4 KEY PRIORITIES FOR SECURITY LEADERS

Major cybersecurity challenges and how to alleviate them with BAS

KEEPING PACE WITH AN EVER-CHANGING THREAT LANDSCAPE

Digital transformation, rising cloud adoption, and remote working continue to create new cybersecurity risks.

A proactive approach to exposure management is vital to identify and address weaknesses before adversaries can exploit them.

$3.6M

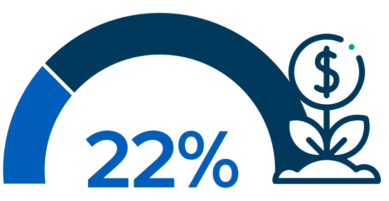
the average estimated cost of a cyber-attack.

World Economic Forum

MAXIMIZING AND RATIONALIZING CYBER INVESTMENTS

The importance of defending against evolving threats has led to the use of more and more security controls. However, more controls does not guarantee greater resilience.

Before investing in new tools, obtaining the best protection from existing ones is essential to maximize ROI and avoid creating additional strain on security operations.



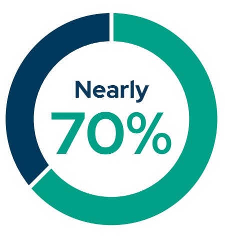
of organizations can quantify in financial terms the effectiveness of their cybersecurity spending.

Gartner

ALLEVIATING MANUAL WORKLOADS

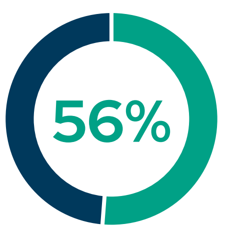
Skills shortages and increasing workloads mean burnout is a real risk for all security professionals.

Reducing manual tasks and alert fatigue is essential to ensure security teams' well-being and make operations more efficient.



of professionals feel their employers are not doing enough to prevent or alleviate burnout within their organization.

Deloitte



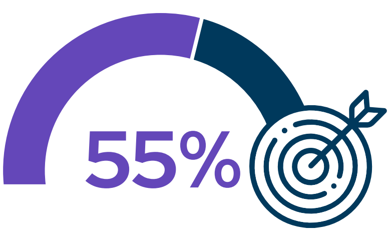
of security professionals believe that threat data is too voluminous and complex to offer timely and actionable intelligence.

Ponemon Institute

COMMUNICATING RISK TO THE BUSINESS

To demonstrate assurance and value, security leaders must ensure they can translate cyber risk into business risk.

Obtaining the right metrics to evidence an organization's threat readiness and demonstrate the need for new investments is imperative.



of security experts lack confidence that cyber spending is aligned to the most significant risks that their organization faces or will face.

PWC

HOW BREACH AND ATTACK SIMULATION (BAS) CAN HELP

1 SIMULATE THREATS CONTINUOUSLY

With BAS, go beyond traditional point-in-time assessments and continuously validate your organization's security posture.

By simulating-real world cyber threats, a BAS solution can help you to measure the effectiveness of your security controls, identify attack paths to critical assets, and optimize prevention and detection capabilities.

2 OPTIMIZE SECURITY CONTROLS

Use the results of attack simulations to identify threat coverage gaps and get actionable insights to prioritize risks and take mitigating actions.

BAS solutions can integrate with your existing controls to identify ineffective prevention and detection policies. Some solutions even provide vendor-specific prevention signatures and detection rules to make addressing policy gaps quick and easy.

3 VALIDATE SWIFTLY USING AUTOMATION

A BAS solution automates manual validation processes to reduce fatigue and help your security teams work together more collaboratively.

With BAS, spend less time identifying issues and more time prioritizing and mitigating them. It acts as a force multiplier across security operations, enabling you to achieve greater impact for less effort.

4 QUANTIFY REPORTING AND DEMONSTRATE COMPLIANCE

With BAS, get real-time metrics to measure your organization's threat readiness and make data-driven decisions.

Dashboards and reports enable you to measure the effectiveness of your security controls over time and share updates with internal stakeholders and auditors.

Test Your Defenses Against the Latest Threats

START YOUR FREE TRIAL

PICUS

www.picussecurity.com

picussecurity