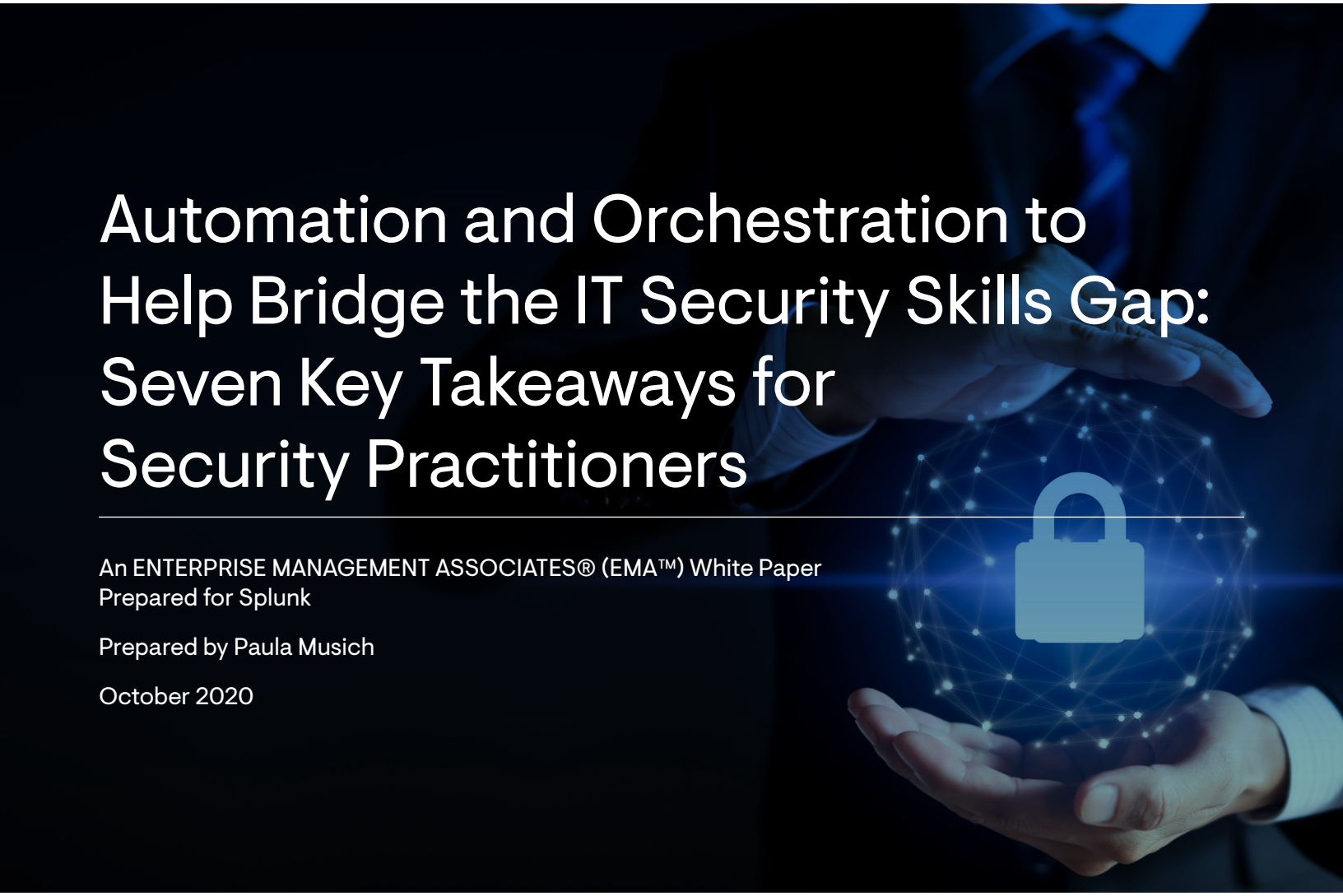


Automation and Orchestration to Help Bridge the IT Security Skills Gap: Seven Key Takeaways for Security Practitioners

