ovum.informa.com

Ovum
TMT intelligence | informa

2018

Trends to Watch: Managed Security Services

Providers invest in automation, tools, and skills as enterprises struggle with new regulations

Summary

Catalyst

Managed security services no longer solely focus on monitoring network or IT assets. Their coverage extends into systems, software, and data, wherever they reside – on customer premises, in the network, in the data center, and in the cloud. Managed security services providers (MSSPs) need to evolve rapidly to meet the needs of enterprise clients within these diverse environments. Customers are inundated with data as they digitize more and more of their processes and operations. Legislation, reputational damage, and the need to respond quickly and effectively to incidents means that managed security is extending beyond monitoring and incident detection to automated incident response. Timescales for detection and response are shrinking, while data volumes are growing exponentially as digitization touches every aspect of enterprise IT.

Ovum view

Ovum has noticed a significant increase in the number of service providers adding managed security to their service portfolios in past 24 to 48 months, along with new MSSPs entering the market. As the volume of incidents and breaches has increased globally, telcos and SIs have responded to the opportunity to sell managed security services, not only as an upsell or as part of a core service to existing customers, but as part of a discrete portfolio of services that covers everything from identity and access management to advanced threat intelligence and managed incident response.

In addition, many new MSSPs are offering a plethora of point or converged solutions to address enterprise security requirements. The delivery of managed security services from the cloud and for the cloud environment is adding new players and categories of managed security providers, while expanding the need for existing providers to partner with niche technology providers and to integrate new services into their existing service portfolios.

Key messages

- Enterprises will continue to build defenses to protect their data, IP, and reputations and to be compliant with stricter regulation. Many will require additional external support to keep up.
- Managed security will become a mainstream service in service providers' portfolios, while also supporting many niche MSSPs.
- Automation will come to security in many flavors but is just one of the new technology ingredients that will improve managed security services outcomes.
- MSSPs must move to Agile development and quicken the pace of new service development and lifecycle management to keep up with the threats and increasing technological and operational sophistication of their adversaries.

Recommendations

Recommendations for service/ content providers

As security tools have grown in sophistication – from monitoring to consolidating log data to employing sophisticated analytics to identify anomalous activity and behavior, for example – the nature of managed security services and the skills required to use the tools effectively have changed. The sheer number of tools and specialist skills required to integrate them into a coherent security architecture is proving a challenge to many enterprises and public sector organizations. This is an opportunity for service providers to offer strategic services that alleviate enterprise pain points in sourcing the skills and services they need to continually maintain and enhance their security posture and responsiveness. MSSPs must also develop new services while continually improving their existing portfolios to stay ahead of the security threats and to stay ahead of some of the newer, nimbler players in the market.

Recommendations for security technology vendors

If security information and event management (SIEM) tools are designed to provide a base level of analysis and filtering of consolidated log data, the next focus of attention for MSSPs will be advanced analytics "above" the SIEM. Vendors should consider adding tools that either complement or replace the SIEM with services that use higher-performing and more customizable data analytics, search, and indexing tools. They must also offer better pricing models that allow MSSPs to compete and provide services that offer value over and above that which customers deploying tools on their own could achieve. MSSPs need tools that monitor and index data in real time from wider sources than log data, highlight unusual activity graphically, and automate standard security hygiene processes. Security professionals now need tools that deliver increasingly granular analysis of user and device behavior or deep network traffic analysis in real time.

The impact of legislation, "as-a-service," and "human + machine" capabilities on MSS

Regulatory compliance will hasten enterprise security investments

The introduction of cybersecurity and data protection legislation in Asia and Europe in the next 18 to 24 months will accelerate the demand for managed security services in both regions and beyond. For example, the Singapore government in July 2017 released a draft cybersecurity bill for public consultation that ended recently. The bill proposes handing broad authority to the Cyber Security Agency (CSA) to coordinate efforts and designate owners of critical information infrastructure (CII). It formalizes the duties of CII owners in ensuring their own cybersecurity well-being, including the need to conduct regular compliance audits and make regular assessments of their vulnerability to cyberthreats. Failure to comply will be a criminal offense carrying a maximum fine of $100,000 or a 10-year prison term, or both. The bill focuses on CII owners, but its impact is much broader because many organizations either have business ties with CII owners or are CII owners. The bill shows that Singapore, like many other countries and federal states around the globe, is taking a holistic approach to cyberthreats to CII. Japan, the Philippines, and the European Union (EU) have similarly either drafted or passed laws covering data privacy and accountability, making it even more critical for enterprises to comply with legislation and improve their ability to deal with cyber-attacks.

