

Proficio® ProBAS Breach and Attack Simulation

With cyber incidents increasing in both complexity and frequency, organizations face numerous challenges. From ransomware attacks disrupting major fuel pipelines to phishing scams targeting remote workforces, the attack arsenal used by cybercriminals is becoming more diverse and sophisticated. This unpredictable landscape demands dynamic and robust security strategies capable of not only responding to threats but anticipating them.

ProBAS rigorously tests your security defenses to ensure they can protect against compromised events and detect attacks throughout the entire threat and detection process. From device alert logs to SIEM, SOC detection, and containment response actions, ProBAS covers every aspect. With ProBAS, cybersecurity teams can rest easy, confident that attacks will be detected and contained by their security team or their SOC partner after testing thousands of scenarios.

ProBAS is a cutting-edge cybersecurity solution designed to assess and enhance the effectiveness of an organization's security defenses.

ProBAS Features and Benefits

- **Real-World Attack Simulations:** From phishing to advanced persistent threats (APTs), ProBAS covers a comprehensive range of attack vectors, ensuring robust defense against thousands of scenarios.
- **Continuous Security Validation:** ProBAS operates round the clock, identifying security leaks and vulnerabilities in real time before they can be exploited.
- **Enhance Accuracy:** Reduces false positives and increases detection accuracy, ensuring that security teams can focus on true threats.
- **Gain Actionable Insights:** Receive detailed reports accompanied by contextual mitigation recommendations tailored to your specific security infrastructure.
- **Improve Detection and Response:** Integrates with existing security tools like SIEM, SOAR and EDR to significantly enhance detection and response capabilities, potentially reducing incident response times by up to 50%.
- **Assure Compliance:** Regularly validate that your security measures meet industry standards and compliance requirements, ensuring regulatory adherence.

How It Works

ProBAS provides a comprehensive solution for bolstering your organization's cybersecurity defenses by incorporating both internal and external security simulations as well as vulnerability assessments.

Internal & External Security Simulations

Drawing on real-world Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK® and Cyber Kill Chain® frameworks, ProBAS mimics both outsider and insider threat behaviors. This tests how well your current security infrastructure, security teams, or SOC partner can detect and respond to attacks.

Security Validation and Vulnerability Assessments

ProBAS isn't penetration testing. It continuously scans and analyzes the external attack surface to identify and remediate vulnerabilities that could be exploited by external actors. This dual approach enhances the detection of potential security gaps, facilitates a more strategic and proactive response to threats, and allows security teams to prioritize risks and vulnerabilities more accurately, ensuring that resources are allocated efficiently to address the most critical security needs. As a result, organizations can achieve a more dynamic and resilient cybersecurity framework, better equipped to handle the rapidly evolving landscape of cyber threats.

Detailed Reporting and Remediation Guidance

After each simulation exercise, ProBAS provides detailed reports outlining:

- **Network Security Controls:** Efficacy of firewalls and other network barrier tools.
- **Endpoint Detection and Response (EDR):** Robustness of endpoint security solutions.
- **Email Security Controls:** Ability to ward off email-based threats.
- **Access Control Measures:** Strength of mechanisms preventing unauthorized access.
- **Vulnerability Management Policies:** Adequacy of policies designed to find and fix security flaws.
- **Data Security Controls:** Security of critical data assets.
- **Incident Response Controls:** Preparedness and speed of the incident response team.

Comprehensive Simulation Approach

ProBAS simulates a variety of attack paths, vectors, and scenarios:

- Network and Infiltration Attacks
- Lateral Movement
- Phishing
- Endpoint and Email Gateway Attacks
- Malware and Ransomware Attacks
- Network IDPS/Firewalls
- URL Testing
- Web Application Firewall (WAF) Testing
- Endpoint Security Testing

As cyber threats evolve, so must our approaches to security. ProBAS represents more than a technological solution; it is a strategic ally in the ongoing battle against cyber threats. By simulating attacks and testing defenses continuously, ProBAS ensures that your organization remains several steps ahead of potential attackers. Embrace the future of cybersecurity with ProBAS and transform your security posture from reactive to proactive.

Ready to redefine your cybersecurity strategy with ProBAS?

Contact us today to learn how our Breach and Attack Simulation solutions can fortify your defenses and secure your business against the unforeseen threats of tomorrow.



Proficio is an award-winning managed detection and response (MDR) service provider that helps prevent cybersecurity breaches by performing and enabling responses to cyber-attacks, compromises, and policy violations. Recognized in Gartner's Market Guide for MDR services annually since 2017, Proficio's experts provide 24/7 security monitoring and alerting from global security operations centers (SOCs) in San Diego, Barcelona and Singapore.

Ready To Get Started? Request a Demo

[GET STARTED](#)

proficio.com | info@proficio.com | +1 800.779.5042