NEAT EVALUATION FOR CAPGEMINI:

Managed Security Services

Market Segment: Overall

Introduction

This is a custom report for Capgemini presenting the findings of the NelsonHall NEAT vendor evaluation for *Managed Security Services* in the *Overall* market segment. It contains the NEAT graph of vendor performance, a summary vendor analysis of Capgemini in managed security services, and the latest market analysis summary for managed security services.

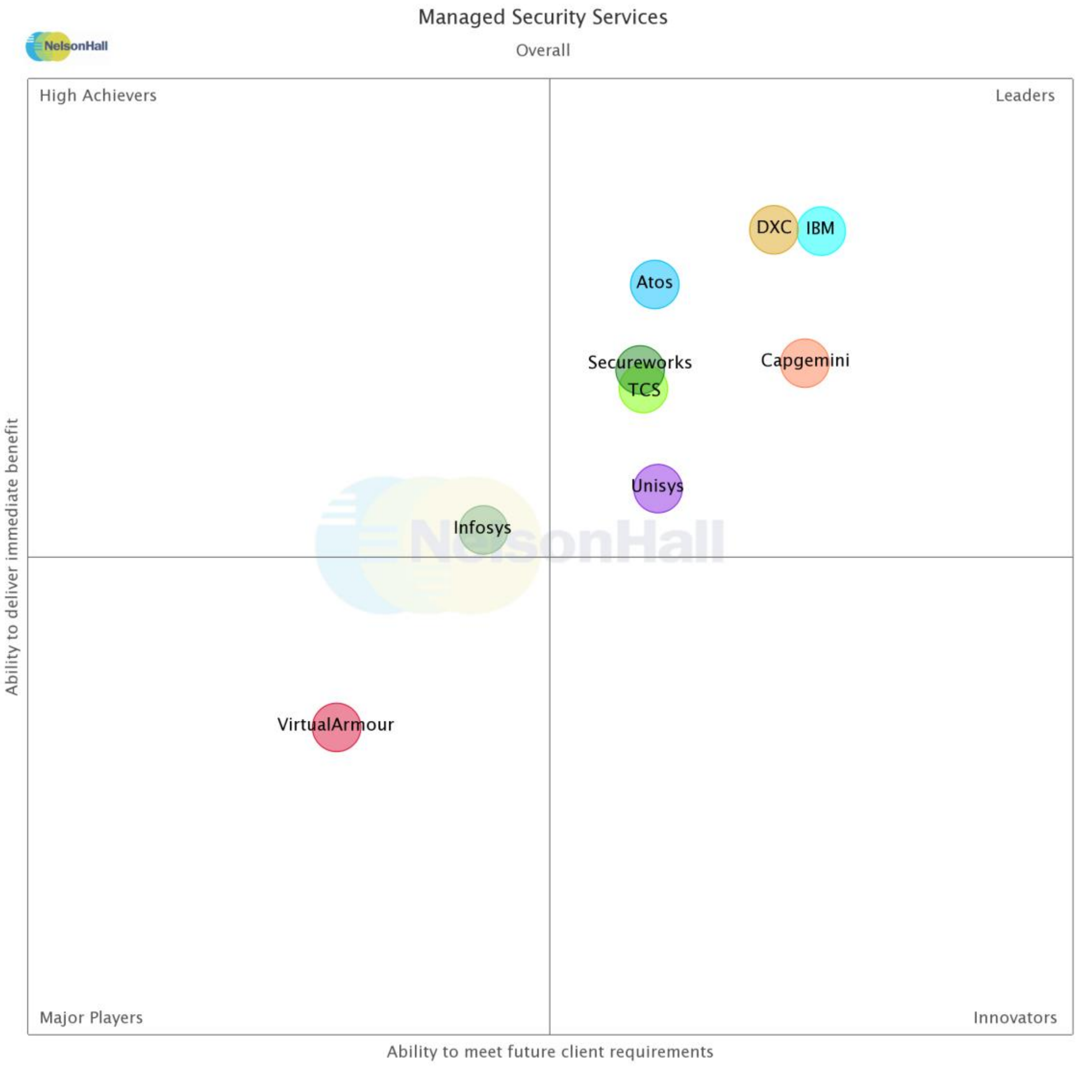
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering managed security services (MSS). The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors overall, and with a specific focus on preventative security services and advanced security services.

