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

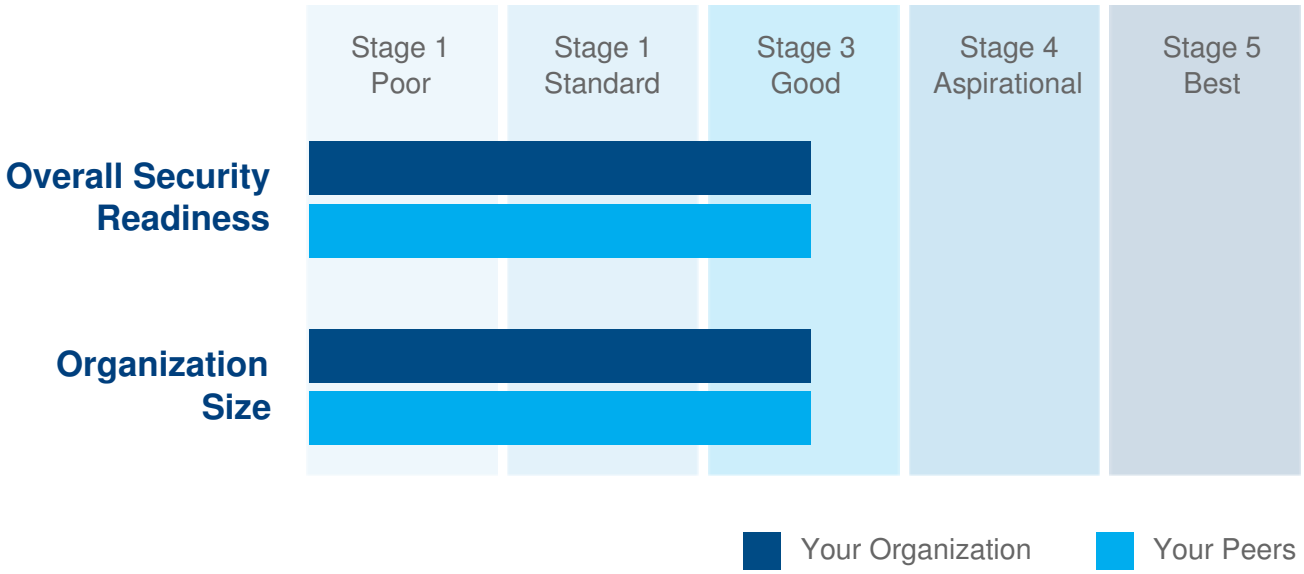
Proactive breach hunting.
Focused on best practice and continuous improvement.
Incident Response plan in place and tested regularly.
Retained Incident Response team (either in-house or 3rd party).
Legal agreement in place to share Incident Response data.
Resourcing of Incident Response is planned using 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.

IDC Security Response Readiness Summary Report

Overall Results

Based on your responses, you are placed within **41**% of companies overall in the readiness group of **Stage 3: Good**, which is the **3rd** level out of five.

Figure 2: Overall Readiness



Overall Summary

Compared to the best in class capabilities, your organization is:

- Inline with the global leaders
- Inline with the leaders in companies of the same size

Your performance in more detail

The assessment tool was designed to help establish your organization's readiness to cope with the evolving threat landscape that impacts on today's digital businesses, both today and into the future.