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Splunk

Prepared by Paula Musich

October 2020

splunk>

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Automation and Orchestration to Help Bridge the IT Security Skills Gap: Seven Key Takeaways for Security Practitioners

EXECUTIVE SUMMARY

In June 2020, Enterprise Management Associates surveyed 200 IT security executives and contributors on the impact of the vast and growing IT security skills gap on their organizations' ability to protect their digital assets from bad actors. Respondents represent organizations with at least 500 employees across a range of industries, with a primary focus on North American markets. They were queried about how automation and orchestration, in various forms, are helping alleviate issues caused directly or indirectly by that gap.

By some estimates, the gap now accounts for several million open IT security jobs globally. Among the EMA survey respondents whose organizations had at least 500 employees, the average number of open IT security jobs they were trying to fill was 1,324. This number has increased over the last year by between 1% and 25% for the largest number of respondents, and will likely increase over the next few years.

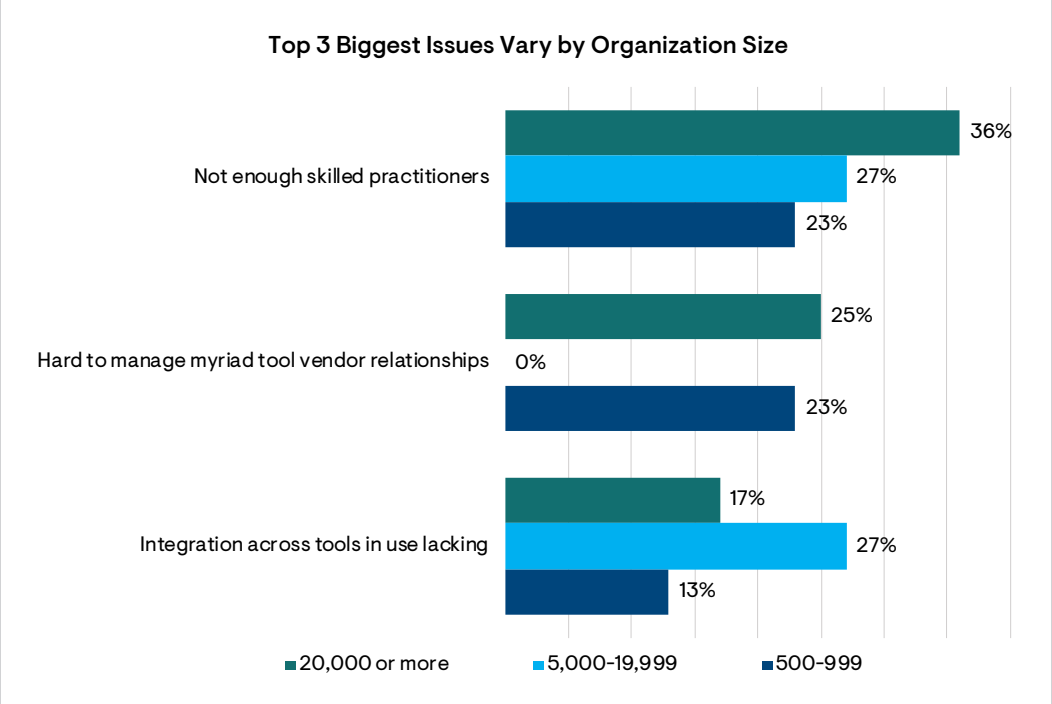
In response, a variety of IT security tool providers have stepped up the level of automation and integration capabilities available within their products. Security orchestration, automation, and response (SOAR) technologies in particular were uniquely engineered to address some of the issues that contribute to the large IT security skills gap seen today. Some of these problems include a lack of integration across too many security tools, a lack of coordination between multiple security practitioners, and a lack of well-defined security processes across the security operations center (SOC).

