SPONSORED CONTENT | WHITE PAPER

CISO Handbook:

Demonstrate the Effectiveness of Your Security Programme With BAS

How Breach and Attack Simulation technology enables you to measure and strengthen cyber resilience by validating the performance of your security controls, 24/7.

CSO

SPONSORED BY PICUS

CISOs Globally Are Facing A Major Cyber Security Dilemma

Due to the complexity of emerging threats, they often struggle to determine how secure they are at any given moment or if the security they have in place is working as expected.

New threats appear on an almost daily basis. On top of this, trends such as digital transformation and growing cloud adoption change infrastructure daily. There are also new assets being added to networks, and configuration changes. These activities create gaps for attackers to exploit.

Organisations have security controls in place to scan vulnerabilities and monitor for breaches. But security teams are deluged daily by the sheer number of vulnerabilities that they must patch and the number of alerts that detection technologies such as SIEM tools can generate. Many metrics that security controls generate may be misleading, providing a false sense of security.

What Is BAS And How Does It Help CISOs Measure Effectiveness?

Initially coined by Gartner in 2017, Breach and Attack Simulation (BAS) technology is used to validate if security controls detect and respond to attacks as they should. The analyst firm defines these tools as ones, "that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines and other means".

Some BAS tools concentrate on attack path management (to help organisations visualise the routes attackers take inside a network to compromise users and assets). However, the primary use case for BAS is Security Control Validation (SCV).

Many metrics that security controls generate may be misleading, providing a false sense of security.

With a BAS tool that specialises in SCV, organisations can constantly monitor their security posture on a 24/7 basis as well as obtain quantifiable metrics to measure and optimize threat prevention and detection capabilities.

The Need For Reliable Metrics

Security teams are struggling to understand the effectiveness of their security posture.

CISOs may not have the best information on hand to present to the board when questions are asked about security - the last place any CISO wants to be.

CISOs are routinely asked the question, 'are we protected against x?' Being able to answer this question and supply quantifiable metrics to support the answer is more essential than ever. Cybersecurity is now a business-level concern and budgets are under scrutiny. According to a survey by analyst firm Gartner, 88% of board members view cybersecurity as a business risk, as opposed to a technology risk.

Traditional metrics used to measure effectiveness (e.g., patched vulnerabilities, alerts and incidents) are unreliable. They do not provide a

full and up-to-date picture and are only useful to assess what is 'known' rather than 'unknown' (e.g. emerging threats using new techniques).

We assume (or hope!) that investments are providing protection against current and emerging threats but without the ability to obtain a real-time view and more reliable data it's hard to know for sure. There is a real risk of discovering coverage gaps only once it's too late.

Why Security Control Validation?

The solution to increasing reliability when measuring security posture is to validate the effectiveness of security controls. Using BAS to simulate attacks to identify coverage and visibility gaps enables organisations to quantify threat readiness and take more effective action to mitigate risks.

BAS not only assists in validating security control effectiveness but also helps organisations become more proactive in their approach to information security by automating costly manual processes.

While there is no such thing as 100 per cent assurance, what BAS does is eliminates assumptions. BAS puts security controls through their paces so that security teams can optimise them to achieve the best possible protection.

Real-time dashboards can help in visualising a security score for every control an organisation has.

The Key Benefits Of BAS

1 Quantifies The Effectiveness Of Existing Security Controls

Many organisations have around 30 to 70 security tools in their stack but in most cases, they just don't know if they are working effectively. A good BAS solution can help organisations test and measure the ability of their security controls to prevent and detect threats as well as deliver actionable mitigation recommedations to help mitigate coverage and visibility gaps.

As the attack surface of organisations increases, with more companies using cloud computing, remote working, and Internet of Things (IoT), there are more challenges to overcome. Misconfiguration of infrastructure and security tools can occur any time and can make any results of annual penetration testing and red teaming exercises obsolete, leaving gaps for attackers to exploit. With BAS, CISOs can get a better idea of their security posture by obtaining metrics to assess the effectiveness of security controls to prevent, detect and respond to attacks.

2 Helps Maximise The Performance Of Investments

Many boardrooms now understand the value of investing in cyber security, but CISOs also need to demonstrate the cost-effectiveness of the security controls they use to achieve optimal return on investment (ROI). Spending needs to be focused in the right areas, but without the right data to support decision making, it can be easy to waste money.

You can better understand your security posture with Picus

BAS tools quantify the performance of tools individually and collectively. They also provide actionable mitigation recommendations to help make it easier to optimize their performance.