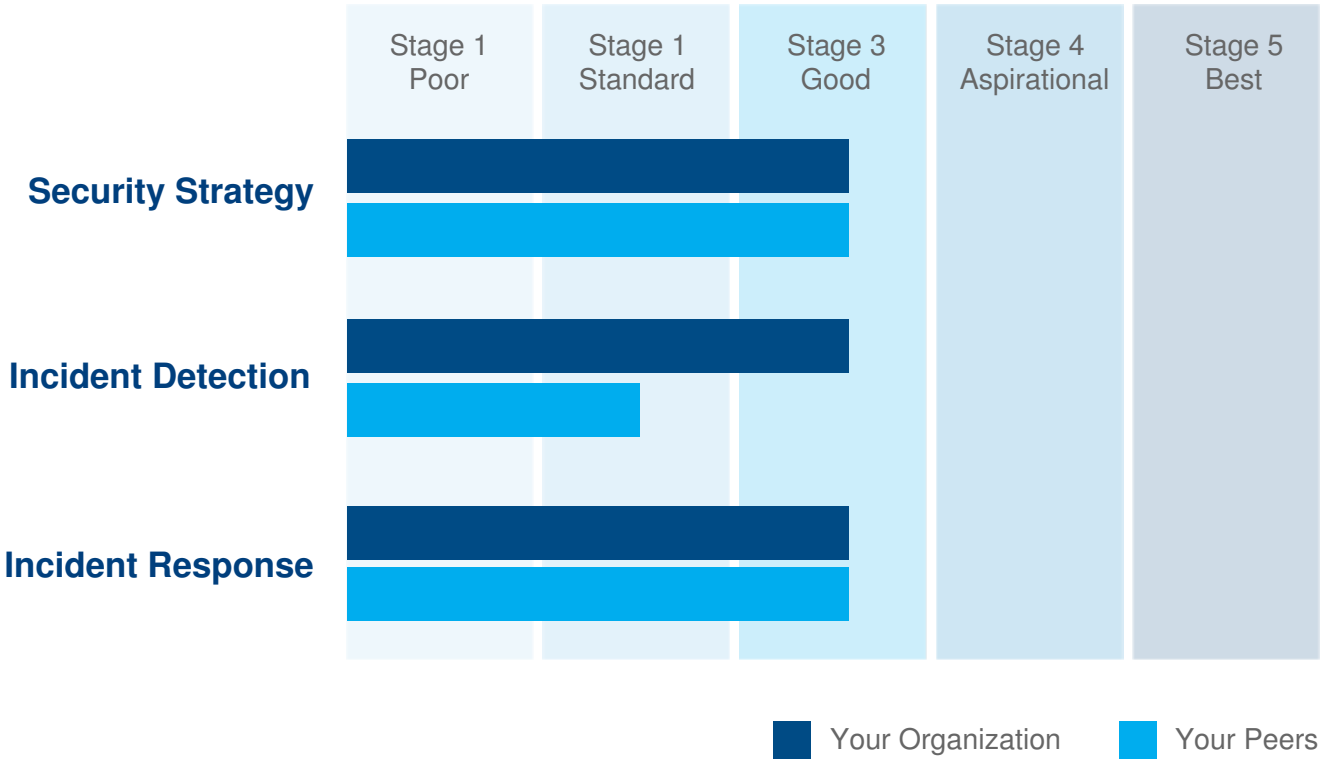
We looked at the following key areas of IT security:

- **Security Strategy**
- **Incident Detection**
- **Incident Response**

Your performance in each area is compared to your peers in Figure 3 on the following page.

IDC Security Response Readiness by Capability

Figure 3: Section Readiness



How to get ahead

No matter what level you are at, there are certain areas that are continuing to evolve and are worth focusing on above all else

- Integration – avoiding the single glass of pain
- Proactive approach – cutting the time between breach and detection from months to hours(or less)
- Keeping ahead of compliance – it is hard enough to gain compliance for most, let alone maintain it
- Best practice – recognizing that the threat landscape never sits still and that compliance and regulatory frameworks are often years out of date even at introduction, adopting a best practice approach is the best way to mitigate threats. The added advantage is that, if done right, compliance will naturally be achieved.

Improvements to Incident Response

Managing your initial response to a security incident will be critical to containing the threat and mitigating any potential damage, but you do not have anything in place now. A platform designed to standardize and manage this can be particularly useful, especially in the light of the breach reporting requirements of new legislation such as GDPR, or for IT Security Breach Insurance compliance.

A well-defined and tested response plan is essential in the event of a breach to ensure that all obligations and requirements are met. Automating this process as much as possible will be a great help in reducing ongoing operational overhead.

The longer that people have to take dealing with a security incident, the greater the impact on productivity and business risk. Reducing the time spend on investigations and remediation should be a key aim, ideally with an approach to standardizing and automating security breach response.

You are struggling to deal with the volume of incidents. Rather than bringing in more people to try to cope, consider ways to make detection and remediation (through approaches such as automation and prioritization) much more effective.

You cannot secure effectively that which you cannot measure, and you are not measuring enough to be able to determine the extent and impact of a breach. Taking a proactive approach to gathering and analysing information will enable you to not only detect a breach more reliably and more quickly, but also will help reverse engineer the breach to be able to improve your security response and risk posture to mitigate future attacks.

IDC Security Response Readiness Summary Report

Essential Guidance

Security is typically top of list of barriers for driving new IT initiatives, from developing and deploying new applications and services, to taking advantage of new IT architectures such as hybrid cloud. Proactive IT security monitoring, detection and response – built on a standardized platform with automation and analytics – will be one of the factors that differentiate the top performing digital businesses that can move quickly with market conditions. Achieving this will not come without risks and pitfalls, including

- Going in without a plan – Security need to be both deliberate and thoughtful, so make a conscious move to avoid buying products to fill gaps in capabilities. Utilize the skills of third party security experts who have hard won experience and insight to help build solutions that are known to work and to be manageable.
- Boiling the ocean – while it may seem the best solution is to rip everything up and start again, that is seldom a productive approach. Instead, look to improve your capabilities in select areas, and then build on your approach. As the level of adoption and experience rises, more of the IT infrastructure can be brought in to benefit from the advancements.
- Open inter-operability – we don't know what the future will bring, and being locked in to proprietary interfaces will hinder the ability to secure the IT estate as it grows and changes. Look to solutions that integrate well as a stack, but also support expansion through open, stable and well defined APIs and interfaces.

sponsored by splunk>