

## NEAT EVALUATION FOR DXC TECHNOLOGY:

# Managed Security Services

### **Market Segments: Overall, Network Security, Advanced Security Services**

*This report presents DXC Technology with the 2017 NelsonHall NEAT vendor evaluation for Managed Security Services (MSS) for three market segments. It contains the NEAT graphs of vendor performance, a summary vendor analysis of DXC Technology in MSS, and the latest market analysis summary for MSS. An explanation of the NEAT methodology is included at the end of the report.*

*The vendors evaluated are: Atos, CGI, Capgemini, CSS Corp, DXC Technology, IBM, Infosys, SecureWorks, TCS, and Unisys.*

## Introduction

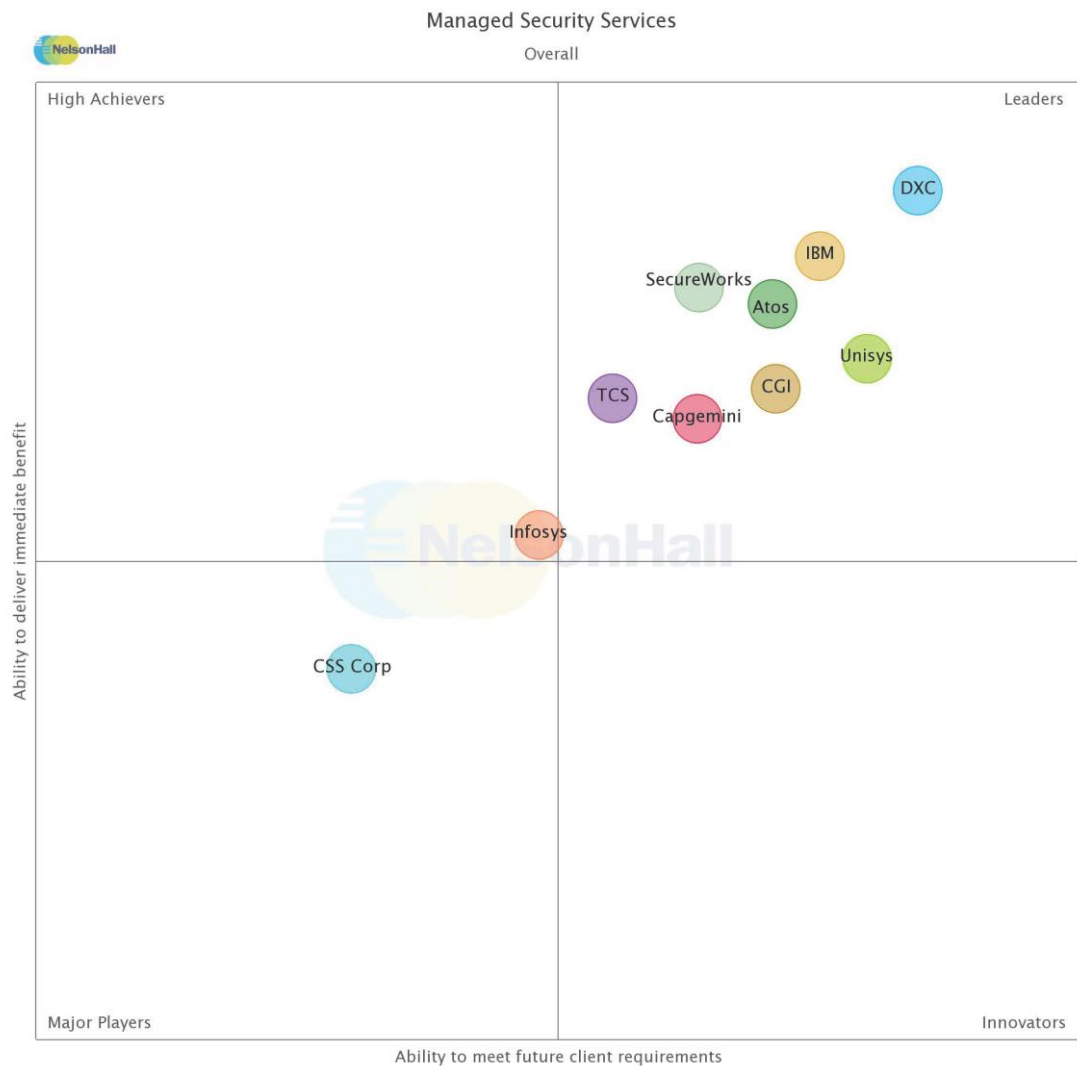
---

This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering Managed Security Services as part of their IT services portfolio. 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 application security, network security, 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.

