IDC Security Operational Readiness Assessment

MANAGING SECURITY OPERATIONS: TOWARDS INTEGRATION AND AUTOMATION

Sponsored by BT and McAfee

Executive Summary

Thank you for completing the IDC Security Assessment, sponsored by BT and McAfee. This assessment has been developed to provide companies with comparative information regarding the operational maturity of their security functions, backed up by independent research developed and carried out by IDC. The survey collected responses from security influencers or budget holders across 450 organisations globally to understand the differences between companies when it comes to security technologies, integration and manageability, and steps towards automation.

IDC scored individual responses and created a comparison framework, built on grouping organisations into five different levels of operational readiness based on their approach to security strategy as well as management and process automation, as seen in Figure 1. Organisations don't have to be at the top of the scale to start seeing benefits. Any improvement can bring about tangible benefits to IT and the business by increasing agility, resilience and innovation through better confidence to adjust strategy to meet changing market conditions.

Foundation

Ad hoc budgeting is typical.
Security product acquisition is ad hoc and fragmented, typically driven by threat-based needs.
Product integration is barely on the agenda.
Automation is regarded with scepticism, with concerns over visibility and control.
No use of advanced technologies, threat intelligence and analytics.
No use of virtualisation approaches.
Security deployment is entirely on-premise.
Overall influence on the board's attitude to risk is absent.

Developing

Budgets defined by project.
Security product typically chosen on a best-of-breed basis, with little consideration given to integration.
Integration is viewed mainly as a side benefit of individual products.
Automation is low on the agenda, with caution top of mind due to concerns over control.
Limited use of threat intelligence and analytics.
Limited use of virtualisation approaches to security.
Limited use of cloud deployment of security functionality.
Influence on the board's attitude to risk is low.

Good

Business unit level budgeting.
Good awareness of the importance of integration between security products, but functionality remains the overriding factor.
Product integration is balanced evenly with security functionality.
Automation is seen mainly as a side benefit of product integration.
Threat intelligence and analytics are used with a good awareness of their benefits to security operations.
Some virtualisation of security processes has taken place.
A balanced approach to security deployment from the cloud is in evidence.
Decent awareness from the board of the importance of security risk.

Aspirational

Enterprisewide budgeting.
Benefits of product integration outweigh individual product features.
Products are procured with integration a strong consideration criteria.
Automation is high on the agenda and seen as a strategic preference.
Threat intelligence and analytics are used widely, including active sharing with peers and outside agencies.
Some security processes have been virtualised, and software-defined security is on the agenda.
A sizeable amount of security functionality is deployed via public cloud.
Good influence on the board's attitude to risk, with opportunity to make the case where needs demand it.

