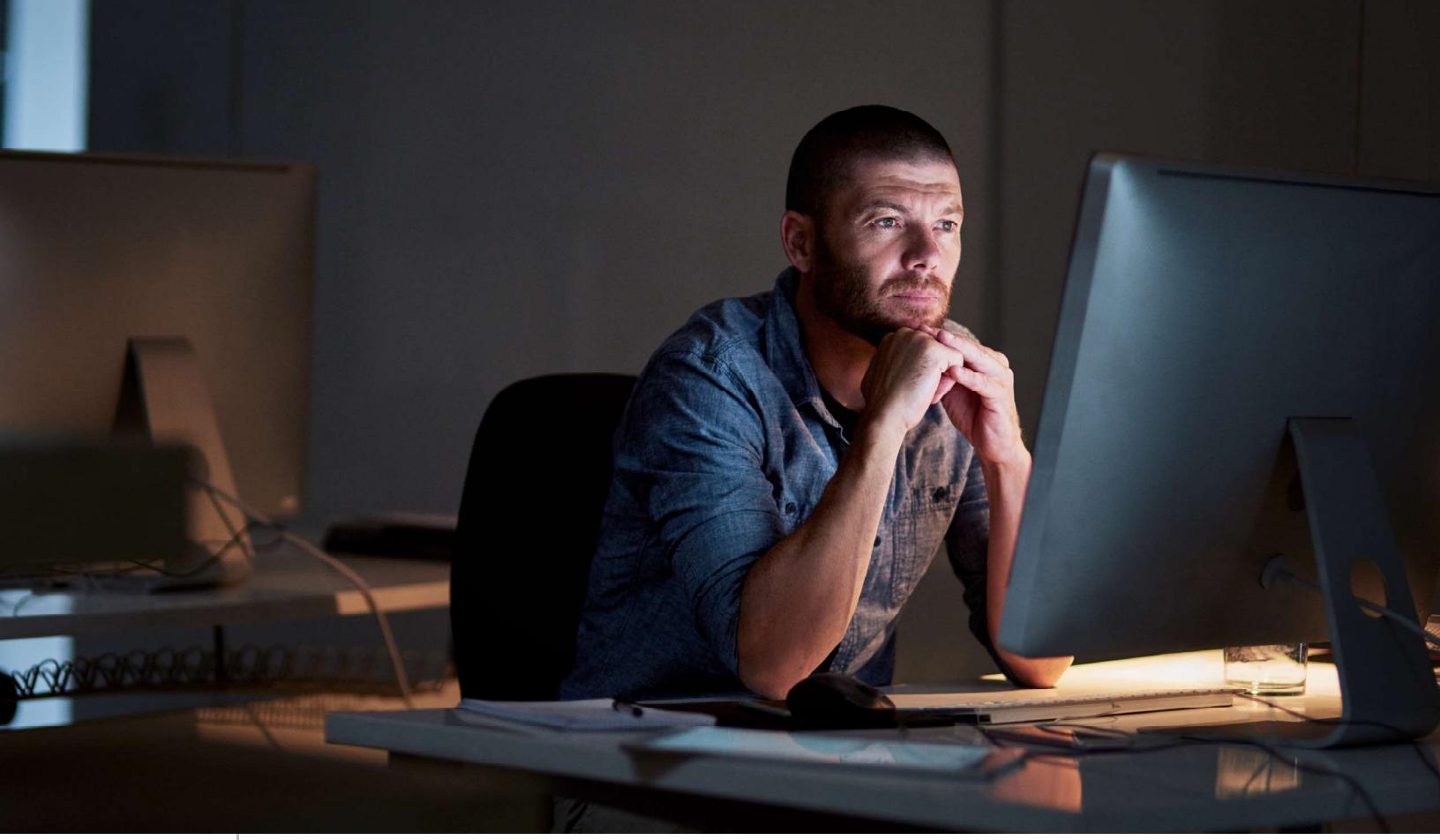
The bridge to possible

Close the Cybersecurity Workforce Gap with Artificial Intelligence



With 3.5 million job vacancies, the global cybersecurity workforce shortage is arguably the greatest vulnerability businesses face today. Security teams around the world are understaffed and overworked. Without adequate cybersecurity staffing, organizations are at increased risk of a security incident. They are ill-equipped to stop today's advanced threats and reduce employee burnout. Unfortunately, the problem isn't going to improve any time soon—even as the number of skilled professionals increases, the workforce gap continues to grow even faster.