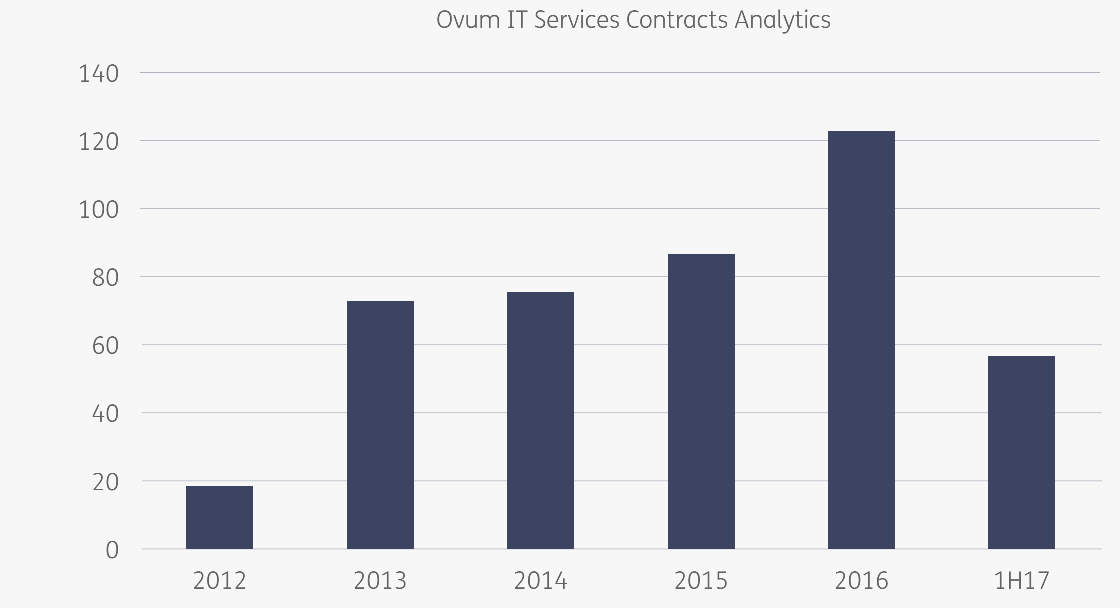
The EU's General Data Protection Regulation (GDPR) threatens stiff penalties for failure to comply with its regulations, specifically those concerning data breaches. According to the regulations, which businesses and public sector organizations have to comply with by May 2018, an organization's data controller must notify the supervisory authorities of a personal data breach (i.e., a breach of any private individual's data held by the organization) no later than 72 hours after becoming aware of such breaches. While there are some mitigating circumstances for failure or delay in reporting the breach, in general failure to do so risks incurring a fine of up to €20m ($24m) or 4% of the company's global annual turnover of the previous financial year, whichever is higher.

A UK government survey published in August 2017 indicated that only 6% of the top FTSE 350 publicly listed companies considered themselves already compliant with the regulations. That suggests that demand among European organizations for GDPR risk and compliance assessments, and subsequent managed security engagements as organizations look to third parties to help them achieve and maintain compliance, will be strong. The imposition of the 72-hour breach notification period not only puts pressure on organizations to ensure that they have appropriate incident response procedures in place, but also that those incident response procedures can quickly mitigate attacks in order to minimize reputational damage subsequent to the organization making the data breach known to the authorities and its customers.

These legislative developments create opportunities for MSSPs to provide data protection and incident response services to ensure that customers are both compliant with the new regulation and able to minimize the impact of attacks. Ovum expects assessment, professional services, and consulting engagements to lead to integration and managed services opportunities as customers look to service providers to make them compliant and ensure that they stay compliant. MSSPs will also need to focus on delivering agreements based on business objectives, versus mere reporting of alerts. That is, it is no longer enough to alert customers to a breach; MSSPs must also help them remediate and recover from that breach.

Ovum has already noted an increase in the volume of comprehensive cybersecurity contracts, combined network/cybersecurity, and combined application or infrastructure management/cybersecurity contracts (Figure 1). We expect a further boost to sales of managed security services in 2017/18, driven by new regulations from both government and industry regulatory organizations.

