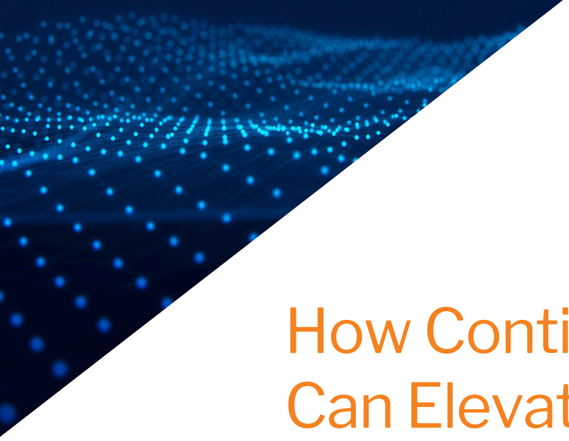


451 Research
Now a Part of
S&P Global Market Intelligence

Business Impact Brief

How Continuous, Automated Red-Teaming Can Elevate Your Security Posture

The 451 Take

Most enterprise security teams struggle to confidently answer key questions about their organization's security posture. For example: What threats or attacks would have the greatest impact on our business if they were to occur? Where are the unknown risks and vulnerabilities in our environment, and what would it take to eliminate them? How have daily infrastructure changes, digital transformation initiatives and the evolving threat landscape impacted our security posture and resilience?

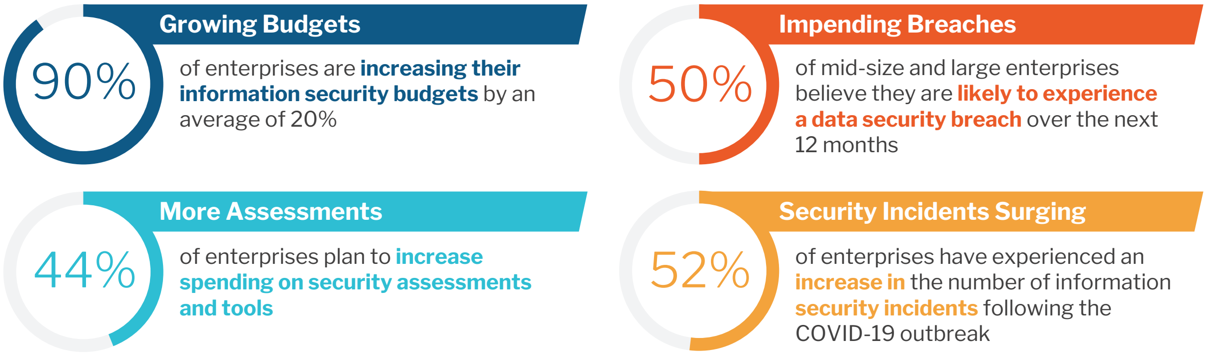
The inability to answer these questions is fueling increased spending as many enterprises try to outspend cybersecurity challenges by investing in more tools, people and assessments. Over 90% of enterprises report that they are planning to increase security budgets for 2020 by an average of 20% (451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2020 survey). Those expectations may have been underestimated as the global pandemic has driven many enterprises to increase security spending even further to protect the exploding number of remote workers.

Enterprises are discovering that this spending strategy isn't working, and budget pressures are rising. And even though enterprises continue to increase their security budgets year after year, half of midsized and large enterprises believe they will experience a data security breach in the next 12 months. Several factors are fueling these notions. Enterprise digital transformation and modernization initiatives are a primary factor, especially as organizations adopt new technologies and computing paradigms faster than security teams can adapt to secure and protect evolving environments. At the same time, the threat landscape continues to grow, and attacks are escalating. For example, 52% of enterprises report they have experienced an increase in the number of security incidents following the COVID-19 outbreak.

Compounding these factors, the tools and technologies that organizations have deployed to protect their critical assets have resulted in additional complexity. This complexity often decreases the effectiveness of the organization's security posture while increasing security gaps, exposures and costs.

