IDC
ANALYZE THE FUTURE

Partner Transformation Guide: Security

Building a Successful Managed Security Services Organisation

May 2020

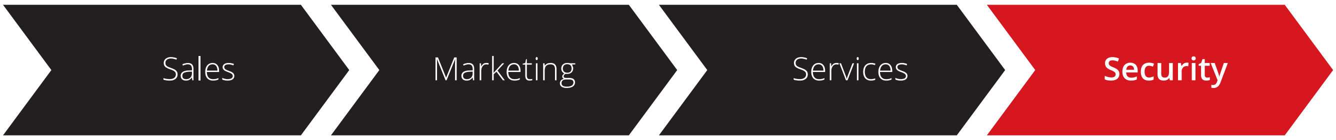
IDC EUR#146171320

An IDC eBook, sponsored by
TREND MICRO™

Authors:
Claudio Stahnke
Andreas Storz

Partner Transformation Guides

Successfully transforming your business to offer managed security services has important implications across several business dimensions. This series of guides describes these across Sales, Marketing, Services and Security, and provides advice on how to get started, grow and excel in managed security services as an IT partner.



Sales

Marketing

Services

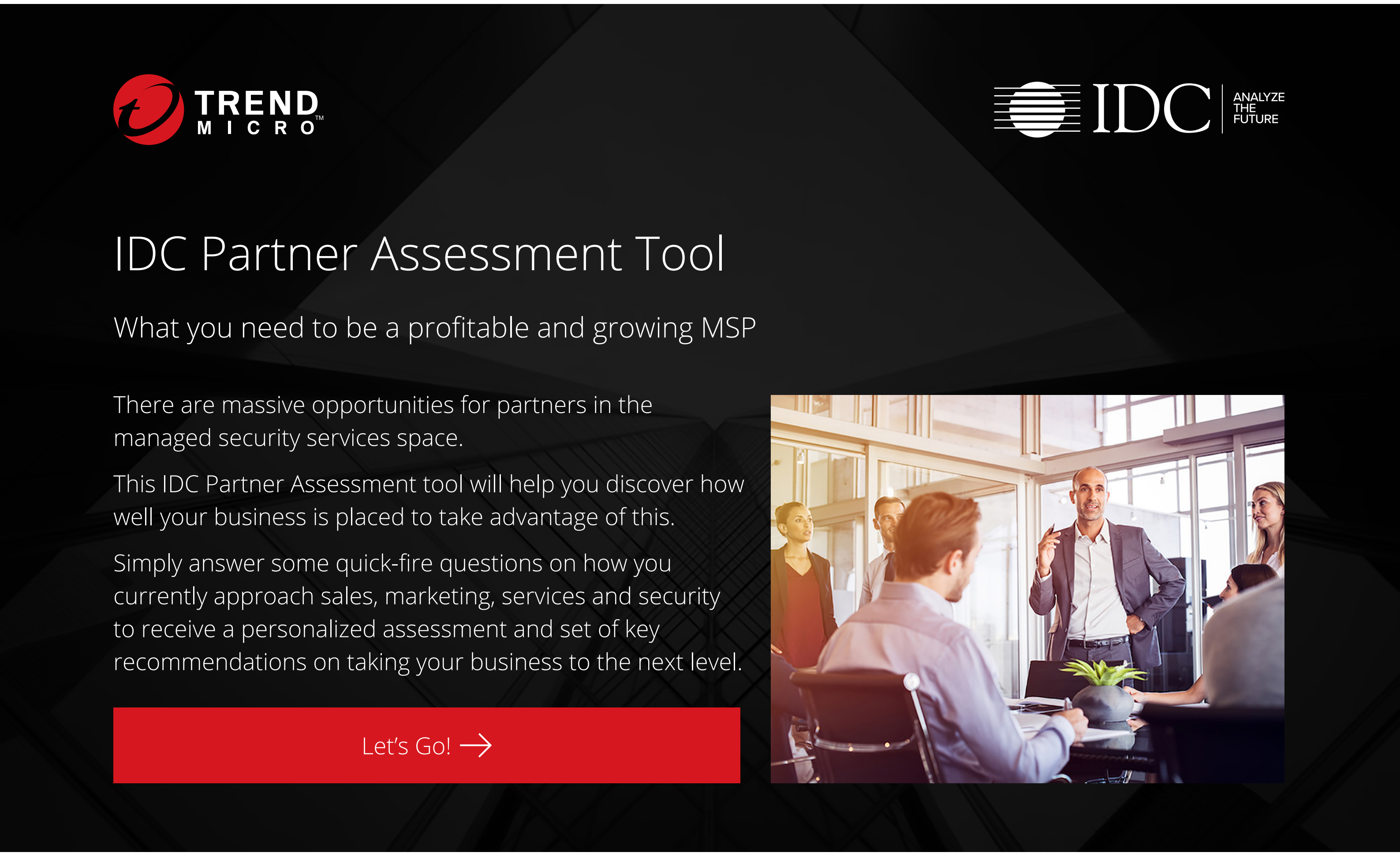
Security

The intended audience for these guides are senior leaders, marketing executives and business owners of channel and partner organisations.

Executive Summary

Channel partners can tap into a growing market opportunity for managed security services. IDC has developed a **Partner Assessment Tool** to help partners better understand how well their business is placed to take advantage of the managed **security services opportunity** in this high-growth market. This assessment tool guides partners to progress from early to advanced stages of maturity across sales, services, marketing and security capabilities.

IDC Partner Assessment tool



IDC Partner Assessment Tool

What you need to be a profitable and growing MSP

There are massive opportunities for partners in the managed security services space.

This IDC Partner Assessment tool will help you discover how well your business is placed to take advantage of this.

Simply answer some quick-fire questions on how you currently approach sales, marketing, services and security to receive a personalized assessment and set of key recommendations on taking your business to the next level.

Let's Go! →

IDC has also developed this series of Partner Transformation Guides to provide deeper insight into how partners need to transform to successfully run a managed security services business.

This edition describes the implications of offering managed security services on your **approach to security services**. In particular, it focuses on the impact of realigning a partner marketing organisation to the market realities of the recurring revenue model found in managed and cloud services.

The Market Opportunity for Managed Security Services

Managed security services is the fastest growing security services segment. IDC's Western Europe Security Services Forecast estimates the compound annual growth rate (CAGR) for managed security services at 14.1% in 2016–2021, far outpacing other security services. This growth is being driven by four key market dynamics:

