NEAT EVALUATION FOR DXC TECHNOLOGY:

# Managed Security Services

Market Segment: Overall

## Introduction

This is a custom report for DXC Technology (DXC) 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 DXC in managed security services, and the latest market analysis summary for managed security services.

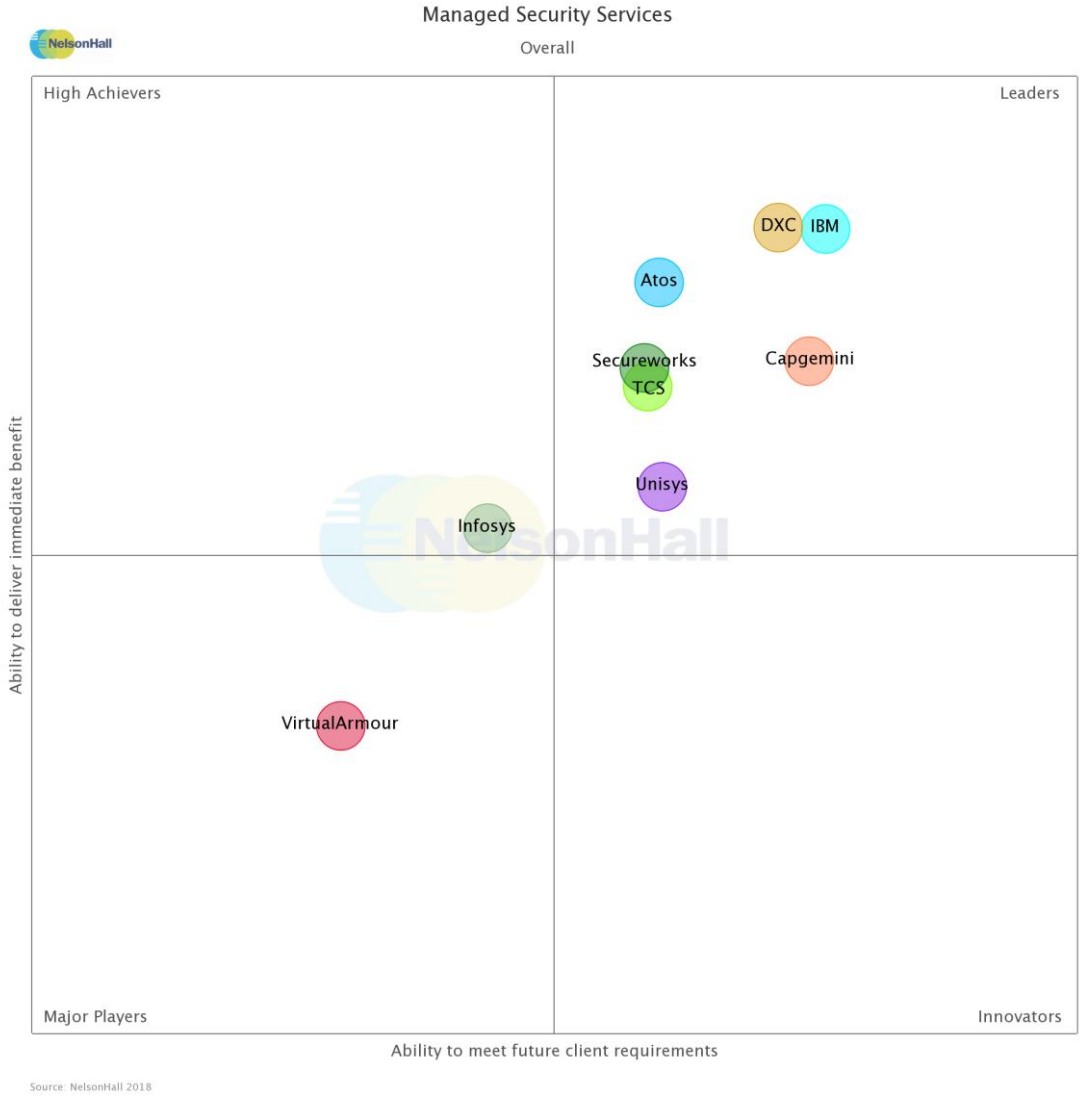
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering managed security services (MSS). The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing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




NelsonHall has identified DXC as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects DXC'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 DXC Technology

## Overview

DXC's intelligent security operations act to monitor the client's environments and reduce the complexity of securing the IT environment. DXC's threat intelligence platform is being designed to be increasingly modular, collecting security information from a number of different sources including ArcSight which currently is the main log collection platform, into a Hadoop data lake for analysis.