Evaluating vendors on both their ‘ability to deliver immediate benefit’ and their ‘ability to meet client future requirements’, vendors are identified in one of four categories: Leaders, High Achievers, Innovators, and Major Players.

Vendors evaluated for this NEAT are Atos, Capgemini, DXC Technology, IBM, Infosys, Secureworks, TCS, Unisys, and VirtualArmour.

Further explanation of the NEAT methodology is included at the end of the report.

NEAT Evaluation: Managed Security Services (Overall)



Source: NelsonHall 2018

NelsonHall has identified Capgemini as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Capgemini's overall ability to meet future client requirements as well as delivering immediate benefits to MSS clients.

Leaders are vendors that exhibit both a high ability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet client future requirements.

Buy-side organizations can access the Managed Security Services NEAT tool (Overall) here.

Vendor Analysis Summary for Capgemini

Overview

Capgemini has incorporated anomalous behavior detection, through a partnership with Pivotal, for the rapid detection of insider threats and compromised accounts or devices. On detecting abnormal behavior, clients can respond by informing management, adjusting security policies, or reducing and removing access rights. Using anomalous behavior detection, Capgemini aims to remove the threat without shutting down access completely. Capgemini is also using Huntsman to provide anomalous behavior detection, especially for the public sector.

Capgemini's Computer Emergency Response Team (CERT) provides cybersecurity incident response services (CIRT) once threats are identified. Typical services provided by the CERT include incident investigations, digital forensics, and penetration testing. If required, Capgemini can deploy members of the CERT to the client's site.

Capgemini's Identity and Access Management as a Service (IDaaS) is a modular IAM stack built on RSA and ForgeRock across IAM governance, IAM administration, and access management functionalities. The IAMaaS can be delivered either in a hosted way or on-premise in a private cloud, as a managed service in a single-tenant solution for increased flexibility. Clients are charged on a per-user, per month model.

Capgemini has built a FastTrack approach to enable the rapid deployment of an IAM project, typically within a period of six weeks. Clients pay no license fees during FastTrack.

Financials

Capgemini's CY17 revenues were ~€12.8bn. Of this, NelsonHall estimates Capgemini's CY17 total cybersecurity revenues at €520m, of which:

- Application security testing: ~€40m
- Security consulting: ~€300m
- Managed security services: ~€180m.

From the creation of the cybersecurity GSL, Capgemini targeted high double-digit growth; NelsonHall estimates that in CY17 the MSS business grew by ~40%.

NelsonHall estimates that its CY17 MSS revenues, by industry, were:

- BFSI ~35%
- Manufacturing ~22%
- Retail ~10%
- E&U ~10%
- Government ~10%
- H&LS ~3%
- Telecoms ~5%
- Other ~5%.

Strengths

- Strong investments in filling gaps in the portfolio such as cloud security services. In the last 12-months, Capgemini has been heavily investing in filling the gaps in the portfolio such as cloud security and has added some advanced services such as espionage to create a well-rounded portfolio
- Heavy investments into strengthening global coverage through the build of SOCs in support of the U.S. both onshore with the opening of Dallas and the plans for Colombia, nearshore in Sao Paulo as well as the plans to build a U.S. cyber experience center on the west coast. Likewise, the establishment of the Melbourne satellite will support APAC operations
- Strong sales and marketing push, through the use of pre-sales, positive marketing, and increasing the number of whitepapers, speaking events, blogs, and video series.

Challenges

- Capgemini is expanding operations in India as well as increasing the use of automation to support the growth in requirements of these centers
- Currently, threat information feeds in the MSS portal lack sector-specific views for clients to view the security landscape for similar organizations
- Investments to automate incident response discovery and remediation tasks are similar to some of the advanced incident response tools such as IBM Resilient.

Strategic Direction

Capgemini has recently changed its marketing around being a 'leader-for-leaders'. Capgemini operates a cybersecurity presales unit in addition to direct sales teams. These presales reach out to Capgemini's clients and provide both commercial content discussions and to provide thought leadership to potential clients. Capgemini has an ambition to have these thought leaders present in each major region. The target of these presales is to push this 'leader-for-leaders' narrative and in helping the clients develop areas of focus and strategy on cybersecurity.

In this 'leader-for-leaders' messaging Capgemini has been avoiding using fear marketing, and as such has not primarily used the likes of the fines associated with GDPR to engage with clients.