Digital Transformation (DX)

European organisations are investing heavily in new technologies — especially cloud — to support their DX projects. They expect better performance from their IT and digital business innovation to remain competitive and be able to deliver new products, services and experiences to their customers. IT spending is undergoing a massive shift toward cloud and cloud-based solutions as well as emerging technologies such as Artificial Intelligence and the Internet of Things. These technologies promise better performance and greater agility, and as such they are the enablers of digital business innovation.

European spending on technologies and services that enable the **digital transformation** of business practices, products and organisations is forecast to reach

$378.2

billion in 2022

Source: Worldwide Semi-annual Digital Transformation Spending Guide

As European organizations struggle to hire IT security specialists to manage their environments, IDC predicts that, by 2021, MSS will grow 12% reaching

€8

billion in Europe alone

IDC European Security Services Forecast, 2019-2023 (IDC #EUR145782919, March 2020)

Increased Complexity

While investments in new technologies drive digital innovation and allow organisations to improve their competitive position, their successful deployment and integration also require organisations to manage much greater complexity. Increasingly, organisations will operate hybrid IT and multicloud environments. They leverage emerging technologies to gain business value from growing amounts of data. A necessarily more complex IT estate makes organisations subject to new vulnerabilities. As a result, organisations face a changing and increased threat potential.

Prioritising Security Investments

Security is a key business priority for European organisations as part of their DX initiatives. Increased threats and complexity therefore drive major security investment as DX forces customers to rethink their security strategies. Along with technology, security requirements are equally becoming more complex and solutions have to evolve accordingly. The top security concerns for organisations include data breaches, malware, denial-of-service attacks, and insecure interfaces and application programming interfaces (APIs). Organisations seek comprehensive solutions that help them mitigate threats and prevent business disruption and reputational damage.

