corelight

GENERATIVE AI IN SECURITY:

Empowering or Divisive?
The search is on for the right approach.

How new AI technology for Cybersecurity Is Dividing IT Decision Makers.
Brand new research from Corelight explores if there could be a perfect formula.

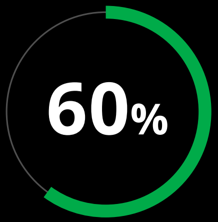
Generative AI (GenAI) is the talk of boardrooms and Security Operations Centres (SOCs) across the globe. And for valid reason. The technology's ability to analyse and summarise huge volumes of complex data, create new content, and enable users to gain insights into datasets via natural language prompts could be transformative for human workflow acceleration. Following the breakout success of ChatGPT, experts have been discussing how the technology could revolutionise industries and roles as diverse as marketing, product development and customer service. Could this be the same for cybersecurity, or is it too early to say?

According to McKinsey, GenAI is already in widespread use. One-third of global respondents told the consulting giant that their organisation is using the technology in at least one function—and 60% of those with reported AI adoption are using GenAI. Yet the same study reveals widespread concerns, topped by inaccuracy (56%) and cybersecurity (53%).

To find out what European IT professionals think, Corelight commissioned Sapio Research to poll 300 IT Decision Makers (ITDMs) in the UK, France and Germany. Respondents hailed from a range of organisation sizes and sectors, and had responsibility for or heavy involvement in cybersecurity in their organisation.

What we found was that GenAI is both a source of optimism and concern among the professional cybersecurity community.

One-third of global respondents told the consulting giant that GenAI is already in widespread use.



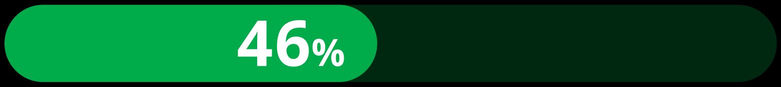
of those with reported AI adoption are using GenAI.

Interest is building

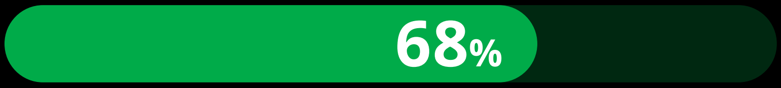
There's no doubt that European businesses are keen to explore the potential in GenAI. Nearly half (46%) of respondents say they're proactively looking at how to incorporate the technology in their cybersecurity approaches. That's ahead of the 44% who are prioritising employee engagement and security awareness raising. Even more (78%) believe that GenAI will strengthen their cybersecurity in some way.

What specifically are teams using the technology for right now? Over two-thirds (68%) of those with dedicated threat hunters say it's helping their threat detection and protection efforts. And a further 28% plan to incorporate these capabilities in the future.

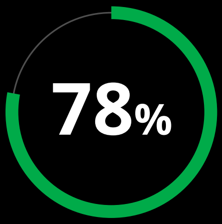
This makes sense from one perspective: SOC teams are often understaffed and analysts struggle with alert overload when tools can't help them to intelligently prioritise alerts. A high degree of manual work is not only exhausting, it is also demotivating for many professionals. One 2023 study claims that 63% of SOC practitioners experience some level of burnout, with over 80% saying their workloads increased in the previous year. If GenAI could help bridge the staff shortages and skills gap and make analysts more productive, it would be invaluable for organisations and for employee retention.



say they're proactively looking at how to incorporate the technology in their cybersecurity approaches.



of those with dedicated threat hunters say it's helping their threat detection and protection effort.



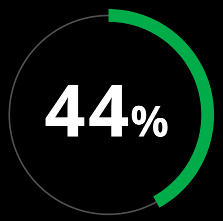
believe that GenAI will strengthen their cybersecurity.

Barriers and scepticism

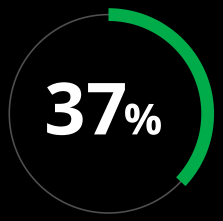
Yet our research also reveals a healthy dose of scepticism when it comes to GenAI in cybersecurity. Over two-fifths (44%) of respondents believe that the sensitive nature of the data involved – and enterprise silos – will make it difficult or impossible to use GenAI in cybersecurity. A further 37% argue that the technology is simply "not safe to use in cybersecurity".

Of the third (32%) of responding organisations that are not using the technology for threat detection and response, a plurality (37%) claim this is because of C-suite concerns, which could stem from the fact that just 16% of security teams participate in boardroom discussions. More dialogue at this level could help to assuage concerns and green light projects. Slightly fewer cite budget, trust and time constraints (all 30%) as a barrier.