3 Reduces Manual Assessment Processes

Security Operations Centres (SOC) are facing ever increasing cyber-attacks, both in volume and severity. Teams are suffering 'alert fatigue', an issue often caused by misconfigured and poorly used security controls. Without well-tuned security systems in place, SOC analysts may well miss clues that point to serious breaches.

A BAS platform can simulate thousands of attacks and attack scenarios to find weaknesses and misconfigurations in Security Incident and Event Management (SIEM) and Endpoint Detection & Response (EDR) tools and provide actionable mitigation recommendations to help quickly address gaps and minimise noise. A BAS Tool that provides prevention signatures and detection rules will significantly reduce manual engineering processes.

4 Enhances Readiness Against The Latest Threats

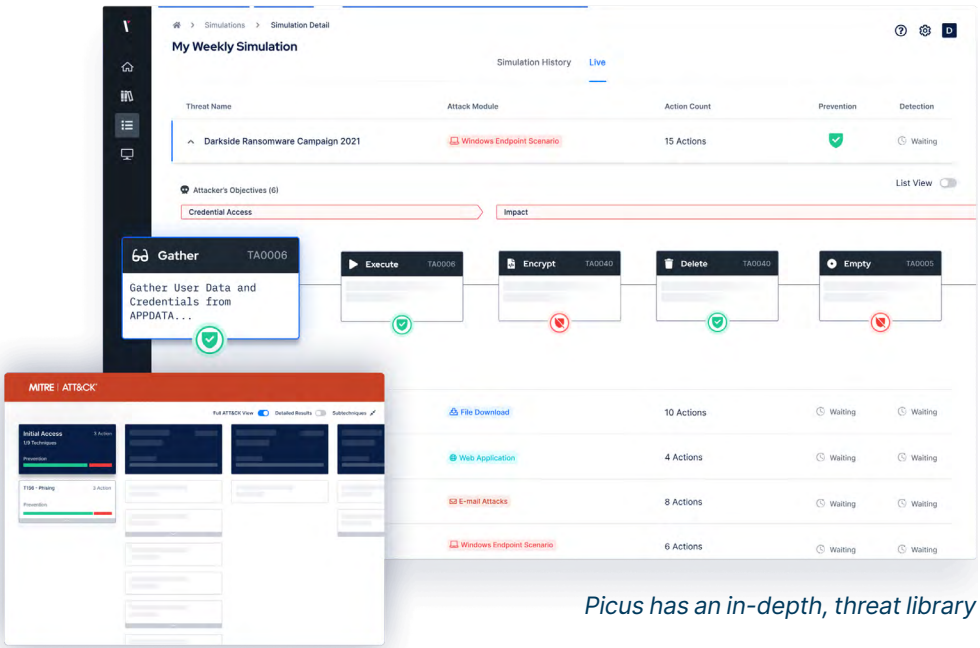
A BAS tool should be able to provide a constantly updated threat library that can collect threat data from a wide variety of sources such as commercial and open-source threat intelligence services, security vendors, researchers, malware sandboxes, and forums. BAS platforms can provide recommendations around mitigations that organisations can take to protect infrastructure against sustained attacks and quickly address gaps.

Cybersecurity is now a business-level concern and budgets are under scrutiny. According to a survey by analyst firm Gartner, 88% of board members view cybersecurity as a business risk, as opposed to a technology risk.

5 Demonstrates Assurance To Stakeholders (Internal And External)

BAS is about quantifying risk. Real-time dashboards can help in visualising a security score for every control an organisation has. Thus, CISOs can measure improvements to those scores as they increase. Dashboards can also display not just individual controls but also show how controls are working together. On top of dashboards, BAS platforms can generate executive reports that provide a summary of activities to the board and C-suite executives. These reports can also show the simulations that have been carried out in a particular environment as well as risk scores. The reports can also be used to measure the performance of security controls over time.

Breaches can also cause legal and compliance issues. Many organisations must comply with national, supra-national, and industry-enforced regulations related to privacy and similar. For instance, the General Data Protection Regulation (GDPR) requires that organisations must have a “process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures.” Other regulations, such as ISO-27001, PCI DSS and frameworks such as NIST 800-53, have comparable requirements. Any robust BAS solution will help CISOs to understand whether critical assets are protected and whether threats could lead to breaches and the loss or encryption of sensitive personal and financial data.



Picus has an in-depth, threat library

What Is The Picus Approach To BAS?