Increasing Budgets, Growing Threats

Source: 451 Research's Voice of the Enterprise, Information Security, Budgets and Outlook, 2020; 451 Research's Voice of the Enterprise, Information Security, Organizational Dynamics, 2019; and 451 Research's Voice of the Enterprise, Digital Pulse, Coronavirus Flash Survey, June 2020



Growing Budgets

90% of enterprises are **increasing their information security budgets** by an average of 20%

Impending Breaches

50% of mid-size and large enterprises believe they are **likely to experience a data security breach** over the next 12 months

More Assessments

44% of enterprises plan to **increase spending on security assessments and tools**

Security Incidents Surging

52% of enterprises have experienced an **increase in** the number of information **security incidents** following the COVID-19 outbreak

Recognizing that they can no longer maintain the status quo and still secure the organization, enterprises are looking for help to gain insights into their security posture and better understand how they can construct a more resilient cybersecurity program. Many enterprises rely on compliance-focused third-party assessments and audits like penetration testing to evaluate the organization's defenses. However, these engagements are a point-in-time assessment, constrained by scope and limited by the amount of time, resources and expertise allocated to the assessment.

The 451 Take (continued)

Many enterprises are seeking to build out internal red teams or engage with a third party for a red-team assessment or exercise. Red-team exercises validate and stress-test an organization's overall security program effectiveness, leveraging wide and deep attack paths, sophisticated scenarios and adaptable techniques. These exercises not only reveal the weaknesses in an organization's security stack but also test its detection and response capabilities. However, building and funding a red team is beyond the reach of most enterprises. And, like other assessments, third-party red-team exercises are point-in-time engagements, limited by time, resources and expertise.

Continuous, automated red-team solutions can address many of these challenges, providing organizations with ongoing insights to validate and improve their security posture, better prioritize security investments and ensure that a security program is resilient enough to counter inevitable attacks and evolving threats.

Business Impact

VALIDATE AND IMPROVE SECURITY POSTURE. By discovering and exploiting the weaknesses of the enterprise's security stack and also those of service providers (e.g., MSP, MSSP, MDR), organizations can continuously measure the potential impact of a broad range of attack vectors and persistently test the resilience and effectiveness of their security posture. These insights empower security teams to answer critical questions such as: Where are our security gaps? Is our security infrastructure keeping pace with adversarial tactics? How vulnerable are we to specific attacks and threats? Are we prepared to detect and respond to the latest attacks? Are our security controls working as intended? Can we disrupt an adversary before a breach occurs?

PRIORITIZE AND MEASURE SECURITY INVESTMENTS. Providing an authentic adversarial assessment, automated red-teaming validates and tests the security stack as a whole, as well as specific controls, enabling enterprises to continuously evaluate and measure the effectiveness of existing security investments. With these insights, security teams can benchmark security initiatives, discover ineffective controls and processes, optimize existing technology investments, and determine where additional security investments are needed to deliver the greatest impact to the organization's risk profile.

PREPARE AND PRACTICE. Testing the organization's response to a cybersecurity incident before having to react to one in real time is key to a successful response. While every incident and attack is different, organizations must have confidence that their programs are prepared and ready to respond to evolving threats. With automated red-teaming, enterprises can continually test the impact of attacks at both the strategic and tactical levels, providing insights into response plans, tactics, people and processes.

Looking Ahead

As organizations continue to transform and modernize, security teams will continue to deal with constant change, increased risk, more data to decipher, more competing priorities and a broader attack surface to protect. At the same time, the enterprise's digital footprint is becoming more disparate and diverse, making it more difficult for cybersecurity teams to ensure that every critical asset, digital process and innovation is protected against the latest threats and attacks.

Security teams are recognizing that this continuously evolving IT ecosystem demands a shift in tactics. Continuous, automated testing can help enterprises adopt a risk-based and adversary-focused security approach to ensure that they are prepared to defend against the evolving threat posed by the adversaries relentlessly targeting their organizations.