NEAT EVALUATION FOR UNISYS:

Cyber Resiliency Services

Market Segment: Overall

Introduction

This is a custom report for Unisys presenting the findings of the NelsonHall NEAT vendor evaluation for *Cyber Resiliency Services* in the *Overall* market segment. It contains the NEAT graph of vendor performance, a summary vendor analysis of Unisys for cyber resiliency services, and the latest market analysis summary.

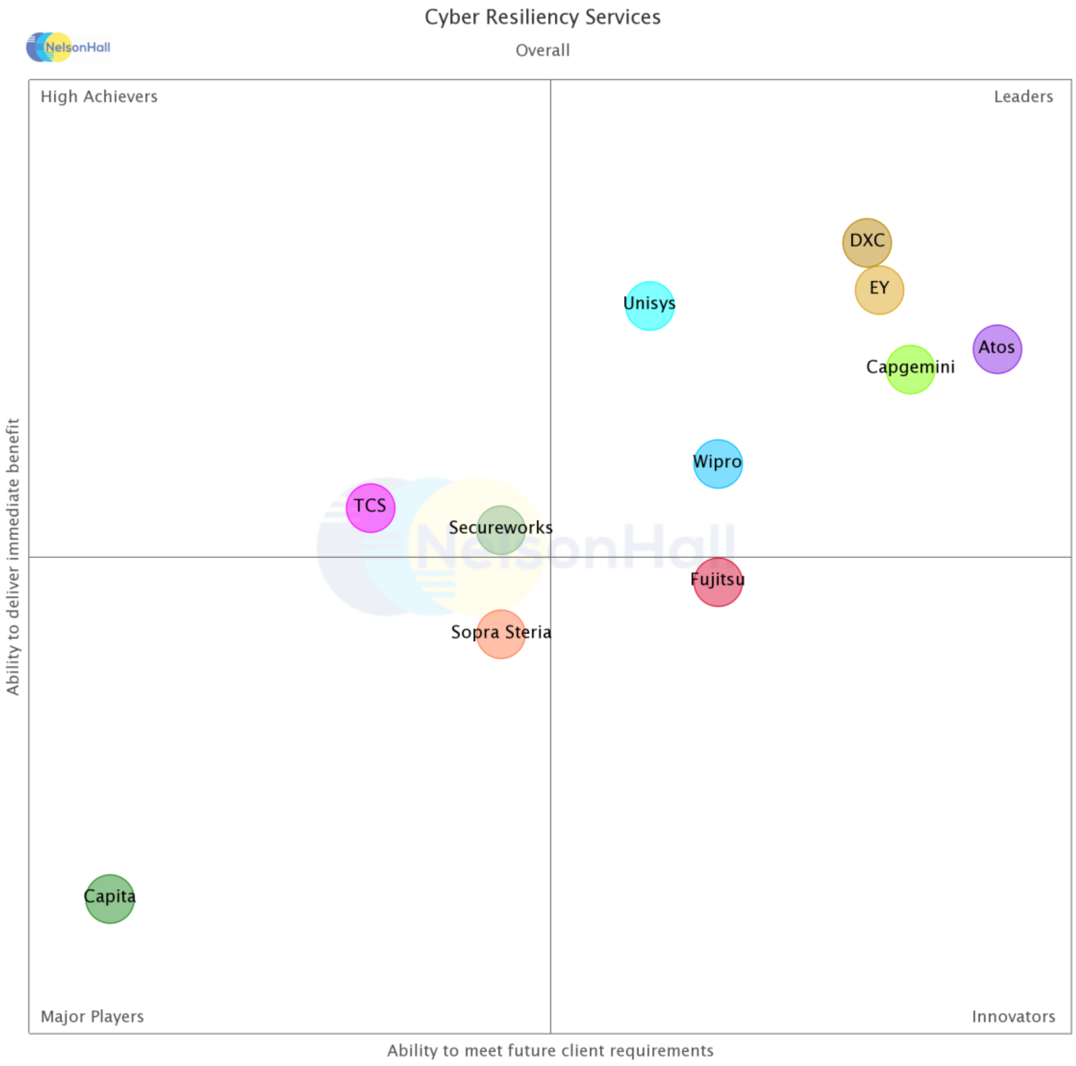
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors overall, and with specific capability in cyber resiliency program design, cyber incident response, and managed cyber resiliency 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, Capita, DXC Technology, EY, Fujitsu, Secureworks, Sopra Steria, TCS, Unisys, and Wipro.