In addition to the 'leader-for-leaders' messaging, Capgemini has produced several new marketing initiatives around cybersecurity including increasing the production of white papers and the weekly 'day in the life of Jane the CISO' blog.

To target geographic expansion, Capgemini has been investing in expanding its network of SOCs, so far this year opening SOCs in both the Netherlands and in Dallas. This year Capgemini intends to open a SOC in Columbia, add a satellite center in Germany with a cyber experience center, and expand the centers in India. There are also plans for the construction of SOCs in Melbourne and Sao Paulo and a cyber experience center on the west coast of the U.S.. The construction of these SOCs will expand the reach of the cybersecurity services deliver, in particular into the U.S. for which client demand and protectionism stresses onshore investment for L2/L3 operations. Likewise in 2018 Capgemini is to develop a chatbot to allow clients to communicate around the cybersecurity offering.

As part of its investments into its MSS portal, Capgemini has been investing in how it relays its threat intelligence to clients. To allow Capgemini to provide more sector-specific plays, it will develop a heavier refined focus on sector-specific threat feeds and views.

Capgemini has been heavily investing in its cybersecurity services for cloud services, in particular for the development of secure DevOps starting on AWS and moving to Azure (see cloud security in offerings) and the automation of blueprints into the iPaaS platform. Capgemini has a rolling two-year plan to instigate more automation into cloud cybersecurity services and plans to look at which areas can be automated in each service in MSS and for the production of more technologies/platforms to support this push. Currently, Capgemini is investing in its IAM platform and automation during incident management and response. Capgemini is also continuing its work with partners including IBM for Watson for Cybersecurity with pilots in Mumbai and Inverness, this work with Watson is viewed as a longer-term target. In addition to the cloud security services, Capgemini has been investing in advanced services such as espionage services.

Outlook

Since establishing the security GSL, Capgemini has been investing in building an end-to-end portfolio of security services with recent investments including its cloud security and attack simulation services.

In 2018, Capgemini will continue building on these services and strengthening its delivery network, both in delivery centers and in technologies to support the high levels of growth within the GSL.

Managed Security Services Market Summary

Overview

As the use of advanced technologies has become more ubiquitous among MSS providers, providers are increasingly focusing on having the experienced people and frameworks to build processes in support of securing clients' operations.

While these services have existed in some form for some time, e.g., awareness training, vendors are repositioning around these services and using the services as an opportunity to interact with the C-level.

An example of this repositioning would be Unisys moving from offering singular wargaming services to offering a fixed price service which provides consulting services should the client not use an incident response retainer.

Market Size & Growth

The current global MSS market size is ~$10.6bn. The breakdown of the market, by activity, is:

- Security management: $3.7bn
- Endpoint and data Security: $1.9bn
- Threat management: $2.0bn
- Application security: $1.8bn
- IAM: $1.2bn.

The global MSS market will reach ~$20.5bn by 2022, a growth of 14.1% CAGR. Growth will be driven by:

- The proliferation of security into services such as Cloud, and Secure DevOps
- Regulatory pressure
- Responses to an increasing number and complexity of attacks.

The introduction of complementary and higher value services.

Success Factors

- Adding cybersecurity into wider ITS contract, e.g., securing cloud configurations and secure DevOps, including the ability to involve cybersecurity teams in bid support on ITS contracts
- Understanding the client's business and operations to best apply the likes of Common Vulnerability Scoring Systems (CVSS) to build cyber-risk reports and allow the organization to balance the value and the cost of remediation and demonstrate ROI
- Ability to demonstrate value in advanced cybersecurity offerings and elevate cybersecurity beyond a hygiene factor in the client's organization

- Ability to have a strong level of cybersecurity research that analyzes past events to strengthen indicators of compromise and reduce the number of false positives and negatives
- The development of strong cybersecurity talent development and recruitment programs. These programs partner with universities to hire graduates, and target white-hat hackers and previously untapped members of the talent pool, and upskill existing employees into security. Upskilling will be of particular importance as vendors bring cybersecurity into wider ITS operations
- The development of security operations centers in regions to support specific clients, such as building capabilities on/nearshore to handle data which regulations state should remain in region
- Ability to keep abreast of upcoming changes in cybersecurity regulations. High-level vendors, working with the public sector, and industry alliances influence these regulations.