Cybersecurity/data security expertise is the most sought-after skill in Europe according to IDC's Technology Skills Survey

Source: IDC's Technology Skills Survey, December 2018 (European responses)

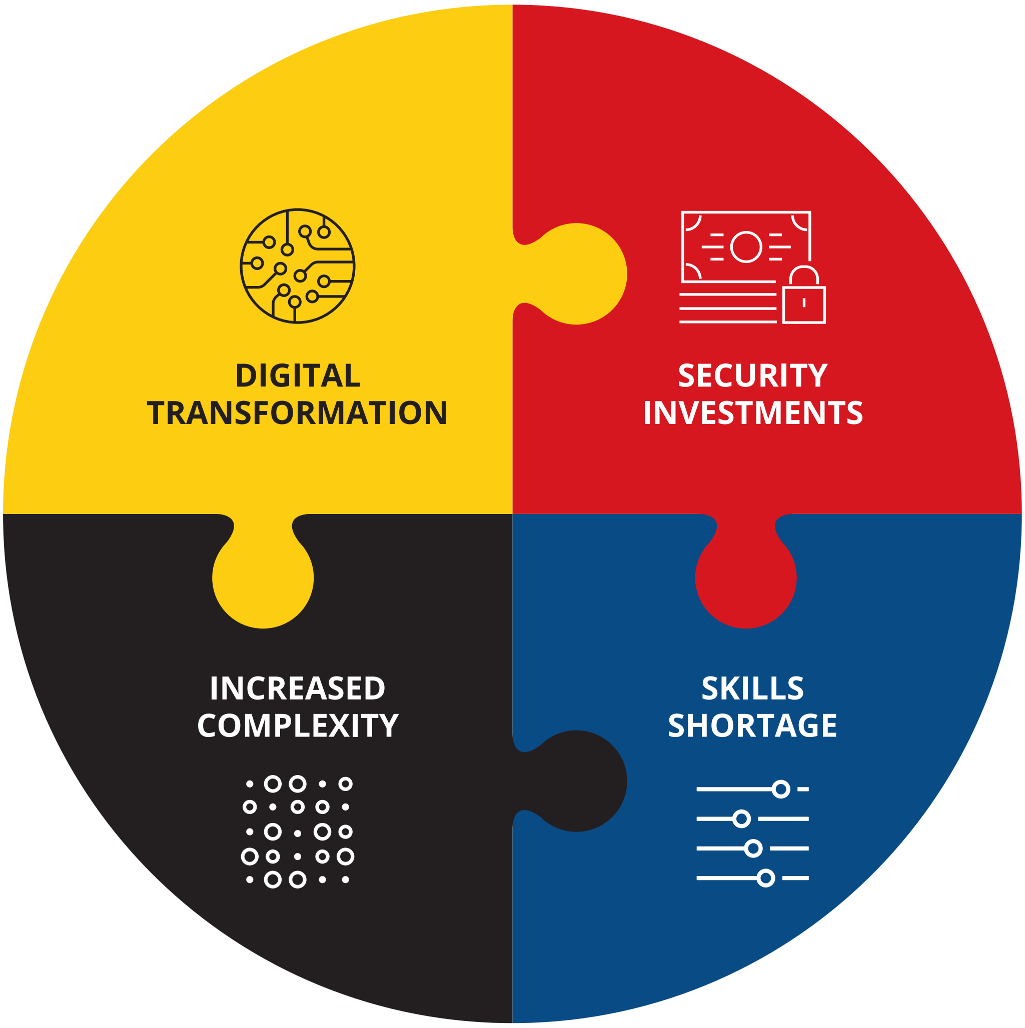
Skills Shortage

Successfully implementing DX initiatives requires organisations to manage increased complexity, but they are struggling to hire specialists with the right skills. This is particularly acute in the case of security skills, which are in high demand, but short supply. The changing nature of security operations, regulatory upheaval and a dynamic threat landscape add to this burden.

The Market Opportunity for Managed Security Services (Cont.)

The Channel Opportunity

These trends reinforce each other and create a **large market opportunity for businesses like yours** as organisations seek support from specialist partners. They will increasingly consider third-party security services providers to either augment their in-house capabilities or fully outsource the management of their IT security function. As a result, there is an opportunity to differentiate against competitors and open new revenue streams by building a practice to offer **managed security services**.