In this MSS NEAT evaluation, DXC Technology has been identified as a Leader in the Overall, Network Security, and Advanced Security Services market segments, as shown in the NEAT graphs on pages 2, 3 and 4.

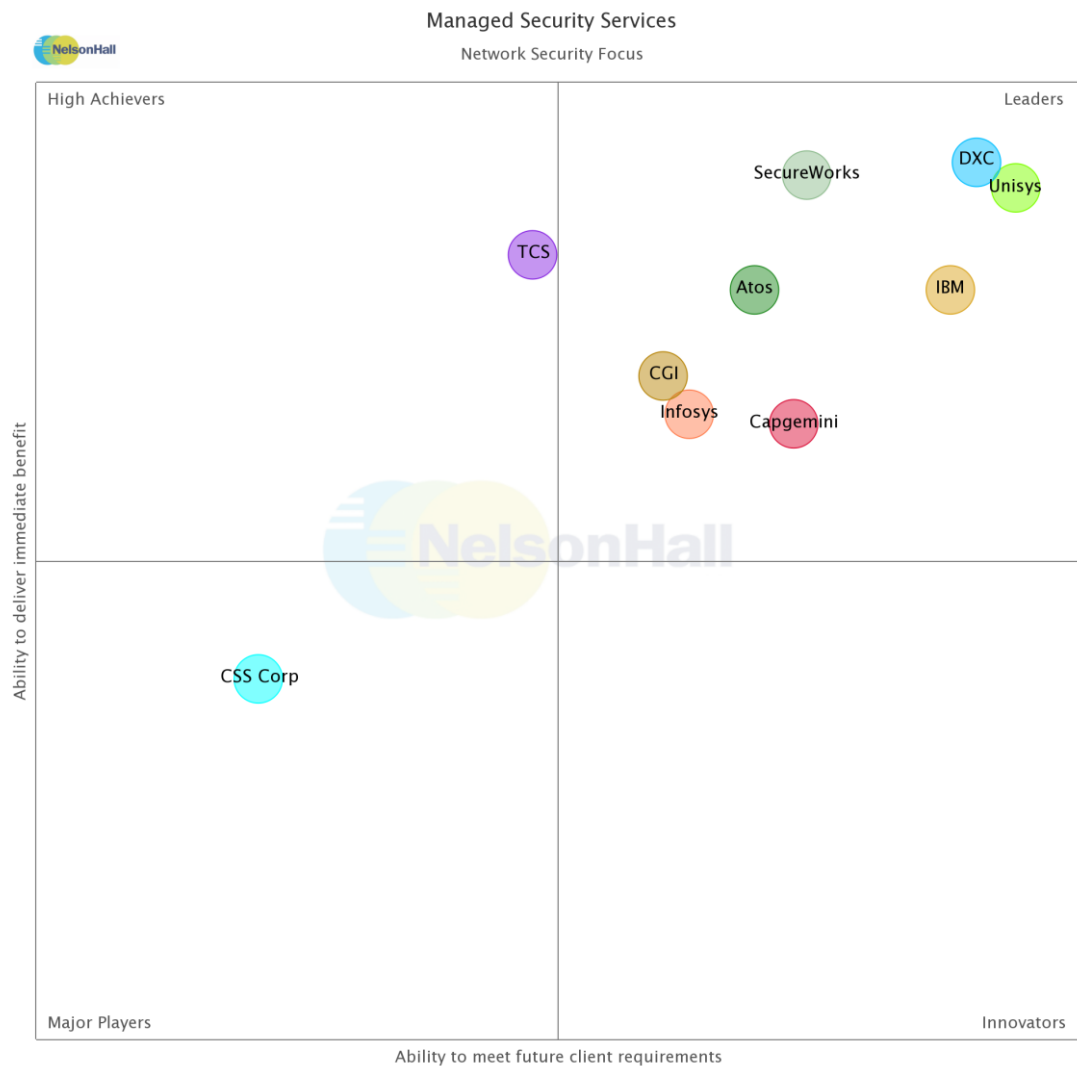
## NEAT Evaluation: MSS (Overall)



The Overall market segment reflects DXC Technology's *overall* ability to meet future client requirements as well as delivering immediate benefits to MSS clients.

