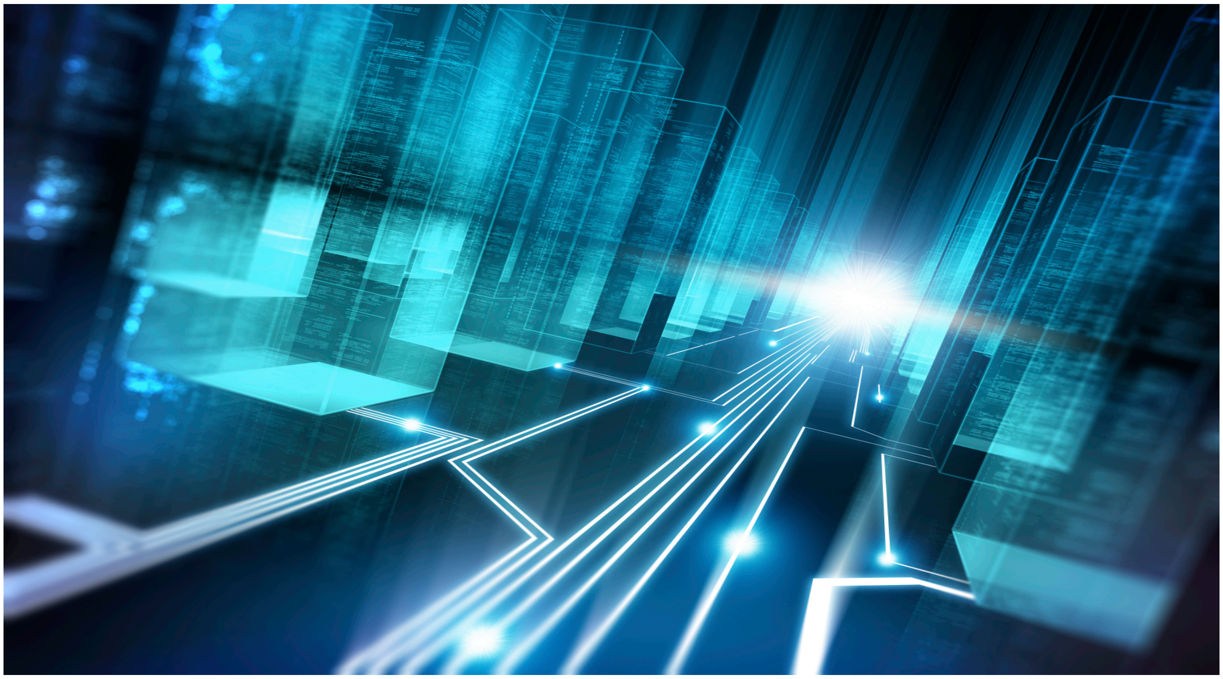


Reducing Cybersecurity Costs & Risk through Automation Technologies Executive Summary

Sponsored by Juniper Networks

Independently conducted by Ponemon Institute LLC

Publication Date: November 2017

Reducing Cybersecurity Costs & Risk through Automation Technologies

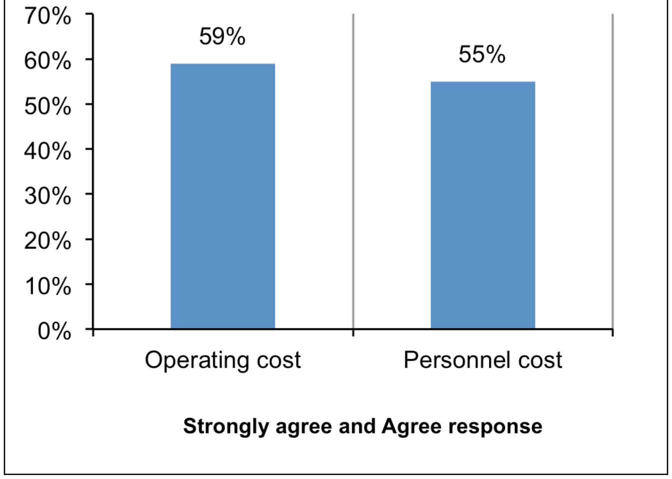
Executive Summary

Ponemon Institute: November 2017

Cyber automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning and orchestration. The purpose of this study, *Reducing Cybersecurity Costs & Risk through Automation Technologies,* is to understand how organizations are deploying these technologies, the benefits of automation and their cost-effectiveness.

A key takeaway from this research is evidence that cyber automation reduces the required hours to deal with security exploits with greater accuracy and as a result can save organizations an average of more than $2.3 million annually while strengthening their security posture.

Figure 1. Cyber automation will reduce costs



As shown in Figure 1, the majority of respondents believe cyber automation reduces both operating and personnel costs (59 percent and 55 percent of respondents, respectively).

In this study, we surveyed 1,524 IT and IT security practitioners in the United States, EMEA and Asia-Pac. All respondents are familiar with their organizations' practices for identifying and/or containing cyber events and have some level of responsibility in directing security program activities and making investments in "next generation" security technologies.

Following are key findings from this study.

Migration to the cloud has increased the need for automation of cyber tools and technologies. As more companies move their IT infrastructure to the cloud, enhanced security, such as cyber automation, is increasing in importance, according to 59 percent of respondents.

Companies are committed to the deployment of cyber automation. Most companies represented in this research (61 percent of respondents) are committed to at some point having cyber automation as part of their security arsenals. One reason, according to 62 percent of respondents, is that the use of cyber automation will reduce the rate of false positives in the investigation of security alerts.

Complexity is a barrier to full deployment. On the downside, 60 percent of respondents say the integration of cybersecurity automation within their companies' existing IT security architectures is a complex and time-consuming process.

Automated tools and technologies reduce the need for human intervention in the containment of cyber exploits. In this research, 53 percent of respondents say their organizations have automated tools and/or technologies that capture intelligence and evaluate the true threat posed by cyber attackers. According to respondents, an average of 51 percent of cyber exploits or the containment of malware can be handled without human intervention.

Companies are slow to rely on automated tools such as machine learning and artificial intelligence. More than half of companies represented have automated tools. However, only 20 percent of respondents say their organizations' approach to cyber defense primarily relies on these technologies. Instead, 34 percent say they rely primarily on manual activities and 25 percent of respondents say their approach is "ad hoc" or not specified.

Will automation replace IT security staff? Most senior managers, according to 60 percent of respondents, do not believe smart machines will replace skilled security personnel and 71 percent of respondents say cyber automation will never fully replace human involvement and expertise. An average of almost 17 security staff members are involved in the cyber exploit or malware containment process and they have an average of 8.5 years of experience.

Cyber automation technologies will help organizations address their staffing concerns. Fifty-five percent of respondents say the use of cyber automation will reduce personnel costs and 53 percent of respondents say the inability to properly staff skilled security personnel has increased investments in the automation of cyber tools and technologies. In addition to reducing personnel costs, operating costs will be reduced as well (59 percent of respondents).

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.