Executive Summary

- In the next section we will look at how an aspiring MSSP can start its journey and differentiate itself in an increasingly crowded market.
- We will start with a list of elements that MSSPs need to keep in mind to create a suitable portfolio and then offer value to their end users.
- We will address the opportunity and challenge represented by the skills shortage, highlighting steps that can be taken to acquire and retain the talent needed to create a sustainable business.
- No one is alone in their journey to become an MSSP. The ecosystem formed by vendors, distributors and local partners can make things much easier than expected if someone knows how to leverage these external resources.
- Finally, we have included a set of short-, medium-, and long-term recommendations for you to follow step by step to evolve from a secure provider to a fully fledged MSSP.

Strategies: How to Differentiate for MSSPs

Depth of advanced capabilities

Breadth of portfolio is not everything; MSSPs should look into specialising based on the profile of the client base they want to focus on.

Innovation and R&D

MSSPs should continuously invest in emerging technologies in order to harness their potential, increasing the value of their proposition.

Automation and orchestration

The ability to automate security tasks and orchestrate security processes is a source of added value for MSS customers.

Broader portfolio

Providing an end-to-end solutions portfolio will help MSSPs to position themselves to end users as a one-stop shop.

MSS portal

This is key to the ability of in-house security professionals to work in step with their MSSPs.

Relationship management

Creating a strong partnership with clients will be a strong differentiator for those MSSPs that struggle to gain scale with their offering.

Vertical expertise

As cybersecurity is increasingly seen as a business enabler, end users expect their security providers to develop expertise in specific verticals.

Creating a Portfolio

The NIST Cybersecurity Framework (CSF) is becoming the de facto standard control framework for large enterprises. It provides a taxonomy of controls to ensure that a cybersecurity program is comprehensive.

The NIST CSF is a taxonomy of 5 functions with 23 categories and 108 sub-categories that express security control outcomes that are important to an enterprise security program.

It provides a useful guideline for aspiring MSSPs as developing services and products that align with the 5 functions will in turn align with your end customers' cybersecurity journey.

NIST Framework

When developing their offering, MSSPs should follow the NIST framework and its core set of functions

Identify

Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.

Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover

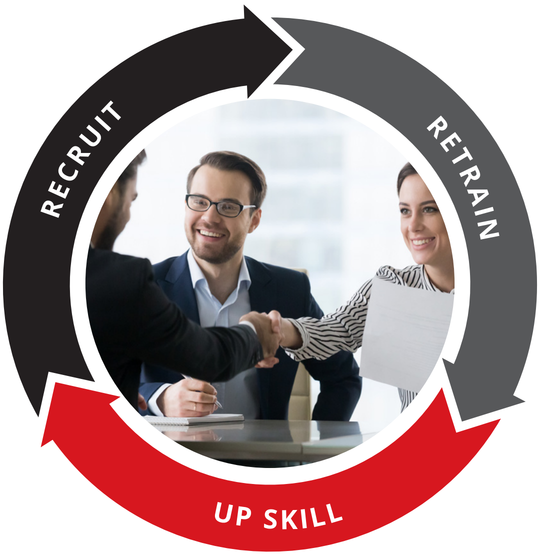
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

National Institute of Standards and Technology (NIST)