Based on the results of the survey, the following are seven key takeaways that put the skills gap problem into perspective, and illustrate how SOAR technology is helping understaffed security teams work more efficiently.

THE IT SECURITY SKILLS GAP IN CONTEXT

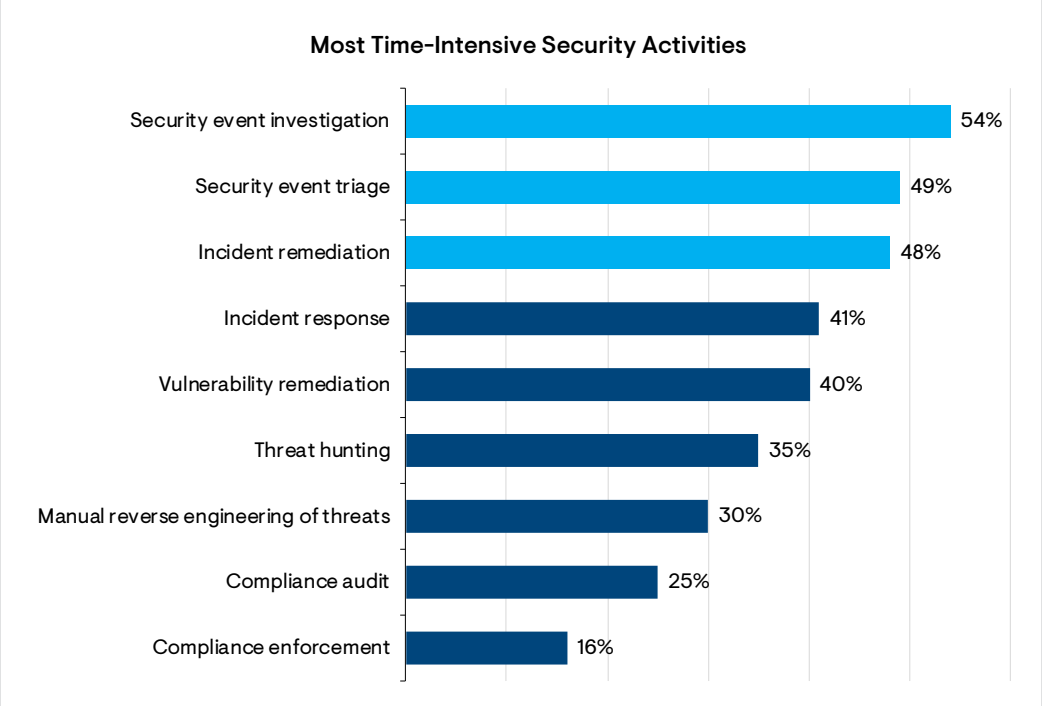
1. The top 3 challenges for security teams.

The survey broke down respondents according to the size of the organizations they represented, including midmarket organizations with 500 to 999 employees, small to medium (SME) enterprises with 1,000 to 4,999 employees, large enterprises with 5,000 to 19,999 employees, and very large enterprises with over 20,000 employees. Respondents in these groups were asked to rank 10 different issues that security teams typically face according to how significant they are for respondent organizations. In looking at the top three highest ranked issues, the majority of midmarket, large enterprises, and very large enterprises all agreed the biggest issues their security teams face today are not enough skilled security practitioners, lack of integration across tools, and hard to manage tool vendor relationships. On the other hand, SMEs said their top issues revolve around too many false positives, difficulty in prioritizing alerts, and high false positive rates causing practitioner burnout.



2. The most time-intensive security activities include security event investigation, security event triage, and incident remediation.

Respondents were asked to indicate which of nine typical security-related activities they viewed as the most time-consuming. Activities fell into three categories, including threat detection, investigation, and response; vulnerability management; and compliance management. Of the nine activities listed, the majority of respondents indicated the following as the most time-consuming.