Figure 1: Volume of cybersecurity contracts recorded in Ovum IT Services Contracts Analytics, 2012–1H17



Source: Ovum

Managed security services enter the mainstream as enterprises face new challenges

In the past three to four years, Ovum has noticed a significant increase in the number of managed service providers adding managed security services to their portfolios. As the volume of incidents and breaches has increased globally, telcos and systems integrators (SIs) have responded to the opportunity to sell managed security services, not only as an upsell to network services or as part of a comprehensive IT outsourcing deal, but as a discrete standalone service line. IT and network service providers have created security services portfolios that cover everything from identity and access management to advanced threat intelligence and managed incident response. Managed security services are no longer solely focused on monitoring the network, but extend into systems, software, and data, wherever they reside – in the network, on customer premises, in the data center, and in the cloud.

Most specialist and telco MSSPs now offer a range of discrete managed security services that extends up the IT security stack from network monitoring to managed security information and event management. The latter may be delivered as a managed service, optimizing and maintaining the customer's on-premises SIEM software, hosted in the service provider's security operations centers (SOCs) or increasingly delivered as-a-service (SIEMaaS). The reason MSSPs have almost universally decided to offer managed SIEM is that it is a complicated, expensive piece of software that is often difficult to configure and optimize. A recent Ovum survey (Figure 2) indicates that around a third of organizations that have deployed a SIEM are confident that they are making the most of their investments, while 40% of respondents were either reviewing their SIEM investments or felt that they had not maximized the return on their SIEM investments. This clearly leaves room for MSSPs to help enhance or replace what customers are doing on their own.

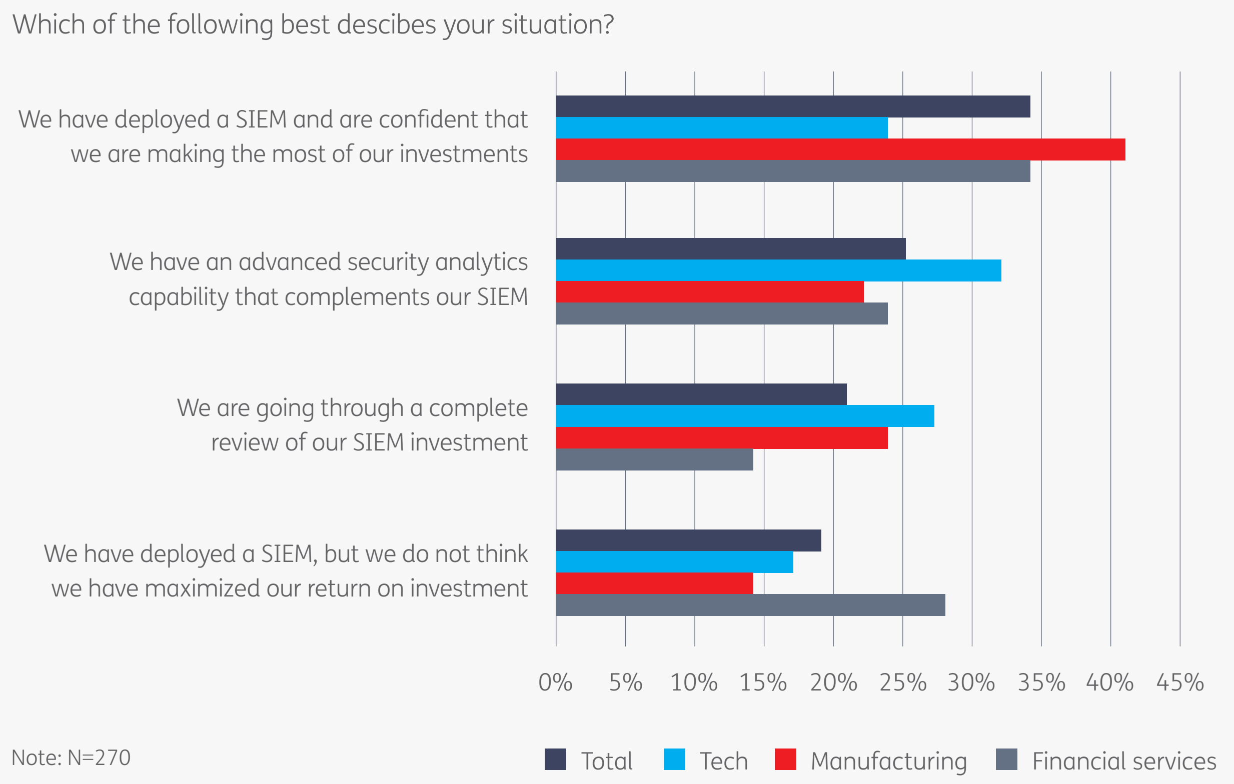
"Security-as-a-service" goes beyond the proof-of-concept phase