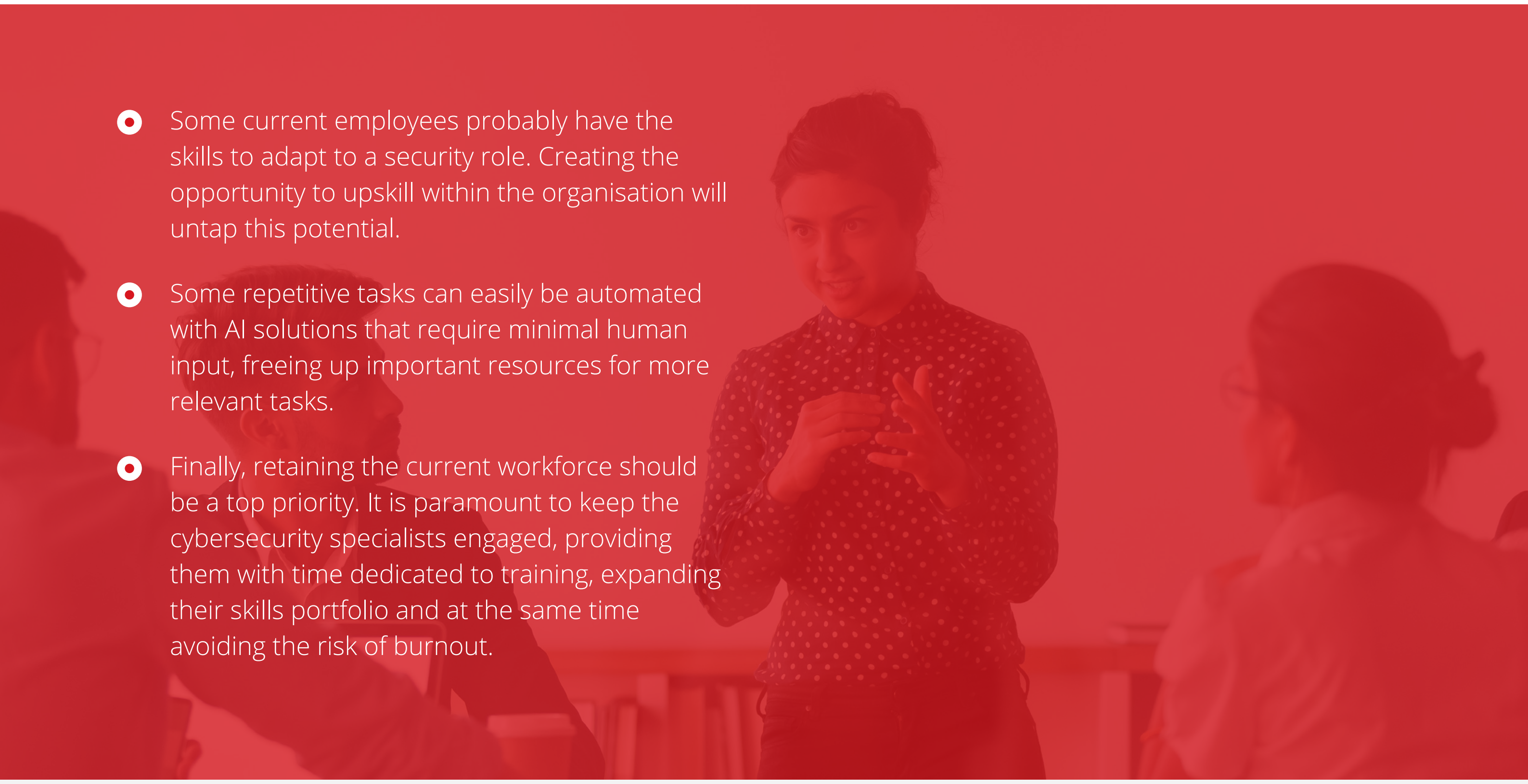
Security Skills

As the industry endures a cybersecurity skills shortage that can only worsen, the requirement for MSS will inevitably increase. But service providers themselves are struggling to find the required talents to meet the growing demand. The following recommendations aim to address this.

- Recruiting processes need to be optimised. The HR department needs to work closely with security specialists to create an enticing description for each role so that job descriptions do not become a box-ticking exercise.
- Grassroot initiatives, though they take longer to bear fruit, are a long-term solution that can promise a constant stream of resources in return for the investment. These can span from creating ad hoc academic paths with local institutions (e.g., Novosco with Belfast University) to recruiting profiles with a set of soft skills easily transferrable to cybersecurity (e.g., Amazon and Fortinet recruiting army veterans).
- Often firms accept only candidates with prior experience. This further restricts the number of suitable applicants and makes the hiring process slower and more costly. Accepting entry-level candidates and training them on the job will help to expand the reach.



- Especially at the early stages of creating a team of cybersecurity experts, investing in contractors is a quick and efficient way to hit the ground running, although this should not be considered a long term solution. Invest in contractors to plug holes while finding more permanent manpower.



