eSENTIRE

eSentire European Executive Forum

At the end of 2023, IT Europa invited senior leaders from MSPs across the Benelux region to attend its European Executive Forum at Pulitzer Amsterdam. The session sponsored by eSentire and hosted by Phil Skelton provided an insightful roundtable session with frank and open discussion around the emerging industry trends and potential strategic partnership options for the delivery of Managed Detection and Response services.

The European cybersecurity market, currently undergoing rapid expansion and innovation, presents a complex landscape shaped by various factors including technological advancements, regulatory pressures, and evolving cyber threats. The Executive Forum examined several issues that service providers face and how strategic partnerships can unlock new opportunities to better address client requirements.

GROWTH DRIVERS

The Forum examined four key areas driving growth within the cybersecurity space.

Digital Transformation: The rapid digitalization of industries across Europe has significantly increased the need for robust cybersecurity measures. Enterprises are investing heavily in protecting their digital assets from cyber threats.

Regulatory Compliance: Regulations such as GDPR have had a profound impact, compelling organizations to bolster their cybersecurity postures. Emerging compliance requirements such as NIS2 are also accelerating investment in cybersecurity solutions and services.

Advanced Technology Integration: The incorporation of AI, machine learning, and blockchain in cybersecurity solutions is enhancing threat detection and response capabilities, thereby driving market growth.

Rising Cyber Threats: The increasing sophistication and frequency of cyber-attacks have heightened the need for comprehensive cybersecurity strategies.

Key insights from the day included several comments from participants that highlighted a major challenge with differentiation of services within highly competitive marketplace. “Many customers don’t really understand cybersecurity,” said one delegate, a founder of a Managed Services Provider based in the North of the Netherlands. “They [clients] know that it is a problem, but they don’t really understand the difference between the various brands of cybersecurity technology. They trust us to deliver something that that will protect them… they don’t care how… just that it works.”

Another theme that was expressed was the fear of tougher regulations. “We had GDPR, and that made people sit up and listen, but GDPR was not really about security. NIS2 is another moment where we can help clients to get more secure, but I believe that there will be a lot more regulations that will impact not just clients but MSPs like us,” said another delegate from an MSP based in Belgium.

MARKET DYNAMICS

The session also looked at several challenges faced by MSPs. Although wide ranging the areas that generated most consensus included:

Cybersecurity Skill Gap: The scarcity of skilled cybersecurity professionals is a critical challenge, impacting the ability of organizations to effectively manage cyber risks.

Complexity of Cyber Threats: The evolving complexity of cyber-attacks, including zero-day threats, poses significant challenges for existing cybersecurity solutions and strategies.

Underinvestment in Security Infrastructures: A lack of understanding of the sophistication of cyber threats leads to underinvestment in security infrastructures, making organisations vulnerable to attacks.

Lack of remediation services: Post breach remediation is an area that is in high demand but limited internal skills within MSPs is limiting growth.

"Even with all the automation within modern cybersecurity platforms, we are still finding it difficult to attract and retain skilled staff," said a CTO from an MSP with a sizeable cybersecurity practice. "Maybe cybersecurity is not glamorous enough," he quips," but even if we offer more money, we still can't compete with the larger enterprises, and I am cautious about investing in training if staff are just going to leave after a year."

"You can always find budget after the client has been breached," added another participant, "But then it is too late. The other issue is that even if you don't look after a client's security, if they have an issue, they want to blame you."

IMPACT OF COVID-19

The COVID-19 pandemic has had a profound impact on the cybersecurity landscape in Europe. With the rapid shift to remote work and increased digital service delivery, there has been a corresponding rise in cyber threats, driving demand for cybersecurity solutions. The pandemic has also accelerated the digital transformation of businesses, further boosting the cybersecurity market.

"Many of our clients have switched to remote working which makes cybersecurity maybe a bit more challenging," said a delegate with headquarters near Amsterdam, "It is not just 9 to 5 anymore and the out of hours support we started offering during Covid is now pretty common for many more of our customers."

FUTURE OUTLOOK

Towards the end of the day, delegates discussed where they see the cybersecurity landscape evolving during 2024. Several of the common themes included:

Technological Advancements: The continued evolution of technologies like AI, IoT, and 5G is expected to drive the development of more sophisticated cybersecurity solutions.

Increasing Cyber Threats: As cyber threats continue to evolve in complexity, the demand for advanced cybersecurity solutions is expected to grow.

Regulatory Influence: Continued regulatory developments, particularly in data protection and privacy, are likely to be key drivers for market growth.

Skills Development: Addressing the cybersecurity skills gap through education and training initiatives will be crucial for market sustainability.

Deeper Strategic Partnerships: Expanded relationships for the delivery of high growth services such as Managed Detection and Response.

"One of our main goals for next year is to strengthen our cyber security portfolio and that means working more strategically with an MDR partner," said one delegate who currently offers a broad portfolio of cybersecurity services with a focus on the mid-market. "We looked at the cost of staffing our own SoC and it is a significant investment. Instead, we are in discussion with a few MDR specialists, and this event has helped us to better understand the alternatives."