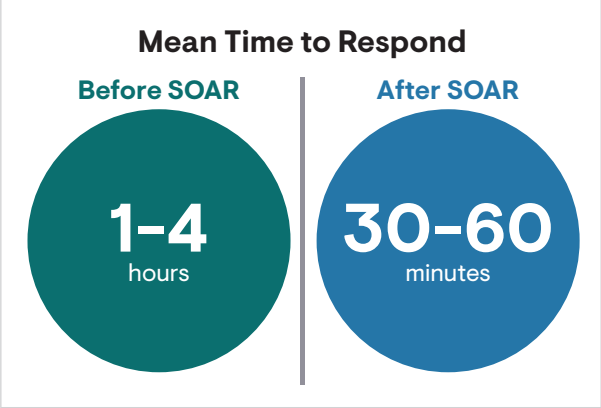


HOW SOAR CAN HELP

3. SOAR helps lower mean time to respond.

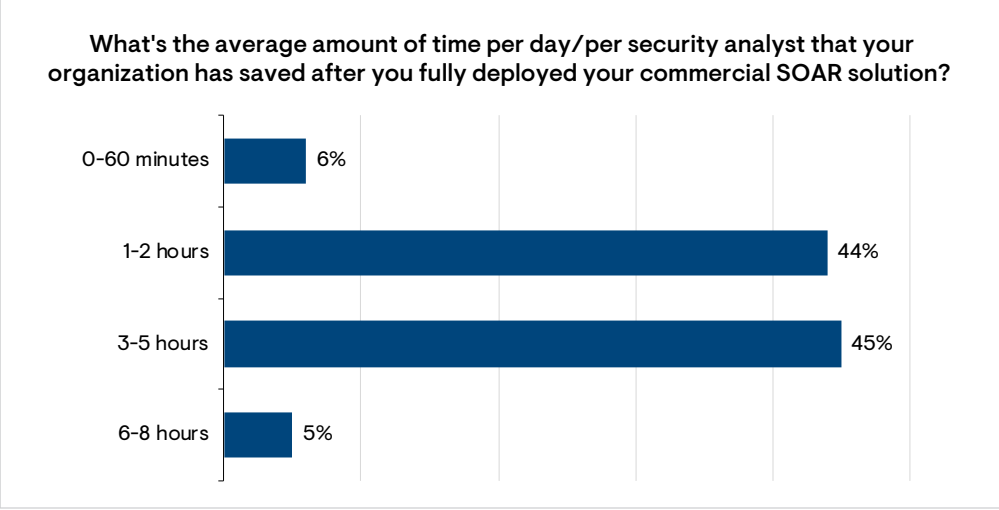
Security teams often use mean time to respond (MTTR), or the average time it takes to remediate a legitimate threat, to measure team efficiency. The survey asked respondents whose organizations were using a commercial SOAR product to indicate which of 10 possible MTTR time ranges their security teams delivered both before and after SOAR deployment.

From the survey, 30% of SOAR users indicated that their security teams' MTTR was around one to four hours before SOAR deployment. Twenty-seven percent of SOAR users indicated that they saw their MTTR decrease to 30 to 60 minutes after SOAR deployment. One respondent indicated that their MTTR went from between 4 and 8 hours to less than 5 minutes.



4. SOAR helps increase SOC efficiency by saving more time per day/per analyst.

Another efficiency metric the EMA survey sought to document is the amount of time per day/per analyst that SOAR deployments enabled for respondent organizations. SOAR user respondents overwhelmingly indicated significant savings, with 89% noting an average savings of between one and five hours per day per analyst.