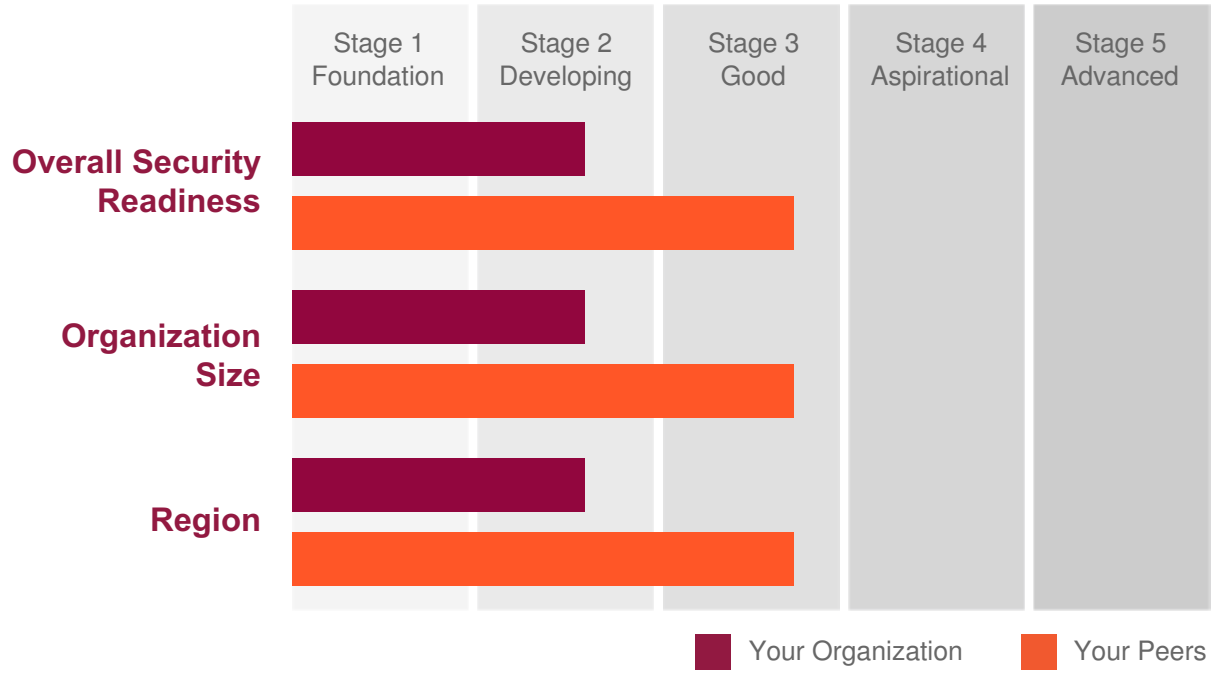
Advanced

Enterprisewide budgeting with ad hoc funding for special projects.
Integration with existing security products is mandatory and best of breed is discouraged in favour of a smaller number of preintegrated products.
Automation of security processes is at the heart of the security operation.
Threat intelligence is sophisticated, with automated policy updates being driven by insights.
Most security processes are virtualised, and software-defined security is a strategic aim.
All security functionality is deployed via the cloud where it is appropriate to do so.
Strong influence on the board, which tends to follow recommendations from the security team.

Overall Results

Based on your responses, you are placed within **32**% of companies overall in the readiness group of **Stage 2: Developing**, which is the **2nd** level out of five.

Figure 2: IDC Security Operational Readiness Assessment Results



Overall Summary

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

- 1 level behind the global leaders
- 1 level behind the leaders in companies of the same size

Your performance in more detail
This assessment tool was designed to help establish your organisation's IT security operational readiness to cope with the evolving threat landscape that impacts digital businesses, both today and in the future.
We looked at the following key areas:

- **Security Integration**
- **Security automation**
- **Unified Intelligence**

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** — focusing on security product integration, for enhanced visibility across the security estate
- **Automation** — exchanging threat information between products and updating policy decisions with minimal human supervision
- **Advanced technology** — utilising the latest technologies to improve detection and remediation
- **Advanced deployment approaches** — prioritising cloud deployments and thus benefitting from specialist security resource at scale, regular maintenance and state-of-the-art updates, with minimal downtime

Week

Security is likely to be regarded as a cost in your organisation. There is little strategic placement of security in the consciousness of business. How to change this? A good first step is to focus on operational effectiveness, where gains are likely in both the efficiency of processes and in achieving more predictable costs. Board influence is vital in the medium to longer term, so measuring security operations is essential in order to communicate good performance in business terms.

Improvements to Integration and Automation

Moderate

You have started your integration journey and are seeing some benefits of automation, albeit most likely within small groups of products. The next step is a holistic integration and automation strategy, and your best approach is to select a platform that provides a wide range of easy-to-implement integrations. The greatest benefits of integration and automation come through a completely integrated architecture, but you are likely to have a security estate composed of products from multiple vendors. So an open platform architecture is essential.

Improvements to Unified Intelligence

Weak
Threat Intelligence

You may be using threat intelligence products today, but these are likely to be straightforward feeds from third-party sources. This is fine as far as it goes, but greater benefits come from having managed threat intelligence, possibly from a specialist provider or (even better) a managed services provider that can provide better contextual information, as well as benefiting from insight from multiple organisations. Make sure you look at sharing threat intelligence, with peers and outside agencies, but understand that in order to get the greatest benefits this sharing must be bidirectional.

You can improve the effectiveness of your security operation by applying more advanced security capabilities. High on your list should be using cloud-based security solutions to secure both on-premise infrastructure and public cloud services. These are now mature and can substantially increase your security posture: the idea that cloud is inherently insecure is out of date. DDoS protection is regarded as a standard capability today, so consider commissioning a service to deliver better availability assurance.

