5 Key Questions for Cybersecurity Vendor Selection

Customer Success Survey: January 2024

CLOUDGUARD

5 Key Questions for Cybersecurity Vendor Selection

As part of CloudGuard's yearly review, our Customer Success Leaders ran a survey across UK and Ireland based businesses to understand the challenges that IT leaders experienced when assessing the market for a dedicated cyber security partner.

The businesses had a wide variety of cyber solutions, experiences and security maturities. The purpose of this document is to summarise the key aspects respondents provided as guidance to others in considering a new cyber security solution and/or partnership.

Many businesses shared similar objectives and goals desired from cyber MXDR services. The following details ke learnings and questions to understand for anyone progressing through the buying process and looking to build out their success criteria, and ultimately, move towards a decision for their elected security partner.

All customers surveyed had a requirement for a fully Managed Detection and Response service

1. Can you provide an accurate response time commitment from detection & alert through to remediation and action?

Follow-up questions

Does this commitment meet the following conditions:

- Lasts for the duration of the contract
- Based on my current security deployment and relevant integrations within the service, not general statistics

Challenges faced

A repeated concern across the survey audience was the response time of the incumbent, or proposed, vendor over time. Specifically, 62% of respondents indicated that post implementation, the service experience did not meet the sales positioning and commitment.

The respondents were a variety of customers who purchased one of two service categories:

- A supplier for MDR services only based on alerting only to customer
- A supplier providing SOC/SIEM/SOAR services where a customer is providing MDR services and support

In certain cases, it was identified that there was a difference between indicated performance and customer experiences due to endpoint solution parameters or performance.

These differences indicated potential response times of up to 1 hour from detection through to genuine action and/or containment.

The concern was that once implemented, this part of the service performance could not be modified or improved. This means that the exfiltration, weaponisation or disruption that could be inflicted by nefarious actors, while having access to customer environments, could last up to an hour at a time from the point of intrusion.

Time to Mitigate and/or Time to Respond are key metrics to define with a supplier alongside in advance with contractual commitments.

2. Will there be access to the data logs ingested into your service?

Challenges faced

Some customers highlighted that a common issue uncovered in the purchasing process were differences in the ability, or lack thereof, to access and/or customise SIEM data that the supplier's SOC captured from the customer environment.

A 'hands-off' approach is of course a key part of any managed service, but 54% of customers required or contracted to have the information readily available to them on demand.

This issue identified is that access was not supported or permitted, coupled with concerns around the standard vendor reporting capabilities. A key consideration for many customers in considering a third party SIEM solution is improving and gaining real-time reporting with behavioural user analysis capabilities.

3. Does the responsibility for incident remediation reside with the provider or with the customer?

Challenges faced

Due to varying automation capabilities and endpoint solutions across the vendor market and respondents, many providers will only alert customers and still require manual intervention from the customer in order to effectively remediate incidents.

This, in turn, can significantly impact the Mean Time to Respond and Resolve metrics within the associated security partnership and should be defined as an absolute time not just provider time.

Respondents encouraged exploration of common scenarios for each customer environment to understand in detail the handoffs, customisations, and RACI to define roles and responsibilities, as well as incident response execution and escalation.

4. What level of tuning is included within the service provision and how is this reported on throughout the partnership?

Challenges faced

The issue here is Alert Fatigue. This was reported as both provider and customer-related. A combination of both insufficient tuning to continually reduce false and benign positive incident volumes, and a lack of support from customer success translated to customers continuing to experience higher than expected volumes of standardised alerts.

Consistent performance improvements via tuning and End User Behavioural Analysis are essential to effective detection, response, resolution and service evolution. It is essential to validate the level of tuning, commitment to ongoing improvement and how effectively this is communicated through reporting. Tuning can be rule, policy, controls or activity based.

5. What is the company's approach and commitment on data export requests on the logs being collected, monitored and transferred?

Challenges faced

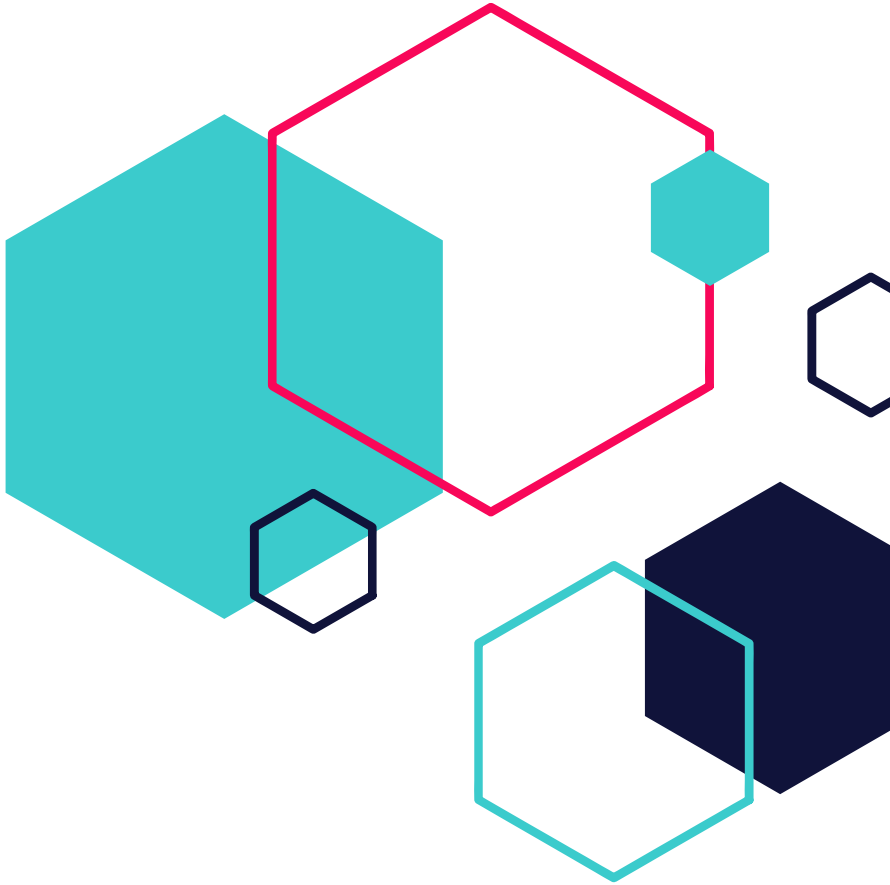
Providers have varying policies relating to the export of the data and associated formats collected from customer environments.

It is essential that back dated information is archived and can be appropriately exported from the service as it forms a crucial part of running Incident Response in the event of an attack as well as future service transition.

When migrating to another platform, or to an internally managed solution, it is essential to gain access to archives and export data for compliance, preservation of priorities, investigations, service continuity and incident histories.

Respondents highlighted that certain providers did not commit to any level of data export during or at contractual completion of MXDR services.

This resulted in many customers having to restart or managing compliance continuity challenges when avoiding vendor lockin.



5 Key Questions for Cybersecurity Vendor Selection

Contact CloudGuard for more information

hello@cloudguard.ai

CLOUDGUARD