection and response as seen in Figure 1. Organizations don't have to be at the top of the scale to start to see benefits. Any improvement can start to see tangible benefits to IT and the business as a whole by increasing agility, resilience and innovation through better confidence to adjust strategy to meet changing market conditions.

Stage 1 Poor



No perceived risk of breach.
Reactive.
No Incident Response plans in pace.
No Incident Response partner.
In crisis mode.
In denial regarding breaches.
Resourcing of Incident Response is unplanned and ad hoc, mostly from internal resources.

Stage 1 Standard



Limited resources to find breaches.
Basic Incident
Response partner
relationship but ad hoc.
Resourcing of Incident
Response is planned,
mostly from internal
resources.
in-house developed
solutions/processes to
detect incidents.

Stage 3 Good



Recognises era of inevitable breach. Have an Incident Response partner to call on. Prepaid blocks of time. Have a formal cyber readiness plan, not tested often. Resourcing of Incident Response is planned, using a combination of internal & external resources. Basic analytics in place drawing from SIEM feeds. Some integration between security products, probably custom-built.

Good understanding of

risk posture.

Stage 4 Aspirational



Assumed breach. Have a panel of Incident Response specialists to call on, tp provide scale and specialist skills. Have a formal Incident Response readiness plan, and tested annually. Resourcing of Incident Response is planned and mostly from external resources. Standardized Incident Response plans based on formal processes and run books.

Stage 5
Best

Proactive breach hunting. Focused on best practice and continuous improvement. Incident Response plan in place and tested regularly. Retained Incident Response team (either in-house or 3rd party). Legal agreement in place to share Incident Response data. Resourcing of Incident Response is planned using combination of internal staff and external resources on retainer, with regular planning meetings. Unified & integrated security management solution for holistic security view. Risk is key driver for assessment and mitigation processes.