Improvements to Security Strategy

Developing

The security you deliver to the business may be perfectly functional, but it is unlikely to be in line with business objectives. For some reason, security operations are unable to influence business decisions, which means that budgets tend to be allocated on an ad hoc, or at least localised, basis with little strategic enterprisewide planning. Aligning security provision with your businesses digital transformation programmes is fundamental, and this places new demands on both the security technology deployed and the efficiency and effectiveness of operations.

Improvements to Integration and Automation

Good

You have intuitively followed a path of security product integration and are realising the benefits of this through automation. However, this is unlikely to be consistent across your entire security estate. The adoption of a holistic, open and strategic integration platform will yield benefits not just for your existing portfolio but for future product acquisitions. Furthermore, you will get even greater gains by automating policy updates and remediation across your entire estate, rather than being restricted to preintegrated products from a single vendor.

Improvements to Security Capabilities

Good

You are making effective use of global threat inside services, and likely doing it in collaboration with peers and outside agencies. If you are not using threat intelligence to drive automated policy updates then this should be on your to-do list. You should also investigate security analytics if you are not already doing so, but make sure you have a process of continuous improvement through quantitative feedback. Managed services may also be appropriate, as they can provide greater context, as well as benefiting from the insight from multiple organisations.

You seem to have a strong set of advanced security technologies at your disposal. You are more likely to be using machine learning today, and looking seriously at cognitive computing for deployment within two years. Beyond this, you should begin looking at the benefits of blockchain and distributed ledger technology, which has a variety of security use cases, plus containerisation and other micro-segmentation approaches that can help to limit the damage suffered from attacks.

Essential Guidance

Security is a continually evolving set of processes and technologies. The challenge is to keep your security operations up to date with changes in the threat landscape as well as the demands from business to support digital transformation programmes and compliance obligations. The demands on security operations are unlikely to ease any time soon. More will be expected of you, but budget and resource increases are unlikely to rise in line.

As you seek to continually improve your security operations there are a number of important considerations to keep in mind:

- **Security is now a strategic priority for businesses. It therefore must be aligned to business strategy, and the executive must be adequately and appropriately informed of risks as they emerge and change. Security should be positioned as a business enabler, so work hard at communicating the risks and benefits in terms members will understand.**
- **An ad hoc and fragmented approach to security technology acquisition is not appropriate for the demands of a modern security operations team. Solutions exist today that enable an integrated and ballistic security architecture that provides both the visibility across the entire estate and the control and management tools to assess security posture. Automation follows integration, and this is essential if security operations are to deliver better efficiency and effectiveness within the prevailing resource constraints.**
- **Innovation in the security world has for too long largely been in the domain of the attacker. This balance is now being restored, and a plethora of new technologies have emerged over the past five years that offer capabilities that drive security to new heights. Many of these new technologies can be deployed in the cloud, and even more through managed security services, helping organisations to maintain a security operation that is state of the art.**

INDUSTRY-LEADING PROTECTION AGAINST NEW AND DYNAMIC THREATS

A Security Incident and Event Management System (SIEM) can help you understand what is happening real time on your networks, detect and highlight malicious activity, threats and attempted hacks before they become an issue. A SIEM, configured and integrated with your network and IT infrastructure, can be used not just to improve situational awareness, but also as a platform to orchestrate and automate responses and to stop attacks well before they become serious breaches.

BT and McAfee have joined forces to gather, analyse and share the latest intelligence, so that protective controls can be updated in real-time. This allows organisations to close the gap between detection and protection. Our partnership means you get access to the latest technology and security intelligence at competitive prices. Together we offer intelligent SOC and SIEM capabilities as a managed service across Europe, able to support customers worldwide. Our joint solutions contain McAfee's dynamic endpoint, Data Loss Prevention, SIEM and associated technologies.

We offer the combined benefits of McAfee's visibility and management of endpoints, currently protecting over 188 million endpoints, alongside BT's heritage in customers' managed security operations and unique carrier-level insight. With BT's 2500+ security specialists on hand, you benefit from expertise in the latest technologies and 24x7x365 cover.

From our 14 global Security Operations Centres we provide a centralised monitoring of your SIEM, giving you the information you need to respond proactively and our highly scalable service can meet the needs of all sizes of organisation – from those organisations with a few sites and hundreds of devices though to global organisations with many thousands of devices that need monitoring.

Get in touch with a BT/McAfee Expert

Book a showcase visit

Download the datasheet