- Some current employees probably have the skills to adapt to a security role. Creating the opportunity to upskill within the organisation will untap this potential.
- Some repetitive tasks can easily be automated with AI solutions that require minimal human input, freeing up important resources for more relevant tasks.
- Finally, retaining the current workforce should be a top priority. It is paramount to keep the cybersecurity specialists engaged, providing them with time dedicated to training, expanding their skills portfolio and at the same time avoiding the risk of burnout.

The following matrix provides guidance on how organisations can start to balance between short- and long-term initiatives to simultaneously address the immediate skills gaps, while investing in longer term sustainable solutions.

The matrix provides four key considerations:

1 Ease of execution

2 Time to realisation

3 Long-term solution or not

4 Cost

● Excellent ◕ Strong ◑ Good ◔ Poor ○ Very poor

	EASE OF EXECUTION	TIME TO REALISATION	LONG-TERM SOLUTION	COST
Hire contractors	●	●	⊗	◔
Grassroot initiatives	◔	○	✓	○
Upskill employees	◑	◔	✓	◑
Train graduates	◑	◔	✓	◔
Automate tasks with AI	◑	◕	✓	◔
Retain current employees	◔	N/A	✓	◑

Leveraging your partner ecosystem can be one of the most effective ways to address the skills shortage, while adding more capacity, capability, and the scale of your security operations.

Leveraging the Ecosystems

The journey to become a fully fledged MSSP can appear complex and resource-draining. But thanks to rapid growth in demand, many established vendors and distributors are investing in partnerships with aspiring service providers. The path to become an MSSP can be easier than expected, if someone knows where to look!

At the beginning of their journey, aspiring MSSPs should leverage the offerings of more mature providers of security services, especially when it comes to more complex offerings like SOC and MDR.

The European market is highly fragmented, and SMEs especially prefer to deal with local players that speak their language and understand local dynamics. **Partnering with national players** before establishing a presence in a new geography will be paramount to create a solid foothold.

Distributors

operate as a middleman between vendors and 2-tier channel partners, streamlining the vast and diverse offerings of security products and providing training and certifications, especially in countries where vendors do not have a direct presence.

Vendors

play a key role in the development of an MSSP, with many offering specific partner programs that include step by step phases. MSSPs should focus on a carefully selected number of vendors, building their portfolio of services upon a standardised technology stack.