Buy-side organizations can access the MSS NEAT tool (Overall) [here](#).

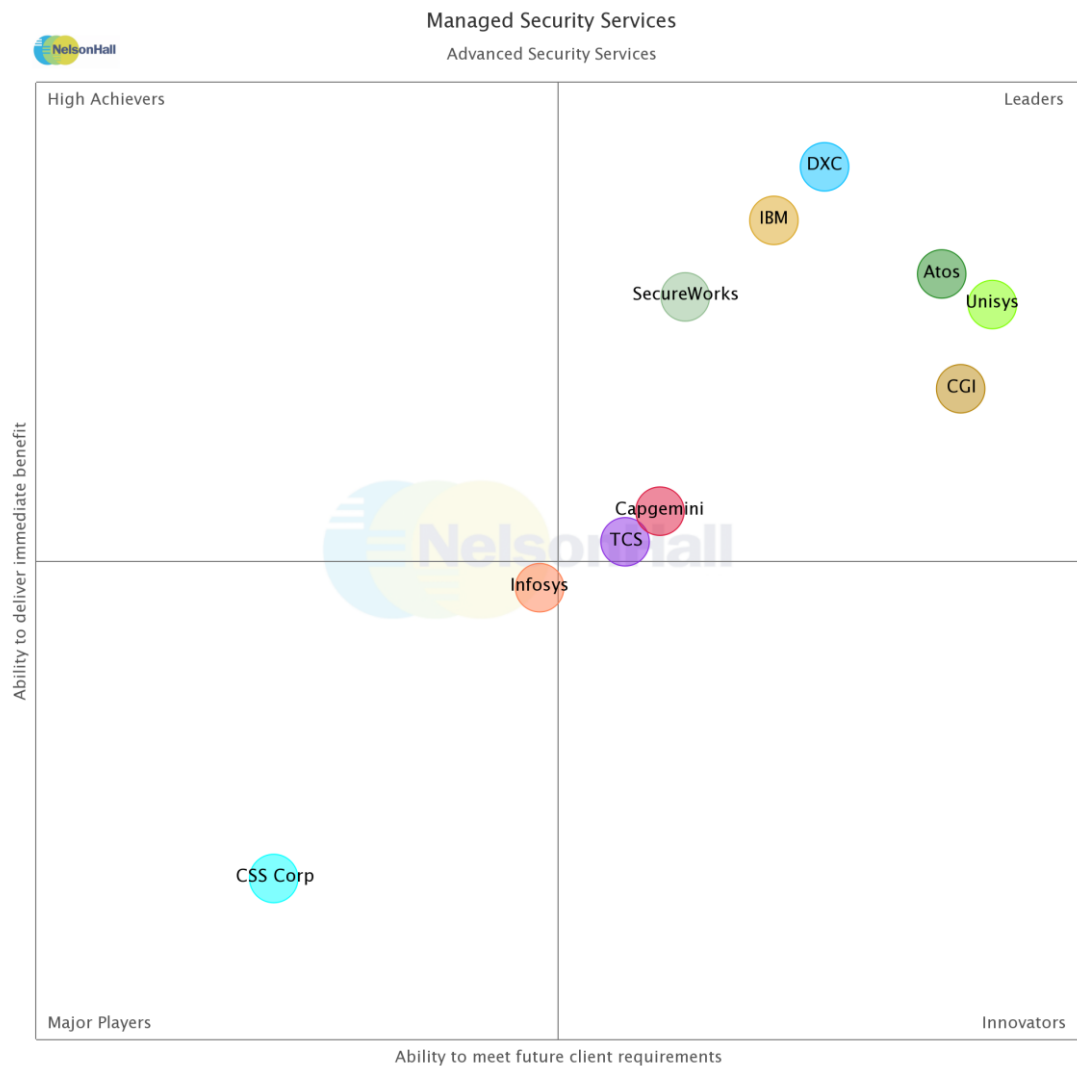
## NEAT Evaluation: MSS (Network Security Focus)



The Network Security Focus market segment reflects DXC Technology's ability to meet future client requirements as well as delivering immediate benefits to MSS clients with a specific focus on network security.

