THREATQUOTIENT

AT A GLANCE

State Of Cybersecurity Automation Adoption

INTRODUCTION

This research was conducted to build on the findings of a survey of senior UK cybersecurity professionals carried out in 2021. The research cohort was expanded to 750 senior executives across the UK, US, and Australia. The study examines the drivers for implementing cybersecurity automation in today's distributed enterprises, exploring the common use cases, the typical challenges faced, and the barriers to automation adoption. The thorny topic of measuring automation ROI is explored and the 2022 report also identifies the level of cybersecurity automation maturity in enterprises. It looks at how the rise of Extended Detection and Response (XDR) is affecting organizations' appetite for automation, and the extent of board-level interest in cybersecurity reporting.

Read this report to understand how CISOs and senior cybersecurity professionals are approaching the challenge of securing the extended enterprise in an intense and complex threat and operational environment. Which automation use cases are working, and which could benefit from more focus?

METHODOLOGY

Leading security operations platform innovator, ThreatQuotient, commissioned a survey, undertaken by independent research organization, Opinion Matters, in July 2022. 750 senior cybersecurity professionals in the UK, US and Australia from companies employing 2,000+ people from five industries took part, including: Central Government, Defense, Critical National Infrastructure - Energy and Utilities, Retail, and the Financial Services Sector.

SUMMARY

The intense and complex cyber threat landscape, coupled with a persistent shortage of skilled security professionals, continues to exert significant pressure on cybersecurity teams. Increasingly, cybersecurity automation offers a solution that enables a more effective security and risk function today, and acts as a foundation to support the protection of the fast-evolving security frontiers of tomorrow.

As businesses and public sector organizations continue to build more agile, distributed working environments alongside highly personalized customer journeys, they must get smarter and more efficient about protecting the data and infrastructure on which they depend. The sheer volume of data generated and the escalation in potential attack vectors mean this cannot be a purely manual undertaking; automation is essential. Our 2022 State of Cybersecurity Automation Adoption research finds that organizations are working to automate various elements of their security strategy and are progressing through different levels of maturity. However, they face challenges along the way. There is evidence that technology complexity, skills shortages, and a lack of senior buy-in are acting as a brake on adoption. Additionally, we identified differences of opinion among the various roles that influence cybersecurity strategy and tactical approach.

HIGH LEVEL FINDINGS

68%
say automation is important

98%
have increased their automation budgets

97%
experienced problems

21%
say technology issues are preventing automation

The full research report covers analysis based on vertical, region and role, and provides recommendations for security professionals to help improve the effectiveness and efficiency of cybersecurity automation. Download a copy of the State of Cybersecurity Automation Adoption Research report **here**.

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

Sales@ThreatQ.com • 703.574.9885