Security-as-a-service is a significant trend, and virtually every major ICT security services vendor has introduced cloud-based services to their portfolios.

Enterprise cyber technology vendors such as IBM and cyber specialists such as SecureWorks have long delivered services in the form of managed software-as-a-service (SaaS), but SIs and telco MSSPs are starting to offer more in the way of managed SaaS.

With cloud and virtualization technology now mature, many enterprises prefer to buy expensive cybersecurity software on-demand as SaaS rather than as an expensive item of licensed software. Consequently, MSSPs are also increasingly using the cloud to deliver common widely used security services such as identity and access management, intrusion detection, and SIEMaaS, but with an overlay of managed services. Although this service model may not address all security solutions, it can replace many legacy services or enhance security solutions that the customer already has in place. It has all the advantages of SaaS in that the MSSP maintains and updates the software, deploying the latest versions of the tools with the most up-to-date functionality.

Figure 2: Customer satisfaction with SIEM investments – financial services, manufacturing, and technology sectors



Note: N=270

Source: Ovum

The most advanced MSSPs are expanding their cloud-based managed SaaS offerings into the equivalent of a security operations center in the cloud (SOCaaS). Ovum believes that such security-as-a-service solutions will be very attractive to midmarket and small- and medium-enterprise (SME) customers that do not have the skills or finances to invest in their own bespoke on-premises SOCs but want to implement SIEMs or other more advanced analytics tools. This is an opportunity for MSSPs to serve a larger segment of the enterprise market.

In addition, a new generation of real-time data analytics tools has superseded traditional SIEMs that simply gather, consolidate, and correlate log data. Many enterprises are avoiding paying for costly SIEM platforms and data storage (a hidden cost in cloud-based deployments), progressing from traditional proprietary solutions, such as QRadar and ArcSight, to deploying data analytics and indexing tools such as Splunk, which offer real-time indexing and monitoring of any machine data and network traffic. Early adopters of SIEMs and their MSSPs now realize the need for new platforms that underpin MSS and go beyond what a traditional SIEM can offer. Hence the drive to place more emphasis on outcome-based security solutions and cloud-based hosted data analytics platforms. Ovum expects that customers will move on from complaining about their SIEMs (aka "SIEM fatigue") and start to move to new options that either overlay or replace SIEMs.

Ovum anticipates that the next focus of attention for enterprises and MSSPs is advanced analytics "above" the SIEM. A growing number of emerging security analytics specialists, such as Cylance and Darktrace, have developed technology (typically delivered as-a-service) that either complements or replaces existing SIEM or endpoint technology with higher-performing and more customizable data analytics, search, and indexing tools. These tools monitor and index data from much wider sources of data in real time, highlighting unusual activity graphically and launching automated responses and blocking technologies against the anomalies they identify. The customer's security professionals can drill down into correlated, intelligently filtered data (versus raw data), or the MSSP can investigate as part of a managed service. MSSPs are starting to develop new services based on these tools, as well as using data analytics tools and expertise to deliver increasingly granular analysis of user and device behavior or deep network traffic analysis in real time. However, the data scientists and data analytics skills needed to get the most out of these tools are often in short supply, which presents further opportunities for MSSPs that do have such skills to architect the solutions, select the tools and services, create the data lakes, and enhance the algorithms to ensure that customers get the most out of their investments.

Deployment and configuration of the tools, indexing and optimizing data, and developing and "training" machine learning algorithms generally require data science skills rather than pure security operations skills. Sourcing such skills among security operations professionals is often hard for enterprises – sometimes it's hard for service providers too, unless they acquire a company working in that space – but that is what makes it an attractive opportunity for service providers. Machine learning training may also require access to very-high-bandwidth systems, networks, and ultra-high-performance computing power owing to the volume of data involved. Access to such technology can be disproportionately expensive even with the advent of such technology in the cloud. Managed services offer enterprises the opportunity to share these costs and benefit from economies of scale, as well as delivering the necessary skills to benefit from them.