Buy-side organizations can access the MSS NEAT tool (Network Security Focus) [here](#).

## NEAT Evaluation: MSS (Advanced Security Services)



The Advanced Security Services market segment reflects DXC Technology's ability to meet future client requirements as well as delivering immediate benefits to MSS clients with a specific focus on advanced security services that go beyond traditional cybersecurity activities. Examples include forensic analysis, wargaming, insider protection and network behavioral analytics, and cybersecurity for the Internet of Things.

Buy-side organizations can access the MSS NEAT tool (Advanced Security Services) [here](#).

## Vendor Analysis Summary for DXC Technology

---

### Overview

DXC Technology, formerly HPE Enterprise Services and CSC, operates two tiers of security operations center: global security operations centers and regional security operations centers.

Its global security operations centers (GSOCs) are based in Plano (Texas, U.S.), Newark (Delaware, U.S.), Warrington (U.K.), and Sydney (Australia).

Its regional security operations centers (RSOCs) are based in Boeblingen (Germany), Costa Rica, Virginia, Bulgaria, India, Malaysia, and Toronto (Canada).

Each of the SOC operates 24x7x365 and is organized with onshore centers paired with nearshore centers, so allocating low-level security events to cheaper centers to reduce costs. The regional SOC are also utilized as domain centers of excellence for specific security activities, e.g. endpoint management, network provisioning and monitoring, identity and access management.

DXC Technology has over 4,000 FTEs in its security services, of which ~1000 are dedicated to managed security services.

Within the SOC, security analysts are aligned to threat levels (see section 3.1), with level 1 analysts performing ArcSight management and initial event analysis, level 2 performing event triage and investigation, level 3 managing incidents and threat hunting, and level 4 performing digital forensics and malware analytics.

DXC Technology's security teams are increasingly working in a 'pod' model in which a set of senior analysts are dedicated to a large client or group of clients. This model aims to forge a stronger collaborative relationship and to increase the analysts' knowledge of the client.

### Financials

Prior to the creation of DXC Technology, NelsonHall estimated HPE ES' managed security services FY16 revenues to be ~\$400m, with the following breakdown, by geography:

- North America: 50% (~\$200m)
- EMEA: 45% (~\$180m)
- APAC: 5% (~\$20m).

The merger of HPE ES and CSC to form DXC Technology creates one of the largest cybersecurity services providers, and NelsonHall estimates DXC Technology's MSS revenues at ~\$550m.

## Strengths

- One of the largest security research capabilities, used to develop detailed blueprints on how to secure clients' environments across 12 domains, 63 sub-domains, and 345 distinct security capabilities
- DXC Technology has a number of contracts in which it offers security services in addition to infrastructure services. The close connection between these teams can enable DXC Technology to interact better and more quickly respond to threats
- Pre-merger, HPE ES had been through the process of modularizing its security services, so services can be delivered to organizations that have either retained their infrastructure or outsourced to other partners
- DXC Technology has invested heavily in cybersecurity, e.g. its new security portal that collects information from all of its services and is designed to make security analysis easier and speed up threat resolution
- DXC Technology's scale in cybersecurity, demonstrated by its strong network of SOCs and a large number of FTEs, can support the majority of large scale deployments. This scale has improved with the integration of CSC and HPE ES' security capabilities
- The April 3, 2017 merger of HPE ES and CSC resulted in one of the largest security services companies globally.