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

NEAT Evaluation: Cyber Resiliency Services (Overall)



Source: NelsonHall 2021

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

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

Buy-side organizations can access the *Cyber Resiliency Services* NEAT tool (*Overall*) here.

Vendor Analysis Summary for Unisys

Overview

Unisys has a long history of cybersecurity and physical security services, particularly around identity management services for establishments such as airports and ports, and defense and intelligence agencies. Across its security offerings, Unisys is aiming to help clients in operationalizing security.

Unisys’ cyber resiliency services consist of:

- Cybersecurity Consulting
- Managed Security
- Unisys Stealth security software suite
- Zero Trust Network Access
- ICS Security
- Biometric Security.

In cybersecurity consulting, Unisys’ main differentiator is its TrustCheck service. TrustCheck assessment ingests security data and uses X-Analytics' software to analyze the client's cyber risk posture and how they associate with financial impacts. The report breaks down the possible scenarios that could affect the client with details on risk posture, threat likelihood, business impact, control effectiveness, cyber peril probability, impact, and expected loss. TrustCheck then measures the expected loss against Unisys' prioritized guidance to evaluate whether the value of securing the client's environment is greater than the cost to remediate a gap.

In managed security, Unisys’ i-SOC platform combines Endpoint Detect and Response (EDR), User and Entity Behavior Analytics (UEBA), and security incident response into a complete, end-to-end managed security service. In addition, Unisys integrates Stealth Core and Stealth ID into the i-SOC platform.

Stealth is Unisys’ micro-segmentation security software, which allows users to create identity-focused communities of interest. Users and devices outside of these communities of interest cannot intercept the network traffic or understand the data between community members. In this way, critical assets and data are hidden from adversaries.

Stealth ID creates contextual awareness within the SIEM which shortens time to identify real threats and creates operational efficiencies through a single dashboard. With Stealth Core integration into the i-SOC platform, Unisys can dynamically isolate nefarious activity, automatically or manually enabling breach containment while remaining resilient.

Unisys’ managed SIEM service leverages LogRhythm as its managed SIEM solution for on-premise requirements and Securonix for their SIEM as-a-Service, cloud-based offering. Unisys monitors a large number of events that are correlated down to ~630m security events per day.

Financials

Unisys' H1 2020 revenues were $954m, down 15.1%, excluding 2019 revenues from the federal business. By business unit:

- $822m was from Services, with cloud and IT infrastructure outsourcing accounting for ~$570m
- $131m was from Technology, of which Stealth security software was up 27%.

NelsonHall estimates Unisys' CY 2020 security services revenue split as:

- Technology-related revenue: $130m
- Security consulting: $145m
- Managed security services: $140m.

Strengths

- Rather than protecting against threats across a client's network, Unisys' Stealth offerings protect important data by effectively making it and its transfer undetectable; no other offering provides this level of obscuring network topology from potential attackers. The Stealth suite has been accredited by the NIAP and has been integrated into partner technologies that can more readily allow organizations to recover from ransomware
- Owing to the Stealth technology, investigations into cybersecurity events have a reduced time contingency
- Unisys has developed services and technologies to more readily relate cybersecurity to the C-level clearly and comprehensively through TrustCheck. Following these TrustCheck assessments, Unisys' scenario labs provide a realistic dollar amount of potential savings that can be realized from embedding security services and technology. As Unisys expands its partner programs, growth is less restricted than previously by its relatively low number of security analysts.

Challenges

- Unisys has chosen to be quite selective with its tool partners for its reference architecture; therefore, advanced security services are less likely to be served through lift and shift technologies
- Simulation labs are fairly custom, as the size of the simulation library is currently somewhat lacking. Unisys is investing in expanding these preconfigured labs to add industry-specific scenarios
- Little evidence of investment in improving staff knowledge into cybersecurity beyond the C-level with its TrustCheck services
- Managed services business has a lower level of language support and delivery capability outside of the U.S.