3.5 million

cybersecurity jobs are left unfilled globally in 2024.

Meanwhile, the IT environment is growing increasingly complex and the threat landscape is becoming more challenging. The shortage of skilled cybersecurity professionals is demanding organizations' immediate attention and prompting a new approach to equipping security operations centers (SOCs) with the proper resources to elevate existing staff and optimize SOC technologies to work more efficiently.

All of this makes for compelling generative AI use cases. In this paper we'll look at how all of AI capabilities can meaningfully impact the work of security analysts to streamline operations and enable organizations to future-proof their SOC.

© 2024 Cisco and/or its affiliates. All rights reserved.

The bridge to possible

The Impact of a Cybersecurity Skills Shortage on the SOC

21%

On average, cybersecurity roles take 21% longer to fill than other IT jobs.

According to ISC2, 75% of cybersecurity professionals view the current threat landscape as the most challenging it has been in the past five years. More alarmingly, only 52% believe their organization has the tools and people needed to respond to cyber incidents over the next two to three years. The job is getting harder on all fronts.

Given the shortage of cybersecurity professionals, staff retention is critical. Unfortunately, without the proper tools, security professionals are unable to manage cyber risk effectively and often face burnout, which negatively impacts retention and the SOC's ability to stop cyberattacks.

Today's SOCs often lack a cohesive technology stack to efficiently and consistently respond to cyber threats. As the IT environment grows beyond the on-premises data center to cloud, hybrid cloud and multicloud country specific data centers, organizations accumulate point solutions to monitor and protect pieces of the environment. As a result, SOC analysts must do a lot of the heavy lifting required to detect and respond to an attack. A lack of threat context and interpretation increases the difficulty of properly assessing risk and makes it challenging to understand the right response actions to remediate the root cause. Repetitive tasks like log analysis, data correlation and response actions are all inefficient. And without standardized processes across the tech stack, the risk of human error increases with the need to go faster and do more across differing tech stacks.

The operational burden caused by a disparate tech stack is only made worse by the cybersecurity skills shortage, and both increase an organization's risk of being susceptible to a successful cyberattack. The current approach to staffing and operating a SOC is not sustainable. With information security analyst jobs projected to grow by 32% between 2022 and 2032, there simply aren't enough skilled professionals to protect IT infrastructures. The growing burden on understaffed teams makes the problem worse by impacting retention and effectiveness.

© 2024 Cisco and/or its affiliates. All rights reserved.

The bridge to possible

AI to the Rescue

Fortunately, advances in AI can address the root problems that lead to analyst burnout and poor cybersecurity outcomes. In fact, according to ISC2, 82% of cybersecurity professionals agree that AI will improve their job efficiency. And ISC2 agrees—with a prediction that AI will play a "meaningful role" in allowing cybersecurity professionals "to focus on more complex, high value, and critical tasks, perhaps alleviating some of the workforce pressure."

By combining AI with the breadth of telemetry across the network, private and public cloud infrastructure, applications, internet, email, and endpoints, AI can bolster security and offer more protection against sophisticated attackers. AI scales the human knowledge that's already in the SOC so that it can be used more effectively, while automating lower-level tasks so analysts can focus their efforts on more strategic initiatives.

AI can empower analysts to be more effective and satisfied in their work, thereby increasing staff retention and SOC efficacy. The result is more accurate, consistent, and reliable security outcomes.

The IBM Cost of a Data Breach Report 2023 found that organizations that use security AI and automation "experienced, on average, a 108-day shorter time to identify and contain" a data breach.

That time translates directly to an organization's bottom line: organizations with sophisticated AI and automation "reported USD $1.76 million lower data breach costs."