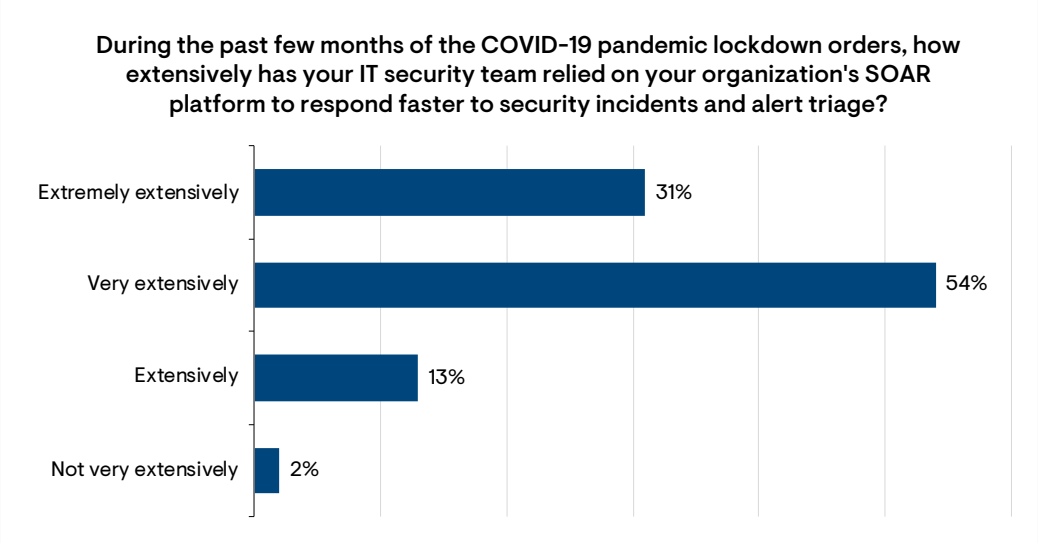
5. SOAR helps lower SOC turnover among security practitioners.

High degrees of practioner burnout and talent turnover are other notable factors contributing to the IT security skills gap. In addition to the stressful nature of IT security, the repetitiveness of manually correlating threats across different domains, investigating an impossible number of false positives, and trying to master a wide variety of different security tools causes security practitioners—particularly lower-tier analysts with less autonomy—to frequently change jobs. When SOAR user respondents were asked whether they thought the deployment of commercial SOAR technology within their organizations helped to lower turnover among their security analysts/staff, 74% indicated that it did. Only 21% said no, and 5% said they were unsure. For those who indicated their organizations experienced lower turnover, the majority estimated the reduction to be between 21% and 40%.

74%
of SOAR users agree that SOAR lowers analyst turnover

6. SOAR delivers value in enabling secure remote work during COVID-19 pandemic.

The sudden exponential increase in the number of employees working from home due to the ongoing pandemic has caused significant challenges for IT security practitioners who had to quickly pivot to protect remotely distant endpoints. During this time, IT security teams leaned on automation and orchestrated workflow delivered through SOAR and other security technologies like never before. The research found that of the respondents using SOAR technology within their organizations, 94% reported that their SOAR platforms were either very or extremely valuable in enabling security teams working remotely to coordinate security workflows. A large majority of those same respondents (85%) also said that their security teams relied either very or extremely extensively on their SOAR platforms to respond faster to security incidents and alert triage since the pandemic began.



7. Interest in SOAR technology adoption is at an all-time high.

Given the benefits that SOAR respondent organizations are seeing with their deployments and the growing need for SOCs to do more with less, it's no surprise that interest in the technology is high. Among EMA survey respondents whose organizations were not yet using commercial SOAR tools, an impressive 93% indicated that their security teams were either evaluating SOAR tools or considering adopting SOAR technology. While the relatively nascent market is still small, interest is quite strong, and for good reason. SOAR may not be a panacea for all the ills afflicting the SOC, but it is obviously creating efficiencies that help to reduce the symptoms of the global IT security skills gap. Any organization thinking about SOAR technology to help ease the side effects of the skills shortage should determine key requirements that potential suppliers must meet, then create a shortlist based on those criteria.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

4032.101220