Yet there are ways to mitigate such concerns via careful instrumentation of this new technology that accounts for data protection sensities. For example, Corelight's answer in its initial integration of GenAI into its commercial Network Detection & Response (NDR) product is to establish a functional firewall between the customer's data and the technology, such that customer-specific data cannot interact with the GenAI model. Instead, Corelight uses pre-vetted GenAI prompts and outputs to contextualise alerts in Corelight's detection catalogue and provide analysts with recommended validation and response actions to accelerate incident response. Corelight then uploads these GenAI created alert enrichments and investigative recommendations in Corelight's SaaS infrastructure and makes them available to customers. That offers a middle ground where users can access AI-accelerated next steps for remediation and investigation of an alert without compromising privacy.



of respondents believe the sensitive nature of data make it difficult or impossible to use GenAI in cybersecurity



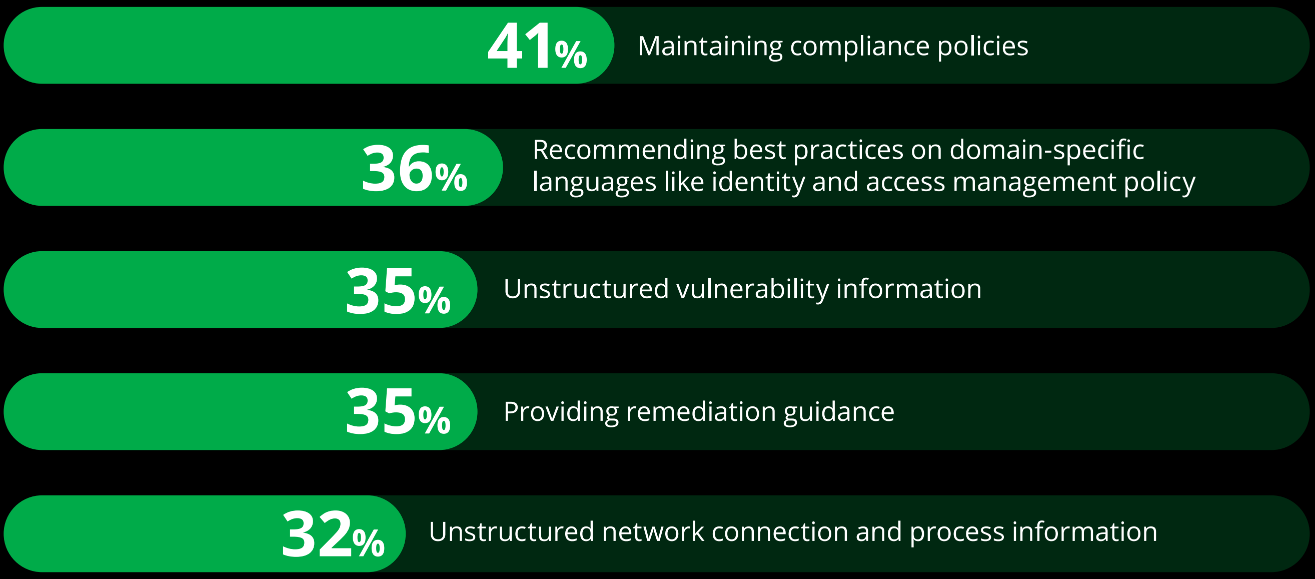
argue that the technology is simply "not safe to use in cybersecurity"

Striving for the perfect formula

While many respondents to our poll are clearly sceptical of the technology, a sizeable share have a more optimistic vision of the future. Some 42% claim AI and automation are central to them creating “the perfect security formula” – just behind “skilled security staff” (53%) and ahead of “relevant threat intelligence” (33%).

Half (50%) believe GenAI will have the biggest impact on providing alert context and analysis. There’s certainly a case for saying GenAI’s ability to summarise and synthesise existing information and present it in natural language is its most effective cybersecurity capability. In so doing, it can deliver powerful context, insight and next steps to accelerate investigation and remediation, and close analyst skills gaps.

RESPONDENTS ALSO CLAIM THAT GENAI COULD HELP MOST WITH:



Recommendations

It is without doubt that AI is now used to detect a wider range of sophisticated attacks, enriching security data with contextual insight, and providing SOC analysts with new capabilities for understanding and reacting to security alerts.

In the minds of cybersecurity leaders, GenAI is clearly no silver bullet nor universally accepted technology. But if concerns over data protection and accuracy can be addressed, and internal roadblocks removed, it could add real value to many organisations. A great deal will depend on how projects are managed and whether vendor solutions adequately address the concerns highlighted in this report.