## Challenges

- While the HPE ES and CSC merger to form DXC Technology adds scale and strengths in GRC, they will have a loss of ownership of the security software including ArcSight, Atalla, Fortify, WebInspect, and HP Threat Central. While the ownership of these software packages is not critical to their cybersecurity services, the detachment will mean that the merged HPE ES/CSC company will have less visibility and influence on changes in the suite
- While DXC Technology's security investments and levels of service are difficult to rival, Indian-centric offshore MSSPs will offer competition on costs.

## Strategic Direction

Pre-merger, HPE ES was continuing to add more streams into its security monitoring tools through partner technologies (particularly cloud activity monitoring tools), and in early 2017 will be launching new endpoint threat detection and response solution through its partnership with both Tanium and FireEye.

In addition to expanding the number of feeds which it ingests, DXC Technology will maximize the use of this data, performing analytics on all captured events. To enable this, DXC Technology will be investing more into its big data platform's entity relationship mapping and search facility for real-time big data hunting. By adding context to events, DXC Technology aims to better prioritize events through threat risk scoring.

DXC Technology is also investing in automation for cybersecurity. In L1/2 levels, automation is used for the generation of tickets (adding supporting information into tickets) and for reducing the number of false positives that require triage. Automations in L2/3 are based on playbooks and drive workflows. Remediation can also be semi-autonomous, with the ability

to delete, isolate, and quarantine. To further its capabilities in the area of automation, the former HPE ES invested in Hexadite.

DXC Technology will continue to develop its cybersecurity blueprints, with blueprints on cybersecurity for connected vehicles and IoT to be produced in 2017. These act as a deep set of highly detailed, granular instructions for accelerating the digital resilience of clients.

Following the merger, DXC Technology will look to combine its individual strengths in cybersecurity: HPE ES in security monitoring and threat detection, in addition to its larger scale in cybersecurity and strong ties to HPE Enterprise Software; and CSC's GRC/risk management capabilities.

HPE ES and CSC had a high overlap within their SOC locations, namely Sydney, Kuala Lumpur, the U.K., and India. While some of these sites will remain to support the existing clients and the growth in those geographies, in the medium term it is expected that there will be some rationalization of SOCs and CoEs.

DXC Technology has seen a resurgence in interest in IAM, with clients moving from manual provisioning to automated provisioning, adding governance into their identity management for more control of user accounts, and through news on IAM and IAM tools.

## Outlook

DXC Technology has a strong set of cybersecurity offerings, built through HPE's prior acquisitions of security software providers and its infrastructure services. Through the merger, DXC Technology will be one of the largest cybersecurity services providers, with NelsonHall estimated revenues in MSS of ~\$550m, and with ~4k cybersecurity professionals. Each party adds strengths and partners in cybersecurity: HPE ES in security monitoring and threat detection capabilities, and CSC in GRC and risk management.

In the term after the acquisition, NelsonHall does not expect much immediate change; both vendors act as technology-agnostic service providers that can provide end to end cybersecurity services from system integration to managed services, and both have ArcSight as their main SIEM technology.

In the mid-term, expect to see a rationalization of SOCs and CoEs, particularly in high-cost locations with overlap. NelsonHall predicts that the centers most likely to experience rationalization are Kuala Lumpur, Sydney, and the U.K.; areas that have low proportions of business (excluding the U.K.), and are fairly high in costs.

Also, expect a rationalization of services that tie to infrastructure services, as well as the construction of more modular security services that are not connected with infrastructure contracts. In particular, this means continuing to build MSS for clouds, particularly AWS/Azure, and a stronger discrete application security offering.

## MSS: Market Summary

---

### Buy-Side Dynamics

Key challenges for organizations looking to outsource MSS are:

- Increasing cost of cybersecurity, while demonstrating ROI
- Access to cybersecurity skills and up-to-date information
- Ability to respond quickly to threats
- Ability to gain a holistic view of cybersecurity
- Strengthening social engineering around security
- Uneven workloads.

### Market Size & Growth

The current global MSS market size is estimated by NelsonHall at ~\$9bn and is on target to reach ~\$17.6bn by 2021, a growth of 12.2% CAGR.

Growth will be driven by:

- Regulatory pressure
- Responses to an increasing number and complexity of attacks
- The introduction of complementary services.