Elevate Analyst Performance

One of the ways AI can help close the cybersecurity workforce gap is by helping and "leveling up" existing talent. AI can elevate analyst performance by providing predictable informed, context-based assistance so that analysts can see issues through completion, regardless of their experience. The emergence of AI security assistants has spurred even further refinements to help SOC analysts through complex tasks, save them time, and eliminate errors and misconfigurations. These assistants can also meaningfully help analysts with simple tasks that are typically time-consuming and repetitive. For example, details that provide context might reside in 50 different consoles, but AI can deliver that full visibility in a couple clicks.

© 2024 Cisco and/or its affiliates. All rights reserved.

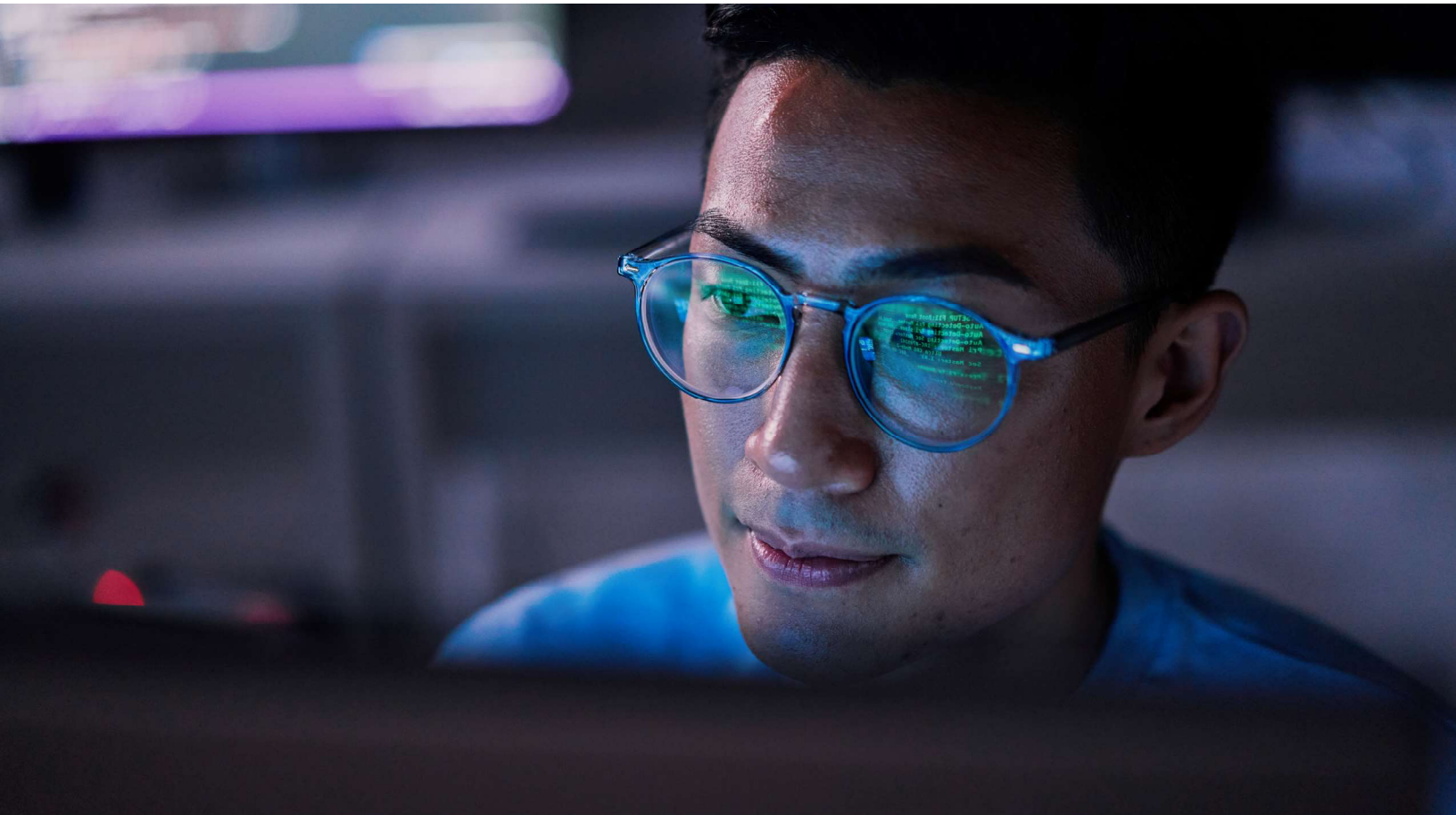
The bridge to possible

Improve the Analyst Experience

AI-powered capabilities allow security teams to run at machine speed so they can focus on what's critical. It works at scale to identify patterns and potential attacks that humans might miss due to alert fatigue. Because AI can correlate data at scale across email, web, process, and network domains, it can detect attacks with greater accuracy. AI can also augment human understanding with deep detections and insights.