As SIs and telcos increasingly focus on cybersecurity as a key pillar in their go-to-market strategies, Ovum expects full-scope cybersecurity contracts to become increasingly popular, whether they are in the form of outsourced security operations centers transferred to the management of the service provider, new "design/build/run" SOC integration projects, remote security operations management hosted in the service provider's SOCs, or evolving "SOCaaS" – essentially, common, off-the-shelf cybersecurity services delivered from the cloud, but in an integrated offer designed for common use cases.

Automation will come to managed security in many flavors

The application of machine learning (ML) and the use of data analytics techniques to identify anomalies are part of a major trend in cybersecurity operations. Automation includes the use of not one but multiple technologies, such as artificial intelligence (AI), ML, deep learning, and various branches of data analytics, including behavioral analytics. MSSPs will continue to integrate these technologies into their SOCs to help correlate data, incidents, and behavior to help isolate and remediate security incidents without human intervention. As the accuracy of these technologies increases, Ovum expects to see further adoption and implementation in customers' SOCs. There is a caveat: it will be a combination of automation and security professionals that will win out. MSSPs are using data analytics and automation to filter out false positives, identify routine easily identifiable low-level incidents and vulnerabilities, and thereby lessen the dependence on security staff to carry out routine security tasks. As they deploy more of these tools and techniques to assist their professionals and relieve them of the basic chores of security hygiene, we expect MSSPs to change their focus away from the provision of individual discrete managed services to a much more holistic, integrated, and automated approach to the customer's overall IT environment and cybersecurity health.

Analytics and automation will free up limited security resources for more strategic and forward-looking security matters and represent a key trend across the whole of the IT services space. AI, ML, and other technologies will be deployed as ways to lessen staffing pressures (cost and headcount), increase monitoring accuracy, and reduce the customer's need to hire more internal staff. A few new providers, such as Darktrace, already claim to deliver these outcomes as part of their offers and have some history to back them up. But in most cases, such solutions and technology solve only part of the security problem. There is a plethora of new niche technology solutions, and they do not and should not operate in splendid isolation.

As enterprise IT expands into the cloud, as devices and even data become the new edge of the network, it is imperative that enterprises develop and plan their enterprise IT security architecture. As competition in the managed security services market heats up, the winners will be those MSSPs that can help enterprises move from silos of tools and expertise protecting pockets of the IT landscape, responding to incidents, and remediating threats, to an architecture in which protection, response, and remediation are part of a cybersecurity immune system. Ovum expects that MSSPs of all stripes will start to develop a more holistic approach to their cybersecurity services, not to "own" the customer's security operations, but to integrate services, fill in the gaps in the customer's capabilities, add automation, augment skills where needed, and deliver the advantages of operating at scale that will help customers move from cybersecurity silos to a more organic cyber immune system.

Appendix

Methodology

Report information and trends come from Ovum's coverage in reports and opinion pieces of the managed security services on offer from large global MSSPs. Security and software vendors provide information and briefings to Ovum on a regular basis, and Ovum undertakes regular projects and surveys on their behalf. These provide additional information and data on security services trends. Ovum analysts attend client analyst sessions that include managed security services and also attend security events such as RSA, Infosec, and Black Hat, where security vendors and providers share new services information and roadmaps.

Further reading

"Defining the next-gen managed security services provider," IT0019-003655 (August 2017)

2017 Trends to Watch: Security, IT0022-000808 (October 2016)

Author

Mike Sapien, Chief Analyst, Enterprise Services
mike.sapien@ovum.com

Ian Brown, Senior Analyst, Network Transformation & Cloud
ian.brown@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at **consulting@ovum.com**.

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum

TMT intelligence | informa

About Ovum

We provide authoritative data & forecasts, market research and analysis, bespoke consulting and end-to-end marketing services to help companies thrive in the connected digital economy.

Ovum helps service providers and their technology partners create business advantage by providing actionable insight to support their business planning, product development and go-to-market initiatives.

Visit **ovum.informa.com** to learn more.

International Offices

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo

Contact us

ovum.informa.com
marketingdepartment@ovum.com