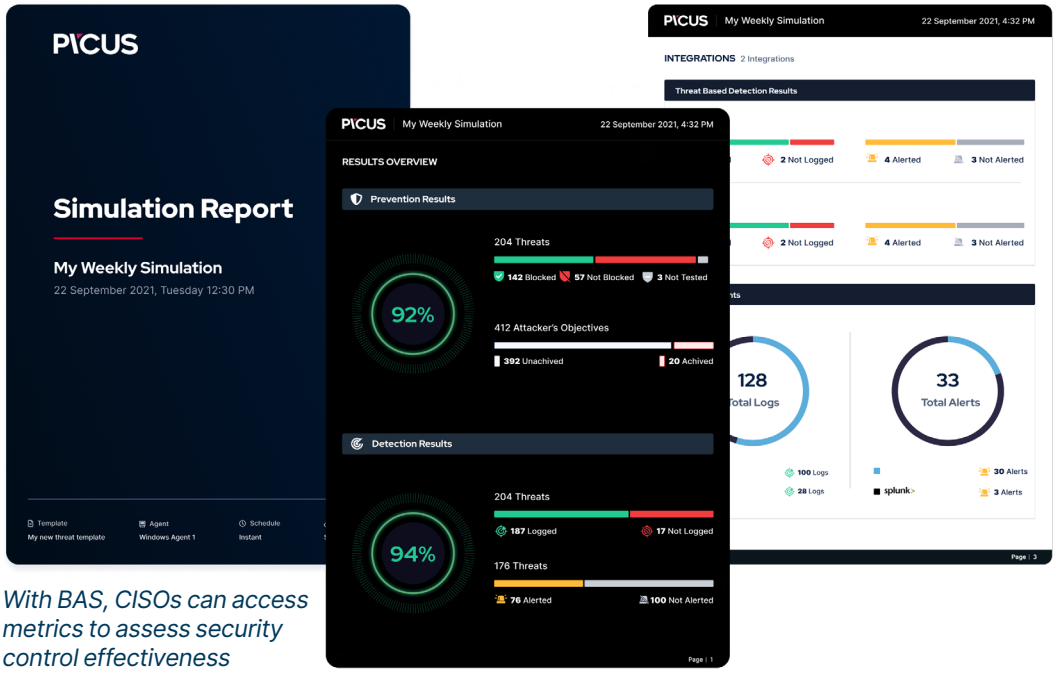
Security leaders can attest to the value of The Picus Complete Security Control Validation Platform.

“The Picus Platform is an easy to use solution that helps us ensure our defences keep pace with evolving threats. The scores and insights it provides help us to assess the effectiveness of our controls and identify ways to better protect our assets and customer data,” adds Elif Seven, Senior Security Manager at Migros.

The Picus Platform provides measurable context about accounts, behaviour, and approaches of attackers by running a widespread set of cyber-threats and attack scenarios on an uninterrupted basis and in production networks.

It has an in-depth, threat library with over 3,600 real-world threats that are updated daily, and adversary-based attack scenarios and techniques mapped to the MITRE ATT&CK framework. The Picus platform simulates web application attacks, email attacks, malware attacks advanced endpoint scenarios, and more

The Picus Platform also provides actionable, vendor-specific mitigation recommendations tailored to organisations and their defences.



With BAS, CISOs can access metrics to assess security control effectiveness

Conclusion

CISOs are facing up to a new paradigm in cybersecurity. They must make decisions in an ever-changing threat landscape to protect their businesses from highly damaging attacks that can shut down key systems. But they must also now be able to measure the effectiveness of their security controls at a time when security teams can feel deluged by a multiplicity of alerts.

In addition to this, business processes, configuration changes, and security updates can all introduce vulnerabilities into the IT infrastructure. With a better understanding of their organisation's threat readiness at any moment in time, CISO's are better placed to answer important security questions and have greater confidence that controls are operating as they should be.

Moreover, automating the process of security control validation using BAS can alleviate fatigue and allow the security team to focus efforts on other critical responsibilities. By using BAS platforms, CISOs can ensure security controls are validated and remain in compliance with an organisation's processes and key regulations. It also ensures that those existing investments are giving organisations the best protection possible.

Validating security controls can also help CISOs demonstrate the effectiveness of their current security programme which can help in making a case for additional spending in the right areas. BAS offers a comprehensive solution to the core challenges facing security teams in an era where business are both digitally transforming while facing an unpredictable threat landscape.