Strategic Direction

The major investment area for Unisys remains its Stealth portfolio. Recently, we have seen Unisys opening up sales channels for the Stealth product suite, first with its sale of the federal business to SAIC and the exclusive partnership there for Stealth to the federal sector, now with the launch of the global partner program, and a digital sales platform for Stealth.

The results of creating these channels are already starting to show, with Unisys reporting its first channel sales in Q2 2020, with one partner winning a multi-year contract with an IT services provider to provide Stealth to its customers. Likewise, the Dell Cyber Vault integration has had strong client interest following its launch in late 2019, especially within organizations that have been victims of ransomware attacks. In Q2 2020, the pipeline of the Stealth practice was up 20% sequentially.

Unisys will continue to expand this partner network and to integrate the Stealth product suite into more technologies.

Unisys will be making a substantial investment across its cyber resiliency services with increasing focus on DLP for endpoints, allowing the Stealth platform to more easily isolate an endpoint – for example, if it is sending sensitive IP over email, without requiring zero-trust network topology.

Outside of its Stealth suite, Unisys is increasing focus on moving services to the cloud, with SaaS solutions being spun up faster to support clients in the process of agile digital transformations.

In its TrustCheck service, Unisys is building out a library of industry-specific scenario labs. Unisys sees TrustCheck as its foot in the door in bringing cyber resiliency conversations into client boardrooms.

Outlook

Unisys' cyber resiliency services are built around its Stealth security suite, and in recent times, it has been creating new sales channels for this suite. As Unisys has never focused on building an expansive delivery capability for its managed security services, thanks to the Stealth suite's ability to reduce the number and severity of incidents by creating these new channels, Unisys will be able to continue to grow its security technology business.

Within the cybersecurity services business, Unisys continues to expand its consulting capability and shift focus into supporting cloud delivery, with traditional MSS and L1/L2 cybersecurity not being an area of focus.

Cyber Resiliency Services Market Summary

Overview

The current global cyber resiliency services market size is estimated by NelsonHall at ~$22bn and will grow to ~$47bn by 2025, a growth of 16.7% CAGR.

North America accounts for 43% of the cyber resiliency market, and is the most mature region for cyber resiliency in general. EMEA is the second largest region and accounts for 36% of the market and is the most mature region for compliance services.

Key vendors' growth strategies include shifting left from managed security services into a heavier consultancy mix of services, building SOAR and MDR capabilities, and expanding geographic presence in support of advanced security services and cyber consulting services.

Vendors are shifting left to reduce dependency on traditional managed security services which are increasingly using ML/AI to automate offerings which are becoming commoditized. These services are in turn becoming standardized as MDR to reduce the level of customization and vendor costs.

A large and ever-present requirement is for vendors to properly configure and patch existing insecure client architectures, and the fact that the cost of upgrading legacy systems to be secure is often higher than the ROI in the context of potential impact of a cyber incident has led to vendors creating platforms to measure the client risk appetite against potential costs to create an ROI.

Supporting cyber consulting services growth will be a continuation of digital transformation projects; for example, the adoption of technologies such as cloud and the adoption of cloud native security tools, IoT, blockchain, ML/AI, and (towards the end of the period) quantum security for critical infrastructure organizations.

Growth in managed security services will be lower than that of consulting and IR, as these segments will be receive a separate boost from the shift-left of cyber resiliency.

IR and backup services – backup is currently detached from cyber resiliency in many cases; growth supported by the shift-left of security and increasing data compliance requirements will ensure backup becomes more enshrined within cybersecurity rather than just being an infrastructure domain.

Buy-Side Dynamics

Drivers for clients in outsourcing cyber resiliency services are the inability for organizations to keep up with best practices and regulations, and cyber research to reduce the mean-time-to-detect and mean-time-to-respond while remaining cost competitive.