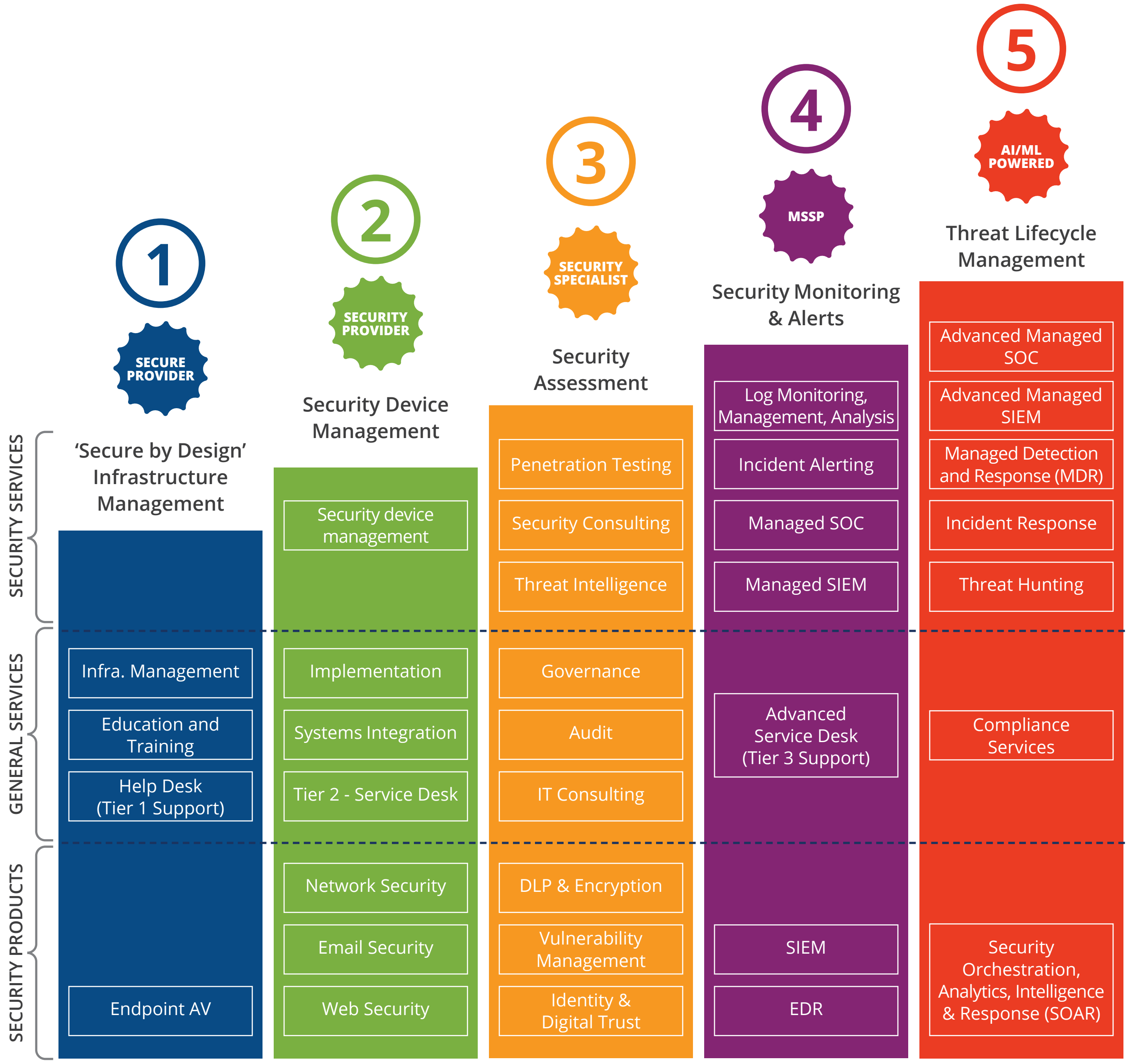
SOC = Security Operations Centres from which MSSPs deliver remote management or monitoring of IT security functions

MDR = IDC defines MDR as a combination of a number of technologies that provide continuous and proactive security and threat monitoring, detection, incident analysis and response services that correlates and collects client environment–specific threat intelligence and telemetry.

A Road Map to Security Services

The journey from SP to MSSP can be taken in incremental steps. Education and training services are an easy and cost-effective way to get started. As you progress, think about adding more advanced services and support, such as security consulting, managed SOC and AI capabilities.

IDC has mapped out the different security services and technologies to the different levels of MSSP maturity. This allows partners of any size to quickly identify where you are on your MSSP journey, from both a services and technology perspective, as well as which solutions you may consider adding into your offering to enhance your MSSP business further.



	1 SECURE PROVIDER 'Secure by Design' Infrastructure Management	2 SECURITY PROVIDER Security Device Management	3 SECURITY SPECIALIST Security Assessment	4 MSSP Security Monitoring & Alerts	5 AI/ML POWERED Threat Lifecycle Management
SECURITY SERVICES		Security device management	Penetration Testing Security Consulting Threat Intelligence	Log Monitoring, Management, Analysis Incident Alerting Managed SOC Managed SIEM	Advanced Managed SOC Advanced Managed SIEM Managed Detection and Response (MDR) Incident Response Threat Hunting
GENERAL SERVICES	Infra. Management Education and Training Help Desk (Tier 1 Support)	Implementation Systems Integration Tier 2 - Service Desk	Governance Audit IT Consulting	Advanced Service Desk (Tier 3 Support)	Compliance Services
SECURITY PRODUCTS	Endpoint AV	Network Security Email Security Web Security	DLP & Encryption Vulnerability Management Identity & Digital Trust	SIEM EDR	Security Orchestration, Analytics, Intelligence & Response (SOAR)

Partner maturity level, investment and business evolution

Getting Started as a Secure Provider

Priorities to grow your managed security services business and accelerate your transformation include:

Build up cybersecurity skills

This can be challenging in the current market, but there are solutions that will provide the necessary skills in the short and long term (e.g., contractors, upskilling current employees).