Outlook

The future direction for managed security services will include:

- Take up of higher-level services and threat intelligence services to drive growth
- Threats to become more complex and new attack vectors to be constructed – for example, attacks on firmware and the chipset for which patches become harder to implement
- Technologies which add machine learning and can perform a proportion of the security research allowing analysts to perform higher value services, e.g., APTs and table top exercises to foster cyber from exec's to the legal, HR and F&A elements all the way to the general corporate culture
- Organizations to take advantage of the use of machine learning and AI solutions in vendors' security tools, and use MSSPs for the implementation and configuration of tools and management of incidents
- Cloud providers to provide more advanced security services that have a low FTE requirement
- As more robust, automated security tools are developed and more clients shift to the cloud, the requirement for vendors to perform security tool training and integration reduces
- Vendors will embed true AI, machine learning, and automation into all their cybersecurity offerings to detect and respond to threats more quickly and accurately and perform vulnerability assessments
- The use of quantum computing will render typical encryption methods useless. This lack of effectiveness will require post-quantum cryptography
- Vendors with high levels of thought leadership and the ability to provide security as part of security by design into other services.

NEAT Methodology for Managed Security Services

NelsonHall's (vendor) Evaluation & Assessment Tool (NEAT) is a method by which strategic sourcing managers can evaluate outsourcing vendors and is part of NelsonHall's *Speed-to-Source* initiative. The NEAT tool sits at the front-end of the vendor screening process and consists of a two-axis model: assessing vendors against their 'ability to deliver immediate benefit' to buy-side organizations and their 'ability to meet client future requirements'. The latter axis is a pragmatic assessment of the vendor's ability to take clients on an innovation journey over the lifetime of their next contract.

The 'ability to deliver immediate benefit' assessment is based on the criteria shown in Exhibit 1, typically reflecting the current maturity of the vendor's offerings, delivery capability, benefits achievement on behalf of clients, and customer presence.

The 'ability to meet client future requirements' assessment is based on the criteria shown in Exhibit 2, and provides a measure of the extent to which the supplier is well-positioned to support the customer journey over the life of a contract. This includes criteria such as the level of partnership established with clients, the mechanisms in place to drive innovation, the level of investment in the service, and the financial stability of the vendor.

The vendors covered in NelsonHall NEAT projects are typically the leaders in their fields. However, within this context, the categorization of vendors within NelsonHall NEAT projects is as follows:

- **Leaders**: vendors that exhibit both a high ability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet client future requirements
- **High Achievers**: vendors that exhibit a high ability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet client future requirements
- **Innovators**: vendors that exhibit a high capability relative to their peers to meet client future requirements but have scope to enhance their ability to deliver immediate benefit
- **Major Players**: other significant vendors for this service type.

The scoring of the vendors is based on a combination of analyst assessment, principally around measurements of the ability to deliver immediate benefit; and feedback from interviewing of vendor clients, principally in support of measurements of levels of partnership and ability to meet future client requirements.

Exhibit 1

'Ability to deliver immediate benefit': Assessment criteria

Assessment Category	Assessment Criteria
Offerings	SIEM Application security Endpoint security IAM Threat database maturity Penetration testing Security compliance services Insider protection and Behavioral Analytics IoT security services Level of automation/cognitive security capabilities Dashboard or portal offered Simulation or espionage services
Delivery	Ability of offer dedicated delivery Delivery in support of U.S. Delivery in support of U.K. Delivery in support of Rest of EMEA Delivery in support of APAC Delivery in support of LATAM Offshore focus for shared service MSS Onshore focus for shared service MSS Onsite support of MSS Language support Scale of FTE support Security IP Single touch point
Presence	Financial services security presence Government security presence Manufacturing security presence Retail security presence Energy & utilities security presence
Benefits Achieved	Detection and response time Value for money Threat avoidance Improved visibility through dashboard or portal Improved staff knowledge

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Investment in Cybersecurity	Area of investment in centers: onshore Area of investment in centers: offshore Investment into security dashboards Investment in automation/cognitive security capabilities Investment in threat database Investment in advanced cybersecurity services Investment in IoT security Investment in insider protection and physical security Investment in network security Investment in application security
Commitment to MSS	Industry-specific security research Security FTE growth Likelihood to partner for security services

For more information on other NelsonHall NEAT evaluations, please contact the NelsonHall relationship manager listed below.

research.nelson-hall.com

Sales Enquiries

NelsonHall will be pleased to discuss how we can bring benefit to your organization. You can contact us via the following relationship manager:

Guy Saunders at guy.saunders@nelson-hall.com

Important Notice