Key challenges for organizations looking to outsource cyber resiliency services include:

- An increasing number of regulations that carry the risk of fines
- Backups can be difficult to manage and are subject to regulations; for example, incorporating GDPR's right to be forgotten, and adding data storage costs
- Cyber resiliency awareness is low within organizations and remains one of the major areas of vulnerability. Data subjects not understanding how to spot an Indicator of Compromise (IoC) increases the dwell time of an incident and the MTTR

- Difficulty in keeping abreast of evolving best practices for next generation technologies such as cloud, IoT, RPA, blockchain, and quantum
- Organizations holding a large number of legacy applications which require heavy investment to patch to meet required standards. Organizations may find that patching these applications is uneconomical
- Increasing ease and sophistication of attacks. Attackers now have online stores in which they can purchase services to attack organizations. At the same time, more sophisticated attackers are leveraging AI/ML to perform attacks which are harder to defend against
- Data subjects becoming more aware of cyber resiliency and wanting their data to be properly secured, while organizations are looking to collect and store more client data
- While cybersecurity talent is becoming less of an issue among the vendors, at the client level, cybersecurity talent can be difficult to assess and retain
- A new wave of security tools and platforms leveraging AI needs to be understood if the organization wants to reduce the severity of incidents.

Success Factors

Critical success factors for vendors within the cyber resiliency services market are:

- Ability to work with partners, or for end-to-end providers to utilize other business units to introduce cyber resiliency upfront as a differentiator for clients
- Ability to work across the client’s business operations, IT, and third-parties
- Ability to build a cyber resiliency consulting capability, either with strong in-house training to leverage existing industry specific knowledge or through acquisitions
- Strong research capability to track cyber resiliency regulations and the impact of cyber digital technologies such as IoT, AI/ML, blockchain, and quantum. Whereas all vendors have this research to some degree, the more advanced technologies such as quantum and the development of quantum encryption are only covered by a small percentage of the vendors analysed
- Ability to build or assess the security IP and platforms for new resiliency services, for example SOAR platforms, platforms to assess the data security requirements of the client, native cloud security platforms, and platforms to assess third-party risk
- Maintaining the commoditized traditional security services while building advanced security services and maintaining margins through the use of automation
- Developing in-country capabilities to support security services such as advanced cyber forensic analysis
- Demonstrating ROI.

Outlook

Over the next few years:

- BCM plans will be built into cybersecurity as standard, in particular to prepare clients for SOAR. Additionally, vendors will build more suggested actions and SOAR will be built into security platforms
- Increasing range of consultancy services to design business continuity strategy services for IoT, quantum computing, blockchain, and securing the client from AI/ML
- Less checkbox exercises for cybersecurity awareness across the company. As of now, proper awareness training tends to be restricted to executives and roles such as F&A
- ML/AI will eliminate the need for L1/L2 services, and support the likes of PAM
- Services for more regulations which will most likely carry as heavy or heavier fines for loss of PII
- The use of AI to identify breaks in compliance
- MDR to be a more prevalent service with more clients opting for services that can resolve incidents more rapidly
- Backup services within infrastructure services to be more closely linked within vendors.

NEAT Methodology for Cyber Resiliency 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 capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements
- High Achievers: vendors that exhibit a high capability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet future client requirements
- Innovators: vendors that exhibit a high capability relative to their peers to meet future client 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.

Note that, to ensure maximum value to buy-side users (typically strategic sourcing managers), vendor participation in NelsonHall NEAT evaluations is free of charge and all key vendors are invited to participate at the outset of the project.

Exhibit 1

'Ability to deliver immediate benefit': Assessment criteria

Assessment Category	Assessment Criteria
Offerings	Simulation or espionage services Cyber resiliency strategy development Legal consultancy services for cybersecurity Penetration services Overall managed detection and response services Endpoint and edge security Digital Identities Security and data compliance Incident response management Backup and recovery services Level of automation/cognitive security capabilities
Delivery Capability	Cyber resiliency delivery capability – North America Cyber resiliency delivery capability – U.K. Cyber resiliency delivery capability – Continental Europe Cyber resiliency delivery capability – Rest of EMEA Cyber resiliency delivery capability – APAC Cyber resiliency delivery capability – LATAM Security IP including accelerators
Client Presence	Financial services security presence Healthcare security presence Government security presence Manufacturing security presence Retail security presence Telecoms and Media Energy & utilities security presence
Benefits Achieved	Cyber resiliency plans Design of minimal viable business operations Threat Detection time Response to cyber threats Value for money Threat avoidance Ability to remain in compliance with regulations Improved staff knowledge

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Level of Investments	Investment into cyber consultancy services Investment into managed detection and response services Investment into cognitive security Investment in geographic expansion
Service Culture	Strength of client partnerships

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:

Beth Lindquist at beth.lindquist@nelson-hall.com

Important Notice