North America accounts for 43% of the MSS market. Vendors with American ties are slow to make progress in APAC. Vendors will continue to look for growth in APAC, firstly through supporting clients from Australia based SOCs, then with CoEs stationed in e.g. Singapore and Hong Kong.

### Success Factors

Critical success factors for vendors within the MSS market are:

- Ability to develop a strong go-to-market that demonstrates vendor strengths in cybersecurity research/delivery
- 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
- Ability to keep abreast of upcoming changes in cybersecurity regulations. High-level vendors, working with the public sector, and industry alliances can influence these regulations
- The development of strong cybersecurity talent and recruitment programs. These programs partner with universities to hire graduates, and target white-hat hackers and previously untapped members of the talent pool, through diversification



- The development of security operations centers in regions to support specific clients. Vendors have additional FTEs in countries outside of SOC's to support languages other than English
- Ability to demonstrate the ROI of cybersecurity services. Vendors run wargame scenarios and vulnerability assessments to demonstrate how a cyber-attack can affect a client's operations
- For traditional ITS providers, the ability to involve cybersecurity teams for bid support on ITS contracts
- The ability to rationalize the services from acquired parties. For example, the merger of HPE ES with CSC (where HPE ES is the stronger party in terms of cybersecurity). The combined company, DXC Technology, will benefit from the strong overlap in cybersecurity tools used by both parties, whatever the overlap in cybersecurity centers and services that require rationalization.

## Outlook

Over the next few years:

- Regulations will come into force, e.g. GDPR in 2018, which will affect organizations with EU operations. These regulations will inform the introduction of cyber regulations in emerging markets
- Security threats that risk corporate reputation and regulations will force cybersecurity to be a hygiene factor
- Vendors to continue to restructure and relaunch cybersecurity portfolios around cloud security and to rationalize acquired offerings
- Vendors to focus branding of security offerings around securing clients' reputation
- As more robust, automated security tools are developed, the requirement for vendors to perform SIEM rule tuning reduces, allowing vendors and clients to focus on more advanced threats
- Vendors will embed true AI, machine learning, and automation into all their cybersecurity offerings to detect and respond to threats more quickly and accurately. A standout example of this is IBM investing in integrating Watson for cybersecurity. Vendors unable to add AI will partner with the typical tool providers
- The lack of effectiveness of typical encryption will require advanced encryption techniques to be built into technologies such as blockchain
- In 2020, revenue from threat management services such as cyber resiliency services will overtake security management to be 24% of the managed security market. Vendors that have partnered with cybersecurity insurers will see the most demand for cyber-resiliency services
- Technology supporting securing new developments such as IoT and full DNS record scanning will require new approaches of collecting, analyzing, and storing security data on a much larger scale. The use of quantum computing for security such as quantum cryptography should be assessed.

## NEAT Evaluation for MSS

---

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
	Ability to offer security as part of a larger ITS contract
	Insider protection
	IoT security services
	Level of automation
Delivery	Dashboard or portal offered
	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
Presence	Security IP
	Single touch point
	Financial services security presence
	Government security presence
	Manufacturing security presence
Benefits Achieved	Retail security presence
	Energy & utilities security presence
	Detection and response time
	Cost reduction
	Threat avoidance
	Improved visibility through dashboard or portal

## 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 Investment in threat database Investment into advanced cybersecurity services Investment into IoT security Investment into insider protection and physical security Investment into network security Investment into application security
Commitment to MSS	Industry specific security research Security FTE growth Financial rating 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](http://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](mailto:guy.saunders@nelson-hall.com)

#### Important Notice

Copyright © 2017 by NelsonHall. All rights reserved. No part of the publication may be reproduced or distributed in any form, or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher. The information provided in this report shall be used only by the employees of and within the current corporate structure of NelsonHall's clients, and will not be disclosed to any other organization or person including parent, subsidiary, or affiliated organization without prior written consent of NelsonHall. NelsonHall exercises its best efforts in preparation of the information provided in this report and believes the information contained herein to be accurate. However, NelsonHall shall have no liability for any loss or expense that may result from incompleteness or inaccuracy of the information provided.