Products and services

At this stage offerings should include infrastructure management, education and training, help desk (Tier 1 support), endpoint AV, secure device management, patch management and system integration.

Choose the right vendors

This is true for both products and support offered.

- When it comes to portfolio priorities, MSSPs can either go for better integration of the different tools or for best in class solutions, but it will be difficult to get both because of the highly fragmented nature of the market.
- Different vendors have different approaches when it comes to partners and especially MSSPs. They can provide different levels of support and have different route to market strategies (e.g., vendors that provide their services directly might end up in conflict with their partners).

Start defining a client base

Not all the current clients will be suitable buyers of managed security offerings. Careful consideration has to be made before starting to upsell and target new clients. Priority should be given to those clients with which there is a stronger relationship, building up trust.

Keep it direct and personal

Building tight relationships with clients at this stage is the best strategy to level the field against bigger and better established MSSPs as these cannot closely follow all their clients, especially SMEs. This will allow the security provider to build customised and targeted solutions with the added positive effect of specialising on a lower set of features, keeping costs down.

Pursuing Growth, Becoming a Security Specialist

Priorities to grow your managed security services business and accelerate your transformation include:

Align with sales

Align dedicated marketing teams with sales so that together they can track the customer journey. The combined marketing and sales function should begin developing messaging around business outcomes with a highly aligned approach.

Improve efficiencies

As they expand their portfolio of offerings, security specialists need to keep an eye on the efficiency of their service delivery. Starting to automate processes, as well as orchestration among solutions, will make scaling up easier, as new deployments consume fewer resources. More efficient operations can also reduce time to market because adding new services does not necessarily require the service provider to add staff with specific skills and expertise.

Add value proposition

In addition to providing a wider range of technology-focused services, security specialists should expand their offering with consulting services, such as penetration testing, digital forensics and risk monitoring. These types of value-added services must be built on a solid foundation of effective and efficient security technologies, both to ensure the accuracy of information being analysed and to minimise the staff time consumed by rote security tasks.

Products and services

At this stage the offering should include penetration testing, security consulting, service desk (Tier 2 support), threat intelligence, DLP & encryption, vulnerability management, identity and digital trust

Reaching Maturity as an MSSP

As you expand and optimise your managed security services business, your marketing strategy should continue to evolve to ensure success and profitability by focusing on the following:

Iterate and improve

Your dedicated marketing team should have a continuous improvement mindset and be looking to analyse and measure the success of modern marketing campaigns on an ongoing basis.

Multitier offering

The augmented sophistication of the offering now allows the MSSP to divide its offering into different tiers, with those that consume more resources (e.g., dedicated SOC analysts) reserved for premium clients.

Specialise and target verticals

As the security portfolio and consulting services mature, it is important for an MSSP to build up expertise in specific verticals to position itself as a partner that fully understands the business outcomes and the best technologies to be implemented by its end users.

Automation potential

AI-driven security tools at this stage are vital, especially to automate time-consuming and repetitive tasks and to operate a filter against the sheer amount of alerts generated by the different security tools. This will greatly increase efficiencies, allowing security analysts to dedicate themselves to better supporting the end user and at the same time reducing the risk of burnout.

Streamline vendors

As the services portfolio broadens, vendor selection becomes increasingly important as managing relationships with tens of different vendors can be cumbersome for security staff. Moreover, the more point products there are in an infrastructure, the less likely they will be to share information about threat detection and mitigation efforts in a timely manner, impacting both security and profitability.

Products and services

At this stage the offering should include: log monitoring/management/analysis, incident alerting and response, 24x7 managed SOC, managed SIEM, MDR, SOAR, threat hunting and advanced service desk (Tier 3 support).

Learn More

Partner assessment tool: *Take the assessment test* →

IDC InfoBrief: *How partners can seize the managed security services market opportunity in Europe* →

Partner Transformation Guides →

Get in touch with Trend Micro →

IDC
ANALYZE THE FUTURE

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Global Headquarters:

5 Speen Street Framingham, MA 01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com