"We know we need a partner if we want to scale," said another delegate. "Cybersecurity is just too broad to do it all ourselves and if there is a major vulnerability that impacts multiple clients, we just don't have enough people to do all the work quickly enough. Partnership is not just a case of IF but rather WHEN."

eSENTIRE

‘Profitable and scalable partnership strategy for cyber security service delivery in Europe’

Phil Skelton, Sales Director, eSentire

Cyber security service revenues in Europe will hit 34 billion euros within 4 years with CAGR at over 12% according to IDC. However, MSSPs wishing to capitalise on this ‘faster than inflation’ growth opportunity are constrained by several challenges.

Phil Skelton, Sales Director, eSentire

The first is the cost and complexity of building, managing, and staffing a 24/7 SOC is prohibitive and difficult to scale in line with new business growth. In addition, remediation services require a higher level of expertise, and a worst-case scenario of mass zero-day attack can overwhelm a smaller MSSP that has multiple clients impacted simultaneously.

MSPs are faced with difficulties in both recruiting and retaining skilled cyber security staff is a pan-European problem. An issue made worse by the likelihood of new cyber security compliance requirements currently under review by both the EU and national governments.

At eSentire, we have invested in building out resources to help MSPs across Europe to not only meet these challenged but to build a scalable and sustainable cybersecurity offering.

We are helping progressive MSSPs to develop closer relationship with us as a specialist provider of Managed Detection and Response services. Although this can include full outsourcing of MDR, a more common approach is a true “strategic partnership model” where our MSP partners use us a trusted provider, working together to build an operational model that provides protection at scale, mitigating risks while delivering a profitable and sustainable business model.

eSENTIRE

What can eSentire offer an MSSP?

eSentire specializes in cybersecurity services and solutions, catering to a wide range of industries and business sizes. The company's offerings are designed to help MSSPs provide comprehensive cyber defense capabilities, leveraging advanced technologies and expert insights to protect clients from cyber threats. Their services can be broadly categorized into several key areas:

Managed Detection and Response (MDR): eSentire's flagship service, MDR, combines cutting-edge technology with human expertise. It involves continuous monitoring and analysis of network activities to detect and respond to threats in real-time. This service ensures that threats are identified and mitigated swiftly, minimising potential damage.

Incident Response: In the event of a security breach, eSentire provides rapid incident response services. Their team of experts assists in identifying the scope of the breach, containing the threat, and restoring normal operations. They also offer guidance on strengthening security postures to prevent future incidents.

Risk Assessment and Management: eSentire offers services to assess and manage cybersecurity risks. This includes evaluating current security measures, identifying vulnerabilities, and providing recommendations to mitigate risks. Their approach is tailored to each organization's specific needs and regulatory requirements.

Threat Intelligence: The company collects and analyses data on emerging and existing cyber threats. This intelligence is used to inform their other services, ensuring that their responses are proactive and informed by the latest information.

Compliance and Advisory Services: eSentire helps organizations comply with various cybersecurity regulations and standards. They offer guidance on implementing policies and procedures that meet regulatory requirements, reducing the risk of non-compliance penalties.

Security Awareness Training: Recognizing that human error can be a significant security vulnerability, eSentire provides training programs to educate employees about cybersecurity best practices. This training is designed to foster a culture of security awareness within organizations.

Cloud Security: With the increasing adoption of cloud computing, eSentire provides specialized security services for cloud environments. They ensure that data stored in the cloud is protected and that cloud-based applications are secure from threats.

eSentire's approach to cybersecurity is holistic, encompassing both technology and human expertise. They leverage AI and machine learning for threat detection and analysis, while also relying on their team of cybersecurity professionals for insights and decision-making. This blend of technology and human intelligence enables them to provide robust and effective cybersecurity solutions.

eSENTIRE

eSentire's Partner Program - A Community Committed to Cybersecurity

eSentire created its e3 ecosystem to simplify security sales and transform how its delivers value through and with its partners to the end user customer. The needs of business leaders are changing and how they're choosing to transact continues to evolve.

The eSentire e3 ecosystem is focused on mapping partner engagement, productivity and overall experience to the ways its end customers want to consume best-in-class cybersecurity services. When you partner with the Authority in Managed Detection and Response, you can expect:

Preferential access to industry-leading solutions.
What makes eSentire different?
- G2 Security Leader in MDR
- Top MDR provider on MSSP Alert Top 250 Global MSSPs
- MDR Industry Leader recognized by IDC, Forrester, and Gartner

Stable recurring revenue. Our clients stick with us for the long haul.
What makes eSentire different?
2000+ customers, in 80+ countries across 35+ industries globally

- 99% of eSentire revenue is in ARR
- Proud of our 72 NPS Score
- Customer Success Survey scores:
- 100% deployment satisfaction
- 97% overall better security posture

Personalized, on-demand training, and sales support.
What makes eSentire different?
- Meaningful attention and customized content
- Technical certifications
- Dedicated Solution Architecture support to win deals fast

Achieve more with the power of the e3 ecosystem behind you.
What makes eSentire different?
eSentire rewards its partners' efforts to engage with all aspects of the e3 ecosystem, expect to get rewarded when you:

- Achieve Sales or Technical Certification
- Register approved deals
- Win your first 3 deals
- Reach selling milestones

eSENTIRE https://www.esentire.com/partners

https://www.linkedin.com/company/esentire-inc-/

Phil.skelton@esentire.com