When indicators of compromise are discovered, DXC uses workflows developed with the CRA to respond to threats quicker.

DXC's Advanced threat protection uses FireEye's advanced threat detection, intelligence, methodologies, and incident response expertise to detect and respond to advanced threats. DXC jointly offers a global incident response with Mandiant, a FireEye company.

DXC's infrastructure and endpoint security services are used to secure a client's endpoints against malware and intrusions.

With its infrastructure and endpoint security, DXC secures over 1.8m connected devices.

DXC performs vulnerability assessments and management of the clients' IT infrastructure and applications as part of a consultancy or managed service arrangement. Vulnerability scans are delivered in ad-hoc, scheduled or as part of a system/application provisioning process.

DXC's identity and access management (IAM) services are delivered via a hybrid of cloud and on-premises based delivery. On-premises delivery allows clients to support agency-specific security policy requirements in their existing IT infrastructure.

## Financials

DXC reports their official earnings and revenue numbers through their financial filings. Based on these filings, NelsonHall estimates DXC's CY17 revenue to be $24.3bn. Within its Global Infrastructure Services (GIS) line which includes enterprise cloud apps, consulting, security, analytics, and cloud, revenue was ~$12.4bn. NelsonHall also estimates that DXC worldwide security revenues to be $800m, with the following estimated breakdown, by geography:

- North America: 50% (~$400m)
- EMEA: 45% (~$360m)
- APAC: 5% (~$40m).

NelsonHall estimates DXC's MSS revenues to be $500m.

## Strengths

- One of the largest security research capabilities, used to develop detailed blueprints and work packages in its CRA to enable DXC to provide clients with quick implementations and estimations of service
- DXC has a large scale in cybersecurity, demonstrated by its global network of SOCs and 4k cybersecurity and compliance FTEs that can support the majority of large-scale security contracts
- Despite no longer having tool ownership, being at DXC's scale allows it access to Micro Focus' roadmaps and its development in modularizing its security portal will allow DXC to ingest data from a wider array of sources and to act in a more tool agnostic manner
- The ability to offer end to end infrastructure services supported by its security capabilities.

## Challenges

- Clients more open to multi-sourcing – less likely to opt for an all in one service from an end-to-end provider security provider or provider that offers security in support of infrastructure services such as DXC
- While DXC's security investments and levels of service are difficult to rival, Indian-centric offshore MSSPs will offer competition on costs.

## Strategic Direction

Following the creation of the company from the merger of HPE and CSC, DXC's security has been undergoing a consolidation of services and optimizing its footprint. With regards to its footprint, areas of focus will be in geographies with heavy overlap specifically Kuala Lumpur and Sydney. Within security services, HPE and CSC had complimentary services, e.g., both had ArcSight as its main SIEM technology and particular strengths, i.e., HPE in security monitoring and security cloud services for Azure, and CSC in GRC/risk management and cloud security for AWS. In the year since the merger, DXC has been combining the company's offerings into a cohesive portfolio.

Likewise, since the split of the HPE Software sale to Micro Focus, DXC security has been able to focus more on being a technology agnostic MSSP. DXC claims that because it is one of the largest partners of Micro Focus and that it has more ability to choose another technology, it still has full access to Micro Focus' software roadmaps and there is more incentive for Micro Focus to invest in its toolsets.

As part of its 'platform DXC' initiative, DXC is evaluating workflow and automation platforms for security for the creation of consistent workflows. In its security platform, DXC is looking to build more modularity; increasing the ability to use more security tools will allow the platform to add more context to the security events.

## Outlook

DXC's security offering is built on the offerings of both CSC and HPE ES, with each party bringing particular strengths and partnerships. Through the merger, DXC has become one of the largest MSSPs in the industry.

While HPE ES through DXC no longer has ownership of some of the industry leading toolset, the new position as one of the largest partners of Micro Focus will enable DXC to both to continue to see the roadmaps of those technologies and act in a more technology agnostic manner.

In the last 12-months DXC has undergone some minor rationalization of services and this can be expected to continue, in particular with regards to the delivery of security service in areas for which it has more than one SOC/CoE but lower market share (e.g. Kuala Lumpur and Sydney are likely to be combined into one larger center).

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

Simon Rodd at simon.rodd@nelson-hall.com