Elevate SOC Performance

AI can also learn from human-to-machine interactions to automate complex playbooks, thereby elevating SOC performance. For example, the SOC may need to isolate 40 different endpoints across several different vendors. This will require doing the work in separate consoles and then validating that the actions have been properly applied. An AI-driven platform, however, can learn continuously from how analysts interact with the environment and deploy a playbook that automates pieces of the workflow. AI can also recommend response actions based on the analysis of disparate siloed information.



The bridge to possible

Putting AI to Work with Cisco

75%

of cybersecurity professionals say AI can help them by automating repetitive tasks.

The modern IT environment demands a robust detection and response solution that can help security analysts detect, prioritize, and mitigate threats from every angle. Cisco XDR simplifies security operations, accelerates responses, and empowers SOC teams with AI-driven and proactive threat detection and response. The cloud-native, extensible solution brings data from multiple security tools and applies machine learning and analytics to arrive at correlated detections. Cisco XDR shifts the focus from endless investigation to remediating the highest priority incidents with evidence-backed automation, helping SOC teams act with greater speed, efficiency, and confidence.

The Cisco AI Assistant in XDR is a generative AI-powered assistant embedded within Cisco XDR that empowers SOC analysts — of all levels — with the information they need to make critical decisions quickly. The AI Assistant helps teams work more effectively by providing more informed decisions, augmenting existing capabilities, achieving consistency in their actions, automating complex tasks, and quickly understanding the next best step in an investigation.

Cisco's AI Assistant in XDR simplifies daily tasks by providing security analysts with a way to ask the AI assistant — using natural language — to produce a concise incident summary. This guidance quickly provides important context about current threats that have been correlated from multiple event sources. With additional prompts, the AI Assistant can return further details about affected assets and observables.

SOC teams are empowered to:

- Perform at a higher level using valuable context and specific next steps
- Prioritize the most critical incidents to investigate
- Gain valuable direction related to incident triage and investigations
- Reduce the time it takes to communicate actions taken on incidents

The AI Assistant in XDR provides direction for complex incidents by giving security analysts actionable guidance informed by historical data of specific incident types. It suggests detailed multi-step workflows in identification, containment, eradication, and recovery based on past incidents.

© 2024 Cisco and/or its affiliates. All rights reserved.

The AI Assistant improves the analyst experience by:

- Recommending response actions (right context at right time)
- Qualifying security events to provide best next steps in an investigation to maximize analyst efficiencies
- Establishing unified visibility with minimal blind spots

For the most consuming tasks, security analysts can review ongoing incidents and employ the AI Assistant to assess impact, investigate, and collaborate with team members in a collaborative war room.

The AI Assistant elevates SOC performance by:

- Increasing collaboration and maximizing efficiency using Webex, Slack, and Teams
- Maintaining uniformity, efficiency and consistency between every SOC analyst to eliminate errors

There simply aren't enough cybersecurity professionals to meet the needs of today's businesses. As long as SOCs remain understaffed and overworked, the cybersecurity workforce shortage will remain a critical vulnerability that impacts the SOC's effectiveness and analyst morale. Organizations need a more advanced approach to operating the SOC, one that empowers analysts and positions the organization to future-proof the security environment. Cisco is harnessing AI to reframe how organizations think about security outcomes and tip the scales in favor of defenders.

Serving as a trusted advisor and leveraging LLM to perform difficult tasks in a consistent and effective way, The Cisco AI Assistant in XDR provides immediate value to SOC teams by maximizing an analyst's attention on more complex and strategic tasks, minimizing routine actions, and providing data driven guidance that drives analyst efficiency, accuracy and speed.

Learn more about Cisco XDR and the Cisco AI Assistant in XDR.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

1326076753 05/24